1

Abelian Varieties (10/06/03: Math 252, by W. Stein)

This chapter provides foundational background about abelian varieties and Jacobians, with an aim toward what we will need later when we construct abelian varieties attached to modular forms. We will not give complete proofs of very much, but will try to give precise references whenever possible, and many examples.

We will follow the articles by Rosen [3] and Milne [1] on abelian varieties. We will try primarily to explain the statements of the main results about abelian varieties, and prove results when the proofs are not too technical and enhance understanding of the statements.

1.1 Abelian Varieties

Definition 1.1.1 (Variety). A *variety* X over a field k is a finite-type separated scheme over k that is geometrically integral.

The condition that X be geometrically integral means that $X_{\overline{k}}$ is reduced (no nilpotents in the structure sheaf) and irreducible.

Definition 1.1.2 (Group variety). A *group variety* is a group object in the category of varieties. More precisely, a group variety X over a field k is a variety equipped with morphisms

$$m : X \times X \to X \quad \text{and} \quad i : X \to X$$

and a point $1_X \in A(k)$ such that m, i, and 1_X satisfy the axioms of a group; in particular, for every k-algebra R they give $X(R)$ a group structure that depends in a functorial way on R.

Definition 1.1.3 (Abelian Variety). An *abelian variety* A over a field k is a complete group variety.

Theorem 1.1.4. *Suppose A is an abelian variety. Then*

1. *The group law on A is commutative.*

2. *A is projective, i.e., there is an embedding from A into $\mathbf{P}^n$ for some n.*

3. *If $k = \mathbf{C}$, then $A(k)$ is analytically isomorphic to V/L, where V is a finite-dimensional complex vector space and L is a lattice in V. (A lattice is a free $\mathbf{Z}$-module of rank equal to $2 \dim V$ such that $\mathbf{R}L = V$.)*

Proof. Part 1 is not too difficult, and can be proved by showing that every morphism of abelian varieties is the composition of a homomorphism with a translation, then applying this result to the inversion map (see [1, Cor. 2.4]). Part 2 is proved with some effort in [1, §7]. Part 3 is proved in [2, §I.1] using the exponential map from Lie theory from the tangent space at 0 to A. □

1.2 Complex Tori

Let A be an abelian variety over $\mathbf{C}$. By Theorem 1.1.4, there is a complex vector space V and a lattice L in V such that $A(\mathbf{C}) = V/L$, that is to say, $A(\mathbf{C})$ is a complex torus.

More generally, if V is any complex vector space and L is a lattice in V, we call the quotient $T = V/L$ a *complex torus*. In this section, we prove some results about complex tori that will help us to understand the structure of abelian varieties, and will also be useful in designing algorithms for computing with abelian varieties.

The differential 1-forms and first homology of a complex torus are easy to understand in terms of T. If $T = V/L$ is a complex torus, the tangent space to $0 \in T$ is canonically isomorphic to V. The $\mathbf{C}$-linear dual $V^* = \mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C})$ is isomorphic to the $\mathbf{C}$-vector space $\Omega(T)$ of holomorphic differential 1-forms on T. Since $V \to T$ is the universal covering of T, the first homology $\mathrm{H}_1(T, \mathbf{Z})$ of T is canonically isomorphic to L.

1.2.1 Homomorphisms

Suppose $T_1 = V_1/L_1$ and $T_2 = V_2/L_2$ are two complex tori. If $\varphi : T_1 \to T_2$ is a (holomorphic) homomorphism, then φ induces a $\mathbf{C}$-linear map from the tangent space of T_1 at 0 to the tangent space of T_2 at 0. The tangent space of T_i at 0 is canonically isomorphic to V_i, so φ induces a $\mathbf{C}$-linear map $V_1 \to V_2$. This maps sends L_1 into L_2, since $L_i = \mathrm{H}_1(T_i, \mathbf{Z})$. We thus have the following diagram:

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ L_1 & \xrightarrow{\rho_{\mathbf{Z}}(\varphi)} & L_2 \\ \downarrow & & \downarrow \\ V_1 & \xrightarrow{\rho_{\mathbf{C}}(\varphi)} & L_2 \\ \downarrow & & \downarrow \\ T_1 & \xrightarrow{\varphi} & T_2 \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array} \tag{1.2.1}$$

We obtain two faithful representations of $\mathrm{Hom}(T_1, T_2)$,

$$\rho_{\mathbf{C}} : \mathrm{Hom}(T_1, T_2) \to \mathrm{Hom}_{\mathbf{C}}(V_1, V_2)$$

$$\rho_{\mathbf{Z}} : \mathrm{Hom}(T_1, T_2) \to \mathrm{Hom}_{\mathbf{Z}}(L_1, L_2).$$

Suppose $\psi \in \mathrm{Hom}_{\mathbf{Z}}(L_1, L_2)$. Then $\psi = \rho_{\mathbf{Z}}(\varphi)$ for some $\varphi \in \mathrm{Hom}(T_1, T_2)$ if and only if there is a complex linear homomorphism $f : V_1 \to V_2$ whose restriction to L_1 is ψ. Note that $f = \psi \otimes \mathbf{R}$ is uniquely determined by ψ, so ψ arises from some φ precisely when f is $\mathbf{C}$-linear. This is the case if and only if $fJ_1 = J_2 f$, where $J_n : V_n \to V_n$ is the $\mathbf{R}$-linear map induced by multiplication by $i = \sqrt{-1} \in \mathbf{C}$.

Example 1.2.1.

1. Suppose $L_1 = \mathbf{Z} + \mathbf{Z}i \subset V_1 = \mathbf{C}$. Then with respect to the basis $1, i$, we have $J_1 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. One finds that $\mathrm{Hom}(T_1, T_1)$ is the free $\mathbf{Z}$-module of rank 2 whose image via $\rho_{\mathbf{Z}}$ is generated by J_1 and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. As a ring $\mathrm{Hom}(T_1, T_1)$ is isomorphic to $\mathbf{Z}[i]$.

2. Suppose $L_1 = \mathbf{Z} + \mathbf{Z}\alpha i \subset V_1 = \mathbf{C}$, with $\alpha^3 = 2$. Then with respect to the basis $1, \alpha i$, we have $J_1 = \left(\begin{smallmatrix} 0 & -\alpha \\ 1/\alpha & 0 \end{smallmatrix}\right)$. Only the scalar integer matrices commute with J_1.

Proposition 1.2.2. *Let T_1 and T_2 be complex tori. Then* $\mathrm{Hom}(T_1, T_2)$ *is a free* $\mathbf{Z}$*-module of rank at most* $4 \dim T_1 \cdot \dim T_2$.

Proof. The representation $\rho_{\mathbf{Z}}$ is faithful (injective) because φ is determined by its action on L_1, since L_1 spans V_1. Thus $\mathrm{Hom}(T_1, T_2)$ is isomorphic to a subgroup of $\mathrm{Hom}_{\mathbf{Z}}(L_1, L_2) \cong \mathbf{Z}^d$, where $d = 2 \dim V_1 \cdot 2 \dim V_2$. □

Lemma 1.2.3. *Suppose $\varphi : T_1 \to T_2$ is a homomorphism of complex tori. Then the image of φ is a subtorus of T_2 and the connected component of* $\ker(\varphi)$ *is a subtorus of T_1 that has finite index in* $\ker(\varphi)$.

Proof. Let $W = \ker(\rho_{\mathbf{C}}(\varphi))$. Then the following diagram, which is induced by φ, has exact rows and columns:

$$
\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
0 & \to & L_1 \cap W & \to & L_1 & \to & L_2 & \to & L_2/\varphi(L_1) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & W & \to & V_1 & \to & V_2 & \to & V_2/\varphi(V_1) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \ker(\varphi) & \to & T_1 & \to & T_2 & \to & T_2/\varphi(T_1) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & & 0 & &
\end{array}
$$

Using the snake lemma, we obtain an exact sequence

$$0 \to L_1 \cap W \to W \to \ker(\varphi) \to L_2/\varphi(L_1) \to V_2/\varphi(V_1) \to T_2/\varphi(T_1) \to 0.$$

Note that $T_2/\varphi(T_1)$ is compact because it is the continuous image of a compact set, so the cokernel of φ is a torus (it is given as a quotient of a complex vector space by a lattice).

The kernel $\ker(\varphi) \subset T_1$ is a closed subset of the compact set T_1, so is compact. Thus $L_1 \cap W$ is a lattice in W. The map $L_2/\varphi(L_1) \to V_2/\varphi(V_1)$ has kernel generated by the saturation of $\varphi(L_1)$ in L_2, so it is finite, so the torus $W/(L_1 \cap W)$ has finite index in $\ker(\varphi)$. □

Remark 1.2.4. The category of complex tori is not an abelian category because kernels need not be in the category.

1.2.2 Isogenies

Definition 1.2.5 (Isogeny). An *isogeny* $\varphi : T_1 \to T_2$ of complex tori is a surjective morphism with finite kernel. The *degree* $\deg(\varphi)$ of φ is the order of the kernel of φ.

Note that $\deg(\varphi \circ \varphi') = \deg(\varphi)\deg(\varphi')$.

Lemma 1.2.6. *Suppose that φ is an isogeny. Then the kernel of φ is isomorphic to the cokernel of $\rho_{\mathbf{Z}}(\varphi)$.*

Proof. (This is essentially a special case of Lemma 1.2.3.) Apply the snake lemma to the morphism (1.2.1) of short exact sequences, to obtain a six-term exact sequence

$$0 \to K_L \to K_V \to K_T \to C_L \to C_V \to C_T \to 0,$$

where K_X and C_X are the kernel and cokernel of $X_1 \to X_2$, for $X = L, V, T$, respectively. Since φ is an isogeny, the induced map $V_1 \to V_2$ must be an isomorphism, since otherwise the kernel would contain a nonzero subspace (modulo a lattice), which would be infinite. Thus $K_V = C_V = 0$. It follows that $K_T \cong C_L$, as claimed. □

One consequence of the lemma is that if φ is an isogeny, then

$$\deg(\varphi) = [L_1 : \rho_{\mathbf{Z}}(\varphi)(L_1)] = |\det(\rho_{\mathbf{Z}}(\varphi))|.$$

Proposition 1.2.7. *Let T be a complex torus of dimension d, and let n be a positive integer. Then multiplication by n, denoted $[n]$, is an isogeny $T \to T$ with kernel $T[n] \cong (\mathbf{Z}/n\mathbf{Z})^{2d}$ and degree n^{2d}.*

Proof. By Lemma 1.2.6, $T[n]$ is isomorphic to L/nL, where $T = V/L$. Since $L \approx \mathbf{Z}^{2d}$, the proposition follows. □

We can now prove that isogeny is an equivalence relation.

Proposition 1.2.8. *Suppose $\varphi : T_1 \to T_2$ is a degree m isogeny of complex tori of dimension d. Then there is a unique isogeny $\hat{\varphi} : T_2 \to T_1$ of degree m^{2d-1} such that $\hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [m]$.*

Proof. Since $\ker(\varphi) \subset \ker([m])$, the map $[m]$ factors through φ, so there is a morphism $\hat{\varphi}$ such that $\hat{\varphi} \circ \varphi = [m]$:

$$\begin{array}{ccc} T_1 & \xrightarrow{\varphi} & T_2 \\ & {\scriptstyle [m]}\searrow & \downarrow{\scriptstyle \hat{\varphi}} \\ & & T_1 \end{array}$$

We have

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

This implies that $\varphi \circ \hat{\varphi} = [m]$, since φ is surjective. Uniqueness is clear since the difference of two such morphisms would vanish on the image of φ. To see that $\hat{\varphi}$ has degree m^{2d-1}, we take degrees on both sides of the equation $\hat{\varphi} \circ \varphi = [m]$. □

1.2.3 Endomorphisms

The ring $\mathrm{End}(T) = \mathrm{Hom}(T, T)$ is called the *endomorphism ring* of the complex torus T. The *endomorphism algebra* of T is $\mathrm{End}_0(T) = \mathrm{End}(T) \otimes_{\mathbf{Z}} \mathbf{Q}$.

Definition 1.2.9 (Characteristic polynomial). The *characteristic polynomial* of $\varphi \in \mathrm{End}(T)$ is the characteristic polynomial of the $\rho_{\mathbf{Z}}(\varphi)$. Thus the characteristic polynomial is a monic polynomial of degree $2 \dim T$.

1.3 Abelian Varieties as Complex Tori

References

[1] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[2] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[3] M. Rosen, *Abelian varieties over* **C**, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 79–101.