Elliptic Curves and Complex Abelian Varieties

Jeffrey Yelton

March 15, 2019

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* ([4]) as well as Michael Rosen's and James Milne's articles on abelian varieties in the book *Arithmetic Geometry* edited by Cornell and Silverman ([6] 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 **??**, more or less everything came from Silverman's (first) book *The Arithmetic of Elliptic Curves* ([7]).

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 [4] 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" here 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 $\mathbb{A}_K \smallsetminus \{0\}$ 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 $E \smallsetminus \{O\}$, 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. For any algebraic extension K' of K the set of points $E(K')$ 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 $K' \supseteq K$, $E(K')$ 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 $E(\bar{\mathbb{Q}}) \smallsetminus \{(0,0)\}$. 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 Outline of these notes

We want to relate the three definitions given above for elliptic curves by studying the more general objects known as abelian varieties. We will show that an abelian variety of dimension 1 has to be a curve with the properties given in Definition 1.1.3 and also 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 Chapter 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 (in §2.6), 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 Chapter **??**) 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 along with their endomorphism rings (in §**??**), and we will end by introducing the Tate module (in §**??**).

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), although many connected compact complex Lie groups of dimension ≥ 2 cannot be given an algebraic structure and therefore are *not* abelian varieties. Our most important result (Theorem 2.3.6) 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 $1 \in T_0\mathbb{C}$ to $v \in T_eX$. 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 (Cartier divisors)**.** *Let Y be a connected complex manifold.*

a) The (additive) group $\mathrm{Div}(Y)$ *of "local function data" on Y is defined as follows. A "local function datum" is given by $D = \{\{U_i\}_{i\in I}, \{f_i\}_{i\in I}\}$, where $\{U_i\}_{i\in I}$ is a finite open cover of Y and, for each $i \in I$, f_i is a nonzero 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 $D_2 = (\{V_j\}_{j\in J}, \{g_j\}_{j\in J})$ 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 "local function datum" $(\{U_i\}_{i\in I}, \{f_i\}_{i\in I})$ defined in this way is said to be ***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.*

c) The group of (Cartier) divisors on Y, denoted $\mathrm{Div}(Y)$*, is defined to be the group equivalence classes of "local function data" on Y modulo trivial elements. 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. It is an easy exercise to check that the property of effectivity is well-defined for elements of* $\mathrm{Div}(Y)$*.*

d) 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.*

There is a very straightforward way to define pullbacks of divisors via surjective 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 the complex tori which can be embedded into projective space as algebraic varieties, it will be necessary to study positive divisors on them. It would be nice

to be able to characterize positive divisors on a complex torus X as principal divisors, since then our investigation would boil down to considering the set of holomorphic functions on X. But unfortunately, since such an 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 $\pi : V \to V/\Lambda = X$ to get a divisor on V, and it turns out that the resulting divisor is principal by the following classical result.

Theorem 2.2.3 (Cousins)**.** *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. (I like to say that such a function is "almost periodic" with respect to Λ; it is only actually periodic if $(f) = \pi^* D$ with $D \in \mathrm{Prin}(X)$.) 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 if a function $H : V \times V \to \mathbb{C}$ is a Hermitian form, 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 $H(v,w) = E(iv,w) + iE(v,w)$. **In light of this, from now on, in any context where we have a Hermitian form H, we will use E to denote its imaginary part, and conversely, whenever we have an alternating $\mathbb{R}$-bilinear form E, we will denote the corresponding Hermitian form by H.**

Definition 2.2.5. *A **theta function** (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. Given a Hermitian form $H : V \times V \to \mathbb{C}$, we say that such a function θ is a **theta function for** H if we have $E(\lambda_1, \lambda_2) = L(\lambda_1, \lambda_2) - L(\lambda_2, \lambda_1)$ for $\lambda_1, \lambda_2 \in \Lambda$.*

Note that the set of all theta functions on V with respect to Λ forms a group under multiplication, and that in fact, the map from this group to the group of divisors $\mathrm{Div}(X)$ defined by sending a theta function θ to the divisor $D \in \mathrm{Div}(X)$ such that $(\theta) = \pi^* D$ is a group homomorphism which we denote by

$$\mathrm{div} : \{\text{theta functions on } V \text{ w.r.t. } \Lambda\} \longrightarrow \mathrm{Div}(X).$$

Its kernel is the subgroup of *trivial theta divisors*, i.e. theta divisors θ which are holomorphic and nonvanishing on V.

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 [4]).

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, or equivalently, the map $\mathrm{div} : \{\text{theta functions}\} \to \mathrm{Div}(X)$ is surjective. Now 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

$$L(v, \lambda_1 + \lambda_2) - L(v, \lambda_1) - L(v, \lambda_2) = 0 \quad (2.4)$$

(here we get equality instead of equivalence modulo $\mathbb{Z}$ because it holds when $v = 0$ and therefore holds for all v by continuity) and

$$J(\lambda_1 + \lambda_2) - J(\lambda_1) - J(\lambda_2) \equiv L(\lambda_1, \lambda_2) \pmod{\mathbb{Z}}. \quad (2.5)$$

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 a tricky but elementary 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 $H(v, w) = E(iv, w) + iE(v, w)$.

We now have a well-defined map from the multiplicative group of theta divisors on V (with repsect to Λ) to the additive group of Hermitian forms on V which is clearly a group homomorphism; we denote it by

$$\mathcal{H} : \{\text{theta functions on } V \text{ w.r.t. } \Lambda\} \longrightarrow \{\text{Hermitian forms on } V \text{ w.r.t. } \Lambda\}.$$

We will now show that its kernel also coincides with the subgroup of trivial theta functions. 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 the zero form.

It follows that the map $\mathcal{H}$ factors through a map

$$\{\text{theta functions}\}/\{\text{trivial theta functions}\} \cong \mathrm{Div}(X) \longrightarrow \{\text{Hermitian forms}\},$$

thus showing that each divisor $D \in \mathrm{Div}(X)$ uniquely determines a Hermitian form H.

□

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 2.2.7. *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 $\Lambda \times \Lambda$.*

Proposition 2.2.8. *Let $H : V \times V \to \mathbb{C}$ be the Riemann form associated to some divisor $D \in \mathrm{Div}(X)$ via Proposition 2.2.6. Then there exists a theta function for H, and any theta function $\theta \in \mathcal{M}(V)$ for H 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*

$$\theta_D(v+\lambda)/\theta_D(v) = e^{2\pi i(\frac{1}{2i}H(v,\lambda)+\frac{1}{4i}\pi H(\lambda,\lambda)+K(\lambda))},$$

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. We first have to show that a function θ_D with the property given in the statement is a theta function for H. This follows from verifying that $L_0(v,\lambda) := \frac{1}{2i}H(v,\lambda)$ satisfies $L_0(\lambda_1,\lambda_2) - L_0(\lambda_2-\lambda_1) = \frac{1}{2i}(H(\lambda_1,\lambda_2) - \overline{H(\lambda_2,\lambda_1)}) = E(\lambda_1,\lambda_2)$.

Now we show that such a function θ_D exists. We know from Proposition 2.2.6 that there exists a theta function θ satisfying $\theta(v+\lambda)/\theta(v) = e^{2\pi i(L(v,\lambda)+J(\lambda))}$ where L is $\mathbb{C}$-linear in the first variable and satisfies $L(\lambda_1,\lambda_2) - L(\lambda_2,\lambda_1) = E(\lambda_1,\lambda_2)$. Then $M := L - L_0$ restricted to $\Lambda \times \Lambda$ is a symmetric $\mathbb{Z}$-bilinear form which can be extended $\mathbb{R}$-linearly to a symmetric $\mathbb{R}$-bilinear form $M : V \times V \to \mathbb{C}$ (actually $\mathbb{C}$-bilinear because L and L_0 are $\mathbb{C}$-bilinear in the first argument). Then $h_1(v) := e^{2\pi i(\frac{1}{2}L(v,v))}$ is clearly a trivial theta function (see the proof of Proposition 2.2.6), and replacing θ by $\theta/h_1(v)$ allows us to replace L by $L_0 = \frac{1}{2i}H$ in our expression for $\theta(v+\lambda)/\theta(v)$. Now the relation (2.5) says that $J(\lambda_1+\lambda_2) - J(\lambda_1) - J(\lambda_2) \equiv \frac{1}{2i}H(\lambda_1,\lambda_2) \pmod{\mathbb{Z}}$ for $\lambda_1, \lambda_2 \in \Lambda$. Setting $K(\lambda) = J(\lambda) - \frac{1}{4i}H(\lambda,\lambda)$, we get

$$K(\lambda_1+\lambda_2) - K(\lambda_1) - K(\lambda_2) \equiv \frac{1}{2i}H(\lambda_1,\lambda_2) - \frac{1}{2i}\Re H(\lambda_1,\lambda_2) = \frac{1}{2i}E(i\lambda_1,\lambda_2) \pmod{\mathbb{Z}}. \quad (2.6)$$

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 $h_2(v) := e^{\Im K(iv)+i\Im K(v)}$, we may assume that K is takes values in $\mathbb{R}$ without affecting $K(\lambda_1 + \lambda_2) - K(\lambda_1) - K(\lambda_2)$, 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 $\mathbb{R}$.

□

We call a theta function satisfying the properties in the statement of the above proposition a *normalized theta function* for the divisor D.

Proposition 2.2.8 tells us in particular that the image of the map $\mathcal{H}$ defined earlier is contained in the additive group of Riemann forms, so that we have group homomorphisms

$$\{\text{theta functions w.r.t. } \Lambda\}/\{\text{trivial theta functions}\} \xrightarrow{\sim} \mathrm{Div}(X) \to \{\text{Riemann forms w.r.t. } \Lambda\}.$$

Lemma 2.3.4(a) below tells us that the second map is in fact also an isomorphism. We shall describe the kernel of the above maps to the group of Riemann forms in §2.5.

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 θ_0 be a theta function whose divisor is π^*D. We define $\mathcal{L}(\theta_0)$ denote the set of all holomorphic functions $\theta \in \mathcal{M}(V)$ which have the same "translation functions" as θ_0 has, i.e. $\theta(v + \lambda)/\theta(v) = \theta_0(v + \lambda)/\theta_0(v)$ (by convention, $0 \in \mathcal{L}(\theta_0)$). It is clear that $\mathcal{L}(\theta_0)$ is also a vector space. In fact, it is easy to see from the definitions that we have an isomorphism $\mathcal{L}(\theta_0) \xrightarrow{\sim} \mathcal{L}(D)$ given by $\theta \mapsto \theta/\theta_0$.

Below we again let θ_D denote a normalized theta function for D as given by Proposition 2.2.8, although it is clear that the statements hold when θ_D is replaced by any θ_0 with the same translation functions.

Definition 2.3.1. *A divisor $D \in \mathrm{Div}(X)$ is **very ample** if there exists a basis $\{\theta_0, ..., \theta_m\}$ of $\mathcal{L}(\theta_D)$ such that the map $\Theta : X \to \mathbb{P}^m_{\mathbb{C}}$ induced by the map $X \to \mathbb{P}^m_{\mathbb{C}}$ given by $v \mapsto (\theta_0(v) : ... : \theta_m(v))$ is an embedding of X into $\mathbb{P}^m_{\mathbb{C}}$; i.e. if we have the following:*

i) Θ is well-defined; that is, we do not have $\theta_0(v) = ... = \theta_m(v) = 0$ for any $v \in V$;

ii) $\Theta : X \to \mathbb{P}^m_{\mathbb{C}}$ is an injection; and

iii) The induced maps on tangent spaces $\Theta_* : T_aX \to T_{\Theta(a)}\mathbb{P}^m_{\mathbb{C}}$ are injections.

*A divisor $D \in \mathrm{Div}(X)$ is **ample** if there is an integer $n \geq 1$ such that nD is very ample.*

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

a) Let $W_0 = \{w \in V \mid H(v, w) = 0 \ \forall v \in V\}$ be the right kernel of the pairing H. Then any function $\theta \in \mathcal{L}(\theta_D)$ must factor through the quotient map $V \twoheadrightarrow V/W_0$. In particular, if H is degenerate, then Θ is not one-to-one.

b) If H is not positive semidefinite (i.e. if $H(v, v) < 0$ for some $v \in V$), then we have $\mathcal{L}(\theta_D) = \{0\}$ and so Θ is not defined.

Proof. Choose any $\theta \in \mathcal{L}(\theta_D)$. We first note that since H is trivial on $V \times (W_0 \cap \Lambda)$, we have $\theta(w + \lambda)/\theta(w) = e^{2\pi i K(\lambda)}$ for all $\lambda \in W_0 \cap \Lambda$. Since K takes values in $\mathbb{R}$, $|e^{2\pi i K(\lambda)}| = 1$. Let $C_0 \subset V$ be a compact subset such that $C_0 + (W_0 \cap \Lambda) = W_0$. For any fixed $v \in V$, we then have $\max_{w \in W}\{|\theta(v + w)|\} = \max_{w' \in C_0}\{|\theta(v + w')|\}$, which is finite because C_0 is compact. Then by the maximum principal for holomorphic functions on W_0, we see that $\theta(v+w)$ must be constant as a function of w, proving statement (a).

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

$$|\theta(v + w)| = |\theta(v + w' + \lambda)| = |\theta(v + w')| e^{\pi \Re H(v+w', \lambda) + \frac{1}{2}\pi H(\lambda, \lambda)}. \tag{2.7}$$

It is straightforward to compute that

$$\Re H(v + w', \lambda) + \frac{1}{2} H(\lambda, \lambda) = \frac{1}{2} H(w, w) + \Re H(v, w) - \Re H(v, w') - \frac{1}{2} H(w', w'). \tag{2.8}$$

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 C 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 $\theta = 0$, proving statement (b).

□

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

Theorem 2.3.3. *Let H be a positive definite Riemann form. Then the divisor $D \in \mathrm{Div}(X)$ corresponding to H is ample. More precisely, for any $n \geq 3$, the divisor $nD \in \mathrm{Div}(X)$ is very ample.*

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 $\det(E)$ is a positive integer if $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$.

Lemma 2.3.4. *(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 $E(\lambda_i, \lambda_{i+g}) = -e_i$ 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 $\sqrt{\det(E)} = e_1 ... e_g$.

For reasons of time, we omit the proof of the above lemma. The following corollary is immediate from the lemma and will be useful later.

Corollary 2.3.5. *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 2.3.3). We will prove this for $n = 3$; the argument for greater n is similar.

To prove show that property (i) in Definition 2.3.1 holds for $3D$, we observe that given any $\theta \in \mathcal{L}(\theta_D)$ and any choice of $a, b \in V$, the meromorphic function $\theta_{a,b} \in \mathcal{L}(V)$ defined by $\theta_{a,b}(v) = \theta(v+a+b)\theta(v-a)\theta(v-b)$ satisfies

$$\theta_{a,b}(v+\lambda)/\theta_{a,b}(v) = e^{2\pi i(\frac{1}{2i}H(v+a+b,\lambda)+\frac{1}{2i}H(v-a,\lambda)+\frac{1}{2i}H(v-b,\lambda)+\frac{3}{4i}H(\lambda,\lambda)+3K(\lambda))}$$

$$= e^{2\pi i(\frac{1}{2i}3H(v,\lambda)+\frac{1}{4i}3H(\lambda,\lambda)+3K(\lambda))} = (\theta(v+\lambda)/\theta(v))^3 \tag{2.9}$$

for $v \in V$, $\lambda \in \Lambda$. So $\theta_{a,b} \in \mathcal{L}(3H)$, and, given any $v_0 \in V$, by choosing appropriate $a, b \in V$ we can ensure that $\theta_{a,b}(v_0) \neq 0$ and therefore not all basis elements of $\mathcal{L}(\theta_{3D})$ vanish at v_0.

To prove that 2.3.1(ii) holds for $3D$, 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

$$\theta(v_1+a+b)^{-1}d\theta - \theta(v_1-a)^{-1}d\theta = \theta(v_2+a+b)^{-1}d\theta - \theta(v_2-a)^{-1}d\theta \tag{2.10}$$

for any $b \in V$. It follows that the differential given by $v \mapsto \theta(v_2+v)^{-1}d\theta - \theta(v_1+v)^{-1}d\theta$ is translation-invariant (after renaming the variable a as v and considering that b can be chosen arbitrarily) and is therefore equal to $dB(v)$ for some linear functional $B : V \to \mathbb{C}$. After integrating and exponentiating, we get

$$\theta(v+v_2)/\theta(v+v_1) = ce^{B(v)} \Longrightarrow \theta(v+(v_2-v_1))/\theta(v) = c'e^{B(v)} \tag{2.11}$$

for some constants $c, c' \in \mathbb{C}^\times$. Using the property given in Definition 2.2.5, we deduce from substituting $v+\lambda$ for v in (2.11) and using our translation formula for θ that $e^{2\pi i(\frac{1}{2i}H(v_2-v_1,\lambda))} = e^{B(\lambda)}$ for all $\lambda \in \Lambda$. Thus, we have that $\pi H(v_2-v_1,\lambda) \equiv B(\lambda) \pmod{2\pi i\mathbb{Z}}$. Now we have $\pi H(v_2-v_1,\lambda) - B(\lambda) = \pi H(\lambda, v_2-v_1) + 2\pi i E(v_1-v_2,\lambda) - B(\lambda) \in 2\pi i\mathbb{Z}$, and it follows from the fact that E is real-valued that $\pi H(\lambda, v_2-v_1) - B(\lambda)$ takes purely imaginary values

for $\lambda \in \Lambda$. Thus, $v \mapsto \pi H(v, v_1 - v_2) - B(v)$ takes purely imaginary values, but this function is $\mathbb{C}$-linear, so we have $\pi H(v, v_2 - v_1) - B(v) = 0$ for $v \in V$. Then

$$\pi H(v_2 - v_1, \lambda) - B(\lambda) = 2\pi i E(v_2 - v_1, \lambda) + \pi H(\lambda, v_2 - v_1) - B(\lambda) = 2\pi i E(v_2 - v_1, \lambda) \in 2\pi i \mathbb{Z}, \tag{2.12}$$

implying that $E(v_2 - v_1, \lambda) \in \mathbb{Z}$ for all $\lambda \in \Lambda$. Thus, letting $\Lambda' = \Lambda + (v_2 - v_1)\mathbb{Z}$, we have $E(\Lambda', \Lambda') \subseteq \mathbb{Z}$. In turn, this implies (as another easy exercise) that the subgroup $\Lambda' \subset V$ is another lattice containing Λ, or equivalently, that $[\Lambda' : \Lambda] < \infty$.

Now (2.11) tells us that we have

$$\theta(v + (v_2 - v_1))/\theta(v) = c' e^{\pi H(v, v_2 - v_1)} = e^{2\pi i (\frac{1}{2i} H(v, v_2 - v_1) + \frac{1}{4i} H(v_2 - v_1, v_2 - v_1) + K'(v_2 - v_1))} \tag{2.13}$$

where $c'' \in \mathbb{C}^\times$ is a constant and $K' : \Lambda' \to \mathbb{C}$ is an extension of K (not necessarily satisfying the perscribed properties for $K : \Lambda \to \mathbb{R}$). Therefore, θ is actually a theta function for H with respect to the lattice Λ'. We write $\det_{\Lambda'}(E)$ for the determinant of the alternating form $E : \Lambda' \times \Lambda' \to \mathbb{Z}$. Note that by Lemma 2.3.4(b), the space $\mathcal{L}_{H,K'}$ of theta functions θ' *with respect to* Λ' for H satisfying $\theta'(v + \lambda')/\theta'(v + \lambda) = e^{2\pi i (\frac{1}{2i} H(v, \lambda') + \frac{1}{4i} H(\lambda', \lambda') + K'(\lambda'))}$ for $\lambda' \in \Lambda'$ has dimension equal to $\sqrt{\det_{\Lambda'}(E)}$.

Suppose that $\Lambda' \supsetneq \Lambda$. Then one can show as an easy exercise in linear algebra that $\det(E) > \det_{\Lambda'}(E)$. We have shown above that every theta function $\theta \in \mathcal{L}(\theta_D)$ belongs to the space of theta functions with respect to Λ' whose translation functions are as in Definition 2.2.5 with $L(v, \lambda) = \frac{1}{2i} H(v, \lambda)$ and $J'(\lambda) = \frac{1}{4i} H(\lambda, \lambda) + K(\lambda)$ for some $K' : \Lambda' \to \mathbb{C}$ extending K. There are only finitely many choices for K' since $[\Lambda' : \Lambda] < \infty$ and the relation in (2.5) must be satisfied, and each space $\mathcal{L}_{H,K'}$ has dimension $\sqrt{\det_{\Lambda'}(E)} < \sqrt{\det(E)}$. We therefore a contradiction. Thus, $\Lambda' = \Lambda$, implying that $v_2 - v_1 \in \Lambda$, as desired.

Finally we show that 2.3.1(iii) holds for $3D$. After fixing a basis for V, we write $z_1, ..., z_g$ for the corresponding set of coordinate functions on V. Let $\widetilde{\Theta} : V \to \mathbb{P}_{\mathbb{C}}$ be the composition with Θ as defined in Definition 2.3.1 with the covering map $V \twoheadrightarrow X$. Then it obviously suffices to show that at every point $v_0 \in V$, the induced map $\widetilde{\Theta}_* : T_{v_0} V \to T_{\widetilde{\Theta}(v_0)} \mathbb{P}^m_{\mathbb{C}}$ is injective. Choose any point $v_0 \in V$, and let $\sum_{i=1}^g \alpha_i \frac{\partial}{\partial z_i} \in T_{v_0} V$ be a tangent vector whose image under $\widetilde{\Theta}_*$ vanishes. If we write $\{\theta_0, ..., \theta_m\}$ for a basis of $\mathcal{L}(\theta_{3D})$ and assume without loss of generality that $\theta_0(z_0) \neq 0$, we then have

$$\sum_{i=1}^g \alpha_i \frac{\partial(\phi/\theta_0)}{\partial z_i}(v_0) = 0 \tag{2.14}$$

for every $\phi \in \mathcal{L}(\theta_{3D})$. Suppose that this choice of tangent vector is nonzero; we may assume without loss of generality that $\alpha_1 \neq 0$. Then we have (using the quotient rule for differentiation)

$$\begin{aligned} &\frac{\alpha_1}{\theta_0(v_0)^2} \big(\theta_0(v_0) \frac{\partial \phi}{\partial z_1}(v_0) - \phi(v_0) \frac{\partial \theta_0}{\partial z_1}(v_0) \big) = 0 \\ \implies &\phi(v_0)^{-1} \frac{\partial \phi}{\partial z_1}(v_0) = \theta_0(v_0)^{-1} \frac{d\theta_0(v)}{\partial z_1}(v_0) =: c \end{aligned} \tag{2.15}$$

for every $\phi \in \mathcal{L}(\theta_{3D})$. Now choose $\theta \in \mathcal{L}(\theta_D)$ and define $\theta_{a,b}(v) \in \mathcal{L}(\theta_{3D})$ as before for any $a, b \in V$. Putting $\theta_{a,b}$ for ϕ in (2.15) gives us

$$\theta(v_0 - a)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 - a) + \theta(v_0 - b)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 - b) + \theta(v_0 + a + b)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 + a + b) = c. \quad (2.16)$$

By treating the expression in (2.16) as a (constant) function in the variable a (which we rename as v) and taking partial derivatives with respect to a, we see that

$$\frac{\partial}{\partial z_i}\big((v_0 - v)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 - a)\big) = \frac{\partial}{\partial z_i}\big(\theta(v_0 + a + b)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 + a + b)\big) \quad (2.17)$$

for $1 \leq i \leq g$ and for any choice of b. In particular, it follows that $\theta(v_0 + v)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 + v)$ is linear (but not necessarily homogeneous) in v; we write it as $\mu z_1 + \nu(v)$ for some constant $\mu \in \mathbb{C}$ and linear function ν not depending on z_1. By integration and exponentiating on both sides of the equation $\theta(v_0 + v)^{-1}\frac{\partial\theta}{\partial z_1}(v_0 + v) = \mu z_1 + \nu(v)$ with respect to z_1, we get that $\theta(v_0 + z_1) = e^{\frac{1}{2}\mu z_1^2 + \nu(v_0)z_1}\theta(v_0)$. Let $e_1 \in V$ be the unit basis vector in the direction of z_1. Then we have

$$\theta(v_0 + de_1)/\theta(v_0) = e^{\frac{1}{2}\mu d^2 + \nu(v_0)d}. \quad (2.18)$$

Similarly to our argument above, we deduce from substituting $v + \lambda$ for v in (2.18) and using our translation formula for θ that $\pi H(z + de_1, \lambda) \equiv d(\nu(v_0 + \lambda) - \nu(v_0)) \pmod{2\pi i\mathbb{Z}}$. Since ν is linear (possibly non-homogeneous), the map $\lambda \mapsto d(\nu(v_0 + \lambda) - \nu(v_0))$ defines a functional on V. Now we see using the same arguments as were used above to show that $E(de_1, \Lambda) \subseteq \mathbb{Z}$ for any $d \in \mathbb{C}$. But this contradicts the nondegeneracy of H and thus also our assumption that the tangent vector $\sum_{i=1}^{g} \alpha_i \frac{\partial}{\partial z_i} \in T_{v_0}V$ is nonzero.

□

We have now more or less shown 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 well-known 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 2.3.6. *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 complex torus 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 2.3.6 and more specifically Theorem 2.3.3 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 2.3.5 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 2.3.3 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.

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

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 $z \in \mathbb{C} \smallsetminus \Lambda$, 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

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

We check that for each $z \in D' \smallsetminus \{0\}$, 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 $P \in X \smallsetminus 0$, 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, implying (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 2.3.4 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

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

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:

$$f(\wp, \wp') := \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \equiv 0. \tag{2.19}$$

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 be abelian varieties of the same dimension, 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 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, the lattice $\tilde{\varphi}(\Lambda_1)$ has rank $2g$, as does Λ_2, and so the induced quotient is finite.

Now suppose that φ is not an isogeny – that is, φ is not surjective. Then clearly $\tilde{\varphi}$ is not a surjection onto V_2. Since V_1 and V_2 have the same dimension, this implies that $\tilde{\varphi}$ is not injective either, so that $\ker(\tilde{\varphi}) \subseteq V_1$ is a subspace of positive dimension. Since $\Lambda_1 \subset V_1$ is discrete, the image of $\ker(\tilde{\varphi})$ in X_1 is positive-dimensional and in particular not finite. Since this is contained in the kernel of φ, we see that φ does not have finite kernel.

□

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. (Actually, Silverman's book [7] includes the trivial map as an isogeny between elliptic curves, but this is inconsistent with our definition and most definitions of the term.)

Corollary 2.5.4. *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 surjective map $\varphi : X \to X'$ 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. In order to show that X' also has the structure of abelian variety, it is enough to find a positive definite Riemann form for X'. It is easy to check that if $H : V \times V \to \mathbb{C}$ is a positive definite Riemann form with respect to Λ and $n = [\Lambda' : \Lambda]$ is the degree of φ, then $n^2 H$ is a positive definite Riemann form with respect to $\frac{1}{n}\Lambda$. Since clearly $\Lambda' \subseteq \frac{1}{n}\Lambda$, we are done.

□

Definition 2.5.5. *The **degree** of an isogeny $\varphi : X_1 \to X_2$ is the order of its kernel.*

We now briefly discuss the most important example of an isogeny.

Example 2.5.6. If X is a complex abelian variety of dimension g, then Corollary 2.1.4 says that the multiplication-by-n map $[n] : X \to X$ is surjective, and that it has finite kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, for any integer $n \geq 1$. Therefore, $[n]$ is an isogeny of degree n^{2g}.

Proposition 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 $V \twoheadrightarrow V/\Lambda_1 \cong X_1$ clearly coincides with $\frac{1}{n}\Lambda_1$. 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 2.5.4, 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 $\varphi' : X_2 \to X_1$ 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 2.5.4, 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 proposition 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; for this purpose, we will only assume for the moment that X is a complex torus which is not necessarily an abelian variety.

In §2.2 we constructed a homomorphism $\mathcal{H}$ from $\mathrm{Div}(X)$ to the group of Hermitian forms on the covering space V (and we showed that in fact, the image coincides with the group of Riemann form for X). We shall 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 2.2.8, 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 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.

Since $\mathcal{H}$ is simply the composition of Φ with the projection to the group of Riemann forms on V, its kernel is some subgroup of $\mathrm{Div}(X)$ containing $\mathrm{Prin}(X)$. We let $\mathrm{Div}^0(X)$ denote this kernel; in other words, $\mathrm{Div}^0(X) \subset \mathrm{Div}(X)$ is the subgroup of all divisors whose associated Riemann form is 0. 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 $\mathrm{Pic}(X)$ (whose kernel is $\mathrm{Pic}^0(X)$).

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 by definition 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 $\mathrm{Div}^0(X)$; therefore, the image of any polarization is contained in $\mathrm{Pic}^0(X)$.

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

$$\theta'(v + \lambda)/\theta'(v) = e^{\pi H(w+v,\lambda) + \frac{1}{2}H(\lambda,\lambda) + 2\pi i K(\lambda)}. \tag{2.20}$$

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 trivial theta function. 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 $\lambda \in \Lambda$,

$$\theta''(v+\lambda)/\theta''(v) = e^{2\pi i(\frac{1}{2i}H(v+w,\lambda)+\frac{1}{4i}H(\lambda,\lambda)+K(\lambda)-\frac{1}{2i}H(\lambda,w)}$$

$$= e^{2\pi i(\frac{1}{2i}H(w,\lambda)-\frac{1}{2i}H(\lambda,w)} \cdot e^{2\pi i(\frac{1}{2i}H(v,\lambda)+\frac{1}{4i}H(\lambda,\lambda)+K(\lambda)}$$

$$= e^{2\pi iE(w,\lambda)} \cdot e^{2\pi i(\frac{1}{2i}H(v,\lambda)+\frac{1}{4i}H(\lambda,\lambda)+K(\lambda)} = e^{2\pi iE(w,\lambda)} \cdot \theta_D(v+\lambda)/\theta_D(v). \tag{2.21}$$

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 $\theta_{t_a^*D-D}(v+\lambda)/\theta_{t_a^*D-D}(v) = e^{2\pi iE(w,\lambda)}$ 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.

□

We will now, for the rest of this section, assume that X is an abelian variety (so X has an ample divisor).

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. Moreover, the injection of $\mathrm{Pic}^0(X)$ into the group of complex characters of Λ given by $\mathfrak{D} \mapsto \chi_{\mathfrak{D}}$ as constructed above is an isomorphism.*

Proof. We first observe that any complex character $\chi : \Lambda \to \mathbb{C}^*$ must be of the form $\lambda \mapsto e^{2\pi iB(\lambda)}$ for some $\mathbb{R}$-linear function $B : \Lambda \to \mathbb{R}$. Meanwhile, by Proposition 2.3.2, 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 $w \in V$. We therefore have $\chi_{\mathfrak{D}} = e^{2\pi iE(w,\cdot)}$ for some $w \in V$, and it follows from Lemma 2.5.11(b) that $\varphi_D(-a) = \mathfrak{D}$ for any divisor class $\mathfrak{D} \in \mathrm{Pic}^0(X)$, where $a = \pi(w)$. Thus, $\mathfrak{D} \mapsto \chi_{\mathfrak{D}}$ is actually an isomorphism from $\mathrm{Pic}^0(X)$ to the group of complex characters on Λ, and φ_D is a surjective map. The fact that φ_D is also a group homomorphism follows easily from our formula $\chi_{\varphi_D(a)} = e^{2\pi iE(w,\cdot)}$.

It is now clear that the kernel of φ_D consists of the images modulo Λ of elements $w \in V$ with $e^{2\pi iE(w,\lambda)} = 1$ and thus $E(w,\lambda) \in \mathbb{Z}$ for all $\lambda \in \Lambda$. It follows quickly from Lemma 2.3.4(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 is therefore an abelian variety by Theorem 2.3.6.*

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^*. Note that if $w \in V$ is an element such that $B(\cdot) \equiv E(w, \cdot)$ modulo $\mathbb{Z}$, then we have $B(iv) - iB(v) = E(-iw, \cdot) - iE(w, \cdot) = H(-w, \cdot)$. It now follows from what we have shown before that the map $\varphi_D : X \to \mathrm{Pic}^0(X) \xrightarrow{\sim} V^*/\Lambda^*$ is given by

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

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 $w \mapsto H(w, \cdot) \in V^*$. Note that $\widetilde{\varphi_D}(\Lambda) \subseteq \Lambda^*$ is a sublattice of (finite) index equal to the order of $\ker(\varphi_D)$, which is $\det(E)$, implying that $\Lambda \subseteq \Lambda^* \subseteq \frac{1}{\det(E)} \widetilde{\varphi_D}(\Lambda)$. 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, we have $H^*(\Lambda^*, \Lambda^*) \subseteq \det(E)^{-2}\mathbb{Z}$, so that $\det(E)^2 H^*$ 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. 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 $\deg(D) = n$, the divisors 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 [5, §1].

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, §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. Choose any divisor $D \in \mathrm{Div}^0(C)$. We deduce from Theorem 2.6.2 that $\ell(D+g(O)) = g+\ell(K-(D+g(O)))-g+1 \geq 1$, so there is a nonzero meromorphic function $h \in \mathcal{L}(D+g(O))$. Then we have $D' := D + (h) > g(O)$, so D' is a divisor of the desired form which lies in the same class as D in $\mathrm{Pic}^0(C)$.

□

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

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

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

2.7 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. By directly using the formula for $\wp$, find the zeroes of the derivative $\wp'$. Relate this to the characterization of the 2-torsion subgroup of an elliptic curve coming from Exercise 1.2.3.

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) Proposition 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).

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

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

[6] Michael Rosen. Abelian varieties over c. In *Arithmetic geometry*, pages 79–101. Springer, 1986.

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