University of California

Santa Barbara

Trace Zero Points on Elliptic Fibrations

A dissertation submitted in partial satisfaction

of the requirements for the degree

Doctor of Philosophy

in

Mathematics

by

Nadir Hajouji

Committee in charge:

Professor David Morrison, Chair

Professor Adebisi Agboola

Professor Bill Jacob

June 2020

The dissertation of Nadir Hajouji is approved.

Professor Adebisi Agboola

Professor Bill Jacob

Professor David Morrison, Chair

May 2020

Trace Zero Points on Elliptic Fibrations

Acknowledgements

I'd like to thank my advisor and committee, Steve Trettel, Paul Konstantin-Oehlmann, etc.

NADIR HAJOUJI

ADDRESS
385 Northgate Dr C
Goleta, CA
(206) 856-8713
hajouji@math.ucsb.edu

EDUCATION

University of California at Santa Barbara
Santa Barbara, CA
PhD in Mathematics
June 2020

University of California at Santa Barbara
Santa Barbara, CA
Master of Arts in Mathematics
July 2016

Reed College
Portland, OR
Bachelor of Arts in Mathematics
December 2012

EMPLOYMENT

Teaching Assistant — University of California, Santa Barbara, Santa Barbara, CA — Fall 2014 to Present

Courses included *Transition to Higher Mathematics*, *Calculus II*, *Vector Calculus II*, *Advanced Linear Algebra I*. Responsible for leading 4 discussion sections a week, holding office hours, grading exams.

REU Mentor — University of California, Santa Barbara, Santa Barbara, CA — Summer 2019

Designed research project and mentored 4 undergraduates in a summer REU program.

Instructor — University of California, Santa Barbara, Santa Barbara, CA — Summer 2018

Instructor of record for *Calculus for the Social Sciences I*.

Tutor — Varsity Tutoring, Seattle, WA — Oct. 2013 to Apr. 2014

Math and French tutor for high school and college students.

Tutor — Frog Tutoring, Seattle, WA — Sept. 2013 to Apr. 2014

Math tutor for high school and college students. Responsible for designing a customized lesson plan for the student, communicating with student's teacher.

Independent Tutor — Reed College, Portland, OR — Sept. 2011 to Dec. 2012

Tutor for all math classes with a tutoring component and 300-level French Stylistics and Composition class.

Math Center Tutor Reed College, Portland, OR — Sept. 2011 to Dec. 2012

Worked primarily with freshmen and sophomores on core math classes.

Grader Reed College, Portland, OR — Sept. 2011 to Dec. 2012

Graded Multivariable Calculus I & II for Prof. Jerry Shurman.

PUBLICATIONS

Hajouji, N., Oehlmann, P. *Modular curves and Mordell-Weil torsion in F-theory.* J. High Energ. Phys. **2020**, 103 (2020).

WORKSHOPS ATTENDED

Illustrating Number Theory and Algebra — October 2019
ICERM, Providence, RI

Note: Presented poster *Modular Curves and Mordell-Weil Torsion in F-Theory.*

Workshop on Diophantine Geometry & Special Varieties — September 2019
Trento, Italy

F-Theory Workshop — April 2019
Florida State University, Tallahassee, FL

Physics and Mathematics of F-Theory

Summer School in Arithmetic Geometry — September 2018
Essen, Germany

Periods, Moduli Spaces and Arithmetic of Algebraic Varieties

Summer School in Arithmetic Geometry — September 2018
Salerno, Italy

BIRS 5-Day Workshop — January 2018
BIRS, Banff, AB

Geometry and Physics of F-Theory

MSRI Graduate Summer School — May 2017
MSRI, Okinawa, Japan

Commutative Algebra

Arizona Winter School — March 2017
University of Arizona, Tucson, AZ

Perfectoid Spaces

MSRI Graduate Summer School July 2016
MSRI Berkeley, CA

An Introduction to Character Theory and the McKay Conjecture

FRG Mini-workshop February 2016
University of Utah Salt Lake City, UT

Unramified Cohomology, Derived categories, and Rationality.

Outreach/Miscellaneous

Supervising a senior capstone project (2019-2020).

Mentor at the Direct Reading Program at UCSB (Fall 2018-Present)

Notetaker for:

RTG Seminar - (UCSB - Winter '16 - Present)

JAMI 2017 - *Local zeta functions and the arithmetic of moduli spaces: A conference in memory of Jun-Ichi Igusa* (Baltimore, MD - March 2017)

Fluent in French

Abstract

Trace Zero Points on Elliptic Fibrations

by

Nadir Hajouji

The goal of this dissertation is to develop tools for studying genus one fibered Calabi-Yau 3-folds without section, with an eye towards applications in F-theory.

In particular:

- Locally trivial fibrations are well-understood via the work of Mark Gross and others - we know that there are only finitely many families parametrizing all of them, we know they are classified by the Tate-Shafarevich group and we can use Ogg-Shafarevich theory to classify all such fibrations with a common Jacobian.

- Since we have an genus one fibration structure, we can always find an equation describing the generic fiber as a genus one curve in some projective vector bundle. Furthermore, we can obtain an equation for the Jacobian from an equation for the torsor.

The work of Mark Gross is especially relevant and helpful, but it has two shortcomings:

- It can only be used to classify fibrations whose geometry is reasonably nice - it requires a smooth base, with a simple normal crossings divisor, and only classifies fibrations without multiple fibers.

  We will see that there are fibrations which simultaneously fail all of these conditions.

- It is important to be able to relate arithmetic phenomena to degenerations on elliptic fibrations in every possible codimension. Purity for the Brauer group means we shouldn't expect to gain precise information about degenerations in codimension 2.

The Jacobian formulae can be used to obtain information about codimension 2 singularities by brute force. However, the problem there is that the formulae become too messy to actually be used to analyze codimension 2 singularities.

In Part I and Part II, we go over the necessary background. In Part III, we begin our analysis of torsors.

We start by reviewing the theory of torsors of index 2 and 3. We will see that the data of the torsor can be recovered from the data a *trace zero point* on the Jacobian.

In the final chapter, we propose using *trace zero varieties* as a tool for studying torsors in general, and explain why this approach is well suited for answering some outstanding questions in F-theory.

- Trace zero points are part of the data used to study torsors in either of the other two settings. If we have a class in Ш, it can be represented by a cocycle, and the cocycle is determined by a set of trace zero points.

- Trace zero points are easy to parametrize. In the final chapter, we construct a variety that parametrizes pairs consisting of an elliptic curve and a point of trace zero on that elliptic curve.

- Trace zero points can be thought of as a generalizing of torsion points. We have a good understanding of moduli space for torsion pairs, and in fact we will use those moduli spaces to bound torsion on elliptically fibered Calabi-Yau 3-folds.

  We will also explain how we hope to use these ideas in future work in the last chapter.

Contents

List of Figures

Part I

Background

Chapter 1

Varieties and Schemes

In this chapter we collect basic definitions and theorems from algebraic geometry and commutative algebra that will be used frequently in the remainder. More details on these topics can be found in [36].

1.1 Varieties and Schemes

Let k be a field. When we say X is a variety over k, we will mean that X is one of the following:

- An affine variety is a subset of k^n of the form:

$$X = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

  where $I \subset k[x_1, \ldots, x_n]$ is an ideal.

- A projective variety is a subset of $\mathbb{P}^n_k$ of the form:

$$X = \{[a_0 : a_1 : \ldots, a_n] \in \mathbb{P}^n_k : f(a_0, a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

where $I \subset k[x_0, x_1, \ldots, x_n]$ is a homogenous ideal.

Every projective variety has an open cover consisting of affine varieties, and which can be obtained by restriction to the standard affine opens of $\mathbb{P}^n_k$. Conversely, every affine variety can be "projectivized":

- We start by choosing polynomials $f_1, \ldots, f_r$ defining X in k^n, and we fix an embedding $k^n \to \mathbb{P}^n_k$, usually $(a_1, \ldots, a_n) \mapsto [1 : a_1 : \cdots : a_n]$.
- Let d_i be the total degree of f_i, and define:

$$F_i(x_0, \ldots, x_n) = x_0^d f_i(x_1/x_0, \ldots, x_n/x_0).$$

  Then F_i is a homogenous polynomial of degree d, and:

$$F_i(1, x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n).$$

The variety in $\mathbb{P}^n$ defined by $F_1, \ldots, F_r$ intersects the image of k^n in $\mathbb{P}^n$ at X.

An (abstract) affine scheme over k is Spec R for a Noetherian k-algebra R. A scheme over k is a space which is a space obtained by gluing together affine schemes. We will mainly be interested in varieties, so we will not review what it means to glue together schemes. However, this is a good time to mention the following classical result:

Proposition 1.1. *Let S be a topological space, let $\cup U_i$ be an open cover of S and suppose we have sheaves $\mathcal{F}_i$ for each U_i.*

We write S_{ij}, S_{ijk} for the intersections $S_i \cap S_j$, $S_i \cap S_j \cap S_k$, respectively.

Then there exists a sheaf $\mathcal{F}$ on S such that $\mathcal{F}|_{U_i} = \mathcal{F}_i$ if and only if:

- *For all i, j, there exist isomorphisms $\phi_{ij} : \mathcal{F}_i|_{S_{ij}} \to \mathcal{F}_j|_{S_{ij}}$ for all i, j.*

- *For all i, j, k, the following condition is satisfied:*

$$\phi_{ik} = \phi_{jk} \circ \phi_{ij}$$

Furthermore, if such a sheaf exists, then it is unique up to isomorphism.

See [11] for a proof.

This theorem is crucial to the construction of many of our main tools.

- We use it to identify $Pic(X)$ with $H^1(X, \mathbb{G}_m)$ in sheaf cohomology.
- The theorem can also be used to prove that twists are classified by $H^1(G, Aut(X))$ in Galois cohomology, see e.g. Ch. 4 of [55].

Definition 1.2. *Let X be a scheme over k and R a k-algebra.*

A k-point on X is a morphism Spec$k \to X$. *An R-point on X is a morphism* Spec$R \to X$. *The set of R-points on X will be denoted $X(R)$.*

Note that k-points on Spec$k[x_1, \ldots, x_n]/I$ are in bijection with points $(a_1, \ldots, a_n) \in k^n$ in the zero set of I, so this definition generalizes the intuitive notion of "point on a variety".

Definition 1.3. *Let X/k be an affine variety, say the zero set of $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ in k^n. Let $p = (a_1, \ldots, a_n) \in X(k)$. We say that X is smooth at p if the matrix:*

$$\begin{pmatrix} \left(\frac{\partial}{\partial x_1} f_1\right)(a_1, \ldots, a_n) & \ldots & \left(\frac{\partial}{\partial x_n} f_1\right)(a_1, \ldots, a_n) \\ \vdots & & \vdots \\ \left(\frac{\partial}{\partial x_1} f_r\right)(a_1, \ldots, a_n) & \ldots & \left(\frac{\partial}{\partial x_n} f_r\right)(a_1, \ldots, a_n) \end{pmatrix}$$

has maximal rank. We say that X is smooth if X is smooth at every point $p \in X(k)$.

Definition 1.4. *Let R be a Noetherian k-algebra of Krull dimension d. Let $\mathfrak{m}$ be a maximal ideal, and let $R_{(\mathfrak{m})}$ be the local ring at $\mathfrak{m}$.*

We say that R is regular at $\mathfrak{m}$ if $\mathfrak{m}$ can be generated by d elements of $R_{(\mathfrak{m})}$. We say that R is regular if it is regular at every maximal ideal.

Finally, we say that a scheme X is regular if X is a union of affine schemes Spec$R$ *with R a regular ring.*

Smoothness and regularity essentially capture the same idea:

Proposition 1.5. *Let k be a perfect field, $R = k[x_1, \ldots, x_n]/I$, $\mathfrak{m}$ a maximal ideal in R and $R_{(\mathfrak{m})}$ be the local ring at $\mathfrak{m}$. Let $X \subset k^n$ be the variety defined by I, and let $p \in X(k)$ be the point associated to $\mathfrak{m}$.*

Then X is smooth at p if and only if $R_{(\mathfrak{m})}$ is a regular local ring.

Proof. [18] □

1.2 Derivations and Canonical Bundle

Let R be a k-algebra.

Definition 1.6. *Let M be an R-module. A k-derivation of R into M is a map $d : R \to M$ satisfying:*

- $d(rr') = rd(r') + r'd(r)$.
- $d(a) = 0$ *for all* $a \in k$.

There is an R-module $\Omega_{R/k}$ and a derivation $R \to \Omega_{R/k}$ that satisfies the following universal property: for every R-module M and every derivation $d : R \to M$, there is a unique R-module homomorphism $\Omega_{R/k} \to M$ making the following triangle commute:

The R-module $\Omega_{R/k}$ can "detect smoothness":

Proposition 1.7. *Let k be a perfect field, R a finitely generated k-algebra and $R_{(\mathfrak{p})}$ the local ring at some prime $\mathfrak{p} \subset R$. Let d be the Krull dimension of $R_{(\mathfrak{p})}$.*

Then $R_{(\mathfrak{p})}$ is a regular local ring if and only if $\Omega_{R/k}$ is a free R-module of rank d.

Proof. [36] Ch. II.Theorem 8.8 □

We can extend these definitions and results to general varieties by replacing modules with sheaves. The analog of the last proposition says that $\Omega_{X/k}$ is a locally free sheaf of rank equal to the dimension of X if and only if X is smooth.

Finally, we define the canonical bundle of X.

If X is smooth, this is straightforward:

Definition 1.8. *Let X/k be a smooth variety of dimension d. The canonical bundle of X, denoted ω_X, is the dth exterior power of $\Omega_{X/k}$:*

$$\omega_X := \bigwedge^d \Omega_{X/k}$$

Since $\Omega_{X/k}$ is locally free of rank d, ω_X is a line bundle on X. If X/k is a singular variety, the dualizing sheaf is a reasonable substitute for ω_X.

Proposition 1.9. *Let X/k be a proper variety.*

- *If X has a dualizing sheaf, then it is unique up to isomorphism.*
- *If X is projective, then a dualizing sheaf exists.*
- *If X is projective and has at worst Gorenstein singularities, then the dualizing sheaf is a line bundle.*

- *If X is a smooth, projective variety, then the dualizing sheaf is isomorphic to ω_X.*

Proof. See [36] for the definition and proof. □

We will tacitly be assuming that all varieties are Gorenstein, and denote the dualizing line bundle by ω_X.

1.3 Valuations

Let K be a field, and $(A, +, \leq)$ a totally ordered abelian group. Let $A' = A \cup \{\infty\}$, and extend the ordering on A to A' by declaring $a < \infty$ for all $a \in A$.

Definition 1.10. *A valuation on K with value group A is a map $\nu : K \to A'$ satisfying the following:*

- *$\nu(x) = \infty$ if and only if $x = 0$.*
- *The restriction $K^\times \to A$ is a surjective group homomorphism.*
- *For all $x, y \in K$:*

$$\nu(x + y) \leq \min\{\nu(x), \nu(y)\} \tag{1.1}$$

Furthermore, if $\nu(x) \neq \nu(y)$, then we have equality in 1.1.

For each valuation $\nu : K \to A'$ is a valuation, we define:

$$R_\nu = \{x \in K : \nu(x) \geq 0\}$$
$$\mathfrak{m}_\nu = \{x \in K : \nu(x) > 0\}$$

Then R_ν is a local ring with maximal ideal $\mathfrak{m}_\nu$. Next, we define valuation rings.

Definition 1.11. *Let K be a field and $R \subset K$ a subring. We say that R is a valuation ring if, for all $x \in K^\times$, $x \in R$ or $x^{-1} \in R$.*

Again, the definition of valuation guarantees that R_ν is a valuation ring. In fact, if $(R, \mathfrak{m})$ is a local ring with fraction field K, then R is a valuation ring.

In fact, one can show that these objects are essentially interchangeable - every valuation ring is local, and every local ring can be obtained from a valuation. This is all standard, but we review the construction of the valuation associated to a local ideal, as it is needed in many definitions later on.

Definition 1.12. *Let R be a commutative ring and I, J ideals. We write IJ to denote the ideal generated by products of the form xy with $x \in I, y \in J$.*

For each positive integer ℓ, we write I^ℓ for the ideal generated by products $x_1 x_2 \cdots x_\ell$ with $x_1, \ldots, x_\ell \in I$.

We will need the following result:

Lemma 1.13. *Let R be an noetherian integral domain and I a proper ideal. Then*

$$\bigcap_{\ell \geq 0} I^\ell = 0$$

Proof. Since I is proper, I is contained in some maximal ideal $\mathfrak{m}$, and since $I^\ell \subset \mathfrak{m}^\ell$, it suffices to prove the result for $\mathfrak{m}$.

Let $M = \cap_{\ell \geq 1} \mathfrak{m}^\ell$. Then $\mathfrak{m}M = \mathfrak{m}$, so by Nakayama's lemma, $M = 0$.

□

Now, let $(R, \mathfrak{m})$ be a Noetherian local ring and let $x \in R$ be a nonzero element. By the previous lemma, $\cap_\ell \mathfrak{m}^\ell = 0$ so $x \in \mathfrak{m}^\ell$ for only finitely many values of ℓ.

- We define $\nu_\mathfrak{m}(x) = \ell$, where ℓ is the largest nonnegative integer such that $x \in \mathfrak{m}^\ell$.

- For $\phi = \frac{x}{y} \in K^\times$, we define $\nu_{\mathfrak{m}}(\phi) = \nu(x) - \nu(y)$.

If $\mathfrak{m}/\mathfrak{m}^2 \neq 0$, this defines a valuation on $K^\times$ with value group $\mathbb{Z}$.

In general, we can start with an integral domain R of finite Krull domain and a prime ideal $\mathfrak{p} \in R$ and define $\nu_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ as we did above. If we then compute $R_{\nu_{\mathfrak{p}}}$, we recover the localization of R at $\mathfrak{p}$.

Finally, note that this definition also makes sense if we replace f by an ideal $I \subset R$ - we define $\nu_{\mathfrak{p}}(I)$ as the largest integer ℓ such that $I \subset \mathfrak{p}^\ell$. We will use this notation in the next section.

1.3.1 Discrete Valuation Rings

A discrete valuation ring is a noetherian valuation ring R satisfying one of the following equivalent conditions:

- R is a principal ideal domain.
- R is a regular local ring.
- Every ideal in R is of the form (ϖ^ℓ), where ϖ is a fixed nonunit in R and ℓ is a nonnegative integer.

The element ϖ is called a uniformizer. For an element $x \in R$, computing $\nu(x)$ boils down to determining the exponent of ϖ in a factorization of $x = u\varpi^\ell$, where $u \in R^\times$.

Discrete valuation rings are particularly easy to work with, and we can usually generalize many results about varieties over fields to varieties over discrete valuation rings without much trouble.

For example:

Lemma 1.14. *Let R be a DVR of characteristic 0, and let $f \in R[x,y]_d$ be a homogenous polynomial of degree d.*

Then there exists $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(R)$ *such that* $f(a_{11}x+a_{12}y, a_{21}x+a_{22}y) = c_0x^d + c_2x^{d-2}y^2 + \cdots$.

In other words, we can eliminate the coefficient of $x^{d-1}y$ without introducing denominators.

Proof. We start by taking care of some easy case.

- If $\nu(c_0) = 0$, then a is a unit in R, so we can use the matrix $\begin{pmatrix} 1 & -\frac{a_1}{d} \\ 0 & 1 \end{pmatrix}$ to eliminate the coefficient of $x^{d-1}y$.
- If $\nu(c_d) = 0$, we can act by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ to obtain a new equation with $\nu(c_0) = 0$.
- Suppose $\nu(c_0), \nu(c_d) \neq 0$ but $\nu(c_0) = \min\{\nu(c_i)\}$ (or $\nu(c_d) = \min\{\nu(c_i)\}$). Then we can factor out $\varpi^{\nu(c_0)}$ from $f(x,y)$ to obtain a new homogenous polynomial $\nu(c_0) = 0$.

  Since the action of $SL_2(R)$ commutes with multiplication by elements of R, we can use the same matrix we used for f_0 to eliminate the coefficient of $x^{d-1}y$ in f.

Finally, we should that we can reduce to the last case using an element of $SL_2(R)$. Let $m = \min\{\nu(c_i)\}$ and let $f_0 = \varpi^{-m}f(x,y)$.

Let $\overline{f_0}$ be the image of f_0 in $(R/(\varpi))[x,y]$. Then $\overline{f_0}(x,y) \neq 0$.

The polynomial $\overline{f_0}(x,1)$ has at most d roots in $R/(\varpi)$. Thus, there exists $t \in R$ such that $\overline{f_0}(t,1) \neq 0$.

Acting by the matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ gives us a new polynomial $g(x, y)$:

$$g(x, y) = c_0 x^d + \cdots + f_0(x, t) y^d$$

The coefficient of y^d is now a unit in R, so we can use the usual change of variable $y \to y + \lambda x$ to eliminate the coefficient of xy^{d-1} (and then act by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$).

□

Tate's algorithm (6.2.1) and the theory of Néron models (see 6.1) work best over Spec$R$, where R is a discrete valuation ring.

Indeed, many of the problems we have to deal with will stem from the fact that we have to work over rings which are not discrete valuation rings.

1.4 Rational maps

Let X, Y be schemes over k.

Definition 1.15. *A rational map $\phi : X \to Y$ is a morphism $\phi : U \to Y$ defined on a dense open set U of X. The domain of ϕ is the open set U.*

Definition 1.16. *Let $\phi, \tilde{\phi} : X \to Y$ be rational maps. We say that $\tilde{\phi}$ extends ϕ if the domain of ϕ is contained in the domain of $\tilde{\phi}$, and the restriction of $\tilde{\phi}$ to the domain of ϕ coincides with ϕ.*

Definition 1.17. *A rational map $X \to Y$ is dominant if the image is dense in Y.*

Dominant rational maps $X \to Y$ are in bijection with injections of the function field of Y into the function field of X.

1.4.1 Rational maps to $\mathbb{P}^1$

Let X/k be an integral scheme with function field K.

- Rational maps $X \to \mathbb{P}^1_k$ are in bijection with elements of K.
- Constant maps $X \to \mathbb{P}^1_k$ correspond to elements in $k \subset K$.

Let $R = k[x_1, \ldots, x_n]/I$ be a UFD, with k algebraically closed, and let $X = \mathrm{Spec}R$. The function field of X is just the fraction field K of R.

Every element of $\phi \in K$ can be written as $\phi = \frac{f}{g}$, where f, g have no factors in common. Note that the pair f, g is uniquely determined by ϕ, up to replacing f, g by tf, tg for some $t \in k^\times$. The associated rational map $X \to \mathbb{P}^1_k$ sends a closed point $x \in X$ to $[f(x) : g(x)] \in \mathbb{P}^1$, where $f(x)$ is the image of $f \in R/\mathfrak{m}_x = k$.[1]

Definition 1.18. *Let R be a UFD with fraction field K, and let $X = \mathrm{Spec}R$. For each $\phi \in K$, we define the* indeterminacy locus *of ϕ as $V(f) \cap V(g) \subset X$. We also define:*

$$m_\phi(\mathfrak{p}) = \nu_\mathfrak{p}((f, g))$$

In other words, $m_\phi(\mathfrak{p})$ is the largest nonnegative integer such that $(f, g) \subset \mathfrak{p}^\ell$.

The following conditions are equivalent:

- $\phi : \mathrm{Spec}R \to \mathbb{P}^1_k$ is a morphism.
- $m_\phi(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in \mathrm{Spec}R$.
- $V(f) \cap V(g) = \emptyset$.

[1] Note that there is a unique isomorphism of $R/\mathfrak{m}$ with k which restricts to the identity on $k/\mathfrak{m}$.

Thus, m_ϕ quantifies the failure of ϕ to be a morphism. This will be crucial to the arguments in (9).

1.4.2 Rational maps between curves

Let k be an algebraically closed field. For each field extension K/k of transcendence degree 1, there is a unique, up to isomorphism, curve C/k which is smooth, projective and has function field K. We refer to C as the curve associated to the extension K/k.

If K, K' are field extensions of transcendence degree 1 and C, C' are the associated curves, there are bijections between the following sets:

- k-algebra homomorphisms $K \to K'$.
- Rational maps $C' \to C$.
- Morphisms $C' \to C$.

One interprets this as an equivalence between the opposite category of the category of k-algebras of transcendence degree 1 over k and the category of curves over k, see

We've already discussed the correspondence between the first two objects, so the content in the equivalence is mainly the assertion that every rational map extends to a morphism.

In other words, the obstruction to extending an element of K to a morphism to $\mathbb{P}^1$ is the indeterminacy locus $V(f) \cap V(g)$, and this has codimension 2, so there are no obstructions if the domain has dimension 1. Furthermore, note that if $K \to K'$ is injective, the associated map $C' \to C$ is surjective.

We derive two easy consequences of this bijection that will be used later on:

- The field $k(t)$ injects into every field extension K/k of transcendence degree 1 - in fact, this is built into the definition of transcendence degree in certain texts.[2] Consequently, every curve C has a surjective morphism to $\mathbb{P}^1$.

- Conversely, Luroth's theorem tells us that every subfield of $k(t)$ which properly contains k is isomorphic to $k(t)$. Thus, if we have a nonconstant rational map $\mathbb{P}^1 \to C$ to a curve C, then $C \cong \mathbb{P}^1$.

1.5 Resolution of Singularities

Definition 1.19. *Let $X, Y/k$ be varieties. A birational map $X \to Y$ is a rational map that induces an isomorphism of function fields.*

Definition 1.20. *Let X/k be a variety. A resolution of singularities of X is a proper, smooth variety $\tilde{X}$ together with a birational map $\tilde{X} \to X$.*

Definition 1.21. *Let X/k be a variety with at worst Gorenstein singularities, and let ω_X be the canonical bundle of X. A crepant resolution of X is a resolution $\rho : \tilde{X} \to X$ satisfying $\rho^*(\omega_X) = \omega_{\tilde{X}}$.*

We summarize results on the existence of resolutions and crepant resolutions.

We start by discussing the existence of resolutions. Not surprisingly, the conclusions become weaker as the dimension gets larger.

- Resolution of singularities for curves is completely straightforward - for every curve C, there is a unique curve $\tilde{C}/k$ which is smooth and proper over k and which has the same function field as C.

- If char $(k) = 0$, then resolutions exist for varieties of arbitrary dimension.

[2] By Noether normalization, K is an algebraic extension of $k(x_1, \ldots, x_d)$; the integer d is the transcendence degree of K/k.

- If char $(k) \neq 2, 3, 5$, then resolutions exist for surfaces and 3-folds. However, resolutions are no longer unique. Furthermore, it is no longer the case that there is a single smooth variety associated to each field - even in dimension 2 and characteristic 0, there are lots of smooth, rational surfaces which are not isomorphic to $\mathbb{P}^2$.

We now assume that k has characteristic 0 and discuss the existence of crepant resolutions.

- Every surface with at worst Gorenstein singularities admits a crepant resolution. Furthermore, the resolution is unique.
- Every 3-fold with at worst Gorenstein quotient singularities admits a crepant resolution, but the resolutions are no longer unique.[3]
- In dimension 4 and higher, crepant resolutions need not exist.

[3]However, they are related by flops.

Chapter 2

Galois Cohomology

In this chapter, we explain what it means to say that objects $X, Y/k$ are twists of each other and we show how Galois cohomology can be used to classify twists.

2.1 Group Cohomology

Let G be a group.

Definition 2.1. *A G-set is a pair (X, μ), consisting of a set X and an action $G \times X \to X$.*

A G-group is a G-set (X, μ), where X is a group, and for all $g \in G$, $x, y \in X$, we have $g \cdot xy = (g \cdot x)(g \cdot y)$.

A G-module is a G-group (M, μ), where M is an abelian group. Note that a G-module is an object in the category of $\mathbb{Z}[G]$-modules.

A morphism of G-sets/groups/modules is a morphism of the underlying sets/groups/modules which is G-equivariant.

The main example to keep in mind is the following: Let X/k is a variety and k'/k is a Galois extension with Galois group G.

- $X(k')$ is a G-set.
- If X/k is an algebraic group, then $X(k')$ is a G-group.
- If X/k is an abelian variety, then $X(k')$ is a G-module.

If X is a G-set, we write X^G to denote the subset of X consisting of elements invariant under the action of G.

Note that X^G is a group if X is a G-group, and M^G is an abelian group if M is a G-module.

2.1.1 Group Cohomology as a Derived Functor

Let G-mod be the category of G-modules and Ab the category of abelian groups.

Let M, N be G-modules and let $f : M \to N$ be a morphism of G-modules. Then f restricts to a morphism $M^G \to N^G$.

Proof. Suppose $m \in M^G$. For any $g \in G$, we compute:

$$g \cdot f(m) = f(g \cdot m) = f(m)$$

Thus, $f(m)$ is invariant under the G-action, so $f(m) \in N^G$.

□

Thus, the assignment $M \mapsto M^G$ gives us a functor from the category of G-modules to the category of abelian groups. In fact, this functor is representable. Let $\underline{\mathbb{Z}}$ be the G-module $(\mathbb{Z}, \text{trivial})$ consisting of the abelian group $\mathbb{Z}$ endowed with the trivial action of G.

A morphism $\mathbb{Z} \to M$ of G-modules is determined by where it sends 1, and the image of 1 has to be fixed by G. However, every element of M^G gives rise to a morphism, so we have a bijection between M^G and $Hom(\underline{\mathbb{Z}}, M)$.

We define the ith cohomology group of G with coefficients in M:

$$H^i(G, M) = Ext^i(\underline{Z}, M)$$

2.1.2 Cocycles and Coboundaries

We can give a uniform description of $H^i(G, M)$ for all M by computing a resolution of $\underline{\mathbb{Z}}$. Such a resolution is described in [59] Ch.7, section 3.

We set $P_0 = \mathbb{Z}[G]$, $P_1 = \mathbb{Z}[G \times G]$, $P_\ell = \mathbb{Z}[G^{\ell+1}]$ in general. These are abelian groups; we endow them with a G-module structure by defining $G \times P_\ell \to P_\ell$:

$$g \cdot (g_0, \ldots, g_\ell) = (gg_0, \ldots, gg_\ell)$$

Let $P_0 \to \underline{\mathbb{Z}}$ be the map $\sum a_g g \mapsto \sum a_g$. For each $\ell \geq 1$, we define a map $P_\ell \to P_{\ell-1}$:

$$(g_0, \ldots, g_\ell) \mapsto (g_1, g_2, \ldots, g_\ell) - (g_0, g_2, \ldots, g_\ell) + (-1)^\ell (g_1, g_2, \ldots, g_{\ell-1})$$

Then:

$$\cdots \to P_1 \to P_0 \to \underline{\mathbb{Z}} \to 0$$

is a free resolution of $\underline{\mathbb{Z}}$ in the category of G-modules.

We can use this to show that $H^1(G, M) \cong Z^1(G, M)/B^1(G, M)$, where:

$$Z^1(G, M) = \{f : G \to M : f(gg') = g \cdot f(g') + f(g)\}$$
$$B^1(G, M) = \{(g \mapsto g \cdot m_0. - m_0) : m_0 \in M\}$$

2.1.3 Subgroups

Let G be a group and H a subgroup. We have a forgetful functor from G-modules to H-modules. Furthermore, we have restriction maps $H^i(G, M) \to H^i(H, M)$ for all $i \geq 0$ and all G-modules M.

If H is a normal subgroup of finite index, we also have a corestriction morphism:

$$cor : H^i(H, M) \to H^i(G, M)$$

for every G-module M.

At the level of H^0, the corestriction map $H^0(H, M) = M^H \to H^0(G, M) = M^G$ is given by by:

$$m \mapsto \sum_{g \in G/H} g.m$$

2.1.4 Non-abelian cohomology

We briefly review a non-abelian generalization of Galois cohomology. The main reference is [27].

Let G be a group and let X be a G-group. Define:

$$Z^1(G, X) = \{f : G \to M : f(gg') = f(g)(g \cdot f(g'))\}$$

If G acts trivially on X, then $Z^1(G, X)$ is simply the set of group homomorphisms from G to X.

We define an equivalence relation on $Z^1(G, X)$ by $f \sim f'$ if there exists $x \in X$ such that for all $g \in G$:

$$f'(g) = x^{-1} f(g)(g \cdot x)$$

If G acts trivially on X, then $f \sim f'$ is equivalent to $f'(g) = x^{-1} f(g) x$ for all $g \in G$.

We write $H^1(G, X)$ to denote the set of equivalence classes for $\sim$. This set contains a distinguished element - the equivalence class of the trivial map $G \to e_X$ that takes every element of G to the identity in X.

- If X is a G-module, then the two definitions of $H^1(G, X)$ agree.
- Let X be a G-group and N a normal subgroup of X which is also a G-group. Then we have a "short exact sequence" of G-groups:

  $$0 \to N \to X \to X/N \to 0$$

  This induces a long exact sequence:

  $$0 \to N^G \to X^G \to (X/N)^G \to H1(G, N) \to H^1(X, N) \to \cdots$$

  If N is contained in the center of X, we can use this idea to obtain a map from the pointed set $H^1(G, X)$, where X is only a G-group, into $H^2(G, N)$, which has a group structure.

Galois cohomology is essentially just group cohomology, where the group under consideration is a Galois group. By restricting to Galois groups, we obtain new interpretations of the groups $H^i(G, M)$, which we discuss in the next section.

2.2 Twists and Galois Cohomology

Galois cohomology can be thought[1] of as the special case of group cohomology where G is a Galois group.

The goal of this section is to explain how Galois cohomology can be used to classify twists.

We start by explaining what a twist is.

2.2.1 Twists

Let k be a non-algebraically closed field, $\overline{k}$ the algebraic closure, $G = Gal(\overline{k}/k)$ and X/k a variety.

A twist of X is a variety Y/k such that $X \times \text{Spec}\overline{k} \cong Y \times \text{Spec}\overline{k}$ as varieties over $\overline{k}$. If Y, Z are twists of X, we write $Y \sim Z$ if Y, Z are isomorphic as varieties over k. We write $Twists(X/k)$ for the set of $\sim$-equivalence classes of twists of X.

- For any variety over any field k, $Twists(X/k) \neq \emptyset$, since $Twists(X/k)$ always contains a class representing the k-isomorphism class of X.
- Let k' be an intermediate field $k \subset k' \subset \overline{k}$. Then we have a map $Twists(X/k) \to Twists(X/k')$.

The problem of classifying twists of X/k is a special case of the more general problem of classifying descents of a variety $\mathcal{X}/\overline{k}$ to k. Weil gave necessary and sufficient conditions for classifying descents of a variety, and Grothendieck generalized the result to (1.1) in [33].

It turns out that the data needed to descend $X_{\overline{k}}$ to back down to a variety over k is the same as the data needed to construct a cocycle in $H^1_{Gal}(G, Aut(X_{\overline{k}})$.

[1] If G is infinite, we have to restrict to morphisms which are continuous under the profinite topology, although in practice we can always reduce to the finite case and take a limit.

Let X/k be a variety, and $X_{\overline{k}}$ as above. We will describe (one half of) a bijection between $Twists(X/k)$ and $H^1(G, Aut(X_{\overline{k}})$. Let Y be a twist of X, and choose an isomorphism $\phi : X_{\overline{k}} \to Y_{\overline{k}}$.

Now, for each $\sigma \in G$, we write Φ_σ for the automorphism of X that takes a point $p \in X$ to $\phi^{-1}(\sigma(\phi(x)))$.

- The map:

$$G \mapsto Aut(X_{\overline{k}})) \qquad \sigma \mapsto \Phi_\sigma \tag{2.1}$$

  satisfies the cocycle condition.

- If we choose a different isomorphism, or if the isomorphism is defined over ϕ, then the associated cocycles differ by a coboundary.

One also has to show that two twists give rise to the same class iff they are isomorphic as varieties over k to complete the proof that this map is injective.

These details can be found in [62] Ch. 10, [59], [55] Ch. 4.

The real content of the proof is surjectivity - that is, the data of a cocycle is enough to argue that a variety exists over k. To prove the result in full generality, one uses the descent theorem of Grothendieck 1.1. See [55] for details. There is a simpler argument if we only wish to prove that this group can be used to classify twists of algebraic curves - see [62] Ch.10.

2.3 Period-Index

Let k'/k be a Galois extension. We write $G = Gal(\overline{k}/k)$ and $N = Gal(\overline{k}/k')$; as usual $Gal(k'/k) \cong G/N$.

Now, recall that we have a forgetful functor from the category of G-modules to the category of N-modules. Furthermore, we have restriction morphisms $H^i(G, M) \to H^i(N, M)$ for every G-module M. If we represent elements of $H^i(G, M)$ as cocycles $G^i \to M$, then the restriction functor takes each cocycle to the restriction $N^i \to M$.

Definition 2.2. *Let $\gamma \in H^q(G, M)$ be a nontrivial class. We say that γ splits over k' if γ is in the kernel of the restriction map $H^q(G, M) \to H^q(N, M)$.*

Proposition 2.3. *Let k be a field, $G = Gal(\overline{k}/k)$, M a G-module, ℓ a positive integer and $\gamma \in H^q(G, M)$ a non-trivial class.*

Then γ splits over a finite extension k'/k.

Definition 2.4. *Let γ be as above. The index of γ is the minimum of $[k' : k]$, taken over all finite extensions k'/k over which γ splits.*

The period of γ is the order of γ as an element of $H^q(G, M)$.

We will show that period divides index - this will prove that the period is always finite.

For this, we need to define corestriction morphisms $H^i(N, M) \to H^i(G, M)$.

At the level of H^0, we have $H^0(N, M) = M^N$, $H^0(G, M) = M^G$ and the morphism $M^G \to M^N$ is given by:

$$m \mapsto \sum_{g \in G/H} g \cdot m$$

If $M = \overline{k}$, then $M^G = k$, $M^N = k'$, the restriction map is just the inclusion $k \to k'$ and the corestriction map $k' \to k$ is the trace map from Galois cohomology. Similarly, if $M = \overline{k}^\times$, then the restriction map is the inclusion and the corestriction map is the norm. We will refer to corestriction maps as *trace* maps in the later chapters.

Now, we can compose these maps to obtain an endomorphism of $H^q(G, M)$.

Lemma 2.5. *Let M be a G-module and N a normal subgroup of G of index m. Then the composition $cor \circ res : H^q(G, M) \to H^q(G, M)$ is simply multiplication by m.*

Proof. This is straightforward - the corestriction map sends an element to the sum of the elements in its G/N orbit. If an element is already fixed by G, then it is fixed by G/N, so the corestriction map just ends up adding m copies of each element of $M^G \subset M^N$.

□

Thus, if γ splits over k', then γ is in the kernel of the restriction map, so of course it is in the kernel of $cor \circ res$. Thus it is in the kernel of the multiplication-by-m map, so the period of γ divides m.

This is true for every field extension that splits gamma, so in particular, it is true for a field of minimal degree, so period divides index. For more details on corestriction maps in general, see [26].

2.4 Important Examples

Before discussing twists of elliptic curves, we discuss twists of some simpler objects.

2.4.1 Twists of Vector Spaces

- Let V/k be a finite-dimensional vector space, and let W/k be a twist of V.

  Then:

  - $V \otimes_k \overline{k} \cong W \otimes_k \overline{k}$ as $\overline{k}$ vectors spaces.

– Thus $\dim_{\overline{k}} V \otimes_k \overline{k} = \dim_{\overline{k}} W \otimes_k \overline{k}$.

– Dimension is preserved by base extension, so $\dim_k V = \dim_k W$.

– Thus $V \cong W$ as vector spaces over k.

Thus, $Twists(V/k) = \{[V]\}$ for any finite-dimensional vectors space V/k.

The automorphism group of $V \otimes_k \overline{k}$ is isomorphic to $GL_n(\overline{k})$, so we can interpret this as $H^1(G, GL_n(\overline{k})) = 1$.

Note that this result can be proven directly by showing that every cocycle is a boundary - the computation is essentially the same as the computation in the proof of Hilbert 90, so this result is sometimes referred to as "generalized Hilbert 90".

To recover classical Hilbert 90, we assume $G = Gal(k'/k)$ is cyclic, we set $n = 1$ and interpret the statement that every cocycle is a coboundary as a statment about the multiplicative group of k' (since G is cyclic every coboundary is determined by the image of σ).

See also 3.6.

2.4.2 Severi-Brauer Varieties and Central Simple Algebras

Next, we discuss twists of $\mathbb{P}^n$.

A twist of $\mathbb{P}^n$ is called a Severi-Brauer variety. For example, the curve:

$$x^2 + y^2 + z^2 = 0$$

is a twist of $\mathbb{P}^1$. It is a trivial twist[2] if and only if -1 can be written as a sum of 2 squares in k.

[2]That is, isomorphic to $\mathbb{P}^1_k$ as a variety over k.

The automorphism group of $\mathbb{P}^n$ is non-abelian, so twists of $\mathbb{P}^n$ do not form a group. However, if we consider Severi-Brauer varieties of all dimensions simultaneously, then they do form a group.

We use the short exact sequence:

$$1 \to \overline{k}^\times \to GL_n(\overline{k}) \to PGL_n(\overline{k}) \to 1$$

to obtain a long exact sequence containing the segment:

$$H^1(G, GL_n(\overline{k})) \to H^1(G, PGL_n(\overline{k})) \to H^2(G, \overline{k})^\times)$$

By the previous example, $H^1(G, GL_n(\overline{k}))$ vanishes for all n, so we have injections:

$$H^1(G, PGL_n(\overline{k})) \to H^2(G, \overline{k})^\times)$$

for all n.

We define $Br(k) = H^2(G, \overline{k}^\times)$. One can show that every class in $Br(k)$ comes from a class in $H^1(G, PGL_n(k))$ for some n, so we can think of classes in $Br(k)$ as representing twists of $\mathbb{P}^n_k$ for some n.

There is another interpretation of $Br(k)$ which is helpful for understanding the equivalence relation and the group law on torsors.

A central simple algebra over k is a finite dimensional k-algebra A which is simple, and with $Z(A) \cong k$.

- Over an algebraically closed field, the only CSAs are $M_n(k)$.
- Thus every CSA is a twist of $M_n(k)$.
- The automorphism group of $M_n(k)$ is $PGL_n(k)$, so twists of $M_n(k)$ are classified by the same object as twists of $\mathbb{P}^n$!

An unexpected consequence is that we have a bijection between classes of Severi-Brauer varieties and classes of central simple algebras.

- To obtain a Severi-Brauer variety from a central simple algebra, we think of the algebra as a k-vector space endowed with a norm. The Severi-Brauer is obtained by setting the norm equal to 0.
- Obtaining a central simple algebra from a Severi-Brauer variety is trickier, but can be done in at least two ways.
  - We can describe the central simple algebra as an extension of the tangent bundle of the Severi-Brauer variety - see [40] for details.
  - If the Severi-Brauer variety is described by a conic, we can construct the associated central simple algebra as a Clifford algebra. See [24] for details.

2.4.3 Elliptic Curves

Finally, we discuss twists of elliptic curves[3].

- Let E/k be an elliptic curve. If E does not have complex multiplication, then every element of $Aut(E_{\overline{k}})$ is either a translation, or a composition of a translation with the negation map.

  Since translations don't commute with negation in general, $Aut(E_{\overline{k}})$ is a non-abelian group.

  However, if we think about twists of E as a set endowed with additional structure, then we can obtain a group structure.

[3]See next chapter for definitions and properties of elliptic curves.

Let E be an elliptic curve. Any automorphism of E as a curve that fixes the identity automatically preserves the group law. Furthermore, every automorphism can be factored into a translation followed by an automorphism that fixes the identity.

The automorphism group of (E, p_0) as a pointed genus one curve coincides with the group of automorphisms of E as an abelian group. If E is sufficiently generic, there are two such automorphisms - the identity and negation. Thus, twists of E/k as an elliptic curve are classified by $H^1(G, \{\pm 1\})$.

Note that this group does not depend on E. We will see that $Twists((E, p_0)) \cong k^\times/k^{\times 2}$ in the next chapter.

- On the other hand, we can look at twists of E as a torsor of itself. That is, we work in the category of torsors, where every object comes equipped with a simply transitive group action of E and where morphisms have to be compatible with the action.

  The automorphism group of E in the category of torsors is exactly the group of translations.

  The Weil-Chatelet group[4] of E/k is $WC(E/k) = H^1(G, E(\overline{k}))$. This group classifies k-isomorphism classes of torsors. The results of the last chapter show that every genus one curve appears in $WC(E/k)$ of its Jacobian, and the class of a genus one curve is trivial in $WC(E/k)$ if and only if $C(k) \neq \emptyset$.

[4]It's clear that $H^1(G, E)$ is a group abstractly. The group law on torsors can be described without using Galois cohomology, see **cite**

2.5 Useful short exact sequences

Let E/k be an elliptic curve, and $G = Gal(\overline{k}/k)$. For every positive integer m, we have a multiplication-by-m map $E(\overline{k}) \to E(\overline{m})$.

Since nonconstant maps of curves over an algebraically closed field are always surjective, we have an exact sequence:

$$0 \to E[m] \to E(\overline{k}) \to E(\overline{k}) \to 0 \tag{2.2}$$

where $E[m]$ denotes the m-torsion subgroup of E.

The long exact sequence in Galois cohomology gives us:

$$0 \to E(k)[m] \to E(k) \to E(k) \to H^1(G, E[m]) \to WC(E/k) \to WC(E/k) \tag{2.3}$$

The map $WC(E/k) \to WC(E/k)$ is multiplication by m, so the image of $H^1(G, E[m])$ coincides with the m-torsion subgroup of $WC(E/k)$.

Thus, we have a short exact sequence:

$$0 \to E(k)/mE(k) \to H^1(G, E[m]) \to WC(E/k)[m] \to 0 \tag{2.4}$$

The short exact sequence 2.4 comes up in the definition of Selmer groups, and plays a crucial role in the proof of the Mordell-Weil theorem, see [62] Ch.10.

Precisely, if k is a field and ν a valuation, we write k_ν for the completion[5] of k with respect to the metric associated to ν. We define $Ш(E/k)$ as the kernel of $WC(E/k) \to \prod_\nu WC(E/k_\nu)$. It parametrizes torsors of E that have a point in every completion[6]

The Selmer group is an auxilliary object which is earlier to compute and con-

[5]Not to be confused with the residue field of the valuation.

[6]When k is a number field or the function field of a curve, it is clear what we mean by every completion. See [20] for the definition of Ш we use for higher dimensional fields.

tains information about $MW(E/k)$ and $Ш(E/k)$ - explicitly, we have a short exact sequence:

$$0 \to E(k)/mE(k) \to S^{(m)}(E/k) \to Ш(E/k)[m] \to 0 \tag{2.5}$$

In practice, this is used to compute the rank of the Mordell-Weil group. We will not really need to use the Selmer group.

2.5.1 Brauer and Weil-Chatelet

In 7.2, we will discuss the role of the Brauer group in the classification of genus one fibered 3-folds without multiple fibers.

There is a simpler version of that story for genus one curves over a field. To state it, we need to define the Brauer group of a variety.

Definition 2.6. *Let X/k be a scheme. The cohomological Brauer group of X is the étale cohomology group $H^2(X, \mathbb{G}_m)$.*

The Azumaya Brauer group of X is the group of Morita equivalence classes of sheaves of Azumaya algebras over X; we denote it $Br_{Az}(X)$. We start by listing some basic properties of these groups. See Ch. 6 of [55] for proofs.:

- For any scheme X, we have an injection $Br_{Az}(X) \to H^2(X, \mathbb{G}_m)$. If X is quasiprojective, this is an isomorphism. We will only be interested Brauer groups of quasiprojective varieties, so we use $Br(X)$ to denote either of the two Brauer groups.

- If X/k is a variety, the structure morphism induces a map $Br(k) \to Br(X)$. If $X(k) \neq \emptyset$, the map $Br(k) \to Br(X)$ has a splitting $Br(X) \to Br(k)$.

- If X is a smooth, irreducible variety with function field K, there is an injection $Br(X) \to Br(K)$.

Now, let E/k be an elliptic curve. There is a (split) short exact sequence:

$$0 \to Br(k) \to Br(E) \to WC(E/k) \to 0 \tag{2.6}$$

See Section 6 of [24] for details.

Chapter 3

Genus One Curves

Let k be a field of characteristic 0, let $\overline{k}$ be the algebraic closure of k.

Definition 3.1. *A marked genus one curve is a pair (C, q) consisting of a non-singular curve C of arithmetic genus 1 and a point $q \in C(\overline{k})$.*

The field of definition of (C, q), denoted $k(q)$, is the intersection of all field extensions k'/k such that $q \in C(k')$.

The degree of (C, q) is the dimension of $k(q)$ as a k-vector space.

The index of C/k is:

$$ind_k(C) = \min_{q \in C(\overline{k})} \deg(C, q)$$

Thus, $ind_k(C) = 1$ iff $C(k) \neq \emptyset$. We will refer to marked genus one curves of degree 1 as elliptic curves.

We will show the following:

- Let (C, q) be a marked genus one curve of degree $d \geq 2$. Then we have an associated map $C \to \mathbb{P}^{d-1}$ which is a double cover if $d = 2$ and an embedding if $d \geq 3$. Furthermore, when $d \geq 3$, the image of C in $\mathbb{P}^{d-1}$ is cut out by polynomials with coefficients in k.

- Let (E, p) be an elliptic curve. Then E is isomorphic to the closure in $\mathbb{P}^2$ of an affine curve in $\mathbb{A}^2$ given by an equation of the form:

$$y^2 = x^3 + fx + g$$

  Furthermore, $E(k)$ can be endowed with a group structure, with p as the identity.

- Let C/k be a genus one curve. Then $C(\overline{k})$ is a torsor of $E(\overline{k})$[1], where E an elliptic curve defined over k.

All three of these theorems will follow easily from Riemann-Roch. Although this is all classical, it is worth reviewing the arguments, since we will be using them with the relative Picard functor later on.

We will be following the exposition in Ch. II of [62].

3.1 Divisors

Let C/k be any smooth curve. Since C is defined over k, the Galois group $G = Gal(\overline{k}/k)$ acts on $C(\overline{k})$. Explicitly, if we choose equations $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ such that:

$$C(\overline{k}) = \left\{(a_1, \ldots, a_n) \in \overline{k}^n : f_i(a_1, \ldots, a_n) = 0\right\}$$

then for any $\sigma \in G$:

$$\sigma(f_i(a_1, \ldots, a_n)) = f_i(\sigma(a_1), \ldots, \sigma(a_n))$$

[1] We will make this precise later, but the basic idea is $E(\overline{k})$ has a simply transitive action on $C(\overline{k})$.

since field automorphisms commute with addition, multiplication and k-scaling. Thus, $f_i(a_1, \ldots, a_n) = 0$ iff $f_i(\sigma(a_1), \ldots, \sigma(a_n)) = 0$, so the action of G on $\overline{k}^n$ restricts to an action on $C(\overline{k})$.

Furthermore, we can use this action to recognize elements of $C(k) \subset C(\overline{k})$: a point $p \in C(\overline{k})$ is defined over k iff p is fixed by every $\sigma \in G$.

Now, let $Div(C)$ be the free abelian group generated by the points on $C(\overline{k})$. We refer to elements of $Div(C)$ as divisors - explicitly, a divisor is just a finite, formal sum $a_1p_1 + \cdots + a_np_n$ with $a_i \in \mathbb{Z}$ and $p_i \in C(\overline{k})$. The G-action on $C(\overline{k})$ induces a G-action on $Div(C)$.

We define $Div_k(C)$ as the subgroup of $Div(C)$ consisting of divisors which are invariant under the G-action.

Let deg be the group homomorphism:

$$\deg : Div(C) \to \mathbb{Z} \qquad \sum a_p p \mapsto \sum a_p$$

We write $Div^0(C)$ to denote the kernel of deg and $Div_k^0(C) = Div_k(C) \cap Div^0(C)$.

Later on, we will also write $Div^\ell(C)$ (resp. $Div_k^\ell(C)$) to denote the preimage $\deg^{-1}(\ell)$ in $Div(C)$ (resp. in $Div_k(C)$.)

Let $D = \sum a_p p \in Div(C)$. We write $D \geq 0$ if $a_p \geq 0$ for all p. We extend this to a partial ordering on $Div(C)$ by setting $D \geq D'$ if $D - D' \geq 0$.

We need to define two more objects to state Riemann-Roch.

Definition 3.2. *Let K be the function field of C and set $\overline{K} = K \otimes_k \overline{k}$. We define a group homomorphism:*

$$\overline{K}^\times \to Div(C) \qquad \phi \mapsto \sum_{p \in C(\overline{k})} \nu_p(\phi) p$$

Here $\nu_p(\phi)$ is the valuation associated to the closed point p.

Note that div has the following properties:

- $div(\phi) = 0$ iff $\phi \in \overline{k}^{\times}$.
- For every $\phi \in K^{\times}$, $\deg(div(\phi)) = 0$.

In other words, we have an exact sequence:

$$0 \to k^{\times} \to K^{\times} \to Div(C)$$

We define $Pic(C)$ as the cokernel of $\overline{K}^{\times} \to Div(C)$. Since $\deg(div(\phi)) = 0$, the map $K^{\times} Div(C)$ factors through the inclusion $Div^0(C) \to Div(C)$. We define $Pic^0(C)$ as the cokernel of $K^{\times} \to Div^0(C)$.

Altogether we have an exact sequence:

$$0 \to \overline{k}^{\times} \to \overline{K}^{\times} \to Div^0(C) \to Pic^0(C) \to 0 \tag{3.1}$$

Finally, we need one more definition before we can state Riemann-Roch.

Definition 3.3. *Let $D = \sum a_p p \in Div(C)$. We associate to D the (finite-dimensional) $\overline{k}$-vector space in $\overline{K}$:*

$$\mathcal{L}(D) = \left\{\phi \in K^{\times} : div(\phi) + D \geq 0\right\}$$

We define $\ell(D) = \dim_{\overline{k}} \mathcal{L}(D)$.

If D, D' are divisors on C, the following are equivalent:

- $\mathcal{L}(D) \cong \mathcal{L}(D')$.
- $D - D' = div(f)$ for some $f \in K^{\times}$.

The point is that $\mathcal{L}(D)$ is a line bundle on C. Furthermore, if C is smooth, then every line bundle on C is of the form $\mathcal{L}(D)$ for some $D \in Div(C)$.

Thus, we will think of elements $Pic(C)$ as representing line bundles on C. We denote elements by $Pic(C)$ as $\mathcal{L}$ or $\mathcal{L}(D)$ if we wish to lift the line bundle to $Div(C)$.

Without further ado:

Theorem 3.4. *(Riemann-Roch for Genus 1 Curves) Let C be a nonsingular genus one curve over an algebraically closed field and let $D \in Div(C)$ be a divisor of positive degree. Then $\ell(D) = \deg(D)$.*

See [62] or [36] for a proof. We will use this theorem to obtain models for genus one curves over our field of choice in (3.2). Then we use it to derive the group law in (3.3) and to show that every marked genus one curve has a natural structure of a torsor of an elliptic curve (3.4).

3.1.1 Generalizations of Picard Group

Of course, we can also define the Picard group of a general variety. There are several ways of doing this, which agree for smooth varieties:

- We can define $Div(X)$ has the free abelian group generated by codimension 1 subvarieties of X and define $Pic(X)$ as above.
- We can define $Pic(X)$ as the group of invertible sheaves/line bundles on X.
- The latter perspective also allows us to identify $Pic(X)$ with a sheaf cohomology group:

$$Pic(X) \cong H^1(X, \mathbb{G}_m)$$

The identification of $H^1(X, \mathbb{G}_m)$ and the group of invertible sheaves holds for most of the usual sites of X - that is.

Since we have an identification of Pic with H^1, that means Pic is a functor from varieties to abelian groups.

- Every morphism of varieties $C' \to C$ induces a map of Picard groups.
- If $X \to Y$ is an isomorphism away from a codimension 2 subset, then the induced map on Picard groups is an isomorphism.

There are two more important technical facts we need:

- So far, we've define the Picard group of $X \to \text{Spec}k$. We will also need the relative Picard group when we study genus one fibrations. We can also define the relative Picard group for S-schemes $X \to S$.
- The Picard group is representable by a variety, and under certain technical hypotheses, we also know that the relative Picard group is represented by an S-scheme. Our constructions/definitions have been chosen so that we are using the same tools to study elliptic curves and elliptic fibrations.[2]

For details on the relative Picard functor and on representability of the Picard functor in general, we refer the reader to [11]. See also Ch.6 of [55].

3.2 Models for Marked Genus One Curves

We use Riemann-Roch to obtain a model for a genus one curve C from a divisor D of positive degree. To begin, we assume that k is algebraically closed.

Let D be a divisor on C, with $\deg(D) = d > 0$. Then 3.4 says $\ell(D) = d$, so we can find $\deg(D)$ $\overline{k}$-linearly independent elements $x_1, \ldots, x_d$ of $\mathcal{L}(D)$.

[2]For example, we only use the Jacobian formula for torsors of index 2 and 3 - the validity of the formula has been checked for genus one curves over arbitrary schemes in this case.

- The dimension of $\mathcal{L}(mD)$ is md.
- Furthermore, $\mathcal{L}(mD)$ contains all products of the form $x_1^{e_1} \cdots x_d^{e_d}$ where $e_i \geq 0$ and $e_1 + \cdots + e_d = m$.

Now, the number of monomials we can obtain from the x_i grows faster than the bound on the dimension. Thus, we can find relations between products of the x_i when m is sufficiently large. These relations give us models of our genus one curve in $\mathbb{P}_k^{d-1}$.

We start by obtaining a more precise description of the model associated to a genus one curve with a divisor of degree $d > 1$. Then, we explain how these ideas are used to obtain models over a nonalgebraically closed ground field.

Proposition 3.5. *Let C/k be a genus one curve and D a divisor of degree $d \geq 1$.*

- *If $\deg D = 1$, we obtain an isomorphism between C and a curve defined by an equation of the form:*

$$y^2 = x^3 + fxz^4 + gz^6 \tag{3.2}$$

  for some $f, g \in k$. Here, x, y, z can be thought of as coordinates in $\mathbb{P}^{2,3,1}$.

- *If $\deg D = 2$, we obtain a description of C as:*

$$w^2 = au^4 + bu^3 + cu^2v^2 + duv^3 + ev^4 \tag{3.3}$$

  where u, v are coordinates on $\mathbb{P}^1$ and C is a double cover branched over the roots of the quartic on the right hand side. Note that the quartic must have distinct roots in order for the double cover to be smooth.

- *If* $\deg D = 3$*, we obtain an embedding* $C \to \mathbb{P}^2$*. The image of* C *is a plane cubic.*

- *Finally, if* $\deg D > 3$*, we obtain a map to* $\mathbb{P}^{d-1}$ *and the image of* C *is cut out by* $\frac{d(d-3)}{2}$ *quadratic forms.*

Proof. We prove this degree by degree.

First, assume that $\deg D = 1$. Then $\mathcal{L}(D)$ is generated by a single element as a vector space. Let z be one such element.

Now, $z^2 \in \mathcal{L}(2D)$, but $\ell(2D) = 2$ so we need one more element to generate it as a vector space. Choose such element, and call it x. Similarly, $z^3 \in \mathcal{L}(3D)$, as is $x^2 z$. We need one more element to obtain a basis. Choose one and call it y.

It is easy to check that the monomials in x, y, z of degree 4,5 (weighted appropriately) form bases of $\mathcal{L}(4D), \mathcal{L}(5D)$, respectively: linear independence of those monomials follows from linear independence of the sets $\{z\}, \{z^2, x\}, \{z^3, xz, y\}$ and 3.4 shows that they have the correct size.

We can obtain 7 monomials in $\mathcal{L}(6d)$, so by 3.4, they must be linearly dependent. Thus, there exist $a_i \in \mathbb{C}$ such that:

$$a_5 y^2 + a_1 xyz + a_3 yz^3 = a_0 x^3 + a_2 xz^2 + a_4 xz^4 + a_6 z^6$$

Furthermore, if a_5 or a_0 vanishes, then we would have an equation of linear dependence in lower degree, which we have ruled out.

Finally, we rescale x, y so that $a_0 = a_5 = 1$ and use changes of variables of the form $y \to y + \lambda xz$ and $x \mapsto \lambda xz^2$ to obtain an equation with $a_1 = a_2 = a_3 = 0$.

If $\deg D = 2$, we choose a basis u, v of $\mathcal{L}(D)$, find $w \in \mathcal{L}(2D)$ so that w, u^2, uv, v^2 is a basis and then obtain a relation in $\mathcal{L}(4D)$:

$$w^2 + Q_2(u, v)w + Q_4(u, v)$$

where $Q_2(u,v), Q_4(u,v)$ are homogenous quartics in u, v of degree 2,4.

We use a change of variable of the form $w \to w + Q_2(u,v)/2$ to obtain an equation:

$$w^2 = Q(u,v)$$

If $\deg D = 3$, we choose a basis x, y, z of $\mathcal{L}(D)$. There are 10 monomials in $\mathcal{L}(3D)$, so we have a single equation describing C as a plane cubic.

Finally, if $\deg D \geq 4$, we fix a basis $x_1, \ldots, x_d$ of $\mathcal{L}(D)$. There are $\frac{d(d-1)}{2}$ monomials in $\mathcal{L}(2D)$, so there must be $\frac{d(d-1)}{2} - d = \frac{d(d-3)}{2}$ relations between the degree 2 monomials.

□

Finally, we need to show that the equation just obtained can be chosen to have coefficients in k if $D \in Div_k(C)$. This follows from:

Lemma 3.6. *Let $\overline{k}/k$ be as above, let V be a vector space over $\overline{k}$ and suppose we have an action of G on V which is compatible with the vector space structure. Let V^G be the subspace of G consisting of elements fixed by G.*

Then $V \cong V^G \otimes_k \overline{k}$.

See ([62], Ch. 2, Lemma 5.8.1) for a proof. We will reinterpret this result in (2.2).

Thus, as long as the line bundle associated to D is invariant under the action of G, we can "descend" $\mathcal{L}(D)$ to a vector space over k. The coefficients in the equation for E are equations of linear dependence, so they can be chosen in k.

Furthermore, note that we can associate a G-invariant divisor D to any marked genus one curve (C, q). Let k'/k be a finite, Galois extension containing the field

of definition of q. Let $D = \sum_{\sigma \in Gal(k'/k)} \sigma(q)$. Then D is clearly G-invariant.[3]

In particular, when the characteristic of k is 0, we can always take k' to be the normal closure of the field of definition of q. This allows us to associate a model over k to each marked genus one curve (C, q), even when k is not algebraically closed.

Of course, if k is algebraically closed, then we can always find a divisor of degree 1 to obtain an equation 3.2.

3.3 Group Law

In this section, we will use Riemann-Roch to show that the set of k-points on an elliptic curve form a group. The key idea is that every divisor of degree 1 is linearly equivalent to the divisor $[p]$ for a unique $p \in C(\overline{k})$.

Now, fix a point $p_0 \in C(k)$. We can define a map $C(k) \to Pic^0(C)$ by sending each point p to the class of $\mathcal{L}(p - p_0)$.

- If p, q map to the same point, then $\mathcal{L}(p-p_0) = \mathcal{L}(q-p_0)$. Tensoring both sides by $\mathcal{L}(p_0)$ shows that $\mathcal{L}(p) = \mathcal{L}(q)$, so $p = q$. Thus, the map $C(k) \to Pic^0(C)$ is injective.

- If D is a divisor of degree 0, then $D+p_0$ has degree 1, so $\mathcal{L}(D+p_0) = \mathcal{L}(p)$ for some $p \in C(k)$. By construction, $\mathcal{L}(p-p_0) = \mathcal{L}(D)$, so the map is surjective.

Thus, we have a bijection between points on $C(k)$ and elements in $Pic^0(C)$. Since $Pic^0(C)$ is a group, this means we can endow $C(k)$ with the group structure

[3]Note that this divisor coincides with the image of q under a corestriction map. While this will not be needed in any proof, we would like to highlight it now, as corestriction maps will play an increasingly important role as one progresses through the dissertation.

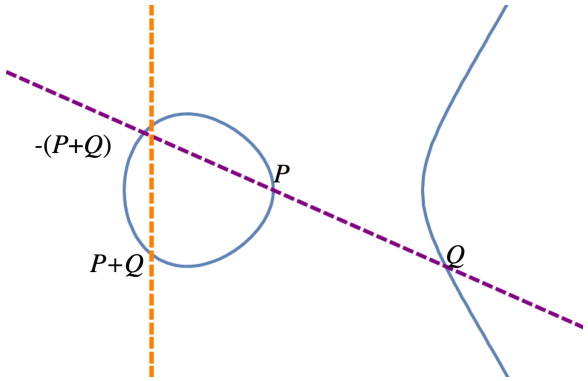


Figure 3.1: *The group law on a real elliptic curve in* $\mathbb{R}^2$.

of Pic^0. Note, however, that we have a (unique) bijection $C(k) \to Pic^0(C)$ taking p_0 to 0 for each choice of $p_0 \in C(k)$.

The Picard group is an abelian group, so the group structure on $C(k)$ is abelian. In fact, much more is true - representability of the Picard functor means $Pic^0(C)$ is an abelian variety. This means that $Pic^0(C)$ is isomorphic to proper algebraic variety, and the multiplication map is a morphism of varieties.

- If we fix a model for C, we can describe the group explicitly using polynomial maps- see Ch. 3 of [62].
- If we embed our curve in $\mathbb{P}^2$, the group law can be described geometrically: three points add up to 0 if and only if they are collinear.

Finally, note that if we have a genus one curve C/k, where k is not necessarily algebraically closed, and we have points $p_0, p_1, p_2 \in C(k)$, then we can endow $C(k)$ with a group structure with p_0 as the identity, and then we can add p_1, p_2 to obtain a point $p_3 \in C(k)$.

We denote the group of points on $C(k)$ by $MW(C/k)$ to indicate we are thinking about it as an abstract group.

The possible isomorphism types of $MW(E/k)$ as an abstract group are well-understood when k is a number field:

Theorem 3.7. *Let E/k be an elliptic curve.*

- *If k has characteristic 0, then $MW(E/k)$ is isomorphic to a subgroup of $S^1 \times S^1$.*
- *(Mordell-Weil) If k is a number field, $MW(E/k)$ is finitely generated. Thus, $MW(E/k) \cong \mathbb{Z}^r \times (\mathbb{Z}/m) \times (\mathbb{Z}/n)$ for integers m, n, r.*
- *(Mazur) If $k = \mathbb{Q}$, the torsion subgroup of $MW(E/k)$ is one of the following groups:*

$$\mathbb{Z}/m \qquad m = 1, 2, 3, \ldots, 10, 12$$

$$\mathbb{Z}/2 \times \mathbb{Z}/(2n) \qquad n = 1, 2, 3, 4$$

Proof. The first point is classical - over $\mathbb{C}$, the group is isomorphic to $S^1 \times S^1$ by Riemann's uniformization theorem. We can embed any field of characteristic 0 into $\mathbb{C}$ to prove the result.

A proof of the second point can be found in [62] Ch. 10.

Finally, see [45] for a proof of the third point.

□

Note, however, that there is no algorithm for computing the rank of an elliptic curve. In practice, one computes the Selmer group and then has to break it up

into a MW component and a Ш component.[4]

3.4 Torsors and Jacobians

Let C/k be a genus one curve. The Jacobian of C/k is the elliptic curve $(Pic^0(C), 0)$.

Definition 3.8. *Let E/k be an elliptic curve. A* torsor *of E/k is a pair (C, μ) consisting of a genus one curve C/k and a simply transitive group action $\mu : E(\overline{k}) \times C(\overline{k}) \to C(\overline{k})$.*

We will typically write $p + q$ to denote $\mu(p, q) \in C(\overline{k})$.

Furthermore, since the action is simply transitive, we can also define a "subtraction map" $C(\overline{k}) \times C(\overline{k}) \to E(\overline{k})$ that takes a pair (q_1, q_2) to the unique point in $p \in E(\overline{(k)})$ satisfying $p + q_1 = q_2$. We represent this point as $[q_2 - q_1]$.

Proposition 3.9.

- *Suppose E is the Jacobian of C/k. Then C/k is a torsor of E.*
- *Suppose C/k is a torsor of E. Then C is a twist of E.*
- *Suppose C is a twist of E. If we choose an isomorphism $E \to C$, then we can endow C with the structure of a torsor.*

Proof. We can use the bijection between $C(\overline{k})$ and $Pic^1(C)$ to define a simply transitive action of $Pic^0(C)$ on $Pic^1(C)$. Thus, every genus one curve is a torsor of its Jacobian.

To prove the second point, choose a point $q \in C(\overline{k})$ and define a map $E \to C$ by $p \mapsto p + q$. Since the action on C is simply transitive, this map is an isomorphism. Thus, every torsor is in fact a twist. □

[4]We will discuss the relationship between MW and Ш in the later sections, e.g. 8.2, although we will be interested in Ш and MW will be the auxiliary tool we have to study.

To explain the difference between twists and torsors, we need to define morphisms of torsors.

Let E be an elliptic curve and C, C' a pair of torsors of E. A morphism of torsors $\phi : C \to C'$ is exactly what it sounds like - it is a morphism of the underlying curves which is compatible with the action of E:

$$(\forall q \in C(\overline{k}), p \in E(\overline{k})) \qquad \phi(p+q) = p + \phi(q)$$

Requiring a morphism to be compatible with a simply transitive action is a very strong condition. For example, every morphism of torsors is an isomorphism.

Fortunately, we don't need to do much to produce a morphism of torsors.

Proposition 3.10. *Let C_1, C_2 be torsors of an elliptic curve and suppose we have a field extension k'/k and points $q_i \in C_i(k')$. Then there is a unique morphism of torsors $C_1 \to C_2$ that takes q_1 to q_2.*

Indeed, once we know that q_1 goes to q_2, the image of any $q \in C_1(k')$ necessarily has to go to $(q-q_1)+q_2$, where $q-q_1$ is the point on $E(k')$ satisfying $(q-q_1)+q_1 = q$. Furthermore, the converse is also true: if we choose points q_1, q_2, we can define a morphism as above. For details, see [46].

In the next chapter, we use these ideas to classify genus one curves over non-algebraically closed fields.

Chapter 4

Classifying Genus One Curves

We now use the results of the last two chapters to classify genus one curves over an arbitrary field k of characteristic 0.

To begin, we show that it is equivalent to compute the moduli space of marked genus one curves over k.

Let C be a genus one curve, and let $q, q' \in C(k)$. We can use the group structure on C to obtain an automorphism of C that takes q to q'. Thus, the forgetful map from the space of isomorphism classes of marked genus one curves to the space of isomorphism classes of genus one curves is injective.

If k is algebraically closed, then every genus one curve has a k-point, so the map is in fact a bijection.

We start by discussing this case.

4.1 $k = \overline{k}$

We explain how elliptic curves over k are classified by their j-invariant.

- Let C be a genus one curve, and let $p \in C(k)$ be a point. Then we can

compute a Weierstrass equation:

$$y^2 = x^3 + fx + g$$

Conversely, every Weierstrass equation as above, with $4f^3+27g^2 \neq 0$, defines a genus one curve. Thus, we can use the space of nonsingular Weierstrass equations as a parameter space:

$$\mathcal{W}_k = \left\{(f,g) \in k^2 : 4f^3 + 27g^2 \neq 0\right\}$$

- We define an action of $k^\times$ on $\mathcal{W}_k$ by $t \cdot (f,g) = (t^4 f, t^6 g)$. Two elements $(f,g), (f',g')$ define isomorphic elliptic curves iff they are in the same $k^\times$ orbit.

- Define a map:

$$j : \mathcal{W}_k \to k \qquad j(f,g) = 1728\frac{4f^3}{4f^3 + 27g^2}$$

Then j is constant $k^\times$ orbits, and separates distinct orbits - i.e. j gives a bijection between $\mathcal{W}_k/k^\times$ and k.

Thus, the space of isomorphism classes of genus one curves over k can be identified with k as a set, and geometrically coincides with the singular quotient $\mathcal{W}_k/k^\times$.

See also B for an alternative description when $k = \mathbb{C}$.

4.2 $k \neq \overline{k}$

4.2.1 Elliptic curves

Next, we classify elliptic curves over k, up to k-isomorphism, over a non-algebraically closed field. Since every elliptic curve can be described by a Weierstrass equation, we can use many of the same tools as we did when $k = \overline{k}$:

- We still have $\mathcal{W}_k$ as a parameter space.
- We still have an action of $k^\times$ on $\mathcal{W}_k$. Furthermore, two points in $\mathcal{W}_k$ define the same elliptic curve over k if and only if they are in the same $k^\times$ orbit.
- We still have a surjective map $j : \mathcal{W}_k \to k$ which is constant on $k^\times$ orbits.

If $k^\times \neq k^{\times 2}$, then j no longer separates points, since quadratic twists have the same j-invariant. This is not a big deal, though, since the set of quadratic twists of any elliptic curve is well-understood.[1]

In the later sections, we will mainly use $\mathcal{W}$ as our parameter space. As a result, we will not need to worry about quadratic twists, since non-isomorphic quadratic twists have different Weierstrass equations.

However, quadratic twists will come up again in 9.5, as they will help us classify torsors that split over quadratic extensions.

4.2.2 Genus one curves without rational points

Every genus one curve C/k with $C(k) \neq \emptyset$ can be endowed with the structure of an elliptic curve over k, and we've already classified those.

[1] The best way to describe it is as a "torsor" of $k^\times/k^{\times 2}$ - there is a simply transitive group action of $k^\times/k^{\times 2}$ on the set of quadratic twists of any elliptic curve E/k.

It remains to classify genus one curves with $C(k) = \emptyset$. Let C/k be *any* genus one curve and let E/k be the Jacobian elliptic curve.

Then C is a torsor of E, so C gives rise to a class in $WC(E/k)$. Furthermore, the class of C is trivial in $WC(E/k)$ if and only if $C(k) = \emptyset$.

Thus, the last step in the classification of genus one curves is understanding $WC(E/k)$ for every elliptic curve E/k.

- This classification appears for genus one curves $C/\mathbb{Q}$ in [46].
- A similar[2] strategy is used in [32] to classify Calabi-Yau genus one 3-folds without multiple fibers.

4.3 Classification using models

Let (C, q) be a marked genus one curve, and assume q is defined over a field extension of degree d. Then C has a map to $\mathbb{P}^{d-1}$ that we can use to obtain an equation for C. Furthermore, there are uniform models for all such curves - e.g. if $d = 3$, then the image of C is a plane cubic. Thus, we can use the space of equations for plane cubics as a parameter space for genus one curves.

Now, we have an action of $PGL(k, d)$ on $\mathbb{P}^{d-1}_k$, and this induces an action on the space of equations on $\mathbb{P}^{d-1}_k$. We denote this space by $\mathcal{C}_d$. If two elements of $\mathcal{C}_d$ are in the same $PGL_(k, d)$ orbit, the associated genus one curves are clearly isomorphic over k. Thus, the quotient of $\mathcal{C}_d$ by the appropriate group parametrizes genus one curves of index d.

However:

[2]One difference is that Gross uses the Tate-Shafarevich group instead of the Weil-Chatelet group, since the Tate-Shafarevich group is finite in that special case, and that allows him to draw stronger conclusions.

- When $d = 2$, it is not hard to find quartics which do not differ by a change of variables, but that define the same genus one curve. For example, let $k = \mathbb{R}$ and $Q(u, v)$ is a positive definite binary quartic, and let C be the genus one curve:

$$C: \quad w^2 = Q(u, v)$$

Since Q is positive definite, the discriminant of this genus one curve is a positive real number.

The Jacobian of a genus one curve has the same discriminant as the curve, so the Jacobian of C has a positive discriminant. In particular, this means the Jacobian has full 2-torsion defined over $\mathbb{R}$, so we can find an equation for the Jacobian as:

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

Now, it's clear that E is also isomorphic to:

$$E: \quad w^2 = v(u - ve_1)(u - ve_2)(u - ve_3)$$

Since $q(u, v)$ is positive definite, $q(u, 1)$ is a square in $\mathbb{R}$, so C has an $\mathbb{R}$-point. This means C is isomorphic to E as an elliptic curve over $\mathbb{R}$. However, it's clear that there is no change of variable taking $Q(u, v)$ to $v(u - ve_1)(u - ve_2)(u - ve_3)$, since the latter splits completely whereas $Q(u, v)$ is never zero.

- By the time we get to $d = 5$, the parameter space is 50-dimensional. Thus, while we technically do have a parameter space, it's too big to be of practical use.

In particular, to use this perspective in F-theory, we need to be able to compute an equation for the Jacobian from the model. In principle, this is possible by recent results of Fisher [1]. However, the methods there are better suited for computing the Jacobian of a single example - there is no closed form polynomial formula from $\mathcal{C}_d$ to the space of Weierstrass equations when $d \geq 5$.

4.4 Example: $k = \mathbb{R}$

When k is not algebraically closed, one should expect the moduli space of genus one curves over k to have infinitely many components:

- For each possible value of $j \in k$, we have as many quadratic twists as we have classes in $k^{\times}/k^{\times 2}$.
- We could assume that k is quadratically closed so that we don't have to worry about quadratic twists. However, if k is quadratically closed but not algebraically closed, then $Gal(\overline{k}/k)$ is infinite.

There is only one situation where there there exist nontrivial torsors, but $\mathrm{Gal}(\overline{k}/k)$ is finite - when k is a real closed field. We run the two "programs" to classify genus one curves over $\mathbb{R}$ - this will allow us to see what types of computations one needs to be able to replicate.

- Elliptic curves over $\mathbb{R}$ are parametrized by $\mathcal{W}_{\mathbb{R}}$.
- The j-map is:

$$j : \mathcal{W}_{\mathbb{R}} \to \mathbb{R} \qquad (f, g) \mapsto 1728\frac{4f^3}{4f^3 + 27g^2}$$

Two elements of $\mathcal{W}_{\mathbb{R}}$ define elliptic curves which are isomorphic over $\mathbb{C}$ if and only if they map to the same element of $\mathbb{R}$ under the j-map. Furthermore, the j-map is surjective.[3] Thus, the space of *real* elliptic curves up to *complex* isomorphism can be identified with $\mathbb{R}$.

- Next, we classify real elliptic curves up to real isomorphism. This means we have to classify quadratic twists. Since $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{[1], [-1]\}$, every elliptic curve over $\mathbb{R}$ admits exactly one nontrivial quadratic twist.

The following elliptic curves represent the two $\mathbb{R}$-isomorphism classes of elliptic curves with j-invariant 1728:

$$E^+ : \quad y^2 = x^3 + x \tag{4.1}$$
$$E^- : \quad y^2 = x^3 - x \tag{4.2}$$

Every other elliptic curve over $\mathbb{R}$ is isomorphic to an elliptic curve of the form:

$$E_f^+ : \quad y^2 = x^3 + fx + 1 \tag{4.3}$$
$$E_f^- : \quad y^2 = x^3 + fx - 1 \tag{4.4}$$

If $4f^3 > 4f^3 + 27g^2$, the elliptic curve has j-invariant greater than 1728. If $0 < 4f^3 < 4f^3 + 27g^2$, the elliptic curve has j-invariant less between 0 and 1728. If $f < 0$, the elliptic curve has negative j-invariant.

Let $E/\mathbb{R}$ be an elliptic curve given by the Weierstrass equation:

$$y^2 = x^3 + fx + g$$

[3]Since the map is continuous on $\mathcal{W}_{\mathbb{R}}$, we can take limits and use the intermediate value theorem to check this.

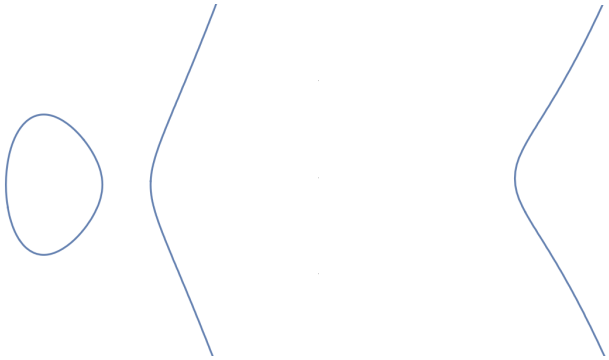


Figure 4.1: *A pair of real elliptic curves. The one on the left has j-invariant greater than 1728 and the one on the right has j-invariant less than 1728.*

Assume that the j-invariant of E is not equal to 1728 (equivalently, $g \neq 0$). Then the following conditions are equivalent:

- The discriminant of $x^3 + fx + g$ is positive.
- $j \geq 1728$.
- The cubics $x^3 + fx \pm g$ split completely over $\mathbb{R}$.
- Both E and the quadratic twist of E have all 2-torsion points defined over $\mathbb{R}$.

If $j = 1728$, one of the $\mathbb{R}$-isomorphism classes satisfies all of these conditions, and the other only satisfies $j \geq 1728$.

Furthermore, these conditions can be checked easily if we represent the set of points on $E(\mathbb{C})$ as $\mathbb{C}/\Lambda$, together with an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

This allows us to obtain pictures of the moduli space of real elliptic curves using the familiar pictures of the moduli space of complex elliptic curves, see 4.2.

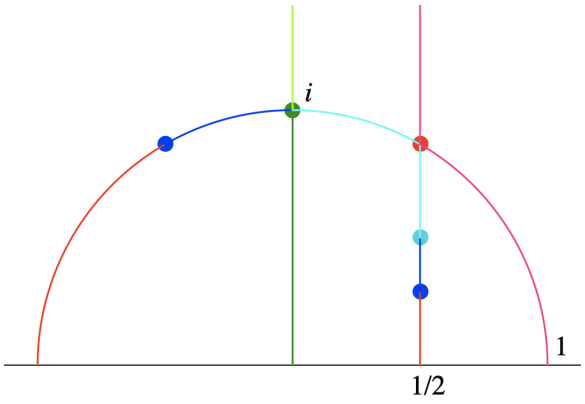


Figure 4.2: *A fundamental domain for the moduli space of real elliptic curves as a subset of the upper half plane. The green segments represent elliptic curves with* $j > 1728$*, the blue segments represent elliptic curves with* $0 < j < 1728$ *and the red/pink segements represent elliptic curves with negative* j*-invariant.*

Thus, the space of elliptic curves over $\mathbb{R}$ consists of two copies of $\mathbb{R}$, although something weird is happening at $j = 1728$.

It remains to classify the genus one curves over $\mathbb{R}$ without an $\mathbb{R}$-point. Of course, every genus one curve over $\mathbb{R}$ has a point after passing to $\mathbb{C}$.

- We can try to compute $WC(E/\mathbb{R})$ for each elliptic curve. Since $WC(E/\mathbb{R})$ is the cohomology group of a $\mathbb{Z}/2$-module, we can compute it explicitly.

- Alternatively, we can use the fact that every genus one curve has a model as $w^2 = q(u, v)$ for some quartic $q(u, v)$, so we can try to understand the quotient of the space of real quartics by $SL_2(\mathbb{R})$.

4.4.1 Weil-Chatelet

To compute the Weil-Chatelet group of an elliptic curve $E/\mathbb{R}$, we need to know the Mordell-Weil group.

Fortunately, we can determine this directly from the j-invariant, provided $j \neq 1728$:

- If $j > 1728$, the Mordell-Weil group is isomorphic to $(\mathbb{Z}/2) \times S^1$.
- If $j < 1728$, the Mordell-Weil group is isomorphic to S^1.
- If $j = 1728$, one of the $\mathbb{R}$-isomorphism classes has Mordell-Weil group $(\mathbb{Z}/2) \times S^1$ and the other has S^1.

To compute $WC(E/\mathbb{R})$, we will use the short exact sequence 2.4:

$$0 \to E(\mathbb{R})/2E(\mathbb{R}) \to H^1(G, E[2]) \to WC(E/\mathbb{R})[2] \to 0$$

Since every class in $WC(E/\mathbb{R})$ has index 2, and period divides index, it follows that every class in $WC(E/\mathbb{R})$ has period 2,so $WC(E/\mathbb{R}) = WC(E/\mathbb{R})[2]$, so the exact sequence above actually says there is a surjection $H^1(G, E[2]) \to WC(E/\mathbb{R})$.

The group $H^1(G, E[2])$ is small: we only need to determine whether an element of $E[2]$ is a possible image for σ. This will depend on how complex conjugation acts on $E[2]$, but there are only 2 ways it could act - trivially, or else it fixes one of the nonidentity points and permutes the other two.

- If G acts trivially on $E[2]$ (i.e. if $E[2]$ is defined over $\mathbb{R}$), then $H^1(G, E[2]) \cong Hom(G, E[2]) \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

  Furthermore, $2E(\mathbb{R}) \cong S^1$ so $E(\mathbb{R})/2E(\mathbb{R}) \cong \mathbb{Z}/2$. THus the exact sequence above is equivalent to:

  $$0 \to \mathbb{Z}/2 \to (\mathbb{Z}/2) \times (\mathbb{Z}/2) \to WC(E/\mathbb{R}) \to 0$$

  so we conclude that $WC(E/\mathbb{R}) \cong \mathbb{Z}/2$.

- Otherwise E only has one two 2-torsion point defined over $\mathbb{R}$. We write P for the 2-torsion point defined over $\mathbb{R}$ and T_1, T_2 for the other nontrivial 2-torsion points.

  Now, $E(\mathbb{R}) = S^1$ and the doubling map $S^1 \to S^1$ is surjective. This means $E(\mathbb{R}) = 2E(\mathbb{R})$ so $E(\mathbb{R})/2E(\mathbb{R}) = 0$. Thus, $WC(E/\mathbb{R}) \cong H^1(G, E[2])$.

  A computation shows that the only cocycles are the maps $\sigma \mapsto 0$ and $\sigma \mapsto P$. Furthermore, since $P = T_1 + T_2 = T_1 - T_2. = T_1 - \sigma(T_1)$, that cocycle is a coboundary. Thus, we conclude that $H^1(G, E[2])$ is also trivial in this case, and thus $WC(E/\mathbb{R}) = 0$.

Thus, to recap: $E/\mathbb{R}$ has nontrivial WC group if and only if $E[2] \subset E(\mathbb{R})$.

Next, we try to extend our previous picture to one that contains these extra genus one curves - we really only need to add a copy of $(1728, \infty)$ and a copy of $[1728, \infty)$ to our two copies of $\mathbb{R}$ in some meaningful way. To achieve this, we use the fact that every genus one curve over $\mathbb{R}$ has a model as $w^2 = Q(u, v)$. We will try to find representatives for each $\mathbb{R}$-isomorphism class in the space of quartics up to the action of $SL_2(\mathbb{R})$.

4.4.2 Models

Finally, we describe a fundamental domain for real genus one curves in the space of real quartics modulo the action of $SL_2(\mathbb{R})$.

Let $Q(u, v)$ be a real binary quartic, and assume that $Q(u, 1)$ has 4 distinct roots in $\mathbb{C}$. Note that $Q(u, v)$ has a factorization:

$$Q(u, v) = Q_1(u, v)Q_2(u, v)$$

where Q_1, Q_2 are real quadratic forms. This factorization is not - if Q splits

completely over $\mathbb{R}$, then there are 6 factorization of Q into quadratic forms which are genuinely distinct.

We restrict attention to quartics that do *not* split completely. The quartics that split completely define elliptic curves with full 2-torsion over $\mathbb{R}$, and we've already classified those.

We assume that $Q_1(u, v)$ is an anisotropic quadratic form over $\mathbb{R}$. Furthermore, replacing Q_1, Q_2 by $-Q_1, -Q_2$ doesn't change Q, so we may further assume that $Q_1(u, v)$ is a positive definite quadratic form.

1. We can do a change of variable so that $Q_1(u, v) = \lambda(u^2 + v^2)$ for some positive real number λ. Furthermore, replacing Q_2 by λQ_2, we may assume that $Q_1(u, v) = u^2 + v^2$.

   In other words, the symmetric matrix that represents[4] $Q_1(u, v)$ is the identity.

2. We can act on the space of binary quadratic forms by $SO(2)$. The action fixes $u^2 + v^2$. Furthermore, every symmetric matrix can be diagonalized using the action of $SO(2)$. Thus, we can find a change of variable that leaves $Q_1(u, v) = u^2 + v^2$ unchanged and puts $Q_2(u, v)$ in diagonal form.

Thus, every genus one curve over $\mathbb{R}$ can be represented by an equation of the form:

$$w^2 = (u^2 + v^2)(au^2 + bv^2)$$

for some $a, b \in \mathbb{R}^\times$.

This gives us a 2-dimensional parameter space for all real genus one curves.

- $C_{a,b}$ can only fail to have an $\mathbb{R}$-point if $a, b < 0$.

[4]This is sometimes referred to as the polarization of Q.

- We can define a j-map on the space of pairs (a, b) by sending each pair (a, b) to the j-invariant of the Jacobian of $C_{a,b}$.

- If we replace (a, b) by (ta, tb) for some $t \in \mathbb{R}$, the new Jacobian is the quadratic twist of the original by t.

  Thus, scaling by positive real numbers doesn't change the $\mathbb{R}$-isomorphism class of the genus one curve, and scaling by a negative real number changes the $\mathbb{R}$-isomorphism class but not the $\mathbb{C}$-isomorphism class.

If $a + b = 0$, the genus one curve has j-invariant 1728. If $ab = 0$, we have a nodal curve.

Altogether, this means we can represent the moduli space by the unit circle in the (a, b)-plane. To determine the isomorphism class of the genus one curve associated to a point (a, b), we use the Jacobian formula to determine the isomorphism class of the Jacobian. Each elliptic curve has at most one nontrivial torsor, and the only pairs (a, b) that represent curves without $\mathbb{R}$-points are the pairs with $a, b < 0$.

We compute:

$$j(a, b) = \frac{16\left(a^2 + 14ab + b^2\right)^3}{ab(a - b)^4} \tag{4.5}$$

For a fixed value of $j_0 \in \mathbb{R}$, there are at most 12 (a, b) with that j-invariant (up to replacing (a, b) by a scalar multiple):

$$j(a, b) = j_0 \quad \Longleftrightarrow \quad 16\left(a^2 + 14ab + b^2\right)^3 = j_0 ab(a - b)^4 \tag{4.6}$$

Now the right hand side of 4.6 is a homogenous polynomial of degree 6 in a, b, so it has at most 6 solutions in $\mathbb{P}^1_{\mathbb{R}}$. Each root in $\mathbb{P}^1$ gives us two pairs (a, b), up to scaling by $\mathbb{R}^+$.

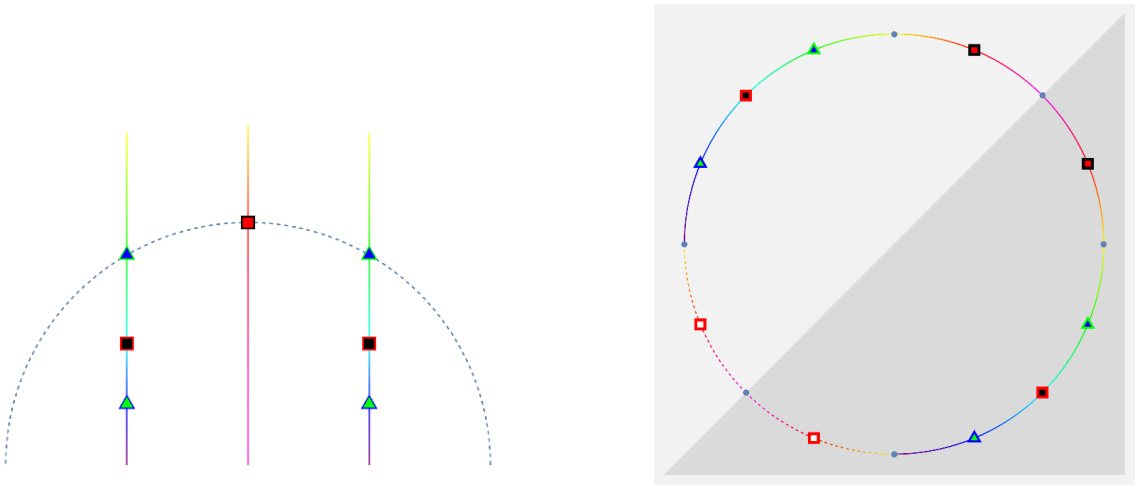


Figure 4.3: *On the left, we have the picture of the moduli space of elliptic curves over* $\mathbb{R}$*, depicted as a subset of the upper half plane. On the right, we have a picture of the moduli space of real genus one curves, depicted as a subset of the space of equations of quartic equations.*

We can determine when the number of roots changes by computing the discriminant of 4.6, and setting $j_0 = 0$.

Altogether, we can show that the unit circle in the (a, b) plane contains a fundamental for $\mathbb{R}$-isomorphism classes of genus one curves. Furthermore, there are no "redundancies" - each isomorphism class is represented exactly once.

For more details on what the picture means, see the author's website.

4.4.3 Comments

- We found a fundamental domain in the set of quartics that do not split completely. This is a little strange - it reflects the fact that completely split quartics and irreducible quartics both give rise to genus one curves with $j > 1728$ (and every curve with $j > 1728$ can be described by both types of models).

- To compute the Weil-Chatelet group, we used the fact that S^1 is a divisible group.
- To compute the quotient of the space of quartics, we needed the spectral theorem.

Part II

Elliptic Fibrations and F-theory

Chapter 5

Elliptic Fibrations

5.1 General Definitions

We start by defining elliptic fibrations in purely geometric terms.

Definition 5.1. *Let k be a field and B/k an irreducible variety of dimension d.*

A genus one fibration over B is a pair (X, π), where:

- *X is a variety of dimension $d+1$ over k.*
- *$\pi : X \to B$ is a proper, flat morphism of k-varieties.*
- *For almost all $b \in B$, $\pi^{-1}(b)$ is a smooth curve of genus 1.*

An elliptic fibration is a pair $((X, \pi), s)$ consisting of a genus one fibration (X, π) and a section $s : B \to X$ of π.

We say that a genus one fibration is:

- *Smooth*
- *Singular*

- *Gorenstein*

if X has that property.

The discriminant locus of an genus one fibration is the subvariety of B containing all points whose fiber is not smooth.

There are two types of elliptic fibrations we will *not* be interested in.

Proposition 5.2. *Let $X \to B$ be an elliptic fibration.*

We say that $X \to B$ is of product type if X is birational to a product $B \times E$. We say that $X \to B$ is isotrivial if the smooth fibers of X have the same j-invariant.

It's clear that every fibration which is of product type is isotrivial. The converse is false. For example, the elliptic surface over $\mathrm{Spec}\mathbb{C}[[t]]$:

$$y^2 = x^3 + tx$$

is not a product, but every smooth fiber has j-invariant 1728.

In fact, if we fix any pair $f, g \in \mathbb{C}$ with $4f^3 + 27g^2 \neq 0$, then we have an isotrivial fibration:

$$y^2 = x^3 + t^2 f x + t^3 g$$

There are several reasons one may want to avoid isotrivial fibrations. They are not used in F-theory[1]. From a mathematical perspective, we gain two crucial tools by restricting to fibrations which are not isotrivial:

- The Mordell-Weil theorem generalizes to elliptic fibrations which are not isotrivial. In particular, we may assume $MW(X/B)_{tors}$ is finite for all fibrations we discuss and the rank of the Mordell-Weil group is finite.

[1] One reason physicists became interested in elliptic fibrations was because the physical data they were studying consisted of a "point varying in $\mathcal{H}/SL_2(\mathbb{Z})$", which one could think of as a family of elliptic curves under the identification of $\mathcal{H}/SL_2(\mathbb{Z})$ with the moduli space of elliptic curves. In an isotrivial fibration, there is no variation in the moduli space.

See [42] or [61] for details.

- The results of [32] and [17] classify Calabi-Yau elliptic fibrations in dimension 3,4 which are not isotrivial. By restricting attention to fibrations which are not isotrivial, we can use their results to reduce our proofs to computations over a finite list of bases.

- Finally, elliptic fibrations which are not isotrivial can't have complex multiplication.

We will mainly be interested in fibrations which are not isotrivial.

Let $X \to B$ be a genus one fibration, and let $b \in B$ be a point in the discriminant locus.

The fiber over b is a singular variety of dimension 1. If $X \to B$ has a section, then the fibers will be one of the following:

- A nodal genus one curve.

- A cuspidal genus one curve.

- A connected union of rational curves.

See 6.2 for details.

If $X \to B$ is a genus one fibration without section, then it may also have fibers which are everywhere singular.

Definition 5.3. *We say that the fiber over b is a multiple fiber if the fiber is everywhere singular.*

Let $\eta \subset B$ be the generic point and K the function field of B. The definition of elliptic fibration allows us to endow the fiber $\pi^{-1}(\eta)$ with the structure of an

elliptic curve E/K: it's clear that the fiber has genus one, and we can use the section $B \to X$ to obtain a marked point defined over K.

We can define analogs of the Mordell-Weil group, and prove analogous theorems about it, using the relative Picard functor. We require fibrations to be proper and flat to guarantee representability of that functor.

In particular, if we have a genus one fibration $Y \to B$ without section, then there is an associated elliptic fibration $X \to B$ that we will refer to as the Jacobian elliptic fibration, and which is defined in exactly the same way as the Jacobian elliptic curve, with the Picard group replace by the relative Picard group over B.

There are two different flavors of elliptic fibrations: fibrations over Spec$R$ and fibrations over projective bases.

5.1.1 Affine Base

Let R be an integral domain with fraction field K. Assume $char(K) \neq 2, 3$, and let $f, g \in R$, with $4f^3 + 27g^2 \neq 0$.

Let $\mathcal{E} \subset \mathbb{P}^2_R$ be the variety:

$$y^2z = x^3 + fxz^2 + gz^3$$

Then $\mathcal{E} \to \text{Spec}R$ is an elliptic fibration.

If we start with an elliptic curve E/K given by a Weierstrass equation, we say the equation spreads out to Spec$R$ if $f, g \in R$. We call the fibration $\mathcal{E} \to \text{Spec}R$ an integral model for E/K.

Finally, we need to define minimal integral models.

Let $\mathcal{E} \to \text{Spec}R$ be an integral model for an elliptic curve E/K:

$$y^2 = x^3 + fx + g$$

We say this is a minimal integral model if, for each irreducible factor ϖ of $\gcd(f, g)$, either $\nu(f) < 4$ or $\nu(g) < 6$. We can always obtain a minimal integral model from an integral model by pulling out factors of ϖ^4 from f and ϖ^6 from g, at least when the base is Spec$R$, for R a UFD.[2]

Furthermore, there is a unique morphism of R-schemes $\mathcal{E} \to \mathcal{E}^{min}$ to the minimal integral model.

5.1.2 Projective Base

Let $B = \mathbb{P}^n$ for some integer $n > 0$ and let $\mathcal{L} = \mathcal{O}(d)$ be an ample line bundle on $\mathbb{P}^n$.

The space of global sections of $\mathcal{L}$ can be identified with the vector space of homogenous polynomials of degree d in $n + 1$ variables.

Let f be a global section of $\mathcal{L}^{\otimes 4}$ and g a global section of $\mathcal{L}^{\otimes 6}$. Define $\Delta = 4f^3 + 27g^2$; note that this is a global section of $\mathcal{L}^{\otimes 12}$. If $\Delta \neq 0$, then we can define:

$$y^2 = x^3 + fxz^4 + gz^6$$

Starting from an elliptic fibration over an affine subset of $\mathbb{P}^n$, we can always be spread out to an elliptic fibration over $\mathbb{P}^n$ by homogenizing the coefficients appropriately.

[2]There are fibrations that do not admit a globally minimal integral model, although we will not need to worry about those.

5.2 Weierstrass models and the fundamental line bundle

Let $X \to B$ be an elliptic fibration. Our goal in this section is to generalize the notion of Weierstrass equation to elliptic fibrations over a general variety B (not necessarily of the form Spec$R$).

If every fiber of $X \to B$ is a smooth elliptic curve, then we have the following result from [53]:

Proposition 5.4. *Let B be a variety over k and $\mathcal{E} \to B$ an elliptic fibration over B. If $V(\Delta) = \emptyset$, then there is an open cover $\cup \text{Spec}R_i$ of B such that, over each $\text{Spec}R_i$, the fibration is isomorphic to:*

$$y^2 = x^3 + f_i x + g_i \qquad (f_i, g_i \in R_i)$$

Furthermore, $4f^3 + 27g^2 \in R_i^\times$ for all i.

If B is projective, then any fibration satisfying the conditions of the previous theorem is simply a product $E \times B$.

To obtain more interesting Weierstrass fibrations over a projective base, we use sections of line bundles to define a global Weierstrass equation.

Definition 5.5. *Let B be a projective variety.*

A Weierstrass triple over B is a triple $(\mathcal{L}, f, g)$, where $\mathcal{L}$ is a line bundle over B, f is a global section of $\mathcal{L}^{\otimes 4}$ and g is a global section of $\mathcal{L}^{\otimes 6}$.

We associate to a Weierstrass triple the form $\Delta = 4f^3 + 27g^2$, which is a global section of $\mathcal{L}^{\otimes 12}$.

Now, let $(\mathcal{L}, f, g)$ be a Weierstrass triple. Let $\mathbb{P}_B$ be the projectivization of the rank 3 vector bundle $\mathcal{L}^{\otimes 2} \oplus \mathcal{L}^{\otimes 3} \oplus \mathcal{O}_B$ over B, endowed with coordinates (x, y, z),

and define a relative curve $X \to B$ in $\mathbb{P}_B$ by:

$$y^2z = x^3 + fxz^2 + gz^3$$

Then $X \to B$ is an elliptic fibration over B. Conversely, every elliptic fibration is birational to a fibration determined by a Weierstrass triple.

First, we define:

Definition 5.6. *The fundamental line bundle of a genus one fibration $\pi : X \to B$ is the line bundle $\mathcal{L}_{X/B} := (R^1\pi_*\mathcal{O}_X)^{-1}$ on B.*

Proposition 5.7. *Let $X \to B$ be an elliptic fibration and let $X_0 \to B$ be the fibration obtained by contracting every curve in the fibers which does not meet the zero section.*

Then X_0 is isomorphic, as a B-scheme, an elliptic fibration defined by a Weierstrass triple $(\mathcal{L}_{X_0/B}, f, g)$.

Proof. [53] □

If one of f, g is 0, then the fibration is isotrivial and has complex multiplication. If both are 0, or more generally if $\Delta = 0$, the associated elliptic fibration is every degenerate. We will assume throughout that f, g, Δ are not everywhere 0 on B.

5.2.1 Calabi-Yau

A projective variety X/k is Calabi-Yau if $\omega_X \cong \mathcal{O}_X$.[3]

A Calabi-Yau variety of dimension 1 is a genus one curve. In higher dimension, genus one fibrations and Calabi-Yau varieties no longer coincide, although they do overlap.

[3]If $\dim X = 2$, then one also has to add the condition that X is simply connected.

- There are many examples of Calabi-Yau's which do not admit an elliptic fibration. For example, the quintic threefold and any K3 surface of Picard rank 1 have no genus one fibration structure.

- However, most known examples of Calabi-Yau's surprisingly *do* admit a genus one fibration.

The canonical bundle formula makes it easy to characterize Weierstrass triples that give rise to Calabi-Yau elliptic fibrations:

Proposition 5.8. *Let $\pi : X \to B$ be an elliptic fibration. Then:*

$$\omega_X \cong \pi^*(\mathcal{L}_{X/B} \otimes \omega_B)$$

Since we're assuming that $X \to B$ has a section, $\phi^* : Pic(B) \to Pic(X)$ is injective so ω_X is trivial iff $\mathcal{L}_{X/B} \cong \omega_B^{-1}$.

This allows us to show that if $X \to B$ is a non-isotrivial Calabi-Yau fibration, then B is Fano[4] and $\mathcal{L}_{X/B} \cong \omega_B^{-1}$.

5.3 Resolutions

Let $X \to B$ be an elliptic fibration, say one of the elliptic fibrations in the examples. Let $Z \subset B$ be an irreducible variety contained in the discriminant locus of B, and let ν_Z be the associated valuation.

Since $Z \subset V(\Delta)$, $\nu_Z(\Delta) \geq 1$. If $\nu_Z(\Delta) > 1$, then the total space X has singularities over each point on Z.

Definition 5.9. *Let $X \to B$ be an elliptic fibration.*

[4]Or a blow-up of a Fano surface.

A resolution of $X \to B$ is an elliptic fibration $X' \to B'$, together with morphisms:

$$\begin{array}{ccc} X' & \longrightarrow & X \\ \downarrow & & \downarrow \\ B' & \longrightarrow & B \end{array} \tag{5.1}$$

such that the horizontal arrows are birational morphisms and X' is nonsingular.

A B-resolution of X is a resolution $X' \to B$, where the morphism $X' \to X$ is a morphism of B-schemes.

If $S \to C$ is any elliptic surface, we can always find a C-resolution $\tilde{S} \to C$, see (6.1). Furthermore, if $S \to C$ is a minimal fibration, then the resolution $\tilde{S} \to S$ is crepant. When $\dim B = 2$, resolutions still exist, but they are no longer unique or crepant. Furthermore, we can no longer guarantee that they are B-resolutions - see (7.1).

In applications, we only want to study models that admit a crepant resolution. However, "existence of a crepant resolution" is not a deformation invariant property - in other words, there are Weierstrass models which admit a crepant resolution, but where any deformation ceases to have a crepant resolution. We will see an example of this is (8.2). This type of phenomenon is also discussed in [9].

In some cases though, we can rely on numerical criteria to conclude that a nice resolution does *not* exist. Precisely:

Definition 5.10. *Let B be a smooth variety over k and let $X \to B$ be an elliptic fibration, with associated Weierstrass triple $(\mathcal{L}, f, g)$.*

Let $Z \subset V(\Delta)$ be an irreducible subvariety, and let ν be the associated valuation. Let d be the codimension of Z in B. We say the triple $(\mathcal{L}, f, g)$ has inadmissible

singularities over Z if:

$$\nu_Z(f) \geq 4d \qquad \text{and} \qquad \nu_z(g) \geq 6d$$

For example, $(\mathcal{L}, f, g)$ has inadmissible singularities over a codimension 1 locus of B iff the fibration is not minimal. The methods of (9) show that while there *are* elliptic 3-folds with trivial canonical bundle and with points of order as high as 10 in the Mordell-Weil torsion group, these 3-folds necessarily have inadmissible singularities if the torsion point has order at least 7.

Chapter 6

Elliptic Surfaces

In this section, k is an algebraically closed field and K is a field of transcendence degree 1 over k. We write C/k to denote the unique smooth, projective curve over k with function field K.

In this chapter we review properties of elliptic surfaces over C.

6.1 Néron models

The goal of this section is to give a brief account of Néron models. Much has already been written about this topic, so we will mainly state and explain the results that are needed later on. For a full account of the theory, see [11]. The results in this section can also be found in [61]. See also [38] for a discussion of these results in the context of F-theory.

We start by defining Néron models for arbitrary K varieties.

Definition 6.1. *Let X/K be a smooth and separated variety. A Néron model for X/K is a smooth and separated variety $\mathcal{X} \to C$ satisfying the following conditions:*

- *The generic fiber of $\mathcal{X} \to C$ is isomorphic to X/K.*

- *For any smooth C-scheme $\mathcal{Y} \to C$, with generic fiber Y/K, and any rational map $Y \to X$, there is a unique morphism of C-schemes $\mathcal{Y} \to \mathcal{X}$ extending ϕ.*

Since Néron models are characterized by a universal property, they are unique, so long as they exist.

Furthermore:

- The universal property, applied to C, shows that there is a bijection between $X(K)$ and $\mathcal{X}(R)$.
- If X/K is an algebraic group, then $\mathcal{X}$ is a group scheme over C (see 6.1.1.

Proposition 6.2. *Let E/K be an elliptic curve, let $\mathcal{S} \to C$ be a model for E/K which is proper, minimal and smooth and let $\mathcal{E} \to C$ the the largest C-subscheme of $\mathcal{S}$ which is smooth over C.*

Then $\mathcal{E} \to C$ is a Néron model for E/K.

Proof. Theorem 6.1 in Ch. 4 of [61].

□

We can always resolve singularities in the fibers of an elliptic curve. Minimality of the fibration is equivalent to the absence of -1 curves in the fibers; since minimal smooth models exist for surfaces, we can always find a model of E/K satisfying the conditons of the previous theorem. Thus, not only do Néron models exist, but we can characterize them geometrically.

Now, to actually construct the minimal smooth model, we need to resolve singularities on the Weierstrass model. This can be achieved using Tate's algorithm.

Note that if $W \to C$ is a *minimal* Weierstrass surface over a smooth curve C, then the singularities on W are locally isomorphic to du Val singularities. In that

case, we can find a crepant resolution $S \to W$, and $S \to C$ is a Néron model for E/K.

We describe the geometry of the resolved fibers in the next section. We also explain how to determine the isomorphism type of the resolved fiber in the Néron model directly from $\nu(f), \nu(g), \nu(\Delta)$.

6.1.1 Group Schemes

In this section, we describe group schemes over an arbitrary base. We continue to write C for the base to make it clear how to relate the results of this section to Néron models.

Definition 6.3. *A group scheme over C is a C-scheme (i.e. a scheme G with a structure morphism $G \to C$), together with morphisms (e, i, μ):*

- *$e : C \to G$ is a section of the structure morphism.*
- *$i : G \to G$ is a morphism of C-schemes that we call the inversion morphism.*
- *$\mu : G \times_C G \to C$ is a morphism of C-schemes that we call the multiplication map.*

These morphisms allow us to formulate a group law over C - the identity is the section $C \to G$, the inversion map takes elements to their inverse and μ takes two elements to their sum.

We require that certain squares constructed using morphisms commute in order to encode the usual group theory axioms.

Every elliptic curve E/K has the structure of a group scheme over Spec$K$.

By the functorial characterization of the Néron model, the group law extends to $\mathcal{E}$. In particular, the group law extends to the singular fibers.

- Suppose we have an I_n singularity over a point. The resolved fiber is a chain of $\mathbb{P}^1$'s. The Néron model is obtained by taking a maximal open set in the $\mathbb{P}^1$ which meets the zero section. Since each $\mathbb{P}^1$ meets exactly two other $\mathbb{P}^1$'s at a single point, the maximal open set is $\mathbb{P}^1 - \{0, \infty\}$.

  We identify $\mathbb{P}^1 - \{0, \infty\}$ with $k^\times$; the group law is simply the group law on $k^\times$. Thus, I_n fibers are sometimes referred to as multiplicative singularities.

- For every other singularity type, the $\mathbb{P}^1$ that meets the zero section only intersects one other $\mathbb{P}^1$. Thus, the Néron model is $\mathbb{P}^1 - \{\infty\}$. The group law is just addition on k, so these fibers are sometimes referred to as additive singularities.

One can use the group structure on singular fibers to relate the geometry of the fibration to arithmetic properties of the generic fiber.

For example, one can use this type of consideration to bound the size of the Mordell-Weil torsion group of an elliptic fibration with an additive fiber in codimension 1 - we have $|MW(E/K)|_{tors} \geq 4$ in this case. See [48] for a proof when $k = \mathbb{C}$ and [58] for a proof in arbitrary characteristic.

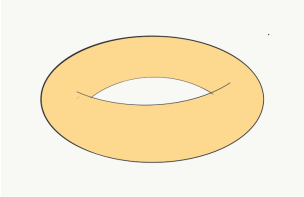
6.2 Kodaira fiber types

Let k be an algebraically closed field, R a DVR with residue field k and fraction field K, and let E/K be an elliptic curve. Let $W \to \text{Spec}R$ be a minimal integral model and let $\mathcal{E} \to \text{Spec}R$ be the Néron model. Let $W_\mathfrak{p}, \mathcal{E}_\mathfrak{p}$ be the fiber over the closed point of Spec$R$.

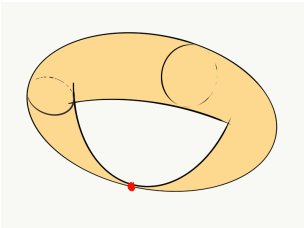
Proposition 6.4. *1. $W_\mathfrak{p}$ has at worst a du Val singularity.*

2. *The resolved fiber is isomorphic to one of the following:*

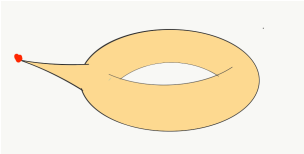
- *If the fiber is irreducible, then it is isomorphic to one of the following:*
  - *A fiber of type I_0 is a smooth elliptic curve E.*



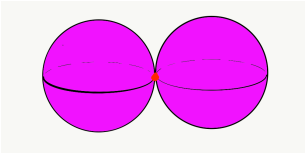
  - *A fiber of type I_1 is a nodal curve of genus one.*



  - *A fiber of type II is a cuspidal curve of genus one.*



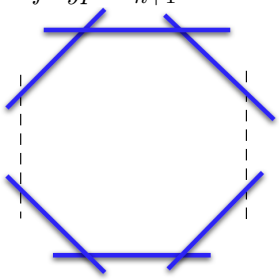
- *Type III: Two $\mathbb{P}^1$'s meeting tangentially at a point.*



- *Type IV: Three $\mathbb{P}^1$'s meeting at a single point.*

- *In all other cases, the singularity is a du Val singularity and the resolved fiber is a configuration of $\mathbb{P}^1$'s arranged so that their incidence graph is an ADE Dynkin diagram. See A for more on ADE singularities.*

– *If the singularity on the Weierstrass model is of type A_n, we say that the resolved fiber is of type I_{n+1}.*



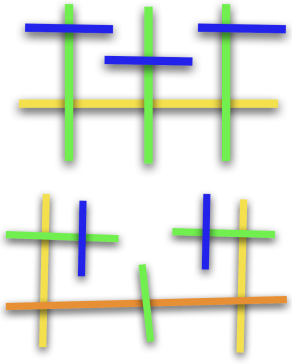
The resolved fiber is a collection of $\mathbb{P}^1$'s arranged in a chain - that is, each $\mathbb{P}^1$ meets exactly two other $\mathbb{P}^1$s.

These singularities are sometimes referred to as fibers of multiplicative type[1]*, or as semistable fibers.*

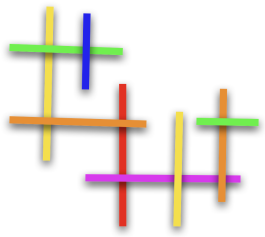
– *If the singularity on the Weierstrass model is of type D_n, the resolved fiber is said to be of Kodaira type I_n^*:*

we say that the resolved fibre is of type I_n^*.

– *Finally, if the singularity on the Weierstrass model is of type E_6, E_7 or E_8, we say that the resolved fiber is of type IV^*, III^*, II^*, respectively.*



[1] To emphasize the group structure in the Néron model.



Proof. See [61] Ch. IV Thm. 8.2.

□

Next, we explain how to determine the singularity type directly from the valuations of f, g, Δ at the singular point.

6.2.1 Tate's algorithm

We start with a minimal, integral Weierstrass model:

$$y^2 = x^3 + fx + g$$

over a DVR. Furthermore, we assume for now that the residue field is algebraically closed.

We have a singularity of type I_n if $\nu(f) = \nu(g) = 0$ and $\nu(\Delta) = n$. Note that this characterization of I_n fibers is valid even if $n = 0, 1$.

If $\nu(f) = 0$ and $\nu(g) \neq 0$ or $\nu(f) \neq 0$ and $\nu(g) = 0$, then the special fiber has complex multiplication, but is otherwise smooth, so we get an I_0 fiber.

In every other case:

- Both $\nu(f)$ and $\nu(g)$ are nonzero.
- Either $\nu(f) < 4$ or $\nu(g) < 6$.

If $3\nu(f) \neq 2\nu(g)$, then $\nu(\Delta)$ is determined by $\nu(f), \nu(g)$. There are only finitely many inequivalent ways to choose f, g with this property:

- If $\nu(g) = 1$ and $\nu(f) \geq 1$, we have $\nu(\Delta) = 2$. The fiber in the Néron model is of type II in this case - we don't actually have to blow anything up.
- If $\nu(f) = 1, \nu(g) \geq 2$, we have $\nu(\Delta) = 3$. The resolved fiber is of type III.
- If $\nu(g) = 2$ and $\nu(f) \geq 2$, we have $\nu(\Delta) = 4$. The resolved fiber is of type IV.

Note that these singularities are all *reduced*, and the remaining ones are not reduced.

Before discussing the remaining singularities with $3\nu(f) \neq 2\nu(g)$, we discuss Weierstrass models with $\nu(f) = 2$ and $\nu(g) = 3$. In this case, $\nu(\Delta)$ depends on f, g- the discriminant vanishes to order at least 6, but can vanish to arbitrarily high order.

We have an I_n^* singularity if $\nu(f) = 2, \nu(g) = 3$ and $\nu(\Delta) = 6 + n$.

There are three more possibilities to consider:

- $\nu(f) \geq 3$, $\nu(g) = 4$ gives $\nu(\Delta) = 8$ and a resolved fiber of type IV^*.
- $\nu(f) = 3, \nu(g) \geq 5$ gives $\nu(\Delta) = 9$ and a resolved fiber of type III^*.
- $\nu(f) \geq 4, \nu(g) = 5$ gives $\nu(\Delta) = 10$ and a resolved fiber of type II^*.

6.3 Elliptic surfaces over $\mathbb{P}^1$

Let $R = \mathbb{C}[t]$, $K = \mathbb{C}(t)$ and let E/K be an elliptic curve.

- We can find a Weierstrass equation for E/K as:

$$y^2 = x^3 + fx + g$$

with $f, g \in K$.

- Next, replacing f, g by $\phi(t)^4 f(t), \phi(t)^6 g(t)$ for some $\phi(t) \in R$ if necessary, we may assume that $f, g \in R$.

- Similarly, replacing $f, g \in R$ by $\phi(t)^{-4} f(t), \phi(t)^{-6} g(t)$ if necessary, we may assume that we have a minimal integral model over R.

Write $\deg(f), \deg(g)$ to denote the degree of f, g, respectively. Let:

$$d = \max\left\{\left\lceil \frac{\deg(f)}{4} \right\rceil, \left\lceil \frac{\deg(g)}{6} \right\rceil\right\}$$

and define:

$$F(t_0, t_1) = t_0^{4d} f\left(\frac{t_1}{t_0}\right) \quad G(t_0, t_1) = t_0^{6d} g\left(\frac{t_1}{t_0}\right)$$

Then:

- $F(1, t) = f(t)$ and $G(1, t) = g(t)$.

- F, G are homogenous polynomials of degree $4d, 6d$ respectively.

- Let $f_\infty(t) = F(t, 1)$ and $g_\infty(t) = G(t, 1)$. Then:

$$y^2 = x^3 + f_\infty x + g_\infty$$

  is a minimal integral model for an elliptic curve E/R.

Thus, $(\mathcal{O}(d), F, G)$ is a Weierstrass triple over $\mathbb{P}^1$, and the associated elliptic surface is minimal.

We can use Tate's algorithm to (crepantly) resolve singularities on the Weierstrass surface, thus obtaining the Néron model $\mathcal{E} \to \mathbb{P}^1$ of the fibration.

- The topological Euler characteristic of $\mathcal{E}$ is $12d$.

- As explained earlier, the canonical bundle of $\mathcal{E}$ is determined by d. Precisely, $\mathcal{E}$ is a rational elliptic surface iff $d = 1$, $\mathcal{E}$ has Kodaira dimension 0 iff $d = 2$ and $\mathcal{E}$ has Kodaira dimension 1 if $d > 2$.

Note that the integer d, and thus $\omega_{\mathcal{E}}$ can be determined directly from the minimal integral equation - we don't actually have to compute the resolution.

6.3.1 Rational Elliptic Surfaces

Elliptic surfaces that appear in the wild may not come in Weierstrass form, and may not even look like an elliptic fibration.

In particular, we need the following characterization of rational elliptic surfaces:

Proposition 6.5. *Let $\pi : S \to \mathbb{P}^1$ be a rational elliptic surface. Then S is isomorphic to the blow-up of $\mathbb{P}^2$ at the base points of a pencil of cubics.*

Proof. Prop 8.1 in [58].

□

6.4 Quadratic Twists and Base Change

Finally, we explain how the singular fibers change if we pass to a quadratic twist or if we base change. We continue to assume that R is a DVR with algebraically closed residue field.

6.4.1 Quadratic Twists

Suppose we have two elliptic curves E_1, E_2 defined over R, and assume they become isomorphic after adjoining $\sqrt{a}$, where $a \in R$. We may assume that a is a nonsquare,

so $\nu(a)$ is odd. Replacing a by at^{-2} if necessary for some $t \in R$, we may assume that $\nu(a) = 1$.

Now, since E_1, E_2 are quadratic twists, there exists $t \in K$ such that $f_1 = t^2 f_2$ and $f_2 = t^2 f_3$.

If we assume $f_i, g_i \in R$, and we assume that both equations are minimal, then:

$$(\nu(f_1), \nu(g_1)) \equiv (\nu(f_2), \nu(g_2)) \pmod{()2\mathbb{Z} \times 3\mathbb{Z}}$$

means one of the elliptic curves has a reduced singularity and the other has a nonreduced singularity.

6.4.2 Base Change

Let E/R be an elliptic curve, K'/K a field extension and $R' \subset K'$ a valuation ring extending R.

If R'/R is unramified, the closed point splits up into several points, and the fiber over each of this points looks like the original singular fiber.

If R'/R is a ramified extension, then valuations get multiplied by some fixed constant after base changing.

Say $R' = R[\varpi^{1/d}]$, where ϖ is a uniformizer of R and $d > 1$. Let ν' be the valuation on R', normalized so $\nu(\varpi^{1/d}) = 1$. Let E/R be the elliptic curve:

$$y^2 = x^3 + fx + g$$

As shown above, the isomorphism type of the special fiber of the Néron model over Spec$R$ is determined by $\nu(f), \nu(g)$. This data also determiens the isomorphism type in the Néron model over SpecR', since $\nu'(f) = d\nu(f)$, $\nu'(g) = d\nu(g)$, etc.

In particular, if the special fiber is smooth, then any base change is smooth. If the special fiber is of multiplicative type, then so is the special fiber after any base

change, although the isomorphism type might change within that class - that is, if we start with an I_n fiber and pass to a ramified extension of degree d, then the special fiber in the new Néron model is of type I_{nd}.

On the other hand, the class of additive fibers is not stable under base extension. For example, if we have a fiber of type I_n^* and we pass to the ring $R[\sqrt{\varpi}]$, then the model over R' is not minimal. After passing to the minimal integral model, we find a singularity of multiplicative type. The semistable reduction theorem says that we can do this for any additve singularity.

Chapter 7

Elliptic 3-folds

In this section we will discuss elliptic 3-folds. Geometrically, this means we are looking at 3-folds X which have an elliptic fibration $X \to B$ to a surface B. Algebraically, we have an elliptic curve E/K, where K is a field of transcendence degree 2 over k.

We start by reviewing some of the ideas in [47], [20], [32] which are relevant to our problem.

The starting point is the idea of a Miranda model.

7.1 Miranda Models

Let $X \to B$ be an elliptic 3-fold. Our goal is to find a resolution $\tilde{X} \to \tilde{B}$. We describe the algorithm in [47] for finding such a resolution.

The main challenge is resolving singularities over collision points.

Definition 7.1. *Let $\pi : X \to B$ be an elliptic fibration, and let $V(\Delta) \subset B$ be the discriminant locus.*

We can write $V(\Delta) = \cup \Gamma_i$, where Γ_i are distinct irreducible subvarieties of B

of codimension 1.

A collision point is a point $b \in B$ such that $b \in \Gamma_i \cap \Gamma_j$ for $i \neq j$.

We say that the collision over b is of type $x + y$ if the fiber over Γ_1 is of type x and the fiber over Γ_2 is of type y.

Now, let $j : B \to \mathbb{P}^1$ be the rational map that sends a point $b \in B$ to the j-invariant of the fiber over b. In principle, j is only defined on the complement of the discriminant locus, but we can extend j generically so that the domain misses at most a codimension 2 locus of B.

Say we have an irreducible, smooth curve $\Gamma \subset B$ contained in the discriminant locus of $X \to B$. Let ν be the valuation associated to Γ.

- If the fiber over Γ is nodal, i.e. if $\nu(f) = \nu(g) = 0$, then the j-invariant is ∞.
- If $3\nu(f) > \nu(\Delta)$, e.g. if we have a type II or IV singularity, then the j-invariant is 0.
- If $3\nu(f) < \nu(\Delta)$, e.g. we have a singularity of type I_n or type III, then the j-invariant is ∞.
- The only other possibility is $3\nu(f) = \nu(\Delta)$, e.g. type I_0^*. In that case the j-map can be extended, and the j-invariant is a nonzero element of k.

Miranda's algorithm essentially proceeds by blowing up the base until only a few types of collisions appear.

- First, we blow up the discriminant locus until it is a simple normal crossing divisor. The local ring at each codimension 1 component is then a DVR, so the fibers over each codimension 1 component are of Kodaiara type.

- Next, we blow up collisions with different j-invariants. Note that this is the same as resolving indeterminacy of the j-map.

  This gets rids of collisions of type $II + III$, e.g.

- Next, suppose we have a collision of type $II{+}II^*, III{+}III^*, IV{+}IV^*, I_0^*{+}I_0^*$. If we blow it up, we obtain a new fibration which is not minimal over the new exceptional divisor. Passing to a minimal fibration over this new base gives us a new 3-fold with those collisions missing.

- We continue blowing up collisions until we are left with only the following:

  - $(j = 0)$ $II + I_0^*$, $II + IV^*$, $IV + I_0^*$.
  - $(j \in k^\times)$: $III + I_0^*$.
  - $(j = \infty)$: $I_{2m_1} + I_{2m_2}, I_{2m_1} + I_{2m_2+1}, I_{m_1} + I_{m_2}^*$.

- Finally, we use Tate's algorithm to resolve singularities over the Γ_i. The singular points over the collisions will automatically be resolved as long as we only have collisions from the list above.

  The fiber type over each collision point is determined by the fiber type of the curves colliding at that point; a description of the fiber types can be found in [47].

To obtain a CY fibration, we need $\mathcal{L}_{X/B} \cong \omega_B^{-1}$ to have global sections. However, if we start with a Fano base and blow up too much, we may end up with a variety whose canonical bundle has positive degree. Fortunately, the work of Grassi [29] addresses this problem.

7.2 Ogg-Shafarevich Theory

Next, we summarize results from [20].

Suppose we have a genus one fibration $Y \to B$ satisfying the following (equivalent) conditions:

- The fiber over each $b \in B$ has a component with multiplicity one.
- For each $b \in B$, there is an open neighborhood U_b such that the fibration $Y_{U_b} \to U_b$ has a section.

Let $X \to B$ be the Jacobian fibration, and E/K the fiber over the generic point of B. We write $Ш(X/B)$ to denote the Tate-Shafarevich group of $X \to B$.[1]

Then:

- We can find a Miranda model for $Y \to B$.
- Once we have the Miranda model, we can reduce the computation of $Ш(E)$ to the computation of $Br(Y)$ and some extra cohomology groups which are, in principle, easier to understand.

To explain how to use this machinery, we fix the following notation:

- $B$is a smooth irreducible complex surface.
- We write η to denote the generic point of B and $i : \eta \to B$ for the inclusion morphism.
- We write K to denote the function field of B.

[1]The Tate-Shafarevich group of an elliptic fibration is the intersection of the kernels of the localization maps $WC(E/K) \to WC(E_\nu/K_\nu)$, where we localize at..

- $\pi : X \to B$ is a genus one fibration[2] with local sections. We denote the fiber over η as C/K.

- We write E/K for the Jacobian of C/K.

Now, C is a torsor of E, so C gives rise to a class in $WC(E/K)$. We write δ' for the index of $[C]$ in $WC(E/K)$. Since we are assuming C has local sections, C actually gives rise to a class in $Ш_B(E)$.

7.2.1 Galois to Étale

The first step is to pass from Galois cohomology to étale cohomology.

- If B is an irreducible variety, then étale cohomology η coincides with Galois cohomology of the generic point. In particular, this means:

$$WC(E/K) \cong H^1_{et}(\eta, E)$$

  On the right hand side of the equation, we are treating E as an étale sheaf that assigns to $B \to \eta$ the abelian group of B-valued points on E.

- The Leray spectral sequence, applied to the inclusion $i : \eta \to B$, gives us the following exact sequence:

$$0 \to H^1(B, i_*E) \to H^1(\eta, E) \to H^0(B, R^1 i_* E) \to \cdots$$

  Note that the middle term, $H^1(\eta, E)$, is $WC(E)$ by the previous comment.

- Next, we use the following theorem:

[2]The map is required to be flat and proper, as in our definition of genus one fibration.

Let $f : X \to S$ be a quasicompact and quasi separated morphism, and let $\mathcal{F}$ be a sheaf of abelian groups on the etale site of X and let $s \in S$ be a closed point. Then:

$$(R^q f_* \mathcal{F})_s \cong H^q(X \times \mathcal{O}_s, p^{-1}\mathcal{F})$$

In particular, taking $q = 1$ and f the inclusion $\eta \to B$, we get:

$$(R^1 i_* A)_b \cong H^1(B \times \eta_b, p^{-1}A) = H^1(\eta_b, E_b) = WC(E_b)$$

Thus, we may identify $\prod_{b \in B} WC(E_b)$ with $\prod_{b \in B}(R^1 i_* E)_b$.

- Now, we know that every the group of global sections of a sheaf injects into the product of its stalks; thus the map $H^0(B, R^1 i_* E) \to \prod (R^1 i_* E)_b \cong \prod WC(E_b)$ is an injection. The kernel of the composition:

$$H^1(\eta, E) \to H^0(B, R^1 i_* E) \to \prod_{b \in B} WC(A_b)$$

coincides with the kernel of $H^1(\eta, E) \to H^0(B, R^1 i_* E)$. This allows us to identify $Ш_B(E)$ with the étale cohomology group $H^1(B, i_* E)$.

7.2.2 Cohomology of $\mathbb{G}_m$

We now focus our attention on the group $Ш_B(E) = H^1(B, i_* E)$. As mentioned earlier, we are going to reduce the computation of this group to the computation of $Br(X)$ and some "error terms".

In order to relate these groups, we use the fact that both can be constructed from $\mathbb{G}_{m,X}$:

- By definition, $Br(X) = H^2_{et}(X, \mathbb{G}_{m,X})$.

- We can think of the Jacobian of X as a the kernel of the degree map from the relative Picard group to $\mathbb{Z}$.

Let $P_{X/B} = R^1\pi_*\mathbb{G}_m, X$. There is a morphism $P_{X/B} \to i_*i^*P_{X/B}$. We denote the kernel of that morphism by $\mathcal{E}$.

Note that if $X \to B$ is a Miranda model, then the morphism above is surjective, so we have a short exact sequence:

$$0 \to \mathcal{E} \to P_{X/B} \to i_*i^*P_{X/B} \to 0$$

Furthermore, the support of $\mathcal{E}$ is contained in the subvariety of B consisting of points $b \in B$ whose fiber $\pi^{-1}(X)$ has multiple components.

7.2.3 Master Diagram

The algorithm for computing Ш boils down to studying the following diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(B) & \longrightarrow & \mathrm{Br}(X) & \longrightarrow & H^1(B, P_{X/B}) & \longrightarrow & H^3(B, \mathbb{G}_m) \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}/\delta\mathbb{Z} & \longrightarrow & Ш_B(E) & \longrightarrow & H^1(B, i_*i^*P_{X/B}) & \longrightarrow & 0 \\
 & & & & & & \downarrow & & \\
 & & & & 0 & \longrightarrow & H^2(B, \mathcal{E}) & \longrightarrow & \bigoplus_{t \in B^{(1)}} H^2(B, i_{t*}i_t^*\mathcal{E})
\end{array}$$

When the geometry of the fibration is simple enough, then the computation of Ш boils down to computing the cokernel of $Br(B) \to Br(X)$:

- If B is a smooth surface, then $H^3(B, \mathbb{G}_m) = 0$.
- If B is smooth and rational, then $Br(B) = 0$.
- If X is smooth and the fibers of $X \to B$ are irreducible, then $H^2(B, \mathcal{E}) = 0$.

7.2.4 Example

We review Example 1.18 in [20] to explain how this machinery is useful in practice.

Let $f_1, f_2, f_3 \in \mathbb{C}[x_0, x_1, x_2]$ be homogenous cubics of degree 3, let V be the $\mathbb{C}$-vector space spanned by f_1, f_2, f_3, let $S = \mathbb{P}V$ and define:

$$X = \left\{([x_0 : x_1 : x_2], [t_1 : t_2 : t_3]) \in \mathbb{P}^2 \times S : (t_1 f_1 + t_2 f_2 + t_3 f_3)(x_0, x_1, x_2) = 0\right\}$$

- X is birational to $\mathbb{P}^3$. Thus $Br(X) = 0$.
- The projection onto S endows X with the structure of a genus one fibration.
- The groups $Br(S)$ and $H^3(S, \mathbb{G}_m)$ vanish because S is a smooth rational surface. Note that this traps $H^1(S, P_{X/S})$ between two zeros in the master diagram, so $H^1(S, P_{X/S}) = 0$.
- For generic f_1, f_2, f_3, the fibration does not have a global section but has local sections. In other words, X represents a class in $Ш_S(J)$, where J is the Jacobian elliptic fibration. Furthermore, we have $\delta = 3$ by construction.
- The discriminant is a singular curve in S. The fibers over smooth points on the discriminant locus are of type I_1. In particular, the fibers are irreducible, so $H^2(S, \mathcal{E}) = 0$, since $\mathcal{E}$ has support on the subvariety of the discriminant locus over which the fibers are reducible.
- We can obtain a Miranda model $J' \to S'$ by blowing up the singularities of the discriminant locus. Furthermore, since the fibers are irreducible in codimension 1, we have a short exact sequence:

$$0 \to Br(S') \to Br(J') \to Ш_{S'}(E) \to 0$$

Note that $Br(S') = 0$ because S' is a smooth rational surface, so we have an isomorphism $Br(J') \cong Ш_{S'}(E)$.

Putting it all together, we see that $Br(J') \cong Ш_{S'}(E) \cong \mathbb{Z}/3\mathbb{Z}$.

Thus, while $X \to S$ and $J' \to S'$ become birational after base changing so that $X \to S$ has a section, they have different Brauer groups. This is especially interesting because $Br(J') \neq 0$ implies J' is not a rational threefold, but becomes rational after a base change. This means that for sufficiently generic f_1, f_2, f_3, the Jacobian of the rational genus one 3-fold is unirational, but not rational.

7.3 Calabi-Yau Fibrations

In [32], Gross does the following:

- He shows that elliptically fibered Calabi-Yau 3-folds form a "bounded family". Concretely, this means there are only finitely many bases that can appear in a Calabi-Yau 3-fold, and for each base, there is a variety of finite type classifying those Calabi-Yau fibrations.

- Furthermore, he shows that one can use Ogg-Shafarevich theory to study families of Calabi-Yau 3-folds. He shows that $Ш_S(E)$ is finite if E is the generic fiber of an elliptically fibered Calabi-Yau 3-fold.

- Finally, he combines these ideas to show that genus one fibered Calabi-Yau 3-folds form a bounded family.

Some of these results have been generalized to elliptically fibered Calabi-Yau d-folds with $d = 4, 5$.

One detail we will need in the later sections is the following: if $X \to B$ is a Calabi-Yau 3-fold which is not isotrivial, then B is either $\mathbb{P}^2, \mathbb{F}_n$ for $n = 0, \ldots, 12$ or a blow up of one of those surfaces.

Ogg-Shafarevich theory is best suited for studying questions of a "global" nature. We can use it to prove existence of torsors without multiple fibers, and we can use it to prove finiteness theorems for those torsors. However, it does not let us see as much of the geometry as we would like.

The reliance on Miranda models makes it difficult to use in settings which are important to F-theory. For example, we may want to study fibrations with mild singularities which can't be resolved further without changing the canonical bundle. Furthermore, we may want to study fibrations with a singular discriminant locus as in [39]. In this case, the local rings are not DVRs, so we can have codimension 1 degenerations which are not of Kodaira type.

Chapter 8

F-Theory

F-theory is a branch of string theory where elliptic fibrations play a key role. We quote [63]:

The F-theory paradigm consists in using [a] one-to-one correspondence between supergravity backgrounds with 7-branes and Calabi-Yau elliptic fibrations in order to study the first using insights on the latter.

It is worth noting that this correspondence sometimes leads to new, string theory-inspired theorems in algebraic geometry. See [30, 30] and [44] for examples.

For more on F-theory in general, one can look in [51, 52], [63] and other places.

One of the virtues of F-theory is that it allows us to determine "properties of the physical theory" by simply computing classical invariants of the associated elliptic fibrations. For example, on the physics side of things, an important invariant is the *gauge group*.

- The gauge group is a semisimple Lie group G, with a decomposition as $G \cong U(1)^r \times G_{na}$, where G_{na} is a nonabelian Lie group.
- Let $\tilde{G_{na}} \to G_{na}$ be the universal cover. Then $\tilde{G_{na}}$ is determined by the

codimension 1 degenerations of X. Precisely, each irreducible factor of the discriminant determines a DVR and the singular fiber over that factor is one of the fibers in Kodaira's list. These fibers are analytically isomorphic to duVal singularities, so we can associate a Dynkin diagram to each factor of the discriminant locus. This Dynkin diagram has an associated Lie algebra, which has an associated simply connected Lie group.

The group $\tilde{G_{na}}$ is the product of these simply connected Lie groups.

- The integer r, and the fundamental group $\pi_1(G)$, are determined by $MW(X/B)$.

  Precisely, the dictionary says $\pi_1(G) = MW(X/B)$, so r is the rank of $MW(X/B)$ and $\pi_1(G_{na}) = MW(X/B)_{tors}$.

The goal of this dissertation is to develop new tools, and refine existing tools, for studying genus one fibered Calabi-Yau 3-folds without section whose Jacobian is also Calabi-Yau, with the goal of answering questions from F-theory. The existence of such fibrations leads to "discrete torsion" in the gauge group.

8.1 Discrete Torsion and Torsors

Let $Y \to B$ be a fibration without a section, and let $X \to B$ be the Jacobian fibration. If we use X, Y to do F-theory, there is no difference between the associated physical theories. However, if we do M-theory, then we can see that one of the fibrations has a section and the other doesn't.

The interpretation for this is that the gauge group G has multiple connected components, one for each (birational class) of fibration $Y \to B$ whose Jacobian is $X \to B$.

An important tool for studying this problem is the Tate-Shafarevich group. In [32], it is shown (Prop 2.2) that the Jacobian of an genus one fibered Calabi-Yau threefold without multiple fibers is also Calabi-Yau.

Thus, whenever $Ш_B(X)$ is nontrivial, we have a gauge group G with multiple connected components. Furthermore, $Ш_B(X)$ can be computed using Ogg-Shafarevich Theory (7.2), so that part of $\pi_0(G)$ is reasonably well-understood.

However:

- There is a well-known construction for torsors in F-theory which produces CY fibrations without section that fail many of the hypotheses in [32]. Thus, Ш is not quite the whole story.

- Ogg-Shafarevich theory works best if we have smooth models. However, in F-theory, we may want to work with models that have mild singularities over a codimension 2 or higher locus. Furthermore, we would like to understand why nontriviality of Ш seems to force the Jacobian to have singularities even if the torsor admits a smooth model. It's not clear how to extract this type of information from Ш.

8.1.1 Goals of this dissertation

The goal of this dissertation is to develop tools for studying genus one fibrations without section in F-theory.

- How do we extend the analysis of 8.2 to higher degree torsors? For example, can we make meaningful predictions about codimension 2 singularities on the Jacobian of a fibration of high index?

- Can we find an explicit (sharp) bound on the index of a genus one fibered Calabi-Yau 3-fold? Even if we restrict attention to fibrations with local sections, where such a bound is in principle computable, there are no known examples of Calabi-Yau fibrations of index exceeding 6.

- How do we classify Calabi-Yau fibrations that do not fit the criteria in [20]? Furthermore, how can we ensure that their Jacobians are also Calabi-Yau?

In the remaining sections in this chapter, we give a brief summary of some relevant results from recent F-theory papers. The goal is mainly to give the reader a sense of what types of details are important in F-theory.

8.2 2-torsors in F-theory

Genus one fibrations with a bisection[1] have been analyzed in depth in the F-theory literature, see e.g. [13], [50]. In this section we summarize some of the important results about 2-torsors, so as to give a sense of what the desired toolkit should be able to accomplish.

Say we have a 3-fold $Y \to \mathbb{P}^2$ without section, and Jacobian $X \to \mathbb{P}^2$. Assume that Y has a section after passing to a double cover of $\mathbb{P}^2$.

Then Y can be described by an equation:

$$w^2 = a_0u^4 + a_1u^3v + a_2u^2v^2 + a_3uv^3 + a_4v^4$$

where a_i are sections of a line bundle on $\mathbb{P}^2$. In order for Y to be Calabi-Yau, we need a_i to be a global section of $\mathcal{O}(6d - 2i\ell)$ for some integer ℓ. If the fibration doesn't have a section, then $(\deg(a_i))$ is necessarily[2] one of $(2, 4, 6, 8, 10), (4, 5, 6, 7, 8)$

[1] This is the geometric name for a 2-torsor, which we will discuss later.
[2] Reversing the roles of u, v if necessary.

or $(6, 6, 6, 6, 6)$.

Furthermore:

- Generically, the discriminant of $Y \to \mathbb{P}^2$ is an irreducible curve with 108 nodes.

- We can resolve singularities on Y, but we can't resolve the singular points over the nodes on X. Thus, we have a situation where Y is smooth and X has 108 singular points that can't be resolved crepantly.

- If we tune a_0 or a_4 so that it becomes a square, then $Y \to B$ will now be a model for an elliptic fibration with nontrivial MW group.

  In this case, X, Y are birational. Furthermore, X still has codimension 2 singularities over the nodes of the discriminant. However, these singularities can now be resolved simultaneously.

In F-theory, it is not enough to know that a singularity exists somewhere. It is important to know exactly what type of singularities appear, how often they appear and where they appear. However, we can't quite extract this type of information from Ogg-Shafarevich theory - e.g. to be the best of my knowledge, I don't know how one would deduce that X has at least 108 I_2 singularities that can't be resolved using only the assumption that $Ш_B(X)$ has nontrivial 2-torsion.

The key tool used to obtain these results is the Jacobian formula. In the later chapters, we study the Jacobian formula for genus one fibered Calabi-Yau 3-folds which acquire a section after passing to a cover of low degree. Although the Jacobian formula very quickly becomes too complicated to be of use, we hope that the trace zero variety 12.2.1 can be used as a substitute for the purposes of analyzing these singularities on Jacobians of high index torsors.

8.3 Quotient Torsors

Next, we discuss "quotient torsors". The construction first appears in [21], and has since been used in several F-theory papers, e.g. [3, 4, 2].

To get started, we need the following data:

- An elliptically fibered Calabi-Yau 3-fold $Y \to B$, given by a Weierstrass equation:

  $$y^2 = x^3 + fx + g$$

  We write $\sigma_0 : B \to Y$ for the zero section of the fibration.

- An automorphism $\alpha \in Aut(B)$ satisfying:

  - $\alpha^n = \alpha \circ \cdots \circ \alpha = \mathbb{1}_B$, i.e. α has finite order n as an element of $Aut(B)$.
  - $\alpha^*(f) = f$ and $\alpha^*(g) = g$.
  - $\sigma_0 \circ \alpha = \sigma_0$ - that is, α "fixes the zero section".

  With this data, we can define an action of $\langle\alpha\rangle$ on the Mordell-Weil group of the fibration.

- Finally, we need an element $P_0 \in MW(X/B)$ which "has trace 0 with respect to α". Precisely, this means we want a (nonidentity) section $B \to X$ satisfying one of the following conditions:

  - P_0 is fixed by α, and $nP_0 = P_0 + \cdots + P_0 = 0$.
  - P_0 is not fixed by α, and $\sum \alpha^i(P) = 0$.

With this data, we define an action of $\langle\alpha\rangle$ on X by combining the action of α on B with the translation-by-P_0 map on the fibers.

We define a new fibration $X/\langle\alpha\rangle \to B/\langle\alpha\rangle$.

- If X is smooth, then the new fibration is smooth.
- If X is Calabi-Yau, then the new fibration is Calabi-Yau.

However, if α has fixed points, then the new base is singular and the new fibration has multiple fibers over the singularities.

Thus, this construction gives a whole new class of torsors that are wildly different from those classified in [32]. For more on these torsors in F-theory, see [2, 12, 4].

8.3.1 Schoen Manifolds

Let $S_1, S_2 \to \mathbb{P}^1$ be a pair of rational elliptic surfaces.

Let $X = S_1 \times_{\mathbb{P}^1} S_2$ be the fiber product.

- X is Calabi-Yau.
- If the discriminant loci of the two fibrations are disjoint, then X is smooth.
- X can be endowed with the structure of an elliptic fibration in two different ways using the projections $X \to S_1$ and $X \to S_2$.

If X is birational to a fiber product of rational elliptic surfaces, we say that X is a Schoen manifold.

Schoen manifolds have more structure than a general elliptic CY 3-fold, so they tend to be easier to study. The quotient construction has been completely analyzed for Schoen manifolds in [12].

8.4 Minimal Singularities and Torsion

In [35], we proved a bound for the size of the Mordell-Weil torsion group of an elliptically fibered Calabi-Yau d-fold for $d \leq 4$. We present the proof in full detail in 9. The goal of this section is to highlight some of the additional geometric information we obtained in that paper that turned out to be important in F-theory.

- Our argument shows that there *are* Weierstrass fibrations with trivial canonical bundle and with points of order as high as 10. However, as soon as we have a point of order exceeding 6, the threefold has singularities over a codimension 2 locus of the base that can't be resolved crepantly.

- Furthermore, we show that the presence of a torsion section of order at least 4 severely constrains the possible degenerations in codimension 1 on the fibration.

  If we have a torsion section of order at least 5, the fibration is necessarily semistable.[3] However, we can say more: for example, every fibration with a 5-torsion section as *at least* 2 I_1 fibers and 2 I_5 fibers. If we have a torsion section of order at least 6, we must have at least an I_1, I_2, I_3 and I_6 fiber.

- The minimal configuration of singularities is determined by the cusps on the corresponding modular curve. In particular, once we've constructed the modular curve for a particular torsion group (either algebraically or analytically), we can immediately determine the minimal configuration of singularities on any 3-fold with that torsion group.

[3] This is actually a well-known property of elliptic surfaces.

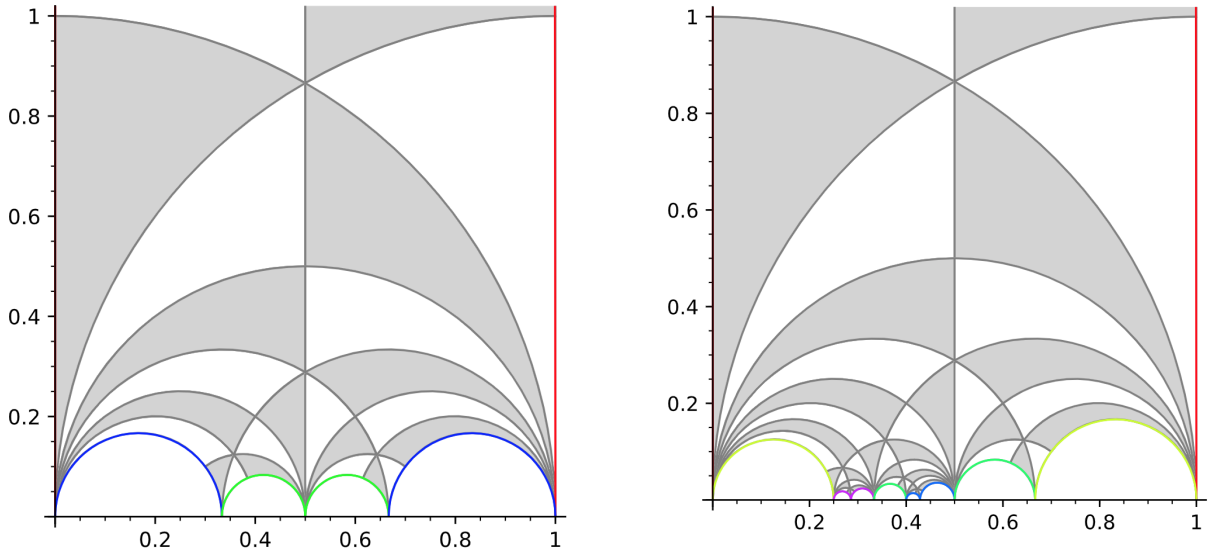


Figure 8.1: *Triangulation of* $X_1(6)$ *and* $X_1(7)$*. Sides with equal colors are to be identified.*

8.4.1 Unexpected lessons for the torsor problem

Finally, we note that the minimal configuration of singularities can be read off of pictures like 8.1, which encodes information about the natural covering map $X_1(n) \to X(1)$.

The moduli space of elliptic curves over $\mathbb{C}$ has a natural triangulation.[4] We pull back the triangulation on $X(1)$ to obtain a triangulation on $X_1(n)$. Furthermore, the picture show us to construct $X_1(n)$ by gluing together multiple copies of $X(1)$. Finally, note that the picture represents a fundamental domain in $\mathcal{H}^*$ for the action of $\Gamma_1(n)$.

Here's the point: the configuration of singularities forced on an elliptic fibration with a torsion section of order n can be read off the picture directly. When $n \geq 5$, the fibers are all of type I_m. The number of I_m fibers in the universal surface is equal to the number of cusps on $X_1(n)$. The widths of the cusps coincide with the

[4]Note that the edges in the triangulation coincide with the subset of the moduli space that represents real elliptic curves.

minimal values of m in the I_m fibers. [5]

Now, the cusps are the points in 8.1 with imaginary part equal to 0. The width of each cusp can be computed by counting the number of triangles that meet at that cusp, and dividing the result by 2. This is one reason there we have made a concerted effort to include reasonably faithful illustrations wherever possible.

Furtbermore, the numbers predicted by these pictures coincide with the singularities we computed on the compactification of the universal elliptic curve over the normalization of the modular curve over $\mathbb{Z}[\frac{1}{6}]$. Thus, we can work "at the level of the generic fiber" and still constrain the geometry of elliptic fibrations in a meaningful way if we can replicate this set-up.

[5] See [35] for a precise statement.

Part III

Torsors

Chapter 9

Special Fibrations

Many of these ideas, and their applications to F-theory, are discussed in [35].

Let $X \to B$ be an elliptic fibration over a positive dimensional base. We say that X is **special** if there is a commutative square:

$$\begin{array}{ccc} X & \overset{\Phi}{\dashrightarrow} & S \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle p} \\ B & \overset{\phi}{\dashrightarrow} & C \end{array} \tag{9.1}$$

where:

- $S \to C$ is an elliptic surface over an irreducible curve.
- The horizontal maps are nonconstant rational maps.
- The vertical maps are proper.
- ϕ is flat.

The usefulness of this definition is summarized in the following proposition:

Proposition 9.1. *Let $\pi : X \to B$ be an elliptically fibered Calabi-Yau 3-fold. Assume that:*

- *X is special.*
- *$\pi : X \to B$ is not isotrivial.*
- *X does not have inadmissible singularities.*

Then X is birational to a fiber product of rational elliptic surfaces.

Before we can prove the proposition, we will need some lemmas.

9.1 Global Lemmas

A variety B is **rationally connected** if two general points b_1, b_2 can be joined by a rational curve, i.e. there exists a regular morphism $\mathbb{P}^1 \to B$ taking $[0:1]$ to b_1 and $[1:0]$ to b_2.

Lemma 9.2. *Let B be a rationally connected variety, C an irreducible, separated curve, and $\phi : B \to C$ a non-constant rational map. Then C has genus 0 and ϕ is flat.*

Proof. Since ϕ is non-constant, we can find points $b_1, b_2 \in B$ such that $\phi(b_1) \neq \phi(b_2)$. Since B is rationally connected, there is a regular map $\mathbb{P}^1 \to B$ taking 0 to b_1 and ∞ to b_2. The composition $\mathbb{P}^1 \to C$ is a non-constant rational map, so by [36][1], C has genus 0.

To prove flatness of ϕ, it suffices to prove that the map is flat over each point in $\mathbb{P}^1$. Any proper open neighborhood of $\mathbb{P}^1$ has the form SpecR_0 for R_0 a principal ideal domain (PID), so we can determine whether the map is flat by studying the morphism of algebras $R_0 \to K(B)$. Since R_0 is a PID, flatness is equivalent to

[1]The assertion is proven in IV.2.5.4 and IV.2.5.5

$K(B)$ being torsion-free, which follows immediately from the fact that the map $B \to \mathbb{P}^1$ is non-constant and $K(B)$ is purely transcendental.

□

As in Section 2, we write $\mathcal{L}_{Y/B} = (R^1\pi_*\mathcal{O}_Y)^{-1}$ for the fundamental line bundle of the elliptic fibration $\pi : Y \to B$ and ω_Y (resp. ω_B) to denote the canonical bundle of Y (resp. B). A variety B is **Fano** if ω_B^{-1} is ample. Note that every Fano variety is rationally connected by Theorem 0.1 of [41].

Lemma 9.3. *Let $\pi : Y \to B$ a special elliptic fibration. Then $\mathcal{L}_{Y/B} \cong \phi^*\mathcal{L}_{S/C}$.*

Proof. The conditions in the definition of a special elliptic fibration allow us to use Prop. III.9.3 in [36] to compute:

$$\mathcal{L}_{Y/B} = (R^1\pi_*\mathcal{O}_Y)^{-1} = (R^1\pi_*\Phi^*\mathcal{O}_S)^{-1} = \phi^*(R^1p_*\mathcal{O}_S)^{-1} = \phi^*\mathcal{L}_{S/C}\,. \tag{9.2}$$

□

Lemma 9.4. *Let B be a rationally connected variety, $\pi : Y \to B$ be a special fibration and let d be the degree of $\mathcal{L}_{S/\mathbb{P}^1}$.*

Then $\omega_Y \cong \pi^*(\omega_B \otimes \phi^*(\mathcal{O}_{\mathbb{P}^1}(1))^{\otimes d})$.

Proof. This follows from the canonical bundle formula for elliptic fibrations, together with the computation from the previous lemma.

□

Proposition 9.5. *Let $\pi : Y \to B$ be a special elliptic fibration, with ω_Y trivial and B Fano. If ϕ is a morphism, then* $\dim B = 1$.

Proof. First, since B is Fano, B is rationally connected so $C \cong \mathbb{P}^1$. Next, since π has section, $\pi^* : Pic(B) \to Pic(Y)$ is injective, so triviality of ω_Y forces $\phi^*(\mathcal{O}_{\mathbb{P}^1}(1))^{\otimes d} \cong \omega_B^{-1}$. Since B is Fano, ω_B^{-1} is ample so $\phi^*(\mathcal{O}_{\mathbb{P}^1}(1))$ is ample.

Finally, suppose ϕ is a morphism. Then $\phi^*(\mathcal{O}(1))$ is generated by global sections. By Corollary 1.2.15 in [43], $\phi^*(\mathcal{O}(1))$ is ample if and only if ϕ is finite. Thus, if ϕ is a morphism, $\dim B = 1$.

□

In applications, we will be using in the contrapositive of the last proposition, i.e. if $\dim B \geq 2$ then ϕ is not a morphism.

Definition 9.6. *Let $\phi = \frac{p}{q} \in K$, with $p, q \in R$ relatively prime. We can think of ϕ as a map* Spec$R \to \mathbb{P}^1$. *The* **locus of indeterminacy** *of ϕ is $V(p) \cap V(q) \subset$* Spec$R$.

Definition 9.7. *Let ϕ be as above, and assume the locus of indeterminacy of ϕ contains a closed point b. Let $\mathfrak{m}_b \subset R$ be the corresponding ideal. We define $\boldsymbol{m_\phi(b)}$ to be the order of vanishing of the ideal (p, q) at $\mathfrak{m}_b$.*

Note that $m_\phi(b)$ makes sense whenever we have a rational map $B \to \mathbb{P}^1$ from a normal scheme B, since the property is local on B. Furthermore, the definition $m_\phi(b)$ makes sense for any irreducible component of the indeterminacy locus, and not just for closed points. To ease the exposition, we will refer to irreducible components of the indeterminacy locus as points, although the arguments do not require this.

Proposition 9.8. *Let $\phi : B \to \mathbb{P}^1$ be a non-constant rational map and f a global section of $\mathcal{O}_{\mathbb{P}^1}(d)$ for some $d > 0$. If $b \in B$ is in the indeterminacy locus of ϕ, then $\phi^*(f)$ vanishes to order $m_\phi(b)d$ at b.*

Proof. The claim is local on B, so we assume B is affine, say $B = \mathrm{Spec}R$. Choosing coordinates $[x_0 : x_1]$ on $\mathbb{P}^1$, we can express $f(x_0, x_1)$ as a homogeneous polynomial of degree d in x_0, x_1. Furthermore, we can write the map $\phi : B \to \mathbb{P}^1$ as $b \mapsto [p(b) : q(b)]$, where $p, q \in R$ have no common factors. In this notation, we have $\phi^*(f)(b) = f(p(b), q(b))$.

Since f is a homogenous polynomial of degree d, $f \in (x_0, x_1)^d \subset k[x_0, x_1]$. If $b \in B$ is in the locus of indeterminacy of ϕ, then $\mathfrak{m}_b^{m_\phi(b)} \supset (p(b), q(b)) = \phi^\#((x_0, x_1))$ so:

$$\phi^* f \in (p(b), q(b))^d \subset \mathfrak{m}_b^{m_\phi(b)d}$$

□

We now easily deduce the following:

Corollary 9.9. *Let $\pi : Y \to B$ be a special fibration, let d be the degree of the fundamental line bundle of $\mathcal{L}_{S/\mathbb{P}^1}$, and let $b \in B$ be a point in the indeterminacy locus of ϕ. Then the Weierstrass coefficients f, g of Y vanish to order $(4n, 6n)$, where $n = d\, m_\phi(b)$.*

Proof. Commutativity of the square (9.1) tells us $f_B = \phi^*(f^1_{\mathbb{P}})$ and $g_B = \phi^*(g^1_{\mathbb{P}})$. The Weierstrass coefficients of the elliptic surface are homogenous polynomials of degree $4d, 6d$ respectively, proving the claim. □

Corollary 9.10. *Let $\pi : Y \to B$ be a special elliptic fibration and suppose the order of vanishing of (f, g) does not exceed $(4, 6)$ over any point $b \in B$. Then either ϕ is a morphism, or S is rational and the locus of poles and the locus of zeros of ϕ intersect transversely.*

Proof. Assume ϕ is not a morphism. Recall that an elliptic surface is rational if and only if the fundamental line bundle has degree 1. If the fundamental line

bundle has degree $d > 1$, then the order of vanishing over all points in the locus of indeterminacy is at least $(4d, 6d)$. The condition on (f, g) forces $d = 1$, hence rationality of S. If the locus of poles meets the locus of zeros non-transversely at some point b, then $m_\phi(b) > 1$ so (f, g) vanish to order at least $(8, 12)$ over b.

□

9.2 Proof of Proposition

The proposition now follows easily from everything we've done:

Proof.

- By 9.10, the assumptions on $X \to B$ guarantee that $S \to C$ is a rational elliptic surface.
- We can resolve indeterminacy in the map $B \to C$ by blowing up the 9 base points of ϕ. By results in [58] or [25], e.g., $\tilde{B} \to C$ is a rational elliptic surface.
- Since X has maps to $\tilde{B}$ and S, there is a unique morphism of C-schemes to the fiber product $X \to \tilde{B} \times_C S$.
- Since X does not have inadmissible singualrities, it is minimal, so the map $X \to \tilde{B} \times_C S$ is an isomorphism.

□

9.2.1 Comments

- When B is a surface, we can use the birational classification of algebraic surfaces to make stronger statements and simplify some of the assumptions.

Simply requiring the fibration to not be isotrivial forces the base to be rational. After contracting all exceptional curves in the base, we may assume that $B \cong \mathbb{P}^2$ or $\mathbb{F}_n$. A computations show that ϕ has 8 or 9 points of indeterminacy, with 9 occurring if and only if $B \cong \mathbb{P}^2$. If we assume that $B = \mathbb{P}^2$ e.g., it is easy to see that resolving indeterminacy of ϕ means blowing up $\mathbb{P}^2$ at the 9 points in the base locus of a pair of cubics, so the new map $\tilde{\phi} : \tilde{B} \to \mathbb{P}^1$ is itself an elliptic fibration. Commutativity of (**??**) gives us a natural map $\tilde{Y} \to \tilde{B} \times_{\mathbb{P}^1} S$. Minimality of the fibration $\tilde{Y} \to \tilde{B}$ then forces that map to be an isomorphism, showing that any special $Y \to B$ is birational to a Schoen manifold.

- Requiring the base to be Fano, and more generally requiring $Y \to B$ to be birational to a fibration over a Fano base, is a mild but necessary requirement for this type of theorem. Even in dimension 2, one has to exclude fibrations of the form $E_1 \times E_2 \to E_2$, where E_1, E_2 are elliptic curves, when giving a bound on Mordell-Weil torsion of K3 surfaces. In dimension three, this condition rules out fibrations over Enriques surfaces, which are also isotrivial and thus can have an non-finitely generated Mordell-Weil group. It also rules fibrations of the form $S \times E \to \mathbb{P}^1 \times E$, where $S \to \mathbb{P}^1$ is a K3 surface. However, our conclusion fails in all of these cases, showing the condition is necessary in dimensions.2 and 3.

- By Theorem 1.8 in [17] every smooth[2] elliptically fibered Calabi-Yau n-fold $Y \to B$ is birationally equivalent to a (possibly singular) fibration over a Fano base, as long as the original base is not of product type. Roughly speaking[3], B is *of product type* if B is birational to a quotient of a product. This

[2]This condition can be relaxed; see [17] for details.
[3]See [17] for the precise definition.

condition is necessary to rule out higher dimensional analogues of isotrivial fibrations in the statement of the boundedness theorem in [17]. However, our theorem also fails for fibrations over a base of product type, and in fact it is easy to construct counterexamples to our theorem in any dimension by taking the product of a K3 with Mordell-Weil group $\mathbb{Z}_8$ with a product of elliptic curves.

- The condition on the order of vanishing of (f, g) is precisely the condition needed to guarantee that the Weierstrass model admits a proper, flat crepant resolution, see e.g. [29]. Thus, any smooth fibration $Y \to B$ is birational to one satisfying the conditions of the previous theorem.

9.3 Mordell-Weil Torsion

In this section, we prove the following:

Theorem 9.11. *Let $\pi : Y \to B$ be an elliptic fibration satisfying the hypotheses of the previous theorem. Then $MW(Y/B)_{tors}$ is isomorphic to one of the following groups:*

$$\begin{aligned} \mathbb{Z}_n : &\qquad (n = 1, 2, 3, 4, 5, 6)\,, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2m} : &\qquad (m = 1, 2)\,, \qquad \mathbb{Z}_3 \times \mathbb{Z}_3\,. \end{aligned}$$

Note that this list of groups is exactly the list studied in [8], and they can all be realized as torsion subgroups of Schoen manifolds in dimension 3.

In order to apply the results of the previous section to rule out the existence of fibrations with a particular torsion group T, we need an elliptic surface $S \to C$ with the following property: for any elliptic fibration $Y \to B$ whose Mordell-Weil

group contains a subgroup isomorphic to T, there exists a special diagram:

$$\begin{array}{ccc} Y & \overset{\Phi}{\dashrightarrow} & S \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle p} \\ B & \overset{\phi}{\dashrightarrow} & C\,, \end{array}$$

We call $S \to C$ a **universal elliptic surface** for T.

Proof. If T is cyclic and $|T| \geq 4$, then there is a well-known construction for a universal elliptic surface. We give a construction for $S \to C$ and ϕ in Appendix **??**. For these groups, $C \cong X_1(n)$, where $n = |T|$. A computation shows that C has positive genus if $n = 11$ or $n \geq 13$, and $\mathcal{L}_{S/C} \cong \mathcal{O}(1)$ for $n = 4, 5, 6$ and $\deg \mathcal{L}_{S/C} > 1$ for $n \geq 7$. Thus, we can immediately rule out the existence of a point of order exceeding 6 in $MW(Y/B)$.

If T is not cyclic, then T is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ for some pair of positive integers m, n with $1 \neq m|n$.[4] The previous argument also shows we may assume $n \leq 6$. If $m = n$ and $m \geq 3$[5], then it is also well-known that a surface $S \to C$ with the desired property exists ([37] Cor. 4.7.2.) and that $C \cong X(m)$. A construction for $S \to C$ is described in [60]. For these groups, one computes that $X(m)$ has genus 0 if $m = 3, 4, 5$ and has positive genus otherwise. Thus, we can rule out any group containing $\mathbb{Z}_6 \times \mathbb{Z}_6$. A computation using the formulae in the appendix of [35] shows that $\mathcal{L}_{S/C} \cong \mathcal{O}(1)$ for $m = 3$ and $\deg \mathcal{L}_{S/C} > 1$ for $m = 4, 5$, which allows us to rule out $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$.

Finally, we have to rule out $\mathbb{Z}_2 \times \mathbb{Z}_6$ and $\mathbb{Z}_3 \times \mathbb{Z}_6$.

See [35] for a construction of the surfaces $S \to C$ for $T \cong \mathbb{Z}_2 \times \mathbb{Z}_{2m}$ ($m \geq 2$) and $T \cong \mathbb{Z}_m \times \mathbb{Z}_{2m}$ ($m \geq 3$ and m odd) with the desired universal property. One can

[4] First, note that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{\gcd(m,n)} \times \mathbb{Z}_{\mathrm{lcm}(m,n)}$, so we may assume $m|n$. Furthermore, we may assume $m \neq 1$, since in that case T is cyclic.

[5] We do not need to consider $\mathbb{Z}_2 \times \mathbb{Z}_2$ since the group is in our list of possible subgroups.

compute the degree of the fundamental line bundle directly from the Weierstrass model obtained from construction, to check that $d = 1$ is possible only in the $\mathbb{Z}_2 \times \mathbb{Z}_4$ case.

That will suffice to complete the proof. □

Note that when $\dim B \geq 3$, the locus of indeterminacy of ϕ still has codimension 2, since it is a nonempty intersection of 2 hypersurfaces in B.

9.4 Quotient Torsors

In this section, we show that any fixed elliptically fibered Calabi-Yau threefolds admits only finitely many quotient torsors. This shows that the results of [32] can be extended to include a slightly larger class of Calabi=Yau 3-folds.

A priori, there is no reason to expect such a bound. Let $K = \mathbb{C}(s,t)$ and let E/K be an elliptic curve given by a Weierstrass equation:

$$y^2 = x^3 + f(s,t)x + g(s,t)$$

Suppose $f(s,t) = f_0(st)$ and $g(s,t) = g_0(st)$, where f_0, g_0 are univariate polynomials. Then there are automorphisms of arbitrarily high order that fix f_0, g_0: for any root of unity ζ, we have an action $h(s,t) \to h(\zeta s, \zeta^{-1}t)$. Furthermore, if we choose f, g so that the elliptic curve has a point of order $n > 1$, then we can use this data to construct torsors of index mn for all positive integers m.

- A quotient torsor is basically a "normal" torsor of a descended version of the original fibration - requiring f, g to be invariant under α is the same as saying the fibration is defined over a proper subfield, and the quotient torsor data lets us construct a torsor over the subfield that splits when we base change back to the original field.

- Let $k = \mathbb{C}(f, g)$. Exactly one of the following holds:
  - $k = \mathbb{C}$; this is the same as saying that the fibration is a product $E \times B$.
  - k has transcendence degree 1 over $\mathbb{C}$.
  - K/k is a finite degree extension.

  We can ignore the first case, since isotrivial fibrations are not suitable for F-theory. We can use the results in this chapter to show that every fibration in the second class is special, hence Schoen. Quotient torsors of Schoen manifolds are classified in [12].

That leaves the third case, which is easy to study, since the assumption that K/k is algebraic means that there are at most finitely many automorphisms of K that fix the coefficients f, g.

For any automorphism α which is compatible with the fibration, we can only obtain finitely many inequivalent quotient torsors: the Mordell-Weil group is finitely generated, and if we have two points in $P_1, P_2 \in \ker(T_\alpha)$ with $P_1 - P_2 \in nE(K)$, where n is the order of α, then the associated cocycles differ by a coboundary, so the associated quotient torsors will be isomorphic as curves over K_α. Since $E(K)/nE(K)$ is finite and $Aut(K/k(E))$ are both finite, it follows that any fixed Calabi-Yau 3-fold admits at most finitely many inequivalent quotient torsors.

9.4.1 Comparison to other dimensions

The previous result shows that there are only finitely many families of genus one fibered Calabi-Yau 3-folds, even if we include quotient torsors. This shows that Gross' finiteness result can be extended "by ε."

It is interesting to note that Ш is always infinite for elliptic K3 surfaces, and the set of quotient torsors is always infinite for genus one Calabi-Yau's of dimension at least 4, but both are finite exactly when the total space is a Calabi-Yau 3-fold.

9.5 Applications to the torsor problem

- If we can construct a universal object classifying torsors, then we might be able to use it to analyze singularities forced on the Jacobians the way we used cusps on minimal singularities in

- If we can prove theorems of the form:

$$(\exists X)(WC(E/K) \neq 0) \Longrightarrow (\exists Y)(MW(Y/B)_{tors}) \neq 0$$

  then we can use the bound on Mordell-Weil torsion on CY 3-folds to obtain bounds on the order of WC.

- The quotient torsor story gives us an example where we have 3 distinct CY 3-folds - the original fibration X/B, the quotient torsor $Y/(B/G)$ and the Jacobian of the quotient torsor.

  This suggests a possible criterion for determining when a class in WC admits a CY model: it might be sufficient (maybe necessary too) that the base extension E_L admit a CY model.

  Now, base extension changes the degree of the fundamental line bundle, so that would mean we can only have torsors if the Jacobian has singularities in codimension 1 that become non-minimal singularities after base change.

In Part II, we will study torsors of index 2 and 3 in depth, and show that we

can construct something like a modular curve that encodes much of the theory. We then show how to generalize that construction to classify torsors that split over an arbitrary (finite) Galois extension L/K.

Chapter 10

Index 2 Torsors

Let E/k be an elliptic curve. We will refer to torsors of E of index 2 as 2-torsors. If C/k is a genus one curve, with $C(k) = \emptyset$ and $C(k(\sqrt{a})) \neq \emptyset$ for some $a \in k^\times$, then C is a 2-torsor of its Jacobian. We will also refer to such genus one curves as 2-torsors, leaving the Jacobian implicit.

- If C/k is a 2-torsor, then C can be described as:

  $$w^2 = Q(u, v)$$

  for a homogenous quartic Q.

- Since period divides index, every 2-torsor of E has period dividing 2. Furthermore, a 2-torsors can't have period 1, so every 2-torsor has period 2.

- If we start with an equation:

  $$w^2 = Q(u, v)$$

  then C is a 2-torsor iff:

– $Q(u,1)$ is an irreducible polynomial of degree 4.

– We can view Q as a map of sets $\mathbb{P}^1 \to k^\times/k^{\times 4}$. In order for C to be a 2-torsor, the image of $\mathbb{P}^1$ in $k^\times/k^{\times 4}$ should be disjoint $k^{\times 2}/k^{\times 4}$.

Concretely, we're just saying that $Q(u,v)$ is not a square for any $u, v \in k$, since otherwise we have a k-point on C.

In particular, we can deform the equation of a 2-torsor to obtain the equation of an elliptic curve with a non-identity MW point, by replacing the leading coefficient of Q by a square.

10.1 Jacobian Formula

If we start with an equation:

$$w^2 = Q(u,v)$$

then we can use the Jacobian formula to obtain an equation for E/k. This is one of the main tools in [50], so we review this now so that we can explain how to generalize it to higher degree in the next chapter.

If we write:

$$Q(u,v) = au^4 + bu^3v + cu^2v^2 + duv^3 + ev^4 \tag{10.1}$$

then the Jacobian of C is the Weierstrass elliptic curve:

$$y^2 = x^3 + cx^2 + (bd - 4ae)x + ad^2 + b^2e \tag{10.2}$$

If $char(k) \neq 3$, the coefficients of the short Weierstrass equation are:

$$f = -4ae - \frac{c^2}{3} \qquad g = -\frac{8ace}{3} + ad^2 + \frac{2c^3}{27}$$

- The cubic used to define the Jacobian coincides with the resolvent cubic of $Q(x, 1)$.
- The invariants f, g are scalar multiples of the classical invariants of Q under the action of $SL_2(\overline{k})$.

We write $\mathcal{Q} = \{(a, b, c, d, e)\}$ for the space of equations of quartics as in 10.1.

Let $\mathcal{C}_2 \subset \mathcal{Q}$ be the subset consisting of nondegenerate quartics. We will think of elements of $\mathcal{C}_2$ as representing smooth genus one curves $w^2 = Q(u, v)$.

The group $SL_2(k)$ acts on $\mathcal{Q}$: The discriminant is invariant under this action, so it restricts to an action on $\mathcal{C}_2$.

Since the coefficients f, g of the Jacobian are $SL_2(\overline{k})$ invaraints, they are also $SL_2(k)$ invariants, so we can think of the Jacobian formula as a map $\mathcal{C}_2 \to \mathcal{W}$ that factors through the quotient $\mathcal{C}_2/SL_2(k)$. The problem of classifying all 2-torsors of fixed elliptic curve E is then the same as computing the fiber over a fixed point (f, g).

We start by studying the action of some subgroups of $SL_2(k)$ on $\mathcal{C}$.

10.1.1 Translations

Let $Q(u, v)$ be a quartic with coefficients in $\mathcal{C}_2^*$, and let C be the associated genus one curve. If $C(k) = \emptyset$, then $Q(u, 1) = a \in k^\times$, where a is a nonsquare in k, and C splits over $k(\sqrt{a})$.

For any such Q, there is a unique $\lambda \in k$ such that $Q(u + \lambda v, v)$ is given by an equation of the form:

$$w^2 = au^4 + cu^2 + du + e$$

Thus, it suffices to consider genus one curves given by an equation with $b = 0$. We denote this subset $\mathcal{C}_2^0$.

Note that the Jacobian formula, when restricted to $\mathcal{C}_2^0$, simplifies to:

$$y^2 = x^3 + cx^2 - 4aex - 4ace + ad^2$$

10.1.2 $k^\times$ action

Let $D \subset SL_2(k)$ be the subgroup of diagonal matrices. Note that $D \cong k^\times$, since every element has the form $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ for some $t \in k^\times$.

Then D acts on quartics by:

$$t \cdot Q(u, v) = Q(tu, t^{-1}v)$$

At the level of coefficients, the action is:

$$t \cdot (a, b, c, d, e) = (t^4 a, t^2 b, c, t^{-2} d, t^{-4} e)$$

- The action respects the monomial structure, so in particular, it restricts to an action on $\mathcal{C}_2^0$.
- If Q, Q' are in the same D orbit, then their leading coefficients are in the same square class.

We write $\mathcal{T}_2$ for the quotient $\mathcal{C}_2^0/D$, and $\mathcal{T}_2^0$ for the subset of $\mathcal{T}_2$ consisting of equations with $d = 0$.

- Note that c, ad^2, ae are invariant under this action, so the Jacobian formula indeed factors through $\mathcal{T}_2 \to \mathcal{W}$.

- Furthermore, we have a projection map $\mathcal{T}_2 \to k$ that sends an equivalence class in $\mathcal{T}_2$ to c.

Let $\mathcal{T}_2 \to \mathcal{W} \times k$ be the product of those maps.

We will show the following:

- The map is surjective.

- This map is a bijection away from $\mathcal{T}_2^0$.

- Elements of $\mathcal{T}_2^0$ map to pairs $((f, g), c)$, where $c^3 + fc + g = 0$. The fiber over such a triple is a $k^\times/k^{\times 2}$ torsor.

This implicitly gives us the desired description of the fibers $\mathcal{C}_2 \to \mathcal{W}$: we have factored the map as:

$$\mathcal{C}_2 \to \mathcal{C}_2^0 \to \mathcal{T}_2 \to \mathcal{W}$$

The fibers of $\mathcal{C}_2 \to \mathcal{C}_2^0$ are k-torsors, the fibers of $\mathcal{C}_2 \to \mathcal{T}_2$ are $k^\times$-torsors and the fibers of $\mathcal{T}_2 \to \mathcal{W}$ look like one of the following:

- If (f, g) defines an elliptic curve with no 2-torsion points over k, then the fiber over (f, g) is isomorphic to k.

- If (f, g) defines an elliptic curve with a single 2-torsion point, then the fiber looks like $(k - \{c_0\}) \sqcup k^\times/k^{\times 2}$, where c_0 is the unique root of $x^3 + fx + g$.

- If (f, g) has full 2-torsion defined over k, then the fiber is $(k - \{c_1, c_2, c_3\}) \sqcup (k^\times/k^{\times 2}) \sqcup (k^\times/k^{\times 2}) \sqcup (k^\times/k^{\times 2})$.

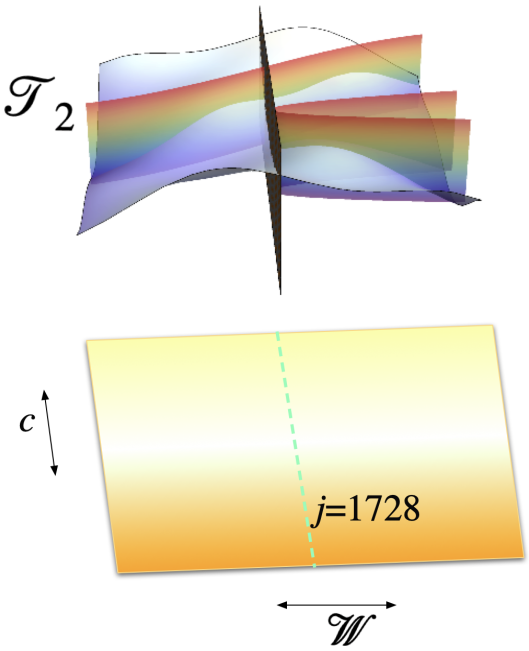


Figure 10.1: *An illustration of the map* $\mathcal{T}_2 \to \mathcal{W}$.

- If $x^3 + fx + g$, the fiber over (f, g) looks like k: for each $c \in k$, there is a unique $a \in k^\times/k^{\times 2}$ such that $a \equiv c^3 + fc + g$. Choosing a representative for that square class lets us solve for d, e.

- If $x^3 + fx + g$ is not irreducible, but we choose $c \in k$ which is not a root of the cubic, we still have a unique point in the fiber over (f, g) with that choice of c.

  If $c^3 + fc + g = 0$, there are $k^\times/k^{\times 2}$'s worth of torsors with $c = 0$ - we choose a freely and solve for e:

$$w^2 = au^4 + cu^2 - \frac{c^2 + 3f}{12a}$$

Thus, if we work with $\mathcal{T}_2$ instead of the full space of quartics, we are not really losing anything - however, the Jacobian map becomes much easier to understand.

10.2 Cocycles and Trace Zero Points

We interpret the results of the previous section using Galois cohomology.

Let C be the 2-torsor:

$$w^2 = au^4 + cu^2v^2 + duv^3 + ev^4$$

Let $k' = k(\sqrt{a})$, σ the generator of $Gal(k'/k)$, and $q \in C(k')$ the point with coordinates $a = 1, u = 0, w = \sqrt{a}$.

The cocycle representing (C, q) in $WC(E/k)$ is the map:

$$Gal(\overline{k}/k) \to E(\overline{k}) \qquad \tau \mapsto [\tau(q) - q] \in E(\overline{k})$$

Since $q \in C(k')$, the orbit of q contains only two elements, so the cocycle can be described as:

$$\tau \mapsto \begin{cases} 0 & \text{if} \quad \tau(\sqrt{a}) = \sqrt{a} \\ [\sigma(q) - q] & \text{if} \quad \tau(\sqrt{a}) = -\sqrt{a}) \end{cases}$$

Thus, we can recover the entire cocycle if we know $\sqrt{a}$ and $p = [\sigma(q) - q] \in E(k')$.

Now, let $p \in E(k')$ and suppose $p = [\sigma(q) - q]$ for some $q \in C(k')$.[1]

Then $p + \sigma(p) = 0$.

- In order to satisfy the cocycle condition, the image of σ has to satisfy $\sigma(p) + p = 0$.
- A different way of seeing this is using the torsor condition: if $p = [\sigma(q) - q]$, then:

$$(\sigma(p) + p) + q = \sigma(p) + (p + q) = \sigma(p) + \sigma(q) = \sigma(p + q) = \sigma(\sigma(p)) = p$$

[1] In other words, suppose the map $\sigma \mapsto p$ satisfies the cocycle conditon.

Thus, $\sigma(p) + p$ fixes a point on C, so it must be the identity since the action is simply transitive.

Thus, cocycles with values in $E(k')$ are in bijection with points in the kernel of the trace map $E(k') \to E(k)$.

10.2.1 Quadratic Twists

Let E/k be an elliptic curve:

$$E: \quad y^2 = x^3 + fx + g$$

and let $a \in k^\times$ be a nonsquare. Let E_a be the quadratic twist of E/k:

$$ay^2 = x^3 + fx + g$$

Let $k' = k(\sqrt{a})$.

- There is an isomorphism $E(k') \cong E_a(k')$.
- The image of $E_a(k)$ in $E(k')$ coincides with the kernel of the trace map $E(k') \to E(k)$.
- The intersection $E(k) \cap E_a(k)$ coincides with the 2-torsion subgroup of $E(k)$.

Proof. Define a map:

$$E(k') \to E_a(k') \qquad (p, q) \mapsto (p, \sqrt{a}q)$$

It's clear that this takes pairs satisfying $y^2 = x^3 + fx + g$ to pairs satisfying $ay^2 = x^3 + fx + g$, and that the map is a bijection.

The image of $E_a(k)$ under the inverse map consists of all points of the form $(p, \sqrt{a}q) \in E(k')$.

This subset of $E(k')$ can be characterized in several ways:

- $P \in E(k')$ such that $x(P) \in k$ and $y(P) \in \sqrt{a}k$.
- $P \in E(k')$ such that $\sigma(x(P)) = x(P)$ and $\sigma(y(P)) = -y(P)$.
- $P \in E(k')$ such that $\sigma(P) = -P$.
- $P \in \ker(E(k') \to E(k))$.
- $P \in E(k')$ satisfying $x(P) \in k$ and exactly one of the following two conditions:
  - $P \in E(k')$.
  - P is a 2-torsion point.
- $x(P) \in k$ and $Tr_{k'/k}(y(P)) = 0$.
- $Tr(P) = 0$.

The equivalence of these conditions is obvious.

Furthermore, it's clear that if $P \in E(k) \cap E(k')$, then P is a 2-torsion point.

□

Thus, the problem of finding all cocycles that split over a given extension k' boils down to finding all k-points on the quadratic twist $E_a(k)$. This is a hard problem.

However, if we instead try to classify all cocycles that split over an arbitrary quadratic extension, then the problem becomes trivial: starting from the Weierstrass equation, we simply evaluate the cubic $x^3 + fx + g$ at every point $c \in k$.

For at most 3 values of c, we get 0. In those cases, we have just found a 2-torsion point on E. Since the 2-torsion points in $E(k)$ are contained in the kernel

of every trace map $E(k') \to E(k)$, we have an associated cocycle for each quadratic extension k'.

A direct construction for the torsor from the cocycle for this special case is given in [62].

In the generic case, i.e. when $c^3+fc+g \in k^\times$, we either have $c^3+fc+g \in k^{\times 2}$, in which case we've found a rational point in $E(k)$, or else there is a unique quadratic extension k'/k where $c^3 + fc + g$ is a square.

10.2.2 Example: $k = \mathbb{R}$

Say we have an elliptic curve $E/\mathbb{R}$:

$$y^2 = x^3 + fx + g$$

Then every $c \in \mathbb{R}$ either gives rise to a point on $E(\mathbb{R})$ or a point on the quadratic twist of E, depending on whether $c^3 + fc + g \geq 0$ or $c^3 + fc + g \leq 0$.

We can represent all of these as a subset of $\mathbb{R}^3$: we use one of the axes to represent x, and the other two axes represent y and iy. The xy-plane represents the points on $E(\mathbb{R})$ and the $x(iy)$-plane represents points on the quadratic twist.

If $j(E) < 1728$, every cocycle is a coboundary. When $j(E) > 1728$, there are cocycles which are not coboundaries. Since we have a surjection of $E(\mathbb{C})$ onto the coboundaries, the space of coboundaries is connected and contains the identity. Thus, we can make a picture (10.2) representing the cocycles and coboundaries of $WC(E/\mathbb{R})$: we will use two axes to represent y, iy and the remaining axis to represent x (with $x, y \in RR$). Plugging in real values into $x^3 + fx + g$ either gives us 0, in which case we have a 2-torsion point, a positive value, in which case we've found a pair of points in $E(\mathbb{R})$ or a negative value, in which case we've found a pair of trace zero points.

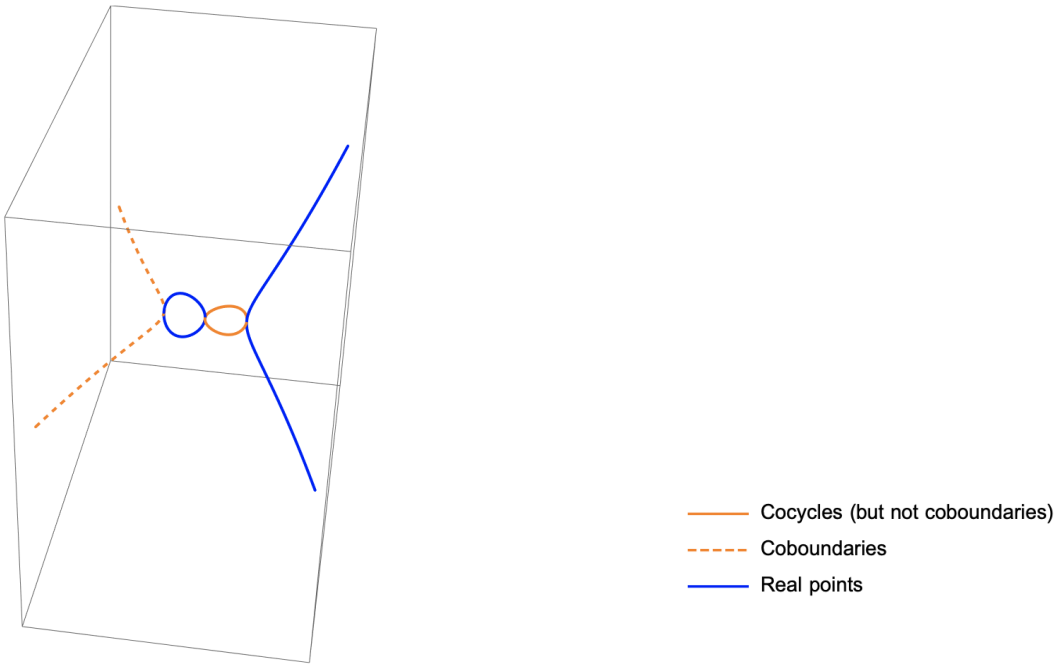


Figure 10.2: *Cocycles and coboundaries for* $WC(E/\mathbb{R})$ *as a subset of* $E(\mathbb{C})$.

10.3 Quaternion Algebras and the Witt Ring

In [34], it is shown how to construct a quaternion algebra over E that represents the class of $[C]$ in $Br(E)$ under the splitting of:

$$0 \to Br(k) \to Br(E) \to WC(E/k) \to 0$$

afforded to us by the section $Br(E) \to Br(k)$, provided we have an equation for C/k.

Let $(c, \sqrt{a}d)$ be a trace 0 point on E. The methods of the previous section show that we can recover an equation for C/k from the Weierstrass coefficients of E and a, c, d.

- We can write down the algebra without having to use the equation for C.
- The trace 0 condition on $(c, \sqrt{a}d)$ allows us to prove that the quaternion algebra spreads out from $Br(k(E))$ to $Br(E)$.
- We use the relationship between the Witt ring of E and the Brauer group of

E, and certain identities between quadratic spaces, to obtain a description of $WC(E/k)[2]$ in terms of generators and relations.

To begin, we show that the trace 0 condition can be used to give a direct proof that $(x+c, a)$ spreads out to an algebra in $Br(E)$.

Lemma 10.1. *Let E be an elliptic curve, $(c, \sqrt{a}d)$ a point of trace 0 and $(x-c, a) \in Br(K(E))$.*

Then $(x-c, a)$ extends to a class in $Br(E)$.

Proof. We have to find new presentations for the algebra that can be used when $x-c$ or a vanish. Note that:

$$y^2 - ad^2 = (x-c)(x^2 + cx + f + c^2)$$

FUrthermore, $y^2 - ad^2$ is the norm of an element in $K(\sqrt{a})$, so:

$$((x-c)(x^2 + cx + f + c^2), a) = (y^2 - ad^2, a) = 0$$

But that means:

$$(x-c, a) \equiv (x^2 + cx + f + c^2, a)$$

If $3c^2 + f = 0$, then our curve is singular at the trace 0 point.

□

Next, we discuss the group law. Suppose we have a pair of 2-torsors C, C' of E. Let P, P' be the associated trace 0 points.

The cocycle that determines C, C' is determined by P, P', and the cocycle that represents their sum is determined by $P + P'$ (the sum taken in Mordell-Weil).

If P, P' are defined over the same quadratic extension, then $P + P'$ is also defined over that extension, so we end up with a third point of the form $(c, \sqrt{a}d)$. We use the previous results to obtain an equation for the associated torsor.

However, if P, P' are defined over distinct quadratic extensions, the sum $P+P'$ has a Galois orbit with 4-elements, so the associated torsor has index 4. We can keep adding new trace 0 points defined over quadratic extensions to obtain 2-torsion classes in $WC(E/k)$ which do not have index 2. However, no matter how many points we add, the associated torsor always has index at most 4.

We can use the Witt ring of E to obtain a model of index 4 for any torsor of period 2. For ease of exposition, we assume that $E[2] \subset E(K)$.

Theorem 10.2. *Let E/k be the elliptic curve:*

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

Let $W(k)$ be the Witt ring of k and $W(E)$ the Witt ring of E.

1. *$W(E)$ is isomorphic, as a $W(k)$-module, to:*

$$W(E) \cong W(k) \oplus W(K)\langle x - e_1\rangle \oplus W(k)\langle x - e_2\rangle \oplus W(k)\langle x - e_3\rangle$$

2. *Every class of index 2 in $Br(E)/Br(k)$ can be represented by a quaternion algebra of the form $(x - e_i, a)$ for $a \in k^\times$.*

3. *Every class of period 2 in $Br(E)/Br(k)$ can be represented by a quaternion algebra or a biquaternion algebra.*

4. *Every class in $WC(E/k)[2]$ has index 2 or 4.*

5. *Period equals index in $WC(E/k)[2]$ if and only if every quadratic form:*

$$aT_0^2 + (x - e_1)T_1^2 - a(x - e_1)T_2^2 = bT_3^2 + (x - e_2)T_4^2 - b(x - e_2)T_5^2$$

is isotropic in $W(E)$. In particular, period equals index if the function field of E is linked.

.

Proof. The proof of (1) is in [5, 6].

We use (1) to prove (2).

The isomorphism $I^2/I^3 \leftrightarrow Br(E)[2]$ identifies the quaternion algebras (α, β) with 2-fold Pfister form $\langle\langle \alpha, \beta \rangle\rangle$. The decomposition of the Witt ring above makes it clear that every 2-fold Pfister form has one of the following forms:

- $\langle\langle a, b \rangle\rangle$ for $a, b \in K^\times$. The corresponding algebras come from $Br(K)$, and can be ignored.
- $\langle\langle x - e_r, a \rangle\rangle$, $a \in K^\times$.
- $\langle\langle x - e_r, x - e_s) \rangle\rangle$.

Consider the quaternion algebra $Q = (x - e_r, x - e_s)$ for $r, s \in \{1, 2, 3\}$.

Case 1: $r = s$. Then:

$$[(x-e_r, x-e_r)] = [(x-e_r, (-1)(e_r-x))] = [(x-e_r, e_r-x)]+[(x-e_r, -1)] = [(x-e_r, -1)]$$

Case 2: $r \neq s$. Say $r = 1, s = 2$ and let i, j, k be the standard orthogonal basis of the space of pure quaternions in $(x - e_1, x - e_2)$. Then:

$$k^2 = -(x - e_1)(x - e_2) = \frac{-y^2}{x - e_3} = -\left(\frac{y}{x - e_3}\right)^2 (x - e_3)$$

$$(i+\sqrt{-1}j)^2 = i^2 + \sqrt{-1}(ij+ji) - j^2 = (x+e_1) - (x-e_2) = e_1 - e_2$$

$$(i+\sqrt{-1}j)k + k(i+\sqrt{-1}j) = (ik+ki) + \sqrt{-1}(jk+kj) = 0$$

so the space of pure quaternions in $(x-e_1, x-e_2)$ is isometric to the space of pure quaternions in $(x-e_3, e_1-e_2)$, so the algebras are isomorphic, i.e. $[(x-e_1, x-e_2)] \equiv [(x-e_3, e_1-e_2)]$. This proves (2).

To prove (3), note first that $Br(E)$ injects into the Brauer group of its function field, and the 2-torsion subgroup of the latter is generated by quaternion algebras by Merkurjev's theorem. We've shown that every (relevant) quaternion algebra has the form $(x-e_r, a)$. By well-known properties of quaternion algebras, we have:

$$(x-e_r, a) \otimes (x-e_r, b) \cong M_2(K) \otimes (x-e_r, ab)$$

so tensor products of arbitrarily long length are always Morita equivalent to a tensor product of the form:

$$(x-e_1, a) \otimes (x-e_2, b) \otimes (x-e_3, c)$$

Finally, using the defining equation of E, we can show that:

$$(x-e_3, c) = ((x-e_1)(x-e_2), c) \equiv (x-e_1, c) \otimes (x-e_2, c)$$

so:

$$(x-e_1, a) \otimes (x-e_2, b) \otimes (x-e_3, c) \equiv (x-e_1, ac) \otimes (x-e_2, bc)$$

This proves (3).

(4) follows easily from (3); the torsor associated to $(x-e_1, a) \otimes (x-e_2, b)$ is:

$$aX_0^2 - bX_1^2 = (e_2 - e_1)X_3^2 \qquad aX_0^2 - abX_2^2 = (e_3 - e_1)X_4^2$$

Finally, (5) is simply the Albert criterion applied to the quaternion algebras above.

□

Remark: As a corollary, we have a formula for the group law in $WC(E/K)[2]$; the results above tell us that every torsor is represented by an algebra of the form $(x - e_1, a) \otimes (x - e_2, b)$, and it's clear how to "add" those algebras. Since we can freely go back and forth between equations for torsors and Azumaya algebras, we have our "group law formula".

Finally, we show how to express a given algebra $(x - c, a)$ in terms of the generators.

Lemma 10.3. *Let $\alpha, \beta \in K^\times$, with $\alpha + \beta \neq 0$. The quaternion algebra $A = (\alpha, \beta)$ is isomorphic to $(\alpha + \beta, -\alpha\beta)$ as K-algebras.*

Proof. We will find an orthogonal basis of A that satisfies the relations of the second algebra.

Let $\tilde{i} = i + j$ and $\tilde{j} = \beta i - \alpha j$.

Observe that:

$$\tilde{i}^2 = (i + j)^2 = i^2 + ij + ji + j^2 = \alpha + \beta$$

$$\tilde{k}^2 = (\beta i - \alpha j)^2 = \beta^2 i^2 - \beta\alpha ij - \beta\alpha ji + \alpha^2 j^2 = \alpha\beta(\alpha + \beta)$$

$$\tilde{i}\tilde{k} = \beta i^2 - \alpha ij + \beta ji - \alpha j^2 = (\beta - \alpha)ji$$

$$\tilde{k}\tilde{i} = \beta i^2 + \beta ij - \alpha ij - \alpha j^2 = (\beta - \alpha)ij$$

The last two displays show that:

$$\tilde{i}\tilde{k} + \tilde{k}\tilde{i} = 0$$

Thus, $A \equiv (\alpha + \beta, \alpha\beta(\alpha + \beta))$.

The usual equivalence $(\gamma, \delta) \equiv (\gamma, -\gamma\delta)$ gives us the final representation $A \equiv (\alpha + \beta, -\alpha\beta)$. □

Proposition 10.4. *Consider E/k:*

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

and suppose we have a torsor $d \neq 0$ with quaternion algebra $(x - c, a)$, with $c \neq e_\ell$ for $\ell = 1, 2, 3$ (in the notation of Prop 5.1).

Then:

$$(x - c, a) \equiv (x - e_1, c - e_1) \otimes (x - e_2, c - e_2) \otimes (x - e_3, c - e_3)$$

in the Brauer group of E.

Proof. By the proposition above, we know that c is the abscissa of a K-point on the quadratic twist of E by $\sqrt{a}$, so:

$$(c - e_1)(c - e_2)(c - e_3) \equiv a \pmod{K^{\times 2}}$$

$$(x - c, a) \equiv (x - c, c - e_1) \otimes (x - c, c - e_2) \otimes (x - c, c - e_3)$$

Applying the lemma:

$$
\begin{aligned}
(x-c,a) &\equiv \bigotimes_{\ell=1}^{3}(x-c, c-e_\ell) \\
&= \bigotimes_{\ell=1}^{3}(x-e_\ell, (x-c)(e_\ell-c)) \\
&\equiv \bigotimes_{\ell=1}^{3}(x-e_\ell, (e_\ell-c)) \otimes (x-e_\ell, x-c) \\
&\equiv ((x-e_1)(x-e_2)(x-e_3), x-c) \otimes \bigotimes_{\ell=1}^{3}(x-e_\ell, (e_\ell-c)) \\
&\equiv (y^2, x-c) \otimes \bigotimes_{\ell=1}^{3}(x-e_\ell, (e_\ell-c)) \\
&\equiv \bigotimes_{\ell=1}^{3}(x-e_\ell, (e_\ell-c))
\end{aligned}
$$

□

10.4 2-Torsors over Discrete Valuation Rings

We quickly comment on the theory of 2-torsors over discrete valuation rings, as many of our tools work better than expected in that setting.

Let R be a DVR over an algebraically closed field of characteristic 0, and let C/R be a 2-torsor. Then we have a model for C of the form 10.1. By 1.14, we can transform that to an equation:

$$w^2 = au^4 + cu^2 + du + e$$

with $\nu(a) = \min\{\nu(a), \nu(c), \nu(d), \nu(e)\}$.

- If $\nu(a) = 0$, then the torsor splits (since we are assuming the residue field is algebraically closed).

- If $\nu(a) \geq 2$, then every coefficient is divisible by ϖ^2 so we can obtain a new equation over R by dividing through by ϖ^2. Thus, we may assume that $\nu(a) = 1$ and $\nu(c), \nu(d), \nu(e) \geq 1$.

Thus, if C does not have a section over R, then the special fiber is singular.

The isomorphism types of singular fibers for 2-torsors are described in [56]. We can determine the isomorphism type directly from the valuations of $\nu(a), \nu(c), \nu(d), \nu(e)$ using the Jacobian formula and the valuative characterizations of singular fibers on the Jacobian.

To begin, we need an analog of a minimal integral equation for 2-torsors.

- Suppose we have an equation for C:

$$w^2 = a_0u^4 + a_1u^3v + a_2u^2v^2 + a_3uv^3 + a_4v^4$$

and $\nu(a_i) \geq i$ for all i.

Then replacing v by ϖv, we obtain a new equation for C with coefficients $a_i' = \varpi^{-i}a_i$. Thus, we may assume $\nu(a_i) < i$ for at least one value of i.

- Next, suppose $\nu(a_i) \geq 2$ for all i. We can replace w by ϖw and divide through by ϖ^2 to obtain a new equation over R. Thus, we may further assume that $\nu(a_i) < 2$ for all i.

- Finally, we can use 1.14 to obtain an equation with $\nu(a_0) = \min\{\nu(a_i)\}$ and $a_1 = 0$.

This will reduce the possibilities for $\nu(a_i)$ that we have to consider.

- We may assume that $\nu(a_0) \leq 1$.

- If $\nu(a_0) = 1$, then $\nu(a_i) \geq 1$ for all i and the Jacobian has a nonreduced singularity.

Now, assume that C is given by an equation as in 3.3, with coefficients in R satisfying the minimality conditions just described. Let f, g be the Weierstrass coefficients of the Jacobian. We compute:

$$\nu(f) \geq \min\{\nu(a) + \nu(e), 2\nu(c)\} \tag{10.3}$$
$$\nu(g) \geq \min\{\nu(a) + \nu(c) + \nu(e), \nu(a) + 2\nu(d), 3\nu(c)\} \tag{10.4}$$

We can determine the isomorphism type of the special fiber on the Jacobian from the valuations of the coefficients of C. For example, recall that we have a singularity of type III if $\nu(f) = 1$ and $\nu(g) \geq 2$.

- It's easy to see that $\nu(f) = 1$ is only possible if $\nu(a) = 0$, $\nu(c) \geq 1$, $\nu(e) = 1$.
- Under the conditions required for $\nu(f) = 1$, we have $\nu(g) \geq \min\{2\nu(d), \nu(c) + 1\}$, since $3\nu(c) > \nu(c) + 1$.

Thus, we have a singularity of type III if and only if $\nu(a) = 0$, $\nu(c), \nu(d) \geq 1$ and $\nu(e) = 1$.

Similar characterizations can be obtained for the other fiber types.

We make some final remarks about the geometry of 2-torsors (over local rings).

- Suppose $\nu(a) = 1, \nu(e) = 3$ and $\nu(c) \geq 2, \nu(d) \geq 3$. Then the equation for the torsor is minimal, but the equation for the Jacobian is not.

  This phenomenon is discussed in [49].

- For more on the geometry of the special fiber in torsors of low degree, see [57].

Chapter 11

Index 3 Torsors

11.1 Field Preliminaries

The next simplest case to consider is torsors that split over a cubic extension. Already, though, there are new challenges:

- Every field (of characteristic not 2) contains a primitive 2nd root of unity. However, fields as big as $\mathbb{R}$ can fail to have any other primitive root of unity.
- Every quadratic extension is Galois. Again, this is no longer the case as soon as we pass to cubic extensions.

We can deal with both of these issues simultaneously by assuming that k is quadratically closed and $6 \in k^\times$; in that case $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.

The map $WC(E/k) \to WC(E/k^q)$ is injective on odd-torsion, so we do not have to worry about accidentally introducing rational points on index 3 torsors that didn't have any to begin. Furthermore, this assumption also guarantees we have a primitive cube root of unity in k, since k must contain roots of $x^2 - x + 1$.

Thus, every cubic extension of k has the form $k(\sqrt[3]{a})$ for some $a \in k^\times$.

Now, say we have a quadratic polynomial $ax^2 + bx + c$ over k and a quadratic extension $k(\sqrt{d})/k$. The polynomial splits over k' iff d is in the same square class as $b^2 - 4ac$.

We will need an analogous results for cubic polynomials.

- We need to be able to find an element $a \in k^\times$ such that $k(\sqrt[3]{a})$ is the splitting field of a given cubic.
- We need a criterion for determining whether an arbitrary cubic splits over a given cubic extension $k(\sqrt[3]{a})$.

Proposition 11.1. *Let $x^3 + fx + g$ be an irreducible cubic.*

- *Let $a \in k^\times$. Then $x^3 + fx + g$ splits over $k(\sqrt[3]{a})$ iff there exist $q, t \in k$ such that:*

$$-3aqt = f \qquad -a^2q^3 - at^3 = g \tag{11.1}$$

- *The cubic $x^3 + fx + g$ splits after adjoining a cube root of:*

$$\frac{g}{2} + \frac{\sqrt{\Delta}}{3\sqrt{6}} \tag{11.2}$$

Proof. If x^3+fx+g is irreducible over k, then its roots in k' have trace zero, so we can write them as $q\alpha + t\alpha^2, q\omega\alpha + t\omega^2\alpha^2, q\omega^2\alpha + t\omega\alpha^2$ for some $q, t \in k$. Equating coefficients in:

$$x^3 + fx. + g = \prod_{i=0}^{2} x - (\omega^i\alpha q + \omega^{2i}\alpha^2 t)$$

we obtain the system of equations:

$$-3aqt = f \qquad -a^2q^3 - at^3 = g$$

If $x^3 + fx + g$ splits over k, we can solve the system above, and if we have a solution q, t to that system, then $q\alpha + t\alpha^2$ is a root of the cubic.

By the cubic formula, we can always take $a = \frac{g}{2} + \frac{\sqrt{\Delta}}{6\sqrt{3}}$.

□

Finally, note that we can still solve 11.1 over k if $x^3 + fx + g$ splits completely over k, and k contains a primitive cube root of unity ω. In that situation, we can find $p, q \in k$ such that:

$$\begin{aligned} x^3 + fx + g &= (x - p)(x - q)(x + p + q) \\ &= x^3 + (pq - p(p + q) - q(p + q))x + pq(p + q) \\ &= x^3 + (p^2 - pq + q^2)x + pq(p + q) \\ &= x^3 + (p + \omega q)(p + \omega^2 q)x + pq(p + q) \end{aligned}$$

11.2 Trace Zero Points

Since we're studying torsors that split over a cyclic extension, it's clear that we will need to use trace zero points on the Jacobian at some point.

We characterize these before discussing torsors.

Let E/k be an elliptic curve given by a Weierstrass equation:

$$y^2 = x^3 + fx + g$$

Let $k' = k(\sqrt[3]{a})$ be a cubic extension and let $P \in E(k')$.

Proposition 11.2. *The following are equivalent:*

- *P is in the kernel of the trace map.*

- *There's a line that meets E at $P, \sigma(P), \sigma^2(P)$* [1]
- $\sigma(P) + \sigma^2(P) = -P$
- $x(\sigma(P) + \sigma^2(P)) = x(P)$.
- *There's a line defined over k that meets E at $P, \sigma(P), \sigma^2(P)$.*

Proof. The equivalence of the first three conditions is clear. Furthermore, it's clear that $\sigma(P) + \sigma^2(P) = -P$ implies $x(\sigma(P) + \sigma^2(P)) = x(P)$, and that the last condition implies the second conditon.

If we assume $x(\sigma(P) + \sigma^2(P)) = x(P)$, then $y(\sigma(P) + \sigma^2(P)) = \pm y(P)$, so either $\sigma(P) + \sigma^2(P) = -P$ or $\sigma(P) + \sigma^2(P) = P$. In the first case, P clearly has trace zero.

If $P \in E(k')$, $x(\sigma(P) + \sigma^2(P)) = x(P)$ and $y(\sigma(P) + \sigma^2(P)) = y(P)$, then $Tr(P) = 2P$. Since $Tr(P) \in E(k)$, this means $Tr(2P) = 6P$. But $Tr(2P) = 2Tr(P) = 4P$ so $2P = 0$.

Thus P is a 2-torsion point on $E(k')$.

If $P \in E(k)$, then $P = \sigma(P) = \sigma^2(P)$, so $\sigma(P) + \sigma^2(P) = 0$. This means $x(P) \neq x(\sigma(P) + \sigma^2(P))$, which contradicts our current assumption. Thus, $P \notin E(k)$.

This means $x(P)$ is a root of $x^3 + fx + g$ and so $P, \sigma(P), \sigma^2(P)$ are all 2-torsion points on $E(k)$. Since they all lie on the line $y = 0$, they are collinear.

Thus, the fourth condition implies the previous 3.

Finally, we show that the first 4 conditions imply the fifth.

Now, let $P \in E(k')$ be a point of trace zero and let λ be the slope of the line through $\sigma(P)$ and $\sigma^2(P)$. We use the formula for the group law to compute:

[1] If P is fixed by σ, then we mean the line passes through P with multiplicity 3.

$$x(\sigma(P) + \sigma^2(P)) = \lambda^2 - x(\sigma(P)) - x(\sigma^2(P))$$

Setting this equal to $x(P)$ and rearranging, we obtain:

$$x(P) + \sigma(x(P)) + \sigma^2(x(P)) = \lambda^2$$

The left hand side of this equation is $Tr(x(P)) \in k$, so $\lambda^2 \in k$. Thus λ is defined over an intermediate extension in k'/k of degree at most 2. But k'/k has degree 3, so $\lambda \in k$.

□

If $P \in E(k')$ has trace zero, we can perform a change of variable of the form over k of the form $y \to y + \lambda x + t$ to obtain a new equation:

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

where the tangent at P has the form $y = t_0$ for some $t_0 \in k$.

The coefficient a_1 is determined by P. However, we still have freedom in choosing the remaining coefficients.

- Regardless of what we do to the left hand side, we will always assume that a change of variable has then been performed on the right hand side to ensure $a_2 = 0$.

- If we have a trace zero point of order 3, we can choose an equation for the Jacobian so that the line passing through our chosen point and its conjugates has the form $y = t$ for some $t \in k$. This choice uniquely determines a_1, but we still have some freedom in choosing t. Different choices of t give will change the remaining coefficients.

- In 11.4 we define unobstructed equations. For each pair (f, g) and each choice of a_1, there is at least one and at most two unobstructed equations. This will allow us to assign one or two unobstructed equations to each pair (E, p) consisting of an elliptic curve E/k and a point $p \in E(k')$ of trace zero.

11.3 Plane cubics

Every torsor of index 3 has a model as a plane cubic in $\mathbb{P}^2_k$. We have a 10-dimensional space $\mathcal{C}_3$ of equations for non-degenerate plane cubics, and we can define a map $\mathcal{C}_3 \to \mathcal{W}$ that sends a cubic to it's Weierstrass coefficients.

We have an action of $PGL_3(k)$ on $\mathcal{C}_3$.

For a given cubic $F(x, y, z)$, the coefficients f, g of the Jacobian turn out to be scalar multiples of the Aronhold invariants of F - that is, the map $\mathcal{C}_3 \to \mathcal{W}$ coincides with the quotient $\mathcal{C}_3 \to \mathcal{C}_3/PGL_3(\overline{k})$.

The Jacobian formula for a general element of $\mathcal{C}_3$ over fields of characteristic not equal to 2 or 3 can be found in [1]. The formula is generalized to plane cubics over arbitrary schemes in any characteristic in [7].

Rather than presenting the full formula, we find a convenient subset of $\mathcal{C}_3$ which contains a fundamental domain for the action of $PGL_3(k)$. We then give the Jacobian formula for cubics in that subset.

Precisely, we will show that there is a change of variable to an equation of the form:

$$ax^3 + by^3 + cz^3 + qy^2z + txy^2 + mxyz = 0$$

We write $\mathcal{C}_3^0$ be the subset of $\mathcal{C}_3$ consisting of equations of that form.

Proof. We will use the normalization process described in [24]. Let $F(x, y, z) \in \mathcal{C}_3$

and let ℓ be a line in $\mathbb{P}^2$.

- The restriction of F to ℓ is a binary cubic. Note that this cubic is necessarily irreducible over k, since otherwise we can find a nontrivial zero of F in k.

- Since k is quadratically closed, the splitting field of $F|_\ell$ is a cyclic extension of degree 3. We can do a change of variables (essentially acting on $\mathbb{P}^2$ by a fractional linear transformation in the coordinates of ℓ) so that:

  $$F(x, y, z) = by^3 + F_1(x, z)y^2 + F_2(x, z)y + (ax^3 + cz^3)$$

  with F_1, F_2 binary forms of degree 1,2 respectively.

  Note that $b \neq 0$, since otherwise the curve would have the point $[0 : 1 : 0]$.

- Next, if we replace x by $x + \lambda y$, we obtain a new equation:

  $$F(x+\lambda y, y, z) = (b+a\lambda^3)y^3+(F_1(x, z)+3a\lambda^2 x)y^2+(F_2(x, z)+3a\lambda x^2)y+(ax^3+cz^3)$$

  If we set λ to be the negative of the coefficient of x^2 in $F_2(x, z)$, we obtain a new equation of the same form but where $F_2(x, z)$ is guaranteed to not have an x^2 term.

- Finally, replacing z by $z+\lambda y$ as above, we can eliminate the yz^2 term without affecting the yx^2 term. Thus, we now have an element of $\mathcal{C}_3^0$.

Thus, $\mathcal{C}_3^0$ contains a fundamental domain for $\mathcal{C}_3/SL_3(k)$. □

11.3.1 $k^\times$ action

Having decided on a "monomial structure", we now describe some actions of $k^\times$ on $\mathcal{C}_3^0$

- First, we have the action of $k^\times$ on $\mathcal{C}_3^0$ that scales a polynomial. One often uses this scaling to obtain an equation with $c = 1$ to eliminate one of the variables.

- We also have an action of $k^\times \times k^\times$ on $\mathcal{C}_3^{unob}$, where we identify $k^\times \times k^\times$ with the subgroup of diagonal matrices in $SL_3(k)$. Explicitly, the action is given by:

$$(t_1, t_2) \cdot F(x, y, z) = F(t_1 x, t_2 y, (t_1 t_2)^{-1} z)$$

Note that the $k^\times$ action changes the coefficients f, g of the Jacobian (see next section) but the $k^\times \times k^\times$ action fixes them. Both actions preserve the k-isomorphism class of the Jacobian, i.e. they don't change the j-invariant.

11.4 Jacobian Formula and Unobstructed Equations

Now, we are going to try to invert the Jacobian formula as we did with 2-torsors. This will be possible if we use unobstructed equations.

Let $\mathcal{W}^{ext}$ be the space of extended Weierstrass equations. Let $F \in \mathcal{C}_3^0$ and let C be the associated genus one curve. The Jacobian of C is isomorphic to the elliptic curve E/k:

$$E: \quad y^2 + a_1 xy + a_3 y = x^3 + a_4 x + a_6$$

where:

$$
\begin{aligned}
a_1 &= m \\
a_2 &= 0 \\
a_3 &= 9abc \\
a_4 &= -3acqt \\
a_6 &= -27a^2b^2c^2 - a^2cq^3 + abcm^3 - ac^2t^3 - acm^2qt
\end{aligned}
$$

We think of this as a map $\mathcal{C}_3^0 \to \mathcal{W}^{ext}$.

Definition 11.4. *Let C be a curve given by an equation $F = 0$ for $F \in \mathcal{C}_3^0$. We say the equation for C is unobstructed if:*

$$-27a^2b^2c^2 + abcm^3 - acm^2qt = 0$$

Let E/k be an elliptic curve, and assume E is given by an extended Weierstrass equation with $a_2 = 0$ and $a_3 \neq 0$. We say that the equation for E is unobstructed if:

$$\frac{a_3^2}{-3} + \frac{a_3a_1^3}{9} + \frac{a_1^2a_4}{3} = 0$$

An easy computation shows:

Lemma 11.5. *TFAE:*

- *The equation for C is unobstructed.*
- *The equation for the Jacobian is unobstructed.*
- *The equation for the Jacobian is:*

$$y^2 + mxy + 9abcy = x^3 - 3acqtx - a^2cq^3 - ac^2t^3$$

We write $\mathcal{C}_3^{unob}$ (resp $\mathcal{W}^{unob}$) for the subset of unobstructed equations in $\mathcal{C}_3^0$ (resp. $\mathcal{W}^{ext}$).

Let $\mathcal{W}^{ext} \to \mathcal{W}$ be the map that takes an extended Weierstrass equation to the invariants f, g.

Now, we show how to associate to each a marked genus one curve of index 3 an unobstructed equation for the Jacobian.

Proposition 11.6. *Let (C, Q) be a marked genus one curve of index 3 that splits over $k' = k(\sqrt[3]{a})$. Let E/k be the Jacobian and let $P \in E(k')$ be the point $[\sigma(Q) - Q]$.*

- *P is a nonidentity point in the kernel of the trace map $E(k') \to E(k)$.*
- *There is an equation for E/k as:*

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

  such that the line through $P, \sigma(P), \sigma^2(P)$ has the form $y = t$ for some $t \in k$. The equation is unique[2] up to translations of the form $y \mapsto y + u$ for $u \in k$.

- *There is at least one, and at most two, values of u that give an unobstructed equation.*

Proof. The only point that requires a proof is the last one.

If we start with an equation:

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

and do a change of variable $y \mapsto y + u$ (followed by $x \mapsto x + \frac{a_2'}{3}$) to obtain a new equation:

[2]Among Weierstrass equations with the same discriminant.

$$y^2 + a_1xy + a_3(u)y = x^3 + a_4(u)x + a_6(u)$$

where:

$$\begin{aligned} a_3(u) &= a_3 + 2u \\ a_4(u) &= a_4 \\ a_6(u) &= a_6 - u^2 \end{aligned}$$

Now, the new equation is unobstructed if and only if:

$$-12u^2 + u\left(2a_1^3 - 12a_3\right) + a_1^3a_3 + 3a_1^2a_4 - 3a_3^2 \tag{11.3}$$

Since k is quadratically closed, we can solve for u to obtain an unobstructed equation.

Thus, there are two values of u if and otherwise there is exactly one.

□

Finally, we show how to obtain an equation for C from an unobstructed equation for an elliptic curve E/k.

- Let a_1, a_3, a_4, a_6 be coefficients of an unobstructed cubic.

  If $x^3 + a_4x + a_6$ has a root in k, then it splits completely in k and we have an elliptic curve with 3 rational points on the line $y = 0$. Otherwise, $x^3 + a_4x + a_6$ splits over an extension of the form $k' = k(\sqrt[3]{a})$. The element a is essentially determined by the extension - any other choice of a has to generate the same subgroup of $k^\times/k^{\times 3}$. We can use 11.1 to find an a.

- By 11.1, the fact that $x^3 + a_4x + a_6$ splits over k' is equivalent to the existence of $q, t \in k$ satisfying 11.1.

- Finally, we set $m = a_1$, $c = 1$ and $b = \frac{a_3}{-9a}$. These choices guarantee that (a, b, c, q, t, m) maps to (a_1, a_3, a_4, a_6) under the Jacobian map.

11.5 Factoring the Jacobian Map

Let $\mathcal{W}^{unob}$ be the space of unobstructed Weierstrass equations. We have a map $\mathcal{W}^{unob} \to \mathcal{W}$ that takes an unobstructed equation to the coefficients of the short Weierstrass equation.

The results of the last section can be interpreted as a factorization of the Jacobian map into several, simpler maps:

$$\begin{array}{ccccccc}
\mathcal{C}_3 & \longrightarrow & \mathcal{W}^{ext} & & & & \\
\downarrow & & \downarrow & \searrow & & & \\
\mathcal{C}^{un} & \longrightarrow & \mathcal{W}^{un} & \longrightarrow & k \times \mathcal{W} & \longrightarrow & \mathcal{W} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathcal{C}^{un}/k^\times & \longrightarrow & \mathcal{W}^{un}/k^\times & \longrightarrow & (k \times \mathcal{W})/k^\times & \longrightarrow & \mathcal{W}/k^\times
\end{array} \tag{11.4}$$

To compute the Jacobian, we start on the left side of 11.4 and work our way to the right side of the diagram. We can describe the fibers of each of these simpler maps.

Then map $k \times \mathcal{W}^s \to \mathcal{W}^s$ is simply a projection, so our first task is understanding the fibers of the map $\mathcal{W}^{un} \to k \times \mathcal{W}^s$. Let $(f, g) \in \mathcal{W}^s$, representing the elliptic curve:

$$y_0^2 = x_0^3 + fx_0 + g$$

and let $m, b \in k$. We can do a change of variables replacing x_0, y_0 by x, y, where $y_0 = y + \frac{mx+b}{2}$ and $x_0 = x + \frac{m^2}{12}$. In the new coordinates, we have:

$$y^2 + mxy + by = x^3 + \left(\frac{m^4}{48} - \frac{bm}{2} + f\right)x + \frac{m^6}{1728} + \frac{fm^2}{12} - \frac{b^2}{4} + g$$

The obstruction of this equation is:

$$\begin{aligned} -3a_3^2 + a_1^3 a_3 + 3a_1^2 a_4 &= -3b^2 + m^3 b + 3m^2\left(\frac{m^4}{48} - \frac{bm}{2} + f\right) \\ &= -3b^2 - \frac{m^3}{2}b + m^2\left(\frac{m^4}{16} + 3f\right) \end{aligned}$$

This is a quadratic equation in b, so:

- For any elliptic curve with short Weierstrass coefficients (f, g), and any $m \in k$, there exists an unobstructed equation with for (f, g) with $a_1 = m$.
- Away from the locus where:

$$m^2(m^4 + 36f) = 0$$

there are exactly 2 unobstructed equations for each choice of f, g, m.

Overall, the map $\mathcal{W}^{un} \to k \times \mathcal{W}$ is a double cover branched along a sextic (if we give f, m the appropriate weights).

Next, we want to understand the fibers of $\mathcal{C}^{un} \to \mathcal{W}^{un}$.

Now, let $(a_1, a_3, a_4, a_6) \in \mathcal{W}^{un}$, and let $a = \frac{a_4}{2} + \frac{\sqrt{4a_4^3 + 27a_6^2}}{6\sqrt{3}}$. Then either a is a cube, in which case $x^3 + a_4.x + a_6$ splits completely and we are in a degenerate situation where the elliptic curve has k-rational points, or else $x^3 + a_4 x + a_6$ is irreducible and splits completely after adjoining a cube root of a. By the previous comment, we can find q, t such that $-3aqt = a_4$ and $-a^2q^3 - at^3 = a_6$. We set $b = \frac{a_3}{-9a}$, $m = a_1$ and $c = -1$ to obtain an element of $\mathcal{C}^{un}$ that maps to (a_1, a_3, a_4, a_6).

Furthermore, for the most part, this lift is essentially unique: as long as $x^3 + a_4x + a_6$ is irreducible, the splitting field k'/k is determined up to isomorphism, so we only need to choose a primitive element A to obtain every other coefficient. We could have chosen a^2 instead of a, but then we would have obtained an element of $\mathcal{C}$ where the roles of x, z have been interchanged. Thus, in the generic case, the fibers contain exactly two elements, unless $a = c$ and $q = t$, in which case the fiber contains a single element.

If $x^3 + a_4x + a_6$ has 3 distinct roots in k, then the associated elliptic curve has three k-rational points whose x-coordinates are the roots of that cubic and whose y-coordinates are 0. They lie in the image of cubics that have a k-rational point, so they do not actually lie in the image of $\mathcal{C}$. We ignore this case for now.

Similarly, if $x^3 + a_4x + a_6$ has 2 distinct roots in k, then the Jacobian has a nontrivial Mordell-Weil group and we ignore these.

If $a_4 = a_6 = 0$, the associated elliptic curve necessarily has a 3-torsion point at $(0, 0)$. We can choose a, c freely and solve for b, m to compute points in the fiber over these points. Note that replacing a, c by a different element in the same coset in $k^\times/k^{\times 3}$ gives the same element in $\mathcal{C}$, so these fibers look like $(k^\times/k^{\times 3})^2/k^\times$, where we are taking the quotient by the kernel of the product map.

This completes the analysis of the horizontal maps.

Next, we remark that $\mathcal{W}^2/k^\times \cong k$, since over a quadratically closed field, the issue of quadratic twists does not come up, so elliptic curves are determined by their j-invariant. Thus $k \times \mathcal{W}/k^\times \cong k \times k$.

The map $\mathcal{W}^{un}/k^\times \to k \times \mathcal{W}/k^\times$ is a double cover of k^2 branched over a sextic, so $\mathcal{W}^{un}/k^\times$ is birational to a K3 surface.

Finally, away from the locus where $a_4 = a_6 = 0$, the map $\mathcal{C}^{un}/k^\times \to \mathcal{W}^{un}/k^\times$ is a bijection, and when $a_4 = a_6 = 0$, the fibers are in bijection with $k^\times/k^{\times 3}$ as

described above.

11.5.1 Parametrizing 3-torsors

We can use these results to construct two different objects that parametrize 3-torsors.

- The space $\mathcal{T}_3 = \{(a, b, c, q, t, m)\} / (k^\times \times k^\times)$ contains a fundamental domain $SL_3(k)$- equivalence classes of equations for 3-torsors. Furthermore it is easy to describe, and it is easy to obtain representatives of each torsor in $\mathcal{T}_3$.

  However, $\mathcal{T}_3$ contains obstructed equations - the space of unobstructed equations is a hypersurface in $\mathcal{T}_3$.

- On the other hand, we can ignore the space of equations altogether and study the family of elliptic curves:

$$y^2 + mxy - 9aby = x^3 - 3aqtx - a^2q^3 - at^3$$

  with $a \in k^\times$ fixed and m, b, q, t varying.

  Each of these elliptic curves has a point of trace zero defined over $k(\sqrt[3]{a})$ with $y = 0$.

In the next chapter, we explain how we can construct objects analogous to the second type of parametrizing space, with no assumptions on the index.

11.6 Singularities on the Jacobian

Let $X \subset \mathbb{P}^2 \times \mathbb{P}^2$ be a bidegree (3,3) hypersurface. Then X is Calabi-Yau, and the projection onto either factor endows X with the structure of a genus one fibration.

Let us further assume[3] that X is given by an equation of the form:

$$ax^3 + by^3 + cz^3 + qy^2z + txy^2 + mxyz = 0$$

Let $J \to \mathbb{P}^2$ be the Jacobian fibration. A computation using **??** shows that over points in $V(a) \cap V(m)$ and $V(c) \cap V(m)$, the coefficients f, g vanish to order $(4, 6)$.

A quick way of verifying this is by checking that over $V(a)$ and $V(c)$, the equation of the Jacobian is:

$$y^2 + mxy = x^3$$

The short Weierstrass coefficients of this curve vanish to order $(4, 6)$ over $m = 0$.

We can characterize this subset of the base geometrically:

- The curves $V(a)$ and $V(c)$ are the branch locus of the cover $S \to \mathbb{P}^2$ that splits X.
- The coefficient m is the slope of the line through the trace zero point and its conjugates.

Thus, if we start with the data of (f, g) and the trace zero point, we can in principle find m, a, c, which means we know where to look for the codimension 2 singularities. Furthermore, we can count them - there are $2 \times [\omega_B].[\omega_B] = 18$ in those intersections, where $[\omega_B].[\omega_B]$ is the self-intersection number of the canonical bundle of the base.[4]

This means we can avoid having to use the full Jacobian formula altogether, and still obtain detailed information about codimension 2 singularities as in [50].

[3] We can always obtain an equation of desired form with coefficients in a quadratic extension of K, but it is not clear how to generalize that result even if we have a DVR.

[4] Since we are assuming the base is $\mathbb{P}^2$ in the example, the self-intersection number is 9.

Chapter 12

Torsors of Arbitrary Index

Finally, we discuss torsors of arbitrary index. The ideas in the chapter are part of ongoing work, and should not be read as a "finished product".

We could, in theory, continue our analysis of torsors by working degree by degree. The results we have for 2-torsors and 3-torsors should allow us to say interesting things about 4-torsors and 6-torsors without doing any new computations:

- Every Galois field extension of degree 4 has an intermediate extension of degree 2. Thus, the problem of classifying points in the kernel of the trace map can be broken down into analyzing two quadratic trace maps.

  It may also be useful to use a degree 2 model for the Jacobian - at the moment, it is not clear which of these tools will prove to be most useful.

- By the Chinese remainder theorem, every torsor of index 6 can be decomposed into a sum of a 2-torsor and a 3-torsor in $WC(E/k)$. Thus, we can parametrize *all* 6-torsors using $\mathcal{T}_2 \times_{\mathcal{W}} \mathcal{T}_3$.

However, the degree-by-degree approach introduces new complications at each

stage:

- For torsors of index 4 and higher, we have to deal with torsors that acquire a point over a non-Galois extensions. Furthermore, even when we have Galois extensions, the structure of the Galois group will not be determined by $|G|$.
- To study torsors of index 5 and higher, the equations are no longer complete intersections, so even choosing an equation for these curves becomes a challenge.
- There *is* a formula for the Jacobian of a genus one curve of arbitrary index[23], although it becomes too complicated to write out once we get to torsors of index 5.

We will change perspective and ask a new question:

Can we find a sharp bound on the index of genus one fibered Calabi-Yau 3-folds?

Such a bound is expected to exist - if we restrict the question to fibrations which are either in Ш *or* arise from the quotient torsor construction, then the results of [32], together with 9.4 show that the index can't get arbitrarily large for torsors of Calabi-Yau 3-folds.

In [15], Căldăraru proves an interesting conditional result: if we can find a Calabi-Yau torsor of index exceeding 6, that would imply the existence of derived equivalent threefolds which are not birational. He points out that there are no known examples whose index is that high.

Now, there's an easy explanation for this - torsors of index exceeding 6 are never complete intersections, so they would not have appeared in the CICY database, and the Jacobian formula for these torsors is not quite ready for use in F-theory.

However, it would also not be surprising if the bound on the index of torsors matches the bound on the order of torsion points. In the rest of this chapter, we

explain how one might go about proving this bound using the theory of trace zero points.

It is worth mentioning that there may be a different approach using mirror symmetry, although much more work would have to be done in order to prove the bound that way. The conjecture predicts that for a mirror pair (X, X'), the Brauer group of X should be isomorphic to the torsion in $Pic(X')$ and vice versa. The idea is to think of $Br(X)$ as the group parametrizing torsors and to show that torsion in $Pic(X')$ comes from Mordell-Weil torsion if X' is elliptically fibered.

See [10], [54] for details.

12.1 Strategy

Instead of trying to classify torsors, we will focus on understanding trace zero points. It is much easier to classify pairs consisting of an elliptic curve and a trace zero point than it is to classify pairs consisting of an elliptic curve and a torsor. Furthermore, in situations where we are able to work with explicit equations for torsors, we were able to show that all of the important information is encoded in the trace zero points.

- For 2-torsors, trace zero points are easily characterized. Furthermore, the coordinates of the trace 0 point encode the equation for the torsor, and from the trace 0 point, we can easily obtain Galois cohomology classes representing the torsor in $WC(E/K)$ and in $Br(E)$.

- For 3-torsors, the situation is a little more complicated, because we had to worry about "obstructed equations". However, every pair (E, P) determines an unobstructed equation for the Jacobian, and the equation of the torsor

can be recovered from the coordinates of P after having computed the unobstructed equation.

In both cases, we were able to construct a space that simultaneously parametrized both torsors and trace 0 points, and contained a fundamental domain for the former.

- For 2-torsors, we had the variety:

$$\left\{(a,c,d,e) \in k^4\right\} / ((a,c,d,e) \sim (t^{-2}a, c, td, t^2 e))$$

which parametrized equations for 2-torsors. Each point on this variety determines a pair (E,p), where E is the Jacobian of the 2-torsor and p is the point with coordinates $x = c, y = \sqrt{a}d$.

- For 3-torsors, the story is more complicated because we have to worry about obstructed equations. However, we can still construct spaces that simultaneously parametrize pairs consisting of an elliptic curve and a torsor or an elliptic curve and a point of trace 0.

We had a space $\mathcal{T}_3$, whose elements are $k^\times \times k^\times$-orbits of 6-tuples (a,b,c,q,t,m).

Each such orbit determines a genus one curve:

$$ax^3 + by^3 + cz^3 + qy^2z + txy^2 + mxyz = 0$$

Inside $\mathcal{T}_3$, we have a hypersurface parametrizing unobstructed equations.

If E is the Jacobian of C, then E has an equation:

$$y^2 + mxy - 9abcy = x^3 + 3acqtx + a^2cq^3 - ac^2t^3$$

and E has the trace zero point $(0, q\sqrt[3]{a} + t\sqrt[3]{a^2})$ which allows us to invert the Jacobian map.

12.2 Trace Zero Variety

Going forward, we will fix a (finite, Galois) field extension L/K and describe a variety whose points parametrize pairs (E, p) with E an elliptic curve over K and p a point in the kernel of the trace map. We can think of the spaces $\mathcal{T}_2, \mathcal{T}_3$ as disjoint unions of $\mathcal{T}_{L/K}$ as L ranges over all quadratic,cubic extensions, respectively.

If we're lucky, we may be able to find a way to recover equations for torsors from points on this space, as we did with 2-torsors and 3-torsors.

Even if we can't achieve that, we hope that understanding $\mathcal{T}_{L/K}$ might allow us to mimic some of the arguments used to understand Calabi-Yau 3-folds with prescribed torsion:

- If we can show that $\mathcal{T}_{L/K}$ does not have K-points, that would mean there are no genus one curves C/K that acquire a new point over L.
- If we can find a nice compactification of $\mathcal{T}_{L/K}$ (or of a quotient of $\mathcal{T}_{L/K}$), we may be able to make more precise predictions regarding the singularities one should expect to find on the Jacobian of a torsor of high index.

We should explain why $\mathcal{T}_{L/K}(K) = \emptyset$ is even a possibility:

- The construction of $\mathcal{T}_{L/K}$ mimics the algebraic construction of modular curves B.2.1. In fact, we will see that we can embed the modular curve $X_1(n)$, where $n = [L : K]$, into $\mathcal{T}_{L/K}$.

- Whenever we have a bound on torsion, that effectively tells us that $X_1(n)$ has no K-points. For example, if K is a purely transcendental extension of $\mathbb{C}$, then $X_1(n)$ has no K-points[1] for all $n > 12$.

- If $n = 2$ (or $n = 3$ and K is quadratically closed), then we have maps $X_1(n) \to \mathcal{T}_{L/K}$ and $\mathcal{T}_{L/K} \to X_1(n)$ such that the composition is the identity on $X_1(n)$.

  Now, suppose we have maps with those properties for all n. Then $\mathcal{T}_{L/K}(K) \neq \emptyset$ would imply $X_1(n)(K) \neq \emptyset$. But we know $X_1(n)(K) = \emptyset$ for sufficiently large n, so $\mathcal{T}_{L/K}(K) = \emptyset$ for sufficiently large L.

- It's possible that those maps no longer exist if n is large. In that case, if we can show that $\mathcal{T}_{L/K}$ has a compactification which is not a special manifold[2], that may be enough to bound the index of Calabi-Yau torsors.

12.2.1 Construction

We fix the following notation:

- L/K is a Galois extension of finite degree. We write G for the Galois group. We also fix a basis $e_1, \ldots, e_n$ of L/K.

- Let $\mathcal{E} \to \mathcal{W}$ be the $\mathcal{W}$-scheme:

$$\left\{((p,q),(f,g)) : q^2 = p^3 + fp + g\right\}$$

  We think of points on $\mathcal{E}$ as representing pairs (E, P) with E/K an elliptic curve and $P \in E(K)$ a non-identity point.

[1] Of course, one has to rule out points with values in $\mathbb{C}$.
[2] In the sense of Campana, see e.g. [16]

- Let $\mathcal{E}_{L/K} \to \mathcal{W}$ be the $\mathcal{W}$-scheme:

$$\mathcal{E}_{L/K} = \left\{((\xi_1, \xi_2), (f, g)) \in L^2 \times \mathcal{W} : \xi_2^2 = \xi_1^3 + f\xi_1 + g\right\}$$

  We have an inclusion $\mathcal{E} \to \mathcal{E}_{L/K}$ of $\mathcal{W}$ schemes. We think of $\mathcal{E}_{L/K}$ as parametrizing pairs (E, P) with E/K an elliptic curve and $P \in E(L)$ a non-identity point.

We write $\overline{\mathcal{E}}$ (resp. $\overline{\mathcal{E}_{L/K}}$) for the disjoint union $\mathcal{E} \sqcup \mathcal{W}$ (resp. $\mathcal{E}_{L/K} \sqcup \mathcal{W}$). We write $\partial\mathcal{E}_{L/K}$ to denote the copy of $\mathcal{W}$ in $\overline{\mathcal{E}_{L/K}} \backslash \mathcal{W}$.

Now $\overline{\mathcal{E}_{L/K}}$ is a group scheme over $\mathcal{W}$: if we have two points lying over the same point in $\mathcal{W}$, then they represent points on a common elliptic curve so we can add them to obtain a new point over the same elliptic curve. The map $\mathcal{W} \to \partial\overline{\mathcal{E}_{L/K}}$ is the zero section. Furthermore, we have an action of G on $\mathcal{E}_{L/K}$ as a $\mathcal{W}$-scheme. Thus, we can define the trace map on the whole family by defining a morphism of $\mathcal{W}$-schemes $\overline{\mathcal{E}_{L/K}} \to \mathcal{E}$.

We define $\mathcal{T}_{L/K}$ as the preimage of $\partial\mathcal{E}$ in $\mathcal{E}_{L/K}$.

- From the construction, it's clear that $\mathcal{T}_{L/K}$ is a sub-$\mathcal{W}$-scheme of $\mathcal{E}_{L/K}$.
- The action of G on $\mathcal{E}_{L/K}$ restricts to an action on $\mathcal{T}_{L/K}$.
- The $\mathcal{W}$-scheme of G-fixed points of $\mathcal{T}_{L/K}$ parametrizes pairs (E, p), where $p \in E(K)$ is in the kernel of the multiplication by n-map.

Thus, $\mathcal{T}_{L/K}$ contains something that looks like a "thickened" modular curve.

To make this precise, write $\mathcal{E}^*$ for the subset of $\mathcal{E}$ consisting of elements $((p, q), (f, g))$ with $q \neq 0$. Abstractly, this is the open set parametrizing pairs (E, p) where $p \in E(k)$ is a point of order greater than 2.

This space is isomorphic to the space of coefficients (a_1, a_2, a_3) of elliptic curves:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2$$

- If we have an element of $\mathcal{E}^*$, we do a change of variable so that (p, q) is at the origin and the tangent has equation $y = 0$. This gives us a new equation with $a_4 = a_6 = 0$.
- If we start with a triple (a_1, a_2, a_3), we can do a change of variable to obtain a short Weierstrass equation. The point $(0, 0)$ goes to a pair (p, q) that satisfy $q^2 = p^3 + fp + g$, giving us an element of $\mathcal{E}^*$.

Now, to construct the modular curve $X_1(n)$, one takes the quotient of (a_1, a_2, a_3) space by the usual action of $k^\times$ on the space of Weierstrass equations. For each triple with $a_2, a_3 \neq 0$[3], there is a unique representative in the $k^\times$ orbit with $a_2 = a_3$.

The modular curve $X_1(n)$ is obtained by computing multiples of $(0, 0)$ on the curve:

$$y^2 + (1 - u)xy - vy = x^3 - vx^2$$

and setting $n(0, 0) = 0$ to obtain a polynomial in (u, v) whose vanishing set is $X_1(n)$.

The point is that the image of $\mathcal{T}_{L/K}$ under the map $\mathcal{E}^* \to \{(a_1, a_2, a_3)\}$ coincides with the "cone over $X_1(n)$" in the codomain.

Thus, we have a map $X_1(n) \to \mathcal{T}_{L/K}$.

[3]If $a_2 = 0$, we have a 3-torsion point at $(0, 0)$. If $a_3 = 0$, the curve is singular.

12.2.2 Maps in the other direction

For 2-torsors and 3-torsors, we also have a map going in the other direction, although it wasn't described that way in the relevant chapters.

- Let (a, c, d, e) be a class in $\mathcal{T}_2$, and let C' be the genus one curve:

$$C' : \quad w^2 = au^4 + cu^2 + e$$

  The Jacobian of C is:

$$E' : \quad y^2 = x^3 + cx^2 - 4aex - 4ace$$

  Setting $x = -c$ yields 0 on the right hand side, so the Jacobian of C has a 2-torsion point. Furthermore, this 2-torsion point coincides with the trace zero point on E'.

- Let (a, b, c, q, t, m) be a class in $\mathcal{T}_2$ and let C' be the genus one curve:

$$C' : \quad ax^3 + by^3 + cz^3 + mxyz = 0$$

  The Jacobian of C is:

$$E' : \quad y^2 + mxy - 9abcy = x^3$$

  The associated trace zero point is $(0, 0)$, which in this case is a 3-torsion point.

In both cases, this gives us a map $\mathcal{T}_d \to X_1(d)$ with the property that $X_1(d) \to \mathcal{T}_d \to X_1(d)$ is the identity.

Note that this is *not* a map of $\mathcal{W}$-schemes, which is the point: we would like to use this to say that if one can find a torsor of high index, then somewhere out there one can find an elliptic curve with equally high torsion.

If we can find such a map, then we can use the known bounds on Mordell-Weil torsion to bound the index of torsors.

12.3 Functorial Interpretation

We may be able to obtain the map $\mathcal{T}_{L/K} \to X_1(n)$ using the formalism of the restriction of scalars functor.

We start with by reviewing basic properties of restriction of scalars.

- Let X/L be a variety. The restriction of scalars of X, if it exists, is a K-variety $\mathcal{X}$ that is characterized by the existence of bijections:

$$X(R \otimes_K L) \qquad \leftrightarrow \qquad \mathcal{X}(R)$$

  for every K-algebra R. In other words, the restriction of scalars is a K-variety that represents the functor of points of X.

- Let X/L be a variety and suppose the restriction of scalars $\mathcal{X}/K$ exists. Then:

$$\mathcal{X}_L \cong \prod_{\sigma \in G} \sigma(X)$$

- Let A/L be a prinicipally polarized abelian variety over L. Then the restriction of scalars $\mathcal{A}/K$ exists, and $\mathcal{A}$ is a prinicipally polarized abelian variety over K.

Now, let E/K be an elliptic curve. Let E_L be the base extension to L, $\mathcal{E}$ the restriction of scalars and $\mathcal{E}_L$ the base extension of the restriction of scalars.

Since E is defined over K, $E_L = \sigma(E_L)$ for all $\sigma \in G$. Thus:

$$\mathcal{E}_L \cong \prod_{\sigma \in G} E_L$$

If E/L is an elliptic curve which is not defined over K, then there exists $\sigma \in G$ such that $E \ncong \sigma(E)$ as varieties over L.

However, the restriction of scalars of E is isomorphic to the restriction of scalars of $\sigma(E)$.

- Base extension and restriction of scalars are adjoints; thus, we can use the unit and counit of the adjunction to obtain well behaved maps $E(k) \to \mathcal{E}(k)$ and $\mathcal{E}_L(L) \to E(L)$.

  Note that $E(k) \to \mathcal{E}(k)$ is an embedding and $\mathcal{E}_L(L) \to E(L)$ is a projection.

- Let E/K be an elliptic curve and $\mathcal{E}, \mathcal{E}_L$ as above. Since $\mathcal{E}_L(L) \cong \prod_{\sigma \in G} E(L)$, we have two embeddings $E(L) \to \mathcal{E}_L$: we can embed a point via the diagonal embedding or via the map $P \mapsto (\sigma(P))_{\sigma \in G}$.

- We can use the group scheme structure on E_L to define a map $\prod_{\sigma \in G} E(L) \to E(L)$ that takes a $|G|$-tuple to the sum of the entires.

- We can compose either of the two maps $E(L) \to \mathcal{E}(L)$ with the map $\mathcal{E}(L) \to E(L)$ to obtain an endomorphism of E. The endomorphism will either be multiplication by $|G|$ or the trace map.

The idea would be to show that the maps $\mathcal{E}(L) \to E(L)$ that come from the adjunction give us the desired map $\mathcal{T}_{L/K} \to X_1(n)$ by showing they take points in the kernel of the trace map to points in the kernel of the multiplication by n map.

Part IV

Appendices

Appendix A

du Val Singularities

Let k be an algebraically closed field, R a k-algebra and assume that R is a discrete valuation ring with residue field isomorphic to k.

Suppose we have a Weierstrass equation:

$$y^2 = x^3 + fx + g$$

with $f, g \in R$, $4f^3 + 27g^2 \neq 0$ and either $\nu(f) < 4$ or $\nu(g) < 6$. The associated[1] R-scheme is not necessarily smooth, but it has *at worst du Val singularities*. The goal of this chapter is to explain what that means.

There are many ways of defining/characterizing du Val singularities - fifteen can be found in [22].

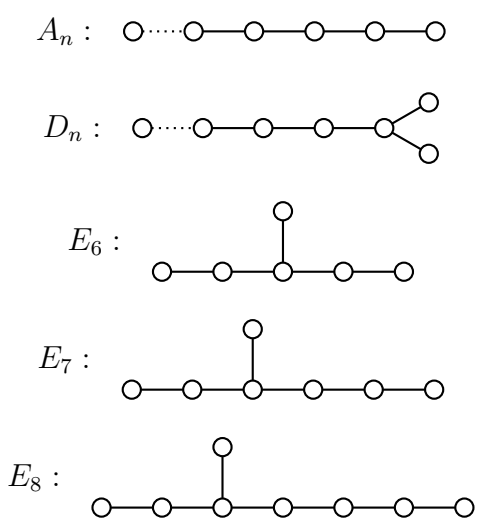
We proceed algebraically. An isolated point on a surface is $X = \mathrm{Spec} k[[x, y, z]]/f(x, y, z)$ for some polynomial f. We say that X is an isolated singularity if $k[[x, y, z]]/f(x, y, z)$ is not a regular ring.

We say that an isolated singularity on a surface is a du Val singularity if it is isomorphic to $\mathrm{Spec} k[[x, y, z]]/f(x, y, z)$, where $f(x, y, z)$ is one of the following:

[1] That is, the R-curve in $\mathbb{P}^2_R$ cut out by the homogenization of the Weierstrass equation.

$$(A_n, n \geq 1): \quad x^2 + y^2 + z^{n+1} \tag{A.1}$$
$$(D_n, n \geq 4): \quad x^2 + y^2 z + z^{n-1} \tag{A.2}$$
$$(E_6): \quad x^2 + y^3 + z^4 \tag{A.3}$$
$$(E_7): \quad x^2 + y^3 + yz^3 \tag{A.4}$$
$$(E_8): \quad x^2 + y^2 + z^5 \tag{A.5}$$

For each of these singularities, there is an associated Dynkin diagram with the same name:



The relationship between the singularity and the Dynkin diagram can be explained in several ways.

- For each du Val singularity, there is a unique minimal, smooth resolution $\tilde{S} \to S$. The fiber over the singular point is a connected union of $\mathbb{P}^1$'s.

  If we construct a graph whose vertices correspond to $\mathbb{P}^1$'s in the resolved fiber and with edges between $\mathbb{P}^1$'s that intersect, we obtain the Dynkin diagram with the same name.

- There is a different approach using representation theory. The starting point is the observation that the du Val singularities can be realized as $\mathbb{C}^2/G$, where G is a finite subgroup[2] of $SL_2(\mathbb{C})$.

  The inclusion $\rho : G \to SL_2(\mathbb{C})$ is a representation of G. We construct a (directed, multi-) graph whose vertex set is the set of irreducible representations of G.

  We draw k edges $\rho_i \to \rho_j$ if $\rho_i \otimes \rho$ contains k copies of ρ_j.

  It turns out that for any pair of irreps ρ_i, ρ_j, we either have no arrows between ρ_i, ρ_j or exactly one arrow going in each direction.[3]

  The graph obtained is an affine Dynkin diagram - that is, it has one more extra vertex than the previous graph, which corresponds to the trivial representation.

This relationship is at the heart of the McKay correspondence, see e.g. [28] or [14].

This correspondence is key to the physics-algebraic geometry dictionary:

- Every minimal elliptic fibration has at worst du Val singularities over codimension 1 components of the discriminant.

- Every du Val singularity has an associated Dynkin diagram.

- Every Dynkin diagram has an associated Lie algebra, hence a simply connected nonabelian Lie group.

[2]Precisely, G is cyclic if we want an A_n singularity, G is a binary dihedral group if we want a D_n singularity and G is the binary tetrahedral/octahedral/icosahedral group if we want E_6, E_7, E_8, respectively.

[3]Note that this fails if we change G or replace ρ by another representation.

Thus, there is a natural way of associated Lie groups to elliptic fibrations. While this construction may seem arbitrary at first sight, the results in [31], [30] show that the representation theory of that group is related to codimension 2 singularities on the fibration in ways that one would not expect.

Appendix B

Modular Curves

In this appendix, we review classical results on modular curves. Since this material is available elsewhere, we will only discuss the modular curves $X(1)$ and $X_1(n)$ for $n > 1$.

B.1 The Modular Curve $X(1)$

The modular curve $X(1)$ classifies isomorphism classes of elliptic curves over $\mathbb{C}$. We already obtained an algebraic description of $X(1)$ in 4:

$$X(1) \quad \leftrightarrow \quad \left\{(f,g) \in \mathbb{C}^2 : 4f^3 + 27g^2 \neq 0\right\} / \mathbb{C}^\times$$

where $\mathbb{C}^\times$ acts on that space by $t \cdot (f,g) = (t^4 f, t^6 g)$.

If $fg \neq 0$, the stabilizer of (f,g) under that action is $\{\pm 1\}$. If $g = 0$, the stabilizer is the group of 4th roots of unity and if $f = 0$, the stabilizer is the group of 6th roots of unity. The j-map:

$$\mathcal{W}_{\mathbb{C}} \to \mathbb{C} \qquad (f,g) \mapsto 1728 \frac{4f^3}{4f^3 + 27g^2}$$

is constant on $\mathbb{C}^\times$ orbits, and gives us a bijection between points on $X(1)$ and points on $\mathbb{C}$.

There is a standard compactification of $X(1)$, denoted $Y(1)$, obtained by allowing nodal genus one curves in the moduli space. This adds a single point to $X(1)$. We identify the compactified modular curve with $\mathbb{P}^1_{\mathbb{C}}$, and think of nodal elliptic curves as curves with j-invariant ∞.

We can also construct the modular curves $X(1), Y(1)$ using a completely different toolkit. The details we just mentioned can also be observed from this perspective.

B.1.1 Uniformization

Let (C, p_0) be a pair consisting of a Riemann surface of genus one, and a point p_0 on C.

- Let γ_1, γ_2 be a pair of cycles that generate $H_1(C, \mathbb{Z})$.
- For each $p \in C$, choose a path γ_p from p to p_0.
- Finally, choose an invariant differential ω on C.

Let $\tau_i = \int_{\gamma_i} \omega$ for $i = 1, 2$ and let $\Lambda \subset \mathbb{C}$ be the free abelian group generated by τ_1, τ_2.

We define a map:

$$C \to \mathbb{C}/\Lambda \qquad p \mapsto \int_{\gamma_p} \omega + \Lambda$$

Note that this map does not depend on the choice of path γ_p, since any two paths differ by an element of $H_1(C, \mathbb{Z})$.

In fact this map is an isomorphism. Thus, if we know Λ, then we essentially know C. Furthermore, the only choice we had was in the choice of ω, and any two choices are scalar multiples of each other. As a result, the lattice obtained by using a different choice of ω is simply a scalar multiple of Λ.

We say that two lattices are homothetic if there exists $t \in \mathbb{C}^\times$ such that $\Lambda = c\Lambda'$.

Thus, we can think of $X(1)$ as classifying lattices up to homothety.

Now, lattices in $\mathbb{C}$ are parametrized by a subset of $\mathbb{C}^2$, where each pair (τ_1, τ_2) determines the lattice $\Lambda = \tau_1\mathbb{Z} \oplus \tau_2\mathbb{Z}$.

However, this space is much too big.

- First, there are lots of pairs that define "degenerate" lattices. We assume $\tau_1\tau_2 \neq 0$ throughout, but of course there are other pairs that do not define a lattice. We discuss the compactification of the space afterwards, and for now will make assumptions as needed.

- Second, we only care about lattices up to scaling. We can reduce to a single copy of $\mathbb{C}^\times$ by rescaling the basis vectors so that one of the generators is 1, e.g. $(1, \frac{\tau_2}{\tau_1})$ instead of τ_1, τ_2.

- The lattice generated by τ_1, τ_2 is the same as the lattice generated by τ_2, τ_1.

  Now, if τ_1, τ_2 are $\mathbb{R}$-linearly independent in $\mathbb{C}$, then exactly one of $\frac{\tau_1}{\tau_2}, \frac{\tau_2}{\tau_1}$ is in the upper half plane and the other is in the lower half plane.

Thus, we can take the upper half plane:

$$\mathcal{H} = \{z \in \mathbb{C} : \text{Re}\,(z) > 0\}$$

as a parameter space, with each point $\tau \in \mathcal{H}$ representing the homothety class of the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$.

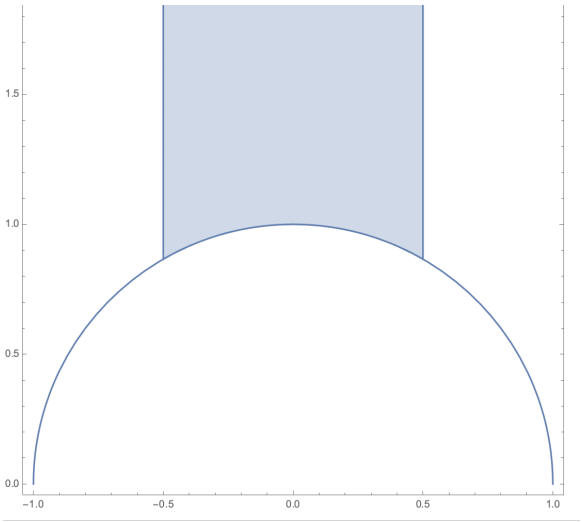


Figure B.1: *Fundamental domain for the moduli space of elliptic curves.*

Finally, we note that there are lots of points in $\mathcal{H}$ that determine the same lattice via the rule above - for example, the lattice generated by $\{\tau + 1, 1\}$ is the same as the lattice generated by $\{\tau, 1\}$.

Two points in $\mathcal{H}$ determine the same homothety class of lattices if and only if they are in the same $SL_2(\mathbb{Z})$ orbit, where $SL_2(\mathbb{Z})$ acts on $\mathcal{H}$ by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

Thus, we can identify $X(1)$ with the quotient $SL_2(\mathbb{Z})\backslash\mathcal{H}$.

In this section we use the letters S, T to denote the generators of $SL_2(\mathbb{Z})$:

$$S = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

- The class of lattices determined by $\tau = i$ corresponds to the class of elliptic curves with $g = 0$.

- The class of lattices determined by $\tau = e^{2\pi i/3}$ corresponds to the class of

elliptic curves with $f = 0$.

- We have an analog of the j-map that gives us an identification of the quotient $SL_2(\mathbb{Z})\backslash\mathcal{H}$ with $\mathbb{C}$. The j-invariant in this case is a modular form.

To construct the compactification $Y(1)$ analytically, we use the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

The fractional linear transformation $z \mapsto \frac{az+b}{cz+d}$ takes ∞ to $\frac{a}{c}$. One can show that $SL_2(\mathbb{Z}) \cdot \infty = \mathbb{Q} \cup \{\infty\}$, so we've added a single orbit to the parameter space.

B.2 $X_1(n)$

Let $n > 1$. The modular curve $X_1(n)$ classifies pairs (E, p), where E is an elliptic curve and p is a point of order n, up to isomorphism.[1]

B.2.1 Algebraic Constructions

If $n = 2, 3$, we can construct $X_1(n)$ algebraically as a quotient.

- If $n = 2$, we can find an equation for E as:

$$y^2 = x(x^2 + ax + b)$$

with the 2-torsion point at $(0, 0)$.

This equation is determined by the pair (a, b), and two pairs $(a, b), (a', b')$ defined isomorphic elliptic curves if and only if there exists t such that $t^2 a = a', t^4 b = b'$. The equation is singular if and only if $b^2(a^2 - 4b) = 0$.

[1] Here, an isomorphism of pairs $(E, p) \to (E', p')$ is an isomorphism of the underlying curves that takes the origin on E to the origin on E' and that takes p to p'.

- If $n = 3$, we can find an equation for C as:

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

  with the 3-torsion point at $(0, 0)$.

  This equation is determined by the pair (a, b), and two pairs $(a, b), (a', b')$ defined isomorphic elliptic curves if and only if there exists t such that $ta = a', t^3 b = b'$.

For $n \geq 4$, there is a well-known construction for $X_1(n)$ as a plane curve.

If $((E, p_0), p)$ is a pair consisting of an elliptic curve and a point p of order exceeding 3, there is a unique equation for E of the form:

$$y^2 + (1 - u)xy - vx^2 = x^3 - vx^2$$

with the point p at $(0, 0)$.

We can treat this as an elliptic curve over $k(u, v)$, and compute multiples of p over this field. For example, we have:

$$2(0, 0) = (v, uv) \qquad 3(0, 0) = (u, v - u)$$

This allows us to find polynomials $\phi_n(u, v)$ whose vanishing encodes the fact that $(0, 0)$ is a point of order n.

We can obtain plane curves $X_1(n)$ in the (u, v)-plane by setting $\phi_n(u, v) = 0$. Note that this construction also gives us a model for the universal elliptic curve with an n-torsion point as an elliptic surface over $X_1(n)$.

To obtain the compactified modular curve algebraically, we projectivize the normalization $\tilde{X_1}(n) \to X_1(n)$. As explained in 1.5, the compactification is determined up to isomorphism as soon as we know the function field of $X_1(n)$, which

in turn is determined by $\phi_n(u, v)$.

The universal property of the normalization guarantees that the universal surface $S \to X_1(n)$ factors through the normalization.

B.2.2 Analytic Construction

- Every elliptic curve over $\mathbb{C}$ is isomorphic to $E_\tau = \mathbb{C}/\Lambda_\tau$, where $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z} \subset \mathbb{C}$ is a rank 2 lattice, and $\tau \in \mathcal{H}$.
- Every point of order n on E_τ has the form $\frac{c\tau+d}{n} + \Lambda_\tau$ for some pair of integers c, d satisfying $\gcd(c, d, n) = 1$.

Thus, it suffices to study pairs $(E_\tau, \frac{c\tau+d}{n})$ for $\tau \in \mathcal{H}$ and $c, d \in \mathbb{Z}$ satisfying $\gcd(c, d, n) = 1$. We now need to determine when two pairs $(E_\tau, \frac{c\tau+d}{n}), (E_{\tau'}, \frac{c'\tau'+d'}{n})$ are isomorphic. We will show that the action of $\mathrm{SL}(2, \mathbb{Z})$ on the space of bases of Λ_τ induces an action on the n-torsion points of E_τ.

Let $p \in E_\tau$ a point on the elliptic curve, that we can write uniquely as

$$p : \quad x\tau + y + \Lambda_\tau \text{ for } x, y \in [0, 1)\,. \tag{B.1}$$

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$, we define the action on that point p as

$$\gamma \cdot p = (a\tau + b)x + (c\tau + d)y + \Lambda_\tau\,. \tag{B.2}$$

It's clear that γ induces an automorphism of E_τ as a group, so it necessarily restricts to an automorphism of the n-torsion of E_τ. Thus $\mathrm{SL}(2, \mathbb{Z})$ acts on n-torsion pairs $(E_\tau, \frac{c\tau+d}{n})$. We next show that it acts transitively on such pairs: in other words, for any pair $(E_\tau, p + \Lambda_\tau)$, we can find $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ such that

$\gamma^{-1} \cdot p + \Lambda_\tau = \frac{1}{n} + \Lambda_\tau$. This will show that the moduli space of pairs $(E, p + \Lambda_\tau)$ is isomorphic to $\mathcal{H}/\Gamma_1(n)$, where $\Gamma_1(n)$ is the stabilizer of the pair $(E_\tau, \frac{1}{n} + \Lambda_\tau)$. Let $\frac{c\tau+d}{n} + \Lambda_\tau$ be an arbitrary point of order n. Since $\gcd(c, d, n) = 1$, there exist integers a, b, k such that $ad - bc + kn = 1$. That is equivalent to saying there is a matrix in $\mathrm{SL}(2, \mathbb{Z}_n)$ with entries congruent to γ' with entries as $ad - bc + kn = 1$. The reduction map $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}_n)$ is surjective, so there exists $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ such that $\gamma \cong \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{n}$. Observe now the inverse action of γ on the pair

$$\gamma^{-1} \cdot \left(E_\tau, \frac{c\tau + d}{n} + \Lambda_\tau \right) = \left(E_\tau, \frac{c(d\tau - b) + d(-c\tau + a)}{n} + \Lambda_\tau \right) = \left(E_\tau, \frac{1}{n} + \Lambda_\tau \right) . \tag{B.3}$$

Thus, if we take a larger fundamental domain in $\mathcal{H}$, we do not have to keep track of the specific coefficients c, d for the point of order n. The problem is now reduced to understanding the stabilizer of $(E_\tau, \frac{1}{n} + \Lambda_\tau)$.

Specifically, we want a characterization of those $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ that fix the torsion point

$$\gamma \cdot \frac{1}{n} + \Lambda_\tau = \frac{1}{n} + \Lambda_\tau \, . \tag{B.4}$$

The new basis is given by $a\tau + b, c\tau + d$, and $\frac{1}{n} + \Lambda_\tau$ is being mapped to $\frac{c}{n}\tau + \frac{d}{n} + \Lambda_\tau$. It is clear that $\frac{1}{n}$ is fixed exactly when $\frac{c}{n} \in \mathbb{Z}$ and $\frac{d}{n} \in \frac{1}{n} + \mathbb{Z}$. An illustration of this action on the torus lattice is depicted in Figure B.2 for a chosen order two torsion point. In particular, we need the entries to satisfy

$$c \equiv 0 \pmod{n} \quad \text{and} \quad d \equiv 1 \pmod{n} \, . \tag{B.5}$$

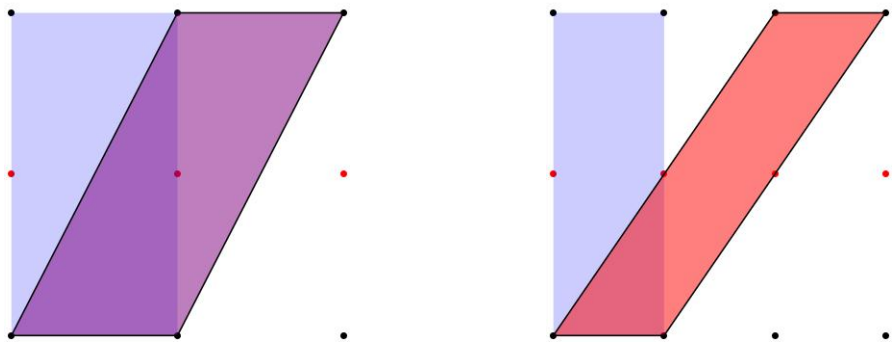


Figure B.2: *Above we have chosen a fundamental domain colored in blue for E_τ the depiction of a 2-torsion point $\frac{\tau}{2}+\Lambda_\tau$ in orange. We act on the basis by the generator T on the left, which translates the point $\frac{\tau}{2}+\Lambda$ to $\frac{\tau+1}{2}+\Lambda$. On the right, we act on the fundamental domain by T^2 in to obtain the pink one while fixing the torsion point.*

It then follows, that the matrices need to satisfy

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \pmod{n} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n}, \tag{B.6}$$

where we have used $ad - bc = 1$ and $c \equiv 0 \pmod{n}$ such that we must have $ad \equiv a \equiv 1 \pmod{n}$.

To summarize, a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ fixes $(E_\tau, \frac{1}{n}+\Lambda_\tau)$ as a torsion pair if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n}.$$

We thus define:

$$\Gamma_1(n) = \left\{ \gamma \in \mathrm{SL}(2,\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}. \tag{B.7}$$

The modular curve is thus identified with $X_1(n) = \Gamma_1(n)\backslash\mathcal{H}$, where $\mathcal{H}$ is the

open upper half plane. This parametrizes pairs (E, p) consisting of a smooth elliptic curve and a point p of order n. The compactified modular curve is $Y_1(n) = \Gamma_1(n)\backslash\mathcal{H}\cup\{\infty\}\cup\mathbb{Q}$. The cusps of the modular curve are the points in $Y_1(n)\backslash X_1(n)$.

For more on the analytic description of modular curves, see [19].

See also the appendix of [35].

Bibliography

[1] Sang Yook An et al. "Jacobians of genus one curves". In: *J. Number Theory* 90.2 (2001), pp. 304–315. ISSN: 0022-314X. DOI: 10.1006/jnth.2000.2632. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1006/jnth.2000.2632.

[2] Lara B. Anderson, James Gray, and Brian Hammack. "Fibrations in non-simply connected Calabi-Yau quotients". In: *J. High Energy Phys.* 8 (2018), 128, front matter+20. ISSN: 1126-6708. DOI: 10.1007/jhep08(2018)128. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/jhep08(2018)128.

[3] Lara B. Anderson et al. "F-theory on quotient threefolds with $(2,0)$ discrete superconformal matter". In: *J. High Energy Phys.* 6 (2018), 098, front matter+76. ISSN: 1126-6708. DOI: 10.1007/jhep06(2018)098. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/jhep06(2018)098.

[4] Lara B. Anderson et al. "F-theory on quotient threefolds with $(2,0)$ discrete superconformal matter". In: *J. High Energy Phys.* 6 (2018), 098, front matter+76. ISSN: 1126-6708.

[5] Jón Kr. Arason, Richard Elman, and Bill Jacob. "On indecomposable vector bundles". In: *Comm. Algebra* 20.5 (1992), pp. 1323–1351. ISSN: 0092-

7872. DOI: 10.1080/00927879208824407. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1080/00927879208824407.

[6] Jón Kr. Arason, Richard Elman, and Bill Jacob. "On the Witt ring of elliptic curves". In: *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*. Vol. 58. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 1995, pp. 1–25.

[7] Michael Artin, Fernando Rodriguez-Villegas, and John Tate. "On the Jacobians of plane cubics". In: *Adv. Math.* 198.1 (2005), pp. 366–382. ISSN: 0001-8708. DOI: 10.1016/j.aim.2005.06.004. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1016/j.aim.2005.06.004.

[8] Paul S. Aspinwall and David R. Morrison. "Non-simply-connected gauge groups and rational points on elliptic curves". In: *J. High Energy Phys.* 7 (1998), Paper 12, 16. ISSN: 1126-6708. DOI: 10.1088/1126-6708/1998/07/012. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1088/1126-6708/1998/07/012.

[9] Paul S. Aspinwall and David R. Morrison. "Stable singularities in string theory". In: *Comm. Math. Phys.* 178.1 (1996). With an appendix by Mark Gross, pp. 115–134. ISSN: 0010-3616. URL: http://projecteuclid.org.proxy.library.ucsb.edu:2048/euclid.cmp/1104286557.

[10] Victor Batyrev and Maximilian Kreuzer. "Integral cohomology and mirror symmetry for Calabi-Yau 3-folds". In: *Mirror symmetry. V*. Vol. 38. AMS/IP Stud. Adv. Math. Amer. Math. Soc., Providence, RI, 2006, pp. 255–270.

[11] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1990,

pp. x+325. ISBN: 3-540-50587-3. DOI: 10.1007/978-3-642-51438-8. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/978-3-642-51438-8.

[12] Vincent Bouchard and Ron Donagi. "On a class of non-simply connected Calabi-Yau 3-folds". In: *Commun. Number Theory Phys.* 2.1 (2008), pp. 1–61. ISSN: 1931-4523. DOI: 10.4310/CNTP.2008.v2.n1.a1. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.4310/CNTP.2008.v2.n1.a1.

[13] Volker Braun and David R. Morrison. "F-theory on genus-one fibrations". In: *J. High Energy Phys.* 8 (2014), 132, front matter+45. ISSN: 1126-6708. DOI: 10.1007/JHEP08(2014)132. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/JHEP08(2014)132.

[14] Tom Bridgeland, Alastair King, and Miles Reid. "The McKay correspondence as an equivalence of derived categories". In: *J. Amer. Math. Soc.* 14.3 (2001), pp. 535–554. ISSN: 0894-0347. DOI: 10.1090/S0894-0347-01-00368-X. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1090/S0894-0347-01-00368-X.

[15] Andrei Căldăraru. "Non-birational Calabi-Yau threefolds that are derived equivalent". In: *Internat. J. Math.* 18.5 (2007), pp. 491–504. ISSN: 0129-167X. DOI: 10.1142/S0129167X07004205. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1142/S0129167X07004205.

[16] Frédéric Campana. "Special manifolds, arithmetic and hyperbolic aspects: a short survey". In: *Rational points, rational curves, and entire holomorphic curves on projective varieties*. Vol. 654. Contemp. Math. Amer. Math. Soc., Providence, RI, 2015, pp. 23–52. DOI: 10.1090/conm/654/13214. URL:

https://doi-org.proxy.library.ucsb.edu:9443/10.1090/conm/654/13214.

[17] Gabriele Di Cerbo and Roberto Svaldi. *Birational boundedness of low dimensional elliptic Calabi-Yau varieties with a section*. 2016. eprint: arXiv:1608.02997.

[18] Steven Dale Cutkosky. *Resolution of singularities*. Vol. 63. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2004, pp. viii+186. ISBN: 0-8218-3555-6. DOI: 10.1090/gsm/063. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1090/gsm/063.

[19] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[20] Igor Dolgachev and Mark Gross. "Elliptic threefolds. I. Ogg-Shafarevich theory". In: *J. Algebraic Geom.* 3.1 (1994), pp. 39–80. ISSN: 1056-3911.

[21] Ron Donagi et al. "Standard models from heterotic M-theory". In: *Adv. Theor. Math. Phys.* 5.1 (2001), pp. 93–137. ISSN: 1095-0761. DOI: 10.4310/ATMP.2001.v5.n1.a4. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.4310/ATMP.2001.v5.n1.a4.

[22] Alan H. Durfee. "Fifteen characterizations of rational double points and simple critical points". In: *Enseign. Math. (2)* 25.1-2 (1979), pp. 131–163. ISSN: 0013-8584.

[23] Tom Fisher. "A formula for the Jacobian of a genus one curve of arbitrary degree". In: *ArXiv e-prints*, arXiv:1510.04327 (Oct. 2015), arXiv:1510.04327. arXiv: 1510.04327 [math.NT].

[24] Tom Fisher. "On some algebras associated to genus one curves". In: *ArXiv e-prints*, arXiv:1707.08330 (July 2017), arXiv:1707.08330. arXiv: 1707.08330 [math.NT].

[25] Yoshio Fujimoto. "On rational elliptic surfaces with multiple fibers". In: *Publ. Res. Inst. Math. Sci.* 26.1 (1990), pp. 1–13. ISSN: 0034-5318. DOI: 10.2977/prims/1195171661. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.2977/prims/1195171661.

[26] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*. Vol. 165. Cambridge Studies in Advanced Mathematics. Second edition of [MR2266528]. Cambridge University Press, Cambridge, 2017, pp. xi+417. ISBN: 978-1-316-60988-0; 978-1-107-15637-1.

[27] Jean Giraud. *Cohomologie non abélienne*. Die Grundlehren der mathematischen Wissenschaften, Band 179. Springer-Verlag, Berlin-New York, 1971, pp. ix+467.

[28] G. Gonzalez-Sprinberg and J.-L. Verdier. "Construction géométrique de la correspondance de McKay". In: *Ann. Sci. École Norm. Sup. (4)* 16.3 (1983), 409–449 (1984). ISSN: 0012-9593. URL: http://www.numdam.org/item?id=ASENS_1983_4_16_3_409_0.

[29] A. Grassi. "Log contractions and equidimensional models of elliptic threefolds". In: *J. Algebraic Geom.* 4.2 (1995), pp. 255–276. ISSN: 1056-3911.

[30] Antonella Grassi and David R. Morrison. "Anomalies and the Euler characteristic of elliptic Calabi-Yau threefolds". In: *Commun. Number Theory Phys.* 6.1 (2012), pp. 51–127. ISSN: 1931-4523. DOI: 10.4310/CNTP.2012.v6.n1.a2. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.4310/CNTP.2012.v6.n1.a2.

[31] Antonella Grassi and David R. Morrison. "Group representations and the Euler characteristic of elliptically fibered Calabi-Yau threefolds". In: *J. Algebraic Geom.* 12.2 (2003), pp. 321–356. ISSN: 1056-3911. DOI: 10.1090/S1056-3911-02-00337-5. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1090/S1056-3911-02-00337-5.

[32] Mark Gross. "A finiteness theorem for elliptic Calabi-Yau threefolds". In: *Duke Math. J.* 74.2 (1994), pp. 271–299. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-94-07414-0. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1215/S0012-7094-94-07414-0.

[33] Alexander Grothendieck. "Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats". In: *Séminaire Bourbaki, Vol. 5*. Soc. Math. France, Paris, 1995, Exp. No. 190, 299–327.

[34] Darrell Haile and Ilseop Han. "On an algebra determined by a quartic curve of genus one". In: *J. Algebra* 313.2 (2007), pp. 811–823. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2006.10.024. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1016/j.jalgebra.2006.10.024.

[35] Nadir Hajouji and Paul-Konstantin Oehlmann. "Modular Curves and Mordell-Weil Torsion in F-theory". In: *JHEP* 04 (2020), p. 103. DOI: 10.1007/JHEP04(2020)103. arXiv: 1910.04095 [hep-th].

[36] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[37] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Vol. 108. Annals of Mathematics Studies. Princeton University Press, Prince-

ton, NJ, 1985, pp. xiv+514. ISBN: 0-691-08349-5; 0-691-08352-5. DOI: 10.1515/9781400881710. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1515/9781400881710.

[38] Sheldon Katz et al. "Tate's algorithm and F-theory". In: *J. High Energy Phys.* 8 (2011), pp. 094, 28. ISSN: 1126-6708. DOI: 10.1007/JHEP08(2011)094. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/JHEP08(2011)094.

[39] Denis Klevers et al. "Exotic matter on singular divisors in F-theory". In: *J. High Energy Phys.* 11 (2017), 124, front matter + 70. ISSN: 1126-6708. DOI: 10.1007/jhep11(2017)124. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/jhep11(2017)124.

[40] János Kollár. *Severi-Brauer varieties; a geometric treatment*. 2016. eprint: arXiv:1606.04368.

[41] János Kollár, Yoichi Miyaoka, and Shigefumi Mori. "Rational connectedness and boundedness of Fano manifolds". In: *J. Differential Geom.* 36.3 (1992), pp. 765–779. ISSN: 0022-040X. URL: http://projecteuclid.org.proxy.library.ucsb.edu:2048/euclid.jdg/1214453188.

[42] S. Lang and A. Néron. "Rational points of abelian varieties over function fields". In: *Amer. J. Math.* 81 (1959), pp. 95–118. ISSN: 0002-9327. DOI: 10.2307/2372851. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.2307/2372851.

[43] Robert Lazarsfeld. *Positivity in algebraic geometry. I.* Vol. 48. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Classical setting: line bundles

and linear series. Springer-Verlag, Berlin, 2004, pp. xviii+387. ISBN: 3-540-22533-1. DOI: 10.1007/978-3-642-18808-4. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/978-3-642-18808-4.

[44] Seung-Joo Lee and Timo Weigand. "Swampland bounds on the Abelian gauge sector". In: *Phys. Rev. D* 100.2 (2019), pp. 026015, 10. ISSN: 2470-0010. DOI: 10.1103/physrevd.100.026015. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1103/physrevd.100.026015.

[45] B. Mazur. "Modular curves and the Eisenstein ideal". In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977). With an appendix by Mazur and M. Rapoport, 33–186 (1978). ISSN: 0073-8301. URL: http://www.numdam.org/item?id=PMIHES_1977__47__33_0.

[46] J. S. Milne. *Elliptic curves*. BookSurge Publishers, Charleston, SC, 2006, pp. viii+238. ISBN: 1-4196-5257-5.

[47] Rick Miranda. "Smooth models for elliptic threefolds". In: *The birational geometry of degenerations (Cambridge, Mass., 1981)*. Vol. 29. Progr. Math. Birkhäuser, Boston, Mass., 1983, pp. 85–133.

[48] Rick Miranda. *The basic theory of elliptic surfaces*. Dottorato di Ricerca in Matematica. [Doctorate in Mathematical Research]. ETS Editrice, Pisa, 1989, pp. vi+108.

[49] David R. Morrison and Daniel S. Park. "Tall sections from non-minimal transformations". In: *J. High Energy Phys.* 10 (2016), 033, front matter+15. ISSN: 1126-6708. DOI: 10.1007/JHEP10(2016)033. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/JHEP10(2016)033.

[50] David R. Morrison and Washington Taylor. "Sections, multisections, and $U(1)$ fields in F-theory". In: *J. Singul.* 15 (2016), pp. 126–149. ISSN: 1949-2006.

[51] David R. Morrison and Cumrun Vafa. "Compactifications of F-theory on Calabi-Yau threefolds. I". In: *Nuclear Phys. B* 473.1-2 (1996), pp. 74–92. ISSN: 0550-3213. DOI: 10.1016/0550-3213(96)00242-8. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1016/0550-3213(96)00242-8.

[52] David R. Morrison and Cumrun Vafa. "Compactifications of F-theory on Calabi-Yau threefolds. II". In: *Nuclear Phys. B* 476.3 (1996), pp. 437–469. ISSN: 0550-3213. DOI: 10.1016/0550-3213(96)00369-0. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1016/0550-3213(96)00369-0.

[53] David Mumford and Kalevi Suominen. "Introduction to the theory of moduli". In: *Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer-School in Math.)* 1972, pp. 171–222.

[54] Paul-Konstantin Oehlmann, Jonas Reuter, and Thorsten Schimannek. "Mordell-Weil torsion in the mirror of multi-sections". In: *J. High Energy Phys.* 12 (2016), 031, front matter+26. ISSN: 1126-6708. DOI: 10.1007/JHEP12(2016)031. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/JHEP12(2016)031.

[55] Bjorn Poonen. *Rational points on varieties*. Vol. 186. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2017, pp. xv+337. ISBN: 978-1-4704-3773-2.

[56] Mohammad Sadek. "Counting models of genus one curves". In: *Math. Proc. Cambridge Philos. Soc.* 150.3 (2011), pp. 399–417. ISSN: 0305-0041. DOI: 10.1017/S0305004110000666. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1017/S0305004110000666.

[57] Mohammad Mohammad Sadek. *Models of genus one curves / Mohammad Sadek.* eng. 2010.

[58] Matthias Schütt and Tetsuji Shioda. "Elliptic surfaces". In: *Algebraic geometry in East Asia—Seoul 2008*. Vol. 60. Adv. Stud. Pure Math. Math. Soc. Japan, Tokyo, 2010, pp. 51–160. DOI: 10.2969/aspm/06010051. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.2969/aspm/06010051.

[59] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241. ISBN: 0-387-90424-7.

[60] Tetsuji Shioda. "Elliptic modular surfaces. I, II". In: *Proc. Japan Acad. 45 (1969), 786-790; ibid.* 45 (1969), pp. 833–837. ISSN: 0021-4280. URL: http://projecteuclid.org.proxy.library.ucsb.edu:2048/euclid.pja/1195520594.

[61] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525. ISBN: 0-387-94328-5. DOI: 10.1007/978-1-4612-0851-8. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/978-1-4612-0851-8.

[62] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986, pp. xii+400. ISBN:

0-387-96203-4. DOI: 10.1007/978-1-4757-1920-8. URL: https://doi-org.proxy.library.ucsb.edu:9443/10.1007/978-1-4757-1920-8.

[63] T. M. Weigand. "TASI Lectures on F-theory". In: *arXiv: High Energy Physics - Theory* (2018).