Dual abelian varieties [1]

Abelian varieties over finite fields

David Kurniadi Angdinata

University College London

Wednesday, 18 January 2023

[1] J S Milne (2008) Abelian Varieties

Dual elliptic curves

Let (E, O) be an elliptic curve over a field K. Recall that

$$\begin{array}{cccl} \lambda_{(O)} & : & E & \longrightarrow & \mathrm{Cl}^0(E) \le \mathrm{Cl}(E) \\ & & P & \longmapsto & (-P) - (O) \end{array} .$$

Here $\mathrm{Cl}(E)$ is the **class group** of Weil divisors $\sum_{P \in E} n_P(P)$ modulo $\sim$, where $D \sim 0$ if D is the divisor (f) of some rational function $f \in \overline{K}(E)^\times$, and $\mathrm{Cl}^0(E)$ is its subgroup with $\sum_{P \in E} n_P = 0$.

Idea: for any $D \in \mathrm{Cl}^0(E)$, the Riemann–Roch space $\mathscr{L}(D + (O))$, where

$$\mathscr{L}(D) := \{f \in \overline{K}(E)^\times : (f) + D \ge 0\} \cup \{0\},$$

is one-dimensional, so $D \sim (-P) - (O)$ for some $P \in E$.

For an elliptic curve E, its *dual* is $\mathrm{Cl}^0(E)$.

Invertible sheaves on smooth varieties

Let X/K be a smooth variety. Then identify

$$\begin{array}{rcl} \mathrm{Cl}(X) & \xrightarrow{\sim} & \mathrm{Pic}(X) \\ D & \mapsto & \mathcal{L}(D). \end{array}$$

Here $\mathrm{Pic}(X)$ is the **Picard group** of invertible sheaves $\mathcal{L}$ modulo $\cong$, with

$$\mathcal{L} \cdot \mathcal{L}' := \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}', \qquad \mathcal{L}^{-1} := \mathcal{H}om(\mathcal{L}, \mathcal{O}_X),$$

and $\mathcal{L}(D)$ is the sheaf of $\mathcal{O}_X$-modules such that for any open $U \subseteq X$,

$$\Gamma(U, \mathcal{L}(D)) := \{f \in K(X)^\times : (f) + D \geq 0 \text{ in } U\} \cup \{0\}.$$

If $f : Y \to X$ is a morphism, then there is also a **pull-back**

$$f^*\mathcal{L} := f^{-1}\mathcal{L} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X \in \mathrm{Pic}(Y).$$

Invertible sheaves on abelian varieties

Let A/K be an abelian variety. For any $a \in A(K)$, the translation map $\tau_a : A \to A$ induces $\tau_a^* : \mathrm{Pic}(A) \to \mathrm{Pic}(A)$. For any $\mathcal{L} \in \mathrm{Pic}(A)$, define

$$\begin{array}{rccc} \lambda_{\mathcal{L}} & : & A(K) & \longrightarrow & \mathrm{Pic}(A) \\ & & a & \longmapsto & \tau_a^* \mathcal{L} \cdot \mathcal{L}^{-1} \end{array} .$$

This is a homomorphism, by **theorem of the square**

$$\tau_{a+b}^* \mathcal{L} \cdot \mathcal{L} \cong \tau_a^* \mathcal{L} \cdot \tau_b^* \mathcal{L}, \qquad a, b \in A(K).$$

This follows from **theorem of the cube** [2] that

$$(f+g+h)^* \mathcal{L} \cdot (f+g)^* \mathcal{L}^{-1} \cdot (f+h)^* \mathcal{L}^{-1} \cdot (g+h)^* \mathcal{L}^{-1} \cdot f^* \mathcal{L} \cdot g^* \mathcal{L} \cdot h^* \mathcal{L}$$

is trivial for any regular maps $f, g, h : V \to A$ from a variety V/K.

In fact, if $\mathcal{L} \in \mathrm{Pic}(A)$ is ample, then $\ker(\lambda_{\mathcal{L}}) \leq A(K)$ is finite. [3]

---

[2] Theorem I.5.1

[3] Proposition I.8.1

Invertible sheaves and Weil divisors

Remark

Equivalently, $\tau_a^* : \mathrm{Cl}(A) \to \mathrm{Cl}(A)$ *translates a Weil divisor* D *by* $-a$*, so*

$$\begin{array}{rccl} \lambda_{\mathcal{L}(D)} & : & A(K) & \longrightarrow & \mathrm{Cl}(A) \\ & & a & \longmapsto & D_{-a} - D \end{array},$$

where D_{-a} *is translation of* D *by* $-a$*. Theorem of the square becomes*

$$D_{-(a+b)} + D \sim D_{-a} + D_{-b}, \qquad a, b \in A(K).$$

If $A = E$*, then*

$$\begin{array}{rccl} \lambda_{\mathcal{L}((O))} & : & E(K) & \longrightarrow & \mathrm{Cl}(E) \\ & & P & \longmapsto & (-P) - (O) \end{array}.$$

In fact, if $D \in \mathrm{Cl}(E)$ *is effective, then* $\deg D = 0$ *iff* $\lambda_{\mathcal{L}(D)} = 0$*.* [4]

[4] Example I.8.3

Translation-invariant invertible sheaves

Let $+ : A \times A \to A$ be the addition map, and let $\pi_i : A \times A \to A$ be the projection map to the i-th component. For any $\mathcal{L} \in \mathrm{Pic}(A)$, define

$$K(\mathcal{L}) := \{a \in A : (+^*\mathcal{L} \cdot \pi_1^*\mathcal{L}^{-1})|_{A\times\{a\}} \cong \mathcal{O}_A\}.$$

Then $K(\mathcal{L})(K) = \ker(\lambda_{\mathcal{L}})$ as subgroups of A, since

$$(+^*\mathcal{L} \cdot \pi_1^*\mathcal{L}^{-1})|_{A\times\{a\}} = \tau_a^*\mathcal{L} \cdot \mathcal{L}^{-1}, \qquad a \in A(K).$$

In fact, $K(\mathcal{L})$ is closed as a subvariety of A. [5]

Define the subgroup of **translation-invariant invertible sheaves**

$$\mathrm{Pic}^0(A) := \{\mathcal{L} \in \mathrm{Pic}(A) : K(\mathcal{L}) = A\}.$$

Then $\tau_a^*\mathcal{L} \cdot \mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$ for any $a \in A(K)$, so $\mathrm{im}(\lambda_{\mathcal{L}}) \subseteq \mathrm{Pic}^0(A)$.

Need an abelian variety $\widehat{A}$ such that $\widehat{A}(K) \cong \mathrm{Pic}^0(A)$.

[5] Proposition I.5.19

Construction of dual abelian varieties

Idea: $\lambda_{\mathcal{L}} : A(K) \to \mathrm{Pic}^0(A)$ has kernel $K(\mathcal{L})(K)$, and in fact is surjective if $\mathcal{L} \in \mathrm{Pic}(A)$ is ample, [6] so $\widehat{A}$ should be the quotient variety $A/K(\mathcal{L})$.

- If $\mathrm{char}(K) = 0$, then $K(\mathcal{L})$ is a reduced subgroup variety of A, and $A/K(\mathcal{L})$ is simply defined as the $K(\mathcal{L})$-orbits of A.
- If $\mathrm{char}(K) \neq 0$, then $K(\mathcal{L})$ may not be reduced in general, so redefine $K(\mathcal{L})$ as the maximal subscheme of A such that $(+^*\mathcal{L} \cdot \pi_1^*\mathcal{L}^{-1})|_{A \times K(\mathcal{L})} \cong \pi_2^*\mathcal{L}'$ for some $\mathcal{L}' \in \mathrm{Pic}(K(\mathcal{L}))$, and $A/K(\mathcal{L})$ is naturally an algebraic space quotient of A.

The **dual abelian variety** of A is $\widehat{A} := A/K(\mathcal{L})$.

Remark

Since $\mathcal{L} \in \mathrm{Pic}^0(A)$ iff $+^*\mathcal{L} \cong \pi_1^*\mathcal{L} \cdot \pi_2^*\mathcal{L}$, addition on A lifts to multiplication on $\mathcal{L}$ and makes $\mathcal{G}(\mathcal{L}) := \mathcal{L} \setminus \{0\}$ an abelian group scheme over K. In fact, $\mathcal{G}(\mathcal{L})$ is an extension of A by $\mathbb{G}_m$, and this defines an isomorphism $\mathcal{G} : \mathrm{Pic}^0(A) \xrightarrow{\sim} \mathrm{Ext}^1_K(A, \mathbb{G}_m)$ of abelian group schemes. [7]

[6] Proposition I.8.14

[7] Proposition I.9.3

Representability of dual abelian varieties

Consider the functor $\mathcal{F} : \mathbf{Var}_K \to \mathbf{Set}$ that associates a variety V/K to the set of isomorphism classes of $\mathcal{L} \in \mathrm{Pic}(A \times V)$ such that

- $\mathcal{L}|_{A \times \{x\}} \in \mathrm{Pic}^0(A_x)$ for any $x \in V$, and
- $\mathcal{L}|_{\{0\} \times V} \cong \mathcal{O}_V$.

Theorem

$\widehat{A}$ represents $\mathcal{F}$. In other words $\mathcal{F}(V) = \mathrm{Hom}(V, \widehat{A})$ for any variety V/K.

Proof.

Sketched in Section I.8. □

By construction, $\widehat{A}(L) = \mathrm{Pic}^0(A_L)$ for any field extension L/K.

By universality, $\widehat{A}$ is unique up to unique isomorphism. Its corresponding universal element is the **Poincaré sheaf** $\mathcal{P}_A \in \mathcal{F}(\widehat{A})$, which associates any $\mathcal{L} \in \mathrm{Pic}^0(A)$ with a unique $\mathcal{P}_A|_{A \times \{a\}}$ for some $a \in \widehat{A}(K)$.

Dualities on abelian varieties

The functor $A \mapsto \widehat{A}$ is a duality theory in the sense that $\widehat{\widehat{A}} \cong A$. This follows from $\mathcal{P}_{\widehat{A}} \cong \mathcal{P}_A$, [8] since $\mathcal{P}_A$ parameterises $\widehat{A}(K) \cong \mathrm{Pic}^0(A)$.

Now let $\phi : A \to B$ be a morphism. Then it has a dual morphism

$$\begin{array}{cccc} \widehat{\phi} & : & \widehat{B} & \longrightarrow & \widehat{A} \\ & & \mathcal{L} & \longmapsto & \phi^*\mathcal{L} \end{array}.$$

If ϕ is an isogeny, then $\ker(\widehat{\phi}) = \widehat{\ker(\phi)}$ is the *Cartier dual* of $\ker(\phi)$, [9] where $\widehat{\widehat{\ker(\phi)}} \cong \ker(\phi)$. If $K = K^s$ with $\mathrm{char}(K) \nmid n := \# \ker(\phi)$, then

$$\widehat{\ker(\phi)} = \mathrm{Hom}(\ker(\phi), \mu_n).$$

This defines a *Weil pairing*

$$e_\phi : \ker(\phi) \times \ker(\widehat{\phi}) \to \mu_n.$$

[8] Theorem I.8.9
[9] Theorem I.9.1

Polarisations on abelian varieties

A **polarisation** on A is an isogeny $\lambda : A \to \widehat{A}$ such that $\lambda = \lambda_{\mathcal{L}}$ over $\overline{K}$ for some ample $\mathcal{L} \in \mathrm{Pic}(A_{\overline{K}})$. It is **principal** if it has degree one.

Remark

Zarhin proved that $(A \times \widehat{A})^4$ is always principally polarised. [10]

Let $\lambda : A \to \widehat{A}$ be a polarisation. This defines an involution on $\mathrm{End}^0(A)$ called the **Rosati involution** $(\cdot)^\dagger : \mathrm{End}^0(A) \to \mathrm{End}^0(A)$, where

$$A \xrightarrow{\phi} A \qquad \longmapsto \qquad A \xrightarrow{\lambda} \widehat{A} \xrightarrow{\widehat{\phi}} \widehat{A} \xrightarrow{\lambda^{-1}} A,$$

which is well-defined since $\lambda^{-1} \in \mathrm{Hom}^0(\widehat{A}, A)$. It satisfies

$$(\phi + \psi)^\dagger = \phi^\dagger + \psi^\dagger, \qquad (\phi \circ \psi)^\dagger = \psi^\dagger \circ \phi^\dagger, \qquad \phi, \psi \in \mathrm{End}^0(A),$$

and $a^\dagger = a$ for any $a \in \mathbb{Q}$.

[10] Theorem I.13.12