Abelian Varieties

Andrew Kobin

Fall 2019 – Spring 2020

Contents

0 Introduction

These notes were taken during the Galois-Grothendieck Seminar at University of Virginia during Fall 2019 - Spring 2020. The theme, abelian varieties, connects several topics presented by faculty and students. These include:

- Group schemes and abelian schemes
- The definition of abelian varieties and basic results
- Complex elliptic curves
- Jacobians of complex curves as complex tori
- Line bundles on complex tori
- Projective embeddings of abelian varieties.

Classical references for many of these topics are the texts by Mumford and Edixhoven-van der Geer-Moonen, both entitled *Abelian Varieties*. More modern references include course notes by Bhatt, B. Conrad and Milne.

1 Group Schemes

1.1 Basic Definitions

Let S be a scheme and $\texttt{Sch}_S$ the category of S-schemes, i.e. the category with objects $X \to S$ and morphisms

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

Then S is a terminal object in $\texttt{Sch}_S$ and group schemes are defined to be the group objects in this category. Here is an explicit definition.

Definition. *A* **group scheme** *over S is a scheme $G \to S$ equipped with morphisms $m : G \times_S G \to G, e : S \to G$ and $i : G \to G$, called* **product**, **unit** *and* **inversion**, *respectively, for which the following diagrams in $\texttt{Sch}_S$ commute:*

(1) (Associativity Law)

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{1 \times m} & G \times_S G \\ {\scriptstyle m \times 1}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G \end{array}$$

(2) (Identity Law)

$$\begin{array}{ccc} G & \xrightarrow{1 \times e} & G \times_S G \\ {\scriptstyle e \times 1}\downarrow & \overset{1}{\searrow} & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G \end{array}$$

(3) (Law of Inverses)

$$\begin{array}{ccc} G & \xrightarrow{i \times 1} & G \times_S G \\ \downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow[e]{} & G \end{array}$$

In addition, G is a **commutative group scheme** *if the diagram*

$$\begin{array}{ccc} G \times_S G & & \\ \downarrow s & \overset{m}{\searrow} & G \\ G \times_S G & \underset{m}{\nearrow} & \end{array}$$

commutes, where s flips the factors of $G \times_S G$.

Definition. *A* **morphism of group schemes** *is a morphism of S-schemes $f : G \to H$ such that*

(1) The diagram

$$\begin{array}{ccc} G \times_S G & \xrightarrow{f \times f} & H \times_S H \\ \downarrow m_G & & \downarrow m_H \\ G & \xrightarrow[f]{} & H \end{array}$$

commutes.

(2) $f \circ e_G = e_H$.

(3) $f \circ i_G = i_H \circ f$.

It should be noted that a group scheme structure does not directly define a group structure on the underlying topological space of G. However, Yoneda's Lemma gives us a way of creating abstract groups from the data of a group scheme, and then applying techniques from abstract algebra to each of these.

Let $\mathcal{C}$ be a category and $\texttt{Fun}(\mathcal{C}) := \texttt{Fun}^{op}(\mathcal{C}, \texttt{Set})$ be the category of contravariant functors $\mathcal{C} \to \texttt{Set}$, with morphisms given by natural transformations. Then there is a functor $h : \mathcal{C} \to \texttt{Fun}(\mathcal{C})$ sending $X \mapsto h_X$, where $h_X : \mathcal{C} \to \texttt{Set}, Y \mapsto \mathrm{Hom}_{\mathcal{C}}(Y, X)$. Recall Yoneda's Lemma:

Theorem 1.1.1 (Yoneda's Lemma)**.** *The functor $h : \mathcal{C} \to \texttt{Fun}(\mathcal{C}), X \mapsto h_X$ is fully faithful.*

Definition. *A functor $F \in \texttt{Fun}(\mathcal{C})$ is* **representable** *if F is naturally isomorphic to h_X for some object $X \in \mathcal{C}$. In this case, we say F is* **represented** *by X.*

Yoneda's Lemma can be generalized to show that for any functor $F \in \texttt{Fun}(\mathcal{C})$, there is a natural isomorphism

$$F(X) \xrightarrow{\sim} \mathrm{Hom}_{\texttt{Fun}(\mathcal{C})}(h_X, F).$$

Applying this to a group object (G, m, e, i) in $\mathcal{C}$ allows us to induce a group structure on the set $h_G(Y)$ for any object Y. Indeed, composition with m induces a multiplication map

$$h_G(Y) \times h_G(Y) = h_{G \times G}(Y) \longrightarrow h_G(Y).$$

Set $G(Y) := h_G(Y)$. Likewise, e and i induce an identity element and inverses on $G(Y)$ such that the axioms of an abstract group are satisfied on $G(Y)$. So we can think of a group object G as a choice of group $G(Y)$ for each $Y \in \mathcal{C}$ that is functorial in Y. In fact, Yoneda's Lemma says that *every* such representable functor $h_G : \mathcal{C} \to \mathtt{Set}$ is representable by a group object. In the case when $\mathcal{C} = \mathtt{Sch}_S$, this says that a group scheme $G \to S$ is equivalent to a functorial choice of group structure on $G(Y) := h_G(Y)$ for every S-scheme Y.

Definition. *Fix a scheme $X \to S$. Then for any $Y \in \mathtt{Sch}_S$, the set $X(Y) := h_X(Y)$ is called the* **set of Y-points** *of X.*

Remark. A subtle point above is that a "group functor", i.e. a functor $F : \mathcal{C} \to \mathtt{Set}$ assigning a group structure to each $F(X)$ in a functorial way, need not be representable. (What we mean to say is that if F is representable, it is represented by a group object.) Examples of this include the functors Pic and Br on $\mathtt{Sch}_S$, which are group functors but are not represented by schemes.

1.2 Hopf Algebras

Let $S = \operatorname{Spec} k$, so that $\mathtt{Sch}_k$ consists of schemes $(X, \mathcal{O}_X)$ with a k-algebra structure on $\mathcal{O}_X(U)$ for each open set $U \subseteq X$.

Example 1.2.1. Let $\mathbb{G}_a : \mathtt{Sch}_k \to \mathtt{Set}$ be the functor sending $X \mapsto \Gamma(X, \mathcal{O}_X)$. Then $\mathbb{G}_a$ is representable by the *additive group* $\mathbb{A}^1 = \operatorname{Spec} k[x]$, also denoted by $\mathbb{G}_a$ when considered as a group scheme. Indeed, $\mathbb{G}_a$ is a group scheme whose canonical maps m, e and i are induced by the following *comorphisms* on $k[x]$:

$$\begin{aligned} m^* : k[x] &\longrightarrow k[x] \otimes_x k[x] \\ x &\longmapsto x \otimes 1 + 1 \otimes x \\ e^* : k[x] &\longrightarrow k \\ x &\longmapsto 0 \\ i^* : k[x] &\longrightarrow k[x] \\ x &\longmapsto -x. \end{aligned}$$

One can deduce these comorphisms from the Yoneda perspective described in Section 1.1. For example, m is defined by considering the map

$$h_{\mathbb{G}_a \times \mathbb{G}_a}(\mathbb{G}_a \times \mathbb{G}_a) = h_{\mathbb{G}_a}(\mathbb{G}_a \times \mathbb{G}_a) \times h_{\mathbb{G}_a}(\mathbb{G}_a \times \mathbb{G}_a) \xrightarrow{m_{\mathbb{G}_a} \times m_{\mathbb{G}_a}} h_{\mathbb{G}_a}(\mathbb{G}_a \times \mathbb{G}_a)$$

and setting $m := m_{\mathbb{G}_a \times \mathbb{G}_a}(\pi_1, \pi_2)$, where $\pi_1, \pi_2 : \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ are the coordinate projections. On the level of k-algebras, these are given by $\pi_1 : k[x] \to k[x] \otimes_k k[x], x \mapsto x \otimes 1$ and $\pi_2 : k[x] \to k[x] \otimes_k k[x], x \mapsto 1 \otimes x$, so we see that

$$m_{\mathbb{G}_a \times \mathbb{G}_a}(\pi_1, \pi_2) = \pi_1 + \pi_2 : x \longmapsto x \otimes 1 + 1 \otimes x.$$

Similar arguments yield the formulas for e^* and i^*.

More generally, if $G = \operatorname{Spec} A$ is an affine group scheme over k, then A possesses the structure of a Hopf algebra over k.

Definition. *A* **Hopf algebra** *is a k-algebra A equipped with k-algebra homomorphisms $\Delta : A \to A \otimes_k A, \varepsilon : A \to k$ and $\sigma : A \to A$, respectively called* **comultiplication**, **counit** *and* **antipode**, *for which the dual axioms to the group scheme axioms hold. That is, the following diagrams commute in $\mathtt{Alg}_k$:*

(1) (Coassociativity Law)

$$\begin{array}{ccc} A \otimes_k A \otimes_k A & \xleftarrow{\;1 \otimes \Delta\;} & A \otimes_k A \\ {\scriptstyle \Delta \otimes 1}\big\uparrow & & \big\uparrow{\scriptstyle \Delta} \\ A \otimes_k A & \xleftarrow[\;\Delta\;]{} & A \end{array}$$

(2) (Coidentity Law)

$$\begin{array}{ccc} A & \xrightarrow{\;1 \otimes \varepsilon\;} & A \otimes_k A \\ {\scriptstyle \varepsilon \otimes 1}\big\downarrow & \overset{1}{\searrow} & \big\downarrow{\scriptstyle \Delta} \\ A \otimes_k A & \xrightarrow[\;\Delta\;]{} & A \end{array}$$

(3) (Law of Antipodes)

$$\begin{array}{ccc} A & \xrightarrow{\;\sigma \otimes 1\;} & A \otimes_k A \\ \big\downarrow & & \big\downarrow{\scriptstyle \Delta} \\ k & \xrightarrow[\;\varepsilon\;]{} & A \end{array}$$

Moreover, A is **cocommutative** *if $\tau \circ \Delta = \Delta$, where $\tau : A \otimes_k A \to A \otimes_k A$ is the map induced by $\tau(a \otimes b) = a \otimes b$.*

Remark. Any k-vector space V satisfying laws (1) – (3) is called a **coalgebra**.

In general, the group of sections $\Gamma(G, \mathcal{O}_G)$ of an affine group scheme G will be a commutative Hopf algebra, but will not always be cocommutative.

Example 1.2.2. Let $\mathbb{G}_m : \mathtt{Sch}_k \to \mathtt{Set}$ be the group functor sending $X \mapsto \Gamma(X, \mathcal{O}_X)^\times$, the multiplicative group of the space of global sections of $\mathcal{O}_X$. Like the additive group, $\mathbb{G}_m$ is representable by a scheme called the *multiplicative group* $\mathbb{A}^1 \smallsetminus \{0\} = \operatorname{Spec} k[x, x^{-1}]$, which is also denoted by $\mathbb{G}_m$ when considered as a group scheme. The k-algebra $k[x, x^{-1}]$ has the following Hopf algebra structure:

$$\begin{aligned} m^* : k[x,x^{-1}] &\longrightarrow k[x,x^{-1}] \otimes_k k[x,x^{-1}] \\ x &\longmapsto x \otimes x \\ x^{-1} &\longmapsto x^{-1} \otimes x^{-1} \\ e^* : k[x,x^{-1}] &\longrightarrow k \\ x, x^{-1} &\longmapsto 1 \\ i^* : k[x,x^{-1}] &\longrightarrow k[x,x^{-1}] \\ x &\longmapsto x^{-1} \\ x^{-1} &\longmapsto x. \end{aligned}$$

Notice that $k[x, x^{-1}] \cong k[\mathbb{Z}]$, the group algebra (over k) of the abelian group $\mathbb{Z}$.

Remark. One can generalize this example by taking any abelian group Λ and equipping the group algebra $k[\Lambda]$ with the following Hopf algebra structure:

$$\begin{aligned} \Delta : \lambda &\longmapsto \lambda \otimes \lambda \\ \varepsilon : \lambda &\longmapsto 1 \\ \sigma : \lambda &\longmapsto \lambda^{-1} \end{aligned}$$

and extending by linearity. An element a in a Hopf algebra A is called *grouplike* if $\Delta(a) = a \otimes a$, so we are declaring above that all elements of $\Lambda \subset k[\Lambda]$ are grouplike under the Hopf algebra structure. The definitions of ε and σ are then required by the Hopf algebra axioms. The group scheme corresponding to this construction is written $D(\Lambda) = \operatorname{Spec} k[\Lambda]$.

Proposition 1.2.3. *A group scheme G is diagonalizable if and only if $G \cong D(\Lambda)$ for some abelian group Λ.*

Lemma 1.2.4. *For any abelian group Λ and any k-scheme X, the X-points of $D(\Lambda)$ are given by $D(\Lambda)(X) = \operatorname{Hom}(\Lambda, \Gamma(X, \mathcal{O}_X)^\times)$.*

Example 1.2.5. When $\Lambda = \mathbb{Z}^n$, the associated group scheme is an *n-dimensional torus*:

$$D(\mathbb{Z}^n) = \mathbb{G}_m^{\times n} := \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n}.$$

Example 1.2.6. When $\Lambda = \mathbb{Z}/n\mathbb{Z}$, the associated group scheme is called the *group scheme of nth roots of unity*, $D(\mathbb{Z}/n\mathbb{Z}) = \mu_n$. This group scheme can alternatively be constructed either as the group functor sending X to the n-torsion subgroup of $\Gamma(X, \mathcal{O}_X)^\times$, or explicitly as the affine k-scheme $\mu_n = \operatorname{Spec} k[x, x^{-1}]/(x^n - 1)$. The latter description makes it clear that μ_n is a closed subgroup of $\mathbb{G}_m$.

Example 1.2.7. Another group scheme we'd like to construct is the *general linear group* GL_n. This will generalize $\mathbb{G}_m = GL_1$ in a different direction than above, as GL_n is not diagonalizable when $n > 1$. Consider the group functor $GL_n : \mathtt{Sch}_k \to \mathtt{Set}$ sending $X \mapsto GL_n(\Gamma(X, \mathcal{O}_X))$. This is representable by the scheme $\operatorname{Spec} B$ where

$$B = k\left[x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}\right] = k[x_{ij} \mid 1 \le i, j \le n][t]/(1 - t\det(x_{ij}))$$

where $\det(x_{ij})$ is the formal determinant of the matrix of indeterminates $x_{11}, \ldots, x_{nn}$, as a polynomial in the x_{ij}. There is a Hopf algebra structure on B specified by:

$$\begin{aligned} \Delta : B &\longrightarrow B \otimes_k B \\ x_{ij} &\longmapsto \sum_{k=1}^{n} x_{ik} \otimes x_{kj} \\ \varepsilon : B &\longrightarrow k \\ x_{ij} &\longmapsto \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \ne j \end{cases} \\ \sigma : B &\longrightarrow B \\ x_{ij} &\longmapsto \frac{1}{\det(x_{ij})} c_{ji} \end{aligned}$$

where c_{ji} denotes the jith cofactor of (x_{ij}).

Example 1.2.8. Let Γ be a finite group and set $A = \operatorname{Hom}_k(\Gamma, k)$. Then A has a k-basis of idempotents e_γ indexed by $\gamma \in \Gamma$, defined by $e_\gamma(\tau) = \delta_{\gamma\tau}$. We give A the structure of a Hopf algebra by declaring

$$\begin{aligned} \Delta : A &\longrightarrow A \otimes_k A, e_\gamma \longmapsto \sum_{\sigma\tau = \gamma} e_\sigma \otimes e_\tau \\ \varepsilon : A &\longrightarrow k, e_\gamma \longmapsto \delta_{\gamma 1_\Gamma} \\ \sigma : A &\longrightarrow A, e_\gamma \longmapsto e_{\gamma^{-1}}. \end{aligned}$$

It is easy to check these operations satisfy the Hopf algebra axioms. Then $G := \operatorname{Spec} A$ is called the *constant group scheme* associated to Γ. For $X = \operatorname{Spec} B$ where B has no nontrivial idempotents, we have $G(X) = \operatorname{Hom}_k(A, B) \cong \Gamma$. In general, one can decompose $B = Be_1 \oplus \cdots \oplus Be_r$ for orthogonal idempotents $e_1, \ldots, e_r$ and then apply the above case to get a description of $G(\operatorname{Spec} B)$. Note that in general, $G(X) \ncong \Gamma$.

1.3 Further Properties

Let $G \to S$ be a group scheme and $S' \to S$ a morphism of schemes. Then the base change $G' := G \times_S S'$ is a group scheme over S' via the multiplication map

$$m' : G' \times_{S'} G' = (G \times_S S') \times_{S'} (G \times_S S') \xrightarrow{\sim} (G \times_S G) \times_S S' \xrightarrow{m \times 1_{S'}} G \times_S S' = G'.$$

On the level of Hopf algebras, this corresponds to the trivial extension of $\Delta : A \to A \otimes_k A$ to A':

$$\Delta' : A' = A \otimes_k k' \xrightarrow{\Delta \otimes 1} (A \otimes_k A) \otimes_k k' = (A \otimes_k k') \otimes_k (A \otimes_k k') = A' \otimes_k A'.$$

Let A be an arbitrary Hopf algebra over k, with algebraic closure $\bar{k} \supseteq k$, and denote $\overline{A} = A \otimes_k \bar{k}$. We will say A is *geometrically reduced* if $\overline{A}$ is reduced.

Theorem 1.3.1 (Cartier). *A Hopf algebra A over a field k of characteristic 0 is geometrically reduced. In particular, every affine group scheme over a field of characteristic 0 is smooth.*

Definition. *Let A be a commutative Hopf algebra. A* **Hopf ideal** *of A is an ideal $I \subset A$ such that*

(1) $\Delta(I) \subseteq I \otimes A + A \otimes I$.

(2) $\varepsilon(I) = 0$.

(3) $\sigma(I) = I$.

These axioms ensure that for any Hopf ideal $I \subset A$, the quotient A/I is again a Hopf algebra. Consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_k A \\ \downarrow & & \downarrow \\ A/I & \underset{\Delta_{A/I}}{\dashrightarrow} & A/I \otimes_k A/I \end{array}$$

We'd like to say Δ descends to a Hopf algebra comultiplication map $\Delta_{A/I}$, and indeed this is valid by axiom (1), since the kernel of $A \otimes_k A \to A/I \otimes_k A/I$ is precisely $A \otimes I + I \otimes A$.

Example 1.3.2. Let $G = \mathbb{G}_a$, with Hopf algebra $A = k[x]$ as in Example 1.2.1. In characteristic 0, G has no nontrivial subschemes and correspondingly, we can't find any Hopf ideals of A to take the quotient by. On the other hand, over a field of characteristic $p > 0$, the relation $\Delta(x^p) = x^p \otimes 1 + 1 \otimes x^p$ holds in $A \otimes_k A$. This means $I = (x^p)$ is a Hopf ideal of A (the other two axioms are easily checked). Thus the quotient $B = k[x]/(x^p)$ is a Hopf algebra. Its corresponding group scheme is denoted $\alpha_p = \operatorname{Spec} k[x]/(x^p)$. This is an example of an *infinitesimal group scheme* since for any field extension L/k,

$$\alpha_p(\operatorname{Spec} L) = \operatorname{Hom}_k(k[x]/(x^p), L) = 0$$

so α_p has *no points over* L. Note that α_p is not smooth, since if $I_0 = (x)$ is the augmentation ideal of A, we have

$$1 = I_0/I_0^2 = (I_0/I)/(I_0/I)^2$$

whereas $\dim B = 0$.

Example 1.3.3. Let $G = \mathbb{G}_m$, with Hopf algebra $A = k[x, x^{-1}]$ as in Example 1.2.2. One can check that $I = (x^n - 1)$ is a Hopf ideal of A, and the Hopf algebra $B = A/I$ corresponds to the group scheme μ_n of nth roots of unity. If $I_0 = (x, x^{-1})$ is the augmentation ideal in A then I_0/I is the augmentation ideal in B and we can detect smoothness by computing its k-dimension. If $\operatorname{char} k = p \nmid n$, then $I_0^2 + I = I_0$ so $I_0/I = 0$ and thus μ_n is smooth. On the other hand, if $p \mid n$, then we can write $x^n - 1 = (x^{n/p} - 1)^p \in I_0^2$ so as above,

$$1 = I_0/I_0^2 = (I_0/I)/(I_0/I)^2$$

and we see that μ_n is not smooth in this case. One should also note that α_p and μ_p are abstractly isomorphic (as schemes), but are not isomorphic as group schemes (they have different Hopf algebras).

Example 1.3.4. If Γ is a finite group, then the constant group scheme $G = G(\Gamma)$ is smooth since the augmentation ideal in its Hopf algebra $\operatorname{Hom}_k(k, \Gamma)$ is spanned by the idempotents $\{e_\gamma\}_{\gamma \neq 1}$.

1.4 Cartier Duality

Let k be a field (this works over a commutative ring in general). Given a k-vector space M, let $M^\vee = \operatorname{Hom}_k(M, k)$. There is a natural map $s_M : M \to M^{\vee\vee}$. Also, if N is another k-vector space and $f \in M^\vee, g \in N^\vee$, then $f \otimes g$ defines an element of $(M \otimes N)^\vee$. In other words, there is a map $t_{M,N} : M^\vee \otimes N^\vee \to (M \otimes N)^\vee$.

Now if C is a k-coalgebra with comultiplication $\Delta : C \to C \otimes C$ and augmentation $\varepsilon : C \to k$, the composition

$$m : C^\vee \otimes C^\vee \xrightarrow{t_{C,C}} (C \otimes C)^\vee \xrightarrow{\Delta^\vee} C^\vee$$

is a multiplication map on C. Likewise, there is an identity

$$e : k \cong k^\vee \xrightarrow{\varepsilon^\vee} C^\vee$$

making $C^\vee$ into a k-algebra. This process can be reversed as follows. For an algebra A with multiplication $m : A \otimes A \to A$ and identity $e : k \to A$, with the property that $t_{A,A} : A^\vee \otimes A^\vee \to (A \otimes A)^\vee$ is an isomorphism, the maps

$$\Delta : A^\vee \xrightarrow{m^\vee} (A \otimes A)^\vee \xrightarrow{t_{A,A}^{-1}} A^\vee \otimes A^\vee$$
$$\varepsilon : A^\vee \xrightarrow{e^\vee} k^\vee \cong k$$

define a coalgebra structure on $A^\vee$. Thus we have a correspondence between algebras and coalgebras given by taking the dual.

Lemma 1.4.1. *Let A be a Hopf algebra over k. Then*

(a) $A^\vee$ is also a Hopf algebra.

(b) *If A is commutative (resp. cocommutative), then so is $A^\vee$.*

(c) *If $s_A : A \to A^{\vee\vee}$ is an isomorphism of vector spaces, then it is an isomorphism of Hopf algebras and $G \cong G^{\vee\vee}$ as affine group schemes.*

(d) *If $\varphi : A \to B$ is a homomorphism of Hopf algebras, then $\varphi^\vee : B^\vee \to A^\vee$ is also a homomorphism of Hopf algebras. In particular, if $H = \operatorname{Spec} B$ is an affine group scheme, then $\operatorname{Hom}(G, H) \cong \operatorname{Hom}(H^\vee, G^\vee)$.*

Definition. *For an affine group scheme $G = \operatorname{Spec} A$, the* **Cartier dual** *of G is $G^\vee := \operatorname{Spec} A^\vee$.*

Example 1.4.2. If Γ is a finitely generated abelian group and $A = \underline{\Gamma} := \operatorname{Spec} k^\Gamma$, where $k^\Gamma = \operatorname{Hom}_k(\Gamma, k)$, then A is a Hopf algebra with multiplication $m(e_\gamma \otimes e_\tau) = \delta_{\gamma\tau} e_\tau$, unit $e(1) = \sum_{\gamma\in\Gamma} e_\gamma$, comultiplication $\Delta(e_\gamma) = \sum_{\gamma=\sigma\tau} e_\sigma \otimes e_\tau$ and counit and antipode defined similarly. The Cartier dual $A^\vee = \underline{\Gamma}^\vee$ corresponds to $(k^\Gamma)^\vee$ with the operations

$$m_{A^\vee}(e_\sigma^\vee \otimes e_\tau^\vee)(e_\gamma) = e_{\sigma\tau}^\vee(e_\gamma) := \begin{cases} 1, & \text{if } \sigma\tau = \gamma \\ 0, & \text{otherwise} \end{cases}$$

where $\{e_\gamma^\vee\}$ is the dual basis, and

$$\Delta_{A^\vee}(e_\gamma^\vee)(e_\sigma \otimes e_\tau) = e_\gamma^\vee(e_\sigma e_\tau) = \begin{cases} 1, & \text{if } \gamma = \sigma = \tau \\ 0, & \text{otherwise.} \end{cases}$$

Therefore $A^\vee = k[\Gamma]$, the group algebra of Γ.

Example 1.4.3. For $\Gamma = \mathbb{Z}/n\mathbb{Z}$, $\underline{\mathbb{Z}/n\mathbb{Z}}^\vee = \operatorname{Spec} k[\mathbb{Z}/n\mathbb{Z}]$, but $k[\mathbb{Z}/n\mathbb{Z}] = k[x]/(x^n - 1)$, so the dual here is the group scheme μ_n of nth roots of unity.

Example 1.4.4. For $\Gamma = \alpha_p$ with Hopf algebra $A = k[x]/(x^p)$, the basis $\{1, x, \ldots, x^{p-1}\}$ can be used to define the multiplication and comultiplication structures on A:

$$m(x^i \otimes x^j) = \begin{cases} x^{i+j}, & \text{if } i + j < p \\ 0, & \text{if } i + j \geq p \end{cases} \quad \Delta(x^i) = \Delta(x)^i = (x \otimes 1 + 1 \otimes x)^i = \sum_{j=0}^{i} \binom{i}{j} x^i \otimes x^{i-j}.$$

Let $\{y_0, y_1, \ldots, y_{p-1}\}$ be the dual basis to $\{1, x, \ldots, x^{p-1}\}$. Then

$$\begin{aligned} m_{A^\vee}(y_i \otimes y_j)(x^k) &= (y_i \otimes y_j)\Delta(x^k) \\ &= (y_i \otimes y_j) \sum_{\ell=0}^{k} \binom{k}{\ell} x^\ell \otimes x^{k-\ell} \\ &= \begin{cases} \binom{i+j}{i}, & \text{if } k = i + j \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

So $m_{A^\vee}(y_i \otimes y_j) = \binom{i+j}{i} y_{i+j}$. Rescaling, we can write this as $m_{A^\vee}(i!y_i \otimes j!y_j) = (i+j)!y_{i+j}$, which looks just like the original algebra structure. Define

$$f : A^\vee \longrightarrow A,\ y_i \longmapsto \frac{x^i}{i!}.$$

(This is sometimes called the *divided power map.*) Then f is an isomorphism of Hopf algebras and hence $\alpha_p^\vee = \alpha_p$.

Example 1.4.5. In characteristic $p > 0$, there are three group schemes of order p:

$$\underline{\mathbb{Z}/p\mathbb{Z}}, \qquad \mu_p, \quad \text{and} \quad \alpha_p$$

no two of which are isomorphic. Indeed, $\alpha_p^\vee = \alpha_p$ but $\underline{\mathbb{Z}/p\mathbb{Z}}^\vee = \mu_p$ and $\mu_p^\vee = \underline{\mathbb{Z}/p\mathbb{Z}}$, and $\underline{\mathbb{Z}/p\mathbb{Z}}$ is an étale group scheme so it can't be isomorphic to α_p.

Proposition 1.4.6. *For any finite commutative group scheme G and k-algebra R, there is a pairing*

$$G^\vee(R) \times G(R) \longrightarrow R^\times.$$

Proof. When $R = k$ and $G = \operatorname{Spec} A$, this comes from identifying $\operatorname{Hom}_k(G, \mathbb{G}_m)$ as the group of characters of G. On the level of group schemes,

$$\operatorname{Hom}_{\mathtt{GpSch}_k}(G, \mathbb{G}_m) = \operatorname{Hom}_{\mathtt{Hopf}_k}(k[x, x^{-1}], A)$$

which is the set of invertible grouplike elements of A (an element $a \in A$ is *grouplike* if $\Delta(a) = a \otimes a$). Thus one can regard grouplike elements as analogues of characters for group schemes. Similarly,

$$G(k) = \operatorname{Hom}_{\mathtt{Alg}_k}(A, k) \hookrightarrow \operatorname{Hom}_{\mathtt{Vect}_k}(A, k) = A^\vee$$

can be characterized as the set of all invertible grouplike elements in $A^\vee$. Thus any $f \in G(k)$ determines a group homomorphism $\chi_f : G^\vee(k) \to k^\times$. This also respects multiplication in $G(k)$, so we have defined a pairing

$$G^\vee(k) \times G(k) \longrightarrow k^\times.$$

Now for any k-algebra R, we have $G(R) = \operatorname{Hom}_{\mathtt{Alg}_k}(A, R) = \operatorname{Hom}_{\mathtt{Alg}_R}(A \otimes_k R, R)$. But there is a map

$$\operatorname{Hom}_{\mathtt{Alg}_k}(A, R) \longrightarrow \operatorname{Hom}_{\mathtt{Vect}_k}(A, R) = \operatorname{Hom}_{\mathtt{Vect}_k}(A, k) \otimes_k R = A^\vee \otimes_k R.$$

Write $A_R^\vee = A^\vee \otimes_k R$. We also have an embedding $G(R) \hookrightarrow A_R^\vee$ whose image is the invertible grouplike elements in $A_R^\vee$. Meanwhile, $\operatorname{Hom}_{\mathtt{Hopf}_R}(k[x, x^{-1}] \otimes_k R, A_R)$ can be identified as the invertible grouplike elements of A_R. Combining these, any element $f \in G(R)$ determines an invertible grouplike element $\chi_f \in A_R^\vee$ which is a group homomorphism $G^\vee(R) \to R^\times$. One checks compatibility with multiplication, resulting in a pairing

$$G^\vee(R) \times G(R) \longrightarrow R^\times$$

as desired. □

Corollary 1.4.7. *For any finite commutative group scheme G, there is a morphism of group schemes*

$$G^\vee \times G \longrightarrow \mathbb{G}_m.$$

Proof. The pairings $G^\vee(R) \times G(R) \to R^\times$ are functorial in R, so apply Yoneda's lemma (Theorem 1.1.1). □

Remark. This pairing $G^\vee \times G \to \mathbb{G}_m$ also corresponds to the Hopf algebra homomorphism

$$\begin{aligned} k[x, x^{-1}] &\longrightarrow A^\vee \otimes A \cong \mathrm{End}_k(A) \\ x &\longmapsto c := \sum_{i=1}^{n} e_i^\vee \otimes e_i \end{aligned}$$

where $\{e_i\}$ is a k-basis of A and $\{e_i^\vee\}$ is the dual basis. Notice that for any k-algebra R, this induces

$$\begin{aligned} (G^\vee \times G)(R) \cong G^\vee(R) \times G(R) &\longrightarrow \mathbb{G}_m(R) = R^\times \\ (\varphi, f) &\longmapsto \langle \varphi, f \rangle := \varphi(f). \end{aligned}$$

Supose G is a group scheme of order n. For $m \in \mathbb{Z}$, define the map $[m] : G \to G$ induced by $g \mapsto g^m$ on R-points. Then, using Cartier duality, one can show that $[n] : G \to G$ is the trivial map.

2 Abelian Varieties

In Chapter 1, all of our examples of group schemes were affine varieties. There are many examples of projective group schemes, although they will behave quite differently from the affine ones. This chapter surveys some of the basic theory of abelian varieties, which are the main non-affine group schemes of interest in arithmetic geometry.

Definition. *An* **abelian variety** *is a complete, connected group variety over k.*

For an abelian variety A, let $m : A \times A \to A$ denote the multiplication map, $i : A \to A$ the inversion map and $0_A \in A(k)$ the identity (as a k-point).

Remark. An abelian variety is always projective and nonsingular. To see the latter, note that any connected variety contains a dense open nonsingular locus, but when the variety is a group variety, the multiplication map allows us to move around this nonsingular locus and cover every point.

Theorem 2.0.1 (Rigidity)**.** *Suppose $\alpha : V \times W \to U$ is a regular map of k-varieties, where V is complete, $V \times W$ is geometrically irreducible and there are points $u_0 \in U(k), v_0 \in V(k), w_0 \in W(k)$ such that $\alpha(\{v_0\} \times W) = \{u_0\} = \alpha(V \times \{w_0\})$. Then α is constant, i.e. $\alpha(V \times W) = \{u_0\}$.*

Proof. First, the assumption that $V \times W$ is irreducible implies $V \times W$ is connected, so therefore V itself is connected. Next, the assumption that V is complete means the projection $q : V \times W \to W$ is closed. Third, since V is complete and connected and U is affine, α must be constant on V, i.e. for *any* $w \in W$, $\alpha(V \times \{w\}) = \{*\}$. Choose an open neighborhood $U_0 \subseteq U$ of u_0 and write $Z = q(\alpha^{-1}(U \setminus U_0))$; by the second observation above, Z is closed. Moreover, $w_0 \notin Z$, so $W \setminus Z$ is nonempty and open. For every $w \in W \setminus Z$, we have $\alpha(V \times \{w\}) \subseteq U_0$, so by the third observation above, $\alpha(V \times \{w\}) = \{u_0\}$. This shows $\alpha(V \times (W \setminus Z)) = \{u_0\}$, but $V \times (W \setminus Z)$ is a nonempty open subset of $V \times W$ and $V \times W$ is irreducible, so $V \times (W \setminus Z)$ is dense in $V \times W$. It follows then that $\alpha(V \times W) = \{u_0\}$ as required. □

Corollary 2.0.2. *Any regular map $\varphi : A \to B$ between abelian varieties is the composition of a group homomorphism and a translation.*

Proof. After composing with a translation, we may assume $\varphi(0_A) = 0_B$. Define a map

$$\alpha : A \times A \longrightarrow B, \quad (a, a') \longmapsto \varphi(m(a, a')) - \varphi(a) - \varphi(a').$$

Then we need to show $\alpha(A \times A) = \{0_B\}$. Notice that $\alpha(\{0_A\} \times A) = \{0_B\} = \alpha(A \times \{0_B\})$ by construction. Since φ is regular, so is α, so the rigidity theorem implies α is indeed the constant map on 0_B. □

Corollary 2.0.3. *Every abelian variety is a commutative group variety.*

Proof. The inversion map $i : A \to A$ is regular by definition and it sends $0_A \mapsto 0_A$, so by Corollary 2.0.2, i is a homomorphism. Thus for every $a, b \in A$, $i(m(a, b)) = m(i(a), i(b))$, which implies m is commutative. □

Remark. The rigidity theorem and Corollary 2.0.2 generalize to say that for any regular map $\alpha : G \to A$, where G is a group variety and A is an abelian variety, α is the composition of a group homomorphism and a translation.

2.1 Morphisms of Abelian Varieties

Let A be an abelian variety over a field k.

Example 2.1.1. For every $m \in \mathbb{Z}$, there is a regular map $[m] : A \to A$, induced by sending $1 \mapsto m1$. If $\operatorname{char} k = 0$, then often these are all the endomorphisms of A, i.e. $\operatorname{End}(A) = \mathbb{Z}$. However, in positive characteristic things are radically different.

Example 2.1.2. The projective closure in $\mathbb{P}^2$ of the affine equation $y^2 = x^3 - x$ defines an abelian variety E called an *elliptic curve* (see Section 2.2) which has an "extra automorphism" given by

$$[i] : E \longrightarrow E, \quad (x, y) \longmapsto (-x, iy).$$

Notice that $[i]^2 = [-1]$, and one can show that this is the only additional endomorphism, that is, $\operatorname{End}(E) = \mathbb{Z}[i]$. We say that an elliptic curve E has *complex multiplication* if $\operatorname{End}(E) \neq \mathbb{Z}$.

Recall the following definition from basic algebraic geometry.

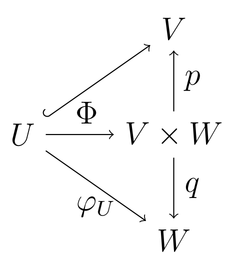
Definition. *If V and W are k-varieties, a* **rational map** $V \dashrightarrow W$ *is an equivalence class of pairs (U, φ_U) consisting of a dense open subset $U \subseteq V$ and a regular map $\varphi_U : U \to W$, where two pairs (U, φ_U) and $(U', \varphi_{U'})$ are said to be equivalent if $\varphi_U|_{U \cap U'} = \varphi_{U'}|_{U \cap U'}$.*

Theorem 2.1.3. *A rational map $\alpha : V \dashrightarrow A$, from a nonsingular variety V to an abelian variety A, always extends to a regular map $V \to A$.*

This follows from the following two lemmas.

Lemma 2.1.4. *A rational map $\varphi : V \dashrightarrow W$, from a normal variety V to a complete variety W, is defined (i.e. regular) on an open subset $U \subseteq V$ whose complement has codimension at least* 2.

Proof. We will show this for curves; for higher dimensional varieties, one can show the result by induction. Pick a representative $\varphi_U : U \to W$ which is regular and consider the diagram



Here, Φ is obtained from φ_U by changing targets and p and q are the coordinate projections. Set $U' = \Phi(U)$ and let Z be the closure of Z in $V \times W$. Since W is complete, $p(Z)$ is closed in V, but U is dense in V so $p(Z) = V$. Also, p maps U' isomorphically onto U, but since Z and V are curves, $p : Z \to V$ is also an isomorphism. Define $\varphi = q \circ p^{-1} : V \xrightarrow{\sim} Z \to W$. Then φ is regular and $\varphi|_U = \varphi_U$ by construction. □

Lemma 2.1.5. *If $\varphi : V \dashrightarrow G$ is a rational map from a nonsingular variety V to a group variety G, then either φ is regular or the subset where φ is not defined is closed of pure codimension* 1.

Proof. Consider the rational map $\psi : V \times V \dashrightarrow G$ given by $(x, y) \mapsto \varphi(x)\varphi(y)^{-1}$ where this element is defined. Then φ is defined at $x \in V$ if and only if ψ is defined at (x, x), and $\psi(x, x) = 1_G$. The comorphism of ψ restricts to $\psi^* : \mathcal{O}_{G,1_G} \to k(V \times V)$ and ψ is defined at (x, x) if and only if $\operatorname{im}\psi^* \subseteq \mathcal{O}_{V\times V,(x,x)}$. By definition, the stalk $\mathcal{O}_{V\times V,(x,x)}$ consists of those rational functions $f \in k(V \times V)$ whose divisor of poles $\operatorname{div}(f)_\infty$ is supported away from (x, x). Thus for φ to fail to be defined at x, there would need to exist some $f \in \operatorname{im}\psi^*$ such that (x, x) appears in $\operatorname{div}(f)_\infty$, or in other words, $(x, x) \in \Delta \cap \operatorname{supp}(\operatorname{div}(f)_\infty)$ where $\Delta \subseteq V \times V$ is the diagonal. On the other hand, it's easy to see that if $(x, x) \in \Delta \cap \operatorname{supp}(\operatorname{div}(f)_\infty)$, then φ is not defined at x. Now $\Delta \cap \operatorname{supp}(\operatorname{div}(f)_\infty)$ is a closed subset of pure codimension 1 inside $\Delta \subseteq V \times V$ (it is divisorial). This proves that the indeterminate locus of φ has pure codimension 1. □

Definition. *Two varieties V and W are said to be* **birationally equivalent** *if there are rational maps $V \dashrightarrow W$ and $W \dashrightarrow V$ which are inverses on their sets of definition.*

Example 2.1.6. Let E be the affine curve with equation $y^2 = x^3$. Then $\varphi : \mathbb{A}^1 \dashrightarrow E, t \mapsto (t^2, t^3)$ is a birational equivalence that does not extend to an isomorphism of varieties.

Example 2.1.7. Every blowup is a birational equivalence.

Theorem 2.1.8. *If two abelian varieties are birationally equivalent, then they are isomorphic as abelian varieties.*

Proof. Suppose $\varphi : A \dashrightarrow B$ is a birational equivalence of abelian varieties, say with rational inverse $\psi : B \dashrightarrow A$. By Theorem 2.1.3, φ extends to a regular map $\overline{\varphi} : A \to B$, as does ψ, say to $\overline{\psi} : B \to A$. Since $\overline{\varphi}$ and $\overline{\psi}$ are inverses on dense open subsets of A and B, they are inverses on all of A and B. Hence $\overline{\varphi}$ is an isomorphism of varieties, so by Corollary 2.0.2, it is the composition of a group homomorphism and a translation. In other words, $\overline{\varphi}$ itself need not be an isomorphism, but after composing with a translation, there *is* an isomorphism $A \cong B$ as abelian varieties. □

Proposition 2.1.9. *For an abelian variety A, every rational map $\mathbb{A}^1 \dashrightarrow A$ and $\mathbb{P}^1 \dashrightarrow A$ is constant. In particular, A is not rational.*

Proof. Suppose $\alpha : \mathbb{A}^1 \dashrightarrow A$ is rational. By Theorem 2.1.3 and Corollary 2.0.2, we may assume $\alpha : \mathbb{A}^1 \to A$ is regular with $\alpha(0) = 0_A$. Then for all $x, y \in \mathbb{A}^1(k)$, $\alpha(x + y) = \alpha(x) + \alpha(y)$. On the other hand, α restricts to a regular map $\alpha|_{\mathbb{G}_m} : \mathbb{G}_m \to A$, where $\mathbb{G}_m$ is viewed as the set of nonzero points in $\mathbb{A}^1$. But $\mathbb{G}_m$ is a group variety under multiplication, so by Corollary 2.0.2, $\alpha|_{\mathbb{G}_m}(xy) = \alpha(x) + \alpha(y) + \alpha(c)$ for some $c \in \mathbb{A}^1(k)$. Taking $y = -x$ shows these can't both be true simultaneously unless α is a constant. The proof for a rational map to $\mathbb{P}^1$ is similar. □

2.2 Elliptic Curves

In this section, we review the theory of elliptic curves, one of the most important examples of abelian varieties.

Definition. *An* **elliptic curve** *over a field k is a pair (E, O) where E is a smooth algebraic k-curve of genus 1 and O is a k-rational point of E.*

Using Riemann–Roch, one can show that the linear system $|3O|$ determines an embedding $E \hookrightarrow \mathbb{P}^2$. An equation

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

defining X in $\mathbb{P}^2$ is called a *Weierstrass equation* of X. If $\operatorname{char} k \neq 2, 3$, E can be given by a *short Weierstrass form*

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

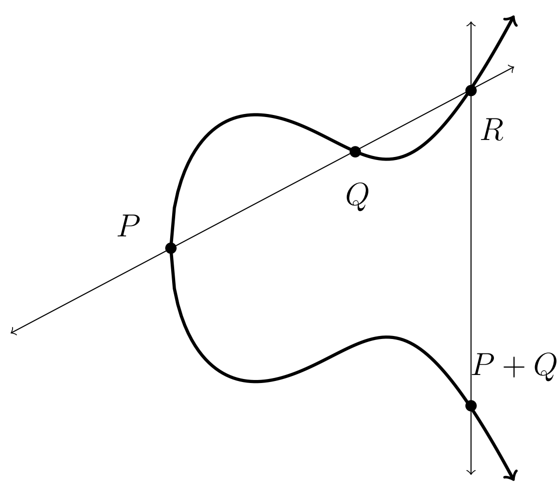
Here, the fixed point O corresponds to $[0, 1, 0] \in \mathbb{P}^2$. Given a Weierstrass equation, it is also natural to ask if it defines an elliptic curve.

Definition. *Let $y^2 = x^3 + Ax + B$ be a short Weierstrass form. Then the number $\Delta = -16(4A^3 + 27B^2)$ is called the* **discriminant** *of the Weierstrass equation.*

One can show that a Weierstrass equation defines an elliptic curve if and only if $\Delta \neq 0$.

By studying the arc length of an ellipse and related shapes, giving rise to elliptic functions, mathematicians such as Abel, Jacobi and Weierstrass discovered that the points on an elliptic curve can be "added" in a certain way so as to define a group structure. Geometrically, this group structure may be realized as the so-called "chord-and-tangent method".

Let E be an elliptic curve over k, let $O \in E(k)$ and fix two points $P, Q \in E(k)$. In the plane $\mathbb{P}^2$, there is a unique line containing P and Q; call it L. (If $P = Q$, then take $L = T_PE$, the tangent line at P.) Then by Bézout's theorem, $E \cap L = \{P, Q, R\}$ for some third point $R \in E(k)$, which may not be distinct from P and Q if multiplicity is counted. Let L' be the line through R and O and call its third point R'.



Definition. *Addition of two points $P, Q \in E(k)$ is defined by $P + Q = R'$, where R' is the unique point lying on the line through R and O. If $R = O$, we set $R' = O$.*

There are also explicit coordinate formulas describing the addition law on $E(k)$. In any case, one can show, with some work, that this operation, plus the inversion $(x, y) \mapsto (x, -y)$ and identity O, makes $E(k)$ into a group. Furthermore:

Theorem 2.2.1. *An elliptic curve E is a commutative group variety.*

Proof. Let $m : E \times E \to E$ denote the addition law. Since E is smooth and projective, the rational map $(x, y) \mapsto (x, -y)$ is automatically regular. On the other hand, for any point $Q \in E(k)$, the map $r_Q : E \to E$ sending $P \mapsto m(P, Q)$ is also rational, so by the same argument, r_Q is regular. In fact, composing with the inversion map gives an inverse to r_Q, so it is even an isomorphism. Now for fixed $Q_1, Q_2 \in E(k)$, consider the composition

$$E \times E \xrightarrow{r_{Q_1} \times r_{Q_2}} E \times E \xrightarrow{m} E \xrightarrow{r_{Q_1}^{-1}} E \xrightarrow{r_{Q_2}^{-1}} E$$

sending $(P, Q) \mapsto (P + Q_1, Q + Q_2) \mapsto P + Q_1 + Q + Q_2 \mapsto P + Q + Q_2 \mapsto P + Q$. Note that m and φ agree where both are defined and rational, namely:

- m is rational away from $(P, P), (P, -P), (P, O)$ and (O, P); and
- φ is rational away from $(P - Q_1, P - Q_2), (P - Q_2, -P - Q_2), (P - Q_1, -Q_2)$ and $(-Q_1, P - Q_2)$.

However, we can choose a finite number of pairs $(Q_{i1}, Q_{i2})_{i=1}^n$ and $\varphi_i = \varphi_{Q_{i1}Q_{i2}}$ as above such that each φ_i is rational, $\varphi_i = \varphi_j$ on overlaps and for every point of $E(k)$, there is some φ_i defined at the point. Then m is represented as a regular map (globally on E) by the φ_i. □

Complex elliptic curves can be studied fruitfully from many different angles, which lead to important results in their basic structure theory. For example, we will see in a moment that there is a dictionary between elliptic curves and lattices in $\mathbb{C}$ that better reflects the group structure than the coordinate approach can (especially when it comes to showing associativity).

Let $\Lambda \subseteq \mathbb{C}$ be a lattice, i.e. a free abelian subgroup of rank 2. Then Λ can be written

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \quad \text{for some } \omega_1, \omega_2 \in \mathbb{C} \text{ such that } \frac{\omega_1}{\omega_2} \notin \mathbb{R}.$$

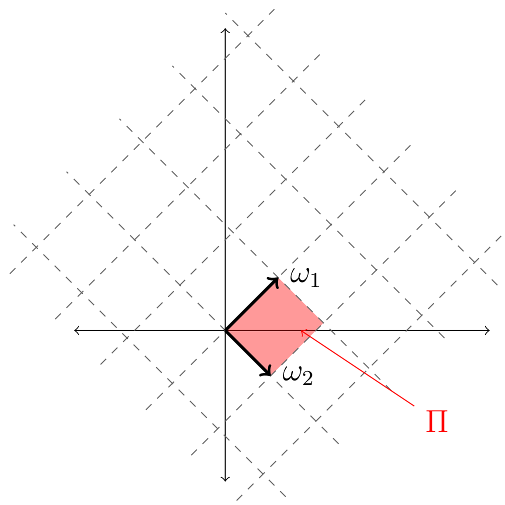
Definition. *A function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is* **doubly periodic** *with* **lattice of periods** Λ *if $f(z + \ell) = f(z)$ for all $\ell \in \Lambda$ and $z \in \mathbb{C}$.*

Definition. *An* **elliptic function** *is a function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ that is meromorphic and doubly periodic.*

Definition. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice. The set*

$$\Pi = \Pi(\omega_1, \omega_2) = \{t_1\omega_1 + t_2\omega_2 \mid 0 \le t_i < 1\}$$

is called the **fundamental parallelogram** *of Λ. We say a subset $\Phi \subseteq \mathbb{C}$ is a* **fundamental domain** *for Λ if the quotient map $\mathbb{C} \to \mathbb{C}/\Lambda$ restricts to a bijection on Φ.*



Lemma 2.2.2. *Let Λ be a lattice. Then*

(a) If Π is the fundamental domain of Λ, then for any $\alpha \in \mathbb{C}$, $\Pi_\alpha := \Pi + \alpha$ is fundamental for Λ.

(b) If Φ is fundamental for Λ, then $\mathbb{C} = \bigcup_{\ell \in \Lambda} \Phi + \ell$.

Corollary 2.2.3. *Suppose f is an elliptic function with lattice of periods Λ and Φ fundamental for Λ. Then $f(\mathbb{C}) = f(\Phi)$.*

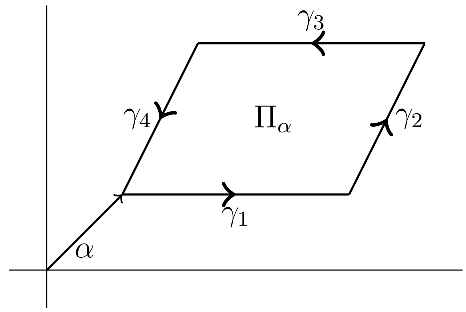
Proposition 2.2.4. *A holomorphic elliptic function is constant.*

Proof. Let f be such an elliptic function and let Φ be the fundamental domain for its lattice of periods. Then $\overline{\Pi}$ is compact and hence $f(\overline{\Pi})$ is as well. In particular, $f(\mathbb{C}) = f(\Pi) \subseteq f(\overline{\Pi})$ is bounded, so by Liouville's theorem, f is constant. □

Proposition 2.2.5. *Let f be an elliptic function. If $\alpha \in \mathbb{C}$ is a complex number such that $\partial\Pi_\alpha$ does not contain any of the poles of f, then the sum of the residues of f inside Π_α equals 0.*

Proof. Fix a basis $[\omega_1, \omega_2]$ of Λ and set $\Delta = \partial\Pi_\alpha$. By the residue theorem, it's enough to show $\int_\Delta f(z)\,dz = 0$. We parametrize the boundary of Π as follows:

$$\begin{aligned}
\gamma_1 &= \alpha + t\omega_1 \\
\gamma_2 &= \alpha + \omega_1 + t\omega_2 \\
\gamma_3 &= \alpha + (1-t)\omega_1 + \omega_2 \\
\gamma_4 &= \alpha + (1-t)\omega_2.
\end{aligned}$$



We show that $\int_{\gamma_1} f(z)\,dz + \int_{\gamma_3} f(z)\,dz = 0$ and leave the proof that $\int_{\gamma_2} f(z)\,dz + \int_{\gamma_2} f(z)\,dz = 0$ for exercise. Consider

$$\begin{aligned}\int_{\gamma_1} f(z)\,dz + \int_{\gamma_3} f(z)\,dz &= \int_0^1 f(\alpha + t\omega_1)(\omega_1\,dt) + \int_0^1 f(\alpha + (1-t)\omega_1 + \omega_2)(-\omega_1\,dt) \\ &= \omega_1 \int_0^1 f(\alpha + t\omega_1)\,dt + \omega_1 \int_1^0 f(\alpha + s\omega_1)\,ds \quad \text{since } f \text{ is elliptic} \\ &= \omega_1 \left(\int_0^1 f(\alpha + t\omega_1)\,dt - \int_0^1 f(\alpha + s\omega_1)\,ds \right) = 0.\end{aligned}$$

Hence the sum of the residues equals 0. □

Corollary 2.2.6. *Any elliptic function has either a pole of order at least 2 or two poles on the fundamental domain of its lattice of periods.*

Proposition 2.2.7. *Suppose f is an elliptic function with fundamental domain Π and $\alpha \in \mathbb{C}$ such that $\Delta = \partial\Pi_\alpha$ does not contain any zeroes or poles of f. Let $\{a_j\}_{j=1}^n$ be a finite set of zeroes and poles in Π_α, with m_j the order of the pole a_j. Then $\sum_{j=1}^n m_j = 0$.*

Proof. For a pole z_0, we can write $f(z) = (z - z_0)^m g(z)$ for some holomorphic function $g(z)$, with $g(z_0) \neq 0$. Then

$$\frac{f'(z)}{f(z)} = (z - z_0)^{-1} \left(m + (z - z_0)\frac{g'(z)}{g(z)} \right).$$

Hence $\operatorname{Res}\left(\frac{f'}{f}; z_0\right) = m$. Then the statement follows from Proposition 2.2.5. □

Proposition 2.2.8. *If f is elliptic as above and $\alpha \in \mathbb{C}$ such that Δ_α contains no zeroes or poles of f, then $\sum_{j=1}^n m_j a_j \equiv 0 \mod \Lambda$.*

Remark. Conversely, given any collection of points $a_j \in \mathbb{C}$ and integers $m_j \in \mathbb{Z}$, if $\sum_{j=1}^n m_j a_j \equiv 0 \mod \Lambda$ then there exists a meromorphic function f with (a_j, m_j) as its precise list of zeroes/poles together with their orders. We will prove this in Section 2.3.

Lemma 2.2.9. *If f is elliptic and $z_0 \in \mathbb{C}$ is a zero (resp. pole) of f of order m, then for any $\lambda \in \Lambda$, $z_0 + \lambda$ is also a zero (resp. pole) of f of order m.*

Corollary 2.2.10. *Suppose $\Phi \subseteq \mathbb{C}$ is a fundamental domain for Λ and f is an elliptic function with $(a_j, m_j)_{j=1}^n$ the finite list of zeroes and poles of f in Φ, together with their multiplicities. Then $\sum_{j=1}^n m_j = 0$ and $\sum_{j=1}^n m_j a_j \equiv 0 \mod \Lambda$.*

Proposition 2.2.11. *Suppose $\Phi \subseteq \mathbb{C}$ is a fundamental domain for Λ and $\{a_i'\}$ (resp. $\{a_i''\}$) are the zeroes (resp. poles) of f in Φ. Let a_i' have order $m_i' > 0$ and a_i'' have order $m_i'' < 0$. Then $\sum m_i' = -\sum m_i'' = n$ for a fixed integer $n \in \mathbb{Z}$, called the order of f. Moreover, for any $c \in \mathbb{C}$, the function $f(z) - c$ has precisely n zeroes in Φ.*

This leads to the construction of the Weierstrass $\wp$-function for a lattice, our first example of an elliptic function.

Definition. *The* **Weierstrass $\wp$-function** *for a lattice Λ is defined by*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left[\frac{1}{(z-w)^2} - \frac{1}{\omega^2}\right].$$

Theorem 2.2.12. *For any lattice Λ, $\wp(z)$ is an even elliptic function with poles of order 2 at the points of Λ and no other poles. Moreover, $\wp(-z) = \wp(z)$ and $\wp'(z) = -2F_3(z)$, where*

$$F_3(z) = \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

which is also elliptic.

Proof. (Sketch) To show $\wp(z)$ is meromorphic, one estimates the summands by

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| \leq \frac{D}{|\omega|^3}$$

for some constant D and all $z \in B_r, \omega \in \Lambda \smallsetminus \Lambda_r$ as in the previous proof.

Next, $\wp(z)$ can be differentiated term-by-term to obtain the expression $\wp'(z) = -2F_3(z)$. And proving that $\wp(z)$ is odd is straightforward:

$$\begin{aligned}\wp(-z) &= \frac{1}{(-z)^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left[\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2}\right] \\ &= \frac{1}{z^2} + \sum_{-\omega \in \Lambda \smallsetminus \{0\}} \left[\frac{1}{(z-(-\omega))^2} - \frac{1}{(-\omega)^2}\right] = \wp(z)\end{aligned}$$

after switching the order of summation.

Finally, proving $\wp(z)$ is doubly periodic is difficult since we don't necessarily have absolute convergence. However, one can reduce to proving $\wp(z+\omega_1) = \wp(z) = \wp(z+\omega_2)$. Then using the formula for $\wp'(z)$, we have

$$\begin{aligned}\frac{d}{dz}[\wp(z+\omega_1) - \wp(z)] &= -2F_3(z+\omega_1) + 2F_3(z) \\ &= -2F_3(z) + 2F_3(z) = 0\end{aligned}$$

since $F_3(z)$ is elliptic. Hence $\wp(z+\omega_1) - \wp(z) = c$ is constant. Evaluating at $z = -\frac{\omega_1}{2}$, we see that $c = \wp\left(\frac{\omega_1}{2}\right) - \wp\left(-\frac{\omega_1}{2}\right) = 0$ since $\wp(z)$ is odd. Hence $c = 0$, so it follows that $\wp(z)$ is doubly periodic and therefore elliptic. $\square$

Lemma 2.2.13. *Let $\wp(z)$ be the Weierstrass $\wp$-function for a lattice $\Lambda \subseteq \mathbb{C}$ and let Π be the fundamental domain of Λ. Then*

(1) For any $u \in \mathbb{C}$, the function $\wp(z) - u$ has either two simple roots or one double root in Π.

(2) The zeroes of $\wp'(z)$ in Π are simple and they only occur at $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$.

(3) The numbers $u_1 = \wp\left(\frac{\omega_1}{2}\right), u_2 = \wp\left(\frac{\omega_2}{2}\right)$ and $u_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$ are precisely those u for which $\wp(z) - u$ has a double root.

Proof. (1) follows from Corollary 2.2.6.

(2) By Theorem 2.2.12, $\deg \wp'(z) = 3$ so it suffices to show that $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are all roots. For $z = \frac{\omega_1}{2}$, we have

$$\wp'\left(\frac{\omega_1}{2}\right) = -\wp'\left(-\frac{\omega_1}{2}\right) = -\wp'\left(\frac{\omega_1}{2} - \omega_1\right) = -\wp'\left(\frac{\omega_1}{2}\right)$$

since $\wp'(z)$ is elliptic. Thus $\wp'\left(\frac{\omega_1}{2}\right) = 0$. The others are similar.

(3) The double roots occur exactly when $\wp'(u) = 0$, so use (2). □

We now prove that any elliptic function can be written in terms of $\wp(z)$ and $\wp'(z)$.

Theorem 2.2.14. *Fix a lattice $\Lambda \subseteq \mathbb{C}$ and let $\mathcal{E}(\Lambda)$ be the field of all elliptic functions with lattice of periods Λ. Then $\mathcal{E}(\Lambda) = \mathbb{C}(\wp, \wp')$.*

Proof. Take $f(z) \in \mathcal{E}(\Lambda)$. Then $f(-z) \in \mathcal{E}(\Lambda)$ as well and thus we can write $f(z)$ as the sum of an even and an odd elliptic function:

$$f(z) = f_{even}(z) + f_{odd}(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

We will prove that every even elliptic function is rational in $\wp(z)$, but this will imply the theorem, since then $f_{even}(z) = \varphi(\wp(z))$ and $\frac{f_{odd}(z)}{\wp'(z)} = \psi(\wp(z))$ for some $\varphi, \psi \in \mathbb{C}(\wp(z))$ and we can then write $f(z) = \varphi(\wp(z)) + \wp'(z)\psi(\wp(z))$.

Assume $f(z)$ is an even elliptic function. It's enough to construct $\varphi(\wp(z))$ such that $\frac{f(z)}{\varphi(\wp(z))}$ only has (potential) zeroes and poles at $z = 0$ in the fundamental parallelogram for Λ, since then by Corollary 2.2.6, $\frac{f(z)}{\varphi(\wp(z))}$ is holomorphic and then by Proposition 2.2.4 it is constant. Suppose $f(a) = 0$ for a some zero of order m. Consider $\wp(z) = u$. If $u \neq \wp\left(\frac{\omega_1}{2}\right), \wp\left(\frac{\omega_2}{2}\right), \wp\left(\frac{\omega_1+\omega_2}{2}\right)$ then $\wp(z) = u$ has precisely two solutions in the fundamental parallelogram, $z = a$ and $z = a^*$ where

$$a^* = \begin{cases} \omega_1 + \omega_2 - a & \text{if } a \in \mathrm{Int}(\Pi) \\ \omega_1 - a & \text{if } a \text{ is parallel to } \omega_1 \\ \omega_2 - a & \text{if } a \text{ is parallel to } \omega_2. \end{cases}$$

(Notice that since f is even, $f(a) = 0$ implies $f(a^*) = 0$ as well.) Moreover, if $\mathrm{ord}_a f = 0$ then $\mathrm{ord}_{a^*} f = m$. Note that $a = a^*$ holds precisely when a is in the set $\Theta := \left\{0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\right\}$.

Let Z (resp. P) be the set of zeroes (resp. poles) of $f(z)$ in Π. Then the assignment $a \mapsto a^*$ is in fact an involution on Z and P, so we can write

$$Z = Z_1' \cup \cdots \cup Z_r' \cup Z_1'' \cup \cdots \cup Z_s''$$
$$P = P_1' \cup \cdots \cup P_u' \cup P_1'' \cup \cdots \cup P_v''$$

where the Z_i' and P_i' are the 2-element orbits of the involution and the Z_j'' and P_j'' are the 1-element orbits. Of course then $s, v \le 3$. For $a_i' \in Z_i'$, set $\operatorname{ord}_{a_i'} f = m_i'$ and for $a_j'' \in Z_j''$, set $\operatorname{ord}_{a_i''} f = m_i''$, which is even. Likewise, for $b_i' \in P_i'$, set $\operatorname{ord}_{b_i'} f = n_i'$ and for $b_j'' \in P_j''$, set $\operatorname{ord}_{b_i''} f = n_i''$ which is even. Then we define $\varphi(\wp(z))$ by

$$\varphi(\wp(z)) = \frac{\prod_{i=1}^{r}(\wp(z) - \wp(a_i'))^{m_i'} \prod_{j=1}^{s}(\wp(z) - \wp(a_j''))^{m_j''/2}}{\prod_{i=1}^{u}(\wp(z) - \wp(b_i'))^{n_i'} \prod_{j=1}^{v}(\wp(z) - \wp(b_j''))^{n_j}}.$$

Then $\varphi(\wp(z))$ has only potential zeroes/poles at $z = 0$ in the fundamental parallelogram, so we are done. □

Definition. *The series* $G_m(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m}$ *is called the* **Eisenstein series** *for* Λ *of weight* m.

Proposition 2.2.15. *The functions* $\wp$ *and* $\wp'$ *satisfy the following relation:*

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

where $g_2 = 60G_4$ *and* $g_3 = 140G_6$.

Consider the polynomial $p(x) = 4x^3 - g_2x - g_3$, which is separable by Lemma 2.2.13. As a result, the equation $y^2 = 4x^3 - g_2x - g_3$ is the affine equation for an elliptic curve.

Theorem 2.2.16. *The map*

$$\varphi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$
$$z + \Lambda \longmapsto \varphi(z + \Lambda) = \begin{cases} [\wp(z), \wp'(z), 1], & z \notin \Lambda \\ [0, 1, 0], & z \in \Lambda \end{cases}$$

is a bijective, biholomorphic map.

Proof. Assume $z_1, z_2 \in \mathbb{C}$ are such that $z_1 + \Lambda \neq z_2 + \Lambda$. Without loss of generality we may assume $z_1, z_2 \in \Pi$, the fundamental domain of Λ (otherwise, translate). If $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$, then with the notation of Theorem 2.2.14, we must have $z_2 = z_1^* \neq z_1$ and thus $z_1, z_2 \notin \Theta = \left\{0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\right\}$. Since $\wp'(z)$ is odd, we get $\wp'(z_1) = \wp'(z_2) = -\wp'(-z_2) = -\wp'(z_1)$, but this implies $\wp(z_1) = 0$, contradicting $z_1 \notin \Theta$. Therefore φ is one-to-one.

Next, we must show that for any $(x_0, y_0) \in E(\mathbb{C})$, $x_0 = \wp(z)$ and $y_0 = \wp'(z)$ for some $z \in \mathbb{C}$. If $\wp(z_1) = x_0$, then it's clear that $\wp'(z_1) = y_0$ or $-y_0$. Now one shows as in the previous paragraph that we must have $\wp'(z_1) = y_0$.

Now consider $F(x, y) = y^2 - p(x)$, where $p(x) = 4x^3 - g_2x - g_3$. If (x_0, y_0) satisfies $F(x_0, y_0) = 0$ and $y_0 \neq 0$, then $\frac{\partial F}{\partial y}(x_0, y_0) \neq 0$ and thus the assignment $(x, y) \mapsto x$ is a local chart about (x_0, y_0). Likewise, $(x, y) \mapsto y$ defines a local chart about (x_0, y_0) when $x_0 \neq 0$. Finally, we conclude by observing that a locally biholomorphic map is biholomorphic. □

Theorem 2.2.17. *The map $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ is an isomorphism of abelian groups.*

Proof. Consider the diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda & \xrightarrow{\varphi \times \varphi} & E(\mathbb{C}) \times E(\mathbb{C}) \\ \alpha \big\downarrow & & \big\downarrow \beta \\ \mathbb{C}/\Lambda & \xrightarrow[\varphi]{} & E(\mathbb{C}) \end{array}$$

where α and β are the respective group operations. Since $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda$ is a topological group, it's enough to show the diagram commutes on a dense subset of $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda$. Consider

$$\widetilde{X} = \{(u_1, u_2) \in \mathbb{C}^2 \mid u_1, u_2, u_1 \pm u_2, 2u_1 + u_2, u_1 + 2u_2 \notin \Lambda\}.$$

Then $\widetilde{X} \cong \mathbb{C}^2$ so $X = \widetilde{X} \mod \Lambda \times \Lambda$ is dense in $\mathbb{C}/\Lambda \times \mathbb{C}/\Lambda$. Take $(u_1 + \Lambda, u_2 + \Lambda) \in X$ and set $u_3 = -(u_1 + u_2)$. Then $u_1 + u_2 + u_3 = 0$ in $\mathbb{C}/\Lambda$. Set $P = \varphi(u_1), Q = \varphi(u_2)$ and $R = \varphi(u_3) \in E(\mathbb{C})$. By the assumptions on X, the points P, Q, R are distinct. We want to show $\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2) = P + Q$. Since $\wp(z)$ is even and $\wp'(z)$ is odd, we see that $\varphi(-z) = -\varphi(z)$ for all $z \in \mathbb{C}/\Lambda$. Thus $\varphi(u_1 + u_2) = -\varphi(-(u_1 + u_2)) = -R$ so we need to show $P + Q + R = O$, i.e. P, Q, R are colinear. Since $u_1 \neq u_2$, the line $\overline{PQ}$ is not vertical, so there exist a, b such that $\wp'(u_i) = a\wp(u_i) + b$ for $i = 1, 2$. Consider the elliptic function

$$f(z) = \wp'(z) - (a\wp(z) + b).$$

Then on the fundamental domain Π, f only has a pole at 0, so $\operatorname{ord}_0 f = -3$. Also, u_1 and u_2 are distinct zeroes of f, so there is a third point $\omega \in \Pi$ such that $\deg(f) = u_1 + u_2 + \omega - 3 \cdot 0 = 0$, i.e. $u_1 + u_2 + \omega = 0$. Solving for ω, we get $\omega = -(u_1 + u_2) = u_3$. It follows that $R = \varphi(u_3)$ is on the same line as P and Q, so we are done. □

2.3 Theta Functions

Definition. *For an algebraic curve X, define:*

- *A* **divisor** *on X is a formal sum $D = \sum n_P P$ over the points $P \in X$, with $n_P \in \mathbb{Z}$. The abelian group of all divisors is denoted* $\operatorname{Div}(X)$*.*

- *The* **degree** *of a divisor $D = \sum n_P P \in \operatorname{Div}(X)$ is $\deg(D) = \sum n_P$. The set of all* **degree 0 divisors** *is denoted* $\operatorname{Div}^0(X)$*.*

- *For a meromorphic function f on $X(\mathbb{C})$, the* **principal divisor** *associated to f is $(f) = \sum \deg_P P$ where $n_P = \operatorname{ord}_P f$. The group of all principal divisors is denoted* $\operatorname{PDiv}(X)$*.*

- *The* **Picard group** *of X is the quotient group $\operatorname{Pic}(X) = \operatorname{Div}(X)/\operatorname{PDiv}(X)$. The degree zero part of the Picard group is written $\operatorname{Pic}^0(X) = \operatorname{Div}^0(X)/\operatorname{PDiv}(X)$.*

Note that $\mathrm{Pic}^0(X)$ is a well-defined quotient because $\mathrm{PDiv}(X) \subseteq \mathrm{Div}^0(X)$ (by Proposition 2.2.7 for elliptic curves and by an algebraic generalization for arbitrary curves). Theorem 2.2.17 can be restated as follows.

Theorem 2.3.1. *If E is an elliptic curve, then the map*

$$\begin{aligned} \mathrm{Pic}^0(E) &\xrightarrow{\sim} E(\mathbb{C}) \\ \left[\sum m_i a_i\right] &\longmapsto \sum m_i a_i \\ [P - O] &\longleftarrow P \end{aligned}$$

is an isomorphism.

Remark. More generally, there is an abelian variety $J(X)$ for any curve X and an isomorphism $\Phi : \mathrm{Pic}^0(X) \xrightarrow{\sim} J(X)$, called the *Abel–Jacobi isomorphism*.

Returning to the theory of lattices, let $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, with $\mathrm{im}(\tau) > 0$.

Definition. *The* **Jacobi theta function** *for Λ is the series*

$$\theta(z, \tau) = \sum_{n=-\infty}^{\infty} e^{\pi i(n^2\tau + 2nz)}.$$

Fixing τ, we will write $\theta(z) = \theta(z, \tau)$. One has $|e^{\pi i(n^2\tau+2nz)}| = e^{-\pi(n^2 \,\mathrm{im}\,\tau + 2n\,\mathrm{im}\,z)}$ for any $z \in \mathbb{C}$, which implies that $\theta(z)$ converges absolutely.

Proposition 2.3.2. *Fix a theta function $\theta(z) = \theta(z, \tau)$. Then*

(1) $\theta(z) = \theta(-z)$.

(2) $\theta(z + 1) = \theta(z)$.

(3) $\theta(z + \tau) = e^{-\pi i(\tau+2z)}\theta(z)$.

This says that $\theta(z)$ is a *modular function of weight* 1.

Remark. There are also weight k versions of theta functions, written $\theta_j(z), 1 \leq j \leq k$, satisfying functional equations

$$\theta_j(z + \tau) = e^{-\pi i k(\tau+2z)}\theta_j(z).$$

One can show that the weight k theta functions $\theta_1, \ldots, \theta_k$ are linearly independent, and they determine a map

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow \mathbb{P}^k \\ z &\longmapsto [\theta_1(z), \ldots, \theta_k(z)] \end{aligned}$$

which is injective if $k \geq 3$.

Lemma 2.3.3. $\theta\left(\frac{1+\tau}{2}\right) = 0$. *In particular, $\theta(z) = 0$ for all $z \in \frac{1+\tau}{2} + \Lambda$.*

Proof. We have:

$$\begin{aligned}\theta\left(\frac{1+\tau}{2}\right) &= \theta\left(-\frac{1+\tau}{2}+(1+\tau)\right) = e^{\pi i\left(\tau+2\left(-\frac{1+\tau}{2}\right)\right)}\theta\left(-\frac{1+\tau}{2}\right)\\ &= e^{\pi i}\theta\left(-\frac{1+\tau}{2}\right) = -\theta\left(\frac{1+\tau}{2}\right).\end{aligned}$$

□

One can show that all zeroes of $\theta(z)$, which we know are of the form $\frac{1+\tau}{2}+\lambda$ for $\lambda\in\Lambda$, are simple zeroes.

Lemma 2.3.4. *For $x\in\mathbb{C}$, set $\theta^{(x)}(z)=\theta\left(z-\frac{1+\tau}{2}-x\right)$. Then $\theta^{(x)}(z)$ satisfies:*

(1) $\theta^{(x)}(z+1)=\theta^{(x)}(z)$.

(2) $\theta^{(x)}(z+\tau)=e^{-\pi i(2(z-x)-1)}\theta^{(x)}(z)$.

We now give a converse to Corollary 2.2.10.

Theorem 2.3.5 (Abel)**.** *Suppose $\Lambda\subseteq\mathbb{C}$ is a lattice with fundamental domain Π and take any set $\{a_i\}\subset\Pi$ such that there are integers $m_i\in\mathbb{Z}$ satisfying $\sum m_i=0$ and $\sum m_ia_i\in\Lambda$. Then there exists an elliptic function $f(z)$ whose set of zeroes and poles is $\{a_i\}$ and whose orders of vanishing/poles are* $\operatorname{ord}_{a_i} f=m_i$.

Proof. Given such a set $\{a_i\}\subset\Pi$, let $x_1,\dots,x_n$ be the list of all a_i with $m_i>0$, listed with repetitions corresponding to the number m_i. For example, if $m_1=2$ then $x_1=x_2=a_1$. Likewise, let $y_1,\dots,y_n$ be the list of all a_i with $m_i<0$, once again with repetitions. By the hypothesis $\sum m_i=0$, there are indeed an equal number of each. Set

$$f(z)=\frac{\prod_{i=1}^n\theta^{(x_i)}(z)}{\prod_{i=1}^n\theta^{(y_i)}(z)}.$$

Then by Lemma 2.3.4, $f(z+1)=f(z)$. On the other hand, the lemma also gives

$$\begin{aligned}f(z+\tau) &= \frac{\prod_{i=1}^n\theta^{(x_i)}(z+\tau)}{\prod_{i=1}^n\theta^{(y_i)}(z)}\\ &= e^{2\pi i\left(\sum_{i=1}^n x_i-\sum_{i=1}^n y_i\right)}f(z)\\ &= e^{2\pi i\sum m_ia_i}f(z)\\ &= f(z)\quad\text{since }\sum m_ia_i=0.\end{aligned}$$

Therefore $f(z)$ is elliptic. □

To summarize, for an elliptic curve E coming from a lattice $\Lambda\subseteq\mathbb{C}$, we have a diagram

$$\begin{array}{ccc} & & E(\mathbb{C})\\ & \overset{\sim}{\swarrow} & \uparrow\\ \operatorname{Pic}^0(E) & \xrightarrow{\sim} & \mathbb{C}/\Lambda\end{array}$$

However, we don't yet have an explicit inverse to the map $\mathbb{C}/\Lambda\to E(\mathbb{C})$. This will be the subject of the next section.

2.4 Complex Jacobians

In this section, we construct the inverse of the map $\mathbb{C}/\Lambda \to E(\mathbb{C})$ for an elliptic curve E. In fact, we will generalize to any abelian variety A and construct a map $\mathbb{C}^g/\Lambda \to A(\mathbb{C})$ where g is the dimension of A.

Theorem 2.4.1. *If A is an complex abelian variety of dimension g, then $A(\mathbb{C})$ is a complex torus of the form $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ where $\Lambda \subseteq \mathbb{C}^g$ is a lattice of rank $2g$.*

Remark. We will take the following facts about a complex abelian variety A as given:

- A is a projective variety. In particular, there is a closed embedding of complex manifolds $A(\mathbb{C}) \hookrightarrow \mathbb{P}^n_{\mathbb{C}}$ for some n.
- Since A is smooth and irreducible, $A(\mathbb{C})$ is a compact, connected complex manifold.
- $A(\mathbb{C})$ has the structure of a complex Lie group. In particular, for any tangent vector $v \in T_0A$ there's a unique one-parameter subgroup $\varphi_v : \mathbb{C} \to A(\mathbb{C})$ determined by $d_0\varphi_v(1) = v$.
- There exists a unique holomorphic map
$$\exp : T_0A \longrightarrow A(\mathbb{C}),$$
the *exponential map*, such that for any $v \in T_0A$, the map φ_v from above factors as
$$\varphi_v : \mathbb{C} \xrightarrow{\lambda_v} T_0A \xrightarrow{\exp} A(\mathbb{C}),$$
where $\lambda_v : z \mapsto zv$. When A is an abelian variety, $\exp : T_0A \to A(\mathbb{C})$ is also a group homomorphism.

Example 2.4.2. For $A = \mathbb{C}^\times$, the exponential map $\exp : T_1A = \mathbb{C} \to \mathbb{C}^\times$ is the familiar exponential map
$$\exp(v) = \sum_{n=0}^{\infty} \frac{v^n}{n!}.$$
This definition extends to any linear algebraic group using the matrix exponential map.

We now prove Theorem 2.4.1.

Proof. Let g be the dimension of A. To show $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$, we will show that the exponential map $\exp : T_0A \to A(\mathbb{C})$ is surjective with kernel $\Lambda = \ker \exp$ a full lattice in $T_0A \cong \mathbb{C}^g$. Notice first that $d_0 \exp$ is the identity on T_0A. By the inverse function theorem, this means that locally about 0, exp is biholomorphic. Let $H = \operatorname{im} \exp \subseteq A(\mathbb{C})$. Then there's an open neighborhood U of 0 in T_0A such that $\exp : U \xrightarrow{\sim} \exp(U) =: V$ is biholomorphic. So $V \subseteq H$ is open, but if $a \in H$, the translate $V_a = V + a$ is an open neighborhood of a in H, which shows H is an open subgroup of $A(\mathbb{C})$. On the other hand, $A(\mathbb{C}) \smallsetminus H$ is just the union of the nontrivial cosets of H, hence also open, so H is also closed. By irreducibility, $H = A(\mathbb{C})$.

Next, we show $\Lambda = \ker \exp$ is a full lattice in T_0A. Since $A(\mathbb{C})$ is compact, it will be enough to show Λ is a lattice. By definition, Λ is a subgroup of T_0A, but it is also discrete: we saw above that for any $v \in T_0A$, there is a neighborhood $U \subseteq T_0A$ of v such that $U \cap \Lambda = \{0\}$. This completes the proof. $\square$

Corollary 2.4.3. $\exp : T_0A \to A(\mathbb{C})$ *is a universal cover of* $A(\mathbb{C})$ *as a complex manifold.*

Remark. We will see in later sections that, in contrast to the $g = 1$ case, not all complex tori of genus $g > 1$ determine abelian varieties.

2.5 Line Bundles and Riemann–Roch

Let X be a compact Riemann surface of genus g and $K = k(X)$ its field of meromorphic functions. Then K has transcendence degree 1 over $\mathbb{C}$, so $K = \mathbb{C}(z, f)$ for parameters z, f satisfying some polynomial relation $p(z, f) = 0$. This means X is also a smooth projective algebraic curve over $\mathbb{C}$. One can also show that $g = \dim_{\mathbb{C}} H^0(X, \Omega^1_{X/\mathbb{C}})$, where $\Omega^1_{X/\mathbb{C}}$ is the line bundle of meromorphic 1-forms on X. Let $\Omega[X]$ denote the full vector space of all meromorphic 1-forms on X; locally, these are of the form df for a locally-defined meromorphic function $f : U \to \mathbb{C}$.

Definition. *A* **canonical divisor** *of X is a divisor $K_X \in \operatorname{Div}(X)$ such that $K_X = [\operatorname{div}(\omega)]$ in $\operatorname{Pic}(X)$, where $\omega \in \Omega[X]$ is any meromorphic 1-form and $\operatorname{div}(\omega) = \sum_{P \in X} \operatorname{ord}_P(\omega)P$ with $\operatorname{ord}_P(\omega)$ defined by $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(h)$ if $\omega = h\,dt$ locally about P.*

Example 2.5.1. For $X = \mathbb{P}^1$, $k(\mathbb{P}^1) \cong \mathbb{C}(t)$, where t is the identity function $\mathbb{P}^1 \to \mathbb{P}^1$. Then $\omega = dt$ is a meromorphic 1-form on $\mathbb{P}^1$, so we can take $K_{\mathbb{P}^1} = [\operatorname{div}(\omega)] = [\operatorname{div}(dt)]$. Notice that if $P \neq \infty$ (where ∞ is thought of as the point $[0, 1]$), then $\omega = 1\,dt$ about P so $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(1) = 0$. Thus the computation of $K_{\mathbb{P}^1}$ comes down to its coefficient at ∞. At $P = \infty$, $\frac{1}{t}$ is a local uniformizer and we have

$$dt = d\left(\frac{1}{1/t}\right) = -\left(\frac{1}{t}\right)^2 d\left(\frac{1}{t}\right)$$

or in other words, $d\left(\frac{1}{t}\right) = -\left(\frac{1}{t}\right)^{-2} dt$. So $\operatorname{ord}_\infty(dt) = -2$ and we get $K_{\mathbb{P}^1} = [\operatorname{div}(dt)] = -2\infty$. As a consequence, we see that *any* meromorphic 1-form on $\mathbb{P}^1$ must have a pole somewhere, so $H^0(\mathbb{P}^1, \Omega^1_{\mathbb{P}^1/\mathbb{C}}) = 0$. In particular, $g(\mathbb{P}^1) = 0$. Notice that $\deg(K_{\mathbb{P}^1}) = -2 = 2g(\mathbb{P}^1) - 2$. This relation can be generalized significantly using the Riemann–Roch theorem.

Given a divisor $D \in \operatorname{Div}(X)$, define a complex vector space

$$L(D) = \{f \in k(X)^\times \mid (f) + D \geq 0\} \cup \{0\},$$

called the *Riemann–Roch space* of D. Let $\ell(D) = \dim_{\mathbb{C}} L(D)$.

Example 2.5.2. When $D = 0$, $L(0)$ is the space of meromorphic functions with no poles, which are just the constant functions. So $\ell(0) = 1$.

Lemma 2.5.3. *For any divisor $D \in \operatorname{Div}(X)$, $\ell(D) < \infty$.*

Theorem 2.5.4 (Riemann–Roch)**.** *Let X be a compact Riemann surface with canonical divisor K_X. Then for any divisor $D \in \operatorname{Div}(X)$, $\ell(D) - \ell(K_X - D) = \deg(D) - g + 1$.*

Corollary 2.5.5. *Let X be a compact Riemann surface of genus g. Then*

(1) $\ell(K_X) = g$.

(2) $\deg(K_X) = 2g - 2$.

(3) For a divisor $D \in \mathrm{Div}(X)$ *with* $\deg(D) > 2g - 2$, $\ell(D) = \deg(D) - g + 1$.

Example 2.5.6. Every compact Riemann surface X with genus $g = 0$ is isomorphic to $\mathbb{P}^1$.

Example 2.5.7. If X is a compact Riemann surface of genus $g = 1$, then X is an elliptic curve. Indeed, by Riemann–Roch, $\deg(K_X) = 0$, so for any effective divisor $D \in \mathrm{Div}(X)$ (meaning $D \geq 0$), $\ell(D) = \deg(D) - g + 1 = \deg(D)$. In particular, for any point $P \in X$, $\ell(P) = 1$ and for any $n \geq 1$, $\ell(nP) = n$. When $n = 2$, this shows that $L(2P)$ contains some nonconstant meromorphic function $x : X \to \mathbb{P}^1$ with at most a double pole at P. If $x \in L(P) \subseteq L(2P)$, then x must be constant ($\ell(P) = 1$), so we must have $\mathrm{ord}_P(x) = -2$. A similar argument shows there exists a nonconstant meromorphic function $y : X \to \mathbb{P}^1$ of order $\mathrm{ord}_P(y) = -3$. Next, $\ell(6P) = 6$, but notice that all of the following meromorphic functions lie in $L(6P)$:

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

So there is linear dependence among these functions. That is, x and y satisfy an equation

$$a_0y^2 + a_1y + a_2xy = b_3x^3 + b_2x^2 + b_1x + b_0$$

for some $a_0, a_1, a_2, b_0, b_1, b_2, b_3 \in \mathbb{C}$, which is a long Weierstrass equation for a complex elliptic curve. Over $\mathbb{C}$ (or any field of characteristic $\neq 2, 3$), this can be simplified to a short Weierstrass equation

$$y^2 = x^3 + ax + b \quad \text{with } \Delta := -16(4a^3 + 27b^2) \neq 0.$$

In $\Omega[X]$, we have an equality $2y\,dy = (3x^2 + a)\,dx$ which can be written

$$\frac{dx}{y} = \frac{2\,dy}{3x^2 + a}.$$

This shows that $\omega = \frac{dx}{y}$ defines a canonical divisor for X, so $K_X = \mathrm{div}(\omega)$.

We now demonstrate that $\mathrm{div}(\omega)$ has degree 0, as prescribed by Riemann–Roch. First, if $P \neq O$ is any nonidentity point on X, write $P = [x_0, y_0, 1]$ for some x_0, y_0 satisfying the Weierstrass equation defining X. Then $x - x_0$ vanishes at P, so $\mathrm{ord}_P(x - x_0) \geq 1$ and thus $\mathrm{ord}_P(dx) = \mathrm{ord}_P(d(x - x_0)) \geq 0$. So ω has a pole only when $y_0 = 0$, but this cannot happen since $\omega = \frac{2\,dy}{3x^2+a}$, so we see that $\mathrm{ord}_P(\omega) \geq 0$. Meanwhile, $\mathrm{ord}_P(x - x_0) \geq 1$ and $x : X \to \mathbb{P}^1$ having degree 2 imply that if $x_0^3 + ax_0 + b \neq 0$, then $y_0 = \pm\sqrt{x_0^3 + ax_0 + b}$ gives two distinct points in the fibre of x at x_0. If $\mathrm{ord}_P(x - x_0) = 1$, then $\mathrm{ord}_P(d(x - x_0)) = 0$ and thus $\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{dx}{y}\right) = 0$. On the other hand, $\mathrm{ord}_P(x - x_0) = 2$ and $\mathrm{ord}_P(y) = 1$ also imply that $\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(\frac{dx}{y}\right) = 0$. Finally, if $P = O = [0, 1, 0]$, then $\mathrm{ord}_O(x) = -2$ and $\mathrm{ord}_O(y) = -3$. If t is a uniformizer at O, then $x = ft^{-2}$ and $y = gt^{-3}$ for some $f, g \in k(X)^\times$ with $\mathrm{ord}_O(f) = \mathrm{ord}_O(g) = 0$. Thus $\mathrm{ord}_O(\omega) = 0$ once again.

Remark. For any abelian variety X and point $Q \in X$, the translation map $\tau_Q : X \to X, P \mapsto P + Q$, induces a pullback map $\tau_Q^* : \Omega[X] \to \Omega[X]$ which is the identity. That is, $\tau_Q^*\omega = \omega$ for any meromorphic differential 1-form ω on X. For this reason, $\omega \in \Omega[X]$ are sometimes called *invariant differential forms*.

3 Complex Tori

3.1 Abelian Varieties as Complex Tori

Let X be a compact Riemann surface of genus g, which can be viewed in two ways:

- algebraically, as a smooth, projective algebraic curve of genus g, or
- topologically, as a g-holed torus.

From the topological perspective, $H_1(X;\mathbb{Z}) = \mathbb{Z}[a_1, b_1, \ldots, a_g, b_g]$ where a_i, b_i are the longitudes/meridians of the torus. In particular, X can be recovered topologically by identifying sides of a planar $4g$-gon. For any finite set of points $P_1, \ldots, P_n \in X$, we can find a (translate of a) polygon such that all the points lie on its interior.

Recall (Corollary 2.5.5) that if K_X is a canonical divisor on X, then $\dim_{\mathbb{C}} L(K_X) = g$. Using linear algebra, it is possible to find a normalized basis $\omega_1, \ldots, \omega_g$ of $L(K_X)$ satisfying

$$\int_{a_i} \omega_j = \delta_{ij} \quad \text{for } 1 \le i, j \le g.$$

Integrating along any loop γ in X determines a map

$$\begin{aligned} \lambda : H_1(X;\mathbb{Z}) &\longrightarrow \mathbb{C}^g \\ [\gamma] &\longmapsto \lambda_\gamma := \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right). \end{aligned}$$

Then we have $\lambda_{a_i} = e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, the ith standard basis vector in $\mathbb{C}^g$; set $B_i = \lambda_{b_i} = \left(\int_{b_i} \omega_1, \ldots, \int_{b_i} \omega_g \right)$.

Definition. *The* **period lattice** *of X with respect to a normalized basis $\omega_1, \ldots, \omega_g \in \Omega[X]$ is the finitely generated $\mathbb{Z}$-module generated by $\{e_1, \ldots, e_g, B_1, \ldots, B_g\}$, denoted $\mathrm{Per}(\omega_1, \ldots, \omega_g)$.*

Definition. *The* **Jacobian** *of a compact Riemann surface X of genus g is*

$$J(X) = \mathbb{C}^g / \mathrm{Per}(\omega_1, \ldots, \omega_g)$$

for any choice of basis $\omega_1, \ldots, \omega_g$ of $\Omega[X]$.

Proposition 3.1.1. *The vectors $e_1, \ldots, e_g, B_1, \ldots, B_g$ are $\mathbb{R}$-linearly independent.*

Proof. (Sketch) Suppose to the contrary that $\Lambda := \mathrm{Per}(\omega_1, \ldots, \omega_g) = \mathbb{Z}[e_1, \ldots, e_g, B_1, \ldots, B_g]$ is contained in a proper $\mathbb{R}$-subspace of $\mathbb{C}^g$. Then there is a nonzero $\mathbb{R}$-linear functional $f : \mathbb{C}^g \to \mathbb{R}$ such that $\Lambda \subseteq \ker f$. We will use without proof the fact that any such f is the real part of some complex linear functional $g : \mathbb{C}^g \to \mathbb{C}$, and in turn, g is of the form $g(x) = \langle x, c \rangle$ for some fixed, nonzero $c \in \mathbb{C}^g$. Thus $f(x) = \mathrm{Re}\langle x, c \rangle$. But then $f(\Lambda) = 0$ implies that

$$\mathrm{Re}\left(\left\langle c, \int_{a_i} \omega \right\rangle \right) = 0 \quad \text{and} \quad \mathrm{Re}\left(\left\langle c, \int_{b_i} \omega \right\rangle \right) = 0$$

for any $1 \leq i \leq g$ and any nonzero $\omega = c_1\omega_1 + \ldots + c_g\omega_g \in \Omega[X]$. But since $c \neq 0$ and $\omega \neq 0$, this means

$$\mathrm{Re}\left(\int_{a_i} \omega\right) = \mathrm{Re}\left(\int_{b_i} \omega\right) = 0$$

for all $1 \leq i \leq g$. Further, we know $H_1(X;\mathbb{Z})$ is generated as an abelian group by $\{a_i, b_i\}$, so this implies

$$\mathrm{Re}\left(\int_{\gamma} \omega\right) = 0$$

for any $\gamma \in H_1(X;\mathbb{Z})$. However, the de Rham pairing $H^1_{dR}(X) \times H_1(X;\mathbb{R}) \to \mathbb{C}$ is nondegenerate, so $\omega \neq 0$, a contradiction. Hence $\Lambda \otimes \mathbb{R} \cong \mathbb{C}^g$ as real vector spaces. □

Fix a basepoint $P_0 \in X$ and define a map

$$\begin{aligned} \mu : X &\longrightarrow J(X) = \mathbb{C}^g/\Lambda \\ P &\longmapsto \left(\int_{P_0}^P \omega_1, \ldots, \int_{P_0}^P \omega_g\right) \quad \mathrm{mod}\ \Lambda. \end{aligned}$$

Then the work above shows:

Proposition 3.1.2. *Each integral $\int_{P_0}^P \omega_i$ is independent of path, so $\mu : X \to J(X)$ is well-defined.*

Further, μ extends to a map $\mathrm{Div}(X) \to J(X)$ by linearity:

$$\mu(a_1P_1 + \ldots a_rP_r) = a_1\mu(P_1) + \ldots + a_r\mu(P_r).$$

Consider the restriction $\mu : \mathrm{Div}^0(X) \to J(X)$.

Theorem 3.1.3 (Abel–Jacobi)**.** *For any compact Riemann surface X,*

(1) (Abel) $\ker \mu = \mathrm{PDiv}(X)$.

(2) (Jacobi) $\mathrm{im}\, \mu = J(X)$.

Therefore μ induces an isomorphism $\Phi : \mathrm{Pic}^0(X) \xrightarrow{\sim} J(X)$.

Definition. $\Phi : \mathrm{Pic}^0(X) \xrightarrow{\sim} J(X)$ *is called the* **Abel–Jacobi map** *of X.*

We prove the Abel–Jacobi theorem with the following lemmas.

Lemma 3.1.4. *Given two distinct points $P, Q \in X$, there exists a meromorphic 1-form $\omega_{P,Q} \in \Omega[X]$ with the following properties:*

(i) $\omega_{P,Q}$ has simple poles at P and Q and is holomorphic elsewhere.

(ii) $\mathrm{Res}_P(\omega_{P,Q}) = 1$ *and* $\mathrm{Res}_P(\omega_{P,Q}) = -1$.

(iii) $\displaystyle\int_{a_i} \omega_{P,Q} = 0$ *for all $1 \leq i \leq g$.*

Moreover, any form satisfying (i) - (iii) for P and Q is unique.

Proof. Let $D = -P - Q$. Then by Riemann–Roch,

$$\ell(K_X - D) = \ell(D) - \deg(D) + g - 1 = 0 + 2 + g - 1 = g + 1.$$

By definition, $L(K_X - D)$ consists of rational functions $f \in k(X)^\times$ with $(f) + K_X + P + Q \geq 0$. Equivalently, $L(K_X - D)$ consists of differential forms $\omega \in \Omega[X]$ such that $\operatorname{div}(\omega) + P + Q \geq 0$, or ω having at most 2 simple poles at P and Q. Note that $L(K_X)$ is a subspace of $L(K_X - D)$ of dimension $\ell(K_X) = g$ by Corollary 2.5.5, so there is some $\omega \in L(K_X - D)$ with at least one simple pole at P or Q. Repeating the same argument for the divisor $-P$ shows $L(K_X + P) = L(K_X)$ and likewise for the divisor $-Q$. So there is some ω with exactly 2 simple poles, one at P and the other at Q, ensuring condition (i) is met. By the residue theorem, $\sum_{P' \in X} \operatorname{Res}_{P'}(\omega) = 0$ and $\operatorname{Res}_{P'}(\omega) = 0$ if P' is not a pole of ω, so we can arrange for condition (ii) to hold. Finally, if $\eta \in \Omega[X]$, then $\omega - \eta$ also satisfies (i) and (ii), so we may further arrange for condition (iii) to hold, that is, $\int_{a_i} \omega = 0$ for each $1 \leq i \leq g$. Uniqueness follows from a dimension argument. □

Lemma 3.1.5. *If $\omega_1, \ldots, \omega_g$ are a normalized basis for $L(K_X)$ and $\omega_{P,Q}$ is as above, then*

$$\int_{b_j} \omega_{P,Q} = 2\pi i \int_Q^P \omega_j \quad \text{for each } 1 \leq j \leq g.$$

Proof. Straightforward. □

Suppose $f \in k(X)^\times$ has principal divisor

$$(f) = \sum_{P \in X} \operatorname{ord}_P(f) P = \sum_{k=1}^{r} (P_k - Q_k) \in \operatorname{PDiv}(X) \subseteq \operatorname{Div}^0(X)$$

for some $P_1, \ldots, P_r, Q_1, \ldots, Q_r \in X$. Let $\omega = \frac{df}{f}$. One can check that ω has simple poles at all zeroes and poles of f and is holomorphic elsewhere. Moreover, at any zero or pole P of f, $\operatorname{Res}_P(\omega) = \operatorname{ord}_P(f)$. Then by Lemma 3.1.4, ω and $\sum_{k=1}^r \omega_{P_k,Q_k}$ have the same poles, multiplicities and residues, so by uniqueness, $\omega - \sum_{k=1}^r \omega_{P_k,Q_k}$ is a holomorphic 1-form. That is,

$$\omega = \sum_{k=1}^{r} \omega_{P_k,Q_k} + \sum_{j=1}^{g} t_j \omega_j$$

for some $t_j \in k(X)$. Integrating,

$$\int_{a_i} \frac{df}{f} = \sum_{k=1}^{r} \int_{a_i} \omega_{P_k,Q_k} + \sum_{j=1}^{g} \int_{a_i} t_j \omega_j = \sum_{j=1}^{g} \int_{a_i} t_j \omega_j,$$

and recalling that $\int_{a_i} \frac{df}{f} \in 2\pi i \mathbb{Z}$, we see that each $t_j = 2\pi i n_j$ for some $n_j \in \mathbb{Z}$. On the other hand,

$$\begin{aligned}\int_{b_i} \frac{df}{f} &= \sum_{k=1}^{r} \int_{b_i} \omega_{P_k,Q_k} + \sum_{j=1}^{g} \int_{b_i} t_j \omega_j \\ &= 2\pi i \sum_{k=1}^{r} \int_{Q_k}^{P_k} \omega_i + \sum_{j=1}^{g} t_j B_j = 2\pi i \sum_{k=1}^{r} \int_{Q_k}^{P_k} \omega_i + 2\pi i \sum_{j=1}^{g} n_j B_j\end{aligned}$$

by Lemma 3.1.5. So for each $1 \leq i \leq g$,

$$m_i := \sum_{k=1}^{r} \int_{Q_k}^{P_k} \omega_i + \sum_{j=1}^{g} n_j B_j$$

is an integer. We use this to prove Abel's theorem (3.1.3(1)).

Proof. Take $(f) \in \mathrm{PDiv}(X)$ as above. Applying the map $\mu : \mathrm{Div}^0(X) \to J(X)$ to (f) yields

$$\mu((f)) = \sum_{k=1}^{r} \left(\int_{Q_k}^{P_k} \omega_1, \ldots, \int_{Q_k}^{P_k} \omega_g \right) = \sum_{i=1}^{g} m_i e_i + \sum_{i=1}^{g} n_i B_i \in \Lambda.$$

Hence $(f) \in \ker \mu$.

Conversely, take $D \in \ker \mu$, say $D = \sum_{k=1}^{r}(P_k - Q_k)$ for $P_k, Q_k \in X$. Then

$$\mu(D) = \sum_{k=1}^{r} \left(\int_{Q_k}^{P_k} \omega_1, \ldots, \int_{Q_k}^{P_k} \omega_g \right) = \sum_{j=1}^{g} m_j e_j + \sum_{j=1}^{g} n_j B_j$$

for some $m_j, n_j \in \mathbb{Z}$. One can show that if $\gamma \in \{a_1, \ldots, a_g, b_1, \ldots, b_g\}$, then

$$\int_\gamma \left(\sum_{k=1}^{r} \omega_{P_k,Q_k} + \sum_{j=1}^{g} 2\pi i n_j \omega_j \right) \in 2\pi i \mathbb{Z}.$$

Fix a basepoint $P_0 \notin \mathrm{supp}(D) = \{P_1, \ldots, P_r, Q_1, \ldots, Q_r\}$ and define a function $f : X \to \mathbb{C}$ by

$$f(P) = \exp\left[\int_{P_0}^{P} \left(\sum_{k=1}^{r} \omega_{P_k,Q_k} + \sum_{j=1}^{g} 2\pi i n_j \omega_j \right) \right].$$

We claim that for any $\gamma \in H_1(X \smallsetminus \mathrm{supp}(D); \mathbb{Z})$,

$$\int_\gamma \left(\sum_{k=1}^{r} \omega_{P_k,Q_k} + \sum_{j=1}^{g} 2\pi i n_j \omega_j \right) \in 2\pi i \mathbb{Z}.$$

Note that $H_1(X \smallsetminus \mathrm{supp}(D); \mathbb{Z})$ is generated as an abelian group by $a_1, \ldots, a_g$, $b_1, \ldots, b_g$, $c_1, \ldots, c_r$, $c_1', \ldots, c_r'$ where c_k (resp. c_k') is represented by a small loop around P_k (resp. Q_k). Thus the claim follows from proving it for $\gamma = c_k$ or c_k'. Observe that each ω_j is holomorphic on the interiors of c_k and c_k', so

$$\int_{c_k} \omega_j = \int_{c_k'} \omega_j = 0.$$

Thus the only contribution to the integral above is from ω_{P_k,Q_k}, but

$$\int_{c_k} \omega_{P_k,Q_k} = 2\pi i \qquad \text{and} \qquad \int_{c_k'} \omega_{P_k,Q_k} = -2\pi i,$$

proving the claim. Thus the exponential expression defining $f(P)$ is well-defined, i.e. independent of path $P_0 \to P$, so f extends to a meromorphic function on X. Finally, as before, $\frac{df}{f}$ has simple poles at all zeroes and poles of f and $\text{Res}_P\left(\frac{df}{f}\right) = \text{ord}_P(f)$, so we have

$$\frac{df}{f} = \sum_{k=1}^{r} \omega_{P_k,Q_k} + \sum_{j=1}^{g} 2\pi i n_j \omega_j.$$

Hence $D = (f) \in \text{PDiv}(X)$, proving Abel's theorem. □

To prove Jacobi's theorem, we need two more results.

Lemma 3.1.6. *Let X be a compact Riemann surface of genus $g \geq 1$. Then there exist distinct points $M_1, \ldots, M_g \in X$ such that no holomorphic 1-form on X vanishes at each of these points.*

Proof. Suppose $\eta_1 \neq 0$ is a holomorphic 1-form on X. Then there exists some $M_1 \in X$ such that $\eta_1(M_1) \neq 0$. By Riemann–Roch,

$$\ell(M_1) - \ell(K_X - M_1) = \deg(M_1) - g + 1 = 2 - g.$$

Since $g \geq 1$, $\ell(M_1) = 1$ (or else $X \cong \mathbb{P}^1$ which is impossible by Example 2.5.6). Thus $\ell(K_X - M_1) = g - 1$. If $g = 1$, we are done. Otherwise, there exists a nonzero holomorphic form $\eta_2 \in L(K_X - M_1)$ such that $\eta_2(M_1) = 0$ and $\eta_2(M_2) \neq 0$ for some other $M_2 \in X$. Repeat until we get $\ell(K_X - (M_1 + \ldots + M_g)) = 0$. Notice that by construction, for each $1 \leq i \leq g$, $\eta_{i+1}, \ldots, \eta_g$ all vanish at M_i but $\eta_i(M_i) \neq 0$. This implies $\eta_1, \ldots, \eta_g$ form a basis of $L(K_X)$, so any $\omega \in L(K_X)$ will be nonzero at some M_i. □

Lemma 3.1.7. *A holomorphic map $f : M \to N$ between compact, connected complex manifolds of the same dimension is surjective if the Jacobian determinant $\det(\text{Jac}(f)_P)$ is nonzero at some point $P \in M$.*

Proof. Standard. □

We now prove Jacobi's theorem (3.1.3(2)).

Proof. Fix $M_1, \ldots, M_g \in X$ as in Lemma 3.1.6. For each $1 \leq i \leq g$, let V_i be a simply connected neighborhood of M_i and consider the map

$$\begin{aligned} \varphi : V_1 \times \cdots \times V_g &\longrightarrow J(X) \\ (P_1, \ldots, P_g) &\longmapsto \mu(P_1 - M_1 + \ldots + P_g - M_g). \end{aligned}$$

Then to prove Jacobi's theorem, it suffices to show φ is surjective on a neighborhood of $0 \in J(X)$ since $J(X)$ is a group (variety) and μ is a homomorphism. Let t_i be a local coordinate on V_i centered at M_i (i.e. so $t_i(M_i) = 0$). For $1 \leq i, j \leq g$, write $\omega_i = h_{ij}(t_j)\, dt_j$ for some $h_{ij} \in k(V_j)^\times$. Let $A = (h_{ij}) \in GL(k(X)^\times)$. Then since $\omega_1, \ldots, \omega_g$ are linearly independent and do not vanish at any M_i, we see that

$$\det(A(0, \ldots, 0)) = \begin{vmatrix} h_{11}(t_1(M_1)) & \cdots & h_{1g}(t_g(M_g)) \\ \vdots & \ddots & \vdots \\ h_{g1}(t_1(M_1)) & \cdots & h_{gg}(t_g(M_G)) \end{vmatrix} \neq 0.$$

Now each h_{ij} is holomorphic on V_j so it can be written as a power series in t_j:

$$h_{ij} = \sum_{n=0}^{\infty} a_{ijnt} t_j^n.$$

Define

$$h_{ij}^* = \sum_{n=0}^{\infty} \frac{a_{ijn}}{n+1} t_j^{n+1}.$$

Then φ can be written in terms of the h_{ij}^* as $\varphi = (H_1, \dots, H_g)$ where

$$H_i(t_1, \dots, t_g) = \sum_{j=1}^{g} h_{ij}^*(t_j).$$

By construction, $\frac{\partial H_i}{\partial t_j} = h_{ij}$, so

$$A = \left(\frac{\partial H_i}{\partial t_j}\right) = \mathrm{Jac}(\varphi)$$

has nonzero determinant. Hence φ is surjective by Lemma 3.1.7. □

3.2 Line Bundles on Complex Tori

For a complex manifold X, let $\texttt{InvSh}_X$ be the group of invertible sheaves on X under $\otimes$. There are canonical bijections

$$H^1(X, \mathcal{O}_X^\times) \longleftrightarrow \mathrm{Pic}(X) \longleftrightarrow \texttt{InvSh}_X$$

In this section, we will freely pass between all three of these groups.

Let $X = \mathbb{C}^n/\Lambda$ be a complex torus, where Λ is a full lattice in $\mathbb{C}^n$. An important fact is that every line bundle over $\mathbb{C}^n$ is trivial, i.e. isomorphic to $X \times \mathbb{C}$. (To prove this, use the exponential sequence $0 \to \mathbb{Z} \to \mathcal{O} \xrightarrow{\exp} \mathcal{O}^\times \to 0$ and the $\overline{\partial}$-Poincaré lemma.) Our goal in this section is to construct line bundles $L \to X$ from (trivial) line bundles $\widetilde{L} \to \mathbb{C}^n$ by taking quotients. Explicitly, suppose there is a group action $\alpha : \Lambda \times \widetilde{L} \to \widetilde{L}$ such that for any $(\lambda, v) \in \Lambda \times \widetilde{L}$, the map

$$\alpha : \widetilde{L}_v \longrightarrow \widetilde{L}_{\lambda+v}$$

is a linear isomorphism. We will show that $L := \widetilde{L}/\Lambda$ is a line bundle on X.

Where does such an action come from? We know by covering space theory that the fundamental group $\pi_1(X)$ is isomorphic to Λ. On the other hand, the trivial line bundle $\widetilde{L}$ is isomorphic to $\mathbb{C}^n \times \mathbb{C}$, where $\mathbb{C}^n$ is identified as the universal cover of X, so there is an induced action of $\Lambda = \pi_1(X)$ on $\widetilde{L}$. It's easy to check that any such action satisfies the compatibility condition above. Fix an isomorphism of line bundles $B : \mathbb{C}^n \times \mathbb{C} \to \widetilde{L}$.

Lemma 3.2.1. *The function $\tau := B(-, 1) : \mathbb{C}^n \to \widetilde{L}$ is a nowhere vanishing section of $\widetilde{L}$. Moreover, we have*

$$\alpha(\lambda, \tau(v)) = a_\lambda(v)\tau(\lambda + v)$$

for all $\lambda \in \Lambda, v \in \mathbb{C}^n$ and for some nonvanishing holomorphic function $a_\lambda : \mathbb{C}^n \to \mathbb{C}$.

Proof. If $\pi : \widetilde{L} \to \mathbb{C}^n$ is the bundle map, then $\pi \circ B(v,1) = v$ since $\pi(v,1) = v$ and B is a bundle map. Moreover, τ is nonvanishing since $(v,1) \neq (0,0)$ in $\mathbb{C}^n \times \mathbb{C}$. Now since the only holomorphic automorphisms of a line bundle $\widetilde{L} \to \mathbb{C}^n$ are given by multiplication by nonzero holomorphic functions, the automorphism $\tau(v) \mapsto \lambda + \tau(v)$ must be of the form $\tau(v) \mapsto a_\lambda(v)\tau(\lambda+v)$ for some $a_\lambda(v) \in \mathbb{C}^\times$. By construction, the functions a_λ are holomorphic and $\alpha(\lambda, \tau(v)) = a_\lambda(v)\tau(\lambda + v)$ as required. □

Definition. *The functions $\{a_\lambda\}_{\lambda\in\Lambda}$ are referred to as a* **factor of automorphy** *for the line bundle $\widetilde{L}$ (with respect to B and Λ).*

Lemma 3.2.2. *The factor of automorphy $\{a_\lambda\}_{\lambda\in\Lambda}$ satisfies the cocycle condition*

$$a_\lambda(v + \mu)a_\mu(v) = a_{\lambda+\mu}(v)$$

for all $\lambda, \mu \in \Lambda$ and $v \in \mathbb{C}^n$. In particular, $\{a_\lambda\}_{\lambda\in\Lambda}$ defines an invertible sheaf (hence a line bundle) on $X = \mathbb{C}^n/\Lambda$.

Proof. Since $\alpha : \Lambda \times \widetilde{L} \to \widetilde{L}$ is a group action, we have

$$\begin{aligned} \alpha(\lambda, \alpha(\mu, \tau(v))) &= \alpha(\lambda + \mu, \tau(v)) \\ \implies \alpha(\lambda, a_\mu(v)\tau(\mu + v)) &= a_{\lambda+\mu}(v)\tau(\lambda + \mu + v) \\ \implies a_\lambda(\mu + v)a_\mu(v)\tau(\lambda + \mu + v) &= a_{\lambda+\mu}(v)\tau(\lambda + \mu + v) \end{aligned}$$

for any $\lambda, \mu \in \Lambda$ and $v \in \mathbb{C}^n$. Cancelling the nonzero τ terms produces the desired cocycle condition. Now define an invertible sheaf $\mathcal{L}$ on $X = \mathbb{C}^n/\Lambda$ using $\{a_\lambda\}$:

$$\mathcal{L}(U) = \{f \in \mathcal{O}(\pi^{-1}(U)) \mid f(\lambda + v) = a_\lambda(v)f(\lambda) \text{ for all } \lambda \in \Lambda, v \in \pi^{-1}(u)\}.$$

□

If $\mathcal{L}$ denotes the invertible sheaf on X constructed above, we will let L be the associated line bundle on X. One can show that every line bundle L on X can be constructed from such an action: pull L back along the universal cover $\pi : \mathbb{C}^n \to \mathbb{C}^n/\Lambda = X$ and check that the induced action of $\Lambda = \pi_1(X)$ on $\widetilde{L} = \pi^*L$ yields L as a quotient. In other words, the natural map $H^1(X, \mathbb{C}) \to H^1(X, \mathcal{O}_X)$ is surjective.

3.3 Appell–Humbert Theorem

Definition. *A* **Hermitian form** *on a complex vector space V is a map $H : V \times V \to \mathbb{C}$ which is linear in the first variable, i.e. $H(v_1 + cv_2, w) = H(v_1, w) = cH(v_2, w)$, and antilinear in the second variable, which amounts to saying $H(w, v) = \overline{H(v, w)}$ where $\overline{(\cdot)}$ denotes complex conjugation. (Such a form is sometimes also called* **sesquilinear***.)*

Definition. *Let $\Lambda \subseteq V$ be a lattice. A Hermitian form $H : V \times V \to \mathbb{C}$ is called a* **Riemann form** *with respect to Λ if the imaginary part* $\mathrm{Im}(H)$ *takes integer values on $\Lambda \times \Lambda \subseteq V \times V$.*

Example 3.3.1. For an elliptic curve $E = \mathbb{C}/[\omega_1, \omega_2]$, the form

$$H(v, w) = \frac{v\bar{w}}{\mathrm{Im}(\omega_1\bar{\omega}_2)}$$

is a Riemann form on $\mathbb{C}$ with respect to $\Lambda = [\omega_1, \omega_2]$. Moreover, every Riemann form on E is a multiple of this H.

Definition. *An* **Appell–Humbert datum** *(or an* **Appell–Humber pair***) on a complex torus $X = \mathbb{C}^n/\Lambda$ is a pair (α, H) where H is a Riemann form on $\mathbb{C}^n$ with respect to Λ and $\alpha : \Lambda \to U(1) = S^1 \subseteq \mathbb{C}^\times$ is a map satisfying*

$$\alpha(\lambda + \mu) = \alpha(\lambda)\alpha(\mu)(-1)^{\mathrm{Im}\, H(\lambda,\mu)}$$

for all $\lambda, \mu \in \Lambda$.

Lemma 3.3.2. *If (α, H) is an Appell–Humbert pair on X, then*

$$a_\lambda(v) := \alpha(\lambda) \exp\left[\pi H(v, \lambda) + \frac{\pi}{2} H(\lambda, \lambda)\right]$$

is a factor of automorphy for the trivial line bundle $\widetilde{L} = \mathbb{C}^n \times \mathbb{C}$ on $\mathbb{C}^n$.

Proof. A pair (α, H) defines an action on $\widetilde{L}$ by

$$\begin{aligned} \Lambda \times \mathbb{C}^n \times \mathbb{C} &\longrightarrow \mathbb{C}^n \times \mathbb{C} \\ (\lambda, v, c) &\longmapsto (\lambda + v, \alpha(\lambda)c). \end{aligned}$$

It is routine to verify the condition at the beginning of Section 3.2 holds for this action, and by construction the a_λ are precisely the factor of automorphy defined in Lemma 3.2.1. □

Let $\mathcal{L}(\alpha, H)$ (resp. $L(\alpha, H)$) denote the invertible sheaf (resp. line bundle) on $X = \mathbb{C}^n/\Lambda$ defined by an Appell–Humbert pair (α, H). The main result in this section is that every line on X has a canonical Appell–Humbert pair.

Theorem 3.3.3 (Appell–Humbert)**.** *Every invertible sheaf on a complex torus is isomorphic to $\mathcal{L}(\alpha, H)$ for a unique Appell–Humbert datum (α, H).*

Example 3.3.4. For an elliptic curve $E = \mathbb{C}/[1, \tau]$, let H be the Riemann form from Example 3.3.1 and consider the function $\alpha_0 : [1, \tau] \to U(1)$ given by

$$\alpha_0(a + b\tau) = (-1)^{ab\, \mathrm{Im}\, H(1,\tau)}.$$

Tracing through the definitions, we see that $\mathcal{L}(\alpha_0, H) \cong \mathcal{O}_E$. More generally, every Appell–Humbert pair on E is of the form (α_P, nH) where $P \in E$, $n \in \mathbb{Z}$ and $\alpha_P : [1, \tau] \to U(1)$ is the function

$$\alpha_P(a + b\tau) = \alpha_0(a + b\tau) \exp[2\pi i\, \mathrm{Im}\, H(P, a + b\tau)].$$

Then we have $\mathcal{L}(\alpha_P, nH) \cong \mathcal{O}_E(nP)$. We will see another proof of this fact later. In particular, this describes all line bundles on an elliptic curve, namely the following is an isomorphism of groups:

$$\begin{aligned} \mathrm{Pic}(E) &\xrightarrow{\sim} E \oplus \mathbb{Z} \\ [L] &\longmapsto (P, n) \text{ if } L \cong L(\alpha_P, nH). \end{aligned}$$

This agrees with the isomorphism $\mathrm{Pic}(E) = \mathrm{Pic}^0(E) \oplus \mathbb{Z} \cong E \oplus \mathbb{Z}$ from Theorem 2.3.1.

For a complex torus $X = \mathbb{C}^n/\Lambda$, let $AH(X)$ be the set of equivalence classes of Appell–Humbert data on X, where $(\alpha_1, H_1) \sim (\alpha_2, H_2)$ if $\mathcal{L}(\alpha_1, H_1) \cong \mathcal{L}(\alpha_2, H_2)$.

Lemma 3.3.5. *For any Appell–Humbert data* (α_1, H_1) *and* (α_2, H_2) *on* X*, there is an isomorphism of invertible sheaves* $\mathcal{L}(\alpha_1, H_1) \otimes \mathcal{L}(\alpha_2, H_2) \cong \mathcal{L}(\alpha_1\alpha_2, H_1 + H_2)$.

This shows that $AH(X)$ is an abelian group under the operation $(\alpha_1, H_1) \cdot (\alpha_2, H_2) = (\alpha_1\alpha_2, H_1 + H_2)$. Moreover, there is a group homomorphism $\Phi : AH(X) \to \mathrm{Pic}(X)$ sending $[(\alpha, H)] \mapsto [\mathcal{L}(\alpha, H)]$. We call Φ the *Appell–Humbert map* for X. To prove Theorem 3.3.3, we will show that Φ is an isomorphism.

Lemma 3.3.6. *If* $\mathcal{L}(\alpha, H)$ *has a nonzero section, then* H *is positive and semi-definite and* $\alpha \equiv 1$ *on* $\Lambda \cap \ker H$.

Proof. (This is one direction of Thm. 2.1 in Kempf.) First assume that $H(v, v) < 0$ for some $v \in \mathbb{C}^n$. Set $C = -H(v, v) > 0$. Then the function $f : \mathbb{C}^n \to \mathbb{C}$ defined by $f(w) = \exp[-\pi H(w, w)]$ is positive, real-analytic and satisfies

$$f(\lambda + w) = \exp[-2\pi \mathrm{Re} H(v, \lambda) - \pi H(\lambda, \lambda)] f(w)$$

for any $\lambda \in \Lambda$ and $w \in \mathbb{C}^n$. Fix $x \in X$ and define a "local norm" $||\cdot||_x$ on $H^0(X, \mathcal{L}(\alpha, H))$ at x by

$$||\sigma||_x^2 = f(w)|\sigma(w)|^2$$

where w is any point in $\mathcal{L}(\alpha, H)_x$ and $|\cdot|$ denotes the ordinary complex norm. This is well-defined (i.e. independent of w) by the above functional equation for f and the action of λ on σ. It's easy to check that $||\cdot||_x$ is a norm.

Now since X is compact, there is a uniform bound $||\sigma||_x \leq M$ for any fixed $\sigma \in H^0(X, \mathcal{L}(\alpha, H))$ and for x varying over X. For the fixed $v \in \mathbb{C}^n$ with $-H(v, v) = C > 0$, look at the assignment $g : \mathbb{C} \to \mathbb{C}, z \mapsto \sigma(zv)$. This is an entire function and satisfies the inequality

$$|g(z)| = |\sigma(zv)| \leq M \cdot \exp[-\pi z^2 C]$$

so g must be identically 0. In particular, $\sigma(v) = 0$, but $H(v, v) < 0$ is an open condition so we conclude that σ is the zero section.

Next, assume α is not the constant function 1 on $\Lambda \cap \ker H$. Take $\sigma \in H^0(X, \mathcal{L}(\alpha, H))$. Then since $\Lambda \cap \ker H$ is a lattice in $\ker H$, our σ is bounded on any coset of $\ker H$, hence constant on such cosets. Assuming $\alpha(\lambda) \neq 1$ for some $\lambda \in \Lambda \cap \ker H$, this implies $\sigma(v) = 0$ for all $v \in \mathbb{C}^n$. Thus if σ is a nonzero section, $\alpha \equiv 1$. □

Proposition 3.3.7. $\Phi : AH(X) \to \mathrm{Pic}(X)$ *is injective.*

Proof. Suppose $\mathcal{L}(\alpha, H)$ is trivial. In particular, $\mathcal{L}(\alpha, H)$ has a nonzero section. Then by Lemma 3.3.5, $\mathcal{L}(\alpha, H)^* \cong \mathcal{L}(\alpha^{-1}, -H)$ so $\mathcal{L}(\alpha^{-1}, -H)$ also has a nonzero section. Thus Lemma 3.3.6 shows that H and $-H$ are both positive and semi-definite, which is only possible if $H = 0$. Moreover, Lemma 3.3.6 also implies $\alpha = 1$, so Φ is injective. □

To prove Φ is surjective, we recall the following construction. The exponential sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^\times \to 0$$

induces a long exact sequence in cohomology:

$$\cdots \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^\times) \xrightarrow{\delta} H^2(X, \mathbb{Z}) \to \cdots$$

Recall that $H^1(X, \mathcal{O}_X^\times) = \mathrm{Pic}(X)$.

Definition. *The* **(first) Chern class** *of a line bundle L on X is the cohomology class $c_1(L) := \delta([L]) \in H^2(X, \mathbb{Z})$.*

To prove surjectivity of the Appell–Humbert map, we have the following well-known interpretation of $H^2(X, \mathbb{Z})$.

Proposition 3.3.8. *For any complex torus X, there are isomorphisms $H^2(X, \mathbb{Z}) \cong H^2(\Lambda, \mathbb{Z}) \cong \bigwedge^2 \mathrm{Hom}(\Lambda, \mathbb{Z})$.*

Proof. First, we claim there is an isomorphism

$$H^1(X, \mathcal{O}_X^\times) \xrightarrow{\sim} H^1(\Lambda, H^0(\mathbb{C}^n, \mathcal{O}^\times))$$

where the latter is the first *group cohomology* of Λ with coefficients in $H^0(\mathbb{C}^n, \mathcal{O}^\times) \cong \mathbb{C}[z_1, \ldots, z_n]^\times$. The map is constructed as follows. Let $[L]$ be the class of a line bundle and let $\widetilde{L}$ be the pullback of L along the universal cover $\pi : \mathbb{C}^n \to \mathbb{C}^n/\Lambda = X$. Then $L = \widetilde{L}/\Lambda$ for a factor of automorphy (a_λ), as described in Section 3.2. In particular, these a_λ are holomorphic functions $\mathbb{C}^n \to \mathbb{C}^\times$, and the cocycle condition on them means $(a_\lambda) \in Z^1(\Lambda, H^0(\mathbb{C}^n, \mathcal{O}^\times))$. Hence we get a class $[(a_\lambda)] \in H^1(\Lambda, H^0(\mathbb{C}^n, \mathcal{O}^\times))$. Conversely, every 1-cocycle (a_λ) defines an action of Λ on the trivial line bundle $\mathbb{C}^n \times \mathbb{C}$ by $\lambda \cdot (v, z) = (v + \lambda, a_\lambda(v) z)$ which descends to a line bundle L on X. This establishes the claimed isomorphism.

Now let $\pi : \mathbb{C}^n \to X$ be the universal cover and consider the short exact sequence coming from pulling back the exponential sequence for X:

$$0 \to H^0(\mathbb{C}^n, \pi^*\mathbb{Z}) \to H^0(\mathbb{C}^n, \pi^*\mathcal{O}_X) \to H^0(\mathbb{C}^n, \pi^*\mathcal{O}_X^\times) \to 0.$$

This induces a long exact sequence in cohomology with Λ coefficients, whose boundary map fits into the following commutative diagram:

$$\begin{array}{ccc} H^1(\Lambda, H^0(\mathbb{C}^n, \mathcal{O}^\times)) & \xrightarrow{\delta} & H^2(\Lambda, \mathbb{Z}) \\ \sim \downarrow & & \downarrow \\ H^1(X, \mathcal{O}_X^\times) & \xrightarrow{\delta} & H^2(X, \mathbb{Z}) \end{array}$$

The left column is an isomorphism by the previous paragraph, so it follows that the right column is also an isomorphism. This establishes the first isomorphism in the statement of the proposition.

Next, define a map $A : H^2(\Lambda, \mathbb{Z}) \to \operatorname{Hom}(\bigwedge^2\Lambda, \mathbb{Z}) = \bigwedge^2 \operatorname{Hom}(\Lambda, \mathbb{Z})$ by $AF(\lambda_1, \lambda_2) = F(\lambda_1, \lambda_2) - F(\lambda_2, \lambda_1)$ for any 2-cocycle $F \in Z^2(\Lambda, \mathbb{Z})$. It is clear that AF is bilinear and alternating, and one can check that $A\delta G = 0$ for any 1-cocycle G. To show A is an isomorphism, it's enough to check that it preserves the exterior algebra structure on $H^\bullet(X, \mathbb{Z})$. This is done in Mumford's *Abelian Varieties* on pp. 16 - 17, for example. □

The next step in our quest to prove the Appell–Humbert theorem is to identify the Chern class of a line bundle directly as an alternating 2-form on Λ, under the isomorphisms in Proposition 3.3.8. Let L be a line bundle on X. Then L determines a 1-cocycle $(e_\lambda) \in Z^1(\Lambda, H^0(\mathbb{C}^n, \mathcal{O}^\times))$. Write $e_\lambda(z) = \exp[2\pi i f_\lambda(z)]$ for some holomorphic $f_\lambda : \mathbb{C}^n \to \mathbb{C}$.

Proposition 3.3.9. *For a line bundle L as above, $c_1(L) \in H^2(X, \mathbb{Z})$ corresponds to $[E] \in \bigwedge^2 \operatorname{Hom}(\Lambda, \mathbb{Z})$, where*

$$E(\beta_1, \beta_2) = f_{\beta_2}(z + \beta_1) + f_{\beta_1}(z) - f_{\beta_1}(z + \beta_2) - f_{\beta_2}(z)$$

for any $z \in \mathbb{C}^n$. In particular, $E(ix, iy) = E(x, y)$ for any $x, y \in \mathbb{C}^n$.

Proof. Check it using the proof of Proposition 3.3.8. □

Lemma 3.3.10. *There is a bijective correspondence*

$$\begin{aligned} \{\text{Hermitian forms on } \mathbb{C}^n\} &\longleftrightarrow \{\text{real skew-symmetric forms } E \text{ with } E(ix, iy) = E(x, y)\} \\ H(x, y) &\longmapsto \operatorname{Im} H(x, y) \\ E(ix, y) + iE(x, y) &\longleftarrow E(x, y). \end{aligned}$$

Proof. Routine. □

Let L, (e_λ) and $c_1(L) = [E]$ be as above. Then by extending scalars to $\mathbb{R}$, the form E is real, skew-symmetric and satisfies $E(ix, iy) = E(x, y)$ for all $x, y \in \mathbb{C}^n$, so by Lemma 3.3.10, it determines a Hermitian form $H(x, y) := E(ix, y) + iE(x, y)$ on $\mathbb{C}^n$. One can check that H is a Riemann form on X. We have thus constructed the H in an Appell–Humbert pair (α, H) for L. To get α, we essentially only need one more result.

Proposition 3.3.11. *For a complex torus $X = \mathbb{C}^n/\Lambda$, there is an isomorphism* $\operatorname{Hom}(\Lambda, S^1) \cong \operatorname{Pic}^0(X)$.

Proof. Note that the Appell–Humbert map $\Phi : AH(X) \to \operatorname{Pic}(X)$ restricts to a homomorphism $\operatorname{Hom}(\Lambda, S^1) \to \operatorname{Pic}^0(X)$, where $\operatorname{Hom}(\Lambda, S^1)$ is viewed as a subgroup of $AH(X)$ via the mapping $\alpha \mapsto (\alpha, 0)$. Suppose $\alpha : \Lambda \to S^1$ has $\Phi(\alpha)$ equal to a trivial line bundle. Write

$$\alpha(\lambda) = \frac{g(z + \lambda)}{g(z)}$$

for $g \in H^0(\mathbb{C}^n, \mathcal{O}^\times)$. Suppose $K \subseteq \mathbb{C}^n$ is a compact set such that $K + \Lambda = \mathbb{C}^n$. Then since $||\alpha|| = 1$, for any $z \in \mathbb{C}^n$, $|g(z)| \leq \sup_{z \in K} |g(z)|$ which implies $g \equiv 1$. Thus $\alpha \equiv 1$, so Φ is injective on $\operatorname{Hom}(\Lambda, S^1)$.

Per the discussion at the end of Section 3.2, every line bundle L on X can be presented as a quotient of a line bundle on $\mathbb{C}^n$ via a Λ-action of the form $\lambda \cdot (v, c) \mapsto (v + \lambda, \alpha(\lambda)c)$ for some homomorphism $\alpha : \Lambda \to \mathbb{C}^\times$. We may normalize α so that $\alpha(\Lambda) \subseteq S^1$, so $\Phi : \operatorname{Hom}(\Lambda, S^1) \to \operatorname{Pic}^0(X)$ is also surjective, hence an isomorphism. □

Putting everything together, any line bundle $L \in \mathrm{Pic}(X)$ determines a Chern class $c_1(L) \in H^2(X, \mathbb{Z})$ which in turn corresponds to an alternating form $[E] \in \bigwedge^2 \mathrm{Hom}(\Lambda, \mathbb{Z})$. By Lemma 3.3.10, E determines a Riemann form $H(x, y) = E(ix, y) + iE(x, y)$ on X. Further, under the splitting $\mathrm{Pic}(X) = \mathrm{Pic}^0(X) \oplus \mathbb{Z}$, the degree 0 part of L corresponds to some $\alpha \in \mathrm{Hom}(\Lambda, S^1)$ by Proposition 3.3.11. The pair (α, H) is called the *canonical pair* for the line bundle L and it is easy to check from the above construction that $\Phi(\alpha, H) = L(\alpha, H) \cong L$. This completes the proof of the Appell–Humbert theorem (3.3.3).

Definition. *The* **canonical factor of automorphy** *for a line bundle L on a complex torus X is the factor of automorphy for the Appell–Humbert pair (α, H) such that $L \cong L(\alpha, H)$.*

Example 3.3.12. For an elliptic curve $E = \mathbb{C}/[1, \tau]$ with Riemann form H and $\alpha_P : [1, \tau] \to S^1$ as defined in Example 3.3.4, the invertible sheaf $\mathcal{L}(\alpha_P, H) = \mathcal{O}_E(P)$ has canonical factor of automorphy

$$a_\lambda(v) = \alpha_P(\lambda) \exp\left[\pi H(v, \lambda) + \frac{\pi}{2} H(\lambda, \lambda)\right].$$

These factors of automorphy are precisely the factors of automorphy in the functional equations for theta functions $\theta \in H^0(E, L)$, generalizing those in Section 2.3.

To see the Appell–Humbert theorem in full for E, consider the short exact sequence

$$0 \to E \xrightarrow{AJ^{-1}} \mathrm{Pic}(E) \xrightarrow{c_1} \mathbb{Z} \to 0$$

where AJ^{-1} is the inverse of the Abel–Jacobi map for E and c_1 is the map sending $[L] \mapsto c_1(L)$. Then $AJ^{-1}(P) = \mathcal{O}_E(P - O)$ where O is the distinguished point of E (the Λ-orbit of $0 \in \mathbb{C}^n$). We claim $\mathcal{O}_E(P - O) \cong \mathcal{L}(\alpha_P, 0)$. One can see this by explicitly presenting the total space of $\mathcal{O}_E(P - O)$ as a quotient of the trivial line bundle $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ by the action $\lambda \cdot (z, w) = (\lambda + z, (-1)^{ab} \exp[2\pi i E(P, \lambda)]w)$ where $\lambda = a + b\tau$. More generally, since the above short exact sequence is split and $c_1(\mathcal{L}(\alpha_P, mH)) = m$ for any $m \in \mathbb{Z}$, we obtain

$$\mathcal{L}(\alpha_P, mH) \cong \mathcal{O}_E((m + 1)P - O) \cong \mathcal{O}_E(mP).$$

Likewise, if $D = \sum r_i P_i$ is a divisor of degree $\deg(D) = m$ on E, then

$$\mathcal{O}_E(D) \cong \mathcal{L}(\alpha_{P_1}^{r_1} \cdots \alpha_{P_n}^{r_n}, mH).$$

This fully describes $\mathrm{Pic}(E)$ for E a complex elliptic curve.

To close, we use the Appell–Humbert theorem to associate to every complex torus a *dual torus*. Let $X = \mathbb{C}^n/\Lambda$ be a complex torus. By Proposition 3.3.11, we have an isomorphism $\mathrm{Pic}^0(X) \cong \mathrm{Hom}(\Lambda, S^1)$. Notice that $\mathrm{Hom}(\Lambda, S^1)$ is a real torus, namely $\mathrm{Hom}(\Lambda, S^1) \cong \mathbb{R}^{2n}/\mathbb{Z}^{2n}$. We claim that one can endow this torus with a complex structure, hence inducing $\mathrm{Pic}^0(X)$ with the structure of a complex torus.

Set $V = \mathbb{C}^n$ and let V^* be the vector space of antilinear maps $f : V \to \mathbb{C}$, i.e. functions $f(z)$ satisfying $f(cz + dw) = \bar{c}f(z) + \bar{d}f(w)$ for all $z, w \in V$ and $c, d \in \mathbb{C}$. For a lattice $\Lambda \subseteq V$, let $\Lambda^* \subseteq V^*$ be the subspace of antilinear maps which take integer values on Λ. Then we have:

Proposition 3.3.13. *For any lattice $\Lambda \subseteq V$,*

(a) Λ^* *is a full lattice in* V^*.

(b) *There is an isomorphism*

$$\begin{aligned} V^*/\Lambda^* &\longrightarrow \mathrm{Hom}(\Lambda, S^1) \cong \mathrm{Pic}^0(X) \\ f &\longmapsto \alpha_f := \exp[2\pi i \,\mathrm{Im}\, f] \mapsto L(\alpha_f, 0). \end{aligned}$$

(c) *If* V/Λ *is an abelian variety, then so is* V^*/Λ^*.

Definition. *For a complex torus* $X = V/\Lambda$, *the corresponding quotient* $\widehat{X} := V^*/\Lambda^*$ *is called the* **dual torus** *of* X.

4 Projectivity of Abelian Varieties

4.1 Projective Morphisms

Let k be an algebraically closed field and recall that a morphism of k-varieties $\varphi : X \to \mathbb{A}^n$ is the same thing as an n-tuple of regular functions $x_1, \ldots, x_n \in \mathcal{O}_X(X)$. On the other hand, for a morphism $\varphi : X \to \mathbb{P}^n$ of the form

$$\varphi(P) = [x_0(P), \ldots, x_n(P)]$$

where $x_i \in \mathcal{O}_X(X)$ are $n+1$ sections having no common zeroes, this *does not* exhaust all morphisms $X \to \mathbb{P}^n$. For example, the identity map $\mathbb{P}^n \to \mathbb{P}^n$ is not of this form since the only regular functions on $\mathbb{P}^n$ are constant.

Instead, fix an open cover $\{U_i\}$ of X and assume that for each U_i, $\varphi_i := \varphi|_{U_i} : P \mapsto [s_0^i(P), \ldots, s_n^i(P)]$ for sections $s_k^i \in \mathcal{O}_X(U_i)$. Of course we must further require that for all $P \in U_i \cap U_j$,

$$[s_0^i(P), \ldots, s_n^i(P)] = [s_0^j(P), \ldots, s_n^j(P)].$$

This is equivalent to having $s_k^i(P) = \lambda_{ij}(P)s_k^j(P)$ for some $\lambda_{ij} \in \mathcal{O}_X(U_i \cap U_j)^\times$ and for *all* $0 \leq k \leq n$. For φ to define a global regular function $X \to \mathbb{P}^n$, the $\{\lambda_{ij}\}$ must satisfy the cocycle condition $\lambda_{i\ell} = \lambda_{ij}\lambda_{j\ell}$ on $U_i \cap U_j \cap U_\ell$. This defines a Čech class in $\check{H}^1(\mathcal{U}, \mathcal{O}_X^\times)$ which further descends to a class $[(\lambda_{ij})] \in H^1(X, \mathcal{O}_X^\times)$. Thus (λ_{ij}) determines an invertible sheaf $\mathcal{L}$ on X, and the s_k^i glue together to form sections $s_k \in \check{H}^0(\mathcal{U}, \mathcal{L}) = H^0(X, \mathcal{L})$.

Example 4.1.1. The twisting sheaf on $\mathbb{P}^n$ is an invertible sheaf $\mathcal{O}(1)$ defined as follows. Write $\mathbb{P}^n = \operatorname{Proj} A$ where $A = k[x_0, \ldots, x_n]$ and let $\mathcal{O} = \mathcal{O}_{\mathbb{P}^n}$ be the structure sheaf. Then any $\mathcal{O}$-module $\mathcal{E}$ corresponds to a graded A-algebra B. For any graded module B, let $B(d)$ be the graded module obtained by shifting the grading $d \in \mathbb{Z}$, i.e. $B(d)_i = B_{i+d}$. If $\mathcal{E}$ is the $\mathcal{O}$-module corresponding to B, then we get an $\mathcal{O}$-module $\mathcal{E}(d)$ corresponding to $B(d)$ for each $d \in \mathbb{Z}$. In particular, $\mathcal{O}$ (corresponding to the graded ring A) determines "twisted sheaves" $\mathcal{O}(d)$ for each $d \in \mathbb{Z}$, including the aforementioned $\mathcal{O}(1)$. For a $f \in A_1$ a homogeneous polynomial of degree 1, we have

$$\mathcal{O}(d)(D_+(f)) = f^d\mathcal{O}(D_+(f)) \quad \text{and} \quad \mathcal{O}(d)|_{D_+(f)} = f^d\mathcal{O}|_{D_+(f)}.$$

Alternatively, $\mathcal{O}(d) = \mathcal{L}(dH)$ where H is a general hyperplane divisor

$$H = a_0x_0 + \ldots + a_nx_n.$$

So for instance $\mathcal{O}(1) = \mathcal{L}(H)$. As a line bundle, (the total space of) $\mathcal{O}(1)$ corresponds to the projection

$$\begin{aligned} \mathbb{P}^{n+1} \smallsetminus \{[0, \ldots, 0, 1]\} &\longrightarrow \mathbb{P}^n \\ [z_0, \ldots, z_n, z_{n+1}] &\longmapsto [z_0, \ldots, z_n]. \end{aligned}$$

Definition. *Let X be a k-variety and $\mathcal{L}$ an invertible sheaf on X. We say $\mathcal{L}$ is* **generated by global sections** $s_0, \ldots, s_n \in H^0(X, \mathcal{L})$ *if for every point $P \in X$, the elements $s_{i,P}$ generate the stalk $\mathcal{L}_P$.*

Example 4.1.2. By construction $\mathcal{O}(1)$ is generated by the $n+1$ coordinate functions $x_0, \ldots, x_n$ on $\mathbb{P}^n$. This can be understood as saying the identity map $\mathbb{P}^n \to \mathbb{P}^n$ is induced by sections $x_0, \ldots, x_n \in H^0(\mathbb{P}^n, \mathcal{O}(1))$. Degree d maps $\mathbb{P}^n \to \mathbb{P}^n$ can be obtained similarly, using:

Proposition 4.1.3. *For each* $n \geq 1$, $\mathrm{Pic}(\mathbb{P}^n) = \langle \mathcal{O}(1) \rangle \cong \mathbb{Z}$.

For the rest of the section, we focus on how to use line bundles and sections to identify morphisms $X \to \mathbb{P}^n$ and when such morphisms are in fact embeddings. This can be stated quite generally.

Theorem 4.1.4. *Let A be a ring and X an A-scheme. Then*

(1) If $\varphi : X \to \mathbb{P}^n_A$ is a morphism of A-schemes, then $\mathcal{L} := \varphi^*\mathcal{O}(1)$ is a line bundle on X generated by global sections $s_i := \varphi^* x_i$ for $0 \leq i \leq n$. s

(2) Conversely, if $\mathcal{L}$ is an invertible sheaf on X with sections $s_0, \ldots, s_n \in H^0(X, \mathcal{L})$ that generate $\mathcal{L}$, then there is a unique morphism $\varphi : X \to \mathbb{P}^n_A$ such that $\mathcal{L} = \varphi^*\mathcal{O}(1)$ and $s_i = \varphi^* x_i$ for each $0 \leq i \leq n$.

Proof. (1) For any point $P \in X$, set $Q = \varphi(P) \in \mathbb{P}^n_A$. Then

$$\begin{aligned} \mathcal{L}_P &= (\varphi^*\mathcal{O}(1))_P \\ &= \mathcal{O}(1)_Q \otimes_{\mathcal{O}_Q} \mathcal{O}_{X,P} \\ &= \sum_{i=0}^{n} x_{i,Q}\mathcal{O}(1)_Q \otimes_{\mathcal{O}_Q} \mathcal{O}_{X,P} \\ &= \sum_{i=0}^{n} s_{i,P}\mathcal{O}_{X,P}. \end{aligned}$$

Thus $\mathcal{L}$ is globally generated.

(2) Now suppose $\mathcal{L}$ and $s_0, \ldots, s_n$ are given. We want to construct a morphism $\varphi : X \to \mathbb{P}^n_A$. Consider the open subsets $U_i = D_+(x_i) \subseteq \mathbb{P}^n_A$, which cover $\mathbb{P}^n_A$. Then $U_i = \mathrm{Spec}\, A[Y_0, \ldots, Y_n]$ where $Y_j = \frac{x_j}{x_i}$. (Usually we drop the redundant $Y_i = \frac{x_i}{x_i}$ from the generating set.) Let

$$X_i = \{P \in X \mid s_{i,P} \notin \mathfrak{m}_P \mathcal{L}_P\}$$

where $\mathfrak{m}_P \subseteq \mathcal{O}_{X,P}$ is the maximal ideal at P. Then each X_i is open and X is covered by $\{X_i\}$ since $s_0, \ldots, s_n$ generate $\mathcal{L}$. For each $0 \leq i \leq n$, we define $\varphi_i : X_i \to U_i$ by the comorphism

$$\begin{aligned} \varphi_i^* : A[Y_0, \ldots, Y_n] &\longrightarrow H^0(X_i, \mathcal{O}_{X_i}) \\ Y_j &\longmapsto \frac{s_j}{s_i}. \end{aligned}$$

Note that φ_i^* is well-defined since $s_i \neq 0$ on X_i and the ratio of two sections of an invertible sheaf defines a regular function. Also, it is clear by construction that φ_i^* is A-linear. These φ_i glue together on $X_i \cap X_j$ to produce a well-defined morphism $\varphi : X \to \mathbb{P}^n_A$. Uniqueness follows by (1). □