Elliptic Curves & Modular Forms

Properly Reviewing #1

Benedikt Arnarsson

Spring 2020

Intro

This is the first entry to a series of notes on topics which I want to thoroughly review. This one will cover elliptic curves and modular forms.

First, I will review Silverman's,*The Arithmetic of Elliptic Curves* [Sil09]. I will be going through the chapters in the following order:
I and II (briefly review), III (§§1-8), IV (§§1-6), V (§1), VII (§§1-5), VIII (§§1-6), IX (§§1-7), X (§§1-6).

Next, I will cover *modular forms*, using [DS05], [Dei13], [Bum98], [Hid00], and [Ste07]. I will cover the main ideas and introduce why Modularity makes sense. In addition, I want to focus on computational tools and approaches, so I might link my own SAGE code or something.

Then, I will cover more advanced topics related to elliptic curves. Mazur's Theorem will be done following a series of video lectures, with a view toward generalizations to number fields other than $\mathbb{Q}$.

Following that, I will look at Falting's Theorem, main source being [CS86]. I will also cover consequences of what Falting proved, as well as Vojta's proof and other approaches.

Finally, I will prove the Modularity Theorem, main sources being the original articles and [Hid00].

If time allows, I might look at some other advanced topics, like Shimura varieties and automorphic forms (or they might just be covered in a different "Properly Reviewed").

The appendices will cover a range of topics, really anything that is relevant to understanding the ideas properly. Some sections include: Tate's Thesis, Artin Reciprocity, Neron Models, abelian varieties and Jacobians, basic alebraic geometry of curves, and the classical Riemann zeta function.

Contents

1 Silverman, The Arithmetic of Elliptic Curves

The two main theorems which I will focus on here are the Mordell-Weil theorem and Siegel's theorem. In general, this section is also the introduction to all of the concepts which will be used later on. I will use Silverman's book [Sil09] as a reference, but I will use my own twist, mainly incorporating scheme theory and other thoughts I have while reading.

Notation

Ideally, every individual "chapter" will have a notational reminder at its start. I will try to keep everything clear (at least in my mind) and I will explain any notation that is not clear.

K	a perfect field
$\overline{K}$	a fixed algebraic closure of K
$G_{\overline{K}/K}$	the Galois group of $\overline{K}/K$
C	an algebraic curve, and $P \in C$ a point
$\mathcal{O}_C$	the structure sheaf of C
C/K	C is defined over K
$\overline{K}(C)$	the function field of C over $\overline{K}$
$K(C)$	the function field of C over K
$\mathcal{O}_{C,P}$	the local ring of C at P
$\mathfrak{M}_P$	the maximal ideal of $\mathcal{O}_{C,P}$

1.1 III: §§1-8

Recall the definition of a nonsingular (projective) curve (integral, separated, 1-dimensional scheme of finite type).

1.1.1 The Weierstrass Equation

Definition 1.1.1. An irreducible plane curve of deg d has **(geometric) genus**

$$g = \frac{(d-1)(d-2)}{2} - s$$

Where s is the number of singularities (finite by appendix).

Definition 1.1.2. An **elliptic curve** is pair (E, O), where E is a nonsingular curve of genus one (i.e. its defining equation is a cubic polynomial) and $O \in E$ (called the *base point*). The elliptic curve is *defined over* K, written E/K, if E is defined over K and $O \in E(K)$.

Note. Elliptic curves (over $\mathbb{C}$) are Riemann surfaces of genus 1, aka a *torus*, so we know that it is an *abelian variety*. See appendix for details. We will explicitly show the group law instead.

Theorem 1.1.3 (Weierstrass Normal Form)**.** *Let E/K be an elliptic curve.*

(a) There exist functions $x, y \in K(E)$ such that the map

$$\phi : E \to \mathbb{P}^2, \quad \phi = [x, y, 1]$$

*with injective image a curve given by a **Weierstrass equation***

$$C/K : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

satisfying $\phi(O) = [0, 1, 0]$.
*The functions x, y are called the **Weierstrass coordinates** for E.*

(b) Any two Weierstrass equations for E as in (a) are related by a linear change of variables of the form

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t$$

with $u \in K^\times$ and $r, s, t \in K$.

(c) Conversely, every smooth cubic curve given by a Weierstrass equation as in (a) is an elliptic curve defined over K with base point $O = [0, 1, 0]$.

Proof. Looking to the first appendix covering Riemann-Roch...

(a) We look at the vector space $\mathcal{L}(n(O))$ for $n \geq 1$. By the Riemann-Roch theorem for $deg(D) > 2g - 2$, we have

$$dim\mathcal{L}(n(O)) = \ell(n(O)) = deg(n(O)) = n \quad \text{for all} n \geq 1$$

Thus, we can choose $x, y \in K(E)$ such that $\{1, x\}$ is a basis for $\mathcal{L}(2(O))$ and $\{1, x, y\}$ is a basis for $\mathcal{L}(3(O))$. Note that x must have a pole of exact order 2 at O and y must have a pole of exact order 3 at O.

Now we observe that $\ell(6(O)) = 6$, but (by counting poles) it contains 7 functions

$$1, x, y, x^2, xy, y^2, x^3$$

It follows that there is a linear relation

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

with $A_1, ..., A_7 \in K$. Note that $A_6A_7 \neq 0$ by order of poles. So, we have a method of algebraically manipulating this linear relation. We precede as follows.

$$x \mapsto -A_6A_7x, \quad y \mapsto A_6A_7^2y$$

Getting:

$$A_1 - A_2A_6A_7x + A_3A_6A_7^2y + A_4A_6^2A_7^2x^2 - A_5A_6^2A_7^3xy + A_6^3A_7^4y^2 - A_6^3A_7^4x^3$$

Dividing by $A_6^3A_7^4$ to get the form

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

This gives a map $\phi : E \to \mathbb{P}^2$, $\phi = [x, y, 1]$ whose image C lies in the locus described by the Weierstrass equation above. Notice that by properties of algebraic curves that $\phi : E \to C$ is a surjection and smoothness of E implies that it is a morphism, not just a rational map. Further, we have $\phi(O) = [0, 1, 0]$, since y has a higher order pole than x at the points O (so we can divide it out).

The next step is to show that $deg(\phi) = 1$ which is equivalent to showing that $K(E) = K(x, y)$. Consider the map $[x, 1] : E \to \mathbb{P}^1$. Since x has a double pole at O and no other poles, we count degree by ramification to get $deg[x, 1] = 2$, so $[K(E) : K(x)] = 2$. Similarly, $deg[y, 1] = 3$, so $[K(E) : K(y)] = 3$. Therefore, $K(E) : K(x, y)]$ has to divide 3 and 2, so it must equal 1.

Next, we show that C is smooth. Suppose that C is singular. Then, by a proposition I will prove below, there is a rational map $\psi : C \to \mathbb{P}^1$ of degree 1. It follows from composition that $\psi \circ \phi : E \to \mathbb{P}^1$ is a map of degree 1 between smooth curves, so it is an isomorphism. This contradicts the fact that E has genus 1 and $\mathbb{P}^1$ has genus 0. Therefore, C is smooth, so $deg(\phi) = 1$ implies that $\phi : E \to C$ is an isomorphism.

(b) Let x, y and x', y' be two sets of Weierstrass coordinate functions on E. Then, x and x' have poles of order 2 at O, and, similarly, y and y' have poles of order 3 at O. Hence, both $\{1, x\}$ and $\{1, x'\}$ are bases for $\mathcal{L}(2(O))$, and, similarly, both $\{1, x, y\}$ and $\{1, x', y'\}$ are bases for $\mathcal{L}(3(O))$. So, we can find linear relations:

$$x = u_1x' + r \quad \text{and} \quad y = u_2y' + s_2x' + t$$

Since both (x, y) and (x', y') satisfy Weierstrass equations in which the Y^2 and X^3 terms have coefficients 1, we have that $u_1^3 = u_2^2$. Letting $u = u_2/u_1$ and $s = s_2/u^2$ we get

$$x = u^2x' + r', \quad y = u^3y' + su^2 + t'$$

(c) Let E be given by a nonsingular Weierstrass equation. By the Hurwitz genus formula, we have

$$genus(E) = \frac{(d-1)(d-2)}{2} = 1$$

and choosing $O = [0, 1, 0]$ we get that E is an elliptic curve.

Alternatively, the differential

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

has neither zeros nor poles (proven below), so $div(\omega) = 0$. Therefore, Riemann-Roch tells us that

$$2genus(E) - 2 = deg(div(\omega)) = 0$$

so, E has genus one.

□

The following proposition was used above to show smoothness of C.

Proposition 1.1.4. *If a curve C given by a Weierstrass equation is singular, then there exists a rational map $\phi : C \to \mathbb{P}^1$ of degree one, i.e. C is birational to $\mathbb{P}^1$.*

Proof. Making a linear change of variables, we may assume that the singular point is $(x, y) = (0, 0)$. Checking partial derivatives, we see that the Weierstrass equation has the form

$$C : y^2 + a_1xy = x^3 + a_2x^2$$

Then, the rational map

$$C \to \mathbb{P}^1, \quad (x, y) \mapsto [x, y]$$

has degree one, since it has an inverse given by (think "$t = y/x$")

$$\mathbb{P}^1 \to E, \quad [1, t] \mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$$

□

The following result was used for the alternate proof of (c):

Proposition 1.1.5. *Let E be an elliptic curve. Then the invariant differential ω associated to a Weierstrass equation for E is holomorphic and nonvanishing, i.e. $div(\omega) = 0$*

Proof. Let $P = (x_0, y_0) \in E$ and

$$E : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

so

$$\omega = \frac{d(x - x_0)}{F_y(x, y)} = \frac{d(y - y_0)}{F_x(x, y)}$$

Thus P can not be a pole of ω, since otherwise $F_y(P) = F_x(P) = 0$, which would say that P is a singular point of E. The map

$$E \to \mathbb{P}^1, \quad [x, y, 1] \mapsto [x, 1]$$

is of degree 2, so $ord_P(x - x_0) \leq 2$. Note that $ord_P(x - x_0) = 2$ if and only if the quadratic polynomial $F(x_0, y_0)$ has a double root. In other words, either $ord_P(x - x_0) = 1$, or $ord_P(x - x_0)$ and $F_y(x_0, y_0) = 0$. Thus, in both cases we can use [Sil09] (II.4.3, see appendix 1 for details) to compute

$$ord_P(\omega) = ord_P(x - x_0) - ord_P(F_y) - 1 = 0$$

This shows that ω has no poles and zeros of the form (x_0, y_0), so it remains to check what happens at O.

Let t be a uniformizer at O. Since $ord_O(x) = -2$ and $ord_O(y) = -3$ we see that $x = t^{-2}f$ and $y = t^{-3}g$ for functions f, g with no poles or zeros at O. Now

$$\omega = \frac{dx}{F_y(x, y)} = \frac{-2t^{-3}f + t^{-2}f'}{2t^{-3}g + a_1t^{-2}f + a_3}dt = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt$$

By (II.4.3b)[Sil09] we know that f' is regular at O. Hence, *assuming that* $char(K) \neq 2$, the function

$$\frac{-2f + tf'}{2g + a_1tf + a_3t^3}$$

is regular and nonvanishing at O, and thus $ord_O(\omega) = 0$. Finally, if $char(K) = 2$

$$\omega = \frac{dy}{F_x(x, y)} = \frac{-3t^{-4}g + t^{-3}g'}{a_1t^{-3}g - 3t^{-4}f^2 - 2a_2t^{-2}f - a_4}$$

so, similarly, we know that g' is regular at O, and hence $ord_O(\omega) = 0$. □

Finally, a quick corollary is seen from the theorem above:

Corollary 1.1.6. *Let E/K be an elliptic curve with Weierstrass coordinate functions x and y. Then*

$$K(E) = K(x, y) \quad \textit{and} \quad [K(E) : K(x)] = 2$$

We next use the Riemann-Roch theorem to describe a group law on the points of an elliptic curve, and then we will give an explicit description using the Weierstrass equation. We start with a simple lemma that serves to distinguish $\mathbb{P}^1$ from curves of genus one:

Lemma 1.1.7. *Let C be a curve of genus one and let $P, Q \in C$. Then*

$$(P) \sim (Q) \quad \textit{if and only if} \quad P = Q$$

Proof. Suppose $(P) \sim (Q)$ and choose $f \in \overline{K}(C)$ such that $div(f) = (P) - (Q)$. Then, $f \in \mathcal{L}((Q))$, but Riemann-Roch tells us that $\ell((Q)) = 1$, so $f \in \overline{K}$ and $P = Q$. □

Proposition 1.1.8. *Let (E, O) be an elliptic curve.*

(a) For every degree-0 divisor $D \in Div^0(E)$ there exists a unique point $P \in E$ satisfying

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

Define

$$\sigma : Div^0(E) \to E$$

to be the map that sends D to its associated P.

(b) The map σ is surjective

(c) Let $D_1, D_2 \in Div^0(E)$. Then

$$\sigma(D_1) = \sigma(D_2) \quad \textit{if and only if} \quad D_1 \sim D_2$$

Thus σ induces a bijection of sets

$$\sigma : Pic^0(E) \xrightarrow{\sim} E$$

(d) The inverse to σ is the map

$$\kappa : E \xrightarrow{\sim} Pic^0(E), \quad P \mapsto (\overline{(P) - (O)})$$

(e) If E is given by a Weierstrass equation, then the "algebraic" group law induced by $Pic^0(E)$ using σ and the "geometric" group law (described below) are the same

Proof. Look below for details on the explicit group law:

(a) Since E has genus one, the Riemann-Roch theorem says that

$$\ell(D + (O)) = 1$$

Let $f \in \overline{K}(E)$ be a nonzero element of $\mathcal{L}(D + (O))$, so f is a basis for the one-dimensional vector space. Since

$$div(f) \geq -D - (O) \quad \text{and} \quad deg(div(f)) = 0$$

it follows that $div(f) = -D - (O) + (P)$ for some $P \in E$. Hence, $D \sim (P) - (O)$ which gives a point with the desired property.

Next, suppose $P' \in E$ has the same property. Then

$$(P) \sim D + (O) \sim (P')$$

so the above theorem tells us that $P = P'$.

(b) For any $P \in E$ we have that

$$\sigma((P) - (O)) = P$$

(c) Let $D_1, D_2 \in Div^0(E)$, and set $P_i = \sigma(D_i)$. Then from the definition of σ we have

$$(P_1) - (P_2) \sim D_1 - D_2$$

Thus if $P_1 = P_2$ then $D_1 \sim D_2$; and, conversely, if $D_1 \sim D_2$ then $(P_1) \sim (P_2)$ which by the above theorem implies $P_1 = P_2$.

(d) Clear by similar construction as (b)

(e) Let E be given by a Weierstrass equation and let $P, Q \in E$. It suffices to show that

$$\kappa(P + Q) = \kappa(P) + \kappa(Q)$$

Let

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

give the line L in $\mathbb{P}^2$ going through P and Q, let R be the third point of intersection with E, and let

$$f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z$$

be the line L' through R and O. By the fact that the line $Z = 0$ intersects E at O with multiplicity 3 gives us

$$div(f/Z) = (P) + (Q) + (R) - 3(O)$$

$$div(f'/Z) = (R) + (P + Q) - 2(O)$$

Hence

$$(P + Q) - (P) - (Q) + (O) = div(f/f') \sim 0$$

s0,

$$\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0$$

□

1.1.2 Lots of Invariants

There are reasons why the Weierstrass equation is the "best" form for elliptic curves. The first one is the following:

Definition 1.1.9. The *Weierstrass elliptic function* is

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{m+n\tau\neq 0} \left(\frac{1}{(z+m+n\tau)^2} - \frac{1}{(m+n\tau)^2} \right)$$

More generally, it is done relative to a lattice with periods ω_1, ω_2, with the form

$$\wp(z;\omega_1,\omega_2) = \frac{1}{z^2} + \sum_{m\omega_1+n\omega_2\neq 0} \left(\frac{1}{(z+m\omega_1+n\omega_2)^2} - \frac{1}{(m\omega_1+n\omega_2)^2} \right)$$

but, we can "shift" the lattice to the form above.

In a punctured neighborhood of the origin, the Laurent series expansion of $\wp$ is

$$\wp(z;\tau) = \frac{1}{z^2} + 3g_2 z^2 + 5g_3 z^4 + O(z^6)$$

where

$$g_2 = \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-4}$$

$$g_3 = \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-6}$$

Both g_2 and g_3 are Eisenstein series, which are *modular forms* (more on that later) when considered as functions of τ with $Im(\tau) > 0$, with weight 4 and 6 respectively.

In addition, $\wp$ satisfies the following differential equation:

$$\wp'(z)^2 = 4\wp(z)^3 - 60g_2\wp(z) - 140g_3$$

Looking at this, we see a familiar form of the Weierstrass equation from above. In fact, by choosing τ (with certain restraints) we can parametrize elliptic curves (an example of a coarse moduli space) by giving coordinates $[\wp(z), \wp'(z), 1]$.

1.1.3 Explicit Group Law

We have already seen that the Picard group gives us a group law on an elliptic curve. How can we explicitly (and geometrically) describe the group law? The first step (which we've already done) is to only look at Weierstrass equations. Next...

1.1.4 Isogenies

In usual mathematical fashion, after we have defined the objects we go about defining the right kind of functions between these objects. For elliptic curves, we need something which is a mix between a morphism for algebraic varieties and a homomorphism for groups. The correct notion for this is:

Definition 1.1.10. Lwr E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$.
Two elliptic curves are *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O\}$.

It follows from basic facts about smooth curves that an isogeny satisfies either

$$\phi(E_1) = \{O\} \quad \text{or} \quad \phi(E_1) = E_2$$

Thus, except for the zero isogeny, every isogeny is a finite map of curves. Hence, we obtain the usual injection of function fields:

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$$

The sum of two isogenies $\phi, \psi : E_1 \to E_2$ is defined by

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

This makes the set of isogenies, $Hom(E_1, E_2)$, a group.

Similarly, we can define a multiplication on the set of endomorphisms (making it a ring). For $\phi, \psi \in End(E)$, let

$$(\phi\psi)(P) = \phi(\psi(P))$$

Note. The *automorphism group* of E (denoted $Aut(E)$) is the set of invertible endomorphisms. This is *just* a group, because the sum of two automorphism is not necessarily invertible. For example, $(id_E + id_E)(P) = 2P$.

Example 1. For each $m \in \mathbb{Z}$ define the *multiplication-by-m* isogeny

$$[m] : E \to E, \quad \text{defined by } P \mapsto m \cdot P$$

Where $m \cdot P = P + ... + P$ (m-times) and if $m < 0$ we define $m \cdot P = (-m) \cdot (-P)$.

Proposition 1.1.11. *A couple facts about the objects which we have defined so far:*

(a) Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$. Then, the map $[m] : E \to E$ is nonconstant.

(b) Let E_1 and E_2 be elliptic curves. Then the group of isogenies, $Hom(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module

(c) Let E be an elliptic curve. Then the endomorphism ring $End(E)$ is a (not necessarily commutative) ring of characteristic 0 with no zero divisors.

Proof. Let $E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$

(a) We start by showing that $[2] \neq [0]$. The duplication formula from above says that if a point $P = (x, y) \in E$ has order 2 then it must satisfy

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

For $char(K) \neq 2$, then there are only finitely many such points.Further, even if $char(K) = 2$, the only way to have $[2] = [0]$ is for the cubic polynomial to be identically 0, which means that $b_2 = b_6 = 0$, which in turn implies that $\Delta = 0$. Hence, in all cases we have $[2] \neq [0]$. Now, using the fact that $[mn] = [m] \circ [n]$, we are reduced to considering the case that m is odd.

Assume that $char(K) \neq 2$. Then, using long division, we verify that

$$4x^3 + b_2x^2 + 2b_4x + b_6$$

does not divide

$$x^4 - b_4x^2 - 2b_6x - b_8$$

(More precisely, if the first polynomial divides the second, then $\Delta = 0$). Hence, we can find an $x_0 \in \overline{K}$ such that the first polynomial vanishes to higher order at x_0 than does the second. Choosing $y_o \in \overline{K}$ such that $P_0 = (x_0, y_0) \in E$, the doubling formula implies that $[2]P_0 = O$. In other words, we have shown that E has a nontrivial points P_0 of order 2. Then for odd integers m we have

$$[m]P_0 = P_0 \neq O$$

Thus, $[m] \neq [0]$

Finally, if $char(K) = 2$, use the "triplication" formula instead.

(b) Follows immediately from (a). Suppose $\phi \in Hom(E_1, E_2)$ and $m \in \mathbb{Z}$ satisfy

$$[m] \circ \phi = [0]$$

Taking degrees gives

$$(\deg\ [m])(\deg\ \phi) = 0$$

so either $m = 0$, or else (a) implies that $\deg[m] \geq 1$, in which case we must have $\phi = [0]$.

(c) From (b), the endomorphism ring End(E) has characteristic 0. Suppose that $\phi, \psi \in$End(E) satisfy $\phi \circ \psi = [0]$. Then

$$(\deg\ \phi)(\deg\ \psi) = \deg(\phi \circ \psi) = 0$$

It follows that either $\phi = [0]$ or $\psi = [0]$. Therefore End(E) has no zero divisors.

□

Definition 1.1.12. Let E be an elliptic curve and let $m \in \mathbb{N}$. The *m-torsion subgroup of E*, denoted by $E[m]$, is the set of all points of E of order m,

$$E[m] \coloneqq \{P \in E \mid [m]P = O\}$$

The *torsion subgroup of E* is the set of points of finite order

$$E_{tors} = \bigcup_{m \geq 1} E[m]$$

The most important fact about the map $[m] : E \to E$ is that it has degree m^2, from which one can deduce the structure of the finite group $E[m]$.

There is one problem: Are all isogenies group homomorphisms (of the natural group structure on elliptic curves)? The following theorem gives an answer:

Theorem 1.1.13. *Let $\phi : E_1 \to E_2$ be an isogeny. Then, $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.*

Proof. If $\phi(P) = O$ for all $P \in E$ then there is nothing to prove. Otherwise, ϕ is a finite map, so it induces

$$\phi_* : Pic^0(E_1) \to Pic^0(E_2)$$

defined by

$$\phi_* \left(\text{class of } \sum n_i(P_i)\right) = \text{class of } \sum n_i(\phi P_i)$$

This then gives us the following commutative diagram

$$\begin{tikzcd}
E_1 \arrow[r, "\sim"] \arrow[d, "\phi"] & Pic^0(E_1) \arrow[d, "\phi_*"] \\
E_2 \arrow[r, "\sim"] & Pic^0(E_2)
\end{tikzcd}$$

Where everything except ϕ is a homomorphism and the bottom arrow is injective, so ϕ is a homomorphism. □

Corollary 1.1.14. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then, $\ker(\phi) = \phi^{-1}(O)$ is a finite group.*

The following theorems encompass the basic Galois theory of elliptic functions fields.

Theorem 1.1.15. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

(a) For every $Q \in E_2$,

$$\#\phi^{-1}(Q) = deg_s(\phi)$$

Further, for every $P \in E_1$,

$$e_\phi(P) = deg_i(\phi)$$

(b) The map

$$\ker(\phi) \to Aut(\overline{K}(E_1)/\phi^*\overline{K}(E_2)), \qquad T \mapsto \tau_T^*$$

(where τ_T is the translation-by-T map) is an isomorphism.

(c) Suppose that ϕ is separable. Then ϕ is unramified,

$$\# \ker(\phi) = deg(\phi)$$

and $\overline{K}(E_1)$ is a Galois extension of $\phi^*\overline{K}(E_2)$.

Proof. For part (a), we know by ramification theory that

$$\#\phi^{-1} = deg_s(\phi) \qquad \text{for all but finitely many } Q \in E_2$$

But for any $Q, Q' \in E_2$ if we choose some $R \in E_1$ with $\phi(R) = Q' - Q$, then the fact that ϕ is a homomorphism implies that there is a one-to-one correspondence

$$\phi^{-1}(Q) \to \phi^{-1}(Q'), \qquad P \mapsto P + R$$

Hence, we can "cover the finitely many" getting

$$\#\phi^{-1}(Q) = deg_s(\phi) \qquad \text{for all } Q \in E_2$$

Now, let $P, P' \in E_1$ with $\phi(P) = \phi(P') = Q$ and let $R = P' - P$. Then, $\phi(R) = O$, so $\phi \circ \tau_R = \phi$. So, we compute

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) = e_\phi(\tau_R(P))e_{\tau_R}(P) = e_\phi(P')$$

Hence, every point in $\phi^{-1}(Q)$ has the same ramification index. We compute

$$\begin{aligned}(deg_s(\phi))(deg_i(\phi)) = deg(\phi) &= \sum_{P\in\phi^{-1}(Q)} e_\phi(P) \\ &= (\#\phi^{-1}(Q))e_\phi(P) \\ &= (deg_s(\phi))e_\phi(P)\end{aligned}$$

So, cancelling gives us $e_\phi(P) = deg_i(\phi)$.

For part (b), if $T \in \ker(\phi)$ and $f \in \overline{K}(E_1)$, then

$$\tau_T^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f$$

Hence, as an automorphism, τ_T^* fixes $\phi^*\overline{K}(E_2)$, and the map from (b) is well-defined.

Next, since $\tau_S \circ \tau_T = \tau_{S+T} = \tau_T \circ \tau_S$, the map is a homomorphism.

Finally, from (a), we have that $\# \ker(\phi) = deg_s(\phi)$, while a basic result from Galois theory says that $Aut(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) \leq deg_s(\phi)$, so we only need to show injectivity. But if τ_T^* fixes $\overline{K}(E_1)$, then in particular every function on E_1 takes the same value at T and O, but we can separate points, so then $T = O$.

For part (c), if ϕ is separable, we see from (a) that

$$\#\phi^{-1}(Q) = deg(\phi) \quad \text{for all } Q \in E_2$$

Hence, ϕ is unramified, and setting $Q = O$ gets us

$$\# \ker(\phi) = deg(\phi)$$

So, from (b), we see that

$$\#Aut(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$$

so $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is a Galois extension. □

Corollary 1.1.16. *Let the following be two nonconstant isogenies*

$$\phi : E_1 \to E_2 \quad \textit{and} \quad \psi : E_1 \to E_3$$

and suppose ϕ is separable and $\ker(\phi) \subseteq \ker(\psi)$*. Then, there is a unique isogeny*

$$\lambda : E_2 \to E_3$$

satisfying $\psi = \lambda \circ \phi$.

Proof. The proof is "immediate by Galois theory"...

Since ϕ is separable, $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is a Galois extension. Then, the inclusion $\ker(\phi) \subseteq \ker(\psi)$ along with the isomorphism from part (b) above gives us that every element of $Gal(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$ fixes $\psi^*\overline{K}(E_3)$. Thus, by Galois theory, there are fields inclusions

$$\psi^*\overline{K}(E_3) \subseteq \phi^*\overline{K}(E_2) \subseteq \overline{K}(E_1)$$

So, by the equivalence of categories, we get a map

$$\lambda : E_2 \to E_3$$

satisfying

$$\phi^*(\lambda^*\overline{K}(E_3) = \psi^*\overline{K}(E_3)$$

which then implies (again by equivalence of categories) that

$$\psi = \lambda \circ \phi$$

Finally, λ is an isogeny because

$$\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$$

□

Proposition 1.1.17. *Let E be an elliptic curve and let Φ be a finite subgroup of E. There is a unique elliptic curve denoted E/Φ and a separable isogeny*

$$\phi : E \to E/\Phi \quad \textit{satisfying} \quad \ker\phi = \Phi$$

Proof. Each points $T \in \Phi$ gives rise to an automorphism τ_T^* of $\overline{K}(E)$. Let $\overline{K}(E)^\Phi$ be the subfield fixed by these automorphisms. Galois theory tells us that $\overline{K}(E)$ is a Galois extension of $\overline{K}(E)^\Phi$ with Galois group isomorphic to Φ.

The field $\overline{K}(E)^\Phi$ is of transcendence degree one over $\overline{K}$, so equivalence of categories gives us a unique smooth curve $C/\overline{K}$ and a morphism

$$\phi : E \to C \quad \text{satisfying} \quad \phi^*\overline{K}(C) = \overline{K}(E)^\Phi$$

Next, we show that ϕ is unramified. Let $P \in E$ and $T \in \Phi$, then, for any $f \in \overline{K}(C)$

$$f(\phi(P+T)) = (\tau_T^* \circ \phi^*)f(\phi(P)) = (\phi^* f)(P) = f(\phi(P))$$

which gives us

$$\phi(T+P) = \phi(T)$$

Now let $Q \in C$ with P in its fiber, so

$$\{P + T \mid T \in \Phi\} \subseteq \phi^{-1}(Q)$$

but

$$\#\phi^{-1}(Q) \leq \deg(\phi) = \#\Phi$$

which gives us equality, implying that all points in the fiber are unramified (because $P+T$ is distinct for every $T \in \Phi$.

Finally, we apply the Hurwitz genus formula to ϕ. Since ϕ is unramified we get the form

$$2g(E) - 2 = (\deg \phi)(2g(C) - 2)$$

So, C must also have genus one, so it is an elliptic curve as soon as we assign it the basepoint $\phi(O)$ (which also automatically makes ϕ an isogeny). □

Remark 1. The fact that this "quotient" E/Φ is an elliptic curve is not immediately obvious, nor that there is the natural homomorphism $\phi : E \to E/\Phi$. In fact, for any variety and a finite group of automorphisms, the quotient is once again a variety.

1.1.5 The Invariant Differential

Let E/K be an elliptic curve defined by the Weierstrass equation

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

Then, we define (as done before) the *invariant differential* as

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

We know that this has neither zeros nor poles on E. We now justify its name of "invariant differential" by proving that it is invariant under translation.

Proposition 1.1.18. *Let E and ω be as above, let $Q \in E$, and let $\tau_Q : E \to E$ be the translation-by-Q morphism. Then $\tau_Q^*\omega = \omega$*

Proof. One can prove this directly by calculation (something which I did on a piece of paper) but it is more enlightening to prove it in the following manner:

Since Ω_E is a one-dimensional $\overline{K}(E)$-vector space, there is a function $a_Q \in \overline{K}(E)^\times$, depending a priori on Q, such that

$$\tau_Q^*\omega = a_Q\omega$$

We compute

$$\begin{aligned} div(a_Q) &= div(\tau_Q^*\omega) - div(\omega) \\ &= \tau_Q^* div(\omega) - div(\omega) \\ &= 0 \quad \text{ since } div(\omega) = 0 \end{aligned}$$

Hence, a_Q is a function on E having neither zeros nor poles, so we know that it is constant,meaning $a_Q \in \overline{K}^\times$.

Next, consider the map

$$f : E \to \mathbb{P}^1, \quad Q \mapsto [a_Q, 1]$$

We see that a_Q can be expressed as a rational function fo $x(Q)$ and $y(Q)$. Hence, f is a rational map $E \to \mathbb{P}^1$, and it is not surjective, since it misses both $[0, 1]$ and $[1, 0]$. We conclude that f is constant.
(because, for smooth curves, rational map ⇒ morphism ⇒ constant or surjective).

Thus a_Q does not depend on Q and we find its value by $a_Q = a_O = 1$. Therefore, $\tau_Q^*\omega = \omega$. □

This then leads us to the following theorem which simplifies that (very complicated) addition law of elliptic curves.

Theorem 1.1.19. *Let E and E' be elliptic curves, let ω be an invariant differential on E, and let $\phi, \psi : E \to E'$ be isogenies. Then,*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

Note. This is useful because the first addition is in $Hom(E, E')$ which uses the group law on E', but the second addition is in the vector space Ω_E.

Proof. AWLOG that $\phi, \psi \neq [0]$. If $\phi + \psi = [0]$, we use

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*$$

to see that it suffices to check

$$[-1]^*\omega = -\omega$$

The negation formula gives us

$$[-1](x, y) = (x, -y - a_1x - a_3)$$

which allows us to calculate

$$\begin{aligned}[-1]^* \left(\frac{dx}{2y + a_1x + a_3} \right) &= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} \\ &= -\frac{dx}{2y + a_1x + a_3}\end{aligned}$$

So, we can now assume that ϕ, ψ, and $\phi + \psi$ are all nonzero. Let (x_1, y_1) and (x_2, y_2) be Weierstrass coordinates on E which satisfy no other algebraic relations. More formally, $([x_1, y_1, 1], [x_2, y_2, 1])$ give coordinates for $E \times E$ sitting inside $\mathbb{P}^2 \times \mathbb{P}^2$.

Let $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, so x_3 and y_3 are rational combinations of x_1, x_2, y_1, y_2 given by the explicit addition formula for Weierstrass equations.

Then, using the addition formula and the standard rules for differentiation, we can express $\omega(x_3, y_3)$ in terms of $\omega(x_1, y_1)$ and $\omega(x_2, y_2)$. This yields

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$$

where f and g are rational functions. In doing this calculation, we remember that since x_i and y_i satisfy the given Weierstrass equation, the differentials dx_i and dy_i are related by

$$(2y_i + a_1x_i + a_3)dy_i = (3x_i^2 + 2a_2x_i + a_4 - a_1y_i)dx_i$$

In this way, we can express $\omega(x_3, y_3)$ as a linear combination of dx_1 and dx_2.

We claim that both f and g are identically 1. We use the fact that ω is invariant under translation to show this fact.

Suppose we assign fixed values to x_2 and y_2, say by choosing some $Q \in E$ and setting

$$x_2 = x(Q) \quad \text{and} \quad y_2 = y(Q)$$

Then

$$dx_2 = dx(Q) = 0, \quad \text{so} \quad \omega(x_2, y_2) = 0$$

Now, using the translation invariance, we get

$$\omega(x_3, y_3) = \tau_Q^*\omega(x_1, y_1) = \omega(x_1, y_1)$$

Which we substitute into the equation to get

$$f(x_1, y_1, x(Q), y(Q)) = 1$$

Thus, f does not depend on x_1, y_1, so $f \in \overline{K}[x_2, y_2]$, but we know that the above equation is true for all $Q \in E$, so it must be identically one on E. A similar argument gives us that g is also identically one.

This gives us exactly the relation leading to

$$(\phi + \psi)^*\omega = \phi * \omega + \psi^*\omega$$

□

We also get the immmediate corollary (set $\phi = [m], \psi = [1]$ and argue by induction)

Corollary 1.1.20. *Let ω be an invariant differential on an elliptic curve E. Let $m \in \mathbb{Z}$. Then*

$$[m]^*\omega = m\omega$$

Now to show the utility of the invariant differential, we will prove something we already knew, but in a "better" way:

Corollary 1.1.21. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$. Assume that $m \neq 0$ in K. Then $[m] : E \to E$ is a finite separable endomorphism.*

Proof. Let ω be an invariant differential on E. Then, $[m]^*\omega = m\omega \neq 0$, so $[m] \neq [0]$, which implies that $[m]$ is finite and $[m]^* : \Omega_E \to \Omega_E$ is injective, so $[m]$ is separable. □

Another corollary, this time involving the separability of the Frobenius morphism:

Corollary 1.1.22. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, let $\phi : E \to E$ be the q^th-power Frobenius morphism, and let $m \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In particular, the map $1 - \phi$ is separable.

Proof. Let ω be an invariant differential on E. We know that $\psi : E \to E$ is inseparable if and only if $\psi^*\omega = 0$. We compute

$$(m + n\phi)^*\omega = m\omega + n\phi^*\omega$$

but, ϕ is inseparable (basic properties of Frobenius(b/c derivative of $n^q = qn^{q-1} = 0$)), so

$$(m + n\phi)^*\omega = m\omega$$

Since we are in characteristic p, we see that $m\omega = 0$ if and only if $p \mid m$. □

Finally, a corollary about the endomorphism ring using the invariant differential:

Corollary 1.1.23. *Let E/K be an elliptic curve and let ω be a nonzero invariant differential on E. We define a map:*

$$a_? : End(E) \to \overline{K}, \quad \phi \to a_\phi \quad \textit{such that } \phi^*\omega = a_\phi\omega$$

(a) $a_?$ is a ring homomorphism

(b) $\ker a_?$ is the set of inseparable endomorphisms of E

(c) If $char(K) = 0$, then $End(E)$ is a commutative ring

Proof. As before, the fact that Ω_E is a one-dimensional $\overline{K}(E)$-vector space implies that $\phi^*\omega = a_\phi\omega$ for some function $a_\phi \in \overline{K}(E)$, and as before we can compute that $div(a_\phi) = 0$ so $a_\phi \in \overline{K}$.

(a) Using the invariant differential, we compute

$$a_{\phi+\psi}\omega = (\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega = a_\phi\omega + a_\psi\omega = (a_\phi + a_\psi)\omega$$

Similarly, we also compute

$$a_{\phi\circ\psi}\omega = (\phi \circ \psi)^*\omega = \psi^*(\phi^*\omega) = \psi^*(a_\phi\omega) = a_\phi\psi^*\omega = a_\phi a_\psi\omega$$

Therefore, $a_?$ is a ring homomorphism

(b) We have

$$a_\phi = 0 \qquad \iff \qquad \phi^*\omega = 0 \qquad \iff \qquad \phi \text{ is inseparable}$$

(c) If $char(K) = 0$, then every endomorphism is separable, so (b) says that $End(E)$ injects into $\overline{K}^\times$. Hence, $End(E)$ is commutative.

□

1.1.6 The Dual Isogeny

Let $\phi : E_1 \to E_2$ be a nonconstant isogeny. We know that ϕ induces a map

$$\phi^* : Pic^0(E_2) \to Pic^0(E_1)$$

On the other hand, we know that (as groups) we have the isomorphisms

$$\kappa_i : E_i \to Pic^0(E_i)$$

This then gives us a homomorphism going in the opposite direction to ϕ:

$$E_2 \xrightarrow{\kappa_2} Pic^0(E_2) \xrightarrow{\phi^*} Pic^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1$$

Later on we will verify that for $\phi(P) = Q$

$$\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P)$$

It is by no means clear that the homomorphism $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ is an isogeny, i.e. that it is given by a rational map. The process of finding P such that $\phi(P) = Q$ involves taking the roots of several polynomials. If ϕ is separable, one needs to check that applying $[\deg \phi]$ to P causes the conjugate roots to appear symmetrically. If ϕ is inseparable, things get more complicated.

Theorem 1.1.24. *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m.*

1. *There exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1 \quad \textit{satisfying} \quad \hat{\phi} \circ \phi = [m]$$

2. *As a group homomorphism, $\hat{\phi}$ equals the composition $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ or*

$$E_2 \to Div^0(E_2) \xrightarrow{\phi^*} Div^0(E_1) \xrightarrow{sum} E_1$$

$$Q \mapsto (Q) - (O) \qquad \sum n_P(P) \mapsto \sum [n_P]P$$

Proof. (a) First, we show uniqueness. Suppose that $\hat{\phi}$ and $\hat{\phi}'$ are two such isogenies. Then

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0]$$

Since ϕ is nonconstant, it follows that $\hat{\phi} - \hat{\phi}'$ must be constant, so $\hat{\phi} = \hat{\phi}'$.

Next, suppose that $\psi : E_2 \to E_3$ is another nonconstant isogeny, say of degree n, and suppose we know that $\hat{\phi}$ and $\hat{\psi}$ exist. Then

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm]$$

Thus $\hat{\phi} \circ \hat{\psi}$ has the requisite property to be $\widehat{\psi \circ \phi}$. If K has characteristic 0, then ϕ is separable, while if K has positive characteristic, then we can write ϕ as the composition of a separable isogeny and a Frobenius morphism. It thus suffices to check the two cases of ϕ being separable and ϕ being the Frobenius morphism

Case 1: Assume ϕ is separable. Since ϕ has degree m, we have that $\# \ker \phi = m$, so every element of $\ker \phi$ has order dividing m implying

$$\ker \phi \subseteq \ker[m]$$

Which we know from Galois theory gives us an isogeny

$$\hat{\phi} : E_2 \to E_1 \quad \text{satisfying} \quad \hat{\phi} \circ \phi = [m]$$

Case 2: AWLOG that ϕ is a p^th-power Frobenius, where $p = char(K)$. In particular, this implies that $deg(\phi) = p$.

We look at the multiplication-by-p map on E. Let ω be an invariant differential. Then we can compute

$$[p]^*\omega = p\omega = 0$$

We conclude that $[p]$ is not separable, and thus we decompose $[p]$ as a Frobenius morphism followed by a separable map. In other words

$$[p] = \psi \circ \phi^e$$

for some $e \geq 1$ and some separable isogeny ψ. Then, we can take:

$$\hat{\phi} = \psi \circ \phi^{e-1}$$

(b) Let $Q \in E_2$. Then the image of Q under the indicated composition is

$$\begin{aligned}
&\sum(\phi^*((Q) - (O))) \\
&\qquad = \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(Q)} [e_\phi(T)]T \\
&\qquad = [\deg_i \phi] \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(Q)} T \right) \\
&\qquad = [\deg_i \phi] \circ [\#\phi^{-1}(Q)]P \\
&\qquad = [\deg \phi]P
\end{aligned}$$

But, by construction

$$\hat{\phi}(Q) = \hat{\phi} \circ \phi(P) = [\deg \phi]P$$

so the two maps are the same.

□

We call $\hat{\phi}$ the *dual isogeny* of ϕ. The next theorem gives the basic properties of the dual isogeny. From these basic facts we will be able to deduce a number of very important corollaries, including a good description of the kernel of the multiplication-by-m map.

Theorem 1.1.25. *Let $\phi : E_1 \to E_2$ be an isogeny.*

(a) Let $m = \deg \phi$. Then

$$\hat{\phi} \circ \phi = [m] \quad \text{on } E_1$$

$$\phi \circ \hat{\phi} = [m] \quad \text{on } E_2$$

(b) Let $\lambda : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

(e) deg$\hat{\phi} = \deg \phi$

(f) $\hat{\hat{\phi}} = \phi$

Proof. □

1.1.7 Kronecker's Jugendtraum

Class field theory implies the following theorem (but it can also be proved without it):

Theorem 1.1.26 (Kronecker-Weber Theorem)**.** *Let $K/\mathbb{Q}$ be a Galois extension, and suppose that $Gal(L/\mathbb{Q})$ is abelian. Then there exists a cyclotomic field $\mathbb{Q}(\zeta)$ such that $K \subseteq \mathbb{Q}(\zeta)$. Hence, the Galois extensions of $\mathbb{Q}$ with abelian Galois groups are precisely that subfields of cyclotomic fields.*

Note. We can use this to construct a series of isomorphisms which show a part of class field theory:

$$\begin{aligned} Gal(\mathbb{Q}^{ab}/\mathbb{Q}) &\xrightarrow{\sim} Aut(\zeta_\infty) \xrightarrow{\sim} Aut(\mathbb{Q}/\mathbb{Z}) \\ &\xrightarrow{\sim} Aut\left(\bigoplus_p \varinjlim p^{-k}\mathbb{Z}/\mathbb{Z}\right) \\ &\xrightarrow{\sim} \prod_p \varprojlim Aut(\mathbb{Z}/p^k\mathbb{Z}) \\ &\xrightarrow{\sim} \varprojlim(\mathbb{Z}/p^k\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times \\ &\xrightarrow{\sim} \mathbb{A}^1/\mathbb{Q}^\times = GL_1(\mathbb{A}_\mathbb{Q}) \end{aligned}$$

This series of isomorphism can be seen using some basic complex analysis and simple Galois theory. We know that for an n^th rooth of unity, ζ_n, we have the following isomorphism:

$$t : Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

In addition, we can describe the root of unity in the following manner. We use the power series

$$f(z) = e^{2\pi iz} = \sum_{k\geq 0} \frac{(2\pi iz)^k}{k!}$$

to construct the root of unity

$$\zeta_n = e^{2\pi i/n} = f\left(\frac{1}{n}\right)$$

Then, we check the action of $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$:

$$\sigma\left(f\left(\frac{1}{n}\right)\right) = f\left(\frac{t(\sigma)}{n}\right)$$

This is Kronecker's *Jugendtraum* ("Dream of Youth"). Essentially, we want to try to describe extensions of number fields by special values of holomorphic (or meromorphic) functions, such that the function behaves well (has a certain "functional equation") with respect to the action of the Galois group.

Elliptic curves (with complex multiplication) help us generalize these ideas to non-abelian extensions, by constructing representations of the form:

$$Gal(L/K) \to GL_2(F)$$

This then gives us certain values which we use to create modular forms. This all ties into modularity (of course).

To begin, remember that for an elliptic curve E, the (contravariant) functor associated with is $Hom_{Sch}(-, E) : Sch \to Grp$, so for any field extension L/K we get that $E(K) \subseteq E(L)$ is a subgroup.

Next, we think of how we obtained the cyclotomic extensions from earlier. The n^th roots of unity are can be described as the kernel of the homomorphism

$$\lambda_n : \mathbb{C}^\times \to \mathbb{C}^\times, \quad \text{defined by } z \mapsto z^n$$

So, we want to imitate this with elliptic curves. We do this using the "multiplication-by-n" map:

$$\lambda_n : E(\mathbb{C}) \to E(\mathbb{C}), \quad \text{defined by } P \mapsto n \cdot P(= P + ... + P)$$

Then, we denote the kernel of the map as follows:

$$E[n] \coloneqq \ker(\lambda_n) = \{P \in E(\mathbb{C})\}$$

Remembering the analytic description of elliptic curves as $\mathbb{C}/L$ for a lattice $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, we get the following description of $E[n]$:

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$$

Now, we actually want to construct the extensions of $\mathbb{Q}$ from these groups $E[n]$. The idea is just to add the coordinates of every point in $E[n]$. Explicitly, let

$$E[n] = \{(x_1, y_1), ..., (x_m, y_m), \mathcal{O}\}$$

(Note, we know from the above description that $m = n^2 - 1$.) Then, we let

$$K \coloneqq \mathbb{Q}(x_1, y_1, ..., x_m, y_m)$$

Claim: $K/\mathbb{Q}$ is a Galois extension.

Proof. Let $\sigma : K \to \mathbb{C}$ be a field homomorphism. In order to prove that K is Galois over $\mathbb{Q}$, we have to show that $\sigma(K) = K$.

Recall that the Galois action on $E(\mathbb{C})$ preserves order of points (because it is an automorphism of groups) so $\sigma(P) \in E[n]$ for all $P \in E[n]$. This shows that the "basis" coordinates for the extension K can only transform to other "basis" coordinates, so $\sigma(K) = K$. □

From here on out, we will denote $\mathbb{Q}(E[n]) = K$ (from above). To begin, note that $E[n]$ is a finitely-generated $(\mathbb{Z}/n\mathbb{Z})$-module, so we can choose a basis. Using this basis, we can represent automorphisms of $E[n]$ with matrices. This amounts to giving a *Galois representation*:

$$\rho_n : Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}), \qquad \sigma \mapsto \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

Where $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ are determined by

$$\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2$$

$$\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2$$

For a choice of basis P_1, P_2 of $E[n]$.

This representation is clearly injective, but it is not always surjective. To illustrate this, here is an example:

Example 2. Consider the elliptic curve given by the equation

$$E : y^2 = x(x-1)(x-2)$$

Then

$$E[2] = \{\mathcal{O}, (0,0), (1,0), (2,0)\}$$

So, $\mathbb{Q}(E[2]) = \mathbb{Q}$, meaning that $Gal(\mathbb{Q}(E[2])/\mathbb{Q})$ is trivial. Therefore, the Galois representation is:

$$\rho_n(Gal(\mathbb{Q}(E[2])/\mathbb{Q})) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

which is obviously not surjective (unlike the case of cyclotomic extensions).

The key to understanding this is *complex multiplication*, (which we will discuss more in depth later in this section). Complex multiplication is (essentially) when the endomorphisms ring of the elliptic curve is special. Remember that all elliptic curves have the "multiplication-by-n" endomorphisms, and, in fact, *most* elliptic curves *only* have those endomorphisms (i.e. we have $End(E) \cong \mathbb{Z}$). So, the following definition comes naturally:

Definition 1.1.27. Let E be an elliptic curve. We say that E has *complex multiplication*, or CM for short, if there is an endomorphism $\phi : E \to E$ which is not defined by $P \mapsto n \cdot P$ (for some $n \in \mathbb{Z}$).

Why is it called "complex multiplication"? Recall that we can view elliptic curves as quotients $\mathbb{C}/L$ for some lattice L (using the Weierstrass $\wp$-function), so an endomorphism gives a holomorphic map $\phi : \mathbb{C}/L \to \mathbb{C}/L$. This means that in a neighborhood of 0, ϕ is given by a convergent power series

$$f(z) = c_0 + c_1 z + c_2 z^2 + ...$$

We also know that f is a homomorphism, so $f(z_1+z_2)=f(z_1)+f(z_2)$ for all z_1, z_2 in a neighborhood of 0. By complex analysis, we then know that $f(z)=cz$ for some $c\in\mathbb{C}$ (because the derivative is constant).

We then know that any endomorphism is of the form

$$f:\mathbb{C}/L\to\mathbb{C}/L, \quad f(z)\equiv cz \bmod L$$

but c can not just be arbitrary; it must satisfy the condition that $cL\subseteq L$. The first obvious choices for c are integers, and it turns out that the only other options are (non-real) complex numbers (basically, they need to rotate the lattice correctly).

So, to what extent are Galois representations associated to elliptic curves "almost surjective", and why are Galois extensions associated to curves with complex multiplication abelian (and, what sort of Galois extensions do we construct)?

First, a theorem by Serre which shows "almost surjectivity" (the proof is in French, I might look at it in more detail later):

Theorem 1.1.28. *Let E be an elliptic curve, and suppose E does not have complex multiplication. Then,*

(a) There is an integer $M\geq 1$ (depending only on E), such that for all n

$$[GL_2(\mathbb{Z}/n\mathbb{Z}):\rho_n(Gal(\mathbb{Q}(E[n])/\mathbb{Q}))]\leq M$$

(b) There is an integer $N\geq 1$ (depending only on E) such that for all n with $gcd(N,n)=1$ we have

$$\rho_n: Gal(\mathbb{Q}(E[n])/\mathbb{Q})\xrightarrow{\sim} GL_2(\mathbb{Z}/n\mathbb{Z}$$

To begin discussion of curves with complex multiplication and their associated extensions, we look at an example:

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

E has complex multiplication $\phi(x,y)=(-x,iy)$. We want this endomorphism to commute with the actions of the Galois group, but for some $\sigma\in Gal(K/\mathbb{Q})$:

$$\sigma(\phi(x,y))=(-\sigma(x),\sigma(i)\sigma(y))$$

$$\phi(\sigma(x,y))=(-\sigma(x),i\sigma(y)$$

So, they commute if and only if $\sigma(i)=i$. Therefore, we want to look at the subgroup $Gal(K/\mathbb{Q}(i))\subseteq Gal(K/\mathbb{Q})$, i.e. we will be studying abelian extension of $\mathbb{Q}(i)$. I will state a couple theorems without proof, but we will go into detail (and generalize this example) later...

Theorem 1.1.29. *Let E be the elliptic curve defined by $y^2 = x^3 + x$. For each integer $n \geq 1$, let $K_n = \mathbb{Q}(i)(E[n])$. Then, K_n is a Galois extension of $\mathbb{Q}(i)$ and its Galois group is abelian*

Theorem 1.1.30. *Let E be the elliptic curve defined by $y^2 = x^3 + x$ and let $F/\mathbb{Q}(i)$ be a finite abelian extension. Then, there is an integer $n \geq 1$ such that $F \subseteq K_n$*

Now, how does this tie into Kronecker's Jugendtraum? Using the Weierstrass $\wp$-function (with lattice corresponding to the specific elliptic curve), we get the following relation for any $\sigma \in Gal(K_n/\mathbb{Q}(i))$ (and similarly for $\wp'$):

$$\sigma\left(\wp\left(\begin{pmatrix} t_1 & t_2 \end{pmatrix}\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}\right)\right) = \wp\left(\begin{pmatrix} t_1 & t_2 \end{pmatrix}\rho_n(\sigma)\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}\right)$$

1.1.8 Tate Modules

In general, just as with p-adic rings, we would like to construct an object which captures all of the possible Galois representations tied to an elliptic curve. This is done in the "obvious" way; we take the limit of the torsion subgroups:

Definition 1.1.31. Let E be an elliptic curve and let $\ell \in \mathbb{Z}$ be a prime. The *(ℓ-adic) Tate module of E* is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

the inverse limit being taken with respect to the natural maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$$

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_\ell$-module. Further, since the multiplication-by-ℓ maps are surjective, the inverse limit topology on $T_\ell(E)$ is equivalent to the ℓ-adic topology is gains by being a $\mathbb{Z}_\ell$-module.

Before getting into representations of the Tate module, we can state a quick proposition about their structure:

Proposition 1.1.32. *Let E be an elliptic curve over K. Then, its Tate module $T_\ell(E)$ has the following structure:*

(a) If $\ell \neq char(K)$, then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module

(b) If $\ell = p = char(K) > 0$, then $T_p(E) \cong \{0\}$ or $\mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module.

Now, we define the Galois representation that we want:

Definition 1.1.33. The *ℓ-adic representation (of $Gal(\overline{K}/K)$ associated to E)* is the homomorphism

$$\rho_\ell : Gal(\overline{K}/K) \to Aut(T_\ell(E))$$

induced by the action of $Gal(\overline{K}/K)$ on the ℓ^n-torsion points of E.

Note. If we pick a $\mathbb{Z}_\ell$ basis for $T_\ell(E)$, then we obtain a representation

$$Gal(\overline{K}/K) \to GL_2(\mathbb{Z}_\ell)$$

Which we then extend using the inclusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ to get:

$$Gal(\overline{K}/K) \to GL_2(\mathbb{Z}_\ell)$$

The Tate module $T_\ell(E)$ is dual to the (etale) cohomology group $H^1(E, \mathbb{Z}_\ell)$. This can be seen by:

$$H^1(E, \mathbb{Z}_\ell) \cong Hom(\pi_1(E), \mathbb{Z}_\ell)$$

so, we need an isomorphism:

$$\pi_1(E) \otimes \mathbb{Z}_\ell \cong T_\ell(E)$$

Because the etale fundamental group only considers etale covers, we only need to worry about covers which permute by the "multiplication" maps, and since we are tensoring by $\mathbb{Z}_\ell$ we only need to consider the "multiplication-by-ℓ^n" maps. Both are "naturally Galois compatible" by construction.

From this duality, one can start to see how this would be generalized to other interesting (arithmetic) schemes.

For now, we will think of the Tate module purely in the context of elliptic curves (as it is defined above).

The Tate module is a useful tool for studying isogenies. Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then ϕ induces maps $\phi : E_1[\ell^n] \to E_2[\ell^n]$, thereby inducing a map $\phi_\ell : T_\ell(E_1) \to T_\ell(E)$. We thus obtain a natural homomorphism

$$Hom(E_1, E_2) \to Hom(T_\ell(E_1), T_\ell(E_2))$$

Further, if $E = E_1 = E_2$ we get a ring homomorphism

$$End(E) \to End(T_\ell(E))$$

Theorem 1.1.34. *Let E_1 and E_2 be elliptic curves and let $\ell \neq char(K)$ be a prime. Then the following natural map is injective*

$$Hom(E_1, E_2) \otimes \mathbb{Z}_\ell \to Hom(T_\ell(E_1), T_\ell(E_2)), \quad \phi \mapsto \phi_\ell$$

Proof. We start by proving the following statement:
Claim: Let $M \subseteq Hom(E_1, E_2)$ be finitely generated and let

$$M^{div} := \{\phi \in Hom(E_1, E_2) \mid [m] \circ \phi \in M, \text{ for some } m \geq 1\}$$

Then, M^{div} is finitely generated.

□

1.1.9 The Weil Pairing

1.2 IV: §§1-6

1.3 V: §1

1.4 VII: §§1-5

1.5 VIII: §§1-6

1.5.1 Weak Mordell-Weil

For the entirety of this (subsub)section, let E denote an elliptic curve.

Lemma 1.5.1. *Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.*

Proof. The inclusion $E(K) \hookrightarrow E(L)$ induces a natural map

$$E(K)/mE(K) \to E(L)/mE(L)$$

Let Φ be the kernel of this map, so

$$\Phi = \frac{E(K) \cap mE(L)}{mE(K)}$$

Then, for each $P \pmod{mE(K)}$ in Φ, we can choose a point $Q_P \in E(L)$ satisfying $[m]Q_P = P$. We then define a 1-cocycle

$$\lambda_P : G_{L/K} \to E[m], \quad \lambda_P(\sigma) = Q_P^\sigma - Q_P$$

Note that $Q_P^\sigma - Q_P$ is in $E[m]$, since

$$[m](Q_P^\sigma - Q_P) = ([m]Q_P)^\sigma - [m]Q_P = P^\sigma - P = O$$

Suppose that $P, P' \in E$ such that $\lambda_P = \lambda_{P'}$. Then for all $\sigma \in G_{L/K}$:

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$$

so, $Q_P - Q_{P'} \in E(K)$. It follows that

$$P - P' = [m]Q_P - [m]Q_{P'} \in mE(K)$$

and hence that $P \equiv P' (\text{mod } mE(K))$. This proves the association

$$\Phi \to Map(G_{L/K}, E[m]), \quad P \mapsto \lambda_P$$

is injective. But, $G_{L/K}$ and $E[m]$ are finite sets, so there are only a finite number of maps between them. Therefore, the set Φ is finite.

Finally, the exact sequence

$$0 \to \Phi \to E(K)/mE(K) \to E(L)/mE(L)$$

shows that $E(K)/mE(K)$ is finite. □

Now, we need something called the *Kummer pairing*, which we will illustrate using cohomology:

We start with the short exact sequence

$$0 \to E[m] \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0$$

where $m \geq 2$ is a fixed integer. Taking $G_{\bar{K}/K}$-cohomology yields the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & E(K)[m] \arrow[r] & E(K) \arrow[r, "{[m]}"] & E(K) \arrow[dll, rounded corners, "\delta"] \\
 & H^1(K, E[m]) \arrow[r] & H^1(K, E(\bar{K})) \arrow[r, "{[m]}"] & H^1(K, E(\bar{K}))
\end{tikzcd}$$

From the middle of this sequence, we get the short exact sequence

$$0 \to \frac{E(K)}{mE(K)} \xrightarrow{\delta} H^1(K, E[m]) \to H^1(K, E(\bar{K}))[m] \to 0$$

Under the assumption that $E[m] \subseteq E(K)$, we get

$$H^1(K, E[m]) = Hom(G_{\bar{K}/K}, E[m]$$

which then means we have an injection

$$E(K)/mE(K) \hookrightarrow Hom(G_{\bar{K}/K}, E[m]$$

Which along with duality gives us a bilinear form

$$E(K) \times G_{\bar{K}/K} \to E[m]$$

which we call the Kummer pairing, satisfying the following properties

(a) The kernel on the left is $mE(K)$

(b) The kernel on the left is $G_{\bar{K}/L}$, where

$$L = K([m]^{-1}E(K)]$$

Meaning that it is a perfect bilinear pairing of

$$E(K)/mE(K) \times G_{L/K} \to E[m]$$

We now prove a reduction lemma:

Lemma 1.5.2. *Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.*

Proof. We use the inflation-restriction sequence from Galois cohomology:

$$\begin{tikzcd}
0 \arrow[r] & \ker(i) \arrow[r] \arrow[d, hook] & E(K)/mE(K) \arrow[r, "i"] \arrow[d, hook] & E(L)/mE(L) \arrow[d, hook] \\
0 \arrow[r] & H^1(G_{L/K}, E[m]) \arrow[r, "inf"] & H^1(G_{\bar{K}/K)}, E[m]) \arrow[r, "res"] & H^1(G_{\bar{L}/L}, E[m])
\end{tikzcd}$$

Noting that $\ker(i)$ must be finite, since $H^1(G_{L/K}, E[m])$ is finite, since $G_{L/K}$ and $E[m]$ are finite.

□

Note. The above proof of the weak Mordell-Weil can be summed up using Galois cohomology as follows:

$$0 \to E[m](\bar{K}) \xrightarrow{\iota} E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 0$$

Which we then extend by $G_{\bar{K}/K}$-invariance to a LES in cohomology:

$$\begin{tikzcd}
0 \arrow[r] & H^0(K, E[m]) \arrow[r, "\iota"] & H^0(K, E) \arrow[r, "{[m]}"] & H^0(K, E) \arrow[dll, rounded corners, "\delta"] \\
 & H^1(K, E[m]) \arrow[r, "\tilde{\iota}"] & H^1(K, E) \arrow[r, "{[\tilde{m}]}"] & H^1(K, E)
\end{tikzcd}$$

This then gives us an exact sequence:

$$0 \to E(K)/mE(K) \xrightarrow{\delta \circ \pi} H^1(K, E[m]) \xrightarrow{\tilde{\iota}} H^1(K, E)[m] \to 0$$

So, we just need finiteness of $H^1(K, E[m])$. We set $m = 2$, to get

$$\begin{aligned}
H^1(K, E[2]) &\cong H^1(K, (\mathbb{Z}/2\mathbb{Z})^2) \\
&\cong Hom(G_{\bar{K}/K}, (\mathbb{Z}/2\mathbb{Z})^2) \\
&\cong Hom(G_{\bar{K}/K}, (\mathbb{Z}/2\mathbb{Z}))^2 \\
&\cong Hom(G_{\bar{K}/K}, \mu_2)^2 \\
&\cong H^1(K, \mu_2)^2
\end{aligned}$$

Then, the Kummer sequence gives us an isomorphism

$$K^\times/K^{\times 2} \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mu_2)$$

Combining the above maps, we obtain an injective homomorphism

$$E(K)/2E(K) \xrightarrow{\delta} H^1(K, \mu_2)^2 \xrightarrow{\delta^{-1} \times \delta^{-1}} (K^\times/K^{\times 2}) \times (K^\times/K^{\times 2})$$

Then, we can show that the image of this map is finite, being contained in

$$K(E[2], 2) = \{f \in K^\times/K^{\times 2} \mid ord_t(f) \equiv 0 (\text{mod } m) \text{ for all } t \notin E[2]\}$$

We prove that this set is finite by reducing to $K(\emptyset, m)$ and pure calculation using divisors. Funnily enough, this isn't any easier than the first proof; the first proof is a simplification of the ideas.

1.5.2 Height Functions and Descent

Theorem 1.5.3 (Descent Theorem)**.** *Let A be an abelian group. Suppose that there exists a height function, $h : A \to \mathbb{R}$, with the following three properties:*

(i) Let $Q \in A$. There is a constant C_1, depending on A and Q, such that for all $P \in A$
$$h(P+Q) \leq 2h(P) + C_1$$

(ii) There is an integer $m \geq 2$ and a constant C_2, depending on A, such that for all $P \in A$
$$h(mP) \leq m^2 h(P) - C_2$$

(iii) For every constant C_3, the set
$$\{P \in A : h(P) \leq C_3\}$$
is finite

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then, A is finitely generated.

Proof. Choose elements $Q_1, ..., Q_r \in A$ to represent the finitely many cosets in A/mA, and let $P \in A$ be an arbitrary element.

We begin by writing
$$P = mP_1 + Q_{i_1}, \quad \text{for some } 1 \leq i_1 \leq r$$

Next, we do the same thing with P_1, then with P_2, etc. This gives us a list of points
$$\begin{aligned} P &= mP_1 + Q_{i_1} \\ P_1 &= mP_2 + Q_{i_2} \\ &\cdots \\ P_{n-1} &= mP_n + Q_{i_n} \end{aligned}$$

For any index j, we have by the properties of the height function:
$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}(h(mP_j) + C_2) \\ &= \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2) \\ &\leq \frac{1}{m^2}(2h(P_{j-1} + C_1' + C_2) \end{aligned}$$

where C_1' is the maximum of the constants from (i) for $Q \in \{-Q_1, ..., -Q_r\}$. Note that C_1' and C_2 do not depend on P.

We use this inequality repeatedly, starting from P_n and working back to P. This yields:

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^8} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2) \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2} \\ &\leq \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \qquad \text{since } m \geq 2 \end{aligned}$$

It follows that if n is sufficiently large, then

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

Since P is a linear combination of P_n and $Q_1, ..., Q_r$, it follows that every element of A is a linear combination of points from the set

$$\{Q_1, ..., Q_r\} \cup \{P \in A : h(P) \leq 1 + \frac{1}{2}(C_1' + C_2)\}$$

Which property (iii) tells us is finite. □

1.5.3 Mordell-Weil over $\mathbb{Q}$

Fix a Weierstrass equation for $E/\mathbb{Q}$ of the form

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}$$

We know from above that $E(\mathbb{Q}/2E(\mathbb{Q})$ is finite, so in order to apply the "descent theorem" we need a proper height function on $E(\mathbb{Q})$.

Definition 1.5.4. Let $t \in \mathbb{Q}$, and write $t = p/q$ as a fraction in lowest terms. The *height of* t is

$$H(t) = max\{|p|, |q|\}$$

Definition 1.5.5. The *(logarithmic) height on $E/\mathbb{Q}\curvearrowleft$*, relative to the Weierstrass equation, is the function

$$h_x : E(\mathbb{Q}) \to \mathbb{R}, \qquad h_x(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases}$$

We note that $h_x(P)$ is always nonnegative.

Now we explore some properties of this height function:

Lemma 1.5.6. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 = x^3 + Ax + B \qquad \textit{with } A, B \in \mathbb{Z}$$

(a) *Let $P_0 \in E(\mathbb{Q})$. There is a constant C_1 that depends on P_0, A, and B such that for all $P \in E(\mathbb{Q})$*

$$h_x(P + P_0) \leq 2h_x(P) + C_1$$

(b) *There is a constant C_2 that depends on A and B such that for all $P \in E(\mathbb{Q})$*

$$h_x([2]P) \leq 4h_x(P) - C_2$$

(c) *For every constant C_3, the set*

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

is finite.

Proof. Much of this proof is done by direct calculation. Strap in...

We may assume that $C_1 > \max\{h_x(P_0), h_x([2]P_0)\}$, which ensures that (a) is true if $P_0 = O$ or if $P \in \{O, \pm P_0\}$. In all other cases we write

$$P = (x, y)$$

□

1.5.4 Heights on Projective Space

To prove the Mordell-Weil Theorem over arbitrary number fields, we need a theory of height functions on projective space over general fields.

First, we consider a point $P \in \mathbb{P}^N(\mathbb{Q})$. Since $\mathbb{Z}$ is a principal ideal domain, we can find homogeneous coordinates (by multiplying by lcm),

$$P = [x_0, ..., x_N]$$

satisfying

$$x_0, ..., x_N \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0, ..., x_N) = 1$$

the natural measure of the *height of P* is

$$H(P) = max\{|x_0|, ..., |x_N|\}$$

With this definition it is clear that the set

$$\{P \in \mathbb{P}^N(\mathbb{Q}) : H(P) \leq C\}$$

is finite with at most $(2C + 1)^N$ elements.

If we generalize this notion of height to arbitrary number fields we run into the problem that its ring of integers may not be a PID. So, we need to normalize the valuations:

Definition 1.5.7. The *set of standard absolute values on $\mathbb{Q}$*, which we denote $M_{\mathbb{Q}}$, consists of the following

(i) $M_{\mathbb{Q}}$ contains one archimedean absolute value, defined by

$$|x|_\infty = \max\{x, -x\}$$

(ii) For each prime $p \in \mathbb{Z}$, the set $M_{\mathbb{Q}}$ contains one nonarchimedean (p-adic) absolute value defined by

$$|p^n \frac{a}{b}|_p = p^{-n} \quad \text{for } a, b \in \mathbb{Z} \text{ satisfying } p \nmid ab$$

The *set of standard absolute values* on a number field K, denoted by M_K, is the set of all absolute values on K which restrict to a standard absolute value on $\mathbb{Q}$.

Definition 1.5.8. Let $v \in M_K$. The *local degree at* v is

$$n_v = [K_v : \mathbb{Q}_v]$$

An some basic facts about the local degree:

Proposition 1.5.9 (Extension Formula)**.** *Let $L/K/\mathbb{Q}$ be a tower of number fields, and let $v \in M_K$. Then*

$$\sum_{w \in M_L, w|v} n_w = [L : K] n_v$$

Proposition 1.5.10 (Product Formula)**.** *Let $x \in K^\times$. Then*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1$$

We are now ready to define a general height function:

Definition 1.5.11. Let $P \in \mathbb{P}^N(K)$ be a point with homogeneous coordinates $P = [x_0, ..., x_N]$. The *height of P (relative to K)* is

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v}$$

Proposition 1.5.12. *Let $P \in \mathbb{P}^N(K)$.*

(a) The height $H_K(P)$ does not depend on the choice of homogeneous coordinates for P.

(b) The height satisfies $H_K(P) \geq 1$.

(c) Let L/K be a finite extension. Then

$$H_L(P) = H_K(P)^{[L:K]}$$

Proof. (a) Any other choice of homogeneous coordinates for P has the form $[\lambda x_0, ..., \lambda x_N]$ for some $\lambda \in K^\times$. Using the product formula, we have that

$$\begin{aligned}\prod_{v\in M_K} \max\{|\lambda x_0|_v, ..., |\lambda x_N|_v\}^{n_v} &= \prod_{v\in M_K} |\lambda|^{n_v} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v} \\ &= \prod_{v\in M_K} \max\{|x_0|_v, ..., |x_N|_v\}^{n_v}\end{aligned}$$

(b) Given any $P \in \mathbb{P}^N(K)$, we can always find homogeneous coordinates such that at least one of the coordinates is 1. Then every factor in the product defining $H_K(P)$ is at least 1.

(c) We compute

$$\begin{aligned}H_L(P) &= \prod_{w\in M_L} \max\{|x_i|_w\}^{n_v} \\ &= \prod_{v\in M_K} \prod_{w|v} \max\{|x_i|_v\}^{n_w} \\ &= \prod_{v\in M_K} \max\{|x_i|_v\}^{[L:K]n_v} \\ &= H_K(P)^{[L:K]}\end{aligned}$$

□

Sometimes it is easier to work with a height function that is not relative to a particular number field. We use part (c) from above to create:

Definition 1.5.13. Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. Choose a number field K such that $P \in \mathbb{P}^N(K)$. The *(absolute) height of* P is

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}$$

where we take the positive root. We see from the proposition above that this is well-defined, independent of choice of K (or homogeneous coordinate), and $H(P) \geq 1$.

We next investigate how the height changes under mappings between projective spaces. We recall the following definition:

Definition 1.5.14. A *morphism of degree* d between projective spaces is a map

$$F : \mathbb{P}^N \to \mathbb{P}^M, \qquad F(P) = [f_0(P), ..., f_M(P)]$$

where $f_0, ..., f_M \in \bar{\mathbb{Q}}[X_0, ..., X_N]$ are homogeneous polynomials of degree d having no common zero in $\bar{\mathbb{Q}}^{N+1} \setminus (0, ..., 0)$.

Theorem 1.5.15. *Let $F : \mathbb{P}^N \to \mathbb{P}^M$ be a morphism of degree d. Then there are positive constants C_1, C_2 depending on F, such that for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$*

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d$$

Proof. Let $F = [f_0, ..., f_M]$ and $P = [x_0, ..., x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$. Choose some number field $K/\mathbb{Q}$ such that $x_i \in K$ for all i and $f_j \in K[x]$ for all j. For each absolute value $v \in M_K$, we let

$$|P|_v = \max_i |x_i|_v \quad \text{and} \quad |F(P)|_v = \max_j |f_j(P)|_v$$

and we also define

$$|F|_v = \max\{|a|_v : a \text{ is a coefficient of some } f_i\}$$

Then, from the definition of height, we get

$$H_K(P) = \prod_{v \in M_K} |P|_v^{n_v} \quad \text{and} \quad H_K(F(P)) = \prod_{v \in M_K} |F(P)|_v^{n_v}$$

so it makes sense to define

$$H_K(F) = \prod_{v \in M_K} |F|_v^{n_v}$$

□

1.6 IX: §§1-7

So, now we know that even though there are an infinite number of rational numbers on an elliptic curve, by Mordell-Weil it is theoretically possible to find a finite number of points to generate this infinite set. What about integral points? Well, it turns out that there are only finitely many, a fact proved by Siegel using the theory of Diophantine approximation. We start our discussion with that:

1.6.1 Diophantine Approximation

The fundamental problem in the subject of Diophantine approximation is the question of how closely an irrational number can be approximated by a rational number.

Example 3. For any rational number p/q, we know that the quantity $|p/q - \sqrt{2}|$ is strictly positive, and since $\mathbb{Q}$ is dense in $\mathbb{R}$, an appropriate choice of p/q makes it as small as desired. The problem is to make it small without taking p and q to be too large. The next two elementary results illustrate the idea.

Proposition 1.6.1 (Dirichlet)**.** *Let $\alpha \in \mathbb{R}$ with $\alpha \notin \mathbb{Q}$. Then there are infinitely many rational numbers $p/q \in \mathbb{Q}$ such that*

$$\left|\frac{p}{q} - \alpha\right| \leq \frac{1}{q^2}$$

Proof. Let Q be a (large) integer and look at the set of real numbers

$$\{q\alpha - \lceil q\alpha \rceil : q = 0, 1, ..., Q\}$$

Since α is irrational, this set contains $Q+1$ distinct numbers in $(0,1)$. Dividing the interval into Q equal-sized pieces and applying the pigeonhole principle, we find that there are integers $0 \leq q_1 \leq q_2 \leq Q$ satisfying

$$|(q_1\alpha - \lceil q_1\alpha \rceil) - (q_2\alpha - \lceil q_2\alpha \rceil)| \leq \frac{1}{Q}$$

Hence

$$\left| \frac{\lceil q_1\alpha \rceil - \lceil q_1\alpha \rceil}{q_2 - q_1} - \alpha \right| \leq \frac{1}{(q_2 - q_1)Q} \leq \frac{1}{(q_2 - q_1)^2}$$

This provides one rational approximation to α having the desired property.

Finally, having obtained a list of such approximations, let p/q be the one for which $|p/q - \alpha|$ is smallest. Then, taking $Q > |p/q - \alpha|^{-1}$ ensures that we get a new approximation that is not already in our list. Hence, there exist infinitely many rational numbers satisfying the condition of the proposition. □

Proposition 1.6.2 (Liouville)**.** *Let $\alpha \in \bar{\mathbb{Q}}$ have degree $d \geq 2$ over $\mathbb{Q}$. There is a constant $C > 0$, depending on α, such that for all rational numbers p/q, we have*

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}$$

Proof. We assume that $\alpha \in \mathbb{R}$, since otherwise $C = Im(\alpha)$ works. Let

$$f(T) = a_0 + a_1T^1 + ... + a_dT^d \in \mathbb{Z}[T]$$

be a minimal polynomial for α, and let

$$C_1 = \sup\{f'(t) : \alpha - 1 \leq t \leq \alpha + 1\}$$

Then, the MVT tells us that

$$\left| f\left(\frac{p}{q}\right) \right| = \left| f\left(\frac{p}{q}\right) - f(\alpha) \right| \leq C_1 \left| \frac{p}{q} - \alpha \right|$$

On the other hand, we know that $q^d f(p/q) \in \mathbb{Z}$, and further that $f(p/q) \neq 0$, since f has no rational roots. Hence

$$\left| q^d f\left(\frac{p}{q}\right) \right| \geq 1$$

Setting $C = \min\{C_1^{-1}, 1\}$ and combining the last two inequalities yields

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}$$

□

Dirichlet's theorem is about approximating numbers in completions of number fields (so, we might want to generalize to p-adic numbers), while Liouville's result concerns numbers in algebraic extensions over $\mathbb{Q}$ (so, we might want to generalize to algebraic extensions over arbitrary fields).

Definition 1.6.3. Let $\tau(d)$ be a positive real-valued function on the natural numbers. A number field K is said to have *approximation exponent* τ if it has the following property:

Let $\alpha \in \bar{K}$, let $d = [K(\alpha) : K]$, and let $v \in M_K$ be an absolute value on K that has been extended to $K(\alpha)$ in some fashion. Thne for any constant C there exist only finitely many $x \in K$ satisfying the inequality

$$|x - \alpha|_v < CH_K(x)^{-\tau(d)}$$

Liouville's elementary estimate says that $\mathbb{Q}$ has approximation exponent $\tau(d) = d + \varepsilon$ for any $\varepsilon > 0$.

The key theorem for proving Siegel's theorem is Roth's theorem:

Theorem 1.6.4. *For every $\varepsilon > 0$, every number field K of degree d has approximation exponent*

$$\tau(d) = 2 + \varepsilon$$

We will not prove this theorem here (but we will sometime later). Instead, we will demonstrate why this is useful:

Example 4. Consider the simple example of trying to solve the equation

$$x^2 - 2y^3 = a$$

in integers $x, y \in \mathbb{Z}$, for $a \in \mathbb{Z}$ fixed. Suppose that (x, y) is a solution with $y \neq 0$. Let ζ be a primitive cube root of unity, and factor the equation as

$$\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta\sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta^2\sqrt[3]{2}\right) = \frac{a}{y^3}$$

The second and third factors in the product are bounded away from zero, so we obtain an estimate of the form

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{C}{y^3}$$

where the constant C is independent. Thus, Roth's theorem implies that there are only finitely many possibilities for x and y. Hence, the equation has only finitely many solutions in integers.

Now, we have a Diophantine inequality

$$|x - \alpha|_v < CH_K(x)^{-\tau(d)}$$

We see that it consists of two parts. First, there is a height function, which measures the *arithmetic* size of x. Second, there is the quantity $|x-\alpha|_v$, which is a *topological* or *metric* measure of distance from x to α, i.e. it measures distance in the v-adic topology. Now, we want a way to measure v-adic distance on curves, deduce some of its basic properties, and reinterpret these Diophantine inequalities in terms of this new distance function.

Definition 1.6.5. Let C/K be a curve, let $v \in M_K$, and fix a point $Q \in C(K_v)$. Choose a function (Riemann-Roch) $t_Q \in K_v(C)$ that has a zero of order $e \geq 1$ at Q and no other zeroes. Then, for $P \in C(K_v)$, we define the *(v-adic) distance from P to Q* by

$$d_v(P,Q) = \min\left\{ |t_Q(P)|_v^{1/e}, 1 \right\}$$

(If t_Q has a pole at P, we formally set $t_Q(P) = \infty$, so $d_v(P,Q) = 1$.)

Proposition 1.6.6. *Let $Q \in C(K_v)$ and let $F \in K_v(C)$ be a function that vanishes at Q. Then the limit*

$$\lim_{P \xrightarrow{v} Q} \frac{\log |F(P)|_v}{\log d_v(P,Q)} = ord_Q(F)$$

exists and is independent of choice of the function t_Q used to define $d_v(P,Q)$.

Proof. Let t_Q be the function vanishing only at Q that we are using to define $d_v(-,Q)$. Let $e = \operatorname{ord}_Q(t_Q)$ and $f = \operatorname{ord}_Q(F)$. Then the function $\phi = F^e/t_Q^f$ has neither a zero nor a pole at Q, so $|\phi(P)|_v$ is bounded away from 0 and ∞ as $P \xrightarrow{v} Q$. Hence

$$\begin{aligned} \lim_{P \xrightarrow{v} Q} \frac{\log |F(P)|_v}{\log d_v(P,Q)} &= \lim_{P \xrightarrow{v} Q} \frac{\log |F(P)|_v}{\log |t_Q(P)|_v^{1/e}} \\ &= \end{aligned}$$

□

1.7 X: §§1-6

2 Modular Forms

2.1 Modularity?

Modular forms are highly related to elliptic curves. In fact, the Modularity Theorem roughly states that all rational elliptic curves arise from modular forms.

To give perspective, we start by considering a situation from elementary number theory. Take a quadratic equation

$$Q : x^2 = d, \quad d \in \mathbb{Z},\ d \neq 0$$

letting $\mathcal{Q} \coloneqq Spec(\mathbb{Z}[x]/Q)$. For each prime number p define

$$a_p(Q) = |\mathcal{Q}(\mathbb{F}_p)| - 1$$

We then extend these values multiplicatively to all of $\mathbb{N}$.

By definition $a_p(Q)$ is the Legendre symbol (d/p) for all $p > 2$, one statement of the Quadratic Reciprocity Theorem is that $a_p(Q)$ depends only on the value of p modulo $4|d|$. This can be reinterpreted as a statement that the sequence of solution counts $\{a_2(Q), a_3(Q), a_5(Q), a_7(Q), a_{11}(Q), ...\}$ arises as a system of eigenvalues on a finite dimensional complex vector space associated to the equation Q. Let $N = 4|d|$, let $G = (Z/NZ)^*$, and let V_N be the vector space of complex valued functions on G. For each prime p define a linear operator T_p on V_N,

$$T_p : V_N \to V_N, \quad (T_p f)(n) = \begin{cases} f(\overline{pn}) & \text{if } p \nmid N \\ 0 & \text{if } p \mid N \end{cases}$$

Consider a particular function $f = f_Q$ in V_N

$$f : G \to \mathbb{C}, \quad f(n) = a_n(Q) \text{ for } n \in G$$

This is well-defined by Quadratic Reciprocity (remember: $N = 4|d|$). It is immediate that if f is an eigenvector for the operators T_p

$$\begin{aligned}(T_p f)(n) &= \begin{cases} f(\overline{pn}) & \text{if } p \nmid N \\ 0 & \text{if } p \mid N \end{cases} \\ &= a_p(Q) f(n) \text{ in all cases}\end{aligned}$$

So, $T_p f = a_p(Q) f$ for all p. This shows that the sequence $\{a_p(Q)\}$ is a system of eigenvalues as claimed.

The Modularity Theorem can be viewed as giving an analogous result. Consider the elliptic curve

$$E : y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in \mathbb{Z},\ g_2^3 - 27g_3^2 \neq 0$$

For each prime number p define

$$a_p(E) = p - |E(\mathbb{F}_p)|$$

One statement of the Modularity is that (again) the sequence of solution-counts $\{a_p(E)\}$ is a system of eigenvalues.

A *modular form* is a function on $\mathbb{H} \coloneqq \{z \in \mathbb{C} \mid Im(z) > 0\}$ that satisfies certain transformation conditions and holomorphy conditions. Let $\tau \in \mathbb{H}$, then a modular form has a Fourier expansion

$$f(\tau) = \sum_{n \geq 0} a_n(f) e^{2\pi i n \tau},\ a_n(f) \in \mathbb{C} \text{ for all } n$$

Each nonzero modular form has two associated integers k and N called its *weight* and its *level*. The modular forms of any given weight and level form a vector space, which we can immediately form linear operators called *Hecke operators* for, one being called T_p for any prime p. An *eigenform* is a modular form that is a simultaneous eigenvector for all the Hecke operators.

By analogy to the situation in elementary number theory, the Modularity Theorem associates to the elliptic curve E and eigenform $f = f_E$ in a vector space V_N of weight 2 modular forms at a level N called the *conductor* of E. The eigenvalues of f are its Fourier coefficients

$$T_p(f) = a_p(f)f \quad \text{for all primes } p$$

A version of Modularity says that "Fourier coefficients give the solution-counts"

$$a_p(f) = a_p(E) \quad \text{for all primes } p($$

Other statements of Modularity include:

(i) If the *j-invariant*, $j(E) = 1728g_2^3/(g_2^3 - 27g_3^2)$ is rational then E is the holomorphic image of a modular curve,

$$X_0(N) \to E$$

(ii) Every complex elliptic curve with rational j-invariant is the holomorphic homomorphic image of a *Jacobian*,

$$J_0(N) \to E$$

(iii) (refinement of (ii)) the elliptic curve is the image of a quotient of a Jacobian, the *abelian variety* associated to a weight 2 eigenform (associating a *cusp form* f to E)

$$A_f \to E$$

(iv) The L-function of the modular form is the L-function of the elliptic curve,

$$L(s, f) = L(s, E)$$

(v) Every Galois representation associated to an elliptic curve over $\mathbb{Q}$ arises from a Galois representation associated to a modular form,

$$\rho_{f,\ell} \sim \rho_{E,\ell}$$

One case of relating "analytic" and "algebraic" L-functions which is of a "lower" dimension than the Modularity Theorem is through Tate's Thesis and Artin Reciprocity, covered in the Appendix.

2.2 $SL_2(\mathbb{Z})$

To start, recall the definition of the special linear group over $\mathbb{Z}$:

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \mid ad - bc = 1 \right\} \subseteq SL_2(\mathbb{R})$$

This group acts on the *upper-half plane*

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$$

by *linear fractional transformations* as follows:

$$\text{For } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

define for any $z \in \mathbb{H}$:

$$\gamma(z) = \frac{az+b}{cz+d} \in \mathbb{H}$$

2.3 Modular Forms of Level 1

We want to construct a modular form for any weight for level 1 (aka for $\mathrm{SL}_2(\mathbb{Z})$): (Remember that there are no modular forms of odd weight of level 1)

Definition 2.3.1. For an integer $k \geq 4$ the *nonnormalized weight k Eisenstein series* is the function on the extended upper-half plane $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ defined by

$$G_k(z) = \sum_{n,m\in\mathbb{Z}}^{*} \frac{1}{(n+mz)^k}$$

Theorem 2.3.2. *The function $G_k(z)$ is a modular form of weight k, i.e. $G_k(z) \in M(SL_2(\mathbb{Z}))$.*

Proof. By complex analysis, $G_k(z)$ defines a holomorphic function on $\mathbb{H}^*$. For modularity, observe that

$$G_k(z+1) = \sum \frac{1}{(n+m(z+1))^k} = \sum \frac{1}{((n+m)+mz)^k} = G_k(z)$$

and

$$G_k(-1/z) = \sum \frac{1}{(n-m/z)^k} = \sum \frac{z^k}{(nz-m)^k} = z^k G_k(z)$$

□

Remark 2. $G_k(\infty) = 2\zeta(k)$, where ζ is the *Riemann zeta function*, because as $z \to \infty$ the terms with $m \neq 0$ go to 0. Thus

$$G_k(\infty) = \sum_{n\in\mathbb{Z}}^{*} \frac{1}{n^k}$$

which gives us twice the zeta function when k is even.

Using the Eisenstein series, we define a function that we have seen before...

Definition 2.3.3. Suppose $E = \mathbb{C}/\Lambda$ is an elliptic curve over $\mathbb{C}$ viewed as a quotient of $\mathbb{C}$ by the lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, with $\omega_1/\omega_2 \in \mathbb{H}$. The *Weierstrass $\wp$-function* of the lattice Λ is

$$\wp = \wp_\Lambda(u) = \frac{1}{u^2} + \sum_{k=4,6,8,\ldots} (k-1)G_k(\omega_1/\omega_2)u^{k-2}$$

This satisfies the differential equation

$$(\wp')^2 = 4\wp^3 - 60G_4(\omega_1/\omega_2)\wp - 140G_6(\omega_1/\omega_2)$$

If we set $x = \wp$ and $y = \wp'$, the above is an (affine) equation for an elliptic curve that is $\mathbb{C}$-isomorphic to $\mathbb{C}/\Lambda$

2.4 Hecke Operators

As an example, think of the modular curve $X_0(N) := \mathbb{H}/\Gamma_0(N)$. Note that every lattice $\mathbb{Z} + \omega\mathbb{Z}$ has a sublattice associated with any prime $p(\mathbb{Z} + \omega\mathbb{Z})$, so we can construct the following diagram:

$$\begin{tikzcd}
X_0(N) \arrow[r, leftarrow, "“push''"] & X_0(pN) \arrow[r, "“pull''"] & X_0(N)
\end{tikzcd}$$

The modular forms associated to $\Gamma_0(N)$ are exactly the differential forms on $X_0(N)$, so we pull them back and then push them forward. This gives us a linear transformation of the space of modular forms. The problem is that there could be many preimages in $\Omega(X_0(N))$, so we have to sum over them.

The way to think about this is using the **hermite normal form** of the matrices.

Example 5. For $SL_2(\mathbb{Z})$

$$\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & n \\ 0 & p \end{bmatrix} \quad (0 \leq n < p)$$

2.5 Hecke Operators Algebraically

From [DS05]:

3 Complex Multiplication

4 Mazur's Theorem

This section will be a bit different, because I will be following a series of video lectures.

5 Falting's Theorem

This section will follow [CS86] in Falting's proof of Mordell's Conjecture.

5.1 Finiteness Theorems for Abelian Varieties over Number Fields

Let K be a finite extension of $\mathbb{Q}$, A an abelian variety over K, $\pi = \mathrm{Gal}(\bar{K}/K)$ the absolute Galois group of K, and ℓ a prime number. Then, π acts on the Tate module

$$T_\ell(A) = \varprojlim_n A[\ell^n](\bar{K})$$

The goal of this chapter is to give a proof of the following results

(a) The representation of π on $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is semisimple (i.e. a direct sum of irreducible representations).

(b) The map $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{End}_\pi(T_\ell(A))$ is an isomorphism.

(c) Let S be a finite set of places of K, and let $d > 0$. Then there are only finitely many isomorphism classes of abelian varieties over K with polarization of degree d which have good reduction outside of S.

It is known that (c) implies the Mordell conjecture. (a) and (b) have already been proven over function fields and finite fields. To prove them over the number field K, we use Arakelov theory, reducing the question to providing "everything" with a hermitian metric. The proof of (c) is done by first showing finiteness only for isogeny classes. We then translate a result from Hodge theory into étale cohomology and a couple other things to finish the proof.

We start with some technicalities:

Definition 5.1.1. Let S be a scheme (or algebraic stack). A *semiabelian variety* of relative dimension g over S is a smooth algebraic group $p : G \to S$ whose fibers are connected of dimension g, and are extensions of abelian varieties by a torus

Example 6. Let $q : C \to S$ be a stable curve of genus $g = 4$. Then, $Pic^\tau(C/S) \to S$ is a semiabelian variety of relative dimension g.

Lemma 5.1.2. *Let S be normal, $U \subseteq S$ open and dense, $p_1 : A_1 \to S$ and $p_2 : A_2 \to S$ two semiabelian varieties, $\phi : A_1/U \to A_2/U$ a homomorphism of algebraic groups defined over U. Then ϕ can be extended uniquely to S.*

Proof. □

6 Abelian Varieties

The easiest way to understand abelian varieties is as higher-dimensional analogues of elliptic curves. Part of the reason why elliptic curves are nice is because of the concrete (Weierstrass) models that gives us explicit equations to work with. Abelian varieties of dimension $g > 1$ do not have that luxury; most of their "defining equations" are too complicated to be of much use, or it is not possible for us to write it down explicitly.

Elliptic curves can also be thought of as nonsingular projective curves with a group structure. Abelian varieties are direct generalizations of this to higher dimensions.

Finally, we can think of elliptic curves analytically as $\mathbb{C}/\Lambda$, and an abelian variety of dimension g over $\mathbb{C}$ can be thought of as $\mathbb{C}^g/\Lambda$. The converse, though, requires a bit more care: given a lattice Λ in $\mathbb{C}^g$ there are certain properties that is must fulfil to make it an abelian variety.

Remember that we can describe the group structure on an elliptic curve E by the following canonical isomorphism

$$P \mapsto [P] - [O] : E(k) \to \mathrm{Pic}^0(E)$$

This statement has two generalizations:

(a) Let C be a curve and choose a point $Q \in C(k)$; then there is an abelian variety J, called the Jacobian variety of C, canonically attached to C, and a regular map $\phi : C \to J$ such that $\phi(Q) = O$ and an isomorphism

$$\mathrm{Pic}^0(C) \xrightarrow{\sim} J(k)$$

The dimension of J is the genus of C.

(b) Let A be an abelian variety. Then there is a dual abelian variety $A^\vee$ such that $\mathrm{Pic}^0(A) \cong A^\vee(k)$ and $\mathrm{Pic}^0(A^\vee) \cong A(k)$. In the case of an elliptic curve, $E^\vee = E$. In general, A and $A^\vee$ are isogenous, but not usually isomorphic.

Appropriately interpreted, most of the statements of Silverman's book [Sil09] hold for abelian varieties, but because we don't have equations the proofs are more abstract.

Definitions; Basic Properties

Definition 6.0.1. A *group variety over k* is an algebraic variety V/k together with regular maps

$$\mu : V \times_k V \to V$$
$$\iota : V \to V$$

and an element $e \in V(k)$ such that the structure on $V(\bar{k})$ defined by μ and ι is a group with identity element e.

A group variety is automatically nonsingular: as with any variety, a group variety contains a nonsingular dense open subvariety, which we then translate to cover it. From this we can then deduce that a connected group variety is irreducible.

A complete connected group variety is called an *abelian variety.* As we shall see, they are projective and (fortunately) commutative.

Theorem 6.0.2 (Rigidity)**.** *Consider a regular map $\alpha : V \times W \to U$, and assume that V is complete and that $V \times W$ is geometrically irreducible. If there are points $u_0 \in U(k)$, $v_0 \in V(k)$, and $w_0 \in W(k)$ such that*

$$\alpha(V \times \{w_0\}) = \{u_0\} = \alpha(\{v_0\} \times W$$

then $\alpha(V \times W) = \{u_0\}$

In other words, if the two "coordinate axes" collapse to a point, then this forces the whole space to collapse to a point.

Proof. Since the hypotheses continue to hold after extending scalars from k to $\bar{k}$, we can assume that k is algebraically closed. Note that V is connected, because otherwise $V \times_k W$ couldn't be connected, much less irreducible. We need to use the following facts:

(i) If V is complete, then the projection map $q : V \times_k W \to W$ is closed (this is the definition of being complete).

(ii) If V is complete and connected, and $\phi : V \to U$ is a regular map from V into an affine variety, then $\phi(V) = pt$

Let U_0 be an open affine neighborhood of $u_0 \in U$. Because of (i), $Z := q(\alpha^{-1}(U \setminus U_0))$ is closed in W. By definition, Z consists of the second coordinate of points of $V \times W$ not mapping into U_0. Thus a point $w \in W$ lies outside of Z if and only if $\alpha(V \times \{w\}) \subseteq U_0$. In particular w_0 lies outside Z, and so $W \setminus Z$ is nonempty. As $V \times \{w\}$ is complete and U_0 is affine, $\alpha(V \times \{w\})$ must be a point whenever $w \in W \setminus Z$. In fact, $\alpha(V \times \{w\}) = \alpha(v_0, w) = \{u_0\}$. Then, α is constant everywhere except Z, but by irreducibility (i.e. density of open sets) and separability of U, α must agree with the constant map on the whole of $V \times W$. □

Corollary 6.0.3. *Every regular map $\alpha : A \to B$ of abelian varieties is the composite of a homomorphism with a translation.*

Proof. The regular map α will send the k-rational point O of A to a k-rational point b of B. After composing α with translation by $-b$, we may assume that $\alpha(O) = O$. Consider the map

$$\phi : A \times A \to B$$

$$\phi(a, a') = \alpha(a, a') - \alpha(a) - \alpha(a')$$

This can be "resaid" as ϕ being the difference of the two regular maps

$$\begin{tikzcd}
A \times A \arrow[r, "\mu"] \arrow[d, "\alpha\times\alpha"] & A \arrow[d, "\alpha"] \\
B \times B \arrow[r, "\mu"] & B
\end{tikzcd}$$

which is a regular map. Then $\phi(A \times O) = O = \phi(O \times A)$ and so $\phi = 0$. This means that α is a homomorphism. □

Note. The corollary shows that the group structure on an abelian variety is uniquely determined by the choice of a zero element (as in the case of elliptic curves).

Corollary 6.0.4. *The group law on an abelian variety is commutative.*

Proof. Commutative groups are distinguished among all groups by the fact that the "inverse" map is a homomorphism. Since the negative map, $(a \mapsto -a) : A \to A$ takes zero to itself, the preceding corollary shows that it is a homomorphism. □

Corollary 6.0.5. *Let V and W be projective varieties over k with k-rational points v_0 and w_0, and let p, q be the projection maps. Let A be an abelian variety. Then a morphism $h : V \times W \to A$ such that $(v_0, w_0) = O$ can be written uniquely as $h = f \circ p + g \circ q$ with $f(v_0) = g(w_0) = O$.*

Proof. Set

$$f = h|_{V \times \{w_0\}}, \qquad g = h|_{\{v_0\} \times W}$$

On points, $f(v) = h(v, w_0)$ and $g(v) = h(v_0, w)$, and so $\Delta := h - (f \circ p + g \circ q)$ is the map that sends

$$(v, w) \mapsto h(v, w) - h(v, w_0) - h(v_0, w)$$

Thus

$$\Delta(V \times \{w_0\}) = O = \Delta(\{v_0\} \times W)$$

and so $\Delta = 0$. □

Abelian Varieties over $\mathbb{C}$

Let A be an abelian variety over $\mathbb{C}$, and assume that A is projective (this will be proved later). Then $A(\mathbb{C})$ inherits a complex structure as a submanifold of $\mathbb{P}^n(\mathbb{C})$. It is a compact, closed, connected complex manifold with a commutative group structure. It turns out that these facts are sufficient to allow us to give an elementary description of $A(\mathbb{C})$.

Let G be a Lie group (i.e. a group object in the category of differentiable manifolds (*maps are differentiable*)). A *one-parameter subgroup* of G is a differentiable homomorphism $\phi : \mathbb{R} \to G$. In elementary differentiable geometry one proves that for every tangent vector v to G at e, there is a unique one-parameter subgroup $\phi_v : \mathbb{R} \to G$ such that $\phi_v(0) = e$ and $(d\phi_V)(1) = v$. Moreover, there is a unique differentiable map

$$exp : Tgt_e(G) \to G$$

such that

$$t \mapsto exp(tv) : \mathbb{R} \to Tgt_e(G) \to G$$

is ϕ_v for all v; thus $exp(v) = \phi_v(1)$. If G is commutative then the exponential map is a homomorphism. These results extend to complex manifolds, and give the first part of the following proposition.

Proposition 6.0.6. *Let A be an abelian variety of dimension g over $\mathbb{C}$.*

(a) There is a unique homomorphism

$$exp : Tgt_O(A(\mathbb{C})) \to A(\mathbb{C})$$

of complex manifolds such that, for each $v \in Tgt_O(A(\mathbb{C}))$, $z \mapsto exp(zv)$ is the one-parameter subroup $\phi_v : \mathbb{C} \to A(\mathbb{C})$ corresponding to v. The differential of exp at O is the identity map

$$Tgt_O(A(\mathbb{C})) \to Tgt_O(A(\mathbb{C}))$$

(b) The map exp is surjective, and its kernel is a full lattice in the complex vector space $Tgt_O(A(\mathbb{C}))$.

Proof. It remains to prove (b). The image H of *exp* is a subgroup of $A(\mathbb{C})$. Because $d(exp)$ is an isomorphism on the tangent space at O, the inverse function theorem shows that *exp* is a local isomorphism at O. In particular, its image contains an open neighborhood U of O in H. But then, for any $a \in H$, $a + U$ is an open neighborhood of a in H, and so H is open in $A(\mathbb{C})$. Because the complement of H is a union of translates of H (cosets), H is also closed. But $A(\mathbb{C})$ is connected, so any clopen subset is the entire space. We have shown that *exp* is surjective.

Denote $Tgt_O(A(\mathbb{C}))$ by V, and regard it as a real vector space of dimension $2g$. Recall that a lattice in V is a subgroup of the form

$$L = e_1\mathbb{Z} + \cdots + e_r\mathbb{Z}$$

with $e_1, \ldots, e_r$ linearly independent over $\mathbb{R}$; moreover, a subgroup $L \subseteq V$ is a lattice if and only if it is discrete for the induced topology, and that it is discrete if and only if O has a neighborhood U in V such that $U \cap L = \{O\}$. Therefore, the fact that *exp* is a local isomorphism at O, then $\ker(exp)$ is a lattice in V. It must be a full lattice (i.e. $r = 2g$) because otherwise $V/L \cong A(\mathbb{C})$ wouldn't be compact. □

We have shown that if A is an abelian variety, then $A(\mathbb{C}) \cong \mathbb{C}^g/L$ for some full lattice $L \subseteq \mathbb{C}^g$. However, unlike the one-dimensional case, not every quotient

$\mathbb{C}^g/L$ is an abelian variety. Before we start stating a necessary and sufficient condition for a quotient to arise in this way, we compute the cohomology of a torus.

The Cohomology of a Torus

Let X be a smooth manifold V/L, where V is a real vector space of dimension n and L is a full lattice in $\mathbb{R}^n$. Note that $V = Tgt_O(X)$ and $L = \ker(exp)$, so X and its points O determine both V and L. We wish to compute the cohomology groups of X.

Recall the following statements from algebraic topology:

(a) Let X be a topological space, and let $H^*(X;\mathbb{Z}) = \bigoplus_r H^r(X;\mathbb{Z})$; then the cup product defines a graded ring structure on $H^*(X;\mathbb{Z})$.

(b) (Kunneth formula): Let X and Y be topological spaces such that $H^r(X;\mathbb{Z})$ and $H^s(Y;\mathbb{Z})$ are free $\mathbb{Z}$-modules for all r, s. Then there is a canonical isomorphism

$$H^m(X \times Y;\mathbb{Z}) \cong \bigoplus_{r+s=m} H^r(X;\mathbb{Z}) \otimes H^s(Y;\mathbb{Z})$$

(c) If X is a "reasonable" topological space, the

$$H^r(X;\mathbb{Z}) \cong \mathrm{Hom}(\phi_1(X), \mathbb{Z})$$

(d) If X is compact and orientable of dimension d, the duality theorems show that there are canonical isomorphisms

$$H^r(X;\mathbb{Z}) \cong H_{d-r}(X;\mathbb{Z}) \cong H^{d-r}(X;\mathbb{Z})^\vee$$

when all the cohomology groups are torsion-free.

We first compute the dimension of the groups $H^r(X;\mathbb{Z})$. Note, that as a real manifold, $V/L \cong (\mathbb{R}/\mathbb{Z})^n \cong (S^1)^n$. We have

$$H^r(S^1;\mathbb{Z}) = \mathbb{Z}, \mathbb{Z}, 0, 0, \dots \text{ for } r = 1, 2, 3, 4, \dots$$

Hence, by the Kunneth formula,

$$H^*((S^1)^2;\mathbb{Z}) = \mathbb{Z}, \mathbb{Z}^2, \mathbb{Z}, 0, \dots$$

$$H^*((S^1)^3;\mathbb{Z}) = \mathbb{Z}, \mathbb{Z}^3, \mathbb{Z}^3, \mathbb{Z}, 0, \dots$$

$$H^*((S^1)^4;\mathbb{Z}) = \mathbb{Z}, \mathbb{Z}^4, \mathbb{Z}^6, \mathbb{Z}^4, \mathbb{Z}, 0, \dots$$

The exponents form a Pascal's triangle:

$$\dim H^r((S^1)^{;}\mathbb{Z}) = \binom{n}{r}$$

Next, we compute the groups $H^r(X;\mathbb{Z})$ explicitly. Recall from linear algebra that if M is a $\mathbb{Z}$-module, then $\bigwedge^r M$ is the quotient of $\bigotimes^r M$ generated by the tensors $a_1 \otimes \cdots \otimes a_r$ in which two of the a_i are equal. Thus,

$$\mathrm{Hom}(\bigwedge^r M, \mathbb{Z}) \cong \{\text{alternating forms } f : M^r \to \mathbb{Z}\}$$

(a multilinear form is alternating if $f(a_1, \dots, a_r) = 0$ whenever two a_i are equal). If M is free and finitely generated, with basis $e_1, \dots, e_d$, say over $\mathbb{Z}$, then

$$\{e_{i_1} \wedge \cdots \wedge e_{i_r} \mid i_1 < i_2 \cdots < i_r\}$$

is a basis for $\bigwedge^r M$; moreover, if $M^\vee$ is the $\mathbb{Z}$-linear dual $\mathrm{Hom}(M, \mathbb{Z})$ of M, then the pairing

$$\bigwedge^r M^\vee \times \bigwedge^r M \to \mathbb{Z}, \qquad (y_1 \wedge \cdots \wedge y_r, x_1 \wedge \cdots \wedge x_r) \mapsto \det(y_i(x_j))$$

realizes each of $\bigwedge^r M^\vee$ and $\bigwedge^r M$ as the $\mathbb{Z}$-linear dual of each other.

Theorem 6.0.7. *Let X be the torus V/L. There are canonical isomorphisms*

$$\bigwedge^r H^1(X;\mathbb{Z}) \to H^r(X;\mathbb{Z}) \to \mathit{Hom}(\bigwedge^r L, \mathbb{Z})$$

Proof. For any manifold X, the cup-product defines a map

$$\bigwedge^r H^1(X;\mathbb{Z}) \to H^r(X;\mathbb{Z}), \qquad a_1 \wedge \cdots \wedge a_r \to a_1 \cup \cdots \cup a_r$$

Moreover, the Kunneth formula shows that, if this map is an isomorphism for X and Y and all r, then it is an isomorphism for $X \times Y$ and all r. Since it is obviously true for S^1, it is true for $X \cong (S^1)^n$. This defines the first map and proves that it is an isomorphism. The space $V \cong \mathbb{R}^n$ is simply connected, and $\mathit{exp} : V \to X$ is a covering map, therefore it realizes V as the universal covering space of X, and so $\pi_1(X)$ is its group of deck transformations, which is L. Hence

$$H^1(X;\mathbb{Z}) \cong \mathrm{Hom}(L, \mathbb{Z})$$

The pairing

$$\bigwedge^r L^\vee \times \bigwedge^r L \to \mathbb{Z}$$

realizes each group as the $\mathbb{Z}$-linear dual of the other, and $L^\vee = H^1(X;\mathbb{Z})$, and so

$$\bigwedge^r H^1(X;\mathbb{Z}) \cong \mathrm{Hom}(\bigwedge^r L, \mathbb{Z})$$

□

Now, we will briefly summarize the theory of *Riemann forms*, which will allow us to characterize complex tori which are abelian varieties:

Lemma 6.0.8. *Let V be a complex vector space. There is a one-to-one correspondence between the Hermitian forms H on V and the real-valued skew-symmetric forms E on V satisfying the identity $E(iv, iw) = E(v, w)$, namely:*

$$E(v, w) = Im(H(v, w))$$

$$H(v, w) = E(iv, w) + iE(v, w)$$

Example 7. Consider the torus $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}i)$. Then

$$E(a + ib, c + id) = bc - ad$$

$$H(z, z') = z\bar{z}'$$

are a pair as in the lemma

Let $X = V/L$ be a complex torus of dimension g, and let E be a skew-symmetric form $L \times L \to \mathbb{Z}$. Since $L \otimes \mathbb{R} = V$, we can extend E to a skew-symmetric $\mathbb{R}$-bilinear form $E_{\mathbb{R}} : V \times V \to \mathbb{R}$. We call E a *Riemann form* if

(a) $E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v, w)$;

(b) the associated Hermitian form is positive definite

We say that X is *polarizable* if it admits a Riemann form.

Theorem 6.0.9. *A complex torus X is of the form $A(\mathbb{C})$ if and only if it is polarizable.*

Brief Sketch. ($\Rightarrow$): Choose an embedding $A \hookrightarrow \mathbb{P}^n$ with n minimal. There exists a hyperplane $H \subseteq \mathbb{P}^n$ that doesn't contain the tangent space to any point on $A(\mathbb{C})$. Then $A \cap H$ is a smooth variety of (complex) dimension $g - 1$. It can be "triangulated" by $(2g - 2)$ simplices, and so defines a class in

$$H_{2g-2}(A; \mathbb{Z}) \cong H^2(A; \mathbb{Z}) \cong \text{Hom} \bigwedge^2 L, \mathbb{Z})$$

and hence a skew-symmetric form on L. This can be shown to be a Riemann form.

($\Leftarrow$): Given E, it is possible to construct enough functions (quotients of theta functions) on V to give an embedding of X into some projective space. (Essentially constructing an ample line bundle) □

Theorem 6.0.10. *The functor $A \mapsto A(\mathbb{C})$ is an equivalence of categories of abelian varieties over $\mathbb{C}$ to the category of polarizable complex tori*

Let $X = V/L$. Then

$$V^* := \{f : V \to \mathbb{C} \mid f(\alpha v) = \bar{\alpha} f(v), \quad f(v + v') = f(v) + f(v')\}$$

is a complex vector space of the same dimension as V. Define

$$L^* := \{f \in V^* \mid Im(f(L)) \subset \mathbb{Z}\}$$

Then, L^* is a lattice in V^*, and $X^\vee := V^*/L^*$ is a polarizable complex torus, called the *dual torus.*

Example 8. If $X = V/L$, then $X[m]$, the m-torsion points, is $m^{-1}L/L$. There is a canonical pairing

$$X[m] \times (X^{\vee})[m] \to \mathbb{Z}/m\mathbb{Z}$$

called the *Weil pairing.*

A Riemann form E on X defines a homomorphism $\lambda_E : X \to X^{\vee}$ as follows: let H be the associated Hermitian form and let λ_E be the map defined by

$$(v \mapsto H(v, -)) : V \to V^*$$

Then λ_E is an isogeny, and we call such a map λ_E a *polarization.* The degree of the polarization is the order of the kernel. The polarization is said to be principal if it is of degree 1. Every polarizable torus is isogenous to a principally polarizable torus. A polarizable torus is simple if it does not contain a nonzero proper polarizable subtorus. Every polarizable torus is isogenous to a direct sum of simple polarizable tori.

Let E be an elliptic curve over $\mathbb{Q}$. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. For a simple polarizable torus, $D = \mathrm{End}(X) \otimes \mathbb{Q}$ is a division algebra over a field and the polarization defines a positive involution $\dagger$ on D. The pairs $(D, \dagger)$ that arise from a simple abelian variety have been classified.

Rational Maps Into Abelian Varieties

Remember that in the theory of elliptic curves rational maps are "just as good" as regular maps, because they are irreducible projective curves. In the theory of abelian varieties, the following theorem is the next best thing:

Theorem 6.0.11. *A rational map $\phi : V \dashrightarrow W$ from a normal variety V to a complete variety W is defined on an open subset $U \subseteq V$ whose complement $V \smallsetminus U$ has codimension ≥ 2.*

Proof. Assume first that V is a curve. Thus, we are given a nonsingular curve V and a regular map $\phi : U \to W$ from an open subset of V which we extend to V. Consider the maps

$$\begin{tikzcd}
 & V \\
U \arrow[ur, hook] \arrow[r, "{(u,\phi(u))}"] \arrow[dr, "\phi"'] & Z \subset V \times W \arrow[u] \arrow[d] \\
 & W
\end{tikzcd}$$

Let U' be the image of U in $V \times W$, and let Z be its closure. The image of Z in V is closed (because W is complete), and contains U (the composite $U \to V$ is the given inclusion), and so Z maps onto V. The maps $U \to U' \to U$ are isomorphisms. Therefore, $Z \to V$ is a surjective map from a complete curve onto a nonsingular curve that is an isomorphism on open subsets. Such a map must be an isomorphism (complete nonsingular curves are determined by their function fields). The restriction of the projection map $V \times W \to W$ to $Z(\cong V)$ is the extension of ϕ to V that we are seeking.

The general case can be reduced to the one-dimensional case (using schemes). Let U be the largest subset on which ϕ is defined, and suppose $V \smallsetminus U$ has codimension 1. Then there is a prime divisor Z in $V \smallsetminus U$. Because V is normal, its associated local ring is a DVR $\mathcal{O}_Z$ with field of fractions $k(V)$. The map ϕ defines a morphism of schemes $\operatorname{Spec}(k(V)) \to W$, which the valuation criterion of properness shows extends to a morphisms $\operatorname{Spec}(\mathcal{O}_Z) \to W$. This implies that ϕ has a representative defined on an open subset that meets Z in a nonempty subset, which is a contradiction. □

Theorem 6.0.12. *A rational map $\alpha : V \dashrightarrow A$ from a nonsingular variety to an abelian variety is defined on the whole of V.*

Proof. Combine the earlier theorem with the following lemma. □

Lemma 6.0.13. *Let $\phi : V \dashrightarrow G$ be a rational map from a nonsingular variety to a group variety. Then either ϕ is defined on all of V or the points where it is not defined form a closed subset of pure codimension 1 in V (i.e. a finite union of prime divisors).*

Proof. Define a rational map

$$\Phi : V \times V \dashrightarrow G, \qquad (x, y) \mapsto \phi(x) \cdot \phi(y)^{-1}$$

More precisely, if (U, ϕ_U) represents ϕ, then Φ is the rational map represented by

$$U \times U \xrightarrow{\phi_U \times \phi_U} G \times G \xrightarrow{id \times \iota} G \times G \xrightarrow{\mu} G$$

Clearly Φ is defined at a diagonal point (x, x) if ϕ is defined at x, and then $\Phi(x, x) = e$. Conversely, if Φ is defined at (x, x), then it is defined on an open neighborhood of (x, x); in particular, there will be an open subset U of V such that Φ is defined on $\{x\} \times U$. After possibly replacing U by a smaller open subset (not necessarily containing x), ϕ will be define on U. For $u \in U$, the formula

$$\phi(x) = \Phi(x, u) \cdot \phi(u)$$

defines ϕ at x. Thus ϕ is defined at x if and only if Φ is defined at (x, x). The rational map Φ defines a map

$$\Phi^* : \mathcal{O}_{G,e} \to k(V \times V)$$

Since Φ sends (x, x) to e if it is defined there, it follows that Φ is defined at (x, x) if and only if

$$Im(\mathcal{O}_{G,e}) \subset \mathcal{O}_{V \times V,(x,x)}$$

Now, $V \times V$ is nonsingular, and so we have a good theory of divisors. for a nonzero rational function f on $V \times V$, write

$$\operatorname{div}(f) = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty$$

Then

$$\mathcal{O}_{V\times V,(x,x)} = \{f \in k(V \times V) \mid \operatorname{div}(f)_\infty \text{ does not contain } (x,x)\} \cup \{0\}$$

Suppose ϕ is not defined on x. Then for some $f \in Im(\phi^*)$, $(x,x) \in \operatorname{div}(f)_\infty$, and clearly Φ is not defined at the points $(y,y) \in \Delta \cap \operatorname{div}(f)_\infty$. This is a subset of pure codimension 1 in Δ, and when we identify it with a subset of V, it is a subset of V of codimension 1 passing through x on which ϕ is not defined. □

Theorem 6.0.14. *Let $\alpha : V \times W \to A$ be a morphism from a product of nonsingular varieties into an abelian variety, and assume that $V \times W$ is geometrically irreducible. If*

$$\alpha(V \times \{w_0\}) = \{a_0\} = \alpha(\{v_0\} \times W)$$

for some $a_0 \in A(k)$, $v_0 \in V(k)$, and $w_0 \in W(k)$, then

$$\alpha(v \times W) = \{a_0\}$$

If V (or W) is complete then this is a special case of the Rigidity theorem. For the general case, we need two lemmas.

Lemma 6.0.15. *(a) Every nonsingular curve V can be realized as an open subset of a complete nonsingular curve C.*

(b) Let C be a curve. Then, there is a nonsingular curve C' and a regular map $C' \to C$ that is an isomorphism over the set of nonsingular points of C.

Proof. We will just sketch the proofs:

(a) Let $K = k(V)$. Take C to be the set of discrete valuation rings in K containing k with the topology which the finite sets and whole set are closed. For each open subset U of C, define

$$\Gamma(U, \mathcal{O}_C) = \bigcap\{R \mid R \in U\}$$

The ringed space $(C, \mathcal{O}_C)$ is a nonsingular curve, and the map $V \to C$ sending $x \mapsto \mathcal{O}_{V,x}$ is regular.

(b) Take C' to be the normalization of C.

□

Lemma 6.0.16. *Let V be an irreducible variety over an algebraically closed field, and let P be a nonsingular point on V. Then the union of the irreducible curves passing through P and nonsingular at P is dense in V.*

Proof. By induction, it suffices to show that the union of the irreducible subvarieties of codimension 1 passing through P and nonsingular at P is dense in V. We can assume V to be affine, and that V is embedded in affine space (this is a local property we are trying to prove). For H a hyperplane passing through

P but not containing $Tgt_P(V)$, $V \cap H$ is nonsingular at P. Let V_H be the irreducible component of $V \cap H$ passing through P, regarded as a subvariety of V, and let Z be a closed subset of V containing all V_H. Let $C_P(Z)$ be the tangent cone to Z at P. Clearly,

$$Tgt_P(V) \cap H = Tgt_P(V_H) = C_P(V_H) \subset C_P(Z) \subset C_P(V) = Tgt_p(V)$$

and it follows that $C_p(Z) = Tgt_P(V)$. As $\dim C_p(Z) = \dim(Z)$ this implies that $Z = V$. □

of Theorem above. Clearly, we can assume k to be algebraically closed. Consider first the case that V has dimension 1. From the lemmas, we know that V can be embedded into a nonsingular complete curve C, and that shows that α extends to a map $\bar{\alpha} : C \times W \to A$. Now, the Rigidity theorem shows that $\bar{\alpha}$ is constant.

In the general case, let C be an irreducible curve on V passing through v_0 and nonsingular at v_0, and let $C' \to C$ be the normalization of C. By composition α defines a morphisms $C' \times W \to A$, which the preceding argument shows to be constant. Therefore, $\alpha(C \times W) = \{a_0\}$ and from the lemma above we know that the set of all C of this form is dense in V, so α is constant on all of V. □

Corollary 6.0.17. *Every rational map $\alpha : G \dashrightarrow A$ from a group variety to an abelian variety is the composite of a homomorphism $h : G \to A$ with a translation.*

Abelian Varieties up to Birational Equivalence

A rational map $\phi : V \dashrightarrow W$ is *dominating* if $Im(\phi_U)$ is dense in W. Then ϕ defines a hommorphism $k(W) \to k(V)$, and every such homomorphism arises from a (unique) dominating rational map.

A rational map is *birational* if the corresponding homomorphism $k(W) \to k(V)$ is an isomorphism. Equivalently, if there exists a rational map $\psi : W \to V$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are both identity maps wherever they are defined. Two varieties V and W are birationally equivalent if there exists a birational map $V \dashrightarrow W$; equivalently, if $k(V) \cong k(W)$.

In general, two varieties can be birationally equivalent without being isomorphic. In fact, every variety (even complete and nonsingular) of dimension > 1 will be birationally equivalent to many nonisomorphic varieties. However, two complete nonsingular curves that are birationally equivalent will be isomorphic. The same is true of abelian varieties:

Theorem 6.0.18. *If two abelian varieties are birationally equivalent, then they are isomorphic (as abelian varieties).*

Proof. Let A and B be abelian varieties. A rational map $\phi : A \dashrightarrow B$ extends to a regular map $A \to B$. If ϕ is birational, its inverse ψ also extends as a regular map, and the composites $\phi \circ \psi$ and $\psi \circ \phi$ will be identity maps because they are on open sets. Hence there is an isomorphism $\alpha : A \to B$ of algebraic varieties. After composing it with translation, it will map 0 to 0, thereby preserving the group structure and giving an isomorphism of abelian varieties. □

Proposition 6.0.19. *Every rational map $\mathbb{A}^1 \dashrightarrow A$ or $\mathbb{P}^1 \dashrightarrow A$ is constant.*

Proof. α extends to a regular map on the whole of $\mathbb{A}^1$. After composing with translation, we may suppose that $\alpha(0) = 0$. Then α is a homomorphism,

$$\alpha(x + y) = \alpha(x) + \alpha(y)$$

but $\mathbb{A}^1 \smallsetminus \{0\}$ is also a group variety, and similarly

$$\alpha(xy) = \alpha(x) + \alpha(y) + c$$

this is absurd, unless α is constant. □

A variety V over an algebraically closed field is said to be *unirational* if there is a dominating rational map $\mathbb{A}^n \dashrightarrow V$ with $n = \dim V$; equivalently, if $k(V)$ can be embedded into $k(X_1, \ldots, X_n)$. A variety over an arbitrary field k is said to be unirational if $V(\bar{k})$ is unirational.

Proposition 6.0.20. *Every rational map $\alpha : V \dashrightarrow A$ from a unirational variety to an abelian variety is constant.*

Proof. We may suppose that k is algebraically closed. By assumption there is a rational map $\mathbb{A}^n \dashrightarrow V$ with dense image, and the composite of this with α extends to a morphism $\beta : \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 \to A$. Recall that a map $V \times W \to A$ can be written as an addition after projection, so there are individual regular maps $\beta_i : \mathbb{P}^1 \to A$ such that $\beta(x_1, \ldots, x_d) = \sum \beta_i(x_i)$ and the lemma shows that the β_i are constant. □

Abelian Varieties are Projective

A projective embedding for an elliptic curve A can be constructed as follows: let $D = P_0$ where P_0 is the zero element of A; for a suitable choice $\{1, x, y\}$ of a basis for $L(3D)$, the map

$$(P \mapsto (x(P) : y(P) : 1)) : A \to \mathbb{P}^2$$

is an isomorphism of A onto a cubic curve in $\mathbb{P}^2$. We now extend this argument to any abelian variety.

For the rest of this mini-section we will assume that k is algebraically closed. Let V be a complete nonsingular variety over k. A nonempty linear equivalence class of effective divisors on V is called a *complete linear system.* Thus, if $\mathfrak{d}$ is a complete linears system and $D_0 \in \mathfrak{d}$, then $\mathfrak{d}$ consists of all effective divisors of the form

$$D_0 + \operatorname{div}(f), \qquad f \in k(V)^\times$$

7 Appendices

7.1 Briefly reviewing: I and II of [Sil09]

First, I will quickly review the basics of algebraic curves. A curve will always mean a projective variety (an integral separated projective scheme of finite type) of dimension one. Generally, we will assume that the curves are smooth (singularities are a whole other story). Other references for this section include [Har77] and [AM69].

7.1.1 Content

Notation:

Ideally, every individual "chapter" will have a notational reminder at its start. I will try to keep everything clear (at least in my mind) and I will explain any notation that is not clear.

K	a perfect field
$\overline{K}$	a fixed algebraic closure of K
$G_{\overline{K}/K}$	the Galois group of $\overline{K}/K$
C	an algebraic curve, and $P \in C$ a point
$\mathcal{O}_C$	the structure sheaf of C
C/K	C is defined over K
$\overline{K}(C)$	the function field of C over $\overline{K}$
$K(C)$	the function field of C over K
$\mathcal{O}_{C,P}$	the local ring of C at P
$\mathfrak{M}_P$	the maximal ideal of $\mathcal{O}_{C,P}$

A quick review of smoothness:

Proposition 7.1.1. *Let C be a curve and $P \in C$ a smooth point. Then, $\mathcal{O}_{C,P}$ is a discrete valuation ring.*

Proof. $P \in C$ is nonsingular, so $dim(\mathfrak{M}_P/\mathfrak{M}_P^2) = dim(C) = 1$. Then, by 9.2 of [AM69], we have that $\mathcal{O}_{C,P}$ is a discrete valuation ring. □

Note. 9.2 of [AM69] also gives us that $\mathfrak{M}_P$ is a principal ideal and that all of the non-zero ideals of $\mathcal{O}_{C,P}$ are powers of $\mathfrak{M}_P$. This means that all $x = up^n$, for any $x \in \mathcal{O}_{C,P}$, u a unit, and p a generator of $\mathfrak{M}_P$.

We have a discrete valuation ring, so let's use its valuation:

Definition 7.1.2. Let C be a curve and $P \in C$ a smooth point.
The **(normalized) valuation** on $\mathcal{O}_{C,P}$ is given by

$$ord_P(f) = sup\{d \in \mathbb{Z} \mid f \in \mathfrak{M}_P^d\}$$

Using $ord_P(f/g) = ord_P(f) - ord_P(g)$ we extend the valuation to $\overline{K}(C)$.

A **uniformizer** for C at P is any function $t \in \overline{K}(C)$ with $ord_P(t) = 1$
(a generator for $\mathfrak{M}_P$)

Proposition 7.1.3. *Let C be a smooth curve and $f \in \overline{K}(C)$, $f \neq 0$. Then there are only finitely many $P \in C$ such that $f(P) = 0$ (zeros) or $1/f(P) = 0$ (poles). Further, if f has no poles, then $f \in \overline{K}$.*

Proof. For the second part, if f has no poles, then $ord_P(f) \geq 0$ for all $P \in C$, so $f \in \mathcal{O}_{C,P}$ for all $P \in C$. Then, by the gluing axiom of sheaves, we can lift to a global section i.e. $f \in \mathcal{O}_C(C)$, but because C is a projective variety, we have that $\mathcal{O}_C(C) = \overline{K}$, so $f \in \overline{K}$.

Note that poles and zeros are equivalent by setting $g = 1/f$, so we just need to check that the set $V(f)$ is finite. First, if $f \in \overline{K}$, then $V(f) = \emptyset$, so assume $f \notin \overline{K}$. We know that all proper closed subsets of C are finite. By hypothesis, we know that $f \neq 0$, so $V(f) \neq C$ (keep in mind that $f \in \overline{K}(C)$ as well). This means that $V(f)$ is finite. □

The next proposition is useful for dealing with curves over fields of positive characteristic.

Proposition 7.1.4. *Let C/K be a curve and let $t \in K(C)$ be a uniformizer at some nonsingular point $P \in C$. Then, $K(C)$ is a finite separable extension of $K(t)$.*

Proof. Since $K(C)$ is finitely generated over K and of transcendence degree 1, we know that $K(C)$ is a finite extension of $K(t)$ because $t \neq K$ (because $t \in \mathfrak{M}_P$). Recall that we assumed that K is a perfect field (way back in the notation section). This means that every finite extension is separable. □

Later, in exercise 2.15, Silverman elaborates on this proposition:

Exercise 1 ([Sil09], 2.15). Claim: Let C/K be a smooth curve, $char(K) = p > 0$, and let $t \in K(C)$. Then, the following are equivalent:

(i) $K(C)$ is a finite separable extension of $K(t)$

(ii) For all but finitely many points $P \in C$, the function $t - t(P)$ is a uniformizer at P.

(iii) $t \notin K(C)^p$

Proof. We will prove each piece individually:

(i)⇒(ii): $K(C)/K(t)$ finite separable implies that $t \notin K$, so, in particular $t \neq 0$, so by Proposition 1.3, t has only finitely many poles and zeros. This means that $ord_P(t - t(P)) = 1$ for all but finitely many $P \in C$.

(ii)⇒(iii): Assume there exists $t_0 \in K(C)$ such that $t_0^p = t$. Then, $t_0^p - t_0(P)^p = (t_0 - t_0(P))^p$ is a uniformizer at P, but $ord_P((t_0 - t_0(P))^p) = p * ord(t_0 - t_0(P)) = 0$. Therefore, $t \notin K(C)^p$.

(iii)⇒(i): Since K is a perfect field for all $f \in K$ then $f \in K^p$. This means that for all $f \in K$ $f \in K(C)^p$, i.e. $t \notin K(C)^p$ implies $t \notin K$. This means that $K(C)/K(t)$ is a finite separable extension. □

As is customary, we now proceed to state a couple facts about morphisms between algebraic curves.

Proposition 7.1.5. *Let C be a curve and $V \subseteq \mathbb{P}^n$ a variety, let $P \in C$ be a smooth point, and let $\phi : C \to V$ be a rational map. Then, ϕ is regular at P. In particular, if C is smooth,then ϕ "extends" to a morphism.*

Note. Rational maps are "morphisms on open sets" and the closed sets are a finite number of points, which we have to "analytically-continue" the morphism over. This is possible because C is a compact Riemann surface.

Proof. Let $\phi = [f_0, ..., f_n]$ for $f_i \in \overline{K}(C)$ and choose a uniformizer $t \in \overline{K}(C)$ at P. Let

$$m = min\{ord_P(f_i)\}$$

Then, $ord_P(t^{-m} f_i) \geq 0$ for all i, and $ord_P(t^{-m} f_j) = 0$ for some j. Therefore, ϕ is regular at P. □

From this we can derive a bijection:

$$K(C) \cup \{\infty\} \leftrightarrow \{\text{maps } C \to \mathbb{P}^1 \text{ defined over } K\}$$

Note. Every $f \in K(C)$ defines a rational map $P \mapsto [1, f(P)]$ with $P \mapsto [0, 1]$ if f has a pole at P. Conversely, $\phi = [f, g] : \mathbb{P}^1 \to C$ gives us f/g, which is "∞" if $g = 0$ (the constant map $[1, 0]$).

Theorem 7.1.6. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Note. This is a conseqeunce of "compactness" i.e. C_1, C_2 are both *projective* curves, meaning *compact* Riemann surfaces.

Proof. Since C_1 and C_2 are projective over K, then they are proper over K, so $\phi(C_1) \subseteq C_2$ is closed. On the other hand, the image of an irreducible set is irreducible (or you could just pullback the disjoint cover), so $\phi(C_1)$ is irreducible *and* closed. This means that $f(C_1) = C_2$ or $f(C_1) = P$ for some $P \in C_2$. □

Theorem 7.1.7. *Let C_1/K and C_2/K be curves.*

(a) Let $\phi : C_1 \to C_2$ be a nonconstant map defined over K. Then, $K(C_1)$ is finite extension of $\phi^* K(C_2)$.

(b) Let $\iota : K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $\phi : C_1 \to C_2$ such that $\phi^* = \iota$

(c) Let $\mathbb{K} \subseteq K(C_1)$ be a subfield of finite index containing K. Then, there exists a smooth curve $\mathfrak{C}/K$ (unique up to K-isomorphism) and a nonconstant map $\phi : C_1 \to \mathfrak{C}$ such that $\phi^* K(\mathfrak{C}) = \mathbb{K}$.

Proof. Assume the hypotheses of the individual theorems:

(a) Since ϕ is nonconstant, $\phi(C_1)$ is dense in C_2, so it induces an injection of function fields $K(C_2) \subseteq K(C_1)$, which are both finitely generated extension fields of transcendence degree 1, so $K(C_1)/K(C_2)$ is finite.

(b) Choose an embedding $C_2 \subseteq \mathbb{P}^n$ and assume without loss of generality that $C_2 \subseteq D(x_0)$. Then

$$\phi = [1, \iota(x_1/x_0), ..., \iota(x_n/x_0)]$$

defines a map from C_1 to C_2 with $\phi^* = \iota$.
Let $\psi = [f_0, ..., f_n] : C_1 \to C_2$ such that $\psi^* = \iota$. Then, for each i,

$$f_i/f_0 = \psi^*(x_i/x_0) = \iota(x_i/x_0)$$

So, $\psi = [1, f_1/f_0, ..., f_n/f_0] = [1, \iota(x_1/x_0), ..., \iota(x_n/x_0)] = \phi$.

(c) A consequence of equivalence of categories for the algebraically closed case. For general (perfect) fields, looking at $G_{\overline{K}/K}$-invariants is the key.

□

Using this equivalence of categories, we can make a couple definitions and have a couple "easy" theorems which follow.

Definition 7.1.8. For a morphism $\phi : C_1 \to C_2$ between two curves, define the **degree of** ϕ as follows:

$$deg(\phi) = [K(C_1) : \phi^* K(C_2)]$$

We say that ϕ is *separable*, *inseparable*, or *purely inseparable* if the field extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $deg_s\phi$ and $deg_i\phi$ respectively.

Theorem 7.1.9. *Let $\phi : C_1 \to C_2$ be a morphism of curves with $deg(\phi) = 1$. Then, ϕ is an isomorphism.*

Proof. By definition, $deg(\phi) = 1$ implies that $[K(C_1) : \phi^* K(C_2)] = 1$, so $\phi^* K(C_2) = K(C_1)$. Hence, from (b) above, for $(\phi^*)^{-1}$ there is a corresponding rational map $\psi : C_2 \to C_1$ such that $\psi^* = (\phi^*)^{-1}$. Further, because C_2 is a smooth curve, ψ is a morphism.
Finally, since $(\psi \circ \phi)^* = \psi^* \circ \phi^* = id_{\overline{K}(C_2)}$ and $(\phi \circ \psi)^* = \phi^* \circ \psi^* = id_{\overline{K}(C_1)}$, the uniqueness assertion of (b) above gives us that $\phi \circ \psi = id_{C_2}$ and $\psi \circ \phi = id_{C_2}$. Hence, ϕ and ψ are isomorphisms. □

We also define a "pushforward" type of map:

Definition 7.1.10. Let $\phi : C_1 \to C_2$ be a nonconstant map of curves defined over K. We use the norm map relative to $\phi^* : K(C_2) \hookrightarrow K(C_1)$ to define a "pushforward" map:

$$\phi_* : K(C_1) \mapsto K(C_2), \qquad \phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}$$

We now do a quick proposition related to hyperelliptic curves which we will use later in chapter X.

Proposition 7.1.11. *Let $f(x) \in K[x]$ with $deg(f) = 4$ and $disc(f) \neq 0$ (i.e. f has no repeated roots). There exists a smooth projective curve $C \subseteq \mathbb{P}^3$ with the following properties:*

(i) $C \cap D(x_0) \cong Z(y^2 - f(x))$.

(ii) Let $f(x) = a_0 + ... + a_4 x^4$, *then* $C \cap Z(x_0) = \{[0, 0, \pm\sqrt{a_4}, 1]\}$

Note. Silverman discusses a "proof" of this proposition on pages 22-23 of [Sil09]. It can be summed up as follows:
For some $f(x) \in K[x]$ of degree d, we consider the affine curve:

$$C_0 : y^2 = f(x)$$

If (x_0, y_0) is a singularity, then $2y_0 = f'(x_0) = 0$, so assuming $disc(f) \neq 0$, we have that C_0 is nonsingular.

We then homogenize the affine equation, getting $C_1 \subseteq \mathbb{P}^2$, but for $deg(f) \geq 4$ we have singularities at infinity, so we blow-up C_1 to get $C \subseteq \mathbb{P}^3$. Obviously, the "original" points are $C \cap D(x_0) = C_0$ and $C \cap Z(x_0) = \{[0, 0, \pm\sqrt{a_4}, 1]\}$.

Now, we want to look at ramification:

Definition 7.1.12. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The *ramification index* of ϕ at P is

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)})$$

Where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$.
If $e_\phi(P) = 1$, then we say that ϕ is *unramified* at P. We say that ϕ us unramified if it is for all $P \in C_1$.

Proposition 7.1.13. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.*

(a) For every $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi)$$

(b) For all but finitely many $Q \in C_2$

$$\#\phi^{-1}(Q) = deg_s(\phi)$$

(c) Let $\psi : C_2 \to C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$

$$e_{\psi\circ\phi}(P) = e_\phi(P) e_{psi}(P)$$

Proof. Taken from [Har77]:

(a)

(b)

(c) Let $t_{\phi P}$ and $t_{\psi\phi P}$ be uniformizers at the indicated points. By definition, the functions

$$t_{\phi P}^{e_\psi(\phi P)} \quad \text{and} \quad \psi^* t_{\psi\phi P}$$

have the same order at P. Applying ϕ^* and taking orders at P yields

$$ord_P(\phi^* t_{\phi P}^{e_\psi(\phi P)}) = ord_P((\psi\phi)^* t_{\psi\phi P})$$

□

Corollary 7.1.14. *A map $\phi : C_1 \to C_2$ is unramified if and only if*

$$\#\phi^{-1}(Q) = deg(\phi) \quad \textit{for all } Q \in C_2$$

Proof. From (a) above, we see that $\#\phi^{-1}(Q) = deg(\phi)$ if and only if

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q)$$

Since $e_\phi(P) \geq 1$, this only happens when each $e_\phi(P) = 1$. □

Remark 3. The proposition above is exactly analogous to the theorems describing the ramification of primes in number fields. Thus let L/K be number fields. Then

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi) \quad \text{is analogous to} \quad \sum e_i f_i = [K : \mathbb{Q}]$$

(b) is analogous to the fact that only finitely many primes of K ramify in L, and (c) gives the multiplicativity of ramification degrees in towers of fields.

Of course, all of these results are merely special cases of basic theorems describing finite extensions of Dedekind domains.

Example 9. Consider the map

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1, \quad \phi([X,Y]) = [X^3(X-Y)^3, Y^5]$$

Then, ϕ is ramified at the points $[0,1]$ and $[1,1]$. Further,

$$e_\phi([0,1]) = 3 \quad \text{and} \quad e_phi([1,1]) = 2$$

so

$$\sum_{P \in \phi^{-1}([0,1])} e_\phi(P) = e_\phi([0,1]) + e_\phi([1,1]) = 5 = deg\phi$$

The Frobenius Map

Assume that $char(K) = p > 0$ and let $q = p^r$. For any polynomial $f \in K[x]$, let $f^{(q)}$ be the polynomial obtained from raising each coefficient of f to the q^{th} power. Then for any curve C/K, we can define a new curve $C^{(q)}/K$ as the curve whose homogeneous ideal is given by

$$I(C^{(q)}) = \langle f^{(q)} \mid f \in I(C) \rangle$$

Furthermore, there is a natural map $\phi : C \to C^{(q)}$, called the *q^th-power Frobenius morphism*, given by

$$\phi([x_0, ..., x_n]) = [x_0^q, ..., x_n^q$$

To see that ϕ maps C to $C^{(q)}$, it suffices to show that for every $P \in C$, $\phi(P)$ is a zero of each generator $f^{(q)}$ of $I(C^{(q)})$. We compute

$$\begin{aligned} f^{(q)}(\phi(P)) &= f^{(q)}(x_0^q, ..., x_n^q) \\ &= (f(x_0, ..., x_n))^q && \text{since } char(K) = p \\ &= 0 && \text{since } f(P) = 0 \end{aligned}$$

Example 10. Let C be the curve in $\mathbb{P}^2$ given by

$$C : Y^2Z = X^2 + aXZ^2 + bZ^3$$

Then $C^{(q)}$ is given by

$$C^{(q)} : Y^2Z = X^2 + a^qXZ^2 + b^qZ^3$$

Next we will describe certain properties of the Frobenius map.

Proposition 7.1.15. *Let K be a field of characteristic $p > 0$, let $q = p^r$, let C/K be a curve, and let $\phi : C \to C^{(q)}$ be the q^th-power Frobenius morphism.*

(a) $\phi^* K(C^{(q)}) = K(C)^q = \{f^q : f \in K(C)\}$

(b) ϕ is purely inseparable

(c) $deg\phi = q$

Proof. (Note: we are assuming that K is perfect. If K is not perfect, then (b) and (c) remain true, but (a) must be modified.)

(a) Recall that $K(C)$ can be described as consisting of quotients f/g of homogeneous polynomials of the same degree, we see that $\phi^* K(C^{(q)})$ is the subfield of $K(C)$ given by the quotients

$$\phi^* \left(\frac{f}{g}\right) = \frac{f(x_0^q, ..., x_n^q)}{g(y_0^q, ..., y_n^q)}$$

Similarly, $K(C)^q$ is the subfield of $K(C)$ given by the quotients

$$\frac{f(x_0, ..., x_n)^q}{g(y_0, ..., y_n)^q}$$

However, since K is perfect, we know that every element of K is a q^th power, so

$$(K[x_0, ..., x_n])^q = K[x_0^q, ..., x_n^q]$$

Thus, $K(C)^q = K(C^{(q)})$.

(b) Immediate from (a).

(c) Taking finite extensions of K if necessary, we may assume that there is a smooth point $P \in C$ with $t \in K(C)$ a uniformizer at P. Then, we know that $K(C)/K(t)$ is separable. Thereby, because we know that $K(C)/K(C)^q$ is purely inseparable, then $K(C) = K(C)^q(t)$, so

$$deg\phi = [K(C)^q(t) : K(C)^q]$$

Now, $t^q \in K(C)^q$, so in order to prove that $deg\phi = q$, we need merely to show that $t^{q/p} \notin K(C)^q$. Assuming $t^{q/p} = f^q$ for some $f \in K(C)$, then

$$\frac{q}{p} = ord_P(t^{q/p}) = q * ord_P(f)$$

which is impossible, since $ord_P(f)$ must be an integer.

□

Corollary 7.1.16. *Every map $\psi : C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as*

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

where $q = deg_i(\psi)$, the map ϕ is the q^th-power Frobenius map, and the map λ is separable.

Proof. Let $\mathbb{K}$ be the separable closure of $\psi^*K(C_2)$ in $K(C_1)$. Then $K(C_1)/\mathbb{K}$ is purely inseparable of degree q, so $K(C_1)^q \subseteq \mathbb{K}$. From (a) and (c) above, we have

$$K(C_1)^q = \phi^*(K(C_1^{(q)})) \quad \text{and} \quad [K(C_1) : \phi^*(K(C_1^{(q)}))] = q$$

Comparing degrees we see that $\mathbb{K} = \phi^*(K(C_1^{(q)}))$. We now have a tower of function fields

$$K(C_1)/\phi^*K(C_1^{(q)})/\psi^*K(C_2)$$

and by equivalence of categories, this corresponds to the factorization of maps above. □

Divisors

Note. A divisor group can be defined over a general scheme, but there are a couple different definitions, one of which only works on integral schemes. The general idea is that a divisor is a hyperplane aka a subscheme of codimension one, which can also be thought of as corresponding to vector bundles (aka locally free coherent sheaves)(aka a piece of the Picard group). Generalizations of this include the group of algebraic cycles (for divisors) and the Grothendieck group (aka K-groups)(for vector bundles).

"Specifications" of this definition include the group of fractional ideal (i.e. the ideal class group) and the adeles $\mathbb{A}$ (and the ideles $\mathbb{I}$, which then generalize to $GL_n(\mathbb{A})$).

Here is the definition to keep in mind for elliptic curves:

Definition 7.1.17. The *divisor group of a curve* C, denoted $Div(C)$, is the free abelian group generated by the points of C.

Thus a divisor $D \in Div(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.

The *degree of* D is defined by

$$deg(D) = \sum_{P \in C} n_P$$

The *divisors of degree 0* form a subgroup of $Div(C)$, which we denote by

$$Div^0(C) = \{D \in Div(C) : deg(D) = 0\}$$

If C is defined over K, we let $G_{\overline{K}/K}$ act on $Div(C)$ and $Div^0(C)$ in the obvious way,

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

Then D is defined over K if $D^\sigma = D$ for all $\sigma \in G_{\overline{K}/K}$.

We note that if $D = n_1(P_1) + ... + n_r(P_r)$ with $n_1, ..., n_r \neq 0$, then to say that D is defined over K is not to say that $P_1, ..., P_r \in C(K)$, just that $G_{\overline{K}/K}$ permutes the P_i appropriately (e.g. there could be some form of cancellation).

We denote the *group of divisors over* K by $Div_K(C)$ and $Div^0_K(C)$.

Assume now that the curve C is smooth, and let $f \in \overline{K}(C)^\times$. Then, we can associate to f the divisor

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

If $\sigma \in G_{\overline{K}/K}$ it is easy to see that

$$div(f^\sigma) = (div(f))^\sigma$$

In particular, if $f \in K(C)$, then $div(f) \in Div_K(C)$.

Since each ord_P is valuation map

$$div : \overline{K}(C)^\times \to Div(C)$$

is a homomorphism of abelian groups. It is analogous to the map that sends an element of a number field to the corresponding fractional ideal. This prompts the following definitions.

Definition 7.1.18. A divisor $D \in Div(C)$ is *principal* if it has the form $D = div(f)$ for some $f \in \overline{K}(C)^\times$.

Two divisors are *linearly equivalent*, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal.

The *divisor class group* (or *Picard group*) of C, is $Pic(C) = Div(C)/\sim$. We let $Pic_K(C)$ be the subgroup of $Pic(C)$ fixed by $G_{\overline{K}/K}$

Proposition 7.1.19. *Let C be a smooth curve and let $f \in \overline{K}(C)^\times$.*

(a) $div(f) = 0$ if and only if $f \in \overline{K}^\times$

(b) $deg(div(f)) = 0$

Proof. If $div(f) = 0$, then f has no poles, so the associated map $f : C \to \mathbb{P}^1$ is constant, so $f \in \overline{K}^\times$. The converse is clear.
Using the map $f : C \to \mathbb{P}^1$ again, we see that

$$deg(div(f)) = deg f^*((0) - (\infty)) = deg(f) - deg(f) = 0$$

□

Claim. On $\mathbb{P}^1$, every divisor of degree 0 is principal.

Proof. Suppose that $D = \sum n_P(P)$ has degree 0. Writing $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$, we see that D is the divisor of the function

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}$$

Note that $\sum n_P = 0$ guarantees that this function is in $K(\mathbb{P}^1)$. It follows that the degree map $deg : Pic(\mathbb{P}^1) \to \mathbb{Z}$ is an isomorphism. The converse is also true, so if C is a smooth curve and $Pic(C) \cong \mathbb{Z}$, then $C \cong \mathbb{P}^1$ □

There exists an exact sequence

$$1 \to \overline{K}^\times \to \overline{K}(C)^\times \xrightarrow{div} Div^0(C) \to Pic^0(C) \to 0$$

This sequence is the function field equivalent of the following fundamental exact sequence in algebraic number theory, which for a number field K reads:

$$1 \to SL_1(K) \to GL_1(K) \to Frac(K) \to CL(K) \to 1$$

Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves. As we have seen, ϕ induces maps on the function fields of C_1 and C_2,

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1) \quad \text{and} \quad \phi_* : \overline{K}(C_1) \to \overline{K}(C_2)$$

(Note: the "pushforward" uses the norm map, $(\phi^*)^{-1} \circ N_{\overline{K}(C_1)/\phi^*\overline{K}(C_2)}$
We can then define maps of divisors as follows

$$\phi^* : Div(C_2) \to Div(C_1), \qquad \phi_* : Div(C_1) \to Div(C_2)$$
$$(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P), \qquad (P) \mapsto (\phi P)$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors

Proposition 7.1.20. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.*

(a) $deg(\phi^* D) = (deg\phi)(deg D)$ for all $D \in Div(C_2)$

(b) $\phi^*(div(f)) = div(\phi^* f)$ for all $f \in \overline{K}(C_2)^\times$

(c) $deg(\phi_* D) = deg(D)$ for all $D \in Div(C_1)$

(d) $\phi_*(div(f)) = div(\phi_* f)$ for all $f \in \overline{K}(C_1)$

(e) $\phi_* \circ \phi^*$ acts as multiplication by $deg(\phi)$ on $Div(C_2)$

(f) If $\psi : C_2 \to C_3$ is another map then

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \quad \text{and} \quad (\psi \circ \phi)_* = \psi_* \circ \phi_*$$

Differentials

Sheaves of differential forms are how we carry the ideas of linearization from calculus to algebraic geometry. In addition, it helps us identify if algebraic maps are separable.

We will give two different definitions.

Definition 7.1.21 ("Easy")**.** Let C be a curve. The *space of (meromorphic) differential forms* on C, denoted by Ω_C is the $\overline{K}$-vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to the relations

(i) $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(C)$

(ii) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$

(iii) $da = 0$ for all $a \in \overline{K}$

More generally we have,

Definition 7.1.22 (Sheaves)**.** Given a morphism $f : X \to S$ of schemes, the *cotangent sheaf* on X (over S) is $\Omega_{X/S}$ with the universal property that for any $\mathcal{O}_X$-module F,

$$Hom_{\mathcal{O}_X}(\Omega_{X/S}, F) \cong Der_S(\mathcal{O}_X, F)$$

Where the second set is the set of S-derivations (look at rules above).

Note. There are two important exact sequences to keep in mind:

1. If $S \to T$ is a morphism of schemes, then

$$f * \Omega_{S/T} \to \Omega_{X/T} \to \Omega_{X/S} \to 0$$

2. If Z is a closed subscheme of X with ideal sheaf $\mathcal{I}$, then

$$\mathcal{I}/\mathcal{I}^2 \to \Omega_{X/S} \otimes_{\mathcal{O}_X} \mathcal{O}_Z \to \Omega_{Z/S} \to 0$$

Also, remember that an algebraic variety is smooth of dimension n if and only if the cotangent sheaf is locally free of rank n.

In addition, letting $\mathcal{I}$ denote the ideal sheaf of $\Delta_S(X) \subseteq W \subseteq X \times_S X$ (the diagonal is locally closed, so $\Delta_S(X)$ is closed in W and W is open in $X \times_S X$), we have the following property:

$$\Omega_{X/S} = \Delta^*(\mathcal{I}/\mathcal{I}^2)$$

Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. The associated function field map $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ induces a map on differentials,

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}, \quad \phi^*\left(\sum f_i dx_i\right) = \sum (\phi^* f_i) d(\phi^* x_i)$$

This map provides a useful criterion for determining when ϕ is separable.

Proposition 7.1.23. *Let C be a curve.*

(a) Ω_C is a 1-dimensional $\overline{K}(C)$-vector space.

(b) Let $x \in \overline{K}(C)$. Then dx is a $\overline{K}(C)$-basis for Ω_C if and only if $\overline{K}(C)/\overline{K}(x)$ is a finite separable extension.

(c) Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. Then ϕ is separable if and only if the map

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

is injective.

Proposition 7.1.24. *Let C be a curve, let $P \in C$, and let $t \in \overline{K}(C)$ be a uniformizer at P*

(a) For every $\omega \in \Omega_C$ there exists a unique function $g \in \overline{K}(C)$, depending on ω and t, satisfying $\omega = gdt$. We denote g by ω/dt

(b) Let $f \in \overline{K}(C)$ be regular at P. Then df/dt is also regular at P

(c) Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity $ord_P(\omega/dt)$ depends only on ω and P, independent of choice of uniformizer t. We call this value the order of ω at P and denote it by $ord_P(\omega)$

(d) Let $x, f \in \overline{K}(C)$ with $x(P) = 0$, and let $p = char(K)$. Then

$$\begin{cases} ord_P(fdx) = ord_P(f) + ord_P(x) - 1 & \text{if } p = 0 \text{ or } p \nmid ord_P(x) \\ ord_P(fdx) \geq ord_P(f) + ord_P(x) & \text{if } p > 0 \text{ and } p \mid ord_P(x) \end{cases}$$

Definition 7.1.25. Let $\omega \in \Omega_C$. The divisor associated to ω is

$$div(\omega) = \sum_{P \in C} ord_P(\omega)(P) \in Div(C)$$

The differential $\omega \in \Omega_C$ is *regular* (or *holomorphic*) if

$$ord_P(\omega) \geq 0 \quad \text{for all } P \in C$$

It is *nonvanishing* if

$$ord_P(\omega) \leq 0 \quad \text{for all } P \in C$$

Remark 4. For any $\omega_1, \omega_2 \in \Omega_C$ (nonzero), there exists $f \in \overline{K}(C)^\times$ such that $\omega_1 = f\omega_2$. Thus,

$$div(\omega_1) = div(f) + div(\omega_2)$$

so the following definition makes sense:

Definition 7.1.26. The *canonical divisor class of* C is the image in $Pic(C)$ of $div(\omega)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a *canonical divisor*.

The Riemann-Roch Theorem

Let C be a curve. We put a partial order on $Div(C)$ in the following way

Definition 7.1.27. A divisor $D = \sum n_P(P)$ is *positive* (or *effective*), denoted by $D \geq 0$ if $n_P \geq 0$ for every $P \in C$. Similarly, for any two divisors $D_1, D_2 \in Div(C)$, we write $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

Example 11. Let $f \in \overline{K}(C)^\times$ be a function that is regular everywhere except at one point $P \in C$, and suppose that it has a pole of order at most n at P. These requirements on f may be succinctly summarized by the inequality

$$div(f) \geq -n(P)$$

Similarly,

$$div(f) \geq (Q) - n(P)$$

says that in addition, f has a zero at (Q). Thus divisorial inequalities are a useful tool for describing poles and zeros of functions.

Definition 7.1.28. Let $D \in Div(C)$. We associate to D the set of functions

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^\times \mid div(f) \geq -D\} \cup \{0\}$$

The set $\mathcal{L}(D)$ is a finite-dimension $\overline{K}$-vector space, and we denote $\ell(D) := dim_{\overline{K}}(\mathcal{L}(D))$

Proposition 7.1.29. *Let $D \in Div(C)$.*

(a) If $deg(D) < 0$, then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$

(b) $\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space.

(c) If $D' \in Div(C)$ is linearly equivalent to D, then

$$\mathcal{L}(D) \cong \mathcal{L}(D')$$

Proof. Let $D \in Div(C)$.

(a) Let $f \in \mathcal{L}(D)$ with $f \neq 0$. Then

$$0 = deg(div(f)) \geq deg(-D) = -deg(D)$$

so $deg(D) \geq 0$.

(b) $\mathcal{L}(D)$ is obviously a $\overline{K}(C)$-vector space w/r/t pointwise addition of functions and usual scalar multiplication.

AWLOG that $D = (P)$ for some $P \in C$, then $deg(D) = 1$ and we can see that $\mathcal{L}(D)$ is (at most) generated by a function f with a pole at P and a constant function. Since $deg(D)$ is finite for all $D \in Div(C)$, we can see that $\mathcal{L}(D)$ is finite-dimensional.

(c) If $D = D' + div(g)$, then the following map is an isomorphism

$$\mathcal{L}(D) \to \mathcal{L}(D'), \quad f \mapsto fg$$

□

Example 12. Let $K_C \in Div(C)$ be a canonical divisor on C, say $K_C = div(\omega)$. Then each function $f \in \mathcal{L}(K_C)$ has the property that $div(f\omega) \geq 0$. In other words, $f\omega$ is holomorphic. Conversely, if the differential $f\omega$ is holomorphic, then $f \in \mathcal{L}(K_C)$. Since every differential on C has the form $f\omega$ for some f, we have established an isomorphism of $\overline{K}$-vector spaces

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C \mid \omega \text{ is holomorphic}\}$$

Theorem 7.1.30 (Riemann-Roch)**.** *Let C be a smooth curve and let K_C be a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every $D \in Div(C)$,*

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

Proof. The divisor $K_C - D$ corresponds to the invertible sheaf $\omega_C \otimes \mathcal{L}(D)^\vee$. Since C is projective, we can apply Serre duality to get that $H^0(C, \omega_C \otimes \mathcal{L}(D)^\vee)$ is dual to $H^1(C, \mathcal{L}(D))$. Therefore, we see that we are relating the Euler characteristic

$$\chi(\mathcal{L}(D)) = deg(D) + 1 - g$$

First, we consider the case $D = 0$, so $\mathcal{L}(D) = \mathcal{O}_C$:

$$dim(H^0(C, \mathcal{O}_C)) - dim(H^1(C, \mathcal{O}_C)) = 0 + 1 - g$$

This is true, because $H^0(C, \mathcal{O}_C) = \overline{K}$ for any projective variety and $dim(H^1(C, \mathcal{O}_C) = g$ by definition.

Next, let $D \in Div(C)$ and $P \in C$. We will show that the formula is true for D if and only if it is true for $D + (P)$.

We consider P as a closed subvariety of C. Its structure sheaf is a skyscraper sheaf $\overline{K}$ at P, which we denote by $\overline{K}(P)$, and its ideal sheaf is $\mathcal{L}(-P)$. Therefore, we have an exact sequence,

$$0 \to \mathcal{L}(-P) \to \mathcal{O}_C \to \overline{K}(P) \to 0$$

Tensoring with $\mathcal{L}(D + (P))$ (b/c it is locally free of rank 1) we get

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D + (P)) \to \overline{K}(P) \to 0$$

Note that $deg(D + (P)) = deg(D) + 1$, the Euler characteristic is additive on short exact sequences, and $\chi(\overline{K}(P)) = dim(H^0(P, \overline{K}(P)) = dim(\overline{K}) = 1$, so

$$\chi(\mathcal{L}(D + (P)) = \chi(\mathcal{L}(D)) + 1$$

□

The following corollary gives different useful forms of Riemann-Roch:

Corollary 7.1.31. *Let C be a smooth curve, $D \in Div(C)$, and K_C a canonical divisor on C. Then,*

(a) $\ell(K_C) = g$

(b) $deg(K_C) = 2g - 2$

(c) If $deg(D) > 2g - 2$, *then*

$$\ell(D) = deg(D) - g + 1$$

Proof. All proofs follow from Riemann-Roch as follows:

(a) Let $D = 0$, then $\ell(0) - \ell(K_C) = -g + 1$, so $\ell(K_C) = g$ (b/c $\mathcal{L}(0) = \overline{K}$)

(b) Let $D = K_C$, then $\ell(K_C) - \ell(0) = deg(K_C) - g + 1$. Thus, by part (a), $deg(K_C) = 2g - 2$.

(c) By part (b), we have that $deg(K_C - D) = deg(K_C) - deg(D) < 0$, so $\ell(K_C - D) = 0$, giving us the desired equation from Riemann-Roch.

□

Example 13. Let $C = \mathbb{P}^1$. We know that there are no holomorphic differentials on C, so $\ell(K_C) = 0$. Then, part (a) above gives us that $g(\mathbb{P}^1) = 0$ and Riemann-Roch read

$$\ell(D) - \ell(-2(\infty) - D) = deg(D) + 1$$

In particular, if $deg(D) \geq -1$, then

$$\ell(D) = deg(D) + 1$$

7.1.2 Exercises

All from chapter II of [Sil09]:

1.

7.2 "An Algebro-Geometric Tool Box"

Here are the pieces from [Hid12] which are used.

7.3 The Classical Riemann Zeta Function

Definition 7.3.1. A function $f : \mathbb{R} \to \mathbb{C}$ is a **Schwarz function** if all of its derivatives are rapidly decreasing, i.e. for all $r \geq 0$ and $n \geq 1$ we have

$$\lim_{x\to\infty} x^n f^{(r)} = 0$$

The **Schwarz space** $\mathcal{S} = \mathcal{S}(\mathbb{R})$ is the set of all Schwarz functions.

Example: If $f \in C^\infty$ has compact support, then $f \in \mathcal{S}$.

Definition 7.3.2. Let $f \in \mathcal{S}(\mathbb{R})$. Define the **Fourier transform** of f as:

$$\hat{f}(y) = \int_{\mathbb{R}} f(x) e^{-2\pi i x y} dx$$

Note: $\hat{f} \in \mathcal{S}(\mathbb{R})$

Lemma 7.3.3 (Fourier Inversion Formula)**.** *If $f \in \mathcal{S}(\mathbb{R})$, then $\hat{\hat{f}}(x) = f(-x)$*

Lemma 7.3.4 (Poisson Summation Formula)**.** *If $f \in \mathcal{S}(\mathbb{R})$, then*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(x)$$

These formulas will be generalized later, but first we will show their usefulness in the context of $\mathbb{R}$ and $\mathbb{C}$.

The Riemann Zeta Function

Now, we will look at (arguably) the most important zeta function, and prove that is has *analytic continuation* to all of $\mathbb{C}$ and that is satisfies certain *functional equations*. These are key terms to remember, as we want to prove these two things when it comes to just about any L-function. It is always good to keep the Riemann zeta function in mind, as it is the base example.

Definition 7.3.5. The **Riemann zeta function** defined for $Re(s) > 1$ is

$$\zeta(s) := \sum_{n\geq 0} n^{-s} = \prod_{\text{prime } p} (1 - p^{-s})^{-1}$$

We need 3 more functions for Riemann's proof:

Definition 7.3.6. The **gamma function** (convergent for $Re(s) > 0$) is:

$$\Gamma(s) \coloneqq \int_0^\infty e^{-t} t^s \frac{dt}{t}$$

We then use the gamma function to define the **completed zeta function**:

$$\xi(s) \coloneqq \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

Important: Note that $\Gamma(s)$ consists of

1. An *additive character* $e^{-t} : \mathbb{R} \to \mathbb{T}$
2. A *multiplicative (quasi)-character* $t^s : \mathbb{R}^\times \to \mathbb{C}^\times$
3. A (multiplicative) *Haar measure* $\frac{dt}{t}$ on $\mathbb{R}^\times$

Recall that a **Haar measure** is a translation invariant measure on locally compact topological groups. Generalizing this, and the characters, to other locally compact topological groups (spoiler: $\mathbb{Q}_p$) is what we use later for our "global" analysis of the zeta function.

Lemma 7.3.7. *In addition, the gamma function has the following properties:*

1. $\Gamma(s+1) = s\Gamma(s)$
2. $\Gamma(s)$ *extends to a meromorphic function on* $\mathbb{C}$
3. $\Gamma(s)$ *has no zeroes*
4. $\Gamma(n) = (n-1)!$ *for all* $n \in \mathbb{N}$
5. $\Gamma(1/2) = \sqrt{\pi}$

Proof. Left to the reader as an exercise ;) □

The final one comes with a proof of its functional equation

Definition 7.3.8. The **theta function** for $t > 0$ in $\mathbb{R}$ is:

$$\Theta(t) \coloneqq \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t}$$

Lemma 7.3.9 (Functional equation for Θ)**.** *For all $t \in \mathbb{R}$ such that $t > 0$, we have*

$$\Theta(t) = t^{-1/2} \Theta\left(\frac{1}{t}\right)$$

Proof. Let $f \in \mathcal{S}(\mathbb{R})$ and $c \neq 0$. Then,

$$\int_{\mathbb{R}} f(x/c)e^{-2\pi ixy}dx = \frac{1}{c}\int_{\mathbb{R}} f(u)e^{-2\pi iu(cy)}du$$

So, the Fourier transform of $f(x/c)$ is $c\hat{f}(cy)$.
Let $f(x) = e^{-\pi x^2}$, then:

$$\hat{f}(y) = \int_{\mathbb{R}} e^{-\pi x^2}e^{-2\pi ixy}dx = e^{-2\pi y^2} = f(y)$$

So, letting $c = t^{-1/2}$ and denoting $f_t(x) \coloneqq f(xt^{1/2})$ we get

$$f_t(x) = e^{-\pi tx^2} \Rightarrow \hat{f}_t(y) = t^{-1/2}e^{-\pi(1/t)y^2}$$

Then, applying the Poisson Summation formula to f_t we get:

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} t^{-1/2}e^{-\pi n^2(1/t)}$$

$$\Theta(t) = t^{-1/2}\Theta(1/t)$$

□

Theorem 7.3.10 (Riemann, 1860)**.** *Let $\xi(s) \coloneqq \pi^{-s/2}\Gamma(s/2)\zeta(s)$, then*

1. $\xi(s) = \xi(1-s)$.
2. *$\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$ with a simple pole at $s = 1$.*

Proof. First, we look at the summands of $\zeta(s)$.

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\sum_{n\geq 0} n^{-s}$$

$$\pi^{-s/2}\Gamma(s/2)n^{-s} = \pi^{-s/2}n^{-s}\int_0^\infty e^{-x}x^{s/2}\frac{dx}{x}$$

Then we substitute $x = \pi n^2 t$:

$$\pi^{-s/2}n^{-s}\int_0^\infty e^{-x}x^{s/2}\frac{dx}{x} = \int_0^\infty e^{-\pi n^2 t}t^{s/2}\frac{dt}{t}$$

Then we sum over the natural numbers:

$$\xi(s) = \int_0^\infty \Theta(t)t^{s/2}\frac{dt}{t}$$

But, $e^{-\pi n^2 t}$ is even, so $1 + 2\Theta(t) = \Theta(t)$, which gives us

$$\xi(s) = \int_0^\infty \left(\frac{\Theta(t) - 1}{2}\right) t^{s/2} \frac{dt}{t}$$

The catch is that we just interchanged the sum and integral, but we know that it is well behaved for $Re(z) > 1$ ($z \in \mathbb{C}$), so we have the following non-problematic integral for $(1, \infty)$:

$$I(s) \coloneqq \int_1^\infty \left(\frac{\Theta(t) - 1}{2}\right) t^{s/2} \frac{dt}{t} = \int_1^\infty \Theta(t) t^{s/2} \frac{dt}{t}$$

Along with this, we have the "problematic" integral for $(0, 1)$, where we substitute $t \mapsto 1/t$:

$$\int_0^1 \left(\frac{\Theta(t) - 1}{2}\right) t^{s/2} \frac{dt}{t} = \int_1^\infty \left(\frac{\Theta(1/t) - 1}{2}\right) t^{-s/2} \frac{dt}{t}$$

Then, we use the functional equation, $\Theta(1/t) = t^{1/2}\Theta(t)$

$$= \int_1^\infty \left(\frac{t^{1/2}\Theta(t) - 1}{2}\right) t^{-s/2} \frac{dt}{t}$$

$$= \int_1^\infty \left(\frac{\Theta(t) - 1}{2}\right) t^{(1-s)/2} \frac{dt}{t} + \frac{1}{2}\int_1^\infty t^{(1-s)/2} \frac{dt}{t} + \frac{1}{2}\int_0^\infty t^{-s/2} \frac{dt}{t}$$

$$= I(1 - s) - \frac{1}{1 - s} - \frac{1}{s}$$

Finally, putting it all back together we get (for $Re(s) > 1$):

$$\xi(s) = I(s) + I(1 - s) - \frac{1}{1 - s} - \frac{1}{s}$$

This gives us the functional equation $\xi(s) = \xi(1 - s)$, which then lets us extend ξ to the entire plane $\mathbb{C}$ with simple poles at $s = 0, 1$.
We then note that $\pi^{-s/2}\Gamma(s/2)$ has poles at $0, -2, -4, ...$, so when we divide $\xi(s)$ by $\pi^{-s/2}\Gamma(s/2)$ to get $\zeta(s)$ we see that it is meromorphic with a simple pole at $s = 1$, along with "trivial" zeros at $-2, -4, -6, ...$ with other zeroes in the "critical strip"$\coloneqq \{z \in \mathbb{C} : 0 \leq Re(z) \leq 1\}$. □

7.4 Dirichlet L-functions

The first generalizations of the Riemann zeta function was the idea of Dirichlet L-functions, associated to Dirichlet characters:

Definition 7.4.1. Let N be an integer. A *Dirichlet character* modulo N is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that

$$|\chi(n)| = \begin{cases} 1 & \text{if } gcd(n, N) = 1 \\ 0 & \text{otherwise} \end{cases}$$

and $\chi(nm) = \chi(n)\chi(m)$

To obtain a Dirichlet character just follow these easy steps,

1. Start with a character $\chi_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{T}$
2. Extend the character by zero to $\mathbb{Z}/N\mathbb{Z}$
3. Compose this function with the canonical map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$

7.5 Zeta Function on $\mathbb{A}$

This appendix covers the results of Tate's Thesis.

7.6 L-Series for Elliptic Curves

The following theorem is a proof of the Weil Conjectures for elliptic curves

Theorem 7.6.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there is an $a \in \mathbb{Z}$ such that*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

Further, we have a functional equation

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T)$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T) \quad \textit{with} \quad |\alpha| = |\beta| = \sqrt{q}$$

Proof. First, remember that we have the Tate module representation for endomorphisms of E:

$$End(E) \to End(T_\ell(E)), \quad \psi \mapsto \psi_\ell$$

Which we can then use to calculating values

$$det(\psi_\ell) = deg(\psi) \quad \text{and} \quad tr(\psi_\ell) = 1 + deg(\psi) - deg(1 - \psi)$$

In particular, both of these values are in $\mathbb{Z}$ and are independent of ℓ.

Next, we use the q^th-power Frobenius endomorphism $\phi : E \to E$ defined by $(x, y) \mapsto (x^q, y^q)$. Note that $(1 - \phi)$ is a separable morphism, so

$$\#E(\mathbb{F}_q) = \# \ker(1 - \phi) = deg(1 - \phi)$$

We then use our representation to compute

$$det(\phi_\ell) = deg(\phi) = q$$

$$tr(\phi_\ell) = 1 + deg(\phi) - deg(1-\phi) = 1 + q - \#E(\mathbb{F}_q)$$

To ease notation, we denote $a \coloneqq tr(\phi_\ell)$.
Hence, the characteristic polynomial of ϕ_ℓ is

$$det(T - \phi_\ell) = T^2 - tr(\phi_\ell)T + det(\phi_\ell) = T^2 - aT + q$$

Since the characteristic polynomial has coefficients in $\mathbb{Z}$, we can factor it over $\mathbb{C}$ as

$$det(T - \phi_\ell) = T^2 - aT + q = (T - \alpha)(T - \beta)$$

For every rational number $m/n \in \mathbb{Q}$, we have

$$det\left(\frac{m}{n} - \phi_\ell\right) = \frac{det(m - n\phi_\ell)}{n^2} = \frac{deg(m - n\phi)}{n^2} \geq 0$$

Thus, the quadratic polynomial $det(T - \phi_\ell)$ is nonnegative for all $T \in \mathbb{R}$, so either it has complex conjugate roots or it has a double root. In either case we have $|\alpha| = |\beta|$, and

$$\alpha\beta = det(\phi_\ell) = deg(\phi) = q$$

Similarly, for each integer $n \geq 1$, the $(q^n)^t h$-power Frobenius morphism satisfies $\#E(\mathbb{F}_{q^n} = deg(1 - \phi^n)$. It follows (from Jordan normal form with α, β in the diagonal) that the characteristic polynomial of ϕ_ℓ^n is given by

$$det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n)$$

In particular,

$$\begin{aligned}\#E(\mathbb{F}_{q^n} &= deg(1 - \phi^n)\\ &= det(1 - \phi_\ell^n)\\ &= 1 - \alpha^n - \beta^n + q^n\end{aligned}$$

Now, we compute

$$\begin{aligned}\log\, Z(E/\mathbb{F}_q; T) &= \sum_{n\geq 1} \frac{\#E(\mathbb{F}_{q^n})T^n}{n}\\ &= \sum_{n\geq 1} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n}\\ &= -log(1 - T) + log(1 - \alpha T) + log(1 - \beta T) - log(1 - qT)\end{aligned}$$

Hence, by usual log calculations,

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

Using this and the fact that

$$a = \alpha + \beta = tr(\phi_\ell) = 1 + q - deg(1-\phi) \in \mathbb{Z}$$

We get the results we want after a simple calculation of the functional equation. □

Note. The Weil Conjecture for elliptic curves are "easy" for three reasons:

1. Elliptic curves are 1-dimensional, so we only have to worry about the first cohomology group, $H^1_{\acute{e}t}(E, \mathbb{Z}_\ell)$.
2. Tate modules are dual to this cohomology group, so we can calculate using these elementary methods.
3. Tate modules "work" because elliptic curves are abelian varieties.

In a more general reflection, many conjectures and theorems in modern number theory are generalizations of ideas which we get from the concrete (and well-behaved) case of elliptic curves.

Note. All reductions in the following part are done with respect to the *Weierstrass minimal model of* E (over $\mathcal{O}_K$). By this we mean the integral Weierstrass equation with minimal discriminant Δ. This is done w/r/t the valuation at all primes (i.e. all finite places). Note that a local minimal Weierstrass model always exists for some place, but the global minimal Weierstrass model might not exist.

Let E/K be an elliptic curve and let $v \in M_K$ be a finite place at which E has good reduction, $\tilde{E}_v$. We denote the residue field of K at v by k_v, with $q_v = \#k_v$ and $k_{v,n}$ the unique extension of k_v of degree n.

Definition 7.6.2. The *local zeta function* of $\tilde{E}_v/k_v$ is

$$Z(\tilde{E}_v/k_v;T) = exp\left(\sum_{n\geq 1} \#\tilde{E}_v(k_{v,n})\frac{T^n}{n}\right)$$

We know from above that $Z(\tilde{E}_v/k_v;T)$ is a rational function

$$Z(\tilde{E}_v/k_v;T) = \frac{L_v(T)}{(1-T)(1-q_vT)}$$

Where

$$L_v(T) = 1 - a_vT + q_vT^2 \in \mathbb{Z}[T] \quad \text{and} \quad a_v = q_v + 1 - \#\tilde{E}_v(k_v)$$

We extend the definition of $L_v(T)$ to the case that E has bad reduction by setting

$$L_v(T) = \begin{cases} 1-T & \text{if } E \text{ has split multiplicative reduction at } v \\ 1+T & \text{if } E \text{ has nonsplit multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v \end{cases}$$

Then, in all cases, we have the relation

$$L_v(1/q_v) = \#\tilde{E}_{ns}(k_v)/q_v$$

Using this we create...

Definition 7.6.3. The *L-series of E/K* is defined by the Euler product

$$L_{E/K}(s) = \prod_{v \in M_K^0} L_v(q_v^{-s})^{-1}$$

There are many conjectures involving the L-series of an elliptic curve, including...

Conjecture 7.6.4. *The L-series $L_{E/K}(s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2-s$.*

Deuring and Weil showed this to be true for elliptic curves with complex multiplication, in which case $L_{E/K}$ is equal to a (product of) Hecke L-series with Hecke characters (using the fact that complex multiplication gives abelian extensions of certain quadratic imaginary extensions of $\mathbb{Q}$). Eichler and Shimura proved the conjecture for modular elliptic curves $E/\mathbb{Q}$, so the Modularity theorem (Wiles et al.) proves the conjecture for all elliptic curves over $\mathbb{Q}$.

7.7 Reciprocity

Here we look at Artin Reciprocity and connect it to a relation of L-functions

7.8 Fermat's Last Theorem

Fermat's Last Theorem is a (not so simple) consequence of modularity. Ken Ribet proved this consequence by showing that the *Frey curve* is not modular.

The Frey curve is...

7.9 Abelian Varieties

7.10 Reduction of algebraic curves

A review of Chapter 10 of [Liu02]. Going over reductions of elliptic curves. This can (of course) be done in a simpler, more concrete way (as we can see from [Sil09]), but I want to review the scheme-theoretic approach.

We have a scheme V over a number field K, and we want to "reduce" it with respect to the finite places of K. This is done by extending V to a "model" $\mathcal{V}$ over the ring of integers $\mathcal{O}_K$ of K, while trying to preserve as many good properties of V as possible. The reduction is then just the fiber of the maximal ideal $\mathfrak{p} \in Spec(\mathcal{O}_k)$. This theory is well understood for algebraic curves.

Definition 7.10.1. Let S be a Dedekind scheme of dimension 1, with function field K. Let C be a normal, connected projective curve over K. For $\eta \in S$ the generic point, we call a normal fibered surface $\mathcal{C} \to S$ together with an isomorphism $f : \mathcal{C}_\eta \cong C$ a *model of C over S*. A morphism $\phi : \mathcal{C} \to \mathcal{C}'$ of two models of C is a morphism of S-schemes that is compatible with the isomorphpisms, i.e. $f' \circ \phi_\eta = f$.

Example 14. If E is an elliptic curve over K, then we can use the Weierstrass equation to create a model over $\mathcal{O}_K$. A concrete example is using the Weierstrass equation of a rational elliptic curve to only look at integral points.

Note. The choice of isomorphism is often supressed when we talk about models, but it will be specified when needed (and it might sometimes be canonical). For example, there are many smooth models of $\mathbb{P}^1_K$ over S that are all isomorphic to $\mathbb{P}^1_S$ but some are not isomorphic to each other, so the choice does matter then.

Example 15. Let C be a normal projective curve over K, defined by homogeneous polynomials $F_1, ..., F_m \in K[T_0, ..., T_n]$. Let us suppose that $S = Spec(A)$. We can make the F_i have coefficients in A. If the scheme $\mathcal{C}_0 := A[T_0, ..., T_n]/(F_1, ..., F_m)$ is normal, then it is a model of C over S, because its generic fiber is isomorphic to C by

$$Proj(K[T_0, ..., T_n]/(F_1, ..., F_m)) \cong Proj(A[T_0, ..., T_n]/(F_1, ..., F_m)) \times_S \eta$$

because of the "tensor rule" for Proj:

$$Proj(B \otimes_A C) \cong Proj(B) \times_{Spec(A)} Spec(C)$$

(Normality is required for integral closure of $\mathcal{O}_{\mathcal{C}_0,\eta}$, for the polynomial ring tensor to work.)

Example 16. Let $q \geq 1$ be a square-free integer. Let C be a projective curve over $\mathbb{Q}$ defined by the equation $x^q + y^q + z^q = 0$. We can easily see (by formal derivative) that C is smooth over $\mathbb{Q}$. Let $\mathcal{C}$ be the closed subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ defined by the same equation. We will show that $\mathcal{C}$ is normal, and therefore a model of C over $\mathbb{Z}$.

The Jacobian criterion shows that $\mathcal{C} \to Spec(\mathbb{Z})$ is smooth outside of the primes p that divide q. Let p be one such prime, then the integer $r = q/p$ is coprime to p by hypothesis (q is square-free). We have

$$\mathcal{C}_p = Proj(\mathbb{F}_p[x, y, z]/(x^r + y^r + z^r)^p)$$

We can see that $\mathcal{C}_p$ is irreducible and that $(\mathcal{C}_p)_{red}$ is the closed subvariety $V(x^r + y^4 + z^r)$ over $\mathbb{F}_p$. As $\mathcal{C}$ is a complete intersection, and is regular at the generic fiber, to show normality of $\mathcal{C}$ it suffices to show its normality at the generic fiber of $\mathcal{C}_p$. We can therefore restrict ourselves to the affine open subscheme

$$U := Spec(\mathbb{Z}[X,Y]/(X^q + Y^q + 1))$$

The prime ideal corresponding to $\mathcal{C}_p$ is generated by $x^r + y^r + 1$. Since we are reducing to characteristic p, we have (in the non-reduced field):

$$X^q+Y^q+1 = (X^r+Y^r+1)^p - p((X^r+Y^r)F(X^r,Y^r)+(X^r+Y^r+1)F(X^r+Y^r,1), \qquad F(T,S) \in \mathbb{Z}[T,S]$$

with F homogeneous and $F \notin p\mathbb{Z}[T,S]$. This shows normality, because we can see that $X^r + Y^r + 1$ does not divide $F(X^r, Y^r)$.

Definition 7.10.2. Let C be a normal projective curve over K and let $\mathcal{C}$ be a model of C over S. Let us fix a closed point $s \in S$. We call the fiber $\mathcal{C}_s$ a *reduction of C at s*. If S is the spectrum of a Dedekind ring A, and if $\mathfrak{p}$ is the maximal ideal of A corresponding to s, we also call $\mathcal{C}_s$ a *reduction of C modulo $\mathfrak{p}$*. It is clear that the notion of reduction depends strongly on the choice of a model $\mathcal{C}$.

Definition 7.10.3. Let C be as above. We will say that C has *good reduction at $s \in S$* if it admits a smooth model over $Spec(\mathcal{O}_{S,s})$. This implies that C is smooth over K. If C does not have good reduction at s, we will say that C has *bad reduction at $s \in S$*.

Reduction of elliptic curves

Let us suppose for the rest of this section that S is the spectrum of a discrete valuation ring $\mathcal{O}_K$ with residue field k. We will suppose k is perfect or char$k \neq 2, 3$. Let E be an elliptic curve over $K = K(S)$ together with the base point $o \in E(K)$. We let $\mathcal{E}$ denote the minimal regular model of E over S, and W the minimal Weierstrass model of E over S. (Note: W is obtained by contracting certain vertical divisors on $\mathcal{E}$. Also, the canonical divisor $K_{\mathcal{E}/S}$ is trivial.)

Lemma 7.10.4. *Let us suppose k is perfect or char$(k) \neq 2, 3$. Let $\Gamma := W_s$ be the special fiber of the minimal Weierstrass model of E over S. Then Γ is a geometrically irreducible cubic. Let Γ^0 denote the smooth locus of Γ. The curve Γ is either smooth over k and therefore an elliptic curve over k, or Γ admits a unique singular points p, and p is rational over k. Then, we can create a normalization $\pi : \Gamma' \to \Gamma$ with $\Gamma' \cong \mathbb{P}^1_k$, and Γ is one of these three possibilities:*

split multiplicative $\pi^{-1}(p)$ *is made up of two k-rational points and* $\Gamma^0 \cong \mathbb{A}^1_k \setminus \{0\}$

non-split multiplicative $\pi^{-1}(p)$ *is a point and $k(p)$ is separable of degree 2 over k.*

additive $\pi^{-1}(p)$ *is a rational point and* $\Gamma^0 \cong \mathbb{A}^1_k$

Proof. Let Δ be the minimal discriminant of E. If $\Delta \in \mathcal{O}_K^\times$, then W is smooth. As Γ contains a rational point $\overline{\{o\}} \cap \Gamma$, it is an elliptic curve. Suppose that Δ is non-invertible. Hence Γ is not smooth. Let us suppose k is perfect. Then Γ is singular, because "smoothness=regularity" over perfect fields. Let us consider the exact sequence of sheaves

$$0 \to \mathcal{O}_\Gamma \to \pi_* \mathcal{O}_{\Gamma'} \to \mathcal{S} \to 0$$

with a skyscraper sheaf $\mathcal{S}$ whose support is the singular locus of Γ. The long exact sequence in cohomology is

$$0 \to k \to k \to \mathcal{S}(\Gamma) \to H^1(\Gamma, \mathcal{O}_\Gamma) \to H^1(\Gamma', \mathcal{O}_{\Gamma'}) \to 0$$

As the arithmetic genus $p_a(\Gamma) = p_a(E) = 1$, and $\mathcal{S} \neq 0$, we obtain $H^1(\Gamma', \mathcal{O}_{\Gamma'}) = 0$, which implies $\Gamma' \cong \mathbb{P}^1_k$, and $dim_k(S(\Gamma)) = 1$; hence Γ contains exactly one singular point p that is rational over k.

The set $\pi^{-1}(p)$ is the support of the finite scheme Γ'_p, which is the spectrum of

$$A := (\pi_* \mathcal{O}_{\Gamma'})_p \otimes k(p)$$

As $(\pi_* \mathcal{O}_{\Gamma'})_p / \mathcal{O}_{\Gamma,p} = \mathcal{S}(\Gamma)$ is of dimension 1 over k, we deduce that A is of dimension 2 over k as a k-vector space. Thus, $Spec(A)$ is either two rational points, a quadratic point, or one rational point (and then A is not reduced), which proves the lemma. □

Let $\mathcal{N}$ denote the open subscheme of $\mathcal{E}$ made up of points that are smooth over S. We are going to show that $\mathcal{N}$ is the Néron model of E over S.

Definition 7.10.5. Let S be a Dedekind scheme of dimension 1, with function field $K = K(S)$. Let A be an abelian variety over K. We define the *Néron model of A over S* to be a scheme $\mathcal{A} \to S$ which is smooth, separated, and of finite type with generic fiber isomorphic to A, and that verifies the following universal property: For any smooth scheme X over S, the following canonical map is bijective:

$$Hom_S(X, \mathcal{A}) \xrightarrow{\sim} Hom_K(X_K, A)$$

The universal property implies that $\mathcal{A}$ is unique up to isomorphism and that the algebraic structure on A extends in a unique way to $\mathcal{A} \to S$ (take $X = \mathcal{A} \times_S \mathcal{A}$).

Lemma 7.10.6. *Let S be a Dedekind scheme of dimension 1, with function field $K = K(S)$. Let (E, o) be an elliptic curve over K, $\mathcal{E}$ its minimal regular model over S, and $\mathcal{N}$ the open subscheme of smooth points of $\mathcal{E}$ over S. Then,*

(a) The canonical maps $\mathcal{N}(S) \to \mathcal{E}(S) \to E(K)$ are bijective.

(b) *For any section $x \in \mathcal{E}(S)$, the translation $t_{x_K} : E \to E$ associated to $x_K \in E(K)$ extends to an automorphism $t_x : \mathcal{E} \to \mathcal{E}$.*

(c) *Let $m : E \times_K E \to E$ be the algebraic group law on E. Then the automorphism $t = (m, q) : E \times_K E \to E \times_K E$ (where q is the second projection) extends to an automorphism $t : \mathcal{E} \times_S \mathcal{N} \to \mathcal{E} \times_S \mathcal{N}$.*

(d) *Let $p : \mathcal{N} \times_S \mathcal{N} \to \mathcal{N}$ be the first projection. Then t induces an automorphism $\tau : \mathcal{N} \times_S \mathcal{N} \to \mathcal{N} \times_S \mathcal{N}$ and $p \circ \tau$ defines a smooth group scheme structure on $\mathcal{N} \to S$*

Proof. Assuming the hypotheses above:

(a) Let $\epsilon : Spec(K) \to E$ be a section. Because E is projective (and therefore proper) ϵ extends to a morphism $Spec(\mathcal{O}_{S,s}) \to \mathcal{E}$ for any $s \in S$. This then extends to a morphism $\epsilon_V : V \to \mathcal{E}$ for an open neighborhood V of s. As $\mathcal{S}$ is separated, the ϵ_V glue together to a (unique) morphism $S \to \mathcal{E}$. Hence $\mathcal{E}(S) \to E(K)$ is surjective, and hence bijective because $\mathcal{E}$ is separated over S. As $\mathcal{E}$ is regular, the sections $\mathcal{E}(S)$ have their image in the smooth locus, which gives the equality $\mathcal{N}(S) = \mathcal{E}(S)$

(b) Because $\mathcal{E}$ is a minimal regular model, we have a bijection

$$Aut_K(E) \xrightarrow{\sim} Aut_S(\mathcal{E}_\eta)$$

which follows from minimality (b/c every birational map is a morphism)

□

Theorem 7.10.7. *Let S be a Dedekind scheme of dimension 1, with function field $K = K(S)$. Let E be an elliptic curve over K with minimal regular model $\mathcal{E}$ over S. Then the open subscheme $\mathcal{N}$ of smooth points of $\mathcal{E}$ is the Néron model of E over S.*

Proof. By the lemma above, $\mathcal{N}$ is a smooth group scheme, separated of finite type over S, with generic fiber isomorphic to E. It remains to show the universal property.

Let X be a smooth scheme over S, and let $f : X_\eta \to E$ be a morphism considered as a rational map $X \dashrightarrow \mathcal{N}$. Let $\xi \in X$ be a point of codimension 1, and $T = Spec(\mathcal{O}_{X,\xi})$. Then, $\mathcal{E} \times_S T \to T$ is a minimal arithmetic surface with smooth locus $\mathcal{N} \times_S T$. □

8 Complex Analytic Theory

This section sets up the framework of analytic geometry and cohomology upon which everything else rests. In the classical theory of modular curves, one attaches to each $z \in \mathfrak{h}$ the elliptic curve $\mathbb{C}/[1, z]$. This allows one to identify the points of various quotients of $\mathfrak{h}$ with *sets* of isomorphism classes of classical elliptic curves with supplementary “level structure”. We want more precise results, namely a *relative* theory of analytic elliptic curves (and even relative complex tori) and an identification of the classical quotients of $\mathfrak{h}$ with *representing objects* (i.e. moduli spaces) for certain functors on analytic spaces. Such a perspective on the classical theory will naturally motivate both the arithmetic theory of modular curves and the considerations with etale cohomology. This will take a lot of effort to set up, but the subsequent chapters should convince the reader that this is effort well spent. We may skip some of the longer proofs.

Much as it is technically useful to allow oneself the generality of (locally) finite type $\mathbb{C}$-schemes instead of restricting our attention to smooth varieties over $\mathbb{C}$, we prefer to work with arbitrary complex analytic spaces instead of just complex manifolds. The advantage of this extra generality lies not only in the great naturality of the conclusions, but also the ease with which we will be able to work with non-smooth generalized elliptic curves and use algebro-geometric techniques (such as infinitesimal fiber arguments) in our analytic considerations. Such an approach forces us to make essential use of non-trivial results in the cohomology theory of coherent analytic sheaves. The statement of these cohomological results (which we will review) are quite similar to what one knows in the theory of schemes, so we should have little difficulty accepting these basic facts on faith.

Basic constructions on $\mathfrak{h}$:

Let S be an arbitrary complex analytic space. We want to define the notion of an "elliptic curve over S" and then, upon choosing $i = \sqrt{-1} \in \mathbb{C}$, we want to "glue" the classical elliptic curves $\mathbb{C}/[1, z]$ for $z \in \mathfrak{h}$ into an elliptic curve $\mathcal{E}^{an} \to \mathfrak{h}$ with suitable universal property. In order to put things in perspective, we wil lcarry this out for "relative complex tori" of any (fixed) relative dimension g, getting a suitably universal obect over a Siegel upper half-space.

To carry out our program, we must analyze the extra data inherent in an elliptic curve of the form $\mathbb{C}/[1, z]$. In other words, we need to determine what kind of *intrinsic* structure on a classical (analytic) elliptic curve E is specified by an isomorphism $\alpha : E \simeq \mathbb{C}/[1, z]$ for $z \in \mathfrak{h}$. there are two essential pieces of data:

1. The tangent space map at the origin $T_0(\alpha) : T_0(E) \simeq \mathbb{C}$ gives a basis of $T_0(E)$, or dually gives a non-zero differential $\omega \in H^0(E, \Omega^1_E)$ corresponding to the standard differential $d\tau$ on $\mathbb{C}$.

2. $H_1(\alpha) : H_1(E, \mathbb{Z}) \simeq [1, z]$ with $z \in \mathfrak{h}$ gives an ordered basis $\{\gamma_1, \gamma_2\}$ of $H^1(E, \mathbb{Z})$ whose ordered dual basis in $H^1(E, \underline{\mathbb{Z}})$ has cup product in $H^2(E, \underline{\mathbb{Z}})$ which is positive w/r/t the i-orientation of E.

We will later make precise how such structure on E are related to the specification of such $\alpha's$, but our first order of business is to set up a good relative notion of a "family of elliptic curves" so that we can make precise how $\mathcal{E}^{an} \to \mathfrak{h}$ (once it is constructed) is going to be universal; formalizing this universality will amount to relativizing the two properties above.

One consequence of this study is an improved understanding of the classical theory of modular curves. Recall that this classical theory identifies the underlying set of $\Gamma_1(N)\backslash\mathfrak{h}$ with isomorphism classes of pairs (E, P) consisting of classical elliptic curves E and a points $P \in E$ with exact order N, via the assignment $z \mapsto (\mathbb{C}/[1, z], 1/N)$. We will use $\mathcal{E}^{an} \to \mathfrak{h}$ and descent to "glues" these objects into a global geometric structure lying over $\Gamma_1(N)\backslash\mathfrak{h}$, recovering the classical objects on fibers. In the same way that Grothendieck's reformulation of moduli space in terms of representable functors gave the theory more strength and flexibility, having a relative analytic theory of elliptic curves will put the analytic theory of modular curves in a more natural light.

Before we can intelligently and naturally "glue" the $\mathbb{C}/[1, z]$'s over $\mathfrak{h}$, we need to spend some time reviewing basic cohomological and geometric facts concering complex analytic spaces. This will allow us to define and study the relative notion of elliptic curves in a purely analytic context.

Definition 8.0.1. A continuous map $f : X \to Y$ of topological spaces is *universally closed* if $X \times_Y Z \to Z$ is closed for "all" continuous maps $Z \to Y$. (Think like "closed with compact fibers")

In here and what follows, we recall that $X \times_Y Z$ in the category of topological spaces is simply the subset of $X \times Z$ which projects to the diagonal in $Y \times Y$, and this is (readily checked to be) a fiber product in the topological category. As in algebraic geometry, we refer to the operation of passing from a map $f : X \to Y$ to the induced map $X \times_Y Z \to Z$ as (topological) *base change.*

Definition 8.0.2. A map $f : X \to Y$ of topological spaces is *separated* if the diagonal map $\Delta_f = \Delta_{X/Y} : X \to X \times_Y X$ is a closed embedding.

It follows from the definition that separatedness is preserved by topological base change, so if $f : X \to Y$ is separated, then the preimage of a Hausdorff subspace of Y is a Hausdorff subspace of X. For example, X is separated over a point if and only if X is Hausdorff. Since the underlying topological space of an analytic fiber product is the topological fiber product, it is easy to see that for a map $f : X \to Y$ of analytic spaces, Δ_f is always an immersion (here we use that analytic spaces are locally Haussdorf), so f is separated if and only if Δ_f is a closed immersion of analytic spaces.

Definition 8.0.3. A map $f : X \to Y$ of topological spaces is *proper* if it is universally closed and separated.

It is clear from the definition that the notion of properness is closed under base change. We use the "preimage of a compact set is compact" property of proper maps when we study maps between analytic spaces (such as families of Tate curves).

Among the conditions we will impose on a morphism $E \to S$ to call it an elliptic curve over S is the condition that it should be proper. Such a morphism should also satisfy the requirement of the following fundamental definition which is inspired by the algebro-geometric relative notion of smoothness:

Definition 8.0.4. A map $f : X \to Y$ of analytic spaces is *smooth* if f is flat (in the sense of locally ringed spaces) and all analytic fibers of f are manifolds. We further say that f has *relative dimension* d if all fibers of f have pure dimension d.

This definition enjoys familiar properties as in algebraic geometry. For a map $f : X \to Y$ of analytic spaces, the following conditions are equivalent:

1. f is smooth in a neighborhood of $x \in X$;

2. $\widehat{\mathcal{O}}_{X,x} \simeq \widehat{\mathcal{O}}_{Y,f(x)}[\![t_1, \ldots, t_d]\!]$ as $\mathbb{C}$-algebras, for some $d \geq 0$;

3. At x, the maps f satisfies the "Artinian" lifting property over Y as in algebraic geometry;

4. Near x and $f(x)$, there is a commutative diagram

$$\begin{tikzcd}
X \arrow[rr, "\simeq"] \arrow[dr] & & U \times Y \arrow[dl] \\
& Y &
\end{tikzcd}$$

   where $U \subseteq \mathbb{C}^d$ is an open ball, for some $d \geq 0$ (necessarily the same as in the second condition above).

When these conditions hold, f has relative dimension d near x. If Y is a manifold near $f(x)$, then these are equivalent to X being a manifold near x and f being a submersion near x. Associated to any smooth map f, we get a locally constant "relative dimension" function on X.

The local constancy of the relative dimension function of smooth morphism implies that a propersmooth map with connected fibers has relative dimension function locally constant *over the base.* We may therefore reasonably speak of proper smooth families of curves, for example. The following definition is fundamental to what follows:

Definition 8.0.5. Let S be an analytic space. An *elliptic curve over* S is a proper smooth map $p : E \to S$ of relative dimension 1, with a specified section $e : S \to E$ and connected fibers of genus 1. We will often omit the section e from the notation.

Our first task is to prove that an elliptic curve $E \to S$ has a natural structure as an S-group object, but first we must review some results on cohomology and base change in the analytic setting. In the discussion that follows, we let $f : X \to Y$ denote a proper map of analytic spaces and let $\mathcal{F}$ be a coherent sheaf on X.

Theorem 8.0.6. *The higher direct images $R^i f_*(\mathcal{F})$ are coherent.*

We will often find it useful to reduce general questions to the case of infinitesimal fibers. For example, let X and Y be two analytic spaces over S, and $f, g : X \to Y$ two S-morphisms. On several occasions we will prove such maps coincide in a general situation. Note that it also suffices to consdier the case of an infinitesimal fiber (i.e S having a single point). Indeed, suppose f and g coincide on infinitesimal fibers. These maps then agree topologically and the structure sheaf maps

$$\mathcal{O}_Y \to f_*\mathcal{O}_X = g_*\mathcal{O}_X$$

coincide because two sections of $\mathcal{O}_X$ on a common open agree if they induce the same sections on infinitesimal fibers: work locally on X and note that for each $x \in X$ over $s \in S$, the Krull intersection theorem ensures that the local Noetherian ring $\mathcal{O}_X$ is separated for the topology defined by the maximal ideal $\mathfrak{m}_s$ of $\mathcal{O}_S$ (so two elements of $\mathcal{O}_X$ which have the same images in all quotients $\mathcal{O}_X/\mathfrak{m}_s^n$ are necessarily equal).

In order to reduce the cohomological question to the setting of infinitesimal fibers, it will be useful to invoke:

Theorem 8.0.7 (Theorem on formal functions)**.** *For integers $n \geq 1$, let X_n denote the nth infinitesimal neighborhood of the fiber X_y in X and let $\mathcal{F}_n$ be the pullback of $\mathcal{F}$ to a coherent sheaf on X_n. For $y \in Y$, the natural map of topological $\widehat{\mathcal{O}}_y$-modules*

$$\widehat{\mathcal{O}}_y \otimes_{\mathcal{O}_y} R^i f_*(\mathcal{F})_y \to \varprojlim H^i(X_n, \mathcal{F}_n)$$

is an isomorphism.

The proof of this theorem is very long, but there are just a handful of ideas: essentially induction on the number of generators of an ideal and fiddling with inverse limits so as to push through the induction. Unfortunately, there are a numbre of technical details which cause the argument to become very long when written out completely. We will make extensive use of this theorem.

By the GAGA theorems, the analytification functor from proper $\mathbb{C}$-schemes to compact Hausdorff complex analytic spaces is fully faithful. We call an analytic space arising in this way *algebraic*. We will often use the above theorem to reduce general questions about analytic families of elliptic curves and principally polarized complex tori to the case of a 1 point base, where the analytic object turns out to be algebraic (so GAGA reduces us to an algebraic situation).

Before stating the next result, we recall that an $\mathbb{O}_X$-module $\mathcal{F}$ is said to be *Y-flat* if $\mathcal{F}_x$ is a flat $\mathcal{O}_{Y,f(x)}$-module for all $x \in X$; in case this holds with $\mathcal{F} = \mathcal{O}_X$, f is a *flat map.*

Theorem 8.0.8 (Cohomology and base change)**.** *Let $f : X \to Y$ be a proper morphism of analytic spaces and let $\mathcal{F}$ be a coherent Y-flat sheaf on X. For $i \in \mathbb{Z}$, if the natural map*

$$\phi^i(y) : R^i f_*(\mathcal{F})_y/\mathfrak{m}_y \to H^i(f^{-1}(y), \mathcal{F}|_{f^{-1}(y)})$$

is surjective for some $y \in Y$, then it is an isomorphism.

If this surjectivity condition holds for all $y \in Y$, then $\phi^{i-1}(y)$ is surjective if and only if the coherent sheaf $R^i f_*(\mathcal{F})$ is locally free on some open U around y, in which case $R^i f_*(\mathcal{F})$ is of formation compatible with arbitrary analytic base change over U.

A standard consequence of this theorem is given in the next result, which we use repeatedly without comment:

Corollary 8.0.9. *Let $f : X \to Y$ be a proper flat morphism of analytic spaces with connected reduced fibers. Then the natural map $\mathcal{O}_Y \to f_*\mathcal{O}_X$ is an isomorphism.*

Classically, this could be thought of as a proper submersion between complex manifolds (with connected fibers). One further important fact about flat maps is the fiber-by-fiber criterion for a map to be flat or an isomorphism. This will allow us to reduce relative questions to a classical situation:

Lemma 8.0.10. *Let X, Y be analytic spaces over S, and $f : X \to Y$ an S-map.*

- *Assume X, Y are S-flat and $f_s : X_s \to Y_s$ is flat for all $s \in S$. Then f is flat and, moreover, f_s is an isomorphism for all $s \in S$ if and only if f is an isomorphism.*
- *If f induces a flat map (resp. an isomorphism) on all infinitesimal fibers over S, then f is flat (resp. an isomorphism). Also, two S-maps $f, g : X \to Y$ which coincide on all infinitesimal fibers are equal.*

Here is another fundamental and very useful theorem concerning passage from fibers to relative situations:

Theorem 8.0.11. *Let $f : X \to Y$ be an S-map between proper analytic spaces over S. If X is S-flat, then the locus U of $s \in S$ for which f_s is an isomorphism is open and $f|_U : X|_U \to Y|_U$ is an isomorphism.*

One application of passage to infinitesimal fibers i the following fact, relativizing a well-known property of pointed genus 1 curves.

Theorem 8.0.12. *Let $E \to S$ be an elliptic curve, defined as above. There is a unique structure of S-group object on an elliptic curve $E \to S$ with e as the identity section. This group structure is commutative, and any S-map $E_1 \to E_2$ respecting the identity sections is a homomorphism.*

Proof. Thanks to the "algebraicity" of the infinitesimal fiber (1-dimensional compact Hausdorff analytic spaces are automatically algebraic) and similarity of cohomological input (as shown above), we precede as follows:

For the rest of the theorem, we are concerned with equalities of S-maps, so, as we have shown, it suffices to consider infinitesimal fibers (i.e. S as a single point). Since 1-dimensional compact Hausdorff analytic spaces are algebraic, one could use the results in the algebraic proof (Katz-Mazur, *Arithmetic moduli of elliptic curves*). However, we prefer to instead give a purely analytic proof which has the advantage of generalizing later to show that group structures on relative complex tori are unique.

When $S = \mathrm{Sp}\mathbb{C}$ is a reduced point, the commutativity and uniqueness of the group structure, as well as its compatibility with identity-preserving morphisms are classical: the algebraic proof on p.43 of Mumford's *Abelian varieties* applies equally well to analytic spaces, as these are locally Stein spaces and the only compact connected analytic sets in a Stein space are points (this replaces the algebraic fact that for an algebraically closed field k, the only proper connected affine variety over k is $\mathrm{Spec}k$).

In the general case with artinian but possibly non-reduced S, it suffices to show quite generally that if G is a group-analytic space over a one point base S, and if $p : X \to S$ is proper with the natural map $\mathcal{O}_S \to p_*\mathcal{O}_X$ an isomorphism, then any S-map $f : X \to G$ with topological image supported at the identity of G factors as

$$X \xrightarrow{p} S \xrightarrow{\eta} G$$

where η is a section. This assertion is clear topologically, so it suffices to give the sheaf map $\eta^\# : \mathcal{O}_G \to \eta_*\mathcal{O}_S$. But η agrees with the identity section ε topologically, so

$$\eta_*\mathcal{O}_S = \epsilon_*\mathcal{O}_S = \epsilon_*p_*\mathcal{O}_X = f_*\mathcal{O}_X$$

Taking $\eta^\#$ to agree with $f^\#$ now gives the desired section.

□

In relative dimension > 1, we must incorporate the group structure into the definition, whereas with elliptic curves we could "cheat". Doing this, the same methods and conclusions as obtained above will apply to the "relative complex tori" which we discuss later.

Example 17. Here are the most important examples to keep in mind:

1. Define an elliptic curve $f^{alg} : E^{alg} \to \mathfrak{h}$ by

$$E^{alg} = \{(z, [x, y, w]) \in \mathfrak{h} \times \mathbb{CP}^2 \mid y^2w = 4x^3 - g_2(z)xw^2 - g_3(z)w^3\}$$

$$f^{alg}(z, [x, y, w]) = z$$

with identity section given by $e(z) = (z, [0, 1, 0])$; here g_2 and g_3 are

$$g_2(z) = 60 \sum_{\tau\in\Lambda_z\setminus\{0\}} \frac{1}{\tau^4} = \frac{(2\pi)^4}{2^2\cdot 3}\left(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\right)$$

$$g_3(z) = 140 \sum_{\tau\in\Lambda_z\setminus\{0\}} \frac{1}{\tau^6} = \frac{(2\pi)^6}{2^3\cdot 3^3}\left(1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\right)$$

and we are giving everything the canonical analytic structure.

2. Define a "relative lattice" over $\mathfrak{h}$

$$\Lambda = \mathbb{Z}^2 \times \mathfrak{h} \hookrightarrow \mathbb{C} \times \mathfrak{h}$$

$$(m, n; z) \mapsto (mz + n; z)$$

We want to view $(\mathbb{C} \times \mathfrak{h})/\Lambda$ as an elliptic curve $\mathcal{E}^{an} \to \mathfrak{h}$. To make sense of this quotient, we use the C^∞-diagram

$$\mathbb{C} \times \mathfrak{h} \simeq \mathbb{C} \times \mathfrak{h}$$

$$(z + iy; z) \mapsto (x + zy; z)$$

taking the "standard lattice"

$$\mathbb{Z}^2 \times \mathfrak{h} \hookrightarrow \mathbb{C} \times \mathfrak{h}$$

$$(m, n; z) \mapsto (mi + n; z)$$

to Λ; of course, the C^∞-map is not holomorphic. Nevertheless, it does show that the quotient topological space $(\mathbb{C} \times \mathfrak{h})/\Lambda$ by the equivalence relation $(\tau, z) \sim (\tau + \lambda, z)$ for $\lambda \in \Lambda_z$ has a unique C^∞-structure such that the projection map

$$\pi : \mathbb{C} \times \mathfrak{h} \to (\mathbb{C} \times \mathfrak{h})/\Lambda$$

is a local C^∞-isomorphism. Indeed, the projection for the standard lattice $\mathbb{C} \times \mathfrak{h} \to (\mathbb{C}/[1, i]) \times \mathfrak{h}$ is a proper covering space map since $\mathbb{C} \to \mathbb{C}/[1, i]$ is, so π is even a proper covering space map. If we give

$$\mathcal{E}^{an} := (\mathbb{C} \times \mathfrak{h})/\Lambda$$

the unique complex structure making π a holomorphic local isomorphism (explained in lemma below), then the projection $f^{an} : \mathcal{E}^{an} \to \mathfrak{h}$ is a holomorphic proper submersion of relative dimension 1. We give $\mathcal{E}^{an} \to \mathfrak{h}$ the obvious holomorphic section $z \mapsto (0; z)$. To check that $\mathcal{E}^{an} \to \mathfrak{h}$ is an elliptic curve, it suffices to check that the fibers are classical elliptic curves. For any $z_0 \in \mathfrak{h}$, the natural holomorphic map $\mathbb{C}/[1, z_0] \to \mathcal{E}^{an}_{z_0}$ is a bijection of compact *Riemann surfaces* and thus is an isomorphism. We conclude that $f^{an} : \mathcal{E}^{an} \to \mathfrak{h}$ is an elliptic curve with the expected complex fibers.

The classical Weierstrass theory with $\wp_z(\tau)$ and $\wp'_z(\tau)$, which are holomorphic on the open set

$$\{(\tau, z) \in \mathbb{C} \times \mathfrak{h} \mid \tau \notin [1, z]\} \subseteq \mathbb{C} \times \mathfrak{h}$$

gives a holomorphic map

$$\mathbb{C} \times \mathfrak{h} \to E^{alg}$$

$$(\tau; z) \mapsto (z, [\wp_z(\tau), \wp'_z(\tau), 1])$$

which is invariant w/r/t the Λ-action on $\mathbb{C} \times \mathfrak{h}$. We thus get a holomorphic map $\mathcal{E}^{an} \to E^{alg}$ over $\mathfrak{h}$ respecting the identity sections and inducing the classical map

$$(\wp_z, \wp_z') : \mathbb{C}/[1, z_0] \to \{(x, y) \mid y^2 = 4x^2 - g_2(z_0)x - g_3(z_0)\}$$

on fibers. By the classical theory, we know that this fiber map is an isomorphism, so we conclude by $\mathfrak{h}$-flatness (or by using the localy structure of sunmersions and the inverse function theorem) that the map $\mathcal{E}^{an} \to E^{alg}$ over $\mathfrak{h}$ is an isomorphism (of elliptic curves).

The elliptic curve $\mathcal{E}^{an} \to \mathfrak{h}$ is nearly universal for being a "line bundle modulo $\underline{\mathbb{Z}}^2$". To be precise, later we will describe a generalization of the above construction of $\mathcal{E}^{an}$ and then we make some cohomological digressions before we return to the matter of formulating the universal property of $\mathcal{E}^{an} \to \mathfrak{h}$ in the category of complex analytic spaces.

Vector bundles and lattices:

Let S be an analytic space and V a rank d vector bundle on S, with $d \geq 1$. We will often identify V with its sheaf of sections. Let

$$\iota : \Lambda \hookrightarrow V$$

be an inclusion of abelian sheaves, with Λ a local system of rank $2d$ free $\mathbb{Z}$-modules (i.e. Λ is a locally constant sheaf on S, locally isomorphic to $\mathbb{Z}^{2d}$) and assume Λ induces a cocompact lattice $\Lambda_s \hookrightarrow V_s$ for all $s \in S$. Since S has a base of connected opens and connected analytic spaces are path connected, for connected S we have $H^0(S, \underline{\Sigma}) = \Sigma$ for any set Σ. In particular, we can identify locally constant sheaves of sets on S with topological covering spaces of S and hence with analytic covering spaces of S. This ensures that there is a unique commutative S-group object, also denoted Λ, which is an analytic covering space of S with sheaf of holomorphic sections isomorphic to the abelian sheaf Λ.

From topological and separatedness considerations, we see that there is a unique way to define a holomorphic map $\Lambda \to V$ over S which recovers the above injective sheaf map ι on sheaves of sections, and in fact $\Lambda \to V$ is a *closed immersion of S-group objects* inducing the original $\Lambda_s \to V_s$ on fibers. Whenever we are given a local system Λ inside a vector bundle V as above, it is always understood that we give Λ and $\Lambda \hookrightarrow V$ these canonical analytic structures over S. Note that these constructions are compatible with arbitrary base change over S.

It is rather important that given such a $\Lambda \hookrightarrow V$, we can endow the topological quotient V/Λ with a good analytic structure (analogous to $\mathcal{E}^{an}$). Before we formulate this precisely, we introduce a convenient definition. For any smooth group object $G \to S$ with identity section e, we define the *relative tangent space* (along the identity section) to be $T_e(G) = e^*(\Omega^1_{G/S})^\vee$, a locally free coherent sheaf (or vector bundle) on S.

Lemma 8.0.13. *Let S and $\Lambda \hookrightarrow V$ be as above. Then*

1. *The projection $\pi : V \to V/\Lambda$ is a covering map of topological spaces, with $V/\Lambda \to S$ proper. Moreover, the formation of the topological space V/Λ is compatible with topological base change on S.*

2. *There is a unique complex structure on V/Λ making π a local analytic isomorphism, and $V/\Lambda \to S$ is then proper smooth, admitting a unique S-group strucutre making π a map of group objects. The natural map $\Lambda \to \pi^{-1}(0)$ is an analytic isomorphism, as is $V \simeq T_0(V) \to T_0(V/\Lambda)$.*

3. *Formation of the complex structure in* (2) *is compatible with analytic base change on S.*

Proof. Locally on S, the map $\Lambda \hookrightarrow V$ has the topological form

$$\mathbb{Z}^{2d} \times S \hookrightarrow \mathbb{R}^{2d} \times S$$

given by continuous functions $f_{ij} : S \to \mathbb{R}$, $1 \leq i, j \leq 2d$. Since $\Lambda_s \hookleftarrow V_s$ is a cocompact lattice for all $s \in S$, $\det f_{ij}$ must be nonvanishing on S. By Cramer's rule, we can then topologically transform the above arbitrary inclusion into the canonical inclusion $\mathbb{Z}^{2d} \times S \hookrightarrow \mathbb{R}^{2d} \times S$, from which it is clear that (1) holds. The uniqueness in (2) implies (3), so it remains to check (2). The uniqueness of the analytic structure on V/Λ is immediate. All we have to show is that V/Λ admits an analytic S-group structure making π an analytic group map and a local analytic isomorphism. By uniqueness, this is a local problem over S.

To give v/Λ an analytic structure, we need to chech that if S is sufficiently small, then for any $x \in V/\Lambda$, any two points $v_1, v_2 \in \pi^{-1}(x)$ have neighborhoods in V inducing the "same" analytic structure on V/Λ near x. Working locally on S, we may choose a closed immersion $S \hookrightarrow S'$ with S' a ball and we may assume that there exist Λ', V' over S' lifting Λ, V on S, as well as an S'-map $\Lambda' \to V'$ lifting $\Lambda \hookrightarrow V$. Indeed, shrinking S, we can assume $\Lambda \simeq \mathbb{Z}^{2g} \times S$, $V \simeq \mathbb{C}^g \times S$, and we can then take $\Lambda' = \mathbb{Z}^{2g} \times S'$, $V' = \mathbb{C}^g \times S'$ compatibly with these isomorphisms.

The map $\Lambda' \to V'$ is given by holomorphic functions f'_{ij}, $1 \leq i \leq 2g, 1 \leq j \leq g$ with $\det(\mathrm{Re}(f'_{ij}), \mathrm{Im}(f'_{ij}))$ nonvanishing along S, and hence also nonvanishing in a neighborhood of S in S'. Thus, shrinking S' allows us to assume that $\Lambda' \to V'$ induces a cocompact lattice on fibers, so *topologically* $\Lambda' \to V'$ is a closed embedding. The analytic map $\Lambda' \to V'$ is proper and quasi-finite, hence finite, so we can check if it is an analytic closed immersion by considering fibers over S' (by Nakayama's Lemma); this condition is clearly satisfied if we shring S' around S. Thus, we have liftered our entire local situation to S'. Since we are just tring to construct *some* analytic group structureon V/Λ making π a local isomorphism of group objects, this shows that to prove that remainder of the lemma we can pass to S' and thus assume that the base S is smooth, so V is a manifold.

Since V and S are reduced (even manifolds), if V/Λ has an analytic structure making π a local isomorphism (ignoring group data), then the obvious topological S-group structure on V/Λ is compatible via π with the topological group structure on V. so this makes V/Λ an S-group and π a group map. Thus, we can now ignore group data and just look for an analytic structure on V/Λ over S making π a local analytic isomorphism.

Choose a small open set $U \subseteq V/\Lambda$ and let U_1, U_2 be two "copies" of U in $\pi^{-1}(U)$. Give U_1, U_2 thier analytic structures as opens in V. We need to check that the composite homeomorphism

$$U_1 \simeq U \simeq U_2$$

is ana analytic isomorphism; we can then us these U_j's to define the desired analytic structure on U. Choose $s \in S$ and $\lambda_s \in \Lambda_s \subseteq V_s$ taking $(U_1)_s$ to $(U_2)_S$ under translation in V_s. From the local topological description of π, by shrinking S there is some $\lambda \in \Lambda(S) \subseteq V(S)$ with fiber λ_s at s; translation by λ takes U_1 to U_2 topologically and hence analytically. □

Return now to the elliptic curve $f^{an} : \mathcal{E}^{an} \to \mathfrak{h}$. What are the special relative properties analogous to the global 1-form ω and the ordered homology basis γ_1, γ_2 on an elliptic curve $\mathbb{C}/[1,z] = \mathcal{E}_z^{an}$?

1. For the fibers $\mathcal{E}_z^{an} \simeq \mathbb{C}/[1,z]$, the 1-dimensional spaces $H^0(\mathcal{E}_z^{an}, \Omega^1_{\mathcal{E}_z^{an}})$ have a natural basis:
$$\frac{dt}{t} = 2\pi i d\tau = 2\pi i \frac{dx}{y}$$
the different forms being given by different incarnations of $\mathcal{E}_z^{an}$:
$$\mathbb{C}^\times/q^{\mathbb{Z}} \simeq \mathbb{C}/[1,z] \simeq \{(x,y) \mid y^2 = 4x^3 - g_2(z)x - g_3(z)\}$$
where $t = e^{2\pi i\tau}$, $q = e^{2\pi i z}$. These all obviously vary "nicely" in $z \in \mathfrak{h}$, and thus should give a trivialization of $f_*^{an}\left(\Omega^1_{\mathcal{E}^{an}/\mathfrak{h}}\right)$.

2. $H^1(\mathcal{E}_z^{an}, \underline{\mathbb{Z}})^\vee$ is isomorphic to $H_1(\mathcal{E}_z^{an}, \mathbb{Z})$, which has ordered basis c_1, c_2 $(z, 1)$. These vary nicely in z, and thus should yield a global trivialization of $(R^1 f_*^{an}\underline{\mathbb{Z}})^\vee$.

To relate higher direct image sheaves for elliptic curves $f : E \to S$ with cohomology on fibers, we will need to investigate the structure of the sheaves $R^1 f_* \underline{\mathbb{Z}}$ and $f_*\Omega^1_{E/S}$, especially how these sheaves behave w/r/t base change (to fibers). That is, we must study higher direct images of coherent sheaves and locally constant sheaves. This will lead us to the universal property of $\mathcal{E}^{an} \to \mathfrak{h}$.

Cohomological considerations

Because of the explicit global C^∞-splitting (open local isomorphism on locus of fiber isomorphisms and interpreting sheaves as "espace etale" or vector bundles), it is clear that the natural map

$$R^1 f_*^{an}(\underline{\mathbb{Z}})_z \to H^1(\mathcal{E}_z^{an}, \underline{\mathbb{Z}})$$

is an isomorphism for all $z \in \mathfrak{h}$ (recall that $\mathfrak{h}$ is obviously path-connected). More generally, how do the stalks of the higher direct images of a sheaf $\mathcal{F}$ via a map $f : X \to Y$ relate to the cohomology of the fibers? This question is simplest when Y is locally compact and locally Hausdorff, as is the cse for f^{an}. However, we ideally want to imagine $\mathcal{E}^{an} \to \mathfrak{h}$ extending to $\overline{\mathcal{E}}^{an} \to \mathfrak{h} \cup \{\infty\}$ with a "Neron polygon with infinitely many sides" over ∞, where $\mathfrak{h} \cup \{\infty\}$ has a base of opens around ∞ the sets

$$\{z \in \mathfrak{h} \mid \mathrm{Im}(z) > N\} \cup \{\infty\}$$

This space $\mathfrak{h} \cup \{\infty\}$ is not locally compact near ∞, but as a "universal cover" of the punctured disk, totally ramified over the origin, it play a critical role in the etale monodromy theory of Lefschetz pencils (and for the compactification of modular curves). By the Urysohn metrization theorem, $\mathfrak{h} \cup \{\infty\}$ is at least metrizable. For this reason, we include the metrizable case in the following fundamental result, even though our immediate needs are just in the locally compact, locally Hausdorff case.

Theorem 8.0.14 (Topological proper base change). *Consider a proper map of topological spaces $f : X \to Y$ with either:*

- *Y locally compact, locally Hausdorff;*
- *all fibers of f admitting metrizable neighborhoods.*

Then, for all abelian sheaves $\mathcal{F}$ on X and all $y \in Y$, the δ-functorial map

$$R^i f_*(\mathcal{F})_y \to H^i(f^{-1}(y), \mathcal{F}_y)$$

is an isomorphism, where $\mathcal{F}_y = \mathcal{F}|_{f^{-1}(y)}$. The formation of $R^i f_* \mathcal{F}$ is compatible with locally compact, locally Hausdorff base change on Y if Y is locally compact, locally Hausdorff.

Proof. AWLOG that Y is a compact Hausdorff space (and thus X is as well) or that X is metrizable. The $i = 0$ case of the theorem is a consequence of the following lemma (consequence of basic sheaf cohomology: Iversen, Ch3 Thm 2.2):

Lemma 8.0.15. *Let x be a compact Hausdorff (resp. metrizable) space and let $i : Z \hookrightarrow X$ be an inclusion of a compact (resp. arbitrary) subset. Then the natural map*

$$\varinjlim_{Z \subset V} H^0(V, \mathcal{F}) \to H^0(Z, i^{-1}\mathcal{F})$$

is an isomorphism for all abelian sheaves $\mathcal{F}$ on X, where $i^{-1}\mathcal{F}$ denotes the topological pullback.

It remains to check that the δ-functor $H^*(f^{-1}(y), (-)_y)$ is erasable. We show that $H^i(f^{-1}(y), \mathcal{F}_y) = 0$ for all $i > 0$ and all flasque sheaves $\mathcal{F}$ on X. In the metrizable case, the above lemma implies that $i^{-1}(\mathcal{F})$ is flasque if $\mathcal{F}$ is flasque, so this case is clear. In the other case, we know that $f^{-1}(y)$ is compact Hausdorff, so ordinary cohomology agrees with compactly supported cohomology, so the proof is immmediate, once again from "basic" results of sheaf cohomology (Iversen, Ch3, Cor 2.5 and Thm 2.7) □

Corollary 8.0.16. *In the above situation, if G is an abelian group then the natural maps*

$$R^iF_*(\underline{G})_y \to H^i(f^{-1}(y), \underline{G})$$

are isomorphisms.

We can use the preceding result to show that in many situations, the higher direct images of constant sheaves are themselves locally constant. Before we do this, we prove a lemma which will often allow us to reduce questions about maps analytic spaces to the case of a smooth base change. This is inspired by the algebraic analogue in Mumford's *Abelian varieties* (p.56). Recall that every analytic space is locally path connected, so the connected components of an analytic space are open and locally path connected.

Lemma 8.0.17. *Let S be a connected complex analytic space and let $s_0 \in S$ be a point. Then for every $s \in S$, there are finitely many points $s_0, s_1, \ldots, s_n = s \in S$ and analytic maps $C_i \to S$ for $0 \leq i < n$ iwht C_i a connected smooth complex analytic curve whose image in S contains s_i and s_{i+1}*

Theorem 8.0.18. *Let $f : X \to S$ be a proper smooth map with connected fibers of dimension d. For any torsion-free abelian group G, $R^if_*\underline{G}$ is locally constant and compatible with base change for all $i \leq 2d$, and vanishes for $i > 2d$. Furthermore, the natural maps*

$$\underline{G} \to f_*\underline{G}$$

$$\underline{G} \otimes R^{2d}f_*\underline{\mathbb{Z}} \to R^{2d}f_*\underline{G}$$

are isomorphisms and $R^{2d}f_*\underline{\mathbb{Z}}$ is a local system of rank 1 free $\mathbb{Z}$-modules.

Note. If S is smooth, then the map f is topologically trivial locally on S and the theorem is easy. In fact, this is the essential case. Also, one can remove the assumption that G is torsion-free if one grants the rather non-trivial fact that S has a base of contractible open sets. We also note that a special case of the theorem is that if $f : E \to S$ is an elliptic curve over an analytic space, then $\underline{\mathbb{Z}} \simeq f_*\underline{\mathbb{Z}}$ and $R^1f_*\underline{\mathbb{Z}}$ is a local system of rank 2 free $\mathbb{Z}$-modules, of formation compatible with base change. We will see later that $R^2f_*\underline{\mathbb{Z}}$ and $R^2f_*\underline{\mathbb{Z}}(1)$ are invertible $\underline{\mathbb{Z}}$-modules of formation compatible with base change. We will see later that $R^2f_*\underline{\mathbb{Z}}(1)$ is *canonically* isomorphic to $\underline{\mathbb{Z}}$ (whereas defining a global trivialization of $R^2f_*\underline{\mathbb{Z}}$ requires a non-canonical choice of isomorphism $\mathbb{Z} \simeq \mathbb{Z}(1)$, which is to say a choice of $\sqrt{-1} \in \mathbb{C}$).

Proof. Since the analytic fiber product gives the topological fiber product on underlying topological spaces and S is locally compact, locally Hausdorff, we can use the above theorem to get

$$R^if_*(\underline{G}_s \simeq H^i(X_s, \underline{G}) \simeq H^i_{top}(X_s, G)$$

for all $s \in S$. Furthermore, the natural map $G \to H^0(X_s, \underline{G})$ is an isomorphism for all $s \in S$. Thus, gluing along stalks, $\underline{G} \xrightarrow{\sim} f_*\underline{G}$.

For the rest of the theorem we first want to reduce to the case where G is finitely generated. Let $\{G_\alpha\}$ be the set of finitely generated subgroups of G, so we have and isomorphism $\varinjlim \underline{G}_\alpha \simeq \underline{G}$. The induced map in cohomology

$$\varinjlim R^i f_* \underline{G}_\alpha \to R^i f_* \underline{G}$$

becomes

$$\varinjlim H^i(X_s, \underline{G}_\alpha) \to H^i(X_s, \underline{G})$$

on stalks, and this is an isomorphism since sheaf cohomology commmutes with direct limits on compact Hausdorff spaces. We conclude that the higher direct image sheaves are isomorphic, and thus we can assume that G is finitely generated. Therefore we may finally assume that G is just $\mathbb{Z}$ by the torsion-freeness assumption (without this assumption we would run into unpleasant problems of torsion-orders varying over the space).

In this case we have isomorphisms

$$H^i(X_s, \underline{G}) \simeq H^i_{top}(X_s, \mathbb{Z})$$

and we know that the second of these groups is finitely generated and vanishes for $i > 2d$ by Poincare duality. We are thus reduced to showing that $R^i f_* \underline{\mathbb{Z}}$ is locally constant for $i \leq 2d$. In the case $i = 2d$, by Poincare duality we also see that all stalks are free of rank 1 over $\mathbb{Z}$, so if $R^{2d} f_* \underline{\mathbb{Z}}$ is locally constant, then it must be locally free of rank 1 as a $\underline{\mathbb{Z}}$-module.

For the remainder of the argument we reduce to the case of a smooth base S as follows: Choose a point $s_0 \in S$ and shrink S around s_0 so that S is connected. We have an isomorphism $R^i f_*(\underline{\mathbb{Z}})_s \simeq H^i(X_{s_)}, \underline{\mathbb{Z}})$, and these are both finitely presented $\mathbb{Z}$-modules. Thus, the inverse isomorphism lifts (after possibly shrinking S around s_0 some more) to a map

$$H^i(X_{s_0}, \underline{\mathbb{Z}}) \to H^0(S, R^i f_* \underline{\mathbb{Z}})$$

for all $i \leq 2d$.

It is now necessary and sufficient to show that the induced map

$$H^i(X_{s_0}, \underline{\mathbb{Z}}) \to R^i f_*(\underline{\mathbb{Z}})_s \simeq H^i(X_s, \underline{\mathbb{Z}})$$

is an isomorphism for all $s \in S$ near s_0, as this will then imply that the map of sheaves

$$\xi : \underline{H^i(X_{s_0}, \underline{\mathbb{Z}})} \to R^i f_* \underline{\mathbb{Z}}$$

is an isomorphism near S, and thus that $R^i f_* \underline{\mathbb{Z}}$ is locally constant.

By the above lemma, we can assume that there is a smooth connected curve $\tilde{S}$ mapping to S whose image contain s_0 and s_1. By proper base change it suffices to check the isomorphism on $\tilde{S}$, so we may assume that S is smooth (and even a curve, although we will not need this). Recall that $R^i f_* \underline{\mathbb{Z}}$ is the sheafification of the presheaf

$$U \mapsto H^i(f^{-1}(U), \underline{\mathbb{Z}})$$

Since S is smooth and f is proper smooth, locally on S we have a C^∞-splitting $X \simeq S \times X_{s_0}$. The sheaf $R^i f_* \underline{\mathbb{Z}}$ is now given by

$$U \mapsto H^i(f^{-1}(U), \underline{\mathbb{Z}}) \simeq H^i(U \times X_{s_0}, \underline{\mathbb{Z}}) \simeq H^i_{top}(U \times X_{s_0}, \mathbb{Z})$$

If U is small enough so as to be contractible (such opens are certainly a base of opens on the smooth S), then the natural pullback map

$$H^i_{top}(U \times X_{s_0}, \mathbb{Z}) \to H^i_{top}(X_{s_0}, \mathbb{Z})$$

is an isomorphism. All of these isomorphisms are functorial in U, so we see that $R^i f_* \underline{\mathbb{Z}}$ is jus the constant sheaf $\underline{H^i(X_{s_0}, \underline{\mathbb{Z}})}$ and the map above is the canonical isomorphism at s_0. Thus, locally on the path connected S this composite map of constant sheaves is an isomorphism, so ξ is an isomorphism. □

If S is contractible, all locally constant sheaves are constant (via the stalk at a fixed base point). For $f^{an} : \mathcal{E}^{an} \to \mathfrak{h}$ with *base point* i, we can explicitly describe the unique isomorphism

$$(\alpha^{an})^\vee : \mathbb{Z}^2 \simeq \underline{H_1(\mathbb{C}/[1,i], \mathbb{Z})} \simeq R^1 f^{an}_*(\underline{\mathbb{Z}})^\vee$$

corresponding to a specific isomorphism on stalks at $i \in \mathfrak{h}$ (the dual α^{an} of this map is what we will use later).

Higher direct images of sheaves of differentials:

We turn now to the analytic base change of the coherent sheaf $f^{an}_* \Omega^1_{\mathcal{E}^{an}/\mathfrak{h}}$. The global relative differential form $2\pi i d\tau$ on $\mathcal{E}^{an} \to \mathfrak{h}$ shows that the map

$$f^{an}_* \left(\Omega^1_{\mathcal{E}^{an}/\mathfrak{h}} \right)_z \to H^0 \left(\mathcal{E}^{an}_z, \Omega^1_{\mathcal{E}^{an}_z} \right)$$

is surjective, since $H^0 \left(\mathcal{E}^{an}_z, \Omega^1_{\mathcal{E}^{an}_z} \right)$ is one-dimensional. It now follows from cohomology and base change that $f^{an}_* \left(\Omega^1_{\mathcal{E}^{an}/\mathfrak{h}} \right)$ is invertible and commutes with base change. The global triviality of this invertible pushforward sheaf (via $2\pi i d\tau$) is not an accident. Quite generally, a holomorphic line bundle on a contractible Stein space (e.g. $\mathfrak{h}$) is *always* (non-canonically) globally trivial. Indeed, the Picard group of such a space X sits in an exact sequence

and the first and the last groups are trivial by Steinness and contractibility respectively.

Lemma 8.0.19. *The local freeness and compatibility with base change for $f_*^{an}\Omega^1_{\mathcal{E}^{an}/\mathfrak{h}}$ are seen more conceptually via the following results:*

1. *Let $p : G \to S$ be an analytic group object with identity section e. Then there exists a canonical isomorphism $p^*e^*\Omega^1_{G/S} \simeq \Omega^1_{G/S}$ of coherent $\mathcal{O}_G$-modules, compatible with base change on S. In particular, if p is smooth of relative dimension g, then $\Omega^1_{G/S} \cong \mathcal{O}_G^{\oplus g}$ locally over S.*
2. *If $f : X \to S$ is proper flat with connected reduced fibers, then $\mathcal{O}_S \simeq f_*\mathcal{O}_X$ and this isomorphism commutes with base change.*

Thus, if X is a proper smooth group object with pure relative dimension g and connected fibers, then $f_*\Omega^1_{X/S}$ is a rank g vector bundle commuting with any base change.

Let $f : E \to S$ be an elliptic curve. We define the invertible sheaf

$$\omega_{E/S} \coloneqq f_*\Omega^1_{E/S} \simeq e^*\Omega^1_{E/S}$$

the last isomorphism coming from the above lemma. The preceding work now allows us to relativize the structures on the $\mathcal{E}_z^{an}$'s. The relativization of choosing a bases of $H^0(\mathcal{E}_z^{an}, \Omega^1_{\mathcal{E}_z^{an}})$ is choosing an isomorphism $\omega_{E/S} \simeq \mathcal{O}_S$, which can be done locally on S.

The relativization of choosing an (oriented) basis of $H_1(\mathcal{E}_z^{an}, \mathbb{Z})$ is choosing an isomorphism $\alpha^\vee : \underline{\mathbb{Z}}^2 \simeq (R^1 f_*\underline{\mathbb{Z}})^\vee$; given such an $\alpha^\vee$ we cna uniquely fill in "?" to make an anti-commutative diagram

$$\begin{tikzcd}
\bigwedge^2 R^1 f_*\underline{\mathbb{Z}} \arrow[r, "\bigwedge^2 \alpha"] \arrow[d, "\cup"] & \bigwedge^2 \underline{\mathbb{Z}}^2 \arrow[d] \\
R^2 f_*\underline{\mathbb{Z}} \arrow[r, dotted, "?"] & \underline{\mathbb{Z}}
\end{tikzcd}$$

where all arrows except the dotted are isomorphisms. We will show that the map $R^2 f_*\underline{\mathbb{Z}} \to \underline{\mathbb{Z}}$ in the bottome row induces the analytic map $H^2(E_s, \underline{\mathbb{Z}}) \simeq \mathbb{Z}$ on fibers corresponding to the i-orientation of each analytic fiber manifold E_s. To check this, we will use the second part of the following theorem. Before stating the result, we make a remark about intrinsic integration on a complex manifold. Let M be a complex manifold with pure dimension d and let ω be a compactly supported, $\mathbb{C}$-valued, C^∞ differential form on M of degree $2d$. Endowing M with the i-orientation for a choice of $i = \sqrt{-1} \in \mathbb{C}$, the integral

$$\frac{1}{(2\pi i)^d} \int_M \omega$$

is independent of the choice of i. Whenever such an integral expression is written down, it will be implicitly understood that the integration is computed w/r/t the i-orientation on M.

Theorem 8.0.20. *Let $f : X \to S$ be a proper smooth map of pure relative dimension d and connected fibers. Then there is a canonical isomorphism of $\mathcal{O}_S$-modules*

$$R^d f_* \Omega^d_{X/S} \simeq R^{2d} f_* \underline{\mathbb{C}} \otimes_{\underline{\mathbb{C}}} \mathcal{O}_S$$

compatible with base change.

Also, there exists a unique isomorphism $R^{2d} f_* \underline{\mathbb{C}} \simeq \underline{\mathbb{C}}$ inducing the map

$$\frac{1}{(2\pi i)^d} \int_{X_s} : H^{2d}(X_s, \underline{\mathbb{C}}) = H^{2d}_{dR}(X_s, \mathbb{C}) \simeq \underline{\mathbb{C}}$$

on fibers. This induces a canonical isomorphism $R^{2d} f_* \underline{\mathbb{Z}}(d) \simeq \underline{\mathbb{Z}}$ via the injection $\underline{\mathbb{Z}}(d) \hookrightarrow \underline{\mathbb{C}}$. Consequently, upon making a choice of i which we use to identify $\mathbb{Z}(1) = \mathbb{Z}$ via $2\pi i \mapsto 1$ (and hence $\mathbb{Z}(r) = \mathbb{Z}$ for all integers r), there is a canonical isomorphism $R^{2d} f_* \underline{\mathbb{Z}} \simeq \underline{\mathbb{Z}}$ inducing the ismormorphism $H^{2d}(X_s, \underline{\mathbb{Z}}) \simeq \underline{\mathbb{Z}}$ corresponding to the i-orientation on X_s for all $s \in S$ (or, equivalently, inducing the map

$$\int_{X_s} : H^{2d}_{top}(X_s, \mathbb{Z}) \to \mathbb{Z}$$

of integration w/r/t the i-orientation on the manifold X_s).

Proof. □

References

[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra.* Addison Wesley, 1969.

[Bum98] D. Bump. *Automorphic Forms and Representations.* Cambridge University Press, 1998.

[CS86] G. Cornell and J.H. Silverman. *Arithmetic Geometry.* Springer-Verlag, 1986.

[Dei13] A. Deitmar. *Automorphic Forms.* Springer, 2013.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms.* Springer, 2005.

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer, 1977.

[Hid00] H. Hida. *Modular Forms and Galois Cohomology.* Cambridge University Press, 2000.

[Hid12] Haruzo Hida. *Geometric Modular Forms and Elliptic Curves.* World Scientific, 2012.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, 2002.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[Ste07] W. Stein. *Modular Forms, a Computational Approach.* American Mathematical Society, 2007.