Elliptic Curves and Complex Abelian Varieties

Jeffrey Yelton

February 17, 2017

Chapter 1

Introduction

This text is essentially a compilation of notes I used to give lectures for a graduate class I taught at the University of Milan in late 2016 and early 2017. My original conception was of a first-semester course on elliptic curves mostly from an algebraic background as was taught to me when I was in graduate school. However, after interviewing some of my students beforehand, I decided to choose which material to include based on their interests and background. As they were very strong in complex analysis and complex algebraic geometry, I wound up spending most of my lecture time on the theory of complex abelian varieties (theta functions on complex tori, algebraization, uniformization of complex elliptic curves, and a quick survey of polarizations), with only a slight emphasis on elliptic curves. In the last several lectures I introduced the algebraic theory of elliptic curves over arbitrary fields and was able to go over certain material on the classification of their endomorphism rings. Unfortunately however, I ran out of time to get to many crucial algebraic topics such as the Weil pairing, reduction of elliptic curves over local fields, and the Mordell-Weil theorem.

I taught the course assuming prerequisite knowledge based on the areas in which my students generally seemed to have strong backgrounds. This is also reflected in the lecture notes. For instance, these notes assume background knowledge of basic complex manifolds and algebraic topology. They also assume that the reader has a reasonably strong background in abstract and linear algebra, and that they have taken a first course in algebraic geometry or at least has basic knowledge of the theory of projective varieties over fields. I went out of my way to avoid any mention of schemes, however, and in developing the theory of theta functions I chose to use the language of Cartier divisors (later changed to Weil divisors in the case of elliptic curves) rather than line bundles. Some facts from algebraic geometry which are a little less basic, such as the Riemann-Roch Theorem, are explained carefully but not proven. The same is true of basic Lie theory, which is used only for §2.1. I have kept algebraic number theory to a minimum (although if the course had gone on longer, of course there would have been much more of it). Several ideas and results that I did not have time to teach are outlined in some of the provided exercises.

My main sources for Chapter 2 were the first chapter of David Mumford's book *Abelian Varieties* ([5]) as well as Michael Rosen's and James Milne's articles on abelian varieties in the book *Arithmetic Geometry* edited by Cornell and Silverman ([7] and [3] respectively), the latter of which was used particularly for the material on polarizations. For the Abel-Jacobi Theorem I mainly consulted Serge Lang's book *Introduction to Algebraic and Abelian*

Functions ([2]) while adopting some variations on his proof; for someone with a more complex analytic background, [1] might be a good alternative. For the algebraic material in Chapter 3, it is not surprising that everything came from Silverman's (first) book *The Arithmetic of Elliptic Curves* ([8]).

1.1 Three definitions for elliptic curves

We begin by giving three definitions for an elliptic curve. Eventually we will explain each definition more clearly and show that the definitions are equivalent. Our first definition presents elliptic curves as a particular case of a much more general object: abelian varieties. Our initial focus in this course will be on examining abelian varieties over the complex numbers (that is, we will assume $K = \mathbb{C}$ in the definition below) with a particular emphasis on complex elliptic curves.

Definition 1.1.1. *A **group variety** over a field K is an algebraic variety A over K with the property that there is a group law on the set of points $A(K)$ such that group multiplication and inversion are given by morphisms $m : A \times A \to A$ and $i : A \to A$. An **abelian variety** is a group variety which is complete.*

*An **elliptic curve** over a field K is an abelian variety of dimension 1 over K.*

Remark 1.1.2. a) We note that an abelian variety is smooth. Indeed, on any variety over K, there is a K-point x_0 at which the variety is smooth. If A is an abelian variety, for each $y \in A$, the translation-by-y map $t_y : A \to A$ given by $x \mapsto yx$ is an invertible morphism from A to itself and therefore induces an isomorphism on the tangent spaces $(t_y)_* : T_{x_0}X \xrightarrow{\sim} T_{yx_0}X$. Since every $a \in A$ is equal to yx_0 for some y, the tangent spaces at all points of A are isomorphic to $T_{x_0}A$, and so A is smooth everywhere.

b) It is possible to show from Definition 1.1.1 that the group law on A is commutative, using in particular the fact that A is complete (see §4 of [5] or §2 of [3]). We will show this for complex abelian varieties (i.e. $K = \mathbb{C}$) in §2.1 but not in the general case. So every abelian variety has the structure of an abelian group; the use of the adjective "abelian" is somewhat coincidental, as they were each independently named after Henrik Abel. However, note that a group variety may have an abelian group structure without being complete and therefore without being an abelian variety, e.g. the affine line $\mathbb{A}^1_K$ with additive group structure, or the punctured affine line $\mathbb{A}_K \setminus \{0\}$ with multiplicative group structure.

The next definition comes more directly from the classical setting of algebraic curves.

Definition 1.1.3. *An **elliptic curve** over a field K is a smooth projective genus-1 curve E over K along with a distinguished K-point $O \in E(K)$.*

Finally, we give the most elementary definition, to provide motivation for what follows by giving a more concrete idea of the structure inherent in an elliptic curve (note that here and everywhere below, $\bar{K}$ denotes an algebraic closure of K).

Definition 1.1.4. *An **elliptic curve** E over a field K is the locus $E(\bar{K})$ of points $(x, y) \in \bar{K}^2$ satisfying an equation of the form $y^2 = f(x) := x^3 + ax + b$ for $a, b \in K$ such that the*

discriminant $-4a^3 - 27b^2$ is nonzero (i.e. the cubic polynomial $f(x)$ doesn't have multiple roots), along with an extra "point at infinity" which we denote by O. It is endowed with a binary operation $(P, Q) \mapsto P + Q$ defined as follows.

For any points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in $E \setminus \{O\}$, let L be the line connecting them. By convention, if $P = Q$, then L is the tangent line to the curve given by $y^2 = f(x)$ at P. Then the line L intersects a unique third point $R = (x_R, y_R)$ in $E(\bar{K})$ (if the line L is vertical, then we take $R = O$). We define the sum of P and Q, denoted $P + Q$ or $Q + P$, to be the point $(x_R, -y_R)$ (which is again O if $R = O$).

For any point $P \in E(\bar{K})$, we define the sum of P and O to be $P + O = O + P = P$.

For any algebraic extension $K' \supseteq K$, we define $E(K')$ to be the set of points in $E(\bar{K})$ whose coordinates lie in K'. By convention, $O \in E(K')$.

Remark 1.1.5. The set of points $E(\bar{K})$ is really the set of K-points of the projective curve given by the homogenization $y^2z = x^3 + axz^2 + bz^3$ of the defining equation. Viewed this way, the "point at infinity" O is given by $(x : y : z) = (0 : 1 : 0)$. Loosely speaking, we may visualize it as a point lying "above" the affine curve on the two-dimensional coordinate plane, with the y-coordinate being infinity. In this way, it makes sense that every vertical line $x = x_0$ intersects the curve at points $P := (x_0, y_0)$, $(x_0, -y_0)$, and O, thus justifying the assignment of $P + O = O + P = P$ and the convention that "if the line L is vertical, then we take $R = O$" above.

It turns out that the binary operation on the set $E(\bar{K})$ which we defined above is a commutative group law (thus justifying our use of the "+" notation).

Proposition 1.1.6. *The binary operation given in Definition 1.1.4 is a group law on the set $E(\bar{K})$. More precisely,*

a) it is commutative, and the point $O \in E(\bar{K})$ acts as an additive identity;

b) any point $P = (x_P, y_P) \in E(\bar{K})$ has an inverse $-P \in E(\bar{K})$ given by $-P = (x_P, -y_P)$; and

c) it is associative, i.e. $(P + Q) + R = P + (Q + R)$ for any $P, Q, R \in E(\bar{K})$.

Parts (a) and (b) of the above proposition are immediate from Definition 1.1.4, while part (c) is very tedious to prove (we will prove it later in an elegant way using the concept of Picard group).

Remark 1.1.7. Note that for any algebraic extension $K' \supset K$, $E(K')$ is a subgroup of $E(\bar{K})$, and if K'' is an algebraic extension of K', then $E(K'')$ is a subgroup of $E(K')$. This follows from the fact that the slope of the line L from the definition must be an element of any field containing the coordinates of the points P and Q.

In fact, it is possible to write down a formula for the addition law involving rational functions of the coordinates of the two imput points, where all coefficients lie in K. In the language of algebraic geometry, this is equivalent to the very important fact that the addition law is a morphism $E \times E \to E$ defined over K.

1.2 Exercises

Exercise 1.2.1. Let E be the elliptic curve over $\mathbb{Q}$ given by the locus of points satisfying $y^2 = x^3 - x$; let $P = (0,0) \in E(\mathbb{Q}) \subset E(\bar{\mathbb{Q}})$; and let $Q := (x_0, y_0)$ be any point in $E(\bar{\mathbb{Q}}) \setminus \{(0,0)\}$. Compute $P + Q = (-1/x_0, -y_0/x_0^2)$.

Exercise 1.2.2. Actually prove directly part (c) of Proposition 1.1.6 – that is, show the addition law given in Definition 1.1.4 satisfies the associative property. (This is extremely tedious and I have never fully attempted it!)

Exercise 1.2.3. Given any elliptic curve $E : y^2 = f(x)$ as in Definition 1.1.4 over a field K, characterize all points of order 2 in $E(K)$. Show that the 2-torsion subgroup of $E(K)$ must be finite. What are the possible structures of the 2-torsion subgroup of $E(K)$, and how do they depend on the cubic polynomial $f(x) \in K[x]$? What is the group structure of the 2-torsion subgroup of $E(\bar{K})$?

1.3 (Tentative) outline of the course

We want to relate the three definitions given above for elliptic curves by studying the more general objects known as abelian varieties and showing that an abelian variety of dimension 1 has to be a curve with the properties given in Definition 1.1.3 and also by showing that any curve satisfying Definition 1.1.3 can be expressed in the form given in Definition 1.1.4 with an additive group law on its points. In our journey through these different ways of viewing elliptic curves, we will stop to further examine many interesting results.

We will first (in §2) study the theory of complex abelian varieties from the point of view of examining complex tori and certain meromorphic functions known as *theta functions* which can be used to realize (some of) them as abelian varieties. We will also state and prove the Abel-Jacobi theorem, which can be used to construct classical examples of complex abelian varieties (where the ground field K is $\mathbb{C}$), including complex elliptic curves.

We will then (in §3) examine elliptic curves over a general ground field K, focusing mainly on maps between elliptic curves and endomorphism rings. In particular, we will study ordinary and supersingular elliptic curves over finite fields and their endomorphism rings, and we will end by introducing the Tate module.

Chapter 2

Complex abelian varieties

The goal of this chapter is to describe as fully as possible what properties characterize complex abelian varieties and in particular complex elliptic curves. We start by noting that by Definition 1.1.1, a complex abelian variety is in particular a complete complex variety. Since completeness of a complex variety implies compactness as a complex manifold, and the group law as in the definition gives this complex manifold the structure of a complex Lie group, every complex abelian variety is a connected compact complex Lie group. We will therefore begin our study of complex abelian varieties by investigating connected compact complex Lie groups. We will see that in dimension 1, every connected compact complex Lie group is an abelian variety (an elliptic curve), but that in dimension ≥ 2, many connected compact complex Lie groups cannot be given an algebraic structure and therefore are *not* abelian varieties. Our most important result will be a criterion for when a connected compact complex Lie group is an abelian variety.

2.1 Connected compact complex Lie groups

We first want to determine the structure of connected compact complex Lie groups (for the moment, we are not considering whether or not they are algebraic).

Proposition 2.1.1. *Let X be a connected compact complex Lie group. Then X is commutative.*

Proof. Let e denote the identity element of X and let T_eX denote the tangent space of X at e; it is a complex vector space of dimension equal to the dimension of X. For any $x \in X$, write $\phi_x : X \to X$ for the conjugation-by-x map $a \mapsto x^{-1}ax$. Then ϕ_x induces an endomorphism $(\phi_x)_* : T_eX \to T_eX$ of the tangent space. It is clear that the map $\phi : X \to \mathrm{End}_{\mathbb{C}}(T_eX)$ sending $x \in X$ to the endomorphism $(\phi_x)_* \in \mathrm{End}_{\mathbb{C}}(T_eX)$ is a homomorphism of groups (so its image lies in the group of automorphisms $\mathrm{Aut}(T_eX)$) as well as a holomorphic map. (In fact, it can be used to define the Lie bracket on T_eX.) Since X is compact and $\mathrm{End}_{\mathbb{C}}(T_eX)$ is affine, ϕ must be a constant map and is therefore the trivial homomorphism; that is, $(\phi_x)_* = 1 \in \mathrm{Aut}(T_eX)$ for all $x \in X$.

Recall that the *exponential map* from the Lie algebra T_eX to the Lie group X is given by $v \mapsto \gamma_v(1)$ where $\gamma_v : \mathbb{C} \to X$ is the unique holomorphic map whose differential $(\gamma_v)_* :$

$\mathbb{C} = T_0\mathbb{C} \to T_eX$ sends 0 to v. The exponential map has the important property of being a biholomorphism when restricted to the inverse image of a small enough open neighborhood of $0 \in T_eX$. Moreover, exponential maps commute with holomorphic homomorphisms between Lie groups and their induced maps on the corresponding Lie algebras (which are the tangent spaces at the identity). It follows from these properties that given some small enough open neighborhood $U \ni 1 \in X$, ϕ_x acts as the identity on U for all $x \in X$. Now we claim that any such U generates X as a group. Indeed, if we let U' denote the subgroup of X generated by U, then U' is also open since for each $x \in U'$, $xU \subseteq U'$, and the connectedness of X proves that its only open subgroup is X itself. It follows from this that since each ϕ_x is a group automorphism, ϕ_x must act as the identity on all of X for any $x \in X$. Thus, X is commutative.

□

In light of the above proposition, from now on, we will use "+" to denote the group operation on X and denote the identity of X by 0.

Proposition 2.1.2. *Let X be a connected compact complex Lie group of dimension g. Then X is a complex torus; that is, $X \cong V/\Lambda$, where V is a complex vector space of dimension g, Λ is a full lattice (i.e. of rank $2g$) in V, and V/Λ is given the Lie group structure it inherits as a quotient of the Lie group V.*

Proof. Let $\pi : T_0X \to X$ be the exponential map defined in the proof of Proposition 2.1.1. One can show directly from the definition of the exponential map that the commutativity of X implies that π is a homomorphism. Let $a \in X$ be an element lying in the image of π, and let U be a small enough open neighborhood of $1 \in X$ such that $\pi|_W : W \to U$ is an isomorphism for some open $W \subseteq \pi^{-1}(U)$ with $0 \in W$. Then clearly the subset $a + U$ is contained in the image of π, and so the image of π is open. Since X is connected, this implies that π is surjective. Now if $v \in T_0X$ is any element of $\ker(\pi)$, it is clear that for W as above, $(v + W) \cap \ker(\pi) = \{v\}$. It follows that $\ker(\pi)$ is a discrete subgroup of T_0X. The fact that X is compact implies that $\Lambda := \ker(\pi)$ is a full lattice in $V := T_0(X)$, and the proposition is proved.

□

Remark 2.1.3. It is easy to see from the holomorphic isomorphism $X \cong V/\Lambda$ that $\pi : V \to X$ is a covering map. Since V is simply connected, it is in fact a universal covering space for X. It immediately follows that the fundamental group $\pi_1(X, 0)$, as well as the first singular homology group $H_1(X, \mathbb{Z})$, can be identified with $\Lambda \cong \mathbb{Z}^{2g}$. Note moreover that this result shows that X is homeomorphic to $(S^1)^{2g}$, so it is very easy to compute the dimensions of the singular homology groups $H_i(X, \mathbb{Z})$ for all $i \geq 0$ in terms of the dimension of X.

Corollary 2.1.4. *As an abstract group, X is divisible; that is, for any nonzero integer n, the multiplication-by-n map $[n] : X \to X$ is surjective. Moreover, the kernel $X[n]$ of $[n]$ is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^{2g}$, where g is the dimension of X.*

Proof. We construct an isomorphism of real vector spaces $V \xrightarrow{\sim} \mathbb{R}^{2g}$ by choosing a basis of the free $\mathbb{Z}$-module $\Lambda \subset V$ and sending each basis element to a standard basis element of $\mathbb{R}^{2g}$. This induces an isomorphism of quotient groups $X \cong V/\Lambda \xrightarrow{\sim} (\mathbb{R}/\mathbb{Z})^{2g}$, from which the statements immediately follow.

□

2.2 Divisors on complex tori

We now want to study the group of divisors on any complex torus X, with our eventual goal being a characterization of all ample divisors on X which (if they exist) may be used to characterize X as an algebraic variety. In this subsection, we will only use a fairly elementary definition of Cartier divisors, which will be more convenient for the moment, although the reader who has studied divisors in the context of algebraic geometry should keep in mind that this is equivalent to the notion of Weil divisors (formal sums of codimension-1 subvarieties) in the case that X is a (smooth) complex variety.

Definition 2.2.1. *Let Y be a connected complex manifold.*

a) The (additive) group $\mathrm{Div}(Y)$ *of* ***Cartier divisors*** *on Y is defined as follows. Each element of* $\mathrm{Div}(Y)$ *is a couple $D = \{\{U_i\}_{i\in I}, \{f_i\}_{i\in I}\}$, where $\{U_i\}_{i\in I}$ is a finite open cover of Y and, for each $i \in I$, f_i is a meromorphic function defined on the open subset $U_i \subset Y$ such that for any $i, j \in I$ such that $U_i \cap U_j \neq \varphi$, the quotient f_i/f_j (and f_j/f_i) is holomorphic and nonvanishing on $U_i \cap U_j$. We define the sum of two elements $D_1 = (\{U_i\}_{i\in I}, \{f_i\}_{i\in I})$ and $D_2 = (\{V_j\}_{j\in J}, \{f_j\}_{j\in J})$ to be $D_1 + D_2 := (\{U_i \cap V_j\}_{(i,j)\in I\times J}, \{f_i g_j\}_{(i,j)\in I\times J})$.*

b) A divisor $D = (\{U_i\}_{i\in I}, \{f_i\}_{i\in I})$ defined in this way is said to be ***positive*** *or* ***effective*** *if each f_i is holomorphic on U_i. It is said to be* ***trivial*** *if each f_i is both holomorphic and nonvanishing on U_i.*

By abuse of notation, we will identify two divisors D and D' if their difference $D - D'$ is a trivial divisor. If a divisor D is identified in this way with some $(\{U_i\}_{i\in I}, \{f_i\}_{i\in I})$ for some open cover $\{U_i\}_{i\in I}$, then we say that D can be "represented by" this data.

c) A divisor $D \in \mathrm{Div}(Y)$ is said to be ***principal*** *if it can be represented by $(\{Y\}, \{f\})$ for some nonzero meromorphic function f on Y. In this case, we denote D by (f).*

We observe right away that the divisor group is commutative (hence the "+" notation) and that the trivial divisor (which we denote by 0) is the identity element. It is easy to verify that the notion of positivity or effectiveness of divisors induces a partial ordering on the divisor group; namely, we write $D \geq D'$ if $D - D'$ is positive (thus a divisor D is positive if and only if $D \geq 0$).

We denote the field of meromorphic functions on Y (resp. the set of principal divisors on Y) by $\mathcal{M}(Y)$ (resp. by $\mathrm{Prin}(Y)$). The following fact is obvious from the definitions.

Proposition 2.2.2. *The set of principal divisors on a complex manifold Y forms a subgroup of* $\mathrm{Div}(Y)$ *and is the image of the homomorphism $\mathcal{M}(Y)^\times \to \mathrm{Div}(Y)$ defined by sending any nonzero meromorphic function f to the divisor represented by $(\{Y\}, \{f\})$. The kernel of this homomorphism is the subgroup of nowhere-vanishing holomorphic functions on Y.*

The functor taking a complex manifold Y to its group of divisors $\mathrm{Div}(Y)$ is contravariant. Indeed, there is a very straightforward way to define pullbacks of divisors via holomorphic maps $f : Y' \to Y$; namely, given any divisor $D \in \mathrm{Div}(Y)$ represented by $(\{U_i\}_{i\in I}, \{f_i\}_{i\in I})$, we let $f^*(D) \in \mathrm{Div}(Y')$ be given by $(\{f^{-1}(U_i)\}_{i\in I}, \{f_i \circ f\}_{i\in I})$. In this way, $f : Y' \to Y$ induces a homomorphism of groups $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(Y')$.

In our quest to characterize ample divisors on our complex torus X (if they exist), it will be necessary to study positive divisors on X. It would be nice to be able to characterize

positive divisors on X as principal divisors, since then our investigation would boil down to considering the set of holomorphic functions on X. But unfortunately, since X is compact, the only holomorphic functions defined everywhere on X are the constant functions, so the only positive principal divisor in $\mathrm{Div}(X)$ is the trivial divisor 0. However, we can pull back any divisor on X via $\pi : V \to X$ to get a divisor on V, and it turns out that the resulting divisor is principal by the following classical result (known as Cousin's Theorem).

Theorem 2.2.3. *Every divisor on the complex manifold $\mathbb{C}^n$ for any $n \geq 1$ is principal.*

Definition 2.2.4. *A divisor on V is said to be **periodic** if it lies in the image of $\pi^* : \mathrm{Div}(X) \to \mathrm{Div}(V)$.*

We now want to characterize all periodic divisors on V by representing them with functions in $\mathcal{M}(V)$ that have nice properties. We observe first of all that if $f \in \mathcal{M}(V)$ has periodic divisor with respect to the lattice Λ, that means that for each $\lambda \in \Lambda$, $g_\lambda(v) := f(v+\lambda)/f(v) \in \mathcal{M}(V)$ must be holomorphic and nonvanishing. Moreover, these functions g_λ satisfy the compatibility condition that

$$g_{\lambda_1+\lambda_2}(v) = g_{\lambda_1}(v) g_{\lambda_2}(v+\lambda_1), \quad \forall \lambda_1, \lambda_2 \in \Lambda. \tag{2.1}$$

Moreover, since each g_λ is holomorphic and nonvanishing, we may write $g_\lambda = e^{2\pi i G_\lambda}$ for some holomorphic function $G_\lambda \in \mathcal{M}(V)$. Then the condition in (2.1) becomes

$$G_{\lambda_1+\lambda_2}(v) \equiv G_{\lambda_1}(v) + G_{\lambda_2}(v+\lambda_1) \mod \mathbb{Z}, \quad \forall \lambda_1, \lambda_2 \in \Lambda. \tag{2.2}$$

Recall that a function $H : V \times V \to \mathbb{C}$ is a Hermitian form on the complex vector space V if it is $\mathbb{C}$-linear in the first argument, and if $H(w,v) = \overline{H(v,w)}$ for all $v, w \in V$. It is an easy exercise in linear algebra to show that a function $H : V \times V \to \mathbb{C}$ is a Hermitian form if its imaginary part $E := \Im H : V \times V \to \mathbb{R}$ is an $\mathbb{R}$-linear alternating form (i.e. $E(w,v) = -E(v,w)$ for all $v, w \in V$) and if $E(iv, iw) = E(v,w)$ for all $v, w \in V$. Conversely, any such $E : V \times V \to \mathbb{R}$, determines a Hermitian form $H : V \times V \to \mathbb{C}$ by $H(v,w) = E(iv,w) + iE(v,w)$.

Definition 2.2.5. *Let $H : V \times V \to \mathbb{C}$ be a Hermitian form with imaginary part E. A **theta function** for H (with respect to the lattice Λ) is a function $\theta \in \mathcal{M}(V)$ which satisfies the property that, for all $v \in V$ and $\lambda \in \Lambda$,*

$$\theta(v+\lambda) - \theta(v) = e^{2\pi i (L(v,\lambda) + J(\lambda))}$$

for some map $J : \Lambda \to \mathbb{C}$ and some map $L : V \times \Lambda \to \mathbb{C}$ which is $\mathbb{C}$-linear in the first argument and such that $E(\lambda_1, \lambda_2) = L(\lambda_1, \lambda_2) - L(\lambda_2, \lambda_1)$ for $\lambda_1, \lambda_2 \in \Lambda$.

We will give an incomplete proof of the following result, as the only full argument I know involves techniques of sheaf cohomology which are beyond the scope of this course (see the arguments in §2 of [5]).

Proposition 2.2.6. *For every divisor $D \in \mathrm{Div}(X)$, there is a unique Hermitian form H and a function $\theta \in \mathcal{M}(V)$ with $(\theta) = \pi^* D$, which is a theta function for H.*

Proof. We omit the proof of the fact that there always exists a function $\theta \in \mathcal{M}(V)$ with $(\theta) = \pi^* D$ such that

$$\theta(v+\lambda)/\theta(v) = e^{2\pi i(L(v,\lambda)+J(\lambda))}, \quad \forall v \in V,\ \lambda \in \Lambda$$

with $L : V \times \Lambda \to \mathbb{C}$ linear in the first argument. The fact that L can be $\mathbb{R}$-linearized to a $\mathbb{C}$-bilinear form on V such that $E : V \times V \to \mathbb{C}$ given by $E(v,w) = L(v,w) - L(w,v)$ is the imaginary part of a Hermitian form is shown in the proof of Proposition 2.2.7 below.

□

Proposition 2.2.7. *Let $H : V \times V \to \mathbb{C}$ be the Hermitian form associated to some divisor $D \in \mathrm{Div}(X)$ via Proposition 2.2.6. Then any function $\theta \in \mathcal{M}(V)$ such that $(\theta) = \pi^* D$ can be written as $h\theta_D$, where h is a trivial theta function (i.e. $(h) = 0 \in \mathrm{Div}(V)$) and $\theta_D \in \mathcal{M}(V)$ is a theta function satisfying*

$$\theta_D(v+\lambda)/\theta_D(v) = e^{\pi H(v,\lambda)+\frac{1}{2}\pi H(\lambda,\lambda)+2\pi i K(\lambda)},$$

where $K : \Lambda \to \mathbb{R}$ satisfies the property that

$$K(\lambda_1+\lambda_2) - K(\lambda_1) - K(\lambda_2) \equiv \frac{1}{2}E(\lambda_1,\lambda_2) \mod \mathbb{Z}, \quad \forall \lambda_1, \lambda_2 \in \Lambda.$$

Moreover, θ_D is unique up to a constant in $\mathbb{C}^\times$.

Proof. Let $\theta \in \mathcal{M}(V)$ be a theta function for H with $(\theta) = \pi^* D$ such that $\theta(v+\lambda) - \theta(v)$ is of the form $e^{2\pi i(L(v,\lambda)+J(\lambda))}$ as in Definition 2.2.5. Then for any $\lambda_1, \lambda_2 \in \Lambda$, condition (2.2) can be written as

$$L(v,\lambda_1+\lambda_2) + J(\lambda_1+\lambda_2) \equiv L(v,\lambda_1) + L(v,\lambda_2) + L(\lambda_1,\lambda_2) + J(\lambda_1) + J(\lambda_2) \mod \mathbb{Z}, \quad (2.3)$$

which forces $L(v,\lambda_1+\lambda_2) \equiv L(v,\lambda_1) + L(v,\lambda_2) \pmod{\mathbb{Z}}$ and $J(\lambda_1+\lambda_2) - J(\lambda_1) - J(\lambda_2) \equiv L(\lambda_1,\lambda_2) \pmod{\mathbb{Z}}$. Moreover, by switching the roles of λ_1 and λ_2, we get $L(\lambda_1,\lambda_2) \equiv L(\lambda_2,\lambda_1) \pmod{\mathbb{Z}}$. In particular, L is $\mathbb{Z}$-linear in the second argument, and we may extend L to a map $V \times V \to \mathbb{C}$ which is $\mathbb{R}$-bilinear and symmetric modulo $\mathbb{Z}$. Set $E(v,w) = L(v,w) - L(w,v)$ for all $v, w \in V$. Then $E : V \times V \to \mathbb{C}$ is clearly $\mathbb{R}$-bilinear and skew-symmetric; moreover, $E(\Lambda,\Lambda) \subseteq \mathbb{Z}$, and so E takes values in $\mathbb{R}$. It is also an easy exercise to check that $E(iv,iw) = E(v,w)$ for all $v, w \in V$. Therefore, in particular E is the imaginary part of the Hermitian form $H : V \times V \to \mathbb{C}$ given by $H(v,w) = E(iv,w) + iE(v,w)$, as in the discussion above.

Now it is easy to see that if $h \in \mathcal{M}(V)$ is any trivial theta function, then h must be of the form $e^{2\pi i(A(v)+B(v)+C)}$, where $A : V \to \mathbb{C}$ is a quadratic form, $B : V \to \mathbb{C}$ is a linear functional, and $C \in \mathbb{C}$ is a constant. Then for any $\lambda \in \Lambda$, $h(v+\lambda)/h(v)$ can be written as

$$e^{2\pi i([A(v+\lambda)-A(v)-A(\lambda)]+[A(\lambda)+B(\lambda)])},$$

with $A(v+\lambda) - A(v) - A(\lambda)$ symmetric and bilinear. Using this, one can check that the Hermitian form H corresponding to such an h is trivial. It follows that there is a well-defined map (which is in fact a group homomorphism) from the set of all theta functions to the group

of all Hermitian forms on V which sends a theta function for some Hermitian form H to H, and that the kernel of this homomorphism contains the group of trivial theta functions.

It thus suffices to check that the $\mathbb{R}$-bilinear map $L_0 : V \times \Lambda \to \mathbb{C}$ given by $L_0(v, \lambda) = \frac{1}{2i}H(v, \lambda) + J(\lambda)$ for $v \in V$, $\lambda \in \Lambda$ satisfies $L_0(v, \lambda) - L_0(\lambda, v) = E(v, \lambda)$. Then by what was shown above, $J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \equiv \frac{1}{2i}H(\lambda_1, \lambda_2) \pmod{\mathbb{Z}}$ for $\lambda_1, \lambda_2 \in \Lambda$ and, setting $K(\lambda) = J(\lambda) - \frac{1}{4i}H(\lambda, \lambda)$, we get $K(\lambda_1 + \lambda_2) - K(\lambda_1) - K(\lambda_2) \equiv \frac{1}{2}E(\lambda_1, \lambda_2) \pmod{\mathbb{Z}}$. Since E takes values in $\mathbb{R}$, the imaginary part $\Im K$ of K is additive on Λ and can therefore be extended to an $\mathbb{R}$-linear functional $\Im K : V \to \mathbb{C}$. Note that $\Im K(iv) + i\Im K(v)$ defines a $\mathbb{C}$-linear functional $V \to \mathbb{C}$ whose imaginary part is $\Im K$. Now by replacing θ with θ divided by the trivial theta function $e^{\Im K(iv)+i\Im K(v)}$, we may assume that K is takes values in $\mathbb{R}$, thus fulfilling the properties given in the statement of the proposition.

The uniqueness of θ_D up to a constant now follows quickly from the fact that there is no nontrivial linear functional $B : V \to \mathbb{C}$ which takes values in $\mathbb{R}$.

□

Note that it was shown in the above proof that if θ is a theta function for some Hermitian form H, the imaginary part E of H must be $\mathbb{Z}$-valued on $\Lambda \times \Lambda$. This motivates the following crucial definition.

Definition 2.2.8. *A **Riemann form** associated to a complex torus $X \cong V/\Lambda$ is a Hermitian form on V whose imaginary part is $\mathbb{Z}$-valued on $\Lambda \times \Lambda$.*

2.3 Algebraization of complex tori

For any divisor $D \in \mathrm{Div}(X)$, we set

$$\mathcal{L}(D) = \{f \in \mathcal{M}(X) \mid (f) + D \geq 0\} \cup \{0\}.$$

(We may think of the divisor associated to the constant function 0 as greater than every other divisor.) Note that $\mathcal{L}(D)$ is a vector space.

For any divisor $D \in \mathrm{Div}(X)$, let $\theta_D \in \mathcal{M}(V)$ be a theta function satisfying the property given in the statement of Proposition 2.2.7 (this is called a *normalized theta function*), and let $\mathcal{L}(\theta_D)$ denote the set of all holomorphic functions $\theta \in \mathcal{M}(V)$ which have the same "translation functions" as θ_D has, i.e. $\theta(v + \lambda)/\theta(v) = \theta_D(v + \lambda)/\theta_D(v)$ (by convention, $0 \in \mathcal{L}(\theta_D)$). It is clear that $\mathcal{L}(\theta_D)$ is also a vector space. In fact, it is easy to see from the definitions that we have an isomorphism $\mathcal{L}(\theta_D) \xrightarrow{\sim} \mathcal{L}(D)$ given by $\theta \mapsto \theta/\theta_D$.

Our goal is to characterize ample divisors $D \in \mathrm{Div}(X)$ in terms of their corresponding Riemann forms. If we can find an ample divisor D, we can use generators of $\mathcal{L}(nD)$ for some integer $n \geq 1$ to embed X into projective space over $\mathbb{C}$ and give X the structure of a variety. The following proposition shows that there is no chance of this unless the Riemann form corresponding to D is positive definite.

Proposition 2.3.1. *Let $D \in \mathrm{Div}(X)$ be a divisor, and let $H : V \times V \to \mathbb{C}$ be its corresponding Riemann form.*

a) If H is degenerate, then any function $f \in \mathcal{L}(D)$ must factor through the quotient map $X \twoheadrightarrow X/N$, where $N \subseteq X$ is the image modulo Λ of a subspace $W \subseteq V$.

b) If H is not positive semidefinite, then $\mathcal{L}(D) = \{0\}$.

Proof. We first note that the isomorphism $\mathcal{L}(\theta_D) \xrightarrow{\sim} \mathcal{L}(D)$ given above shows that it is sufficient to prove statements (a) and (b) for holomorphic theta functions $\theta \in \mathcal{L}(\theta_D)$ rather than meromorphic functions $f \in \mathcal{L}(D)$.

Suppose that H is degenerate, i.e. the subspace $W := \{w \in V \mid H(v,w) = 0 \ \forall v \in V\}$ is not trivial, and choose any $\theta \in \mathcal{L}(\theta_D)$. Since H is trivial on $V \times (W \cap \Lambda)$, we have $\theta(w+\lambda)/\theta(w) = e^{2\pi i K(\lambda)}$ for all $\lambda \in W \cap \Lambda$. Note that since K takes values in $\mathbb{R}$, $|e^{2\pi i K(\lambda)}| = 1$. Let $K \subset V$ be a compact subset containing 0 such that $K + (W \cap \Lambda) = W$. For any fixed $v \in V$, we then have $\max_{w \in W}\{|\theta(v+w)|\} = \max_{w' \in K}\{|\theta(v+w')|\}$, which is finite because K is compact. Then by the maximum principal for holomorphic functions on W, $\theta(v+w)$ must be constant as a function of w, proving statement (a).

Now suppose that H is not positive semidefinite; i.e. there is some $v \in V$ such that $H(v,v) < 0$. Let $W \subseteq V$ be a nontrivial subspace such that $H(w,w) < 0$ for all nonzero $w \in W$. Let $K \subset V$ be a compact subset containing 0 such that $K + \Lambda = V$. Fix any $v \in V$ and $\theta \in \mathcal{L}(\theta_D)$, and consider the function on W given by $w \mapsto \theta(v+w)$. If we write $w = w' + \lambda$ for $w' \in K$ and $\lambda \in \Lambda$, then we get

$$|\theta(v+w)| = |\theta(v+w'+\lambda)| = |\theta(v+w')| e^{\pi \Re H(v+w',\lambda) + \frac{1}{2}\pi H(\lambda,\lambda)}. \tag{2.4}$$

It is straightforward to compute that

$$\Re H(v+w',\lambda) + \frac{1}{2}H(\lambda,\lambda) = \frac{1}{2}H(w,w) + \Re H(v,w) - \Re H(v,w') + \frac{1}{2}H(w',w') - \Re H(w',w'). \tag{2.5}$$

Note that as $w \to \infty$, we have $H(w,w) \to -\infty$, which dominates the other terms on the right-hand side, because $\Re H(v,w)$ is linear in w and the rest of the terms depend only on w' which varies over the compact subset K and are therefore bounded. Thus, $|\theta(v+w)| \to 0$ as $w \to \infty$. Then by the maximum principal for holomorphic functions on W, $\theta(v+w) = 0$ for all $w \in W$ and therefore $\theta \equiv 0$, proving statement (b).

□

The next result, known as the Lefschetz Embedding Theorem, says that the converse is also true.

Theorem 2.3.2. *Let H be a positive definite Riemann form. Then any divisor $D \in \mathrm{Div}(X)$ whose associated Riemann form is H is ample. More precisely, for any $n \geq 3$, the divisor $nD \in \mathrm{Div}(X)$ is very ample and there is a basis of meromorphic functions in $\mathcal{L}(nD)$ which give a closed embedding of X into projective space.*

Before we can prove this theorem, we need a major lemma that is due to Frobenius. Recall that for any $\mathbb{R}$-bilinear alternating form $E : V \times V \to \mathbb{R}$, the Pfaffian of E is defined to be the nonnegative real number $\sqrt{\det(E)}$, where $\det(E)$ is understood to be the determinant of the matrix $(E(\lambda_i, \lambda_j))$ for some (any) $\mathbb{Z}$-basis $\lambda_1, ..., \lambda_{2g}$ of Λ. We observe that $\sqrt{\det(E)}$ is a positive integer if $E(\Lambda, \Lambda) \in \mathbb{Z}$.

Lemma 2.3.3. *(a) Let Λ be any free $\mathbb{Z}$-module of rank $2g$, and let $E : \Lambda \times \Lambda \to \mathbb{Z}$ be a nondegerate alternating form. Then there is a basis $\{\lambda_1, ..., \lambda_{2g}\}$ of Λ and positive integers $e_1, ..., e_g \in \mathbb{Z}$ with $e_i | e_{i+1}$ for $1 \leq i \leq g-1$, such that $E(\lambda_i, \lambda_{i+g}) = -1$ for $1 \leq i \leq g$ and $E(\lambda_i, \lambda_j) = 0$ otherwise for $1 \leq i, j \leq 2g$.*

(b) Resuming the notation of this section, let $D \in \mathrm{Div}(X)$ be a divisor whose associated Riemann form H is positive definite with imaginary part E. Then the dimension of the complex vector space $\mathcal{L}(D)$ is $\sqrt{\det(E)}$.

Proof (sketch). Part (a) is elementary and classical and the proof is omitted.

Roughly speaking, the idea for proving (b) is to show that the vector space $\mathcal{L}(\theta_D) \cong \mathcal{L}(D)$ is $\sqrt{\det(A)}$-dimensional by representing each theta function (after multiplication by a suitable trivial theta function) as a Fourier series and showing that any such theta function is determined by $\sqrt{\det(A)}$ independent choices of coefficient. We first observe that since E is bilinear and alternating on a free $\mathbb{Z}$-module of rank $2g$, there is a rank-g sublattice $\Lambda' \subset \Lambda$ such that E is trivial on Λ' (i.e. Λ' is isotropic with respect to E). Then $V' := \mathbb{R} \otimes_{\mathbb{Z}} \Lambda'$ is a real subspace of V and $V' \cap iV'$ is a complex subspace of V on both of which H is trivial. Since H is nondegenerate, $V' \cap iV' = \{0\}$ and by dimension arguments, $V = V' \oplus iV' \cong \mathbb{C} \otimes V'$. Moreover, H is symmetric and $\mathbb{R}$-valued on $V' \times V'$ and extends uniquely to a symmetric $\mathbb{C}$-bilinear form on V which we denote by B. In fact, since H is $\mathbb{C}$-linear in the first argument, $B(v, w) = H(v, w)$ for all $v \in V$ and $w \in W$.

Now let $\theta \in \mathcal{M}(V)$ be a theta function for H which satisfies the property of normalized theta functions given in the statement of Proposition 2.2.7. Note that $K : \Lambda \to \mathbb{R}$ is linear on Λ' since E is trivial there, and so K extends uniquely to a $\mathbb{C}$-linear function $L : V \to \mathbb{C}$ which is $\mathbb{R}$-valued on V'. Then if we define $\psi \in \mathcal{M}(V)$ as $\psi(v) = e^{-\frac{1}{2}\pi B(v,v) - 2\pi i L(v)}\theta(v)$ for $v \in V$, we see that ψ is also a theta function for H and moreover, for $\lambda \in \Lambda$,

$$\psi(v + \lambda)/\psi(v) = e^{\pi(H-B)(v,\lambda) + \frac{1}{2}\pi(H-B)(\lambda,\lambda) + 2\pi i(K-L)(\lambda)}. \tag{2.6}$$

If $\lambda \in \Lambda'$, this expression becomes trivial, and it follows that ψ is periodic with respect to the rank-g sublattice Λ'. Then it is possible to write $\psi(v)$ as a Fourier series, i.e. as a sum over all functionals $\alpha : \Lambda' \to \mathbb{Z}$ of $c_\alpha e^{2\pi i \alpha(v)}$ for some coefficients c_α. By manipulating these coefficients and using the fact that H is positive definite, it is then possible to show that the set of such holomorphic functions periodic with respect to Λ' is in one-to-correspondence with the set of choices of c_α where α ranges over a set of representatives of $(\Lambda')^\vee := \mathrm{Hom}_{\mathbb{Z}}(\Lambda', \mathbb{Z})$ modulo the image of the $\mathbb{Z}$-linear map $\epsilon : \Lambda \to (\Lambda')^\vee$ given by $\lambda \mapsto E(\cdot, \lambda) : \Lambda' \to \mathbb{Z}$. Thus, the dimension of $\mathcal{L}(\theta_D)$ is equal to the index of the image of ϵ inside $(\Lambda')^\vee$.

It remains to show that the image of ϵ has (finite) index in $\mathrm{Hom}_{\mathbb{Z}}(\Lambda', \mathbb{Z})$ equal to $\sqrt{\det(E)}$, which is an elementary (though slightly tricky) exercise (hint: it follows from part (a) that the index in $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$ of the image of the map $\Lambda \to \Lambda^\vee := \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$ given by $\lambda \mapsto E(\cdot, \lambda) \in \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$ is $\det(E) = e_1 \cdot ... \cdot e_g$). □

The following corollary is immediate from the lemma and will be useful later.

Corollary 2.3.4. *If $D \in \mathrm{Div}(X)$ is a divisor whose associated Riemann form H is positive definite with imaginary part E, then for any integer $n \geq 1$, the dimension of the complex vector space $\mathcal{L}(nD)$ is $n^g\sqrt{\det(E)}$.*

Proof (of Theorem 2.3.2, sketch). We will prove this for $n = 3$. One sees from the isomorphism $\mathcal{L}(\theta_D) \xrightarrow{\sim} \mathcal{L}(D)$ given above that we need to show three things: (i) that if $\{\theta_0, ..., \theta_d\} \subset \mathcal{L}(3H)$ is a basis, then $v \mapsto (\theta_0(v) : ... : \theta_d(v)) \in \mathbb{P}^d_{\mathbb{C}}$ is well-defined everywhere on V; (ii) that the map $V \to \mathbb{P}^d_{\mathbb{C}}$ given above is injective modulo Λ; and (iii) that this map induces an injection of tangent spaces.

To prove (i), we observe that if $\theta \in \mathcal{L}(\theta_D)$ is a theta function with $\theta(v+\lambda)/\theta(v)$ in the form given in the statement of Proposition 2.2.7, then for any $a, b \in V$, the meromorphic function $\psi \in \mathcal{L}(V)$ defined by $\psi(v) = \theta(v+a+b)\theta(v-a)\theta(v-b)$ satisfies

$$\psi(v+\lambda)/\psi(v) = e^{\pi(H(v+a+b,\lambda)+H(v-a,\lambda)+H(v-b,\lambda))+\frac{3}{2}\pi H(\lambda,\lambda)+6\pi i K(\lambda)} = (\theta(v+\lambda)/\theta(v))^3 \quad (2.7)$$

for $v \in V$, $\lambda \in \Lambda$ (using the fact that H is $\mathbb{C}$-linear in the first argument). Thus, $\psi \in \mathcal{L}(3H)$, and by choosing appropriate $a, b \in V$, we can ensure for a particular $v_0 \in V$ that $\psi(v) \neq 0$ and therefore not all basis elements ψ_i vanish at v_0.

To prove (ii), it suffices to show that for any $\theta \in \mathcal{L}(\theta_D)$, for $v_1, v_2 \in V$, if $\theta(v_1+a+b)\theta(v_1-a)\theta(v_1-b)$ is a constant multiple of $\theta(v_2+a+b)\theta(v_2-a)\theta(v_2-b)$ for all $a, b \in V$, then $v_1 - v_2 \in \Lambda$. Taking logarithmic differentials with respect to a, we get

$$\frac{d\theta}{\theta}(z_1+a+b) + \frac{d\theta}{\theta}(z_1-a) = \frac{d\theta}{\theta}(z_2+a+b) + \frac{d\theta}{\theta}(z_2-a) \quad (2.8)$$

for any $b \in V$. It follows that the differential given by $v \mapsto \frac{d\theta}{\theta}(v_1+v) + \frac{d\theta}{\theta}(v_2+v)$ is translation-invariant and is therefore equal to $dL(v)$ for some linear functional L on v. After integrating and exponentiating, we get

$$\theta(v+v_2)/\theta(v+v_1) = ce^{L(v)} \Rightarrow \theta(v+(v_2-v_1))/\theta(v) = c'e^{L(v)} \quad (2.9)$$

for some constants $c, c' \in \mathbb{C}^\times$. By the property given in Definition 2.2.5 we deduce that $e^{\pi H(v_2-v_1,\lambda)} = e^{L(\lambda)}$ for all $\lambda \in \Lambda$. It is then easy to see from properties of H and L that $H(\lambda, v_2-v_1) = L(\lambda)$ for $\lambda \in \Lambda$. Now we can use this to manipulate the expression $\theta(v+\lambda)/\theta(v)$ characterizing theta functions for H in Definition 2.2.5 to show that $\theta(v+(v_2-v_1))/\theta(v)$ can also be written in such a form. Thus, θ is actually a theta function for H with respect to the lattice $\Lambda' := \Lambda + (v_2-v_1)\mathbb{Z} \supseteq \Lambda$ (note that the converse is trivially true). Since $\theta \in \mathcal{L}(\theta_D)$ was chosen arbitrarily, and by Lemma 2.3.3, the dimension of $\mathcal{L}(\theta_D)$ is $\sqrt{\det(E)}$, we see that the dimension of the vector space of theta functions for H with respect to the lattice Λ' is also $\sqrt{\det(E)}$. But it is easy to see that $\Lambda' \supsetneq \Lambda$ would imply that the determinant of the bilinear alternating form E with respect to a basis of Λ' is strictly less than the determinant with respect to a basis of Λ, which is a contradiction by applying Lemma 2.3.3 to Λ', so $\Lambda' = \Lambda$ and $v_2 - v_1 \in \Lambda$ as desired.

We omit the proof of (iii) here, except to mention that it uses a similar technique of choosing $\theta \in \mathcal{L}(\theta_D)$, taking a corresponding $\psi \in \mathcal{L}(3H)$ as above, and manipulating equations by taking logarithmic derivatives as above to reach a contradiction when one assumes that there is a nontrivial tangent vector at a point $v_0 \in V$ which goes to a trivial tangent vector via the aforementioned map $V \to \mathbb{P}^d_{\mathbb{C}}$. $\square$

We have now more or less seen the main theorem of this entire chapter, which gives a criterion for any complex torus X to be algebraic. (Note that this in turn is equivalent to X being an abelian variety, because a result of Chow shows that the multiplication and inverse maps associated to X are in fact morphisms due to the compactness of X.) We may think of it as a sort of "main theorem of complex tori" or "main theorem of complex abelian varieties" although, to my knowledge, it is not given such a name anywhere in the literature.

Theorem 2.3.5. *A complex torus $X \cong V/\Lambda$ has the structure of an abelian variety if and only if there exists a positive definite Riemann form $H : V \times V \to \mathbb{C}$ associated to X.*

It turns out to be the case that for $g \geq 2$, "most" complex tori of dimension g *do not* possess any positive definite Riemann form and are therefore not abelian varieties (we will not give a proof of this here). However, as we will see immediately at the start of the next section, every 1-dimensional has a positive definite Riemann form and is therefore an elliptic curve.

2.4 Uniformization of elliptic curves

In this subsection we deal only with a complex torus X of dimension $g = 1$, which can always be realized as an elliptic curve over $\mathbb{C}$ because it always has a positive definite Riemann form. Indeed, let $\{\lambda_1, \lambda_2\}$ any ordered basis of Λ ordered so that $\Im(\lambda_2/\lambda_1) > 0$, and define $E : \mathbb{C} \times \mathbb{C} \to \mathbb{R}$ to be the unique alternating $\mathbb{R}$-bilinear form such that $E(\lambda_1, \lambda_2) = -1$. (In fact, E does not depend on the choice of ordered basis with this property – see Exercise 2.7.1.) Then clearly $E(\Lambda, \Lambda) = \mathbb{Z}$ and it is easy to check that $E(iz, z) > 0$ for any nonzero complex number z, and so E is the imaginary part of a positive definite Riemann form $H : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$. It follows from Theorem 2.3.5 and more specifically Theorem 2.3.2 that any divisor $D \in \mathrm{Div}(X)$ whose associated Riemann form is H is ample, and in fact that $3D$ is very ample so that a basis of $\mathcal{L}(3D)$ can be used to embed X into some projective space (this is called "uniformization"). Our goal now is to make this more explicit.

It will now be more convenient to switch from viewing elements of $\mathrm{Div}(X)$ as Cartier divisors to viewing them as Weil divisors – that is, each divisor $D \in \mathrm{Div}(X)$ is a finite formal sum of points in X. Since X is a smooth curve, the notions of Cartier divisor and Weil divisor are equivalent. In particular, looking at Weil divisors allows us to use the notion of "degree": if an element $D \in \mathrm{Div}(X)$ can be written as $D = \sum_{i=1}^{m} n_i(P_i)$ for integers $n_i \in \mathbb{Z}$ and points $P_i \in X$, its *degree* is $\deg(D) = \sum_{i=1}^{m} n_i$. In this way, $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ is a homomorphism which preserves the partial ordering on $\mathrm{Div}(X)$.

Proposition 2.4.1. *There exist meromorphic functions $x, y \in \mathcal{M}(X)$ satisfying a cubic polynomial equation $f(x, y) = 0$ such that X can be identified with the closure in $\mathbb{P}^2_{\mathbb{C}}$ of the curve defined by the relation $f(x, y) = 0$.*

Proof. Let $D \in \mathrm{Div}(X)$ be a divisor whose associated Riemann form is the H defined with respect to an ordered basis $\{\lambda_1, \lambda_2\} \subset \Lambda$ as above. We note that the 2×2 matrix given by $(E(\lambda_i, \lambda_j))$ has determinant 1, so $\sqrt{\det(E)} = 1$, and so Corollary 2.3.4 says that $\dim_{\mathbb{C}} \mathcal{L}(nD) = n$ for all $n \geq 1$.

We first observe that $\deg(D) \geq 0$. Indeed, the fact that $\mathcal{L}(D)$ is nontrivial implies that there exists a nonzero function $f_0 \in \mathcal{M}(X)$ such that $(f_0) + D \geq 0$, which implies that $\deg((f_0)) \geq -\deg(D)$. But every nonzero meromorphic function on a compact Riemann manifold has as an equal number of poles and zeros (counting multiplicity), so $\deg((f_0)) = 0$ and $\deg(D) \geq 0$. Now note that if we subtract any principal divisor from D, the associated Riemann form is still H, so in particular we may and will replace D with $D - (f_0)$. Then we get $1 \in \mathcal{L}(D)$. Since $(1) = 0 \in \mathrm{Div}(X)$, in fact we have $D \geq 0$. If $D = 0$ then $\dim_{\mathbb{C}} \mathcal{L}(nD) = \dim_{\mathbb{C}} \mathcal{L}(0) = 1$ for all $n \geq 1$, a contradiction, so $D > 0$.

Since $\mathcal{L}(D)$ has dimension 1 and contains the constant functions, there are no nonconstant meromorphic functions on X whose associated divisors are $\geq -D$.

Since $\mathcal{L}(2D)$ has dimension 2, it must be generated by $\{1, x\}$, where $x \in \mathcal{M}(X)$ is some nonconstant function such that $(x) \geq -2D$.

Since $\mathcal{L}(3D)$ has dimension 3 and $\langle 1, x\rangle = \mathcal{L}(2D) \subsetneq \mathcal{L}(3D)$, there is a function $y \in \mathcal{M}(X)$ such that $\{1, x, y\}$ is a basis of $\mathcal{L}(3D)$ and $(y) \geq -3D$. We claim that y cannot be a polynomial function of x. Indeed, Theorem 2.3.2 says that $3D$ is very ample and so the function $X \to \mathbb{P}^2_{\mathbb{C}}$ given by $[1 : x : y]$ is a projective embedding. Then if y is a rational function of x, the injectivity of $[1 : x : y] : X \hookrightarrow \mathbb{P}^2_{\mathbb{C}}$ implies that $[1 : x] : X \to \mathbb{P}^1_{\mathbb{C}}$ is also injective. Note that the only possible images of $[1 : x]$ are constant or the entire Riemann sphere since X is compact and connected. But X has nontrivial fundamental group, so this is a contradiction. Therefore, $y \notin \mathbb{C}(x)$. Moreover, $\mathcal{M}(X)$ is the fraction field of $\mathbb{C}[x, y]$ modulo some polynomial relation $f(x, y) = 0$, or equivalently, $[1 : x : y]$ realizes X as the closure in $\mathbb{P}^2_{\mathbb{C}}$ of the curve defined by $f(x, y) = 0$. It remains only to show that $f \in \mathbb{C}[x, y]$ has degree 3.

Since $\mathcal{L}(4D)$ has dimension 4 and $(x^2) = 2(x) \geq -4D \in \mathrm{Div}(X)$, we get $\{1, x, y, x^2\}$ as a basis.

Since $\mathcal{L}(5D)$ has dimension 5 and $(xy) = (x) + (y) \geq -2D - 3D = -5D \in \mathrm{Div}(X)$, we get $\{1, x, y, x^2, xy\}$ as a basis.

Since $\mathcal{L}(6D)$ has dimension 6, any set of 7 elements in $\mathcal{L}(6D)$ is linearly dependent. But $1, x, y, x^2, xy, x^3, y^2 \in \mathcal{L}(6D)$ because $(x^3) = 3(x) \geq -6D \in \mathrm{Div}(X)$ and $(y^2) = 2(y) \geq -6D \in \mathrm{Div}(X)$. Since $\{1, x, y, x^2, xy\}$ is linearly independent, there must be some relation among the functions $1, x, y, x^2, xy, x^3, y^2$ where the coefficients of x^3 and y^2 are both nonzero, so x and y satisfy a cubic relation $f(x, y) = 0$.

□

In fact, with a little ingenuity it is possible to write down such meromorphic functions explicitly as functions $\mathbb{C} \to \mathbb{C} \cup \{\infty\}$ which are periodic with respect to a given lattice Λ. Consider the below function discovered by Weierstrass.

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

This is called the "Weierstrass P-function". It is clear upon inspection that $\wp(z + \lambda) = \wp(z)$ for any $z \in \mathbb{C}$ and $\lambda \in \Lambda$, and so $\wp$ is periodic with respect to Λ. It is a little less trivial to see that the expression for $\wp(z)$ converges for every $z \in \mathbb{C} \setminus \Lambda$, and that in fact the function $\wp$ is meromorphic, with poles of order 2 at every element of Λ. Therefore, $\wp$ can also be considered as a function in $\mathcal{M}(X)$. We finally note that $\wp$ is an even function; i.e. $\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$. Therefore its derivative $\wp'$ is an odd meromorphic function on $\mathbb{C}$ (i.e. $\wp'(-z) = -\wp'(z)$ for all $z \in \mathbb{C}$) which is also periodic with respect to Λ (thus, it may also be considered as a function in $\mathcal{M}(X)$) and whose only poles are poles of order 3 at every element of Λ.

Proposition 2.4.2. *The field $\mathcal{M}(X)$ of meromorphic functions on X is given by $\mathbb{C}(\wp, \wp')$.*

Proof. We want to show that every meromorphic function on $\mathbb{C}$ which is periodic with respect to the lattice Λ is a rational function of $\wp$ and $\wp'$. Now every meromorphic function is the sum of an odd function and an even function each periodic with respect to Λ (easy exercise), and every such odd function divided by the odd function $\wp'$ becomes an even function, so it suffices to show that every even nonzero meromorphic function f on $\mathbb{C}$ which is periodic with respect to Λ is a rational function of $\wp$.

Let $(f) = \sum_{P \in X} n_P(P) \in \mathrm{Div}(X)$ be the Weil divisor associated to f considered as a function in $\mathcal{M}(X)$. We first note that for each $P \in X$, we have $n_{-P} = n_P$. Moreover, we claim that if $P \in X$ with $P = -P$, then n_P is even. To prove this, let $z \in \mathbb{C}$ lie in the inverse image of such a P under the map $\pi : \mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda = X$ (so $2z \in \Lambda$), and let $f^{(n)}$ denote the nth derivative of f for $n \geq 0$. Then we check that $f^{(i)}(z) = f^{(i)}(-z) = (-1)^{i-1} f^{(i)}(z)$, which implies that $f^{(i)}(z) = 0$ for i even. It follows that the order of f at z is even. Thus, the divisor of f on X is given by $\sum_{P \in X} n_P(P) + n_P(-P) \in \mathrm{Div}(X)$ with $n_P \in \mathbb{Z}$ almost all 0.

Let $D \subset \mathbb{C}$ be a fundamental domain of the lattice Λ; that is, $D + \Lambda = \mathbb{C}$ and $(D+\lambda) \cap D = \varnothing$ for any $\lambda \in \Lambda$ (note that there is an obvious bijection between D and X). Let $D' \subset D$ be a subset such that $(D' + \Lambda) \cup (-D' + \Lambda) = \mathbb{C}$ and $(D' + \Lambda) \cap (-D' + \Lambda) = \frac{1}{2}\Lambda$. Assume that $0 \in D' \subset D$. Now consider the meromorphic function g on $\mathbb{C}$ given by

$$g(z) = \prod_{w \in D' \setminus \{0\}} (\wp(z) - \wp(w))^{n_{\pi(w)}}.$$

We check that for each $z \in D' \setminus \{0\}$, the divisor associated to $\wp(z) - \wp(w)$ considered as a function on X is $(P) + (-P) - 2(0) \in \mathrm{Div}(X)$. It follows that for each $P \in X \setminus 0$, the functions f and g have the same order; thus, when considered as functions in $\mathcal{M}(X)$, they have the same associated divisor except possibly for the coefficient at $0 \in X$. But then they must have the same order at 0 as well, since $(f/g) \in \mathrm{Div}(X)$ is a principal divisor and must have degree 0. So f/g has no zeros or poles on X and therefore must be a constant function since X is compact. Thus, since $g \in \mathbb{C}(\wp)$, we have $f \in \mathbb{C}(\wp)$ as desired.

□

Corollary 2.4.3. *a) The divisor $(0) \in \mathrm{Div}(X)$ is ample, and $3(0) \in \mathrm{Div}(X)$ is very ample (i.e. there is a basis of $\mathcal{L}(3(0))$ which can be used to embed X into some projective space).*

b) The imaginary part E of the positive definite Riemann form associated to the divisor $(0) \in \mathrm{Div}(X)$ satisfies $\sqrt{\det(E)} = 1$, so that it is given by $E(\lambda_1, \lambda_2) = -1$ for some (any) basis $\{\lambda_1, \lambda_2\}$ of Λ with $\Im(\lambda_2/\lambda_1) > 0$.

c) The set $\{1, \wp, \wp'\}$ of meromorphic functions on $\mathbb{C}$ viewed as functions in $\mathcal{M}(X)$ is a basis of $\mathcal{L}(3(0))$, and the map $[1 : \wp : \wp'] : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ induces an embedding of X as the projective curve in $\mathbb{P}^2_{\mathbb{C}}$ defined by a cubic relation $f(\wp, \wp') = 0$.

Proof. We already know that X has the structure of an projective curve over $\mathbb{C}$, and Proposition 2.4.2 tells us that the function field of the curve X is $\mathcal{M}(X) = \mathbb{C}(\wp, \wp')$. Since the function field of a complex curve must have transcendence degree 1 over $\mathbb{C}$ and $\wp$ and $\wp'$ are obviously transcendental over $\mathbb{C}$, it is then clear that there must be some algebraic relation $f(\wp, \wp') = 0$. This means that X is the closure in projective space of the variety given by the relation $f(x, y) = 0$, where x and y are the functions induced on $X = \mathbb{C}/\Lambda$ by $\wp$ and $\wp'$ respectively. Thus, $[1 : \wp : \wp']$ induces an embedding $X \hookrightarrow \mathbb{P}^2_{\mathbb{C}}$.

Now x has a double pole at $0 \in X$ and no poles anywhere else while y has a triple pole at $0 \in X$ and no poles anywhere else, so $x, y \in \mathcal{L}(3(0))$. Then $\{1, x, y\}$ can be extended to a basis of $\mathcal{L}(3(0))$ whose elements clearly induce an embedding of X into some projective space, so the divisor $3(0) \in \mathrm{Div}(X)$ is very ample and $(0) \in \mathrm{Div}(X)$ is ample, thus proving part (a).

To prove part (b), we only need to show that the imaginary part E of the positive definite Riemann form associated to the ample divisor $(0) \in \mathrm{Div}(X)$ satisfies $\sqrt{\det(E)} = 1$, since then it is easy to see that the only such E is defined as given in the statement. Lemma 2.3.3 tells us that $\dim_{\mathbb{C}} \mathcal{L}((0)) = \sqrt{\det(E)}$, and clearly every constant function lies in $\mathcal{L}((0))$, so it suffices to show that $\mathcal{L}((0)) = \mathbb{C}$. If a function $g \in \mathcal{L}((0))$ has no pole at $0 \in X$, then it is holomorphic and therefore a constant function because X is compact. Thus, we assume that there exists $g \in \mathcal{L}((0))$ with a simple pole at $0 \in X$ and no poles anywhere else. Then $g : X \to \mathbb{C} \cup \{\infty\}$ is actually a degree-1 morphism $X \to \mathbb{P}^1_{\mathbb{C}}$ and thus identifies X with $\mathbb{P}^1_{\mathbb{C}}$ itself. This is a contradiction since X has nontrivial fundamental group, so we get the desired statement.

Now part (c) results from the same argument as in the proof of Proposition 2.4.1 (in fact, x and y play the same roles as in that proof).

□

Again using a little ingenuity, it is possible to write down a cubic polynomial equation relating $\wp$ and $\wp'$, whose existence is guaranteed by Corollary 2.4.3. For any $k \in \mathbb{Z}$, define

$$G_{2k} = \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-2k}.$$

One can show that this sum converges for any $k \geq 2$. Then it is possible to show using Laurent approximations of $\wp$ and $\wp'$ that the following relation holds:

$$f(\wp, \wp') := \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \equiv 0. \tag{2.10}$$

This is remarkable in showing that in fact, X can be viewed as the projective closure of a variety given by a cubic equation of the rather simple form $y^2 = 4x^3 + Bx + C$ for constants $B, C \in \mathbb{C}$. One checks easily that the identity element $0 \in X$ corresponds to the unique point at infinity on this projective variety. We have now partially proven that Definition 1.1.1 implies Definition 1.1.4. That is, any complex abelian variety (in fact, any complex torus!) of dimension one can be defined algebraically by a cubic polynomial of the form given in Definition 1.1.4 (note that we can easily get rid of the "4" in the equation by scaling x by $4^{1/3}$ to get the equation in exactly the right form). We have not yet seen that the group operation can be defined by the formula given in that definition, however.

2.5 Isogenies, polarizations, and duals

This subsection will provide only a brief introduction to the construction of duals in the world of complex abelian varieties which should lend some intuition for some of the algebraic results on elliptic curves that will come later.

2.5.1 Isogenies of complex abelian varieties

Definition 2.5.1. *An isogeny of abelian varieties X_1 and X_2 of the same dimension is a surjective morphism $X_1 \to X_2$ which is a homomorphism of groups.*

In order to understand isogenies of complex abelian varieties, the following proposition is essential.

Proposition 2.5.2. *For $i = 1, 2$, let V_i/Λ_i be a complex torus, where V_i is a complex vector space and $\Lambda_i \subset V_i$ is a lattice. Then any holomorphic homomorphism $\varphi : V_1/\Lambda_1 \to V_2/\Lambda_2$ can be lifted to a unique $\mathbb{C}$-linear map $\tilde{\varphi} : V_1 \to V_2$ satisfying $\tilde{\varphi}(\Lambda_1) \subseteq \Lambda_2$. Moreover, if φ is an isogeny, then $\tilde{\varphi}$ is an isomorphism.*

Proof. Recall that each quotient map $V_i \twoheadrightarrow V_i/\Lambda_i$ is homeomorphic onto its image when restricted to a small enough open neighborhood of the identity $0 \in V_i$. Then the proof is an easy exercise in complex analysis.

□

Corollary 2.5.3. *Let X_1 and X_2 are abelian varieties of the same dimension g, and let $\varphi : X_1 \to X_2$ be a morphism which is a homomorphism of groups. Then φ is an isogeny if and only if it has finite kernel.*

Proof. Suppose that φ is an isogeny. Then its lifting $\tilde{\varphi}$ is an isomorphism from the covering space V_1 of $X_1 \cong V_1/\Lambda_1$ to the covering space V_2 of $X_2 \cong V_2/\Lambda_2$, so we may identify V_1 and V_2 and consider $\tilde{\varphi}$ to be an automorphism of a vector space V of dimension g such that $\tilde{\varphi}(\Lambda_1) \subseteq \Lambda_2$, where Λ_1 and Λ_2 are rank-$2g$ lattices in V. Then to prove the claim, it suffices to show that the quotient $\Lambda_2/\tilde{\varphi}(\Lambda_1)$ is finite. But since $\tilde{\varphi}$ is an $\mathbb{R}$-linear isomorphism, $\tilde{\varphi}(\Lambda_1)$ has rank $2g$, as does Λ_2, and so the induced quotient is finite.

□

The above corollary gives an equivalent definition of "isogeny" which is used in many texts. In the case of elliptic curves, the "surjection" and "finite kernel" conditions are also equivalent to the condition that the homomorphism is nontrivial.

Example 2.5.4. The multiplication-by-n map on a complex abelian variety X is an isogeny $[n] : X \to X$ whose kernel is the n-torsion subgroup of X, which by Corollary 2.1.4 has order n^{2g}.

Corollary 2.5.5. *Let X be a complex abelian variety, and let N be a finite subgroup of X. Then there exists a complex abelian variety X' and an isogeny $\varphi : X \to X'$ whose kernel is N, so that $X' \cong X/N$. The isogeny φ is unique up to automorphism of X'.*

Proof. The inverse image of N under $V \twoheadrightarrow V/\Lambda \cong X$ is a lattice $\Lambda' \subset V$ which contains Λ. If we let $X' = V/\Lambda'$, it is clear that the identity automorphism on V induces a unique isogeny $\phi : X \to X'$ whose kernel coincides with N. The uniqueness up to automorphism is clear from considering the liftings of two such isogenies $X \to X'$ to automorphisms of V.

□

Definition 2.5.6. *The **degree** of an isogeny $\varphi : X_1 \to X_2$ is the order of its kernel.*

Corollary 2.5.7. *Let $\varphi : X_1 \to X_2$ be an isogeny of degree n of complex abelian varieties of dimension g. Then there is an isogeny $\varphi' : X_2 \to X_1$ of degree n^{2g-1} such that $\varphi' \circ \varphi$ and $\varphi \circ \varphi'$ are the multiplication-by-n maps $[n]_{X_1}$ and $[n]_{X_2}$ on X_1 and X_2 respectively.*

Proof. We again identify the covering spaces of X_1 and X_2, so that $X_1 = V/\Lambda_1$ and $X_2 = V/\Lambda_2$ for a g-dimensional complex vector space V and rank-$2g$ lattices $\Lambda_1 \subseteq \Lambda_2 \subset V$. Let $X_1[n]$ denote the kernel of the multiplication-by-n map $X_1 \to X_1$. Then the inverse image of $X_1[n]$ under $V \twoheadrightarrow V/\Lambda_1 \cong X_1$ is clearly $\frac{1}{n}\Lambda_1$. It is easy to see that we have the inclusions of lattices $\Lambda_1 \subseteq \Lambda_2 \subseteq \frac{1}{n}\Lambda_1$. Then $N' := \frac{1}{n}\Lambda_1/\Lambda_2$ has order n^{2g-1}, and by Corollary 2.5.5, there is an abelian variety X_3 and an isogeny $\varphi' : X_2 \to X_3$ with kernel N'. But clearly $X_3 = V/\frac{1}{n}\Lambda_1$, which is isomorphic to X/Λ_1 via the multiplication-by-n homothety on V, so $\phi' : X_2 \to X_1$ is an isogeny of degree n^{2g-1}. Moreover, the kernel of $\varphi' \circ \varphi : X_1 \to X_1$ is $\frac{1}{n}\Lambda_1/\Lambda_1 \cong X_1[n]$. Since the multiplication-by-n map $[n]_{X_1} : X_1 \to X_1$ has this kernel, by the uniqueness given in the statement of Corollary 2.5.5, after composing φ' with an automorphism of X_1 we can assume that $\varphi' \circ \varphi = [n]_{X_1}$. The claim that $\varphi \circ \varphi' = [n]_{X_2}$ now follows from a similar argument.

□

Remark 2.5.8. The above corollary shows that if X_1 and X_2 are abelian varieties with an isogeny $X_1 \to X_2$, then there is also an isogeny from X_2 to X_1. Therefore, it makes sense to simply say "X_1 and X_2 are isogenous", with "isogenous" being an equivalence relation.

2.5.2 Polarizations of complex abelian varieties

We will define a particular type of holomorphic homomorphism φ from a complex abelian variety X to another complex torus $X^\vee$, and we will prove that $X^\vee$ is also an abelian variety and φ is an isogeny. In order to do this, we first need to further develop the theory of Riemann forms associated to divisors on X.

It was mentioned in the proof of Proposition 2.2.7 that there is a homomorphism from $\mathrm{Div}(X)$ to the group of Hermitian forms on the covering space V (in fact, every such Hermitian form is a Riemann form for X). In fact, we may take this notion further. We first observe that the set of normalized theta functions is closed under multiplication, and in fact, $\theta_D\theta_{D'} = \theta_{D+D'}$ for any divisors $D, D' \in \mathrm{Div}(X)$. Thus, $D \mapsto \theta_D$ defines a homomorphism from $\mathrm{Div}(X)$ to the group of theta functions. Moreover, if we associate to each normalized theta function θ_D the corresponding Riemann form $H : V \times V \to \mathbb{C}$ and map $K : \Lambda \to \mathbb{R}$ as in the statement of Proposition 2.2.7, we see that this association respects addition of divisors in $\mathrm{Div}(X)$. In other words, the map $\Phi : D \mapsto (H_D, K_D)$, where $H_D : V \times V \to \mathbb{C}$ and $K_D : \Lambda \to \mathbb{R}$ are the Riemann form and map associated to θ_D, defines a homomorphism

$$\mathrm{Div}(X) \to \{\text{additive group of Herm. forms } V \times V \to \mathbb{C}\} \times \{\text{additive group of maps } \Lambda \to \mathbb{R}\}.$$

The kernel of Φ is clearly the subgroup of principle divisors $\mathrm{Prin}(X) \subset \mathrm{Div}(X)$, because a normalized theta function θ_D has trivial H and K if and only if θ_D is periodic with respect to $\Lambda \subset V$, which means that it induces a meromorphic function on X whose associated divisor is D.

We let $\mathrm{Div}^0(X)$ denote the kernel of the composition of Φ with the projection to the group of Riemann forms on V; in other words, $\mathrm{Div}^0(X) \subset \mathrm{Div}(X)$ is the subgroup of

all divisors whose associated Riemann form is 0. Clearly, $\mathrm{Div}^0(X) \supseteq \mathrm{Prin}(X)$. We let $\mathrm{Pic}(X) := \mathrm{Div}(X)/\mathrm{Prin}(X)$ denote the Picard group of X and write $\mathrm{Pic}^0(X)$ for the subgroup $\mathrm{Div}^0(X)/\mathrm{Prin}(X)$. From now on, we consider Φ as a homomorphism on $\mathrm{Pic}(X)$.

Note that Φ associates to each divisor class $[D] \in \mathrm{Pic}^0 \subseteq \mathrm{Pic}(X)$ a map $K : \Lambda \to \mathbb{R}$ which satisfies the property that $K(\lambda_1 + \lambda_2) - K(\lambda_1) - K(\lambda_2) \equiv \frac{1}{2}E(\lambda_1, \lambda_2) = 0$ modulo $\mathbb{Z}$, so that $\theta_D(v + \lambda)/\theta_D(v) = e^{2\pi i K(\lambda)}$ is actually a group homomorphism $\Lambda \to \mathbb{C}^\times$ which does not depend our choice of a fixed $v \in V$. In other words, for $[D] \in \mathrm{Pic}^0(X)$ and $K : \Lambda \to \mathbb{R}$ the associated map, the function $\lambda \mapsto e^{2\pi i K(\lambda)}$ is a complex character $\chi_{[D]}$ on Λ. It is easy to check that $\chi_{[D_1+D_2]} = \chi_{[D_1]}\chi_{[D_2]}$ for $D_1, D_2 \in \mathrm{Div}(X)$, so Φ induces an injective homomorphism from $\mathrm{Pic}^0(X)$ to the group of complex characters on Λ (we will soon see that this is an isomorphism. A "complex character" is understood to take values in the unit circle.)

Now in order to define a polarization, for any $a \in X$, we denote the translation-by-a morphism taking $b \in X$ to $b + a$ by $t_a : X \to X$. It induces an pullback automorphism $t_a^* : \mathrm{Div}(X) \to \mathrm{Div}(X)$. Note that t_a^* stabilizes $\mathrm{Prin}(X)$ (for any $(f) \in \mathrm{Prin}(X)$, check that $t_a^*(f) = (f \circ t_a)$), so it may be considered as an automorphism of $\mathrm{Pic}(X)$ as well.

Definition 2.5.9. *A **polarization** is a map $X \to \mathrm{Pic}(X)$ of the form*

$$\varphi_D : a \mapsto [t_{-a}^* D - D]$$

for some ample divisor $D \in \mathrm{Div}(X)$.

Remark 2.5.10. This definition as well as the results below would all still be valid with "a" in place of "$-a$" above, but we include the minus sign in order to get a nicer description of principal polarizations on elliptic curves later.

2.5.3 The dual of a complex abelian variety

Our main goal now is to show that $\mathrm{Pic}^0(X)$ has the structure of a complex abelian variety and that any polarization φ_D is an isogeny. We will first show that a polarization is surjective with finite kernel. In order to show this, we need a lemma.

Lemma 2.5.11. *For any $D \in \mathrm{Div}(X)$ and $a \in X$, we have the following.*

a) The divisor $t_a^* D - D$ lies in $\mathrm{Div}^0(X)$.

b) Under the homomorphism from $\mathrm{Pic}^0(X)$ to the group of complex characters on Λ defined above, $t_a^* D - D$ goes to the character $\lambda \mapsto e^{2\pi i E(w,\lambda)}$, where E is the imaginary part of the Riemann form associated to D and w is some (any) element of V whose image modulo Λ is $a \in X \cong V/\Lambda$.

Proof. Let $H : V \times V \to \mathbb{C}$ be the Riemann form and $K : \Lambda \to \mathbb{R}$ be the map such that $\Phi(D) = (H, K)$. Fix a point $w \in V$ whose image modulo Λ is $a \in X$. Let θ_D be a normalized theta function for D. Then it is clear that $\theta' := (\theta_D \circ t_w) = \pi^* t_a^* D$, where $t_w : V \to V$ is the translation-by-w function on V. For $v \in V$ and $\lambda \in \Lambda$, we compute

$$\theta'(v + \lambda)/\theta'(v) = e^{\pi H(w+v,\lambda) + \frac{1}{2}H(\lambda,\lambda) + 2\pi i K(\lambda)}. \tag{2.11}$$

Let $\theta''(v) = e^{\pi H(v,w)}\theta'(v)$, which is a theta function with the same divisor as θ' since $v \mapsto e^{-\pi H(v,w)}$ is a nonvanishing holomorphic function on V. This contributes a factor of $e^{-\pi H(\lambda,w)}$ to the functional equation above, so that now we have, for $v \in V$ and $\lambda \in \Lambda$,

$$\theta''(v+\lambda)/\theta''(v) = e^{\pi H(v+w,\lambda)+\frac{1}{2}H(\lambda,\lambda)+2\pi i K(\lambda)-H(\lambda,w)}$$

$$= e^{\pi H(w,\lambda)-\pi H(\lambda,w)} \cdot e^{\pi H(v,\lambda)+\frac{1}{2}H(\lambda,\lambda)+2\pi i K(\lambda)}$$

$$= e^{2\pi i E(a,\lambda)} \cdot e^{\pi H(v,\lambda)+\frac{1}{2}H(\lambda,\lambda)+2\pi i K(\lambda)} = e^{2\pi i E(a,\lambda)} \cdot \theta_D(v+\lambda)/\theta_D(v). \tag{2.12}$$

Therefore we see that θ''/θ_D is a normalized theta function with $(\theta''/\theta_D) = \pi^*(t_a^*D - D) \in \mathrm{Div}(V)$, so $\theta''/\theta_D = \theta_{t_a^*D-D}$. Moreover, we have $\theta_{t_a^*D-D}(v+\lambda)/\theta_{t_a^*D-D}(v) = e^{2\pi i E(w,\lambda)}$ for $v \in V$ and $\lambda \in \Lambda$, and so the associated Riemann form is 0 while the associated map $\Lambda \to \mathbb{R}$ is $\lambda \mapsto E(w,\lambda)$ (note that this is independent modulo $\mathbb{Z}$ of our choice of w since $E(\Lambda,\Lambda) \subseteq \mathbb{Z}$). Then (a) and (b) both follow from the definition of $\mathrm{Div}^0(X)$ and constructions in the discussion above.

□

Proposition 2.5.12. *Let $\varphi_D : X \to \mathrm{Pic}^0(X)$ be a polarization as defined in Definition 2.5.9, where $D \in \mathrm{Div}(X)$ is an ample divisor. Then φ_D is a surjective homomorphism of abstract groups with kernel of order $\det(E)$, where E is the imaginary part of the Riemann form associated to D.*

Proof. It was shown in the above discussion that any divisor class in $\mathfrak{D} \in \mathrm{Pic}^0(X)$ is determined uniquely by an associated complex character $\chi_{\mathfrak{D}}$ on Λ. In turn, any complex character $\chi : \Lambda \to \mathbb{C}^*$ must be of the form $\lambda \mapsto e^{2\pi i B(\lambda)}$ for some $\mathbb{R}$-linear function $B : \Lambda \to \mathbb{R}$. Meanwhile, by Proposition 2.3.1, since D is ample, the $\mathbb{R}$-bilinear form $E : V \times V \to \mathbb{R}$ is nondegenerate. Therefore, any $\mathbb{R}$-linear function $B : \Lambda \to \mathbb{R}$ is given by $E(w,\cdot)$ for some $w \in V$. Thus, $\chi_{\mathfrak{D}} = e^{2\pi i E(w,\cdot)}$ for some $w \in V$, and it follows from Lemma 2.5.11(b) that $\varphi_D(-w) = \mathfrak{D}$. Thus, φ_D is a surjective map. Moreover, we have shown that $\mathfrak{D} \mapsto \chi_{\mathfrak{D}}$ as constructed above is actually an isomorphism from $\mathrm{Pic}^0(X)$ to the group of complex characters on Λ. Thus, to show that φ_D is a group homomorphism, it suffices to check from the above construction that $\chi_{\mathfrak{D}_1+\mathfrak{D}_2} = \chi_{\mathfrak{D}_1}\chi_{\mathfrak{D}_2}$.

It is now clear that the kernel of φ_D consists of the images modulo Λ of elements $w \in V$ with $e^{2\pi i E(w,\lambda)} = 1$ and thus $E(w,\lambda) \in \mathbb{Z}$ for all $\lambda \in \Lambda$. It follows quickly from Lemma 2.3.3(a) that the subset $\Lambda' \subset V$ consisting of all such w is a lattice containing Λ such that the quotient Λ'/Λ has order $\det(E)$.

□

The next proposition shows that $\mathrm{Pic}^0(X)$ is not only a complex torus but a complex abelian variety.

Proposition 2.5.13. *Let V^* be the complex vector space of all $\mathbb{C}$-antilinear functions $\xi : V \to \mathbb{C}$, and let Λ^* be the subset of all $\xi \in V^*$ satisfying $\Im\xi(\Lambda) \subseteq \mathbb{Z}$. Then Λ^* is a lattice of maximal rank in V^*, and there is a canonical isomorphism of groups $\mathrm{Pic}^0(X) \xrightarrow{\sim} V^*/\Lambda^*$, thus giving $\mathrm{Pic}^0(X)$ the structure of a complex torus. Moreover, $\mathrm{Pic}^0(X) \cong V^*/\Lambda^*$ has a positive definite Riemann form and thus is an abelian variety by Theorem 2.3.5.*

Proof. It is an elementary exercise to check that V^* and Λ^* have the same dimension and rank as V and Λ respectively, so that V^*/Λ^* is a complex torus. Fix an ample divisor $D \in \mathrm{Div}(X)$, and let E be the imaginary part of its associated Riemann form. Now we have already shown that $\mathrm{Pic}^0(X)$ is isomorphic to the group of complex characters on Λ, each of which is of the form $\lambda \mapsto e^{2\pi i B(\lambda)}$ for some $\mathbb{R}$-linear function $B : V \to \mathbb{R}$. Since for such a B there always exists a $\mathbb{C}$-antilinear function on V whose imaginary part is $-B$ (take $B(iv) - iB(v)$), we get a surjection $V^* \twoheadrightarrow \mathrm{Pic}^0(X)$ given by $\xi \mapsto e^{-2\pi i \Im \xi(\cdot)}$ whose kernel is clearly Λ^*.

Now it follows from what we have shown before that the map $\varphi_D : X \to \mathrm{Pic}^0(X) \cong V^*/\Lambda^*$ is given by

$$a \mapsto t_{-a}^* D - D \mapsto (E(-iw, \cdot) - iE(-w, \cdot)) + \Lambda^* \in V^*/\Lambda^*,$$

where w is some (any) element of V mapping to $a \in X$. Therefore, it lifts to the isomorphism $\widetilde{\varphi_D} : V \xrightarrow{\sim} V^*$ given by $w \mapsto E(-iw, \cdot) - iE(-w, \cdot) = H(w, \cdot) \in V^*$. Note that $\widetilde{\varphi_D}(\Lambda) \subseteq \Lambda^*$ is a sublattice of finite index (in fact equal to the order of $\ker(\varphi_D)$, which is $\det(E)$). Now define $H^* : V^* \times V^* \to \mathbb{C}$ by $H^*(\xi_1, \xi_2) = H(\widetilde{\varphi_D}^{-1}(\xi_1), \widetilde{\varphi_D}^{-1}(\xi_2))$. It is immediate to check that H^* is a positive definite Riemann form on V^* with $H^*(\widetilde{\varphi_D}(\Lambda), \widetilde{\varphi_D}(\Lambda)) \subseteq \mathbb{Z}$. Therefore, $H^*(\Lambda^*, \Lambda^*) \subseteq \det(E)^{-2}\mathbb{Z}$, so $\det(E)^2 H^*$ is a positive definite Riemann form for V^*/Λ^*. □

We denote the group $\mathrm{Pic}^0(X)$ with its structure as an abelian variety by $X^\vee$ and call it the *dual abelian variety* of X. Any polarization $\varphi_D : X \to X^\vee$ is an isogeny of degree $\det(E)$ (note that this is always a perfect square). If there exists an ample divisor $D \in \mathrm{Div}(X)$ whose associated Riemann form satisfies $\det(E) = 1$, then this isogeny is an isomorphism $\varphi_D : X \xrightarrow{\sim} X^\vee$. In this case, we say that φ_D is a *principal polarization* and that X is "self-dual". It is not too deep to show that there is always a natural isomorphism $(X^\vee)^\vee \xrightarrow{\sim} X$, as one expects, but we will not do it here.

Remark 2.5.14. Note that for any complex torus X (even one which is not an abelian variety), what we have shown implies that $\mathrm{Pic}^0(X)$ still has the structure of a complex torus, called the *dual complex torus* of X. This intuitively makes sense if one identifies $\mathrm{Pic}^0(X)$ with the group of complex characters on X as above. (Note in particular that as a real Lie group, $X \cong (\mathbb{R}/\mathbb{Z})^{2g}$ and a complex character on X is a homomorphism of real Lie groups $\chi : \mathbb{Z}^{2g} \to \mathbb{R}/\mathbb{Z}$ which lifts to an $\mathbb{R}$-linear functional $\tilde{\chi} : \mathbb{R}^{2g} \to \mathbb{R}$ which is unique up to functionals which take values in $\mathbb{Z}$ on the standard basis of $\mathbb{R}^{2g}$.)

However, we need an ample divisor D with a positive definite Riemann form H in order to construct a positive definite Riemann form on the dual complex torus, as well as to get a map φ_D which is surjective.

2.5.4 Polarizations and self-duality of elliptic curves

We now apply the theory of polarizations to the elliptic curve case. Assume now that X has dimension 1. Then we know from Corollary 2.4.3 that the divisor $(0) \in \mathrm{Div}(X)$ is ample and that the associated Riemann form is positive definite and satisfies $\det(E) = 1$. Thus, $\varphi_{(0)} : X \to X^\vee$, defined using the above notation, is a principal polarization and so $X \cong X^\vee$

is self-dual. Explicitly, $\varphi_{(0)}$ is given by $P \mapsto [(P) - (0)] \in \mathrm{Pic}^0(X)$. We will see this map again in other contexts. (This is the reason for the minus sign in Definition 2.5.9.)

We also get a simple description of $\mathrm{Div}^0(X)$ as well as of ample divisors on X in the elliptic curve case.

Proposition 2.5.15. *If X is an elliptic curve, then $\mathrm{Div}^0(X) \subset \mathrm{Div}(X)$ coincides with the subgroup of divisors of degree 0. Moreover, a divisor on X is ample if and only if it has positive degree.*

Proof. The subgroup of divisors of degree 0 is generated by divisors of the form $(P) - (0) \in \mathrm{Div}(X)$ for a point $P \in X$. But $(P) - (0) = t^*_{-P}(0) - (0) \in \mathrm{Div}^0(X)$ by Lemma 2.5.11. Therefore, any two divisors in $\mathrm{Div}(X)$ with the same degree have the same associated Riemann form. Let H be the positive definite Riemann form associated to the ample divisor $(0) \in \mathrm{Div}(X)$. For any divisor $D \in \mathrm{Div}(X)$ with $\deg(D) = n$, then D and $n(0)$ have the same associated Riemann form, which is nH. Since $nH = 0$ (resp. nH is positive definite) if and only if $n = 0$ (resp. $n \geq 1$), we get both claims of the proposition.

□

2.6 Jacobians of compact Riemann surfaces

In this section we discuss the classical theory which first led to the discovery of elliptic curves and abelian varieties over $\mathbb{C}$ in the early 19th century. Given any given compact Riemann surface C of genus g, we will construct a complex abelian variety J of dimension g called the *Jacobian* of C, which as an abstract group is isomorphic to $\mathrm{Pic}^0(C)$. This will help to provide some more concrete examples of complex abelian varieties of dimension ≥ 2 as well as a deeper understanding of complex elliptic curves.

Throughout this section, we will resume the same notation of $\mathrm{Div}(C)$ (group of Weil divisors), $\mathrm{Div}^0(C)$ (subgroup of degree-0 divisors), $\mathrm{Prin}(C)$, $\mathrm{Pic}(C)$, $\mathrm{Pic}^0(C)$, etc. exactly as they were defined for elliptic curves in §2.4.

2.6.1 Differential forms and the Riemann-Roch theorem

Since we will only be dealing with differential forms on smooth curves, we will follow the definition of Silverman: the complex vector space of *differential forms* on a complex curve C, denoted $\Omega(C)$, is the set of all symbols df for any f in the field of meromorphic functions $\mathcal{M}(C)$ satisfying the following relations: $d(f + g) = df + dg$; $d(cf) = c(df)$; and $d(fg) = f(dg) + g(df)$ for any $f, g \in \mathcal{M}(C)$ and $c \in \mathbb{C}$.

It is easy to show that if $\omega_1, \omega_2 \in \Omega(C)$, then $\omega_2 = f\omega_1$ for some unique $f \in \mathcal{M}(C)$, so $\Omega(C)$ may also be viewed as a 1-dimensional $\mathcal{M}(C)$-vector space. This fact enables us to define the order of a differential form at any point on the curve. Given any differential form $\omega \in \Omega(C)$ and any point $P \in C$, the *order* of ω at P is the order of the function $\omega/dt \in \mathcal{M}(C)$ at P, where $t \in \mathcal{M}(C)$ is some (any) uniformizer at P. So there is a divisor associated to each differential form $\omega \in \Omega(C)$, denoted $(\omega) \in \mathrm{Div}(C)$, given by $\sum_{P \in C} n_P(P)$ where each n_P is the order of ω at P. In fact, for $\omega_1, \omega_2 \in \Omega(C)$, if we let $f = \omega_2/\omega_1 \in \mathcal{M}(C)$, then we see that $(\omega_2) = (\omega_1) + (f) \in \mathrm{Div}(C)$, so the divisors of all differential forms on C lie

in the same divisor class in $\mathrm{Pic}(C)$. We denote this divisor class by $[K] \in \mathrm{Pic}(C)$ and call any representative $K \in \mathrm{Div}(C)$ a *canonical divisor* of C.

The algebraic definition of the genus of a curve is the dimension over $\mathbb{C}$ of the vector space of all holomorphic differential forms on C (differential forms whose associated divisor is positive; we will see from the Riemann-Roch theorem below that this dimension is always finite). One can show, by taking triangulations and computing Euler characteristics, that this definition of "genus" agrees with the topological definition, where the genus of a compact Riemann surface is the "number of holes".

Example 2.6.1. (hyperelliptic curves)

We define a *hyperelliptic curve* over $\mathbb{C}$ to be a smooth projective curve defined by an equation of the form $y^2 = f(x)$ for some polynomial $f \in \mathbb{C}[x]$ of degree $d \geq 1$ which has d distinct roots. If d is odd, then there will be one added "point at infinity" ∞, and if d is even, there will be two added "points at infinity" denoted ∞_1 and ∞_2. Note that a hyperelliptic curve is a conic if $d = 1, 2$, and an elliptic curve is a hyperelliptic curve for $d = 3$ by Definition 1.1.4. (In fact, we will see below that the genus of a hyperelliptic curve C of degree $d = 4$ is 1, and so by Definition 1.1.3, such a curve C with a distinguished point is also an elliptic curve.)

In order to visualize C as a complex manifold, we consider the function $x \mapsto y = \sqrt{f(x)}$ on the Riemann sphere $\mathbb{C} \cup \{\infty\}$. In fact, $\sqrt{f(x)}$ can't be defined as a meromorphic function on the Riemann sphere, but it can be defined on the compliment of some branch cuts which connect the zeroes of the polynomial f. Define the subset $B \subset \mathbb{C} \cup \{\infty\}$, called the subset of *branch points*, to be the set of roots of f if d is even, and let $B \subset \mathbb{C} \cup \{\infty\}$ be the set of roots of f along with the point ∞ if d is odd (note that the cardinality of B is always even and equal to either d or $d+1$). We partition B into cardinality-2 subsets and for each such subset draw a line connecting the corresponding two points in B, so that none of the $\#B/2$ lines intersect. Then there is a well-defined meromorphic function $\sqrt{f(x)}$ whose square is $f(x)$ defined on the compliment of these branch cuts. Of course, $-\sqrt{f(x)}$ is another such function. With a little visual intuition, one can see that the Riemann surface defined by the equation $y^2 = f(x)$ can be constructed by taking two copies of the Riemann sphere, one on which y takes the value $\sqrt{f(x)}$ and the other on which y takes the value $-\sqrt{f(x)}$, "opening" their branch cuts, and gluing them together along their opened branch cuts. Since each copy of the Riemann sphere had $\#B/2$ branch cuts, the resulting Riemann surface has $\#B/2 - 1$ holes. Since $\#B \in \{d, d+1\}$, it follows that the genus of C is equal to $\lfloor (d-1)/2 \rfloor$.

We can show that this agrees with the algebraic definition of genus as follows. One can compute that the differential form $dx/y \in \Omega(C)$ has associated divisor $(d-3)(\infty) \in \mathrm{Div}(C)$ (resp. $(d/2-2)(\infty_1) + (d/2-2)(\infty_2) \in \mathrm{Div}(C)$) if d is odd (resp. if d is even). Moreover, one can compute that a nonzero polynomial function $h \in \mathbb{C}[x] \subset \mathcal{M}(C)$ of degree $d' \geq 0$ has only a pole at ∞ of order $2d'$ (resp. only poles at ∞_1 and ∞_2, each of order d') if d is odd (resp. if d is even). Thus, the space of all holomorphic differentials on C consists of all differentials of the form $h \cdot dx/y$ where $h \in \mathbb{C}[x] \subset \mathcal{M}(C)$ is a polynomial function of degree $d' \leq \lfloor (d-1)/2 \rfloor - 1$, which has dimension $\lfloor (d-1)/2 \rfloor$. Thus, again we see that the genus of C is equal to $g := \lfloor (d-1)/2 \rfloor$. So if a hyperelliptic curve has genus g, then the polynomial f used to define it has degree $2g+1$ or $2g+2$, and there are always $2g+2$ branch points.

In fact, we may easily describe a basis for the singular homology of C as follows. Order

the points in B as $\{z_1, z_2, ..., z_{2g+2}\}$ so that the jth branch cut connects the point z_{2i-1} to z_{2i} for $1 \leq i \leq g+1$. Let $\bar{a}_i$ (resp. $\bar{b}_i$) be a simple closed loop surrounding only the points z_{2i-1} and z_{2i} (resp. the points $z_{2i}, z_{2i+1}, ..., z_{2g+1}$) for $1 \leq i \leq g$. Then the $\bar{a}_i$'s and $\bar{b}_i$'s lift to simple closed loops a_i and b_i on the compact Riemann surface C. This set of loops is a basis for the homology group $H_1(C, \mathbb{Z})$, which is a free abelian group generated by $\{a_1, ..., a_g, b_1, ..., b_g\}$.

Note that the case of $d = 3$ shows that an elliptic curve given by $y^2 = f(x)$ as in Definition 1.1.4 always has genus 1, and its only holomorphic differentials are constant multiples of dx/y. In fact, these holomorphic differentials have trivial associated divisor, so that the class of canonical divisors for an elliptic curve C is $[K] = 0 \in \mathrm{Div}(C)$. Recall that an elliptic curve of this form can be identified with $\mathbb{C}/\Lambda$ for some rank-2 lattice $\Lambda \subset \mathbb{C}$, and that there is a periodic function $\wp$ defined on $\mathbb{C}$ inducing $x \in \mathcal{M}(C)$ such that its derivative $\wp'$ induces $y \in \mathcal{M}(C)$. Then note that the differential form $dx/y \in \Omega(C)$ lifts to $\wp' dz/\wp' = dz \in \Omega(\mathbb{C})$, and clearly the only holomorphic differentials on $\mathbb{C}$ are constant multiples of dz (which has trivial divisor). Any constant multiple of dx/y is called an *invariant differential* of the elliptic curve C and will be important later.

The curious reader may find more details in §1 of [6].

The Riemann-Roch theorem gives a formula which can be used to compute (among other things) the dimension of the vector space $\mathcal{L}(D)$ for any divisor D on a compact smooth curve C. From now on, for any divisor $D \in \mathrm{Div}(C)$, we define $l(D)$ to be the dimension of the vector space $\mathcal{L}(D)$. Note that $l(D)$ does not depend on the choice of representative D of the divisor class $[D] \in \mathrm{Pic}(C)$.

Theorem 2.6.2. *(Riemann-Roch)*
For any divisor $D \in \mathrm{Div}(C)$ and canonical divisor K of C, there is an integer $g \geq 0$ which depends only on C, such that

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

This is a standard theorem in algebraic geometry, and we do not prove it in these notes. A proof can be found in §2 of [2].

Corollary 2.6.3.
a) The constant g given in the statement of Theorem 2.6.2 is the genus of C.
b) The degree of any canonical divisor of C is $2g - 2$.

Proof. First we observe that there is an isomorphism from the vector space of holomorphic differentials on C to $\mathcal{L}(K)$, given by $\omega \mapsto \omega/\omega_0$ for some $\omega_0 \in \Omega(C)$ such that $(\omega_0) = K \in \mathrm{Div}(C)$. Thus, the genus of C is equal to $l(K)$.

Part (a) is proven by putting $D = 0$ into the formula given by Theorem 2.6.2. Then part (b) is proven by instead putting $D = K$ into that formula.

□

The following corollary is useful in proving the Abel-Jacobi theorem below.

Corollary 2.6.4. *Let $O \in C$ be an arbitrary point. Then each divisor class in $\mathrm{Pic}^0(C)$ can be represented by a divisor of the form $\sum_{i=1}^{g} n_i(P_i) - g(O)$ for some points $P_i \in C$ (not necessarily distinct) and integers n_i.*

Proof. First we show that any divisor $D \in \mathrm{Div}^0(C)$ is equivalent modulo $\mathrm{Prin}(C)$ to a divisor of the form $\sum_{i=1}^m n_i(P_i) - m(O)$ for some $m \geq g+1$. Indeed, putting $(g+1)(O)$ into the formula given by Theorem 2.6.2 gives us $l((g+1)(O)) = g+1-l(K-(g+1)(O))-g+1 \geq 2$, so there exists a nonconstant meromorphic function $\psi \in \mathcal{L}((g+1)(O))$. Then the function $\xi := \prod(1/\psi - 1/\psi(P))$, where the terms are multiplied for each $P \in C$ which appers in the divisor D with negative coefficient, has zeros at each P and a pole of some order $m \geq g+1$ only at O. Then it is clear that $D + (\xi)$ is of the desired form.

It now suffices to show that for any $m \geq g+1$ and divisor of the form $\sum_{i=1}^m n_i(P_i) - m(O)$, there is a divisor of the form $\sum_{i=1}^{m-1} n_i'(P_i') - (m-1)(O)$ in the same equivalence class modulo $\mathrm{Prin}(C)$. This is equivalent to the claim that given $m \geq g+1$ and any points $P_1, ..., P_m \in C \setminus \{O\}$, there exists a nonzero function in $\mathcal{M}(C)$ which has a zero at O and which lies in $\mathcal{L}(\sum_{i=1}^m P_i))$. Let $D = \sum_{i=1}^m P_i$. Then Theorem 2.6.2 gives us $l(D) = \deg(D) - l(K-D) - g + 1 \geq m - g + 1 \geq 2$. Thus, $\mathbb{C} \subsetneq \mathcal{L}(D)$, so there exists a nonconstant function $h \in \mathcal{L}(D)$. Since functions in $\mathcal{L}(D)$ don't have poles at O, the function h takes some value in $\mathbb{C}$ at the point O, which we denote by $z_0 \in \mathbb{C}$. But then $h - z_0$ is a nonconstant function in $\mathcal{L}(D)$ with a zero at O, thus proving our claim.

□

2.6.2 The Abel-Jacobi map

The singular homology group $H_1(C, \mathbb{Z})$ of our compact genus-g Riemann surface C is freely generated by a cardinality-$2g$ set $\{a_1, ..., a_g, b_1, ..., b_g\}$ of simple closed loops which look exactly like the loops explicitly constructed in the case that C is a hyperelliptic curve (Example 2.6.1). In fact, as a topological space, C may be constructed by taking a $4g$-sided polygon, called a *fundamental polygon* of C, and identifying the sides by considering each one as a loop in $H_1(C, \mathbb{Z})$ in the order $\{a_1, b_1, -a_1, -b_1, ..., a_g, b_g, -a_g, -b_g\}$. Now choose a basis $\{\omega_1, ..., \omega_g\}$ of the g-dimensional vector space of holomorphic differential forms on C.

The Abel-Jacobi theorem arose from attempts to calculate integrals of certain differential forms along paths on hyperelliptic curves. As we know from complex analysis, such a path integral is only well-defined up to integrals along closed loops in the homology group: in general, an integral of a differential form along a nontrivial closed loop will not equal 0. Let $\Lambda \in \mathbb{C}^g$ be the additive subgroup generated by

$$\left\{\left(\int_{a_i} \omega_1, ..., \int_{a_i} \omega_g\right), \left(\int_{b_i} \omega_1, ..., \int_{b_i} \omega_g\right)\right\}_{1 \leq i \leq g} \subset \mathbb{C}^g.$$

(We will later show that Λ is a rank-$2g$ lattice.)

Now we define the Abel-Jacobi map as follows. Fix a point $O \in C$. Now for any point $P \in C$, path integrals of the form $\int_O^P \omega$ for some holomorphic differential form $\omega \in \Omega(C)$ are not well-defined, because composing any path from O to P with a nontrivial closed loop of base O may change the value of the integral. However, if we let AJ (named after Abel and Jacobi) be the function on C given by

$$P \mapsto \left(\int_O^P \omega_1, ..., \int_O^P \omega_g\right),$$

we see that this takes values in $\mathbb{C}^g$ determined up to elements of Λ. Thus, $AJ : C \to \mathbb{C}^g/\Lambda$ is a well-defined function, which can be extended $\mathbb{Z}$-linearly to a function $AJ : \mathrm{Div}(C) \to \mathbb{C}^g/\Lambda$.

Remark 2.6.5. In the case that C is an elliptic curve given by an equation of the form $y^2 = f(x)$ where $f \in \mathbb{C}[x]$ is a cubic polynomial in x, we have already seen from Example 2.6.1 that all holomorphic differentials in $\Omega(C)$ are of scalar multiples of dx/y. In this case, the map $AJ : C \to \mathbb{C}/\Lambda$ is a biholomorphism (see Exercise 2.7.7) which is essentially an inverse to the map $\mathbb{C} \to C$ given by $z \mapsto (\wp(z), \wp'(z))$.

In fact, this entire area of mathematics first came to light when mathematicians in the early 1800's were attempting to solve integrals of the form $\int dx/\sqrt{f(x)}$ with $f(x)$ a cubic. Such integrals naturally came up in calculations of the arclegnth of an ellipse and were therefore called "elliptic integrals". Researchers soon realized that functions like $1/\sqrt{f(x)}$ couldn't be defined everywhere on the complex plane and path integrals of them should instead by studied on the curve given by $y^2 = f(x)$, and that is why this curve was called an "elliptic curve".

Definition 2.6.6. *The Jacobian of a compact Riemann surface C of genus g is the g-dimensional complex manifold $J := \mathbb{C}^g/\Lambda$.*

The function $AJ : \mathrm{Div}(C) \to J$ is called the *Abel-Jacobi map*. One easily verifies that when restricted to $\mathrm{Div}^0(C)$, this map does not depend on our choice of basepoint $O \in C$. From now on we will mainly consider the Abel-Jacobi map restricted to $\mathrm{Div}^0(C)$. We are finally ready to present the Abel-Jacobi Theorem, which will be proven in the next two subsections.

Theorem 2.6.7. *(Abel-Jacobi)*

(Abel) The kernel of the map $AJ : \mathrm{Div}^0(C) \to J$ coincides with the subgroup of principal divisors $\mathrm{Prin}(C) \subseteq \mathrm{Div}^0(C)$.

(Jacobi) The map AJ is surjective.

Thus, the Abel-Jacobi map induces an isomorphism of abstract groups $\mathrm{Pic}^0(C) \xrightarrow{\sim} J$.

2.6.3 Proof of Abel's Theorem

Our goal in this section is to prove Abel's part of Theorem 2.6.7, which is that the kernel of the Abel-Jacobi map coincides with $\mathrm{Prin}(C) \subseteq \mathrm{Div}^0(C)$. For the proof, we fix a fundamental polygon $\mathcal{P}$ of C which contains O in its interior, whose sides form a homology basis $\{a_1, ..., a_g, b_1, ..., b_g\}$ as in §2.6.2. We first need some lemmas.

Lemma 2.6.8. *Let ω and η be two differential forms on C. Then we have the identities*

$$\int_C \omega \wedge \eta = \int_{\partial \mathcal{P}} \left(\int_O^P \omega \right) \eta(P) = \sum_{i=1}^{g} \left(\int_{a_i} \omega \int_{b_i} \eta - \int_{a_i} \eta \int_{b_i} \omega \right),$$

where the integrals from O to P above are defined using a path which is contained in the interior of $\mathcal{P}$.

Proof. The argument follows fairly straightforwardly from Stokes' Theorem, but the details are omitted here (this can be found in [1]).

□

Corollary 2.6.9. *The set of vectors* $\{(\int_{a_i}\omega_1,...,\int_{a_i}\omega_g)\}_{1\leq i\leq g}\subset\mathbb{C}^g$ *is linearly independent over* $\mathbb{C}$ *and thus spans* $\mathbb{C}^g$*.*

Proof. The claim is equivalent to the statement that if $\omega\in\Omega(C)$ is a holomorphic differential form with $\int_{a_i}\omega=0$ for $1\leq i\leq g$ then $\omega=0$. Suppose that $\omega\in\Omega(C)$ is a holomorphic differential satisfying this hypothesis. Then, writing $\bar{\omega}$ for the complex conjugate of ω, Lemma 2.6.3 yields

$$\int_C\omega\wedge\bar{\omega}=\sum_{i=1}^{g}\left(\int_{a_i}\omega\int_{b_i}\bar{\omega}-\int_{b_i}\omega\int_{a_i}\bar{\omega}\right)=0. \tag{2.13}$$

This implies that $\omega=0$ as desired, since it is fairly intuitive to verify using local charts that $\int_C\omega\wedge\bar{\omega}\neq 0$ if and only if $\omega\neq 0$.

□

Note that we may use Lemma 2.6.3 to "normalize" our basis $\{\omega_1,...,\omega_g\}$ so that $\int_{a_j}\omega_i=\delta_{i,j}$ for $1\leq i,j\leq g$. From now on, we will assume that our basis of holomorphic differentials satisfies this property. We write Π for the $g\times g$ matrix given by $\Pi_{i,j}=\int_{b_j}\omega_i$; we observe that now our lattice Λ is generated by $\mathbb{Z}^g$ and the columns of Π, so $\Lambda=\mathbb{Z}^g+\Pi\mathbb{Z}^g$. We now note that Π is symmetric (this is the first of what are called "Riemann's relations").

Corollary 2.6.10. *The matrix* Π *is symmetric; that is,* $\int_{b_j}\omega_i=\int_{b_i}\omega_j$ *for* $1\leq i,j\leq g$*.*

Proof. It is clear that since ω_i and ω_j are both holomorphic and therefore one is a meromorphic function times the other, we have $\omega_i\wedge\omega_j=0$. Then Lemma 2.6.3 gives us

$$0=\int_C\omega_i\wedge\omega_j=\sum_{k=1}^{g}\left(\int_{a_k}\omega_i\int_{b_k}\omega_j-\int_{a_k}\omega_j\int_{b_k}\omega_i\right)=\int_{b_i}\omega_j-\int_{b_j}\omega_i. \tag{2.14}$$

□

Lemma 2.6.11. *For any degree-0 divisor of the form* $D:=\sum_{P\in C}n_P(P)\in\mathrm{Div}^0(C)$*, there is a differential form* $\omega_D\in\Omega(C)$ *whose only poles are simple poles with residue* n_P *at each point* $P\in C$ *such that* $n_P\neq 0$*. We may further guarantee that* ω_D *satisfies* $\int_{a_i}\omega_D=0$ *for* $1\leq i\leq g$ *(this uniquely determines* ω_D*).*

Proof. It is clear that since $\mathrm{Div}^0(C)$ is generated by divisors of the form $(P)-(Q)$ for points $P,Q\in\mathrm{Div}^0(C)$, it suffices to prove this claim for $(P)-(Q)$. It suffices to show the existence of a differential form $\omega\neq 0$ whose only poles are a simple pole at P (with residue 1) and a simple pole at Q (with residue -1). One checks that the space of all differential forms whose only poles are possibly simple poles at P and Q is isomorphic to $\mathcal{L}(K+P+Q)$. Putting $D=-P-Q$ into the formula given in Theorem 2.6.2 gives

$$\deg(-P-Q)=l(-P-Q)-l(K+P+Q)+g-1\Rightarrow -2=0-l(K+P+Q)+g-1, \tag{2.15}$$

so $l(K+P+Q) = g+1$ and there exists a function in $\mathcal{L}(K+P+Q) \setminus \mathcal{L}(K)$ and thus a differential form ω_D which is not holomorphic but whose only poles are simple poles at P and/or Q. Because the sum of the residues of a differential form must be 0, we know that this ω_D must have simple poles at both P and Q with opposite residues. After scaling by a suitable constant, we may assume that the residues at P and Q are 1 and -1 respectively.

Since Corollary 2.6.9 tells us that $\{(\int_{a_i} \omega_1, ..., \int_{a_i} \omega_g)\}_{1 \le i \le g}$ spans $\mathbb{C}^g$. Therefore there is some holomorphic differential $\omega \in \Omega(C)$ satisfying $(\int_{a_1} \omega, ..., \int_{a_g} \omega) = (\int_{a_1} \omega_D, ..., \int_{a_g} \omega_D)$. By subtracting this ω from ω_D, we guarantee that ω_D satisfies $\int_{a_i} \omega_D = 0$ for $1 \le i \le g$, and uniqueness also follows quickly from Corollary 2.6.9.

□

Lemma 2.6.12. *(reciprocity)*

Choose any $D \in \mathrm{Div}^0(C)$ and let $\omega_D \in \Omega(C)$ be the corresponding differential form given by Lemma 2.6.11. Then we have the identity

$$AJ(D) = \frac{1}{2\pi i}\left(\int_{b_1} \omega_D, ..., \int_{b_g} \omega_D\right) + \Lambda \in J. \tag{2.16}$$

Proof. First note that Lemma 2.6.3 says that for a fixed j,

$$\int_{\partial \mathcal{P}} \left(\int_O^P \omega_j\right) \omega_D(P) = \sum_{i=1}^{g} \left(\int_{a_i} \omega_j \int_{b_i} \omega_D - \int_{a_i} \omega_D \int_{b_i} \omega_j\right) = \int_{b_j} \omega_D, \tag{2.17}$$

where the second inequality follows from the properties $\int_{a_j} \omega_i = \delta_{i,j}$ and $\int_{a_i} \omega_D = 0$ for $1 \le i \le g$. Meanwhile, we may evaluate the integral on the left-hand side by calculating residues, as follows. Note that the function $P \mapsto \int_O^P \omega_j$ has no poles anywhere because ω_j is holomorphic, but if we write $D = \sum_{k=1}^{r} n_k(P_k)$ with $n_k \neq 0$ then ω_D has only a simple pole at each P_k with residue n_k. The residue formula then yeilds

$$\int_{\partial \mathcal{P}} \left(\int_O^P \omega_j\right) \omega_D(P) = 2\pi i \sum n_k \int_O^{P_k} \omega_j, \tag{2.18}$$

where the paths from O and P lie in the interior of $\mathcal{P}$. The statement of the lemma now follows from (2.17) and (2.18) and the definition of AJ.

□

Lemma 2.6.13. *If a function $f \in \mathcal{M}(C)$ is holomorphic on a loop $a \in H_1(C, \mathbb{Z})$, then the value of the integral $\int_a df/f$ is an integer multiple of $2\pi i$.*

Proof. This is a standard fact in complex analysis and arises intuitively from the observation that $df/f = d(\log f)$ with $\log f$ defined up to an integer multiple of $2\pi i$.

□

We are finally ready to begin the proof of Abel's Theorem. We have to show that a divisor $D \in \mathrm{Div}^0(C)$ is in the kernel of AJ if and only if D is the divisor associated to some meromorphic function on C. First choose any $f \in \mathcal{M}(C)$ and write $(f) =: D = \sum n_k(P_k) \in \mathrm{Div}^0(C)$ with integers $n_k \neq 0$. Now we easily verify that the only poles of $df/f \in \Omega(C)$ are

simple poles at each P_k with residue n_k. Then df/f has the same poles with the same residues as the differential $\omega_D \in \Omega(C)$ as given by Lemma 2.6.11, so we must have $df/f = \omega_D + \omega$ for some holomorphic differential $\omega = \sum_{i=1}^g m_i\omega_i \in \Omega(C)$ with $m_i \in \mathbb{C}$. Now, using Lemma 2.6.12, we have

$$AJ(D) = \frac{1}{2\pi i}\left(\int_{b_1}\omega_D, ..., \int_{b_g}\omega_D\right)+\Lambda = \frac{1}{2\pi i}\left(\int_{b_1}\frac{df}{f}, ..., \int_{b_g}\frac{df}{f}\right)-\frac{1}{2\pi i}\left(\int_{b_1}\omega, ..., \int_{b_g}\omega\right)+\Lambda$$

$$= \frac{1}{2\pi i}\left(\int_{b_1}\frac{df}{f}, ..., \int_{b_g}\frac{df}{f}\right) - \frac{1}{2\pi i}\sum_{i=1}^g m_i\left(\int_{b_1}\omega_i, ..., \int_{b_g}\omega_i\right) + \Lambda. \tag{2.19}$$

Note that Lemma 2.6.13 implies that the first term in (2.19) lies in $\mathbb{Z}^g \subset \Lambda$. Moreover, we claim that each m_i is an integer multiple of $2\pi i$. Indeed, for any j, we have $0 = \int_{a_j}\omega_D = \int_{a_j} df/f - \sum_{i=1}^g m_i\int_{a_j}\omega_i = \int_{a_j} df/f - m_i$. The claim now follows from the fact that $m_i = \int_{a_i} df/f$ is an integer multiple of $2\pi i$ again by Lemma 2.6.13. Therefore, the second term in (2.19) lies in $\mathbb{Z}^g\Pi$. But since Π is symmetric by Corollary 2.6.10, $\mathbb{Z}^g\Pi = \Pi\mathbb{Z}^{2g} \subset \Lambda$ and so $AJ(D) = 0 \in \mathbb{C}^g/\Lambda = J$, as desired.

We now prove the converse – if $D = \sum n_k(P_k) \in \mathrm{Div}^0(C)$ is a divisor such that $AJ(D) = 0 \in J$, then D is the divisor associated to some function $f \in \mathcal{M}(C)$ – by essentially running the above argument backwards. We again define $\omega_D \in \Omega(C)$ to be the differential form given by Lemma 2.6.11. We would like to be able to set $f(P) = e^{\int_O^P \omega_D}$, noting that $df/f = \omega_D$ and so $(f) = D$, but this function is not well-defined unless the integral $\int_O^P \omega_D$ is well-defined up to an integer multiple of $2\pi i$. We claim that there is a holomorphic differential $\omega \in \Omega(C)$ such that each $\int_{a_i}\omega_D+\omega$ and $\int_{b_i}\omega_D+\omega$ is an integer multiple of $2\pi i$. Indeed, since $AJ(D) = 0$, we have $(\sum_k n_k\int_O^{P_k}\omega_1, ..., \sum_k n_k\int_O^{P_k}\omega_g) \in \Lambda = \mathbb{Z}^g + \Pi\mathbb{Z}^g = \mathbb{Z}^g + \mathbb{Z}^g\Pi$, where each integral is defined along a path lying in the interior of $\mathcal{P}$. Therefore, for $1 \le j \le g$, we have $\sum_k n_k\int_O^{P_k}\omega_j = s_j + \sum_{i=1}^g t_i\Pi_{i,j}$ for some integers $s_j, t_1, ..., t_g \in \mathbb{Z}$. Now we let $\omega = -2\pi i\sum_{i=1}^g t_i\omega_i$. Then for each j, we have $\frac{1}{2\pi i}\int_{a_j}(\omega_D+\omega) = \frac{1}{2\pi i}\int_{a_j}\omega = -t_j \in \mathbb{Z}$. Moreover, using Lemma 2.6.12, we have

$$\frac{1}{2\pi i}\int_{b_j}\omega_D+\omega = \sum_k n_k\int_O^{P_k}\omega_j - \sum_{i=1}^g m_i\int_{b_j}\omega_i = s_j + \sum_{i=1}^g m_i\Pi_{i,j} - \sum_{i=1}^g m_i\Pi_{i,j} = s_j \in \mathbb{Z}. \tag{2.20}$$

Therefore, $\int_a(\omega_D+\omega) \in 2\pi i\mathbb{Z}$ for all $a \in H_1(C,\mathbb{Z})$, and so the expression $\int_O^P(\omega_D+\omega)$ is defined up to integer multiples of $2\pi i$. Thus, the meromorphic function $f(P) := e^{\int_O^P(\omega_D+\omega)}$ is well-defined. Moreover, since ω is holomorphic, $\omega_D+\omega$ has the same poles with the same residues as ω_D does, and it follows that $(f) = D$. Abel's Theorem is proved.

2.6.4 Proof of Jacobi's Theorem

We now prove Jacobi's part of Theorem 2.6.7. This proof is much simpler and (in my opinion) a little more intuitive. The idea is that by Corollary 2.6.4, given a basepoint $O \in C$, every

divisor in $\mathrm{Div}^0(C)$ can be represented by a divisor of the form $\sum_{i=1}^{g}(P_i) - g(O)$. Therefore, Abel's Theorem implies that it suffices to study the map $\Psi : C^g \to J$ given by

$$\Psi : (P_1, ..., P_g) \mapsto \sum_{i=1}^{g} \left(\int_O^{P_i} \omega_1, ..., \int_O^{P_i} \omega_g \right)$$

and to show that it is surjective. (In fact, it is possible to show in the algebraic case that J is a g-dimensional variety and Ψ induces a birational map from the g-fold symmetric product of C to J, but we will not show this here.)

Lemma 2.6.14. *There exists a divisor of the form $D' := \sum_{i=1}^{g}(Q_i) \in \mathrm{Div}(C)$ for some distinct points $Q_i \in C$ such that there is no nonzero holomorphic differential form ω with $(\omega) \geq D'$.*

Proof. Choose a holomorphic differential form $\omega_0 \in \Omega(C)$, and choose a point $Q_1 \in C$ at which ω_0 does not have a zero. Since by Corollary 2.6.3, the dimension of the space of holomorphic differentials has dimension g, it follows that the space of holomorphic differentials ω with $(\omega) \geq (Q_1) \in \mathrm{Div}(C)$ has dimension strictly less than g. But it follows from putting $D = (Q_1)$ into the formula in Theorem 2.6.2 that $l(K - (Q_1)) \geq g - 1$, and thus the dimension of the latter space, which is isomorphic to $\mathcal{L}(K - (Q_1))$, is equal to $g - 1$. Now choose a holomorphic differential form $\omega_1 \in \Omega(C)$ with $(\omega_1) \geq (Q_1)$, and choose a point $Q_2 \in C$ at which ω_1 does not have a zero. By a similar argument, we get $l(K - (Q_1) - (Q_2)) = g - 2$. We may repeat this process until we have distinct points $Q_1, ..., Q_g$ such that $l(K - (Q_1) - ... - (Q_g)) = g - g = 0$, which implies the desired property. □

Lemma 2.6.15. *Choose distinct points $Q_1, ..., Q_g \in C$ satisfying the property given in the statement of Lemma 2.6.14. Then there is an open neighborhood U of $(Q_1, ..., Q_g) \in C^g$ such that the map $C^g \to J$ given by*

$$(P_1, ..., P_g) \mapsto \sum_{i=1}^{g} \left(\int_{Q_i}^{P_i} \omega_1, ..., \int_{Q_i}^{P_i} \omega_g \right) + \Lambda,$$

when restricted to U, is a biholomorphism of U onto an open neighborhood of $0 \in J$.

Proof. Choose an open neighborhood U' of $(Q_1, ..., Q_g) \in C^g$ such that each projection of U' is simply connected. Now consider the map $\tilde{\Psi} : U' \to \mathbb{C}^g$ given by

$$(P_1, ..., P_g) \mapsto \sum_{i=1}^{g} \left(\int_{Q_i}^{P_i} \omega_1, ..., \int_{Q_i}^{P_i} \omega_g \right),$$

which is well-defined because of simple connecteness. Let t_i be a local parameter of Q_i for $1 \leq i \leq g$. Then locally $\tilde{\Psi}$ can be expressed as a map $\mathbb{C}^g \to \mathbb{C}^g$ given by $(t_i)_{i=1}^g \mapsto (\psi_j(t_1, ..., t_g))_{j=1}^g$ for functions ψ_j such that $d\psi_j/dt_i = \omega_j/dt_i$ for $1 \leq i, j \leq g$. Thus the Jacobian matrix of the holomorphic function $\tilde{\Psi}$ at the point $(Q_1, ..., Q_g) \in U'$ is given by (ω_j/dt_i). This Jacobian matrix can be viewed as a linear map from the space of holomorphic

differential forms on C to $\mathbb{C}^g$, where each holomorphic $\omega = \sum_{j=1}^g m_j\omega_j \in \Omega(C)$ is considered as the column vector $(m_j)_{1\leq j\leq g} \in \mathbb{C}^g$. So if the kernel of this map were nontrivial, then there would exist a nonzero holomorphic $\omega \in \Omega(C)$ with $\omega/dt_i = 0$ for $1 \leq i \leq g$. In other words, ω would have a zero at all points Q_i, which contradicts the property of the Q_i's given in the hypothesis. Thus, the Jacobian matrix is invertible, and by the Inverse Function Theorem there is a neighborhood $U \subseteq U'$ of $(Q_1, ..., Q_g) \in \mathbb{C}^g$ such that the map given in the statement is a biholomorphism of U onto an open neighborhood of $0 \in J$.

□

Remark 2.6.16. Obviously it is no coincidence that in determining the group structure of what we now call the "Jacobian variety" of a curve, the mathematician Jacobi used what we now call a "Jacobian matrix". Referring simply to "Jacobians" can occasionally cause confusion in my experience, because many mathematicians and physicists often assume that one is talking about the somewhat better-known Jacobian matrices.

Now we can prove Jacobi's theorem. We choose distinct points $Q_1, ..., Q_g$ satisfying the property given in Lemma 2.6.14, which we know exist by that lemma. Then it follows from Lemma 2.6.15 and the above discussion that the map $AJ : \mathrm{Div}^0(C) \to J$ is surjective onto an open neighborhood of $v := \sum_{i=1}^g (\int_O^{Q_i} \omega_1, ..., \int_O^{Q_i} \omega_g) + \Lambda \in J$. Since $v = AJ(\sum_{i=1}^g (Q_i) - g(O))$, we see that AJ is surjective onto a translation of that open neighborhood by $-v$, which is an open neighborhood of $0 \in J$ which we denote by U''. It is easy to see that given any $a \in J$, we have $a/N \in U''$ for some large enough integer N. Therefore, there is some divisor $D \in \mathrm{Div}^0(C)$ with $AJ(D) = a/N$ and therefore, $AJ(N \cdot D) = a$. Therefore, the Abel-Jacobi map AJ is surjective onto all of J, and Jacobi's Theorem is proved.

The following easy corollary directly implies that J is actually a complex torus.

Corollary 2.6.17. *The lattice $\Lambda \in \mathbb{C}^g$ has rank $2g$.*

Proof. The statement is equivalent to the claim that $\mathbb{C}^g = \Lambda + A$ for some compact neighborhood of A of $0 \in \mathbb{C}^g$. Theorem 2.6.7 tells us that any $a \in J$ is the image under AJ of some $[D] \in \mathrm{Pic}^0(C)$, and in fact, Corollary 2.6.4 tells us that we can choose a representative of $[D]$ of the form $D = \sum_{i=1}^g (P_i) - g(O)$ (here O is the basepoint used to define the map AJ). Thus, $v := \sum_{i=1}^g (\int_O^{P_i} \omega_1, ..., \int_O^{P_i} \omega_g) \in \mathbb{C}^g$ maps to $a \in J$ under the quotient map $\mathbb{C}^g \twoheadrightarrow \mathbb{C}^g/\Lambda = J$, where the path from O to each P_i lies inside a fixed fundamental polygon $\mathcal{P}$ defining the Riemann surface C (see the beginning of §2.6.2). The set A of all such elements $\sum_{i=1}^g (\int_O^{P_i} \omega_1, ..., \int_O^{P_i} \omega_g) \in \mathbb{C}^g$ for $P_1, ..., P_g \in C$ is clearly bounded with respect to the usual norm of $\mathbb{C}^g$ and therefore compact, thus proving the corollary.

□

Remark 2.6.18. a) Note that Theorem 2.6.7 and Corollary 2.6.17 give us a canonical isomorphism $H_1(C, \mathbb{Z}) \xrightarrow{\sim} \Lambda = H_1(J, \mathbb{Z})$ of $\mathbb{Z}$-lattices of rank $2g$.

b) It can be shown using Riemann's relations (Corollary 2.6.10 and Exercise 2.7.9) that there is a positive definite Riemann form on $\mathbb{C}^g$ with respect to Λ induced by the intersection pairing on $H_1(C, \mathbb{Z}) \cong \Lambda$. It follows that J is in fact a complex abelian variety of dimension g. Moreover, since the determinant of the intersection pairing is 1, we see that J has a canonical principal polarization so that J is self-dual.

c) It is possible also for any smooth, proper curve C over any field K to show that the group $\mathrm{Pic}^0(C)$ also has the structure of an abelian variety over K and thus to define the Jacobian of a curve in a completely algebraic setting. This is done by Milne in [4].

2.7 Exercises

Exercise 2.7.1. Show that the Riemann form defined at the beginning of §2.4 is well-defined regardless of choice of basis of Λ.

Exercise 2.7.2. Show in two different ways (directly from definitions, and as a corollary to Proposition 2.5.15), that the group of Riemann forms for an elliptic curve is isomorphic to $\mathbb{Z}$, so that any Riemann form for an elliptic curve is an integer multiple of the one defined at the beginning of §2.4. (The group of Riemann forms for an abelian variety X is called the *Néron-Severi group* of X.)

Exercise 2.7.3. Show that the subgroup $\mathrm{Div}^0(X) \subseteq \mathrm{Div}(X)$ may instead be defined as consisting of all divisors $D \in \mathrm{Div}(X)$ such that $t_a^* D - D \in \mathrm{Prin}(X)$ for all $a \in X$ (this is how $\mathrm{Div}^0(X)$ is defined in a purely algebraic setting).

Exercise 2.7.4. Let $\varphi : X_1 \to X_2$ be an isogeny of complex abelian varieties. In a natural way, construct an isogeny $\varphi^\vee : X_2^\vee \to X_1^\vee$, called the *dual isogeny*. This shows that taking duals is in some sense a contravariant functor from the category of abelian varieties to itself. (Hint: in fact, the map $\varphi^\vee : \mathrm{Pic}^0(X_2) \to \mathrm{Pic}^0(X_1)$ is given by pulling back divisors as discussed earlier; the hard part is showing that $\varphi^\vee$ is an isogeny. This exercise is rather long and difficult but can be done by unwinding several definitions and constructions.)

Exercise 2.7.5. Show that if $\varphi : X_1 \to X_2$ is an isogeny of complex elliptic curves, and we identify each elliptic curve with its dual, then the dual isogeny $\varphi^\vee : X_2 \to X_1$ defined in the above exercise is actually the isogeny φ' guaranteed by (and constructed in the proof of) Corollary 2.5.7.

Exercise 2.7.6. Use the Riemann-Roch formula (Theorem 2.6.2) to verify some of what was shown in Example 2.6.1.

Exercise 2.7.7. Show that the Abel-Jacobi map defined on points of C, which was denoted $AJ : C \to \mathbb{C}^g/\Lambda$ in §2.6.2 is always injective as long as $g \geq 1$. Conclude that AJ is an isomorphism if $g = 1$ (this is another way to see that a complex curve which has genus 1 according to the algebraic definition can be realized as $\mathbb{C}$ modulo a lattice).

Exercise 2.7.8. Formulate a shorter argument for one direction of Abel's Theorem – the claim that $\mathrm{Prin}(C) \subseteq \ker(AJ)$ – based on the following ideas. For any $f \in \mathcal{M}(C)$, one may define a holomorphic map $\mathbb{C} \cup \{\infty\} \to J$ by composing the map $\mathbb{C} \cup \{\infty\} \to \mathrm{Div}(C)$ given by $z \mapsto f^*((z)) \in \mathrm{Div}(C)$ with AJ. First show that this map is constant. Then use this to prove that $AJ((f)) = 0 \in J$.

Exercise 2.7.9. Using Lemma 2.6.3, prove the second of "Riemann's relations", which says that the imaginary part of Π is positive definite. (Hint: use the fact that $\frac{1}{2i}\int_C \omega \wedge \bar{\omega} > 0$ for any holomorphic $\omega \neq 0$.)

Chapter 3

Elliptic curves and arithmetic

We now turn to the second part of the course, where we focus solely on elliptic curves (rather than abelian varieties) and study them from a purely algebraic point of view. This means that we will no longer assume that a given elliptic curve is defined over the complex numbers, and we will instead specify a field K over which the curve is defined. Of course, if in many cases, such as when K is finitely generated over $\mathbb{Q}$, there is obviously an embedding $K \hookrightarrow \mathbb{C}$ and our elliptic curve can still be defined over $\mathbb{C}$, which at times will allow us to draw from the theory of complex elliptic curves.

3.1 Defining equations and the group law

We start this chapter by finally uniting the three definitions of "elliptic curve" given in §1.1. For the most part, we have already shown (at least in the complex case) that they are equivalent. We sum up most of the relevant facts in the following proposition. Note that we will only prove part (b) below in the case that $K = \mathbb{C}$.

Proposition 3.1.1. *a) Given a smooth projective curve C over a field K of characteristic different from 2, the following are equivalent:*

i) C has genus 1;

ii) C can be defined by an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in K$ such that there are no singular points; and

*iii) C can be defined by an equation of the form $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic polynomial without multiple roots in $\bar{K}$ (this is called **Weierstrass form**).*

Moreover, if these equivalent conditions hold, then distinguishing a K-point $O \in C$ gives C the structure of a 1-dimensional abelian variety over K whose identity element is O.

b) Let A be an abelian variety of dimension 1. Then conversely, A is a smooth projective curve of genus 1 and can therefore be defined using an equation of a form given in (a)(ii) or in (a)(iii).

Proof. For part (a), we first note that (iii) immediately implies (ii), while given an equation of the form in (ii), one can get rid of a_1 and a_3 by a simple completing-the-square operation which replaces y by $y - (a_1x + a_3)/2$. Therefore, (ii) and (iii) are equivalent, and it remains to show that both are equivalent to (i). Given a smooth projective curve C of genus $g = 1$,

recall that we showed using the Riemann-Roch theorem (which holds over general fields as well as $\mathbb{C}$) that any canonical divisor $K \in \mathrm{Div}(C)$ has degree $2g-2=0$. Given a K-point $O \in C$, it follows that $l(n(O)) = n$ for $n \geq 1$. Then we may apply the same argument in the proof of Proposition 2.4.1 to show that C may be defined by a polynomial relation in two variables x and y which is a linear combination of $1, x, y, x^2, xy, y^2, x^3 \in K[x,y]$, where the coefficients of both x^3 and y^2 must be nonzero. Thus, after possibly scaling x and y, we get a defining equation of the form given in (ii). Conversely, suppose that C is defined by an equation of the form given in (iii). Then it is straightforward to verify that all holomorphic differentials on C are scalar multiples of dx/y and therefore the genus is 1.

To prove the second statement of (a), we note that in the complex case, a genus 1 curve C is isomorphic via the Abel-Jacobi map AJ (which we define with respect to the chosen point O) to its Jacobian J, which is an 1-dimensional abelian variety (see Exercise 2.7.7). For general K, first let C be defined by an equation of the form in (a)(iii). We may assume that the distinguished K-point O is the infinity point ∞, because otherwise we may "subtract by O" using the operation described in Definition 1.1.4, which is clearly algebraic and defined over K. Now, in order to show that C is an abelian variety it suffices to show that this law is in fact a group law as claimed, which we will do below (Proposition 3.1.2).

To prove (b) in the complex case, we use the results in §2.1 as well as Proposition 2.4.1, which show that every 1-dimensional abelian variety is given by $\mathbb{C}$ modulo a lattice, which can be uniformized as a complex curve defined by a cubic polynomial of the form in (a)(ii). □

In order to finish proving that our three Definitions 1.1.1, 1.1.3, and 1.1.4 are all equivalent, all we need to do is to show that the law described in the last definition is in fact a group law. Actually, all the group axioms were proven for this law except for the associative property. In order to show this, we will show that if E is a curve of genus 1 over any field K with a distinguished K-point $O \in E$, then there is a bijection of sets $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ (which in the complex case is just the Abel-Jacobi map) such that the group law on $\mathrm{Pic}^0(E)$ can be defined for the points of the curve E as in Definition 1.1.4. Before stating this next proposition, we note that the law given in the definition is essentially equivalent to saying that the sum of three points on the cubic add up to 0 if and only if there is a line in $\mathbb{P}^2_K$ which intersects E at exactly those three points (counting multiplicities).

Proposition 3.1.2. *Let E be a smooth projective curve of genus 1 over a field K, and let O be a K-point of E.*

a) The map on $\bar{K}$-points of E given by $P \mapsto [(P)-(O)] \in \mathrm{Pic}^0(E)$ defines a bijection of sets $\phi : E(\bar{K}) \xrightarrow{\sim} \mathrm{Pic}^0(E)$. In this way, $E(\bar{K})$ inherits a group law from $\mathrm{Pic}^0(E)$ in which O is the identity element (which we also denote by $0 \in E(\bar{K})$).

b) Now let E be given by an equation of the form in Definition 1.1.4 and let $O = \infty$. The group law on $E(\bar{K})$ which we obtain as in part (a) can be defined by the following rule: for any points $P, Q, R \in E(\bar{K})$, we have $P+Q+R=0$ if and only if there is a line in $\mathbb{P}^2_K$ which intersects E at exactly P, Q, and R (counting multiplicities).

Proof. We note that in the complex case, (a) is given by Exercise 2.7.7. For general K, note first that there cannot be a function $h \in \bar{K}(E)$ with a pole of order 1 at one point

$P \in E(\bar{K})$ and no poles anywhere else because then $h : E \to \mathbb{P}^1_K$ would be a degree-1 morphism which would force $E = \mathbb{P}^1_K$ (this can also be checked using Riemann-Roch). Therefore $(P) - (\infty) \in \mathrm{Div}^0(E)$ is not principal for $P \neq \infty$ and the map is injective. Surjectivity follows from Corollary 2.6.4, which says that every divisor class in $\mathrm{Pic}^0(E)$ can be represented by a divisor of the form $(P) - (\infty) \in \mathrm{Div}^0(E)$.

Now let $P, Q, R \in E(\bar{K})$ be any points, and assume that $P, Q, R \neq \infty$ (the full argument in the case that some of these points are ∞ is very similar). Suppose first that there is a line in $\mathbb{P}^2_K$ as in the statement of part (b). That is to say, if this line is given by a linear equation $h(x, y) = 0$ for some $h \in \bar{K}(E)$, then the linear function h has associated divisor $(P)+(Q)+(R)-3(\infty)$ (note that a line intersects a cubic at 3 points by Bézout's Theorem, so h cannot have any other zeros). Then $0 = [(P)+(Q)+(R)-3(\infty)] = \phi(P)+\phi(Q)+\phi(R) \in \mathrm{Pic}^0(E)$ and therefore $P + Q + R = 0$.

Conversely, suppose that $P+Q+R = 0$. Then $[(P)+(Q)+(R)-3(\infty)] = \phi(P)+\phi(Q)+\phi(R) = 0 \in \mathrm{Pic}^0(E)$, so there is some function $h \in \bar{K}(E)$ with $(h) = (P)+(Q)+(R)-3(\infty)$. Then $h \in \mathcal{L}(3(\infty))$, which has dimension 3 by Riemann-Roch. Since $1, x, y \in \mathcal{L}(3(\infty))$ with no linear relations between them, $\mathcal{L}(3(\infty)) = \langle 1, x, y \rangle$ and h is a linear function in x and y. Therefore, the line in $\mathbb{P}^2_K$ given by $h(x, y) = 0$ intersects E at exactly the points P, Q, and R (counting multiplicities).

□

3.2 Isogenies and endomorphisms of elliptic curves

For this entire section, we make the simplifying assumption that the characteristic of the ground field K is not 2. For a treatment of elliptic curves in characteristic 2, see Appendix A of [8].

3.2.1 Isomorphisms and the j-invariant

We assume for this subsection that every elliptic curve E over K is defined using a model in Weierstrass form ($y^2 = f(x)$ for some cubic polynomial $f \in K[x]$ with no multiple roots in $\bar{K}$). We now investigate how to tell from any cubic polynomial $f \in K[x]$ whether the curve given by $y^2 = f(x)$ is smooth or has a particular type of singularity, and whether or not it is isomorphic to another curve of this form. First we define some important constants associated to a Weierstrass cubic $y^2 = f(x)$.

Definition 3.2.1. *Let $f(x) = x^3 + bx^2 + cx + d$ with $b, c, d \in K$. Then the **discriminant** of the (projective) cubic curve E given by $y^2 = f(x)$ is defined to be 16 times the discriminant of the cubic f (it's given by $\Delta(E) = 16(b^2c^2 - 4c^3 - 27d^2 + 18bcd) \in K$). If $\Delta \neq 0$, then the j-**invariant** of E is given by $j(E) = (16b^2 - 48c)^3/\Delta(E) \in K$.*

Proposition 3.2.2. *a) Let E be the projective curve over K given by an equation of the form $y^2 = f(x)$ as in Definition 3.2.1. Then E is an elliptic curve (i.e. E is smooth) if and only if $\Delta(E) \neq 0$. If $\Delta(E) = 0$, then E has a node (resp. a cusp) if the cubic f has a double root and a single root (resp. has a triple root) in $\bar{K}$.*

b) If E_1 and E_2 are elliptic curves over K given by equations of the form $y^2 = f_1(x)$ and $y^2 = f_2(x)$ respectively, then the following are equivalent:

i) E_1 and E_2 are isomorphic over some algebraic extension K'/K;

ii) $f_2(x) = f_1(u^2x + v)$ for some elements u, v in some algebraic extension K'/K; and

iii) $j(E_1) = j(E_2)$.

c) For any $j_0 \in \bar{K}$, there is an elliptic curve E defined over $K(j_0)$ with $j(E) = j_0$. (In particular, for any $j_0 \in K$, there is an elliptic curve E defined over K with $j(E) = j_0$.)

Proof. Part (a) can be proven through an elementary computation using algebraic geometry, noting that $\Delta(E) = 0$ if and only if the cubic $f(x)$ has a multiple root $\alpha \in \bar{K}$. If this is the case, then the point $(\alpha, 0) \in E(\bar{K})$ is a singular point, and it is a node (resp. a cusp) if α is a double root (resp. a triple root).

For (b), we first check that any isomorphism of elliptic curves $E_1 \xrightarrow{\sim} E_2$ must fix the point at infinity and therefore projects to an affine transformation on the x-line, so $x \mapsto u'x + v$ for some $u, v \in K'$. Since scaling x by u' forces y to be scaled by $\pm u'^{3/2}$, it is clear that $u' = u^2$ for some $u \in K'$. Now it is straightforward to check that $x \mapsto u^2x + v$ multiplies the discriminant of the cubic f, and therefore also $\Delta(E)$, by u^{12}. However, it also multiplies the expression $(16b^2 - 48c)^3$ by u^{12} and therefore doesn't change $j(E)$. Meanwhile, translating x by v changes neither the discriminant $\Delta(E)$ nor the expression $(16b^2 - 48c)^3$, so that also doesn't change $j(E)$. Finally, assume that E_1 and E_2 two elliptic curves such that $j(E_1) = j(E_2)$. Then if we assume that the characteristic of K is different from 3 (for fields of characteristic 3, this is a separate exercise), we can reduce the cubics in the equations defining E_1 and E_2 so that the x^2-terms vanish, and directly find some $u \in \bar{K}$ such that the map $(x, y) \mapsto (u^2x, u^3y)$ is an isomorphism $E_1 \xrightarrow{\sim} E_2$.

For (c), choose any $j_0 \in \bar{K}$. Then if $j_0 \neq 0, 1728$, consider the elliptic curve E_{j_0} over the field $K(j_0)$ defined by the equation

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}. \tag{3.1}$$

Then we check that this equation describes a smooth curve in these cases and compute $j(E_{j_0}) = j_0$. If $j_0 = 0$, then we let E_0 be given by $y^2 = x^3 - 1$ and check that $j(E_0) = 0$. If $j_0 = 1728$, then we let E_{1728} be given by $y^2 = x^3 - x$ and check that $j(E_{1728}) = 1728$.

□

Remark 3.2.3. The reader may wonder why quantities like $\Delta(E)$ and $j(E)$ are defined with "extra" factors like 1728 and 16^3 which actually play no role in the statement of the above proposition nor in its proof. The main explanation is that when considering reduction of elliptic curves over local fields of residue characteristic 2 and 3, it becomes useful to define these quantities to have certain divisibilities by 2 and by 3 so that results can be stated more elegantly.

3.2.2 Isogenies and their duals

We recall the definition of an "isogeny" of abelian varieties which was given as Definition 2.5.1: an *isogeny* of elliptic curves E_1 and E_2 is a surjective morphism $E_1 \to E_2$ which is

a homomorphism of groups. We now present an equivalent definition in the case of elliptic curves.

Definition 3.2.4. *An **isogeny** of elliptic curves E_1 and E_2 is a nonconstant morphism $\varphi : E_1 \to E_2$ with $\varphi(0) = 0$.*

Proposition 3.2.5. *The definition of "isogeny" of elliptic curves given as Definition 2.5.1 is equivalent to Definition 3.2.4.*

Proof. Clearly Definition 2.5.1 implies Definition 3.2.4. Now let $\varphi : E_1 \to E_2$ be a nonconstant morphism satisfying $\varphi(0) = 0$. Let $\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ be the induced homomorphism on divisor classes given by $[\sum_i n_i(P_i)] \mapsto [\sum_i n_i(\varphi(P_i))]$. Then if we let $\phi_j : E_j \xrightarrow{\sim} \mathrm{Pic}^0(E_j)$ be the isomorphism given in Proposition 3.1.2 for $j = 1, 2$, it is easy to check that the maps $\varphi : E_1 \to E_2$ and $\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ commute with the ϕ_j's (using the fact that $\varphi(0) = 0$). Therefore, φ is also a group homomorphism. Moreover, since any nonconstant map between proper curves is surjective, φ is a surjection.

□

Note that one can easily verify using the Hurwitz Formula that every isogeny is an unramified morphism (see Exercise 3.3.1).

Proposition 3.2.6. *Let E be an elliptic curve over a field K, and let $N \subset E(\bar{K})$ be a finite subgroup. Then there is an elliptic curve E' defined over some algebraic extension K' of K and a separable isogeny $\varphi : E \to E'$ defined over K' whose kernel coincides with N. In other words, the quotient E/N is an elliptic curve.*

Remark 3.2.7. Note that this was already shown for complex elliptic curves in Corollary 2.5.5. In fact, the extension K' is the subfield of $\bar{K}$ fixed by the elements of the absolute Galois group of K which stabilize $N \subset E(\bar{K})$, but we will not prove this here.

Proof. For each point $P \in E(\bar{K})$, let $t_P : E \to E$ be the translation-by-P morphism defined over $\bar{K}$ which is given by $Q \mapsto P + Q$, and let $t_P^* : \bar{K}(E) \to \bar{K}(E)$ be the pullback of this morphism to an automorphism of the function field. Let Φ be the (finite) group of automorphisms of $\bar{K}(E)$ consisting of elements t_P^* for each $P \in N$, and let $\bar{K}(E)^\Phi$ be the subfield of $\bar{K}(E)$ fixed by this automorphism group. Then clearly $\bar{K}(E)$ is a finite Galois extension of $\bar{K}(E)^\Phi$ with Galois group Φ. Since $\bar{K}(E)^\Phi$ also has transcendence degree 1 over $\bar{K}$, there is a smooth curve E' over $\bar{K}$ with $\bar{K}(E') = \bar{K}(E)^\Phi$, and the inclusion $\bar{K}(E') \hookrightarrow \bar{K}(E)$ corresponds to a morphism $\varphi : E \to E'$ (we can always find a subfield $K' \subseteq \bar{K}$ finite over K over which E' and φ are defined). It is easy to check that the inverse image of any point in $E'(\bar{K})$ is a coset of the subgroup $N \subset E(\bar{K})$ by showing that $f \circ \varphi \circ t_P = f \circ \varphi$ for every $f \in \bar{K}(E')$. Thus, the morphism φ is unramified. It follows from an application of the Hurwitz Formula that E' has genus 1, and therefore, by choosing the distinguished point $\varphi(0) \in E'(\bar{K})$, we see that E' is an elliptic curve and that φ is an isogeny.

□

As we saw before in §2.5.1, an isogeny always has finite degree and finite kernel. It is clear from basic algebraic principles that the degree is equal to the order of the kernel if and only if the isogeny is separable (which is always the case when K has characteristic 0). Moreover, as in the complex situation described in §2.5.1, for any elliptic curve E and integer $n \neq 0$, one can prove without much difficulty that the multiplication-by-n map $[n] : E \to E$ is an isogeny (see Exercise 3.3.2).

We denote by $\mathrm{Hom}(E_1, E_2)$ the set of all isogenies from the elliptic curve E_1 to the elliptic curve E_2, along with the trivial map $0 : E_1 \to E_2$. Then it is clear from the abelian group structure on E_2 that $\mathrm{Hom}(E_1, E_2)$ has the structure of a $\mathbb{Z}$-module. It is clear that $\mathrm{Hom}(E_1, E_2)$ is torsion-free.

In §2.5, given an isogeny of abelian varieties $\varphi : X_1 \to X_2$, we came up with two notions of a dual isogeny: the isogeny $\varphi' : X_2 \to X_1$ given by Corollary 2.5.7 and the isogeny $\varphi^\vee : X_2^\vee \to X_1^\vee$ constructed in Exercise 2.7.4. One can show (Exercise 2.7.5) that these two notions coincide in the case of complex elliptic curves, and we will now show that dual isogenies can be constructed in the purely algebraic situation as well. Note that this will allow us to say that two elliptic curves are "isogenous" (satisfying an equivalence relation) if there is an isogeny from one to the other, as we did for complex abelian varieties (see Remark 2.5.8).

Definition 3.2.8. *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. Then we define the **dual isogeny** $\varphi^\vee : E_2 \to E_1$ as the map given by $\phi_1^{-1} \circ \varphi^* \circ \phi_2$, where $\varphi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$ is the pullback map on divisor classes induced by φ, and where $\phi_j : E_j \xrightarrow{\sim} \mathrm{Pic}^0(E_j)$ is the isomorphism given in Proposition 3.1.2 for $j = 1, 2$.*

It might not be immediately obvious from the definition of "dual isogeny" that this map $\varphi^\vee$ is actually an isogeny. The next proposition claims this and much more.

Proposition 3.2.9. *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves.*

a) We have $\varphi^\vee \circ \varphi = [m] : E_1 \to E_1$ and $\varphi \circ \varphi^\vee = [m] : E_2 \to E_2$, where $m = \deg(\varphi)$.

b) If $\psi : E_1 \to E_2$ is another isogeny, then $(\varphi + \psi)^\vee = \varphi^\vee + \psi^\vee$ and $(\varphi \circ \psi)^\vee = \psi^\vee \circ \varphi^\vee$.

c) We have $[n]^\vee = [n] : E \to E$ and $\deg([n]) = n^2$ for any integer n.

d) The map $\varphi^\vee$ is an isogeny with $\deg(\varphi^\vee) = \deg(\varphi)$.

e) We have $(\varphi^\vee)^\vee = \varphi : E_1 \to E_2$.

Proof. Choose some $Q \in E_2(\bar{K})$ and $P_0 \in \varphi^{-1}(Q)$, and let φ^{insep} denote the inseparable part of φ (so that $\varphi = \varphi^{\mathrm{sep}} \circ \varphi^{\mathrm{insep}}$ with φ^{sep} separable). Now compute

$$\varphi^\vee(Q) = \phi_1^{-1}(\varphi^*([(Q) - (O)])) = \phi_1^{-1}\left(\left[\deg(\varphi^{\mathrm{insep}}) \cdot \left(\sum_{P \in \varphi^{-1}(Q)} (P) - \sum_{T \in \varphi^{-1}(O)} (T)\right)\right]\right)$$

$$= \phi_1^{-1}\left(\left[\deg(\varphi^{\mathrm{insep}}) \cdot \left(\sum_{T \in \varphi^{-1}(O)} (P_0 + T) - \sum_{T \in \varphi^{-1}(O)} (T)\right)\right]\right)$$

$$= \phi_1^{-1}\left(\deg(\varphi)^{\mathrm{insep}} \cdot \#\varphi^{-1}(Q) \cdot [(P_0) - (O)]\right) = \deg(\varphi)\phi_1^{-1}([(P_0] - [O]) = mP_0.$$

Therefore $\varphi^\vee \circ \varphi = [m]$. Now we verify

$$[m] \circ \varphi = \varphi \circ [m] = \varphi \circ (\varphi^\vee \circ \varphi) = (\varphi \circ \varphi^\vee) \circ \varphi,$$

from which it follows that $\varphi \circ \varphi^\vee = [m]$ since φ is surjective, proving (a).

We omit the proof of the first claim in (b) (which is surprisingly difficult), and the second claim follows immediately from the definition of the dual isogeny.

To prove (c), we can see directly that $[0]^\vee = [0]$ and $[1]^\vee = [1]$, and the fact that $[n]^\vee = [n]$ for general $n \geq \mathbb{Z}$ follows from an obvious inductive argument using the additivity given in (b). Now let $m = \deg([n])$ and note that by (a), $[m] = [n]^\vee \circ [n] = [n] \circ [n] = [n^2]$. Since then $[0] = [m] - [n^2] = [m - n^2]$ and multiplication by any nonzero integer is a nonconstant map, we have $m - n^2 = 0$ and so $\deg([n]) = n^2$.

To prove (d), it suffices to show that there always exists an isogeny $\varphi' : E_2 \to E_1$ with the property that $\varphi' \circ \varphi = [m]$, from which it will follow from (a) that as maps from E_2 to E_1, $\varphi^\vee = \varphi'$ and therefore $\varphi^\vee$ is an isogeny. If φ is separable, this claim follows from an algebraic argument which we omit here concerning inclusions among the function fields $\bar{K}(E_1)$ and $\bar{K}(E_2)$. We will defer the proof of the claim in the case that φ is not separable to the next subsection.

Now using (a) and the fact that $\deg(\phi^\vee) = m$ by (d), we have

$$\varphi \circ [m] = [m] \circ \varphi = ((\varphi^\vee)^\vee \circ \varphi^\vee) \circ \varphi = (\varphi^\vee)^\vee \circ (\varphi^\vee \circ \varphi) = (\varphi^\vee)^\vee \circ [m].$$

Since $[m]$ is surjective, it follows that $\varphi = (\varphi^\vee)^\vee$, proving (e).

□

For any elliptic curve E over a field K and integer $n \geq 1$, we denote by $E[n] \subset E[\bar{K}]$ the kernel of the multiplication-by-n map $[n] : E(\bar{K}) \to E(\bar{K})$.

Corollary 3.2.10. *If the characteristic of K does not divide n, then $E[n]$ has order n^2, and we have $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

Proof. By Proposition 3.2.9(c), we have $\deg([n]) = n^2$, and $\#E[n] = \deg([n])$ since $[n]$ is not divisible by the characteristic of K and therefore separable. Now by decomposing the finite abelian group $E[n]$ into a direct sum of cyclic subgroups and considering that $\#E[d] = d^2$ for each d dividing n, we see that the only possible group structure for $E[n]$ is given by $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

□

Corollary 3.2.11. *For elliptic curves E_1 and E_2 over K, the degree map* $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a positive definite quadratic form.*

Proof. We already know that $\deg(\varphi) \geq 0$ for all $\varphi \in \mathrm{Hom}(E_1, E_2)$ with equality if and only if $\varphi = 0$, and it is clear that $\deg(n\varphi) = n^2 \deg(\varphi)$ from Proposition 3.2.9(c). It remains to prove that $(\varphi, \psi) \mapsto \deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)$ is a bilinear form. To do this, we compute

$$[\deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)] = (\varphi + \psi)^\vee \circ (\varphi + \psi) - \varphi^\vee \circ \varphi - \psi^\vee \circ \psi = \varphi^\vee \circ \psi - \psi^\vee \circ \varphi,$$

which is bilinear (here we have used (a) as well as the additivity given by (b) in Proposition 3.2.9).

□

3.2.3 The endomorphism ring

Following the notation of §3.2.2, for any elliptic curve E, the $\mathbb{Z}$-module $\mathrm{Hom}(E, E)$ clearly has the structure of a ring via composition of elements. We denote this ring by $\mathrm{End}(E)$ and call it the *endomorphism ring* of E. Our goal in this subsection is to investigate the possible structure of this ring. Since each multiplication-by-n map is an endomorphism, there is always a natural inclusion of rings $\mathbb{Z} \subseteq \mathrm{End}(E)$ and we may consider $\mathrm{End}(E)$ as a $\mathbb{Z}$-algebra. In order to find all possible ring structures of $\mathrm{End}(E)$, we recall the following facts that were shown in §3.2.2: (i) there is an anti-involution $(\cdot)^\vee : \mathrm{End}(E) \to \mathrm{End}(E)$ given by $\varphi \mapsto \varphi^\vee$ which preserves addition and reverses the order of multiplication and (ii) $\varphi^\vee\varphi = \varphi\varphi^\vee =: m \in \mathbb{Z}_{\geq 0}$ for any $\varphi \in \mathrm{End}(E)$ with $m = 0$ if and only if $\varphi = 0$. It is also a fact that the $\mathbb{Z}$-rank of $\mathrm{End}(E)$ is ≤ 4, but we will not show this until §3.2.5 (Corollary 3.2.23).

The following lemma is purely a statement in abstract algebra, and we leave it as Exercise 3.3.5.

Lemma 3.2.12. *Suppose that R is a $\mathbb{Z}$-algebra satisfying the following properties:*

(i) as an additive group, R is a free $\mathbb{Z}$-module of rank ≤ 4;

(ii) there is an anti-involution $(\cdot)^\vee : R \to R$ fixing $\mathbb{Z} \subseteq R$ and satisfying $(\varphi + \psi)^\vee = \varphi^\vee + \psi^\vee$, $(\varphi\psi)^\vee = \psi^\vee\varphi^\vee$, and $(\varphi^\vee)^\vee = \varphi$ for all $\varphi, \psi \in R$; and

(iii) $\varphi^\vee\varphi = \varphi\varphi^\vee =: m \in \mathbb{Z}_{\geq 0}$ with $m = 0$ if and only if $\varphi = 0$.

Then we have $R = \mathbb{Z}$; or $R \otimes \mathbb{Q}$ is a quadratic imaginary number field; or $R \otimes \mathbb{Q}$ is a definite quaternion algebra over $\mathbb{Q}$.

Proposition 3.2.13. *Let E be an elliptic curve over a field K. Then the $\mathbb{Z}$-algebra $\mathrm{End}(E)$ either coincides with $\mathbb{Z}$, is an order in an imaginary quadratic number field, or is an order in a definite quaternion algebra. Moreover, if K has characteristic 0, $\mathrm{End}(E)$ must be commutative (and therefore must be $\mathbb{Z}$ or an order in an imaginary quadratic field).*

Proof. The first claim comes from the observations summarized in the discussion above along with Lemma 3.2.12. Now if K has characteristic 0, we may assume $K \subseteq \mathbb{C}$ by the Lefschetz Principle (see Chapter VI, §6 of [8]), and it suffices to show that $\mathrm{End}(E)$ is commutative for any elliptic curve E over $\mathbb{C}$. Indeed, it follows from Proposition 2.5.2 that any endomorphism $\varphi : E \to E$ can be lifted uniquely to a $\mathbb{C}$-linear map $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$ which is an isomorphism if and only if $\varphi \neq 0$. Obviously $\tilde{\varphi}$ is just a homothety $z \mapsto az$ for some $a \in \mathbb{C}$ with $a = 0$ if and only if $\varphi = 0$, so we have an injection $\mathrm{End}(E) \hookrightarrow \mathbb{C}$ and $\mathrm{End}(E)$ is commutative. □

In general, elliptic curves over fields of characteristic 0 have endomorphism rings equal to $\mathbb{Z}$, and it is considered to be exceptional if $\mathrm{End}(E)$ is instead an order in an imaginary quadratic field. In this case, we say that E "has complex multiplication" or is "a CM elliptic curve".

Example 3.2.14. Let E be the elliptic curve over any field K of characteristic different from 2 given by the equation $y^2 = x^3 - x$. Then we check that the map $\varphi : E \to E$ given by $(x, y) \mapsto (-x, iy)$ is an endomorphism of E by noting that it is a morphism with $\varphi(0) = 0$. Now we check that $\varphi^2 : E \to E$, which is given by $(x, y) \mapsto (x, -y)$, is in fact

the map $[-1] : E \to E$. Therefore, we may identify φ with a square root of -1 in the endomorphism ring, and it follows from Proposition 3.2.13 that $\mathrm{End}(E) \cong \mathbb{Z}[i]$ and E has complex multiplication. In fact, it is possible to show that over $\mathbb{C}$, this elliptic curve E is isomorphic to $\mathbb{C}/\langle 1, i\rangle$, from which it is apparent that the endomorphism ring is identified with the ring of homotheties $\mathbb{Z}[i] \subset \mathbb{C}$.

3.2.4 The endomorphism ring in positive characteristic

For this subsection, we assume that E is an elliptic curve defined over a field K of characteristic $p \geq 3$. For simplicity, we will assume that K is perfect, although most of the below results would hold anyway with slight modifications. Our main goal is to investigate the possible structures of $\mathrm{End}(E)$ in this case. First it is essential to define the Frobenius isogeny.

Definition 3.2.15. *For any integer $r \geq 0$, let $E^{(r)}$ be the elliptic curve defined over K by the equation given by raising all the coefficients of the equation defining E to the p^rth power. Then the (rth power) **Frobenius isogeny** $\mathrm{Fr}^r : E \to E^{(r)}$ is the map given by $(x, y) \mapsto (x^{p^r}, y^{p^r})$. In the case that $K = \mathbb{F}_{p^r}$, we have $E = E^{(r)}$ and $\mathrm{Fr}^r \in \mathrm{End}(E)$ is called the **Frobenius endomorphism**.*

Note that each Fr^r is obviously a nonconstant morphism with $\mathrm{Fr}^r(0) = 0$ and therefore an isogeny; moreover, as the notation suggests, each Fr^r is the rth power of the Frobenius map $\mathrm{Fr} := \mathrm{Fr}^1 : E \to E^{(1)}$. It is clear that each Frobenius isogeny Fr^r is purely inseparable of degree p^r from checking that $(\mathrm{Fr}^r)^* : K(E^{(r)}) \to K(E)$ is the inclusion $K(E)^{p^r} \hookrightarrow K(E)$. It is also clear from basic field theory that if E' is another elliptic curve over K, then every isogeny $\varphi : E \to E'$ factors as the composition of the purely inseparable map $\mathrm{Fr}^r : E \to E^{(r)}$ for some $r \geq 0$ and a separable map $\varphi^{\mathrm{sep}} : E^{(r)} \to E'$. In other words, Fr^r is the inseparable part φ^{insep} of φ.

The next result functions as a lemma both to Proposition 3.2.9 above (it almost immediately implies the statement of part (d) for the inseparable case) and to Proposition 3.2.17 below.

Lemma 3.2.16. *The multiplication-by-p map $[p] : E \to E$ is inseparable, and there exists an isogeny $\varphi' : E^{(1)} \to E$ such that $\varphi' \circ \mathrm{Fr} = \mathrm{Fr} \circ \varphi' = [p]$.*

Proof. It can be shown either through direct computations or through an abstract argument using functoriality that for any elliptic curve over a field of any characteristic, if $\omega \in \Omega(E)$ is a holomorphic differential, we have $[n]^*(\omega) = n\omega$ for $n \geq \mathbb{Z}$. It follows that since K has characteristic p, we have $[p]^*(\omega) = 0$, and therefore, $[p] : E \to E$ is inseparable. By the above discussion, we much have $[p] = [p]^{\mathrm{sep}} \circ \mathrm{Fr}^r$ for some $r \geq 1$ and some separable map $[p]^{\mathrm{sep}} : E^{(r)} \to E$. The claim then follows by taking $\varphi' = [p]^{\mathrm{sep}} \circ \mathrm{Fr}_{r-1}$.

□

One can see from the proof of Proposition 3.2.9(d) that the isogeny φ' above is the dual isogeny $\mathrm{Fr}^\vee$. Our main tool in proving the following proposition will be studying this dual isogeny.

Proposition 3.2.17. *a) The following are equivalent:*

i) $E[p^r] = 0$ *for any (every)* $r \geq 1$ *(i.e. the map* $[p] : E \to E$ *is purely inseparable);*

ii) $\mathrm{Fr}^\vee$ *is (purely) inseparable;*

iii) $j(E) \in \mathbb{F}_{p^2}$*;*

iv) $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

b) If the above equivalent conditions do not hold, then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ *for all* $r \geq 0$*, and if* $j(E) \cong \bar{\mathbb{F}}_p$*, then* $\mathrm{End}(E)$ *is an order in an imaginary quadratic field.*

Remark 3.2.18. If the equivalent conditions in part (a) above do not hold and $j(E)$ is transcendental over $\mathbb{F}_p$, then it is possible to show that in fact $\mathrm{End}(E) = \mathbb{Z}$.

Proof. We first show that (i) and (ii) are equivalent. It is immediately clear that $E[p] = 0$ implies that $E[p^r] = 0$ for every $r \geq 1$. Now Lemma 3.2.16 and the discussion below it show that $[p] : E \to E$ factors as the composition $\mathrm{Fr}^\vee \circ \mathrm{Fr}$. Note that Fr obviously has degree p and so $\mathrm{Fr}^\vee$ also has degree p by Proposition 3.2.9(d). Moreover, the kernel of Fr is trivial since Fr is purely inseparable, so the kernel of $[p]$ is trivial if and only if $\mathrm{Fr}^\vee$ is also purely inseparable.

Now we show that (ii) implies (iii). Assume that $\mathrm{Fr}^\vee$ is inseparable. Then the inseparable part of $\mathrm{Fr}^\vee$ is some power of the Frobebius map $\mathrm{Fr} : E^{(1)} \to E^{(2)}$. By comparing degrees, we see that the inseparable part of $\mathrm{Fr}^\vee$ is this Frobenius map, while the separable part is an isomorphism $E^{(2)} \xrightarrow{\sim} E$. We note from the formula for the j-invariant that $j(E^{(2)}) = j(E)^{p^2}$. But $j(E) = j(E^{(2)})$ by Proposition 3.2.2(b), so $j(E) = j(E)^{p^2}$ and it follows that $j(E) \in \mathbb{F}_{p^2}$.

Now assume that $j(E) \in \mathbb{F}_{p^2}$, and we will show (iv) by assuming that $\mathrm{End}(E)$ is commutative and deriving a contradiction. If $\mathrm{End}(E)$ is commutative, then by Proposition 3.2.13 we have that either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is an order in an imaginary quadratic field. One can show that for any elliptic curve E' which is isogenous to E, we have $\mathrm{End}(E') \otimes \mathbb{Q} = \mathrm{End}(E) \otimes \mathbb{Q}$ (see Exercise 3.3.6). Moreover, we observe that for any such E', the map $[p] : E' \to E'$ is also purely inseparable and so we get $j(E') \in \mathbb{F}_{p^2}$. This implies (using Proposition 3.2.2(b) and the fact that $\mathbb{F}_{p^2}$ is finite) that there are only finitely many isomorphism classes of elliptic curves over $\bar{K}$ which are isogenous to E.

We claim that there exists a prime integer ℓ such that the ideal (ℓ) remains prime in $\mathrm{End}(E')$ for every elliptic curve E' isogenous to E. If $\mathrm{End}(E) = \mathbb{Z}$, then each $\mathrm{End}(E')$ is also $\mathbb{Z}$ and then the claim is trivial (we can take any ℓ). If $\mathrm{End}(E)$ is an order in an imaginary quadratic field, then each $\mathrm{End}(E')$ is an order in that same imaginary quadratic field. Then it is an elementary exercise in algebraic number theory to show that there always exists a prime integer ℓ such that (ℓ) is a prime ideal in all of a given finite set of orders in a fixed imaginary quadratic field. Note that this ℓ is different from p, since (p) decomposes in $\mathrm{End}(E)$ as $(\mathrm{Fr}^\vee)(\mathrm{Fr})$.

Choose such a prime ℓ, and note from Corollary 3.2.10 that $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. Thus, we may choose a sequence of subgroups $0 = N_0 \subset N_1 \subset N_2 \subset ... \subset E(\bar{K})$ with $N_i \cong \mathbb{Z}/\ell^i\mathbb{Z}$ for $i \geq 0$, with none of these subgroups containing $E[\ell^r]$ for any $r \geq 1$. By Proposition 3.2.6, we see that this sequence of subgroups corresponds to a sequence of isogenies

$$E = E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} ...$$

with $E_i \cong E/N_i$ and $\ker(\varphi_i) \cong N_i/N_{i-1}$ for each $i \geq 0$. But as was observed above, there are only finitely many elliptic curves isogenous to E up to isomorphism, so for some $i, j \geq 1$ we

have $E_{i+j} \cong E_i$ and so the composition $\varphi_{i+j} \circ \ldots \circ \varphi_{i+1} : E_i \to E_{i+j} \cong E_i$ is an endomorphism $\psi \in \mathrm{End}(E_i)$ with kernel isomorphic to N_{i+j}/N_i. Since $\deg(\psi) = \ell^j$ and (ℓ) is prime in $\mathrm{End}(E')$, we have that j is even and ψ is the composition of $[\ell^{j/2}]$ with some isomorphism. But this implies that $E[\ell^{j/2}] \subseteq N_{i+j}$, a contradiction.

We finish the proof of (a) by showing that (iv) implies (ii). To do this, we assume that (ii) is false (i.e. $\mathrm{Fr}^\vee$ is separable) and show that then (iv) is false (i.e. $\mathrm{End}(E)$ is commutative). Indeed, since $\mathrm{Fr}^\vee$ is separable and has order p while Fr is purely inseparable, we have $\#E[p^r] = \#\ker((\mathrm{Fr}^\vee)^r) \cdot \#\ker(\mathrm{Fr}^r) = p^r$ for any $r \geq 0$. By a similar argument to the one used in the proof of Corollary 3.2.10, we see that the only possible group structure for $E[p^r]$ is given by $\mathbb{Z}/p^r\mathbb{Z}$.

We now claim that for any nonzero endomorphism $\varphi \in \mathrm{End}(E)$, there is some $r \geq 1$ such that $\varphi(E[p^r]) \neq 0$. Indeed, since φ has finite kernel, we get $\varphi(E[p^r]) \neq 0$ for any r such that $p^r > \#\ker(\varphi)$. It follows that the obvious map from $\mathrm{End}(E)$ to the ring of $\mathbb{Z}_p$-endomorphisms of $\varprojlim_r E[p^r]$ is injective. (Here $\mathbb{Z}_p$ denotes the ring of p-adic integers, while the inverse limit above is taken with respect to multiplication-by-p maps $E[p^r] \to E[p^{r-1}]$ and is obviously a $\mathbb{Z}_p$-module.) But since $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$, we have $\varprojlim_r E[p^r] \cong \mathbb{Z}_p$ and so $\mathrm{End}_{\mathbb{Z}_p}(\varprojlim_r E[p^r]) \cong \mathbb{Z}_p$ is commutative, so $\mathrm{End}(E)$ is commutative.

To prove (b), we assume that the equivalent conditions in (a) do not hold. It was already shown above that then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for $r \geq 0$. Now we assume in addition that $j(E) \in \bar{\mathbb{F}}_p$ and proceed to show that $\mathrm{End}(E) \supsetneq \mathbb{Z}$. Clearly there is some $r \geq 1$ such that $j(E) \in \mathbb{F}_{p^r}$, and so it follows from Proposition 3.2.2(c) that we may assume that E is defined over $\mathbb{F}_{p^r}$. Then we have the Frobenius endomorphism $\mathrm{Fr}^r \in \mathrm{End}(E)$. Suppose that $\mathrm{Fr}^r = [n] \in \mathbb{Z}$. Then since $\deg(\mathrm{Fr}^r) = \deg(\mathrm{Fr}^r) = p^r$, we have that r is even and $n = \pm p^{r/2}$. Since Fr is purely inseparable, this implies that $[p^{r/2}]$ and hence also $[p]$ are purely inseparable, which contradicts condition (i) of (a). Therefore, $\mathrm{Fr}^r \notin \mathbb{Z}$ and $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

□

The fact that any elliptic curve E satisfying the equivalent conditions in part (a) of the above proposition must have $j(E) \in \mathbb{F}_{p^r}$ suggests that such elliptic curves are rather exceptional (since $\mathbb{F}_{p^r}$ is a small subfield of any algebraically closed field of characteristic $p > 0$). This is reflected in the terminology defined as follows.

Definition 3.2.19. *If E is an elliptic curve over a field of charaacteristic $p > 0$, then E is said to be **supersingular** if E satisfies the equivalent conditions in Proposition 3.2.17(a) and is said to be **ordinary** otherwise.*

We end by noting that the notion of supersingularity has nothing to do with singularities in the context of algebraic geometry (after all, every elliptic curve is nonsingular). This potentially confusing terminology came about because the word *singular* was commonly used to mean "unusual" or "special".

3.2.5 The Tate module

In the proof of Proposition 3.2.17(b) we made use of the inverse limit of the groups $E[p^n]$ for an elliptic curve E over a field of characteristic $p > 0$. This was a particular case of an important object associated to any elliptic curve E (over any field) for each prime integer ℓ.

Definition 3.2.20. *Let E be an elliptic curve and let ℓ be a prime integer. Then the* ***ℓ-adic Tate module*** *of E is the group given by the inverse limit $T_\ell(E) := \lim_{\leftarrow r} E[\ell^r]$, where the limit is taken with respect to the multiplication-by-ℓ maps $E[\ell^r] \to E[\ell^{r-1}]$.*

The ℓ-adic Tate module earns its name by being a module in two different senses. First of all, since each $E[\ell^r]$ is a free $\mathbb{Z}/\ell^r\mathbb{Z}$-module by Corollary 3.2.10 and Proposition 3.2.17, it is clear that $T_\ell(E)$ is a free module over the inverse limit of the rings $\mathbb{Z}/\ell^r\mathbb{Z}$ with respect to the multiplication-by-ℓ map $\mathbb{Z}/\ell^r\mathbb{Z} \to \mathbb{Z}/\ell^{r-1}\mathbb{Z}$. This inverse limit is the ring of ℓ-adic integers, denoted $\mathbb{Z}_\ell$, which can also be constructed as the completion of $\mathbb{Z}$ with respect to the ℓ-adic metric. Thus, $T_\ell(E)$ is always a free $\mathbb{Z}_\ell$-module whose structure is described in the following proposition.

Proposition 3.2.21. *Let E be an elliptic curve over a field of characteristic $p \geq 0$, and let ℓ be a prime integer. Then as a $\mathbb{Z}_\ell$-module, $T_\ell(E) \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$ if $\ell \neq p$. If $p > 0$, then we have $T_p(E) \cong \mathbb{Z}_p$ if E is ordinary and $T_p(E) = 0$ if E is supersingular.*

Proof. This follows immediately from the facts that, for $r \geq 0$, we have $E[\ell^r] \cong \mathbb{Z}/\ell^r\mathbb{Z} \oplus \mathbb{Z}/\ell^r\mathbb{Z}$ if $\ell \neq p$ by Corollary 3.2.10 and that if $p > 0$, we have $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ if E is ordinary and $E[p^r] = 0$ if E is supersingular by Proposition 3.2.17.

□

Tate modules of elliptic curves are also modules in another sense. Note that if E is defined over a field K, the map $[\ell] : E \to E$ is defined over K and therefore, the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ acts on each $\mathbb{Z}/\ell^r\mathbb{Z}$-module $E[\ell^r]$ (see Exercise 3.3.3(a)) and is compatible with the multiplication-by-ℓ maps $E[\ell^r] \to E[\ell^{r-1}]$. It follows that $\mathrm{Gal}(\bar{K}/K)$ acts on the $\mathbb{Z}_\ell$-module $T_\ell(E)$. Therefore, $T_\ell(E)$ may be considered as a Galois module, and it provides us with a rank-2 ℓ-adic Galois representation associated to the elliptic curve E (or, one can think of this as a representation of the Galois group on the 2-dimensional $\mathbb{Q}_\ell$-vector space $T_\ell(E) \otimes \mathbb{Q}_\ell$).

As one immediate use of the Tate module, we may finally prove our assertion about $\mathrm{End}(E)$ having $\mathbb{Z}$-rank ≤ 4 which was given at the beginning of §3.2.3. Note that any isogeny of elliptic curves $E_1 \to E_2$ takes each group $E_1[\ell^r]$ to $E_2[\ell^r]$ and therefore induces a homomorphism of $\mathbb{Z}_\ell$-modules $T_\ell(E_1) \to T_\ell(E_2)$. This gives us a homomorphism of $\mathbb{Z}_\ell$-modules $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$. We need the following proposition, which can be proven in a fairly elementary and straightforward manner (Exercise 3.3.9).

Proposition 3.2.22. *The above homomorphism $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ is injective.*

Corollary 3.2.23. *For elliptic curves E_1 and E_2, the free $\mathbb{Z}$-module $\mathrm{Hom}(E_1, E_2)$ has $\mathbb{Z}$-rank ≤ 4. In particular the endomorphism ring of any elliptic curve has $\mathbb{Z}$-rank ≤ 4.*

Proof. Note that since $T_\ell(E_1)$ and $T_\ell(E_2)$ are each free $\mathbb{Z}_\ell$-modules of rank ≤ 2, the $\mathbb{Z}_\ell$-module $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ has rank ≤ 4. Since $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ injects into this, we see that $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ also has rank ≤ 4 and therefore, the free $\mathbb{Z}$-module $\mathrm{Hom}(E_1, E_2)$ has rank ≤ 4.

□

We close with the following remarks. For elliptic curves E_1 and E_2 over a field K, let $\mathrm{Hom}_K(E_1, E_2) \subseteq \mathrm{Hom}(E_1, E_2)$ denote the subset of maps which are defined over K. Then clearly $\mathrm{Hom}_K(E_1, E_2)$ is a free $\mathbb{Z}$-submodule of $\mathrm{Hom}(E_1, E_2)$, and elements of $\mathrm{Hom}_K(E_1, E_2)$ commute with Galois automorphisms in $\mathrm{Gal}(\bar{K}/K)$. Moreover, the image of $\mathrm{End}_K(E_1, E_2) \otimes \mathbb{Z}_\ell$ in $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ is contained in the $\mathbb{Z}_\ell$-submodule $\mathrm{Hom}_{\mathrm{Gal}(\bar{K}/K)}(T_\ell(E_1), T_\ell(E_2))$ consisting of all $\mathbb{Z}_\ell$-homomorphisms which are compatible with the actions of Galois on $T_\ell(E_1)$ and $T_\ell(E_2)$. We therefore have a map

$$\mathrm{Hom}_K(E_1, E_2) \to \mathrm{Hom}_{\mathrm{Gal}(\bar{K}/K)}(T_\ell(E_1), T_\ell(E_2)).$$

It follows from Proposition 3.2.22 that this map is injective. It was suspected that this map is in fact an isomorphism for many fields K (and not just for elliptic curves but for abelian varieties of any dimension) – these are known as the Tate Conjectures. These conjectures are quite powerful: they suggest that one is able to determine all isogenies between any two abelian varieties of the same dimension by understanding the Galois actions on the associated ℓ-adic Tate modules and determining using linear algebra which $\mathbb{Z}_\ell$-linear maps commute with them. Eventually this was proven for the case that K is a finite field by John Tate, for the case that K is a function field over a finite field by Yuri Zarhin, and finally for the case that K is a number field by Gerd Faltings.

3.3 Exercises

For all of the following exercises, we retain the assumption that K is not a field of characteristic 2.

Exercise 3.3.1. Let C_1 and C_2 be smooth curves of genus g_1 and g_2 respectively and $\varphi : C_1 \to C_2$ is a nonconstant separable morphism of degree d, and assume that the characteristic of K doesn't divide any of the ramification indices. Recall the Hurwitz Formula

$$2g_1 - 2 = d(2g_2 - 2) + \sum_{P \in C_1(\bar{K})} (e_P - 1),$$

where e_P is the ramification index of φ at the point P (note that this is equal to 1 for all but finitely many $P \in C_1(\bar{K})$).

a) Suppose that C_1 is an elliptic curve. Show that C_2 can also be given the structure of an elliptic curve if and only if φ is unramified eveerywhere.

b) Show that every elliptic curve E over K has a degree-2 morphism $\varphi : E \to \mathbb{P}^1_K$ which is ramified at exactly 4 points. Show furthermore that these four points are the elements of the 2-torsion subgroup $E[2]$.

c) Prove the converse statement that if $\varphi : C \to \mathbb{P}^1_K$ is a morphism of degree 2 which is ramified at exactly 4 points, then C is isomorphic over $\bar{K}$ to an elliptic curve E over K such that these four ramification points correspond to the elements of $E[2]$. (Hint: choose one of the ramification points to be the distinguished point $O \in E(K)$ and study the only nontrivial automorphism $\iota : C \to C$ satisfying $\varphi \circ \iota = \varphi$. It might be easier to assume that K does not have characteristic 3, which allows us to reduce the cubic polynomial defining E by getting rid of the x^2-term.)

Exercise 3.3.2. Prove that each multiplication-by-n map is an isogeny. To do this, refer to Exercise 1.2.3, or perhaps the above exercise instead, which shows that the 2-torsion subgroup $E[2]$ is finite.

Exercise 3.3.3. Let E is an elliptic curve over K given by an equation of the form $y^2 = f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ for distinct $\alpha_1, \alpha_2, \alpha_3 \in \bar{K}$. For $n \geq 1$, write $K(E[n])$ for the (algebraic) extension generated over K by coordinates of all of the points in $E[n] \subset E(\bar{K})$.

a) Show that elements of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ permute the points in each $E[n]$. Conclude that each field extension $K(E[n])/K$ is Galois.

b) Show that $K(E[2]) = K(\alpha_1, \alpha_2, \alpha_3)$, so that the Galois group of the extension $K(E[2])/K$ is canonically isomorphic to the Galois group of the cubic polynomial $f \in K[x]$.

c) Compute $K(E[4]) = K(\alpha_1, \alpha_2, \alpha_3, \sqrt{\alpha_1 - \alpha_2}, \sqrt{\alpha_1 - \alpha_3}, \sqrt{\alpha_2 - \alpha_3})$. (This is difficult but can be proven either by direct computations using doubling formulas, by directly considering divisor classes in $\mathrm{Pic}^0(E)$, or by formulas for computing 2-descent given in section X.1 of [8]. For formulas for generators of $K(E[8])/K$, see §2.5 of my dissertation!)

Exercise 3.3.4. Let $\beta, \gamma \in \bar{K}$ be distinct and nonzero and consider the elliptic curves E and E' over $\bar{K}$ given by the following Weierstrass equations:

$$E : y^2 = x(x-\beta)(x-\gamma), \qquad E' : y^2 = x^3 + 2(\beta+\gamma)x^2 + (\beta-\gamma)^2 x.$$

Let $\varphi : E \to E'$ be the morphism over K given by $(x, y) \mapsto (\frac{y^2}{x^2}, y(\frac{\beta\gamma}{x^2} - 1))$.

a) Show that φ is an isogeny of degree 2 whose kernel is cyclically generated by $(0, 0) \in E[2]$.

b) Define the elliptic curve E'' and the isogeny $\varphi' : E' \to E''$ in the same way that E' and φ were defined respectively, except with respect to $\beta' := -(\beta+\gamma) + 2\sqrt{\beta\gamma}$ and $\gamma' := -(\beta+\gamma) - 2\sqrt{\beta\gamma}$. Check that the kernel of $\varphi' \circ \varphi$ is $E[2]$ and that there is an isomorphism $E'' \xrightarrow{\sim} E$ defined over K. Conclude that this isomorphism composed with φ' is the dual isogeny $\varphi^\vee$ (at least up to an automorphism of E).

c) Use these formulas to construct an elliptic curve E over $\mathbb{Q}$ with $\mathrm{End}(E) \cong \mathbb{Z}[\sqrt{-2}]$.

Exercise 3.3.5. Prove Lemma 3.2.12 (this is a lengthy but elementary algebraic argument). As an immediate corollary, show that if $\mathrm{End}(E)$ is commutative, then the dual of any endomorphism $\varphi \in \mathrm{End}(E)$ is its complex conjugate.

Exercise 3.3.6. If $\varphi : E_1 \to E_2$ is an isogeny of elliptic curves, show that there is a canonical $\mathbb{Q}$-algebra isomorphism $\mathrm{End}(E_1) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{End}(E_2) \otimes \mathbb{Q}$. (Hint: use the dual isogeny.)

Exercise 3.3.7. Assume for this exercise that K doesn't have characteristic 3.

a) Prove that the automorphism group $\mathrm{Aut}(E)$ of an elliptic curve E over K is always finite and cyclic and of order 2, 4, or 6. Show that there is only one elliptic curve E up to isomorphism with $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$ and show the same for $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$. (Hint: refer to the proof of Proposition 3.2.2(c).)

b) Note that the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ acts on $\mathrm{Aut}(E)$. Show that as a $\mathrm{Gal}(\bar{K}/K)$-module, $\mathrm{Aut}(E)$ is isomorphic to the multiplicative group $\langle \zeta_d \rangle \subset K^\times$ where d is its order and ζ_d is a primitive dth root of unity. Check that we have $\varphi^\vee = \varphi^{-1}$ for any $\varphi \in \mathrm{Aut}(E)$.

Exercise 3.3.8. Let E be an elliptic curve over a finite field $\mathbb{F}_{p^r}$. Clearly the group $E(\mathbb{F}_{p^r})$ is finite, and it is natural to ask how large it is. The purpose of this exercise is to prove the *Hasse Bound*, which says

$$|\#E(\mathbb{F}_{p^r}) - p^r - 1| \leq 2p^{r/2}.$$

You may assume without proof that the endomorphism $\mathrm{Fr}^r - 1 \in \mathrm{End}(E)$ is separable (but this can be proven by direct computation using the invariant differential).

a) Show that $\#E(\mathbb{F}_{p^r}) = \deg(\mathrm{Fr}^r - 1)$.

b) Verify using Corollary 3.2.11 that for any endomorphisms $\varphi, \psi \in \mathrm{End}(E)$, we have $|\deg(\varphi - \psi) - \deg(\varphi) - \deg(\psi)| \leq 2\sqrt{\deg(\varphi)\deg(\psi)}$.

c) Conclude that the Hasse Bound holds.

Exercise 3.3.9. Prove Proposition 3.2.22. (This is quite long and tricky but requires no new concepts. The first key step is to define, for any finitely generated subgroup $M \subseteq \mathrm{Hom}(E_1, E_2)$, the larger subgroup M^{div} consisting of all $\varphi \in \mathrm{Hom}(E_1, E_2)$ with $[m] \circ \varphi \in M$ for some integer $m \geq 1$, and to show using a little topology that M^{div} is also finitely generated.)

Bibliography

[1] Irwin Kra and Hershel M. Farkas. *Riemann surfaces. Graduate Texts in Mathematics*, 71, 1995.

[2] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89. Springer Science & Business Media, 2012.

[3] James S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer, 1986.

[4] James S. Milne. Jacobian varieties. In *Arithmetic geometry*, pages 167–212. Springer, 1986.

[5] David Mumford. *Abelian varieties*, volume 108. Oxford Univ Press, 1974.

[6] David Mumford. *Tata lectures on theta II. Progress in Mathematics*, 43, 1984.

[7] Michael Rosen. Abelian varieties over $\mathbf{C}$. In *Arithmetic geometry*, pages 79–101. Springer, 1986.

[8] Joseph H. Silverman. *The arithmetic of elliptic curves. Graduate Texts in Mathematics*, 106, 2009.