1.4 A Summary of Duality and Polarizations

Suppose A is an abelian variety over an arbitrary field k. In this section we summarize the most important properties of the dual abelian variety $A^\vee$ of A. First we review the language of sheaves on a scheme X, and define the Picard group of X as the group of invertible sheaves on X. The dual of A is then a variety whose points correspond to elements of the Picard group that are algebraically equivalent to 0. Next, when the ground field is $\mathbf{C}$, we describe how to view $A^\vee$ as a complex torus in terms of a description of A as a complex torus. We then define the Néron-Severi group of A and relate it to polarizations of A, which are certain homomorphisms $A \to A^\vee$. Finally we observe that the dual is functorial.

1.4.1 Sheaves

We will use the language of sheaves, as in [1], which we now quickly recall. A *pre-sheaf of abelian groups* $\mathcal{F}$ on a scheme X is a contravariant functor from the category of open sets on X (morphisms are inclusions) to the category of abelian groups. Thus for every open set $U \subset X$ there is an abelian group $\mathcal{F}(U)$, and if $U \subset V$, then there is a restriction map $\mathcal{F}(V) \to \mathcal{F}(U)$. (We also require that $\mathcal{F}(\emptyset) = 0$, and the map $\mathcal{F}(U) \to \mathcal{F}(U)$ is the identity map.) A *sheaf* is a pre-sheaf whose sections are determined locally (for details, see [1, §II.1]).

Every scheme X is equipped with its structure sheaf $\mathcal{O}_X$, which has the property that if $U = \mathrm{Spec}(R)$ is an affine open subset of X, then $\mathcal{O}_X(U) = R$. A *sheaf of $\mathcal{O}_X$-modules* is a sheaf $\mathcal{M}$ of abelian groups on X such that each abelian group has the structure of $\mathcal{O}_X$-module, such that the restriction maps are module morphisms. A *locally-free sheaf* of $\mathcal{O}_X$-modules is a sheaf $\mathcal{M}$ of $\mathcal{O}_X$-modules, such that X can be covered by open sets U so that $\mathcal{M}|_U$ is a free $\mathcal{O}_X$-module, for each U.

1.4.2 The Picard Group

An *invertible sheaf* is a sheaf $\mathcal{L}$ of $\mathcal{O}_X$-modules that is locally free of rank 1. If $\mathcal{L}$ is an invertible sheaf, then the sheaf-theoretic Hom, $\mathcal{L}^\vee = \mathcal{H}\mathrm{om}(\mathcal{L}, \mathcal{O}_X)$ has the property that $\mathcal{L}^\vee \otimes \mathcal{L} = \mathcal{O}_X$. The group $\mathrm{Pic}(X)$ of invertible sheaves on a scheme X is called *the Picard group* of X. See [1, §II.6] for more details.

Let A be an abelian variety over a field k. An invertible sheaf $\mathcal{L}$ on A is *algebraically equivalent to* 0 if there is a connected variety T over k, an invertible sheaf $\mathcal{M}$ on $A \times_k T$, and $t_0, t_1 \in T(k)$ such that $\mathcal{M}_{t_0} \cong \mathcal{L}$ and $\mathcal{M}_{t_1} \cong \mathcal{O}_A$. Let $\mathrm{Pic}^0(A)$ be the subgroup of elements of $\mathrm{Pic}(A)$ that are algebraically equivalent to 0.

The *dual* $A^\vee$ of A is a (unique up to isomorphism) abelian variety such that for every field F that contains the base field k, we have $A^\vee(F) = \mathrm{Pic}^0(A_F)$. For the precise definition of $A^\vee$ and a proof that $A^\vee$ exists, see [2, §9–10].

1.4.3 The Dual as a Complex Torus

When A is defined over the complex numbers, so $A(\mathbf{C}) = V/L$ for some vector space V and some lattice L, [4, §4] describes a construction of $A^\vee$ as a complex torus, which we now describe. Let

$$V^* = \{f \in \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{C}) \,:\, f(\alpha t) = \overline{\alpha} f(t), \text{ all } \alpha \in \mathbf{C}, t \in V\}.$$

Then V^* is a complex vector space of the same dimension as V and the map $\langle f, v\rangle = \mathrm{Im} f(t)$ is an $\mathbf{R}$-linear pairing $V^* \times V \to \mathbf{R}$. Let

$$L^* = \{f \in V^* : \langle f, \lambda\rangle \in \mathbf{Z}, \text{ all } \lambda \in L\}.$$

Since A is an abelian variety, there is a nondegenerate Riemann form H on A. The map $\lambda : V \to V^*$ defined by $\lambda(v) = H(v, \cdot)$ is an isomorphism of complex vector spaces. If $v \in L$, then $\lambda(v) = H(v, \cdot)$ is integer valued on L, so $\lambda(L) \subset L^*$. Thus λ induces an isogeny of complex tori $V/L \to V^*/L^*$, so by Lemma 1.3.7 the torus V^*/L^* possesses a nondegenerate Riemann form (it's a multiple of H). In [4, §4], Rosen describes an explicit isomorphism between V^*/L^* and $A^\vee(\mathbf{C})$.

1.4.4 The Néron-Several Group and Polarizations

Let A be an abelian variety over a field k. Recall that $\mathrm{Pic}(A)$ is the group of invertible sheaves on A, and $\mathrm{Pic}^0(A)$ is the subgroup of invertible sheaves that are algebraically equivalent to 0. The *Néron-Severi group* of A is the quotient $\mathrm{Pic}(A)/\mathrm{Pic}^0(A)$, so by definition we have an exact sequence

$$0 \to \mathrm{Pic}^0(A) \to \mathrm{Pic}(A) \to \mathrm{NS}(A) \to 0.$$

Suppose $\mathcal{L}$ is an invertible sheaf on A. One can show that the map $A(k) \to \mathrm{Pic}^0(A)$ defined by $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is induced by homomorphism $\varphi_{\mathcal{L}} : A \to A^\vee$. (Here $t_a^*\mathcal{L}$ is the pullback of the sheaf $\mathcal{L}$ by translation by a.) Moreover, the map $\mathcal{L} \mapsto \varphi_{\mathcal{L}}$ induces a homomorphism from $\mathrm{Pic}(A) \to \mathrm{Hom}(A, A^\vee)$ with kernel $\mathrm{Pic}^0(A)$. The group $\mathrm{Hom}(A, A^\vee)$ is free of finite rank, so $\mathrm{NS}(A)$ is a free abelian group of finite rank. Thus $\mathrm{Pic}^0(A)$ is saturated in $\mathrm{Pic}(A)$ (i.e., the cokernel of the inclusion $\mathrm{Pic}^0(A) \to \mathrm{Pic}(A)$ is torsion free).

Definition 1.4.1 (Polarization). A *polarization* on A is a homomorphism $\lambda : A \to A^\vee$ such that $\lambda_{\overline{k}} = \varphi_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}(A_{\overline{k}})$. A polarization is *principal* if it is an isomorphism.

When the base field k is algebraically closed, the polarizations are in bijection with the elements of $\mathrm{NS}(A)$. For example, when $\dim A = 1$, we have $\mathrm{NS}(A) = \mathbf{Z}$, and the polarizations on A are multiplication by n, for each integer n.

1.4.5 The Dual is Functorial

The association $A \mapsto A^\vee$ extends to a contravariant functor on the category of abelian varieties. Thus if $\varphi : A \to B$ is a homomorphism, there is a natural choice of homomorphism $\varphi^\vee : B^\vee \to A^\vee$. Also, $(A^\vee)^\vee = A$ and $(\varphi^\vee)^\vee = \varphi$.

Theorem 1.4.2 below describes the kernel of $\varphi^\vee$ in terms of the kernel of φ. If G is a finite group scheme, the *Cartier dual* of G is $\mathrm{Hom}(G, \mathbf{G}_m)$. For example, the Cartier dual of $\mathbf{Z}/m\mathbf{Z}$ is μ_m and the Cartier dual of μ_m is $\mathbf{Z}/m\mathbf{Z}$. (If k is algebraically closed, then the Cartier dual of G is just G again.)

Theorem 1.4.2. *If $\varphi : A \to B$ is a surjective homomorphism of abelian varieties with kernel G, so we have an exact sequence $0 \to G \to A \to B \to 0$, then the kernel of $\varphi^\vee$ is the Cartier dual of G, so we have an exact sequence $0 \to G^\vee \to B^\vee \to A^\vee \to 0$.*

References

[1] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

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

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

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

[5] H. P. F. Swinnerton-Dyer, *Analytic theory of abelian varieties*, Cambridge University Press, London, 1974, London Mathematical Society Lecture Note Series, No. 14. MR 51 #3180

The Dual Abelian Variety

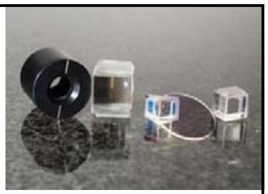
The **dual of *A*** is an abelian variety isogenous to *A* that parametrizes classes of invertible sheaves on *A* that are algebraically equivalent to zero.

$$A^\vee = \mathrm{Pic}^0(A)$$

The dual is functorial:

$$\text{If } A \to B \text{ then } B^\vee \to A^\vee.$$

Polarized Abelian Varieties



A *polarization* of *A* is an isogeny (homomorphism) from *A* to its dual that is induced by a divisor on *A*. A polarization of degree 1 is called a *principal polarization.*

Theorem. *If A is the Jacobian of a curve, then A is canonically principally polarized. For example, elliptic curves are principally polarized.*

Cassels-Tate Pairing

A/F: abelian variety over number field

Theorem. If A is principally polarized by a polarization arising from an F-rational divisor, then there is a nondegenerate alternating pairing on $Ш(A/F)_{/\mathrm{div}}$, so for all p:

$$\#Ш(A/F)[p^\infty]_{/\mathrm{div}} = \square$$

(Same statement away from minimal degree of polarizations.)

Corollary. If $\dim A = 1$ and $Ш(A/F)$ finite, then

$$\#Ш(A/F) = \square$$

What if the abelian variety *A* is not an elliptic curve?

Assume $\#Ш(A/F)$ is finite. Overly optimistic literature:

- Page 306 of [Tate, 1963]: If *A* is a Jacobian then

$$\#Ш(A/F) = \square.$$

- Page 149 of [Swinnerton-Dyer, 1967]: Tate proved that

$$\#Ш(A/F) = \square.$$

Michael Stoll's Computation

During a grey winter day in 1996, Michael Stoll sat puzzling over a computation in his study on a majestic embassy-peppered hill near Bonn overlooking the Rhine. He had implemented an algorithm for computing 2-torsion in Shafarevich-Tate groups of Jacobians of hyperelliptic curves. He stared at a curve X for which his computations were in direct contradiction to the previous slide!

$$\#Ш(\mathrm{Jac}(X)/\mathbf{Q})[2] = 2.$$

What was wrong????

Poonen-Stoll

```
From: Michael Stoll (9 Dec 1996)
Dear Bjorn, Dear Ed:
[...] your results would imply that Sha[2] = Z/2Z
in contradiction to the fact that the order of Sha[2] should
be a square (always assuming, as everybody does, that Sha is finite).
So my question is (of course): What is wrong ?

From: Bjorn Pooenen (9 Dec 96)
Dear Michael:
Thanks for your e-mails. I'm glad someone is actually taking the time
to think about our paper critically! [...]
I would really like to resolve the apparent contradiction,
because I am sure it will end with us learning something!
(And I don't think that it will be that Sha[2] can have odd dimension!)

From: Bjorn Poonen (11 hours later)
Dear Michael:
I think I may have resolved the problem. There is nothing wrong with
the paper, or with the calculation.  The thing that is wrong is the
claim that Sha must have square order!
```

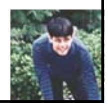
Poonen-Stoll Theorem

Theorem (Annals, 1999): *Suppose J is the Jacobian of a curve and J has finite Shafarevich-Tate group. Then*

$$\#\text{Ш}(J/F) = \square \text{ or } 2\cdot\square$$

Example: The Jacobian of this curve has Sha of order 2

$$y^2 = -3(x^2+1)(x^2-6x+1)(x^2+6x+1)$$



Is Sha Always Square or Twice a Square?

Poonen asked at the Arizona Winter School in 2000, *"Is there an abelian variety A with Shafarevich-Tate group of order* ***three****?"*

In 2002 I finally found Sha of order 3 (times a square):

$$0 = -x_1^3 - x_1^2 + (-6x_3x_2 + 3x_3^2)x_1 + (-x_2^3 + 3x_3x_2^2 + (-9x_3^2 - 2x_3)x_2 + (4x_3^3 + x_3^2 + (y_1^2 + y_1 + (2y_3y_2 - y_3^2))))$$

$$0 = -3x_2x_1^2 + ((-12x_3 - 2)x_2 + 3x_3^2)x_1 + (-2x_2^3 + 3x_3x_2^2 + (-15x_3^2 - 4x_3)x_2 + (5x_3^3 + x_3^2 + (2y_2y_1 + ((4y_3 + 1)y_2 - y_3^2))))$$

$$0 = -3x_3x_1^2 + (-3x_2^2 + 6x_3x_2 + (-9x_3^2 - 2x_3))x_1 + (x_2^3 + (-9x_3 - 1)x_2^2 + (12x_3^2 + 2x_3)x_2 + (-9x_3^3 - 3x_3^2 + (2y_3y_1 + (y_2^2 - 2y_3y_2 + (3y_3^2 + y_3)))))$$

$$\begin{aligned} 0 = {} & x_1^2x_2^4 - 8x_1^2x_2^3x_3 + 30x_1^2x_2^2x_3^2 - 44x_1^2x_2x_3^3 + 25x_1^2x_3^4 - 2/3x_1x_2^5 + 26/3x_1x_2^4x_3 + 2/3x_1x_2^4 \\ & - 140/3x_1x_2^3x_3^2 - 16/3x_1x_2^3x_3 + 388/3x_1x_2^2x_3^3 + 20x_1x_2^2x_3^2 - 2/3x_1x_2^2y_2^2 + 8/3x_1x_2^2y_2y_3 \\ & - 10/3x_1x_2^2y_3^2 - 490/3x_1x_2x_3^4 - 88/3x_1x_2x_3^3 + 8/3x_1x_2x_3y_2^2 - 40/3x_1x_2x_3y_2y_3 \\ & + 44/3x_1x_2x_3y_3^2 + 250/3x_1x_3^5 + 50/3x_1x_3^4 - 10/3x_1x_3^2y_2^2 + 44/3x_1x_3^2y_2y_3 - 50/3x_1x_3^2y_3^2 \\ & + 1/9x_2^6 - 2x_2^5x_3 - 2/9x_2^5 + 15x_2^4x_3^2 + 26/9x_2^4x_3 + 1/9x_2^4 - 544/9x_2^3x_3^3 - 140/9x_2^3x_3^2 \\ & - 8/9x_2^3x_3 + 2/9x_2^3y_2^2 - 8/9x_2^3y_2y_3 + 10/9x_2^3y_3^2 + 135x_2^2x_3^4 + 388/9x_2^2x_3^3 + 10/3x_2^2x_3^2 \\ & - 2x_2^2x_3y_2^2 + 80/9x_2^2x_3y_2y_3 - 94/9x_2^2x_3y_3^2 - 2/9x_2^2y_2^2 + 8/9x_2^2y_2y_3 - 10/9x_2^2y_3^2 \\ & - 150x_2x_3^5 - 490/9x_2x_3^4 - 44/9x_2x_3^3 + 50/9x_2x_3^2y_2^2 - 244/9x_2x_3^2y_2y_3 + 30x_2x_3^2y_3^2 \\ & + 8/9x_2x_3y_2^2 - 40/9x_2x_3y_2y_3 + 44/9x_2x_3y_3^2 + 625/9x_3^6 + 250/9x_3^5 + 25/9x_3^4 - 50/9x_3^3y_2^2 \\ & + 220/9x_3^3y_2y_3 - 250/9x_3^3y_3^2 - 10/9x_3^2y_2^2 + 44/9x_3^2y_2y_3 - 50/9x_3^2y_3^2 + 1/9y_2^4 \\ & - 8/9y_2^3y_3 + 10/3y_2^2y_3^2 - 44/9y_2y_3^3 + 25/9y_3^4 \end{aligned}$$

Plenty of Non-square Sha!

- **Theorem (Stein):** *For every prime* $p < 25000$ *there is an abelian variety A over* **Q** *such that*

$$\#\text{Ш}(A/\mathbf{Q}) = p\cdot\square$$

- **Conjecture (Stein):** *Same statement for all p.*

How to Construct Non-square Sha

While attempting to connect groups of points on elliptic curves of high rank to Shafarevich-Tate groups of abelian varieties of rank 0, I found a construction of non-square Shafarevich-Tate groups.

The Main Theorem

Theorem (Stein). *Suppose E is an elliptic curve and p an odd prime that satisfies various technical hypothesis. Suppose* ℓ *is a prime congruent to 1 mod p (and not dividing* N_E*) such that*

$$L(E,\chi_{p,\ell},1) \neq 0 \text{ and } a_\ell(E) \not\equiv \ell+1 \pmod{p}$$

Here $\chi_{p,\ell} : (\mathbf{Z}/\ell)^* \twoheadrightarrow \mu_p$ *is a Dirichlet character of order p and conductor* ℓ *corresponding to an abelian extension K. Then there is a twist A of a product of p - 1 copies of E and an exact sequence*

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to \text{Ш}(A/\mathbf{Q})[p^\infty] \to \text{Ш}(E/K)[p^\infty] \to \text{Ш}(E/\mathbf{Q})[p^\infty] \to 0.$$

If E has odd rank and $\text{Ш}(E/\mathbf{Q})[p^\infty]$ *is finite then* $\text{Ш}(A/\mathbf{Q})[p^\infty]$ *has order that is* ***not a perfect square****.*

Proof Uses the Weil Restriction of Scalars

F/K: finite extension of number fields
A/F: abelian variety over F

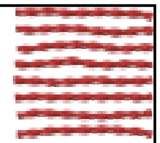
$R = \mathrm{Res}_{F/K}(A)$ abelian variety over K with

$$\dim(R) = \dim(A) \cdot [F:K]$$

Functorial characterization:
For any K-scheme S,

$$R(S) = A(S \times_K F)$$

What is the Abelian Variety *A*?



Let R be the Weil restriction of scalars of E from K down to $\mathbf{Q}$, so R is an abelian variety over $\mathbf{Q}$ of dimension p (i.e., the degree of K). Then A is the kernel of the map induced by trace:

$$0 \to A \to R \to E \to 0$$

Note that
- A has dimension $p - 1$
- A is isomorphic over K to a product of copies of E
- Our hypothesis on ℓ and Kato's finiteness theorems imply that $A(\mathbf{Q})$ and $\#Ш(A/\mathbf{Q})$ are both finite.
- Is isogenous to A_f where f is a twist of newform attached to E.

Proof Sketch (1): Exact Sequence of Neron Models

The exact sequence

$$0 \to A \to R \to E \to 0$$

extends to an exact sequence of *Néron models* (and hence sheaves for the étale topology) over $\mathbf{Z}$:

$$0 \to \mathcal{A} \to \mathcal{R} \to \mathcal{E} \to 0.$$

To check this, we use that formation of Néron models commutes with unramified base change and Prop. 7.5.3(a) of [*Néron Models*, 1990].

Proof (2): Mazur's Etale Cohomology Sha Theorem

Mazur's *Rational Points of Abelian Varieties with Values in Towers of Number Fields*:

For $F = A, R, E$ let $\mathcal{F} = \text{Néron}(F)$. Then

$$H^1_{\text{ét}}(\mathbf{Z}, \mathcal{F})[p^\infty] \cong Ш(F/\mathbf{Q})[p^\infty]$$

In general this is not true, but our hypothesis on p and ℓ are exactly strong enough to kill the relevant error terms.

Proof (3): Long Exact Sequence

The long exact sequence of étale cohomology begins

$$0 \to A(\mathbf{Q}) \to R(\mathbf{Q}) \to E(\mathbf{Q}) \xrightarrow{\delta} H^1_{\text{ét}}(\mathbf{Z}, \mathcal{A}) \to H^1_{\text{ét}}(\mathbf{Z}, \mathcal{R}) \to H^1_{\text{ét}}(\mathbf{Z}, \mathcal{E}) \to H^2_{\text{ét}}(\mathbf{Z}, \mathcal{A})$$

Take the p-power torsion in this exact sequence then use Mazur's theorem. Next analyze the cokernel of δ...

Proof (4): Apply Kato's Finiteness Theorems

We have $\mathrm{Coker}(\delta) = E(\mathbf{Q})/pE(\mathbf{Q})$ since

$$L(E, \chi_{p,\ell}, 1) \neq 0 \quad \text{and} \quad a_\ell \not\equiv \ell + 1 \pmod{p}.$$

(To see this requires chasing some diagrams.)

Also $H^2_{\text{ét}}(\mathbf{Z}, \mathcal{A})[p^\infty] = 0$ (proof uses Artin-Mazur duality).

Both of these steps use Kato's finiteness theorem in an essential way. Putting everything together yields the claimed exact sequence

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to Ш(A/\mathbf{Q})[p^\infty] \to Ш(E/K)[p^\infty] \to Ш(E/\mathbf{Q})[p^\infty] \to 0.$$