Lecture 2: Abelian varieties

The subject of abelian varieties is vast. In these notes we will hit some highlights of the theory, stressing examples and intuition rather than proofs (due to lack of time, among other reasons). We will note analogies with the more concrete case of elliptic curves (as in [Si]), as well as places where elliptic curves provide a poor guide for what to expect. In addition, we will use the complex-analytic theory and the example of Jacobians as sources of inspiration and examples to illustrate general results. For arithmetic purposes it is essential to allow the ground field to be of arbitrary characteristic (e.g., finite fields), and not algebraically closed.

At the end, we explain Chabauty's clever argument that proves the Mordell conjecture for curves of genus $g \geq 2$ whose Jacobian has Mordell–Weil rank less than g. In later lectures we will bootstrap from the case of individual abelian varieties to "families" of abelian varieties, or as we will call them, *abelian schemes*. This concept, along with related notions such as "good reduction" and "semistable reduction" will be an essential ingredient in Faltings' method. But for this lecture we restrict attention to the more concrete setting of a single fixed abelian variety over a field. Nonetheless, the later need for a mature theory of families over a parameter space of mixed-characteristic (even for the special case of modular curves over $\mathbf{Z}_{(p)}$, required to make sense of "reduction mod p" for modular curves) forces us to allow *arbitrary* ground fields, including imperfect ones like $\mathbf{F}_p(t)$, as those always show up at generic points of special fibers when the parameter space has positive-dimensional fibers in each characteristic, as will happen in nearly all examples of moduli spaces that arise in Faltings' work and throughout arithmetic geometry.

Some excellent references are [Mi1], [Mi2], and [Mu] (which together contain proofs for most of what we assert below). The latter develops the complex-analytic theory as well as the algebraic theory in all essential respects (using scheme-theoretic methods when necessary), but assumes the ground field is algebraically closed. In [Mi1], the theory over a general field is deduced from the theory over an algebraically closed field. One can also take a more "direct" approach and develop the entire theory from the beginning over a general field (often reducing to the algebraically closed case in many proofs, provided one has good techniques at one's disposal). This is what is done in a forthcoming book by B. Moonen and G. van der Geer on abelian varieties (see Moonen's webpage). Mumford's elegant (yet terse) writing style is hard to improve upon.

Notation. We write $\mathbf{Z}(1)$ to denote the kernel of $\exp : \mathbf{C} \to \mathbf{C}^\times$ (so $\mathbf{Z}(1)$ is free of rank 1 over $\mathbf{Z}$, with basis $\pm 2\pi\sqrt{-1}$). Using $\exp(z/n)$, we identify $\mathbf{Z}(1)/n\mathbf{Z}(1)$ with the ground $\mu_n(\mathbf{C})$ of nth roots of unity in $\mathbf{C}$.

For a field k with $\mathrm{char}(k) \nmid n$, we often write μ_n to denote the cyclic group $\mu_n(k_s)$ of nth roots of unity in a separable closure k_s when k is understood from context; this is naturally a module over $\mathrm{Gal}(k_s/k)$. Likewise, for a prime $\ell \neq \mathrm{char}(k)$ we write $\mathbf{Z}_\ell(1)$ to denote the ℓ-adic Tate module $\varprojlim \mu_{\ell^r}(k_s)$ of the algebraic group GL_1 over k (equipped with the natural continuous action of $\mathrm{Gal}(k_s/k)$). These arise in Weil pairings and generalizations.

1. Some motivation

We begin by describing Weil's idea for how to prove the Mordell Conjecture. First, we have to review an important construction with compact Riemann surfaces. Let X be a

connected compact Riemann surface with genus $g \geq 0$. The vector space $\Omega^1(X)$ of global holomorphic 1-forms on X is g-dimensional, and its linear dual $\Omega^1(X)^*$ contains the rank-$2g$ finite free $\mathbf{Z}$-module $\mathrm{H}_1(X, \mathbf{Z})$ as a sublattice via the inclusion $\mathrm{H}_1(X, \mathbf{Z}) \to \Omega^1(X)^*$ that assigns to any loop σ the functional $\int_\sigma : \omega \mapsto \int_\sigma \omega$ on holomorphic 1-forms. By using a little bit of Hodge theory on X, one proves that this really is a lattice: a discrete subgroup with compact quotient

$$J_X := \Omega^1(X)^*/\mathrm{H}_1(X, \mathbf{Z})$$

that is called the *Jacobian* of X.

Fix a base point $x_0 \in X$. For any $x \in X$ we get a linear functional $\int_{x_0}^x : \Omega^1(X) \to \mathbf{C}$ by integrating along a chosen path from x_0 to x. This functional is not actually well-defined: if we change the choice of path then this functional may change. However, any two such paths "differ" by a loop, and more specifically the ambiguity lies in the lattice $\mathrm{H}_1(X, \mathbf{Z})$. Hence, we do get a well-defined map

$$i_{x_0} : X \to J_X$$

via $i_{x_0}(x) = \int_{x_0}^x \mathrm{mod} \mathrm{H}_1(X, \mathbf{Z})$.

Example 1.1. If $g = 1$ then this recovers the classical uniformization of elliptic curves.

It turns out that if $g \geq 1$ then i_{x_0} is an isomorphism onto a closed (complex) submanifold. (The Abel–Jacobi theorem gives even finer information.) In particular, if $g \geq 2$ then X is a curve in a *higher-dimensional* complex torus J_X.

Now we can formulate Weil's idea. Let us suppose that, despite the apparently very analytic method of construction of J_X and i_{x_0}, there is a way to make them entirely within algebraic geometry. More specifically, if C is a smooth projective (geometrically connected) curve of genus $g \geq 1$ over a number field $K \subset \mathbf{C}$ and $c_0 \in C(K)$ is a point then *assume* there is a projective group variety J_C of dimension g over K and a closed embedding of K-varieties $i_{c_0} : C \to J_C$ such that extending scalars to $\mathbf{C}$ and passing to the corresponding complex manifolds recovers the above analytic constructions. Of what use would this be?

If such objects over K exist compatibly with the complex-analytic theory (as we will later see *does* always happen) then $C(K)$ is identified with $C(\mathbf{C}) \cap J_C(K)$. Hence, if $J_C(K)$ is *finitely generated* (a purely arithmetic assertion, once the definition of J_C over K is understood), then the finiteness of $C(K)$ would be reduced to the following purely analytic assertion for $X = C(\mathbf{C})$: if Γ is a finitely generated subgroup of J_X then $i_{x_0}(X) \cap \Gamma$ is *finite*.

It was to carry out this idea that Weil proved the Mordell–Weil theorem in his thesis (using an older language of divisor classes on curves over number fields, since at the time there was no algebro-geometric theory of projective group varieties; e.g., the formulation of the Mordell–Weil theorem in terms of general abelian varieties only came much later). In the end the Mordell–Weil theorem has no role to play in Faltings' proof, and surprisingly the only known way to prove Weil's purely analytic conjecture concerning finiteness of $\Gamma \cap i_{x_0}(X)$ is to *derive* it from (Faltings' later generalization of) the Mordell Conjecture!

2. The complex-analytic theory: first definitions

Exactly as in the case of elliptic curves, a tremendous amount of intuition for abelian varieties will arise from their complex-analytic incarnation. To that end, we begin with

some analytic considerations. One big difference between real-analytic and complex-analytic functions in several variables is that the latter satisfy a maximum principle. Consequently, connected compact complex manifolds admit only *constant* global functions, in contrast with connected compact real-analytic manifolds (such as spheres). Likewise, whereas there is an extremely rich and nontrivial theory of non-commutative compact real Lie groups, in the complex-analytic case things are much simpler:

Proposition 2.1. *For $g \geq 1$, every g-dimensional connected compact complex Lie group is commutative, and has the form V/L for a g-dimensional $\mathbf{C}$-vector space V and a rank-$2g$ discrete lattice $L \simeq \mathbf{Z}^{2g}$ in V.*

We call any such group a *complex torus*, since any $\mathbf{Z}$-basis of L viewed as an $\mathbf{R}$-basis of V yields $V/L \simeq (\mathbf{R}/\mathbf{Z})^{2g} = (S^1)^{2g}$ as real Lie groups.

In striking contrast with the case $g = 1$, when $g > 1$ it turns out that "most" lattices L in $\mathbf{C}^g$ yield a complex torus $\mathbf{C}^g/L$ admitting no non-constant meromorphic functions whatsoever. That is, $\mathbf{C}^g$ does not admit non-constant L-periodic meromorphic functions. Those admitting "many" such functions are given a special name:

Theorem 2.2. *For a complex torus X of dimension $g > 0$, the following are equivalent:*

(1) *X is isomorphic to a submanifold of a complex projective space;*
(2) *there is a complex variety W whose associated complex manifold is isomorphic to X;*
(3) *there exist g algebraically independent meromorphic functions on X.*

In such cases, W is unique and functorial in X, and the group law on X arises from a unique group variety structure on W.

Such complex tori are called *abelian varieties* (over $\mathbf{C}$). To be precise, it is really W in (2) that is the abelian variety, but since W is unique and functorial in X it is permissible to abuse terminology and call X the abelian variety. There is a subtle explicit condition on a lattice L in $\mathbf{C}^g$ (called *Riemann's bilinear relations*) which characterizes when $\mathbf{C}^g/L$ is an abelian variety.

Example 2.3. Let $K/\mathbf{Q}$ be a CM field of degree $2g$, so K is quadratic over its maximal totally real subfield K_0 and there are $2g$ distinct embeddings $K \hookrightarrow \mathbf{C}$. These embeddings come in conjugate pairs. Fix a set Φ of g such embeddings, one from each conjugate pair. (There are 2^g such choices of Φ.) In other words, Φ is a choice of lifting of each embedding $K_0 \hookrightarrow \mathbf{R}$ to an embedding $K \hookrightarrow \mathbf{C}$.

Define the $\mathbf{C}$-vector space $V_\Phi = \mathbf{R} \otimes_{\mathbf{Q}} K$ as follows:

$$\mathbf{R} \otimes_{\mathbf{Q}} K = (\mathbf{R} \otimes_{\mathbf{Q}} K_0) \otimes_{K_0} K = \prod_{v_0|\infty} (\mathbf{R} \otimes_{v_0, K_0} K),$$

where $\mathbf{R} \otimes_{v_0,K_0} K$ is identified with $\mathbf{C}$ by using the unique $\varphi \in \Phi$ whose restriction to K_0 is v_0.

For instance, if $g = 1$ then Φ is a choice of one of the two embeddings of the imaginary quadratic field K into $\mathbf{C}$, and this chosen embedding identifies $\mathbf{R} \otimes_{\mathbf{Q}} K$ with $\mathbf{C}$, thereby defining the complex structure on V_Φ.

The integer ring $\mathscr{O}_K$ is a lattice in K, and hence in $\mathbf{R} \otimes_{\mathbf{Q}} K = V_\Phi$, so we get a complex torus $X_\Phi := V_\Phi/\mathscr{O}_K$. It is a deep fact that such complex tori are abelian varieties.

Example 2.4. The analytic Jacobian of a connected compact Riemann surface is always an abelian variety. In this case, Riemanns' bilinear relations amount to some properties of the intersection form on the degree-1 homology of the Riemann surface.

Example 2.5. Let V/L be a complex torus. Let $\overline{V}$ be the conjugate space (i.e., V with $\mathbf{C}$-structure twisted by complex conjugation), and for any $v \in V$ let $\overline{v} = 1 \otimes v \in \overline{V}$. Let $V' = \overline{V}^*$ be the $\mathbf{C}$-linear dual, and define L' to consist of those $\ell \in V'$ such that $\ell(\overline{\lambda}) \in \mathbf{Z}(1) := 2\pi\sqrt{-1}\mathbf{Z}$ for all $\lambda \in L$. Then it turns out that L' is a lattice in V', and V'/L' is called the *dual complex torus*. Using Riemann's bilinear relations, one can show that if V/L is an abelian variety, so is V'/L'. Rather non-obvious is that fact (which we will address later) that the construction of V'/L' from V/L can be described in purely algebro-geometric terms that make sense over ground fields different from $\mathbf{C}$.

3. Algebraic theory: first definitions

Let k be an arbitrary field.

Definition 3.1. An *abelian variety* over k is a smooth connected complete group variety A over k.

Recall that *group variety* means that there are given maps of k-varieties

$$m : A \times A \to A, \;\; i : A \to A$$

and a point $e \in A(k)$ such that habitual diagrams describing the group axioms (associativity, 2-sided identity, etc.) all commute. It is a nontrivial fact that abelian varieties over k are necessarily projective over k, and that their group law is *commutative*. In the 1-dimensional case, we recover the notion of elliptic curve. In higher dimensions, the first natural class of examples (beyond silliness like products of several elliptic curves) is:

Example 3.2. Let X be a smooth projective (geometrically connected) curve over k, with genus $g > 0$. Then attached to X is a certain abelian variety J_X over k of dimension g called its *Jacobian*. We will address the precise definition of J_X later (see Definition 4.10). For now we simply record that $J_X(\overline{k})$ is identified with the degree-0 divisor class group of the curve $X_{\overline{k}}$ over $\overline{k}$, and that if $k = \mathbf{C}$ then this can be canonically identified with the Jacobian we have already seen in the complex-analytic theory.

Here are some facts for elliptic curves that are *false* for abelian varieties in general (due to the richer geometry in higher dimensions):

Example 3.3. A nonzero homomorphism between abelian varieties of the same dimension need not be surjective, nor have finite kernel. Also, in contrast with the planar cubic realization of every elliptic curve, for a fixed $g > 1$ there is *no* evident uniform upper bound of the dimension of a projective space into which all g-dimensional abelian varieties can be embedded as closed subvarieties (even over an algebraically closed field). Such an upper bound does actually exist, using a result called Zarhin's trick; see Example 5.15.

Some familiar facts from the theory of elliptic curves remain true, but with much harder proofs (since we cannot appeal to the theory of algebraic curves):

Theorem 3.4. *Let A be an abelian variety of dimension $g > 0$ over a field k.*

(1) *The group law on A is uniquely determined by the origin $e \in A(k)$, and if A' is another abelian variety then any k-variety map $f : A \to A'$ satisfying $f(e) = e'$ automatically respects the group laws and inversions.*
(2) *Every global 1-form on A is translation-invariant.*
(3) *For any homomorphism $f : A \to A'$ between abelian varieties with the same dimension $g > 0$, the following conditions are equivalent: f is surjective, f has finite fibers,* $\ker f$ *is finite on $\overline{k}$-points. Such maps are called* isogenies*, and the finite degree $[k(A) : k(A')]$ of the function field extension is called the* degree *of the isogeny f.*
(4) *For every nonzero integer n, the map $[n]_A : A \to A$ is an isogeny of degree n^{2g}.*

Since a finite extension of fields in characteristic $p > 0$ is separable whenever its degree is not divisible by p, it follows that an isogeny of degree not divisible by $\mathrm{char}(k)$ is always separable. In particular, if an integer n is not divisible by $\mathrm{char}(k)$ then $[n]_A$ is a separable isogeny. The following basic result makes precise the sense in which a separable isogeny is like a quotient map:

Proposition 3.5. *Let $f : A \to A'$ be a separable isogeny of degree $d > 0$.*

(1) *Every point in the kernel of $A(\overline{k}) \to A'(\overline{k})$ is defined over k_s and there are exactly d such points. This subgroup of $A(k_s)$ is* $\mathrm{Gal}(k_s/k)$*-stable.*
(2) *Every k-homomorphism $h : A \to B$ to another abelian variety over k such that $h_{\overline{k}}$ kills* $(\ker f)(\overline{k})$ *uniquely factors as*

$$A \xrightarrow{f} A' \xrightarrow{h'} B$$

for a k-homomorphism h'.
(3) *Conversely, if $G \subset A(k_s)$ is a* $\mathrm{Gal}(k_s/k)$*-stable finite subgroup of size d then there exists a degree-d separable isogeny $A \to \overline{A}$ of abelian varieties over k whose kernel on $\overline{k}$-points is exactly G; we often write A/G to denote $\overline{A}$.*
(4) *If $f : A \to A'$ is an isogeny with degree d then there is an isogeny $f' : A' \to A$ such that $f' \circ f = [d]_A$ and $f \circ f' = [d]_{A'}$. Conversely, if $f : A \to A'$ is a k-homomorphism such that f factors through $[n]_A$ or $[n]_{A'}$ for a nonzero integer n then f is an isogeny.*

In view of (4), it is a symmetric condition on a pair of abelian varieties over k that there exist an isogeny between them over k in either direction. We then say that the two abelian varieties are *k-isogenous*.

There is a variant on the first three parts of the preceding proposition when the separability hypothesis on the isogenies is dropped. This is very important, since over finite fields (and even general fields of positive characteristic), Frobenius-type homomorphisms are ubiquitous in the theory, just as for elliptic curves. However, the appropriate formulation of the preceding proposition in the absence of separability conditions requires the theory of group schemes, so we ignore it here.

Example 3.6. Let n be an integer not divisible by $\mathrm{char}(k)$. Then $A[n] \subset A(k_s)$ denotes the $\mathrm{Gal}(k_s/k)$-stable subgroup of n-torsion elements, and $[n]_A : A \to A$ identifies the target A with the quotient $A/A[n]$.

4. Tate modules, duality, and applications

By exactly the same arguments as one uses for elliptic curves, we obtain:

Proposition 4.1. *Let A be an abelian variety over a field k of dimension $g > 0$.*

(1) *If $n, m \geq 1$ are integers not divisible by $\mathrm{char}(k)$ then the sequence of groups*

$$0 \to A[n] \to A[nm] \stackrel{[n]_A}{\to} A[m] \to 0$$

is short exact and $\mathrm{Gal}(k_s/k)$-equivariant.

(2) *For a prime $\ell \neq \mathrm{char}(k)$, each $A[\ell^r]$ is a finite free $\mathbf{Z}/(\ell^r)$-module of rank $2g$, and the* Tate module $T_\ell(A) := \varprojlim A[\ell^r]$ *is a finite free $\mathbf{Z}_\ell$-module of rank $2g$ such that the natural map*

$$T_\ell(A)/(\ell^r) \to A[\ell^r]$$

is an isomorphism for all $r \geq 1$. The natural $\mathrm{Gal}(k_s/k)$-action on $T_\ell(A)$ is continuous for the ℓ-adic topology.

As for elliptic curves, we also work with the $\mathbf{Q}_\ell$-vector space $V_\ell(A) = \mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} T_\ell(A)$ of dimension $2g$.

In the special case $k = \mathbf{C}$, if A is an abelian variety over k with dimension $g > 0$ and if V/L is the corresponding analytic uniformization of the complex torus $A(\mathbf{C})$ then $A[n] = (1/n)L/L$. Using multiplication by n to identify $(1/n)L/L$ with L/nL, the quotient map $[m]_A : A[nm] \to A[n]$ is identified with the reduction map $L/(nm)L \twoheadrightarrow L/nL$. Hence, $T_\ell(A)$ is identified with the ℓ-adic completion of $L = \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$, so

$$T_\ell(A) \simeq \mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z}) \simeq \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z}_\ell).$$

This is very interesting, exactly as for elliptic curves, since if $f \in \mathrm{End}(A)$ is an endomorphism then the induced endomorphism $\mathrm{H}_1(f) \in \mathrm{End}(L)$ uniquely determines f and its ℓ-adic scalar extension is identified with the induced endomorphism $T_\ell(f)$. In other words, the $\mathbf{Z}_\ell$-linear endomorphism $T_\ell(f)$ of $T_\ell(A)$ has characteristic polynomial in $\mathbf{Z}[t] \subset \mathbf{Z}_\ell[t]$ which is *independent of* ℓ. In the algebraic theory over a general field (especially in positive characteristic) there is nothing like integral homology, but the ℓ-adic Tate modules provide an excellent substitute:

Theorem 4.2. *Let A and A' be nonzero abelian varieties over a field k, and $\ell \neq \mathrm{char}(k)$ a prime.*

(1) *The natural map $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A, A') \to \mathrm{Hom}_{\mathbf{Z}_\ell[\mathrm{Gal}(k_s/k)]}(T_\ell(A), T_\ell(A'))$ is injective.*

(2) *The $\mathbf{Z}$-module $\mathrm{Hom}_k(A, A')$ is finitely generated with rank at most $4 \dim A \cdot \dim A'$.*

(3) *If A and A' have a common dimension $g > 0$, then a k-homomorphism $f : A \to A'$ is an isogeny if and only if $V_\ell(f)$ is an isomorphism.*

(4) *For any $f \in \mathrm{End}_k(A)$, the characteristic polynomial of $T_\ell(f)$ on $T_\ell(A)$ lies in $\mathbf{Z}[t] \subset \mathbf{Z}_\ell[t]$ and is independent of ℓ.*

The $\mathbf{Z}$-finiteness in part (2) is proved by a method that is similar in spirit to the case of elliptic curves, except that heaver geometric input is needed to push through the idea.

Example 4.3. Let $f : A \to A'$ be a map between abelian varieties of a common dimension $g > 0$ over a field k, and $\ell \neq \mathrm{char}(k)$ a prime. Then f is an isogeny if and only if $V_\ell(f) : V_\ell(A) \to V_\ell(A')$ is an isomorphism of $\mathbf{Q}_\ell$-vector spaces. Indeed, if f is an isogeny and $f' : A' \to A$ is another isogeny such that $f' \circ f = [d]_A$ and $f \circ f' = [d]_{A'}$ for a nonzero integer d then $(1/d)V_\ell(f')$ is inverse to $V_\ell(f)$. Conversely, if $V_\ell(f)$ is an isomorphism then the abelian subvariety $B := f(A)$ in A' has the property that $V_\ell(f)$ factors through $V_\ell(B)$, forcing $V_\ell(B) = V_\ell(A')$. Comparing $\mathbf{Q}_\ell$-dimensions, it follows that $\dim B = \dim A'$, which is to say $B = A'$, so f is surjective. Since A and A' are assumed to have the same dimension, this forces f to be an isogeny.

Remark 4.4. Sam will later present Tate's proof of the important fact that the injective map in Theorem 4.2(1) is an isomorphism when k is *finite*. Many of the ideas in that argument influenced later developments (including Faltings' proof of the Mordell Conjecture), and Tate conjectured that this map is an isomorphism whenever k is finitely generated over its prime field. The case of positive characteristic was settled by Zahrin (modulo some difficulties in characteristic 2 that were cleared up by Moret-Bailly), and the case of characteristic 0 was settled by Faltings. In the case of number fields, this result of Faltings was an essential step in his proof of the Mordell Conjecture.

Theorem 4.5 (Weil)**.** *Let A be an abelian variety of dimension $g > 0$ over a finite field k of size q. Let $f_A \in \mathbf{Z}[t]$ be the common monic characteristic polynomial of degree $2g$ for the q-Frobenius endomorphism of A acting on $T_\ell(A)$ for all $\ell \neq \mathrm{char}(k)$.*

Every root of f_A is an algebraic integer whose $\mathbf{C}$-embeddings all have absolute value $q^{1/2}$.

To go further, it becomes necessary to introduce a concept which is invisible in the case of elliptic curves: the *dual abelian variety*. This is an algebraic substitute for Example 2.5. To explain this, we need to make a brief digression to discuss families of line bundles.

Definition 4.6. Let X be a projective variety over a field k. For any (possibly disconnected) k-variety T, a *family of line bundles on X parameterized by T* is a line bundle $\mathscr{L}$ on $X \times T$. For any $x_0 \in X(k)$, a *trivialization* of $\mathscr{L}$ along x_0 is an isomorphism $\varphi : (x_0 \times 1_T)^*(\mathscr{L}) \simeq \mathscr{O}_T$ on T.

A line bundle $\mathscr{N}$ on X is *algebraically equivalent to* 0 if there is a family $\mathscr{L}$ as above with *connected* T such that for some $t_0, t_1 \in X(\overline{k})$ we have $\mathscr{L}_{t_0} \simeq \mathscr{N}_{\overline{k}}$ and $\mathscr{L}_{t_1} \simeq \mathscr{O}_{X_{\overline{k}}}$ on $X_{\overline{k}}$.

Loosely speaking, we think of $\mathscr{L}$ as the collection of line bundles $\mathscr{L}_t$ on X_t for each $t \in T$, and a trivialization along x_0 is a "continuously varying" choice of $k(t)$-basis of the fiber line $\mathscr{L}_t/\mathfrak{m}_{x_0}\mathscr{L}_t$ at x_0 as we vary $t \in T$.

Example 4.7. If X is a curve then algebraic equivalence to 0 turns out to be the same as "degree 0" (but this is not at all obvious).

Example 4.8. Let X be a smooth projective curve over k, and suppose there is a point $x_0 \in X(k)$. The divisors $X \times \{c_0\}$, $\{x_0\} \times X$, and the diagonal Δ on $X \times X$ define a line bundle

$$\mathscr{L} = \mathscr{O}_{X\times X}(\Delta - X \times \{x_0\} - \{x_0\} \times X)$$

on X parameterized by $T = X$, with fiber over $x \in X$ given by $\mathscr{O}_X(x - x_0)$ (argue separately depending on whether or not $x = x_0$). By the universal property, this defines a k-variety

map $i_{x_0} : X \to J_X$ such that on $\overline{k}$-points it carries x to the degree-0 line bundle $\mathscr{O}_{X_{\overline{k}}}(x_0 - x)$. By a non-obvious calculation, when $k = \mathbf{C}$ this recovers the analytic Jacobian map defined via integration along paths from the base point x_0.

The key point is the following deep result:

Theorem 4.9 (Grothendieck)**.** *Let X be a curve or abelian variety over a field k.*

(1) *If $X(k) \neq \emptyset$ then for each $x_0 \in X(k)$ there exists a universal triple $(P_X, \mathscr{N}, \varphi)$ consisting of a connected k-variety P_X, a line bundle $\mathscr{N}$ on $X \times P_X$ with a trivial fiber over some $e \in P_X(k)$, and an x_0-trivialization of $\mathscr{N}$.*

(2) *The formation of this triple commutes with any extension on k, and the resulting map $P_X(\overline{k}) \to \mathrm{Pic}(X_{\overline{k}})$ defined by $\xi \mapsto \mathscr{N}_\xi$ is a bijection on the group $\mathrm{Pic}^0(X_{\overline{k}})$ of line bundles algebraically equivalent to 0. There exists a unique structure of k-group variety on the* Picard variety *P_X making $P_X(\overline{k}) \to \mathrm{Pic}^0(X_{\overline{k}})$ a group isomorphism.*

(3) *The k-group variety P_X is an abelian variety, and it is canonically independent of the choice of x_0.*

Definition 4.10. The universal line bundle $\mathscr{N}$ on $X \times P_X$ is called the *Poincaré bundle* of X. When X is a smooth projective curve, we call P_X the *Jacobian* X and denote it as J_X. If X is an abelian variety, we call P_X the *dual abelian variety* and denote it as $X^\vee$.

When X is a curve, J_X has dimension equal to the genus of X. If X is an abelian variety, its dual $X^\vee$ has the same dimension at X. There is a version of these concepts for any projective k-variety X, but then P can fail to be smooth and so cannot be discussed with a lot of preliminaries with group schemes. Even for singular curves this generalization is extremely useful (e.g., it arises in the generalization of Theorem 4.12(2) below when we allow some ramification). The general concept which unifies these is called the *Picard scheme*. But it should be stressed that to construct the dual abelian variety in positive characteristic it is essential to use schemes even though the end result of the construction is a variety.

Remark 4.11. In general, a curve X over a field k may have no rational point. But there is always a finite Galois extension K/k such that $X(K)$ is non-empty. Thus, the Jacobian can be constructed over K. Using the precise meaning of "independent of x_0" in part (3) above, one can use a Galois descent argument to canonically construct the Jacobian J_X over k even when $X(k)$ is empty.

There are a couple of reasons for the significance of Jacobians in the study of curves:

Theorem 4.12. *Let X be a smooth projective curve over a field k, and $x_0 \in X(k)$ a point.*

(1) *The map $i_{x_0} : X \to J_X$ carrying x_0 to 0 is initial among all k-variety maps $X \to A$ carrying x_0 to 0.*

(2) *For every finite separable covering of curves $f : X' \to X$ that is everywhere unramified and becomes abelian over k_s, there is a unique separable k-isogeny $A \to J_X$ whose pullback along i_{x_0} is $X' \to X$.*

In Theorem 4.12, the intervention of k_s in part (2) is unavoidable. For example, any separable isogeny $f : E' \to E$ of elliptic curves over k becomes abelian over k_s (using translation by the points of $\ker(f_{\overline{k}})$, all of which are k_s-rational due to separability of f.

However, if some of these points are not k-rational then some of these translation covering automorphisms are not defined over k! Property (1) is often called *Albanese functoriality*. It makes J_X covariant in the pointed curve (X, x_0): if $X' \to X$ is a finite covering of smooth curves carrying some $x_0' \in X'(k)$ to $x_0 \in X(k)$ then by (1) we can uniquely fill in the right side of a commutative diagram

$$\begin{array}{ccc} X' & \xrightarrow{i_{x_0'}} & J_{X'} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \mathrm{Alb}(f)} \\ X & \xrightarrow[i_{x_0}]{} & J_X \end{array}$$

using a map of abelian varieties $\mathrm{Alb}(f)$. On $\overline{k}$-points, this commutativity and the homomorphism property of $\mathrm{Alb}(f)$ forces it to be induced by "pushforward" at the level of degree-0 Weil divisors.

In contrast with the covariance of the Albanese construction, there is a *contravariant* "Picard functoriality" that we turn to next. We will focus on the special case of curves and abelian varieties because we have not discussed the Picard scheme that is needed to handle more general varieties.

Example 4.13. Let $f : X \to X'$ be a map between smooth projective varieties that are each either a curve or an abelian variety over a common ground field k. Consider the pullback map $f^* : \mathrm{Pic}(X'_{\overline{k}}) \to \mathrm{Pic}(X_{\overline{k}})$. This carries $\mathrm{Pic}^0(X'_{\overline{k}})$ into $\mathrm{Pic}^0(X_{\overline{k}})$ because if T is a connected $\overline{k}$-variety and $\mathscr{L}$ is a line bundle on $X'_{\overline{k}} \times T$ containing the trivial line bundle as its restriction to the fiber over a point $t_0 \in T$ then the same holds for $(f_{\overline{k}} \times 1_T)^*(\mathscr{L})$ on $X_{\overline{k}} \times T$. But the fiber of this line bundle over $t \in T$ is $f_{\overline{k}}^*(\mathscr{L}_t)$, so we conclude that pullback preserves algebraic equivalence to 0.

It is natural to ask if there is a k-homomorphism $P_{X'} \to P_X$ such that on $\overline{k}$-points it recovers $f_{\overline{k}}^*$ on Pic^0's. The answer turns out to be affirmative (by unraveling some universal mapping properties), and when f is a k-homomorphism of abelian varieties we call this the *dual map* to f (in the other direction!) and denote it as $f^\vee : {X'}^\vee \to X^\vee$.

A not entirely trivial example is that $[n]_A^\vee = [n]_{A^\vee}$ for any integer n. In particular, since isogenies are characterized by the property that they factor through $[n]$ on either the source or target for some nonzero integer n, it follows that if $f : A \to A'$ is an isogeny then so is the dual map $f^\vee$. In fact, these two isogenies turn out to have the same degree.

Example 4.14. In the complex-analytic case, the dual map (and dual isogeny) can be described rather concretely. Let $f : V_1/L_1 \to V_2/L_2$ be a map between complex tori. This uniquely lifts to a $\mathbf{C}$-linear map $V_1 \to V_2$ between universal covers (it is just the tangent mapping at the origin), and as such carries L_1 into L_2. The $\mathbf{C}$-conjugate map $\overline{V}_1 \to \overline{V}_2$ has a $\mathbf{C}$-linear dual $V_2' \to V_1'$ that one checks carries L_2' into L_1'. This defines a map between complex tori $f' : V_2'/L_2' \to V_1'/L_1'$ in the other direction, and is exactly the dual map in the case of complex tori arising from abelian varieties. In particular, the homology maps are $\mathbf{Z}$-dual, which explains why the dual of an isogeny is again an isogeny with the same degree, at least when the ground field is $\mathbf{C}$.

Example 4.15. In a natural way, one can show that $(A \times B)^\vee$ is naturally isomorphic to $A^\vee \times B^\vee$. This is not a triviality, since it is *not* true that $\mathrm{Pic}(A \times B) = \mathrm{Pic}(A) \times \mathrm{Pic}(B)$ in general; restriction to the line bundles algebraically equivalent to 0 is essential here. This can already be seen quite vividly over $\mathbf{C}$, where the analytic theory gives an exact sequence

$$0 \to V'/L' \to \mathrm{Pic}(V/L) \to \ker(\wedge^2(L'_{\mathbf{C}}) \twoheadrightarrow \wedge^2(V')) \to 0,$$

illustrating a "quadratic" feature of $\mathrm{Pic}(V/L)$ that interacts poorly with direct products in V/L.

Theorem 4.16 (double duality)**.** *Let A be an abelian variety, $A^\vee$ its dual, Let $\mathscr{P}$ be the corresponding universal line bundle on $A \times A^\vee$ trivialized along $A \times 0'$. Then $\mathscr{P}$ admits a unique trivialization along $0 \times A^\vee$ such that the two trivializations coincide on the fiber line $\mathscr{P}(0, 0')$ over k, and this identifies $(A, \mathscr{P})$ with the corresponding universal pair for $A^\vee$.*

In other words, $\mathscr{P}$ defines a canonical isomorphism $i_A : A \simeq A^{\vee\vee}$. Moreover, its dual $i_A^\vee : A^{\vee\vee\vee} \simeq A^\vee$ is inverse to $i_{A^\vee}$.

Remark 4.17. For an abelian variety A over k, one should think of the Poincaré bundle $\mathscr{P}_A$ on $A \times A^\vee$ as an analogue of the canonical bilinear evaluation pairing $e_W : W \times W^* \to F$ for finite-dimensional vector spaces over a field F. For example, double duality of abelian varieties corresponds to the fact that $w \mapsto e_W(w, \cdot)$ induces an isomorphism $i_W : W \simeq W^{**}$ (double duality for vector spaces) that satisfies $e_{W^*}(\ell, i_W(w)) = e_W(w, \ell)$ (as is immediate from the definitions).

For a second finite-dimensional F-vector space W', to give a linear map $f : W' \to W^*$ is "the same" as to give a bilinear map $B : W \times W' \to F$ (the link being that $f(w') = B(\cdot, w')$ and $B(w, w') = f(w')(w)$). This is analogous to the universal property that to give a map of abelian varieties $f : A' \to A^\vee$ is "the same" as to give a line bundle $\mathscr{L}$ on $A \times A'$ equipped with trivializations along $A \times \{0'\}$ and $\{0\} \times A'$ (in which case $f(a') = \mathscr{L}|_{A \times \{a'\}}$ on $\overline{k}$-points). In terms of the universal property of the Poincaré bundle $\mathscr{P}_A$ on $A \times A^\vee$, f is characterized by the condition that $(1 \times f)^*(\mathscr{P}_A) \simeq \mathscr{L}$.

A crucial application of duality is the fact that abelian varieties taken up to isogeny decompose into "simple factors" in a manner reminiscent of the decomposition of finite group representations into irreducibles. *This has no counterpart in the theory of elliptic curves*! To make a precise formulation, we first require:

Definition 4.18. An abelian variety A over k is *simple* (or *k-simple* for emphasis) if it is nonzero and contains no nonzero proper abelian k-subvarieties.

For dimension reasons, elliptic curves are simple and remains so after any ground field extension. In general, a k-simple abelian variety may not remains simple after a ground field extension. This is analogous to the fact that a finite group G can have an irreducible linear representation over a field such that extension of the ground field ruins irreducibility (as already happens for the extension $\mathbf{C}/\mathbf{R}$).

Example 4.19. Imitating arguments for finite group representations (and doing a bit more work in positive characteristic), if $f : A \to A'$ is a nonzero k-homomorphism between simple abelian varieties over k then f turns out to be an isogeny. In particular, if A is k-simple

then the *endomorphism algebra* $\mathrm{End}_k^0(A) := \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_k(A)$ is a division algebra; its center is some number field. (The subring $\mathrm{End}_k(A)$ is called the *endomorphism ring* of A.)

The possibilities for these algebras are vast when $\dim A > 1$, in contrast with the case of elliptic curves (for which it is easy to describe all possibilities), and a full understanding rests on global class field theory. The description of endomorphism rings is a hopeless mess, on par with describing all orders in the ring of integers of a number field.

Example 4.20. Consider an abelian variety A of dimension $g > 0$ over a finite field k of size q. When Tate proved that the map in Theorem 4.2(1) is an isomorphism for such k, he also deduced the important consequence that A is k-simple if and only if the characteristic polynomial $f_A \in \mathbf{Q}[t]$ of the q-Frobenius on the $T_\ell(A)$'s has a single irreducible factor. In such cases the data of f_A amounts to specifying its degree $2g$ and a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-orbit of Weil q-integers (as in Theorem 4.5). It is natural to ask if one can identify the division algebra $\mathrm{End}_k^0(A)$ in such cases. The answer is part of Honda–Tate theory, and it requires the theory of p-divisible groups ($p = \mathrm{char}(k)$).

Theorem 4.21 (Poincaré reducibility)**.** *For every nonzero abelian variety A over a field k and abelian subvariety B of A over k, there is another such $B' \subseteq A$ so that $B \times B' \to A$ is an isogeny. In particular, there exists a non-empty finite set $\{A_i\}$ of pairwise non-isogenous k-simple abelian varieties and integers $e_i \geq 1$ such that A is k-isogenous to $\prod A_i^{e_i}$.*

The collection of A_i is unique up to k-isogeny and rearrangement, and the multiplicities e_i are unique. In particular,

$$\mathrm{End}^0(A) \simeq \prod \mathrm{Mat}_{e_i \times e_i}(D_i)$$

for the division algebras $D_i := \mathrm{End}_k^0(A_i)$, so $\mathrm{End}^0(A)$ is a central simple algebra and it is a division algebra if and only if A is k-simple.

We say that a nonzero abelian variety B over k is an *isogeny factor* of a nonzero abelian variety A over k if B is isogenous to an abelian subvariety of A over k. For instance, the preceding theorem says that A has a well-defined non-empty finite set of k-simple isogeny factors. This leads to:

Definition 4.22. The *isogeny category* of abelian varieties over a field k has as objects the abelian varieties over k and as morphism groups

$$\mathrm{Hom}_k^0(A, A') := \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Hom}_k(A, A')$$

(so for $A' = A$ this recovers the endomorphism algebra $\mathrm{End}_k^0(A)$ as defined above). Composition is defined in the evident manner.

Example 4.23. It is an instructive exercise to check that a k-homomorphism $A \to A'$ of abelian varieties over k becomes an isomorphism in the isogeny category (i.e., admits an inverse up to multiplication by a nonzero integer) if and only if it is an isogeny. This is the reason for the terminology "isogeny category": it is the category obtained by "inverting" exactly the isogenies.

The Poincaré reducibility theorem says that the isogeny category of abelian varieties over k is a semisimple category: every object is isomorphic (in the isogeny category!) to a product of finitely many simple objects. Working in the isogeny category attains the same kind

of simplifications one gets by working with $\mathbf{Q}[G]$-modules rather than $\mathbf{Z}[G]$-modules for a finite group G: some important information is lost, but for many purposes it is an adequate framework.

The following striking example used to be very important in the foundations of the theory of abelian varieties, and now it is a powerful trick (e.g., *Gabber's Lemma* to be discussed later will exploit this to bypass some severe difficulties in Faltings' method):

Example 4.24. Let A be an abelian variety of dimension $g > 0$ over an infinite field k. Fix a projective embedding $A^\vee \hookrightarrow \mathbf{P}^N_k$ over k. By using $g-1$ artfully chosen hyperplane slices via Bertini's theorem (this require infinitude of k), we obtain a smooth projective (connected!) curve $X \subseteq A^\vee$ over k. Applying Example 4.13 and double duality, there is an induced map in the other direction

$$A \simeq A^{\vee\vee} \to J_X$$

that turns out to have *finite* kernel, and hence is an isogeny factor over k. In other words, *every abelian variety over an infinite field k is an isogeny factor of a Jacobian over k.* We have very little control over the genus of X, and hence of the dimension of J_X. Over finite fields, one can use Poonen's refinement of Bertini's theorem [P] to get the existence of such an X in such cases as well.

But up to isogeny, how far is a general abelian variety from a Jacobian? Moduli space dimension-counting arguments show that for $g \geq 3$, "most" abelian varieties of dimension g over $\mathbf{C}$ are not Jacobians. Such soft methods do not apply over countable fields, and for several decades it was a long-standing open problem to product an abelian variety of dimension $g \geq 3$ over $\overline{\mathbf{Q}}$ that is not isogenous to a Jacobian. This was only very recently solved (by J. Tsimerman)!

5. Pairings and polarizations

The last general topic we turn to is that of "pairings", generalizing the Weil pairing for elliptic curves. The general case reveals some subtleties that cannot be seen in the case of elliptic curves: the natural pairing (for n not divisible by $\mathrm{char}(k)$) is actually a $\mathrm{Gal}(k_s/k)$-equivariant perfect bilinear pairing

$$\langle \cdot, \cdot \rangle_{A,n} : A[n] \times A^\vee[n] \to \mu_n$$

and *not* a symplectic form on $A[n]$ as for elliptic curves. For a special class of k-isomorphisms $f : A \simeq A^\vee$ the resulting bilinear form

$$\langle \cdot, \cdot \rangle_{f,n} : A[n] \times A[n] \to \mu_n$$

will turn out to be symplectic and for A an elliptic curve will recover the traditional Weil pairing (up to a sign that is hard to keep straight) upon using a certain canonical choice of f ("self-duality of elliptic curves"). An inspection of the construction of the Weil pairing in [Si] reveals the mixed roles of pairings against degree-0 divisor classes and the self-duality of elliptic curves. In higher dimensions these two aspects are kept more clearly separate because abelian varieties of higher dimension are rarely self-dual (and even when they are self-dual, there is generally not a "preferred" self-duality as in the 1-dimensional case).

Theorem 5.1. *Let A be an abelian variety of dimension $g > 0$ over a field k, and n a positive integer not divisible by* $\mathrm{char}(k)$.

(1) *There is a canonical* $\mathrm{Gal}(k_s/k)$*-equivariant perfect pairing*

$$\langle \cdot, \cdot \rangle_{A,n} : A[n] \times A^\vee[n] \to \mu_n$$

of free $\mathbf{Z}/n\mathbf{Z}$*-modules of rank* $2g$ *that makes the diagram*

$$\begin{array}{ccc} A[nm] \times A^\vee[nm] & \xrightarrow{\langle \cdot, \cdot \rangle_{A,nm}} & \mu_{nm} \\ {\scriptstyle [m]\times[m]}\downarrow & & \downarrow{\scriptstyle t^m} \\ A[n] \times A^\vee[n] & \xrightarrow[\langle \cdot, \cdot \rangle_{A,n}]{} & \mu_n \end{array}$$

commute for any integer m not divisible by $\mathrm{char}(k)$. *In particular, for a prime $\ell \neq \mathrm{char}(k)$ there is a perfect $\mathbf{Z}_\ell$-bilinear* $\mathrm{Gal}(k_s/k)$*-equivariant pairing*

$$T_\ell(A) \times T_\ell(A^\vee) \to \mathbf{Z}_\ell(1).$$

(2) *If $f : A \to B$ is a k-homomorphism and $f^\vee : B^\vee \to A^\vee$ is the dual map then*

$$\langle a, f^\vee(b') \rangle_{A,n} = \langle f(a), b' \rangle_{B,n}$$

for $a \in A[n]$ and $b' \in B^\vee[n]$.

(3) *Via the double duality isomorphism $i_A : A \simeq A^{\vee\vee}$ we have*

$$\langle a', i_A(a) \rangle_{A^\vee,n} = \langle a, a' \rangle_{A,n}$$

for $a \in A[n]$ and $a' \in A^\vee[n]$.

Example 5.2. This can be made rather explicit for $k = \mathbf{C}$. Since $\mathbf{Z}(1)/n\mathbf{Z}(1) \simeq \mu_n$ via $z \mapsto \exp(z/n)$, if $A(\mathbf{C}) = V/L$ then using the uniformization $A^\vee(\mathbf{C}) = V'/L'$ with

$$L' = \{\ell \in V' = \overline{V}^\vee \mid \ell(\overline{\lambda}) \in \mathbf{Z}(1) \text{ for all } \lambda \in L\}$$

gives $(1/n)L'/L' = \mathrm{Hom}((1/n)L/L, \mu_n)$ via

$$(1/n)\ell \bmod L' \mapsto ((1/n)\lambda \bmod L \mapsto \exp(\ell(\overline{\lambda})/n).$$

Example 5.3. Let $f : A' \to A^\vee$ be a k-homomorphism between abelian varieties. (By the universal property of $A^\vee$, this corresponds to a line bundle on $A \times A'$ trivial along $A \times \{0'\}$ and along $\{0\} \times A$.) The map f defines $\mathrm{Gal}(k_s/k)$-equivariant pairings

$$\langle \cdot, \cdot \rangle_{f,n} : A[n] \times A'[n] \to A[n] \times A^\vee[n] \overset{\langle \cdot, \cdot \rangle_{A,n}}{\to} \mu_n$$

for every integer n not divisible by $\mathrm{char}(k)$, as well as a $\mathbf{Z}_\ell$-bilinear variant

$$(\cdot, \cdot)_{f,\ell} : T_\ell(A) \times T_\ell(A') \to \mathbf{Z}_\ell(1)$$

for every prime $\ell \neq \mathrm{char}(k)$. This corresponds to an induced map

$$V_\ell(A') \to \mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(A), \mathbf{Z}_\ell(1))$$

of $\mathbf{Q}_\ell[\mathrm{Gal}(k_s/k)]$-modules that is exactly $V_\ell(f)$ under the identification of $V_\ell(A^\vee)$ with the $\mathbf{Z}_\ell(1)$-dual of $V_\ell(A)$ under the pairings $\langle \cdot, \cdot \rangle_{A,\ell^r}$ $(r \geq 1)$.

By Example 4.3, it follows that f is an isogeny if and only if $(\cdot,\cdot)_{f,\ell}$ is non-degenerate. This is analogous to the fact that for vector spaces W and W' of the same finite dimension over a field F, a linear map $f : W' \to W^*$ is an isomorphism if and only if the induced bilinear pairing

$$B_f = e_W \circ (1 \times f) : (w, w') \mapsto f(w')(w)$$

is non-degenerate.

Now we focus on the special case $A' = A$ in the preceding example. That is, we consider k-homomorphisms $f : A \to A^\vee$, which is to say line bundles $\mathscr{L}$ on $A \times A$ trivial along $A \times \{0\}$ and $\{0\} \times A$. This is analogous to considering linear maps $W \to W^*$ for a finite-dimensional vector space W over a field F, which is to say bilinear forms $B : W \times W \to F$.

For such bilinear forms there is a special property of *symmetry*, which is characterized in two equivalent ways: we can say that B is invariant under the "flip" of its factors, or that the corresponding linear map $T_B : W \to W^*$ is *symmetric* in the sense that by using double-duality for vector spaces, the composite map

$$W \simeq W^{**} \stackrel{T_B^*}{\to} W^*$$

is equal to T_B.

The analogue for abelian varieties works out in two equivalent ways as well: if $f : A \to A^\vee$ corresponds to $\mathscr{L}$ on $A \times A$, we can ask if $\mathscr{L} \simeq s^*(\mathscr{L})$ where $s : A \times A \to A \times A$ is the involution that swaps the factors, and we can ask if double duality for abelian varieties makes f a *symmetric* homomorphism in the sense that the composite map

$$A \simeq A^{\vee\vee} \stackrel{f^\vee}{\to} A^\vee$$

is equal to f. These two conditions do indeed turn out to be equivalent. Somewhat surprising is how this works out at the level of ℓ-adic pairings:

Proposition 5.4. *Let $\ell \neq \mathrm{char}(k)$ be a prime. A k-homomorphism $f : A \to A^\vee$ is symmetric if and only if the induced pairing*

$$(\cdot,\cdot)_{f,\ell} : T_\ell(A) \times T_\ell(A) \to T_\ell(A) \times T_\ell(A^\vee) \to \mathbf{Z}_\ell(1)$$

is skew-symmetric. In particular, f is a symmetric isogeny if and only if $(\cdot,\cdot)_{f,\ell}$ is a non-degenerate skew-symmetric form on $T_\ell(A)$.

Let us at least explain where the sign discrepancy in the symmetry aspect is coming from. This can be seen more directly in the complex-analytic case, so consider a complex torus V/L and a homomorphism $f : V/L \to V'/L'$. This corresponds to a $\mathbf{C}$-linear map $V \to V' = \overline{V}^*$ carrying L into L', or in other words a Hermitian form $H : V \times V \to \mathbf{C}$ carrying $L \times L$ into $\mathbf{Z}(1)$. Extending scalars to $\mathbf{Z}_\ell$ on the lattice pairings and using the compatible isomorphisms $(1/n)\mathbf{Z}(1)/\mathbf{Z}(1) \simeq \mu_n$ to identify $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathbf{Z}(1) \simeq \varprojlim \mu_{\ell^r} = \mathbf{Z}_\ell(1)$, we obtain

$$(\cdot,\cdot)_{f,\ell} : (\mathbf{Z}_\ell \otimes_{\mathbf{Z}} L) \times (\mathbf{Z}_\ell \otimes_{\mathbf{Z}} L) \to \mathbf{Z}_\ell(1).$$

The associated map

$$f' : V/L \simeq V''/L'' \stackrel{f^\vee}{\to} V'/L'$$

corresponds to the Hermitian form $H' : V \times V$ defined by $H'(v_1, v_2) = \overline{H(v_2, v_1)}$, and upon restricting to the lattices we get the corresponding pairing $L \times L \to \mathbf{Z}(1)$ that is obtained from the initial one by swapping factors and applying complex conjugation on $\mathbf{Z}(1)$. Hence, $(\cdot,\cdot)_{f',\ell}$ is related to $(\cdot,\cdot)_{f,\ell}$ through two steps: we swap the $T_\ell(V/L)$-factors *and* we applying complex conjugation on $\mathbf{Z}(1)$ in $\mathbf{Z}_\ell(1) = \mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathbf{Z}(1)$. But complex conjugation on $\mathbf{Z}(1)$ is *negation*, whence

$$(\lambda_1, \lambda_2)_{f',\ell} = -(\lambda_2, \lambda_1)_{f,\ell}.$$

Since $f = f'$ if and only if $T_\ell(f) = T_\ell(f')$ if and only if $(\cdot,\cdot)_{f,\ell} = (\cdot,\cdot)_{f',\ell}$, we conclude that $f = f'$ if and only if $(\cdot,\cdot)_{f,\ell}$ is *skew-symmetric*!

It turns out that there is a beautiful way to describe *all* symmetric homomorphisms $A \to A^\vee$, at least when k is algebraically closed. This is called the *Mumford construction*, and it goes as follows. Let $\mathscr{L}$ be any line bundle on A. Then we get a line bundle on $A \times A$ by the recipe

$$\wedge(\mathscr{L}) = m^*(\mathscr{L}) \otimes p_1^*(\mathscr{L})^{-1} \otimes p_2^*(\mathscr{L})^{-1}$$

where $m : A \times A \to A$ is the group law. (This is inspired by the formula $q(w+w') - q(w) - q(w')$ for quadratic forms q, which produces all *symmetric* bilinear forms modulo some difficulties in characteristic 2). By inspection $\wedge(\mathscr{L})$ is a symmetric line bundle on $A \times A$ since the group law m is commutative. Moreover, $\wedge(\mathscr{L})$ has restrictions to $A \times \{0\}$ and $\{0\} \times A$ that are visibly trivial since $m(a, 0) = a = m(0, a)$ for all $a \in A$. Hence, by the universal property of $A^\vee$ there is a unique k-homomorphism

$$\phi_{\mathscr{L}} : A \to A^\vee$$

such that $(1 \times \phi_{\mathscr{L}})^*(\mathscr{P}_A) \simeq \wedge(\mathscr{L})$.

Explicitly, on $\overline{k}$-points we have

$$\phi_{\mathscr{L}}(a) = t_a^*(\mathscr{L}) \otimes \mathscr{L}^{-1}$$

where $t_a : x \mapsto m(x, a) = x + a$ is the translation map. By symmetry of $\wedge(\mathscr{L})$, the homomorphism $\phi_{\mathscr{L}}$ is symmetric. The induced *skew-symmetric* pairing on $T_\ell(A)$ is denoted $e_{\mathscr{L},\ell}$.

Example 5.5. In the language of Weil divisors, if $\mathscr{L} = \mathscr{O}(D)$ for a Weil divisor D then $t_a^*(\mathscr{L}) = \mathscr{O}(t_{-a}(D)$ and $\mathscr{L}^{-1} = \mathscr{O}(-D)$, so $\phi_{\mathscr{O}(D)}(a) = \mathscr{O}(t_{-a}(D) - D)$. In the special case of elliptic curves, if $D = [0]$ then $\phi_{\mathscr{O}([0])}(a) = \mathscr{O}([-a] - [0])$. In other words, $\phi_{\mathscr{O}([0])} : E \to E^\vee$ is the *negative* of the "traditional" autoduality of elliptic curves. This has led some to suggest that Mumford's construction has a sign problem. But that is wrong: Mumford's construction is the right thing, and it is the traditional autoduality that has a sign problem. This will become apparent in Example 5.11.

Amusingly, the construction of $\langle\cdot,\cdot\rangle_{A,n}$ in [Mu] involves a certain ratio of rational functions that is the *reciprocal* of the one used in [Si], so the sign discrepancy just noted cancels against the sign discrepancy arising from these reciprocal ratios to imply that for elliptic curves E the skew-symmetric pairing

$$e_{\mathscr{O}([0]),\ell} : T_\ell(E) \times T_\ell(E) \to \mathbf{Z}_\ell(1)$$

coincides with the ℓ-adic Weil pairing in [Si].

The importance of Mumford's construction is due to the second part of:

Theorem 5.6. *Let $\mathscr{L}$ be a line bundle on a nonzero abelian variety A over k, and $\phi_{\mathscr{L}} : A \to A^\vee$ the associated symmetric homomorphism.*

(1) *The homomorphism $\phi_{\mathscr{L}}$ determines $\mathscr{L} \in \mathrm{Pic}(A)$ modulo tensoring against a point of $A^\vee(k) = \mathrm{Pic}^0(A) \subset \mathrm{Pic}(A)$.*
(2) *If $k = k_s$ then every symmetric homomorphism $A \to A^\vee$ arises in this way.*
(3) *If $\mathscr{L}$ is ample then $\phi_{\mathscr{L}}$ is an isogeny, and in general when $\phi_{\mathscr{L}}$ is an isogeny then its degree is a perfect square.*

The square condition in part (3) is analogous to the fact that a non-degenerate symplectic form over $\mathbf{Z}$ has square determinant (equivalently, when converted into the language of a linear map between $\mathbf{Z}$-lattices, it is injective with cokernel of square order). This analogy is a logical implication in the special case $k = \mathbf{C}$ when everything is expressed in terms of analytic uniformizations.

It is very important to keep in mind that $\phi_{\mathscr{L}}$ is a more fundamental object than $\mathscr{L}$, since map line bundles can give rise to the same symmetric isogeny, as noted in (1) above.

Example 5.7. Consider the case of elliptic curves, so $E^\vee$ classifies degree-0 line bundles. Theorem 5.6(1) says that $\phi_{\mathscr{L}}$ only depends on the degree of $\mathscr{L}$. But $\deg(n[0]) = n$, so by Theorem 5.6(2) it follows that the symmetric homomorphisms $E \to E^\vee$ are exactly the maps

$$\phi_{\mathscr{O}(n[0])} : x \mapsto \mathscr{O}(t_{-x}(n[0]) - n[0]) = \mathscr{O}(n[-x] - n[0]) = \mathscr{O}([-x] - [0])^{\otimes n} = n\phi_{\mathscr{O}([0])}.$$

Example 5.8. To appreciate the extent to which different $\mathscr{L}$'s can define the same map $\phi_{\mathscr{L}}$, consider the case of a symmetric homomorphism $f : A \to A^\vee$ for an abelian variety A over a field k. By Theorem 5.6(2), there is a line bundle $\mathscr{N}$ on A_{k_s} such that $f_{k_s} = \phi_{\mathscr{N}}$. But can $\mathscr{N}$ be found on A? No! To see the problem, observe that for any $\sigma \in \mathrm{Gal}(k_s/k)$ we have

$$\phi_{\mathscr{N}} = f_{k_s} = \sigma^*(f_{k_s}) = \sigma^*(\phi_{\mathscr{N}}) = \phi_{\sigma^*(\mathscr{N})},$$

so by Theorem 5.6(1) we have $\sigma^*(\mathscr{N}) \otimes \mathscr{N}^{-1} \in A^\vee(k_s)$. This defines a class

$$[f] \in \mathrm{H}^1(k_s/k, A^\vee)$$

which vanishes if and only if $\mathscr{N}$ can be chosen to be defined over k.

If k is finite then by a general result of Lang the entire group $\mathrm{H}^1(k_s/k, A^\vee)$ vanishes (because $A^\vee$ is a smooth connected group variety). But otherwise the cohomology class $[f]$ can be nonzero. This is not merely an idle curiosity, but has striking arithmetic consequences. In the remarkable paper [PS], Poonen and Stoll show that the non-vanishing of such classes occurs for Jacobians of curves over $\mathbf{Q}$ and it closely tied up with whether or not the order of the Tate–Shafarevich group of the Jacobian (if finite!) is a perfect square.

The fact that $\phi_{\mathscr{N}}$ can have a strictly smaller field of definition than $\mathscr{N}$ is one of the reasons that this map is a more basic object than the line bundle (which provides a description of the map over k_s).

Although $\mathscr{L}$ cannot be recovered from $\phi_{\mathscr{L}}$, some properties of $\mathscr{L}$ *can* be recovered. More specifically, the pullback $(1, \phi_{\mathscr{L}})^*(\mathscr{P}_A)$ on A under the map

$$(1, \phi_{\mathscr{L}}) : A \to A \times A^\vee$$

turns out to be a $\mathrm{Pic}^0(A)$-twist of $\mathscr{L}^{\otimes 2}$, and that ampleness of a line bundle on A is invariant under $\mathrm{Pic}^0(A)$-twisting. Since $\mathscr{L}$ is ample if and only if $\mathscr{L}^{\otimes 2}$ is ample, we arrive at the important:

Proposition 5.9. *Let $f : A \to A^\vee$ be a symmetric homomorphism, and choose a line bundle $\mathscr{L}$ on A_{k_s} such that $f_{k_s} = \phi_{\mathscr{L}}$. Then $\mathscr{L}$ is ample on A_{k_s} if and only if $(1, f)^*(\mathscr{P}_A)$ is ample on A, in which case f is an isogeny.*

Under the dictionary of analogies between duality of abelian varieties and duality in linear algebra, according to which the Poincaré bundle is analogous to the evaluation pairing on a finite-dimensional vector space, the operation assigning to a symmetric homomorphism $f : A \to A^\vee$ the line bundle $(1, f)^*(\mathscr{P}_A)$ on A is analogous to the operation assigning to a symmetric bilinear form $B : W \times W \to F$ the quadratic form $q_B : w \mapsto B(w, w)$ (since the associated symmetric linear map $T_B : W \to W^*$ is $w \mapsto B(w, \cdot) = B(\cdot, w)$, and composing $(1, T_B) : W \to W \times W^*$ with the evaluation pairing yields $w \mapsto B(w, w)$). Since ampleness in algebraic geometry is a kind of "positivity" property, the ampleness of $(1, f)^*(\mathscr{P}_A)$ is analogous to the condition that a quadratic form over $\mathbf{R}$ be positive-definite. (Thus, the automatic non-degeneracy of symmetric $\mathbf{R}$-bilinear form with positive-definite associated quadratic form is analogous to the above assertion that f is an isogeny whenever $(1, f)^*(\mathscr{P}_A)$ is ample.)

The preceding results inspire the following important concept, to be considered as an analogue of a positive-definite quadratic form on a finite-dimensional $\mathbf{R}$-vector space.

Definition 5.10. A *polarization* of an abelian variety A over a field k is a symmetric homomorphism $f : A \to A^\vee$ such that the line bundle $(1, f)^*(\mathscr{P}_A)$ on A is ample (so f is an isogeny).

The preceding discussion shows that it is equivalent to say that $f_{k_s} = \phi_{\mathscr{L}}$ for an *ample* line bundle $\mathscr{L}$ on A_{k_s}, and moreover that any such f necessary has square degree. When a polarization f has degree 1, it is called a *principal polarization*.

Example 5.11. By Example 5.7, there are exactly two symmetric isomorphisms $E \simeq E^\vee$ for an elliptic curve E, namely $\pm\phi_{\mathscr{O}([0])}$. We have seen that $-\phi_{\mathscr{O}([0])} = \phi_{\mathscr{O}(-[0])}$ is the autoduality used in [Si] and this is *not* a polarization because $\mathscr{O}(-[0])$ is *not* ample. In contrast, $\phi_{\mathscr{O}([0])}$ is a polarization. This is why the autoduality in [Si] is the "wrong" one from the viewpoint of the general theory of abelian varieties (even though computations with divisors may seem to suggest it is the more natural one, as we saw in Example 5.5).

Example 5.12. If A is an abelian variety, then $A \times A^\vee$ is canonically self-dual since

$$(A \times A^\vee)^\vee \simeq A^\vee \times A^{\vee\vee} \simeq A^\vee \times A \simeq A \times A^\vee.$$

Moreover, this self-duality is even a symmetric homomorphism. But this is *not* a polarization because it violates the ampleness requirement. This is analogous to the fact that if W is a finite-dimensional $\mathbf{R}$-vector space, the canonical bilinear form

$$(W \oplus W^*) \times (W \oplus W^*) \to \mathbf{R}$$

defined by $((w,\ell),(w',\ell')) \mapsto \ell'(w) + \ell(w')$ is symmetric and non-degenerate, but its associated quadratic form $(w,\ell) \mapsto \ell(w)$ on $W \oplus W^*$ is not positive-definite (even when $\dim W = 1$!).

Example 5.13. Since every abelian variety is projective, and so admits an ample line bundle, there is always *some* polarization. But can we control the degree? It is a basic fact of life that many higher-dimensional abelian varieties do *not* admit a principal polarization, in contrast with the case of elliptic curves (for which we just saw that there is a *unique* principal polarization). Even worse, in characteristic $p > 0$ one can make examples of abelian surfaces (isogenous to a product of two supersingular elliptic curves) such that there is no *separable* polarization! It is an amazing observation of Yuri Zahrin (Zahrin's trick) that $(A \times A^\vee)^4$ always admits a principal polarization!

But there is one important class of abelian varieties for which there is exists a principal polarization, even a canonical one: Jacobians. Let X be a smooth projective (geometrically connected) curve of genus $g > 0$ over a field k, and consider the Jacobian J_X. Pick a finite Galois extension k'/k so that $X(k')$ is non-empty. Using a point $x_0 \in X(k')$, we get a closed embedding $i_{x_0} : X_{k'} \hookrightarrow J_{X_{k'}} = (J_X)_{k'}$ carrying x_0 to 0. Using the contravariant Picard functoriality, consider the induced pullback map of abelian varieties

$$(J_X)^\vee_{k'} = P_{J_{X_{k'}}} \to P_{X_{k'}} = (P_X)_{k'} = (J_X)_{k'}.$$

This map turns out to be (i) an isomorphism, (ii) independent of the choice of x_0. Due to (ii), this map between abelian varieties over k' is $\mathrm{Gal}(k'/k)$-equivariant (the point being that if $\mathrm{Gal}(k'/k)$ moves x_0, there is no effect on the construction).

By Galois descent we get an inverse map of abelian varieties $J_X \simeq (J_X)^\vee$, and this turns out to be the *negative* of a polarization. (For example, if X is an elliptic curve and we take $x_0 = 0$ then $i_{x_0} : E \to E^\vee$ is the autoduality from [Si] which we saw in Example 5.11 is the negative of the unique principal polarization of E.) The paper [PS] gives examples over $\mathbf{Q}$ of curves X with $X(\mathbf{Q}) = \emptyset$ such that the resulting principal polarization of J_X does *not* arise from an ample line bundle on X over $\mathbf{Q}$.

We end our discussion of ample line bundles on abelian varieties by recording a striking generalization of the familiar fact that $\mathscr{O}(3[0])$ is very ample for elliptic curves (plane cubic!).

Theorem 5.14. *If $\mathscr{L}$ is an ample line bundle on an abelian variety A over a field k, with $\deg \phi_{\mathscr{L}} = d^2$, then $\mathscr{L}^{\otimes 3}$ is very ample. Moreover, the corresponding projective embedding of A (using the corresponding complete linear system $|3D|$ with $\mathscr{O}(D) = \mathscr{L}$) is in a projective space $\mathbf{P}^{3^g d}_k$ as a subvariety with degree $g!3^g d$.*

The importance of this result cannot be overestimated for the theory of moduli spaces of abelian varieties (which we will need to use later). It says that if we consider abelian varieties with a fixed dimension g and equipped with a polarization of a fixed square degree d^2 then *all* of them can be found in a known projective space as subvarieties of a known degree depending only on g and d, not on k or anything else. In the case $g = d = 1$ this recovers the fact that every elliptic curve over any field occurs in $\mathbf{P}^2$ as a cubic curve, a result which is certainly ubiquitous in many approaches to constructing modular curves.

Example 5.15. As we have noted earlier, Zahrin's trick provides a mechanism for constructing a principal polarization on $(A \times A^\vee)^4$ for any abelian variety A of dimension $g > 0$ over a field k. This abelian variety has dimension $8g$, so by Theorem 5.14 it is a subvariety of $\mathbf{P}_k^{3^{8g}}$ with degree $(8g)!3^{8g}$. Since A occurs as an abelian subvariety, we conclude that every g-dimensional abelian variety over k can be found insider of $\mathbf{P}_k^{3^{8g}}$. We do not know if there is a uniform upper bound on the degree of such subvarieties; probably there is no bound.

6. Chabauty's method

We conclude by giving a remarkable application of Jacobians to the Mordell Conjecture. Consider a smooth projective (geometrically connected) curve C of genus $g \geq 2$ over a number field K, with Jacobian J. Long before Faltings, Chabauty [Ch] discovered that finiteness of $C(K)$ can be proved when $r := \mathrm{rank}(J(K))$ is not too big:

Theorem 6.1. *If $r < g$ then $C(K)$ is finite.*

Proof. The main idea is apparently due to Thue: although $J(K)$ is usually dense in $J(\mathbf{C})$ when $r > 0$, it can fail to be dense in $J(K_v)$ for many places v of K. We will work with a non-archimedean place v such that v is totally split over $\mathbf{Q}$ (and there are infinitely many such v, by Chebotarev).

We can assume $C(K)$ is non-empty, so we pick $c_0 \in C(K)$ and consider the resulting embedding $i_{c_0} : C \hookrightarrow J$. The closure G of $J(K)$ inside $J(K_v)$ is a topologically closed subgroup of the group $J(K_v)$ that is compact since J is projective. If ℓ is the rational prime below v, so $\mathbf{Q}_\ell = K_v$, $J(K_v)$ is an ℓ-adic Lie group. We refer to [Se, Part II] for a general discussion of Lie groups over fields such as $\mathbf{Q}_\ell$. One consequence of this theory is that by commutativity, $J(K_v)$ contains a compact open subgroup U isomorphic to $\mathbf{Z}_\ell^g$. By compactness of $J(K_v)$, it follows that U has finite index. Hence, a finite-index subgroup of $J(K)$ lies in the pro-ℓ subgroup U, whence the closure of this finite-index subgroup in $J(K_v)$ is simply the $\mathbf{Z}_\ell$-linear span. This must be $\mathbf{Z}_\ell^{r'}$ (up to finite subgroups) for some $r' \leq r < g$, so we conclude that the original $J(K)$ has closure G that contains $\mathbf{Z}_\ell^{r'}$ with finite index.

To prove that $C(K)$ is finite, we note that $C(K)$ is contained in $C(K_v) \cap J(K)$, so it suffices to prove that $C(K_v)$ meets $J(K)$ with finite intersection. If this intersection is infinite, then by compactness of $C(K_v)$ it follows that $C(K_v) \cap J(K)$ has an accumulation point $\xi \in C(K_v) \cap G$. In a neighborhood of ξ in the K_v-analytic submanifold $C(K_v)$ of the K_v-analytic Lie group $J(K_v)$, there are infinitely many points contained in the lower-dimensional subgroup G. But if an analytic function on a 1-dimensional K_v-analytic disc has infinitely many zeros then it is identically zero. Hence, a local nonzero equation for G in $J(K_v)$ vanishes identically on $C(K_v)$ near ξ.

It follows that it we map a translation from our original K-rational base point c_0 to the K_v-point ξ, the resulting embedding $C_{K_v} \to J_{K_v}$ carries a neighborhood $\mathscr{U}$ of the base point into the proper closed subgroup G. Hence, for any $n \geq 1$, the multiplication map $\mathscr{U}^n \to J(K_v)$ factors through G. But the theory of Jacobians (especially the Riemann–Roch theorem) ensures that for large enough n the map $C^n \to J$ is a projective space bundle, and in particular induces an *open* mapping on K_v-points. Hence, $\mathscr{U}^n$ has open image in $J(K_v)$. The is a contradiction, since the image is contained in the proper K_v-analytic submanifold G! ∎

The preceding argument looks rather non-effective, but Coleman showed in [Co] that the method can be refined (using p-adic integration) to give explicit upper bounds on the size of $C(K)$ when Chabauty's hypothesis $r < g$ is satisfied. For instance, he obtained the general upper bound $\#C(K) \leq q_v + 2g(1 + \sqrt{q_v}) - 1$ for a place v of good reduction for C that is unramified over $\mathbf{Q}$ (with q_v the size of the residue field of K at v), provided that this place also has residue characteristic $> 2g$. Even more explicitly, if $K = \mathbf{Q}$ and $r \leq 1$ then any C with good reduction at 2 and 3 satisfies $\#C(\mathbf{Q}) \leq 12$. All such results fail to give an explicit upper bound on the heights of rational points, and so are no good for rigorously finding all rational points.

References

[Ch] C. Chabauty, *Sur les points rationels des courbes algébriques de genre supérieur à l'unité*, C.R. Acad. Sci. **212** (1941), pp. 882–884.

[Co] R. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), pp. 765–770.

[Mi1] J. Milne, "Abelian Varieties" in *Arithmetic geometry* (Cornell/Silverman ed.), Springer–Verlag, 1986.

[Mi2] J. Milne, "Jacobian Varieties" in *Arithmetic geometry* (Cornell/Silverman ed.), Springer–Verlag, 1986.

[Mu] D. Mumford, *Abelian varieties*, Oxford Univ. Press, 1970.

[P] B. Poonen, *Bertini theorems over finite fields*, Annals of Math. **160** (2004), pp. 1099–1127.

[PS] B. Poonen, M. Stoll, *Cassels–Tate pairing on polarized abelian varieties*, Annals of Math. **150** (1999), pp. 1109–1149.

[Se] J-P. Serre, *Lie groups and Lie algebras* (5th ed.), SLN 1500, Springer–Verlag, 2006.

[Si] J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.