The Tate module and finiteness theorems for abelian varieties

Gregor Bruns

29.04.2015

In this note we are following the beginning of chapter IV in [Mum08] and sections I.10–I.15 in [Mil08]. For omitted proofs, have a look there.

1 On isogenies

First we're going to prove the following interesting fact:

Theorem 1.1. *Let X be an abelian variety and $f\colon Y \to X$ an étale cover by another variety Y. Assume $Y(k) \neq \emptyset$. Then Y can be given a group scheme structure such that it is also an abelian variety and f is an isogeny.*

We are going to make use of the following two results.

Proposition 1.2. *Let X be a proper variety over $k = \overline{k}$, $e \in X(\overline{k})$ and let*

$$m\colon X \times X \to X$$

be a morphism such that $m(e, x) = m(x, e) = x$ for all $x \in X(\overline{k})$. Then X is an abelian variety with m as the multiplication map and e as the identity element.

Lemma 1.3. Let $f\colon X \to Y$ be a proper smooth morphism of irreducible varieties and assume there is a section $\sigma\colon Y \to X$ of f, i.e. $f \circ \sigma = \mathrm{id}_Y$. Then all fibers of f are irreducible.

Proof of Theorem 1.1. We may base change to $X_{\overline{k}}$ and $Y_{\overline{k}}$ since all required properties descend (note that we have assumed the existence of a k-rational point of Y, so if Y is geometrically an abelian variety, it is so already over k).

Let $\Gamma_m \subseteq X \times X \times X$ be the graph of m and let $\Gamma' \subseteq Y \times Y \times Y$ be the inverse image of Γ_m under the map $f \times f \times f$. Our strategy of proof is as follows. We will choose a component $\Gamma \subseteq \Gamma'$ that is isomorphic to $Y \times Y$ and then use that identification to obtain a map

$$Y \times Y \xrightarrow{\cong} \Gamma \hookrightarrow \Gamma' \xrightarrow{p_3} Y$$

which will (because of the definition of the graph) induce a group structure on Y "pulled-back" from X.

We start with the observation that the projection $p_{12}\colon \Gamma_m \to X \times X$ onto the first two factors is an isomorphism. Then $\Gamma' \to \Gamma_m$ is an étale cover. Consider the following commutative diagram (not necessarily cartesian):

$$\begin{array}{ccc} \Gamma' & \longrightarrow & \Gamma_m \\ \downarrow{\scriptstyle p_{12}} & & \downarrow{\scriptstyle p_{12}} \\ Y \times Y & \xrightarrow[f \times f]{} & X \times X \end{array}$$

Since the maps on the top, right and bottom are étale covers, by the cancellation theorem the left projection map p_{12} is also an étale covering.

Choose a point $y_0 \in Y$ such that $f(y_0) = 0_X$ (of course y_0 is going to be our identity element on Y). Then the point (y_0, y_0, y_0) lies in Γ' and we denote by Γ the connected component containing it. The restriction $p = p_{12}|_\Gamma\colon \Gamma \to Y \times Y$ is again an étale cover. In order to show it is an isomorphism we will show $p^{-1}(y_0, y_0)$ contains only one point.

Define the two morphisms $\sigma_1, \sigma_2\colon Y \to \Gamma$ by $\sigma_1(y) = (y_0, y, y)$ and $\sigma_2(y) = (y, y_0, y)$. Then the restriction $p|_{\sigma_2(Y)}$ induces a bijection $\sigma_2(Y) \to Y \times \{y_0\}$. We will show $p^{-1}(Y \times \{y_0\}) = \sigma_2(Y)$, proving that over each y there is only one point in Γ. Equivalently, if $q\colon \Gamma \to Y$ is the restriction of $p_2\colon Y \times Y \times Y \to Y$ to Γ, then $q^{-1}(y_0) = \sigma_2(Y)$.

By dimension reasons, $\sigma_2(Y)$ is an irreducible component of $q^{-1}(y_0)$, so it is enough to show that $q^{-1}(y_0)$ is irreducible. Since Γ is étale over $X \times X$, it is smooth by the smoothness of $X \times X$. But Γ is also connected, so it is irreducible. Furthermore the morphism q is also smooth, since it is the composition of an étale morphism with a projection. Observe now that σ_1 is a section for q. By Lemma 1.3, we can conclude that the fiber $q^{-1}(y_0)$ is irreducible.

Now that we have the isomorphism $p\colon \Gamma \to Y \times Y$, we consider the composition $\nu = p_3 \circ p^{-1}\colon Y \times Y \to Y$ and check that

$$\nu(y, y_0) = (p_3 \circ \sigma_2)(y) = y, \quad \nu(y_0, y) = (p_3 \circ \sigma_1)(y) = y$$

Proposition 1.2 implies that Y is an abelian variety with multiplication map ν and neutral element y_0. ∎

Proposition 1.4. *Let $f\colon X \to Y$ be an isogeny of degree n. Then there exists an isogeny $g\colon Y \to X$ with $g \circ f = [n]_X$ and $f \circ g = [n]_Y$.*

Proof. The proof that a finite algebraic group scheme G of rank n is annihilated by $[n]$ is long and technical, so we direct the reader to [EvGM14], Exercise 4.4. and all results cited there. We only remark here that you can reduce to the case where the characteristic of k is prime and $G = G^0$ is local. Here we use that in characteristic 0 all finite group schemes are reduced anyway, so $G^0 = \{\star\}$ (a theorem of Cartier). A short proof of this fact can be found in [Oor66]. In fact, *all* group schemes in characteristic 0 are reduced, but this is harder.

Now since $\deg(f) = n$, the finite group scheme $\ker(f)$ has rank n. Then $\ker(f) \subseteq \ker([n]_X)$, so there is an isogeny

$$g\colon Y = X/\ker(f) \to X/\ker([n]_X) = X$$

such that $[n]_X = g \circ f$. Now

$$[n]_Y \circ f = f \circ [n]_X = (f \circ g) \circ f$$

and since f is flat and surjective, it is an epi and cancels on the right, so $[n]_Y = f \circ g$. ■

Definition 1.5. For abelian varieties X, Y we set $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ as well as $\mathrm{Hom}^0(X, Y) = \mathrm{Hom}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Q}$. ◊

By the previous proposition, all isogenies become invertible in $\mathrm{Hom}^0(X, Y)$, since we can always choose an inverse up to multiplication by n, which is invertible in $\mathbb{Q}$.

Definition 1.6. An abelian variety A is **simple** if there is no nontrivial abelian subvariety $B \subseteq A$. ◊

Theorem 1.7 (Poincaré's irreducibility theorem)**.** *For any abelian variety A, there are simple abelian subvarieties $A_1, \dots, A_m \subseteq A$, pairwise nonisogenous, and integers $n_1, \dots, n_m$ such that the addition map*

$$A_1^{n_1} \times \cdots \times A_m^{n_m} \to A$$

is an isogeny. The numbers n_i and the isogeny type of the A_i are uniquely determined.

Proof. By induction it suffices to show that for each abelian subvariety $B \subseteq A$ there is another abelian subvariety $C \subseteq A$ such that $B + C \to A$ is an isogeny. So let $i\colon B \to A$ denote the inclusion and let $\mathcal{L}$ be any ample line bundle on A. Consider the composition

$$i^\vee \circ \lambda_{\mathcal{L}}\colon A \to B^\vee$$

and define B' to be the connected component of the identity of its kernel. If B' is geometrically reduced, it is an abelian variety and we will assume this. Then

$$\dim B' \geqslant \dim A - \dim B$$

Consider the restriction of $i^\vee \circ \lambda_{\mathcal{L}}$ to B:

$$\begin{aligned}(i^\vee \circ \lambda_{\mathcal{L}} \circ i)(b) &= i^*(t_b^*\mathcal{L} \otimes \mathcal{L}^{-1}) \\ &= i^* t_b^* \mathcal{L} \otimes i^* \mathcal{L}^{-1} \\ &= \mathcal{L}|_B \otimes \mathcal{L}|_B^{-1}\end{aligned}$$

So this is just $\lambda_{\mathcal{L}|_B}$. Ampleness is inherited when restricting to subvarieties, so $\mathcal{L}|_B$ is also ample and therefore $\ker \lambda_{\mathcal{L}|_B}$ is finite. This implies $B \cap B'$ is finite and hence $B \times B' \to A$ is an isogeny by dimension reasons. ■

Remark 1.8. Using a finiteness result about semisimple algebras and the Poincaré irreducibility theorem, Lenstra, Oort and Zarhin proved in [LOZ96] that every abelian variety X over a field contains only finitely many abelian subvarieties, up to isomorphism. More precisely, the number of orbits of the set of abelian subvarieties under the automorphism group of X is finite. ◊

2 The Tate module

In this section we are always working with the rational points of A over a separable closure of k. For notational simplicity, we will therefore assume that k is separably closed. Recall that in this case, for any n not divisible by $p = \mathrm{char}(k)$, we have

$$A(k)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g} \tag{2.1}$$

Of particular interest are the torsion subgroups for n a power of some prime ℓ. We collect the information of the ℓ^m-torsion of A for all exponents m in a single object.

Definition 2.1 (Tate module)**.** Let ℓ be a prime. The ℓ-adic **Tate module** of A is

$$T_\ell(A) = \varprojlim_m A(k)[\ell^m] \qquad \Diamond$$

Equation (2.1) yields a structure theorem for $T_\ell(A)$.

Proposition 2.2. *Let $\ell \neq \mathrm{char}\, k$ be a prime. Then $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$.*

The proof just uses the definition of the ℓ-adic integers and some structure properties of torsion groups. Since the Tate module is free, all abelian varieties of a fixed dimension have isomorphic Tate modules. The object may therefore appear to be trivial or not of great use. But note that the isomorphism given in (2.1) is noncanonical, and the same is true for $T_\ell(A) \cong (\mathbb{Z}_\ell)^{2g}$. It turns out that actually a lot of structure is hidden in the Tate module. We are particularly interested in the action of the absolute Galois group of k on $T_\ell(A)$.

Remark 2.3. How should we think of $T_\ell(A)$? Consider the case $k = \mathbb{C}$. Then $H_1(A, \mathbb{Z})$ is a lattice in $\mathbb{C}^g$ and if we choose a basis, so that $A \cong \mathbb{C}^g/\Lambda$, then

$$\begin{aligned} T_\ell(A) &\cong \varprojlim(\ell^{-m}\Lambda)/\Lambda \\ &= \varprojlim \Lambda \otimes (\ell^{-m}\mathbb{Z}/\mathbb{Z}) \\ &= \Lambda \otimes (\varprojlim \ell^{-m}\mathbb{Z}/\mathbb{Z}) \\ &= \Lambda \otimes \mathbb{Z}_\ell \end{aligned}$$

and therefore $T_\ell(A) = H_1(A, \mathbb{Z}) \otimes \mathbb{Z}_\ell$. This is true for general fields k, i.e. $T_\ell(A)$ is always the first étale homology group of A. $\Diamond$

We can immediately employ the Tate module to show several things about $\mathrm{Hom}(A, B)$. Torsion-freeness is easy:

Lemma 2.4. For any prime $p \neq \ell$, the map

$$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

is injective. As a consequence, $\mathrm{Hom}(A, B)$ is torsion-free.

Proof. Assume $T_\ell(\alpha) = 0$ for some $\alpha \in \mathrm{Hom}(A, B)$ (the map is applied componentwise). Let A' be any simple abelian subvariety of A. Then $\ker \alpha|_{A'}$ contains $A'[\ell^m]$ for all m, so it is not finite. But since A' is simple, the kernel must be the whole A', so $\alpha|_{A'} = 0$ for all simple abelian subvarieties of A. This implies $\alpha = 0$ by the Poincaré irreducibility theorem. ∎

We actually would like that $\mathrm{Hom}(A, B)$ is a free $\mathbb{Z}$-module of finite rank, which we cannot conclude yet because $\mathbb{Z}_\ell$ is not of finite rank over $\mathbb{Z}$. Our wish comes true anyway, and in fact we can even give a bound on the rank in terms of the dimensions of A and B:

Theorem 2.5. *Let A, B be abelian varieties and $\ell \neq \mathrm{char}\, k$. Then the natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

is injective with torsion-free cokernel. In particular, $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of rank at most* $4 \dim(A) \dim(B)$.

The proof requires more time and lemmas than we can afford, so the interested reader is instead directed to Theorem I.10.15 in [Mil08].

Corollary 2.6. The Néron–Severi group $\mathrm{NS}(A)$ of an abelian variety is a free $\mathbb{Z}$-module of rank at most $4 \dim(A)^2$.

Proof. The association $\mathcal{L} \mapsto \lambda_{\mathcal{L}}$ defines an injective map $\mathrm{NS}(A) \to \mathrm{Hom}(A, A^\vee)$. ∎

Could it actually be that the map

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

is an isomorphism? This is certainly not true in full generality; we need at least some sensible finiteness hypotheses on k, for example that k is finitely generated over its prime field. But then still, all homomorphisms $A \to B$ are equivariant under the action of the absolute Galois group $\Gamma = \mathrm{Gal}(\overline{k}/k)$. This is not true for all the elements on the right hand side. So we at least have to restrict to the Γ-equivariant part. Amazingly, it turns out these restrictions are enough.

Theorem 2.7 (Tate's isogeny conjecture)**.** *Let k be finitely generated over its prime field. The natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]}(T_\ell A, T_\ell B)$$

is an isomorphism.

We will discuss Tate's conjecture and its proof in later talks. It was first proved for finite fields by Tate himself, later extended by Zarhin to many cases of function fields in positive characteristic and then proved for number fields by Faltings. His proof can be extended to prove the conjecture for all finitely generated fields.

3 The Weil pairing

Let A be an abelian variety over k and n be any integer not divisible by $p = \operatorname{char} k$. The **Weil pairing** of A is a nondegenerate pairing on geometric points of A and its dual:

$$e_n \colon A(\overline{k})[n] \times A^\vee(\overline{k})[n] \to \mu_n(\overline{k})$$

Here $\mu_n(\overline{k}) \cong \mathbb{Z}/n\mathbb{Z}$ is the group of roots of unity in $\overline{k}$. In this section we will assume $k = \overline{k}$ to reduce notational complexity.

To define the Weil pairing, choose $x \in A(k)[n]$ and $y \in A^\vee(k)[n]$. Then y corresponds to a divisor D on A. By previous lemmas we know that $[n]_A^* D$ is linearly equivalent to nD, which is itself linearly equivalent to 0 (by definition). We may therefore choose two rational functions f and g with $(f) = nD$ and $(g) = [n]_A^* D$. We can calculate the divisor of the rational function $f \circ [n]_A$:

$$\operatorname{div}(f \circ [n]_A) = [n]_A^* \operatorname{div}(f) = n \cdot [n]_A^* D = n \operatorname{div}(g) = \operatorname{div}(g^n)$$

Hence $g^n/(f \circ [n]_A)$ is a constant function (say with value c). Then, for all $a \in A(k)$,

$$g^n(a + x) = cf(na + nx) = cf(na) = g^n(a)$$

so the rational function $g/(g \circ t_x)$ is a root of unity in $K(A)$, hence lies in $\mu_n(k)$.

Example 3.1 (Elliptic curves)**.** We can make all of this very explicit for an elliptic curve $(E, 0_E)$. There is a canonical isomorphism $E \to \operatorname{Pic}^0(E)$ given by $P \mapsto \mathcal{O}_E(P - 0_E)$. Choose $x, y \in E[n]$. Then y corresponds to the line bundle $\mathcal{O}_E(y - 0_E)$ (so $D = y - 0_E$) and we have the divisors

$$nD = n \cdot y - n \cdot 0_E$$

and

$$[n]^* D = \sum_{P \in \sqrt[n]{y}} P - \sum_{Q \in E[n]} Q$$

both linearly equivalent to 0. Pulling this divisor back by t_x we see that g and $g \circ t_x$ have the same poles and zeroes. ◊

Remark 3.2 (See [Sil10])**.** Morally, we can identify $\operatorname{Ext}(A, \mathbb{G}_m)$ and $A^\vee = \operatorname{Pic}^0(A)$ as follows. For any line bundle $\mathcal{L} \in \operatorname{Pic}^0(A)$ we denote by L the total space. Then the multiplication on A induces a multiplication on L and we get various compatibility conditions. If we denote by $G(L)$ the variety that is L with the zero section removed, then these conditions force a group structure on $G(L)$ and we obtain

$$1 \to \mathbb{G}_m \to G(L) \to A \to 0$$

In the other direction, taking any element in $\operatorname{Ext}(A, \mathbb{G}_m)$, we have to "compactify" to get a line bundle over A.

As soon as we have the identification $A^\vee = \operatorname{Ext}(A, \mathbb{G}_m)$, the Weil pairing arises much more naturally. Consider

$$0 \to A[n] \to A \xrightarrow{[n]} A \to 0$$

and apply $\mathrm{Hom}(-, \mathbb{G}_m)$:

$$0 \to \mathrm{Hom}(A, \mathbb{G}_m) \xrightarrow{[n]} \mathrm{Hom}(A, \mathbb{G}_m) \to \mathrm{Hom}(A[n], \mathbb{G}_m) \xrightarrow{\delta} \\ \xrightarrow{\delta} \mathrm{Ext}(A, \mathbb{G}_m) \xrightarrow{[n]} \mathrm{Ext}(A, \mathbb{G}_m)$$

Using that $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ (there are no nonconstant maps from the compact variety A to the affine variety $\mathbb{G}_m$) and $\mathrm{Hom}(A[n], \mathbb{G}_m) = \mathrm{Hom}(A[n], \mu_n)$, we get

$$0 \to \mathrm{Hom}(A[n], \mu_n) \to A^\vee \xrightarrow{[n]} A^\vee$$

so $\mathrm{Hom}(A[n], \mu_n)$ is naturally isomorphic to $A^\vee[n]$ which immediately gives the Weil pairing. ◊

Definition 3.3. Set $\mathbb{Z}_\ell(1) = \varprojlim_n (\mu_{\ell^n}(k))$. By componentwise application, we get a Weil pairing on the Tate module:

$$e_\ell \colon T_\ell(A) \times T_\ell(A^\vee) \to \mathbb{Z}_\ell(1)$$ ◊

Definition 3.4. For any homomorphism $\lambda \colon A \to A^\vee$ we define the induced pairings

$$e_n^\lambda \colon A(k)[n] \times A(k)[n] \to \mu_n(k)$$

and

$$e_\ell^\lambda \colon T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1)$$

by sending $(a, a') \mapsto e_n(a, \lambda(a'))$ and $(a, a') \mapsto e_\ell(a, \lambda(a'))$, respectively. If $\mathcal{L}$ is a line bundle, we set $e_n^{\mathcal{L}} = e_n^{\lambda_{\mathcal{L}}}$ and $e_\ell^{\mathcal{L}} = e_\ell^{\lambda_{\mathcal{L}}}$. ◊

Proposition 3.5 (Properties of the Weil pairing)**.** *Let* $\varphi \colon A \to B$ *be a homomorphism,* $\lambda \in \mathrm{Hom}(B, B^\vee)$ *and* $\mathcal{L} \in \mathrm{Pic}(B)$*. The Weil pairing satisfies*

1. $e_{mn}(a, a')^n = e_m(na, na')$ *for all* m, n *not divisible by* $\mathrm{char}\, k$ *and all* $a \in A(k)[mn]$, $a' \in A^\vee(k)[mn]$.
2. $e_\ell(a, \varphi^\vee(b)) = e_\ell(\varphi(a), b)$ *for all* $a \in T_\ell(A)$, $b \in T_\ell(B)$.
3. $e_\ell^{\varphi^\vee \circ \lambda \circ \varphi}(a, a') = e_\ell^\lambda(\varphi(a), \varphi(a'))$ *for all* $a, a' \in T_\ell(A)$.
4. $e_\ell^{\varphi^* \mathcal{L}}(a, a') = e_\ell^{\mathcal{L}}(\varphi(a), \varphi(a'))$ *for all* $a, a' \in T_\ell(A)$.
5. *The map* $\mathcal{L} \mapsto e_\ell^{\mathcal{L}}$ *is a homomorphism* $\mathrm{Pic}(A) \to \mathrm{Hom}(\wedge^2 T_\ell(A), \mathbb{Z}_\ell(1))$*. In particular,* $e_\ell^{\mathcal{L}}$ *is skew-symmetric.*

Proof. Omitted. ■

It is now time to put all these definitions to some use.

4 Zarhin's trick

An abelian variety A (by definition) always carries a polarization. But it is not true that there is always a principal polarization on A. On the other hand, it is true that $(A \times A^\vee)^\vee \cong A \times A^\vee$. The problem is that we don't know whether this isomorphism comes from a principal polarization, i.e. is of the form $\lambda_{\mathcal{L}}$ for some line bundle $\mathcal{L}$. These facts make (finiteness) results about the moduli of abelian varieties harder than they should be. Zarhin found an interesting trick to circumvent this problem. He shows that we just have to take a higher power: $(A \times A^\vee)^4$ always carries a principal polarization.

Theorem 4.1 (Zarhin's trick)**.** *Let A be an abelian variety. Then $(A \times A^\vee)^4$ is principally polarizable.*

We will need some intermediate results, but their proofs require either étale cohomology or Mumford's theory of theta groups. We will therefore proceed without proving anything more refined. Let $p = \operatorname{char} k$. The various restrictions on the degrees of the polarizations in the statements below can be removed, but that requires work. See chapters 20 and 23 in [Mum08].

Theorem 4.2. *Let $\varphi\colon A \to B$ be an isogeny of degree d with $(d, p) = 1$ and $\lambda \in \mathrm{NS}(A)$ be the equivalence class of a polarization. Then $\lambda = \varphi^*\lambda'$ for some $\lambda' \in \mathrm{NS}(B)$ if and only if for all $\ell \mid d$ there exists a skew-symmetric form*

$$e\colon T_\ell(B) \times T_\ell(B) \to \mathbb{Z}_\ell(1)$$

such that

$$e_\ell^\lambda(a, a') = e(\varphi(a), \varphi(a'))$$

for all $a, a' \in T_\ell(A)$.

In other words, if there are skew-symmetric forms behaving like a Weil pairing for the pullback of a line bundle (see property 4 in Proposition 3.5), then they are indeed induced by one.

Definition 4.3. Let $\lambda\colon A \to A^\vee$ be a polarization and suppose $\ker(\lambda) \subseteq A[n]$ for some n. Then we define

$$e^\lambda\colon \ker(\lambda) \times \ker(\lambda) \to \mu_n$$

as follows. Let $a, a' \in \ker(\lambda)$ and choose a point b with $mb = a'$. Then set

$$e^\lambda(a, a') = e_m(a, \lambda(b))$$

Note that $m \cdot \lambda(b) = \lambda(m \cdot b) = 0$, so e_m is defined on these two points. One uses the properties of the Weil pairing in Proposition 3.5 to show that the definition is independent of the choice of m and b. ◊

Remark 4.4. By passing to the Tate module, i.e. sending a, a' to $(a_n), (a'_n)$ in $T_\ell(A)$, and using property 5 of Proposition 3.5, we can show that e^λ is skew-symmetric. ◊

Proposition 4.5. *Let* $\varphi\colon A \to B$ *be an isogeny of degree* d *where* $(d,p) = 1$ *and fix a polarization* $\lambda\colon A \to A^\vee$*. Then*

$$\lambda = \varphi^\vee \circ \lambda' \circ \varphi$$

for some polarization $\lambda'\colon B \to B^\vee$ *of* B *if and only if*

$$\ker(\varphi) \subseteq \ker(\lambda) \text{ and } e^\lambda|_{\ker(\varphi)\times\ker(\varphi)} = 1$$

Corollary 4.6. Let $\lambda\colon A \to A^\vee$ be a polarization such that $\ker(\lambda) \subseteq A[n]$ with $(n,p) = 1$. If there is exists a $\varphi \in \mathrm{End}(A)$ with $\varphi(\ker(\lambda)) \subseteq \ker(\lambda)$ and $\varphi^\vee \circ \lambda \circ \varphi = -\lambda$ on $A[n^2]$, then $A \times A^\vee$ is principally polarized.

Proof. Let

$$N = \{(a, \varphi(a)) \mid a \in \ker(\lambda)\} \subseteq A \times A\}$$

Then $N \subseteq \ker(\lambda \times \lambda) = \ker(\lambda) \times \ker(\lambda)$. Observe that N is of rank $\deg(\lambda)$. We show that the restriction of $e^{\lambda\times\lambda}$ to N is trivial. Let $(a, \varphi(a)), (a', \varphi(a')) \in N$. Then

$$\begin{aligned} e^{\lambda\times\lambda}((a,\varphi(a)),(a',\varphi(a'))) &= e^\lambda(a,a')e^\lambda(\varphi(a),\varphi(a')) \\ &= e^\lambda(a,a')e^{\varphi^\vee\circ\lambda\circ\varphi}(a,a') \\ &= e_n(a,\lambda(a'))e_n(a,(\varphi^\vee\circ\lambda\circ\varphi)(a')) \\ &= e_n(a,\lambda(a'))e_n(a,-\lambda(a')) \\ &= 1 \end{aligned}$$

We now apply Proposition 4.5 to the projection

$$p\colon A \times A \to (A \times A)/N$$

and the polarization $\lambda \times \lambda\colon A \times A \to A^\vee \times A^\vee$. Since $\ker(p) = N \subseteq \ker(\lambda \times \lambda)$ and $e^{\lambda\times\lambda}$ restricted to $N \times N$ is trivial, we get that $(A \times A)/N$ carries a polarization λ' such that

$$p^\vee \circ \lambda' \circ p = \lambda \times \lambda$$

which implies

$$\deg(\lambda')\deg(p)^2 = \deg(\lambda)^2$$

But $\deg(p) = \deg(\lambda)$, so $\deg(\lambda') = 1$ and $(A \times A)/N$ is principally polarized by λ'. Now consider the map

$$A \times A \to (A \times A)/N, \quad (a, a') \mapsto (a, \varphi(a) + a')$$

Its kernel is exactly $\ker(\lambda) \times \{0\}$, so it factors over $A \times A^\vee$:

$$A \times A \to A \times A^\vee = (A \times A)/(\ker(\lambda) \times \{0\}) \to (A \times A)/N$$

where the last map is an isomorphism by degree reasons. Therefore $A \times A^\vee$ is principally polarized as well. ∎

Proof of Theorem 4.1. Let (A, λ) be a polarized abelian variety and choose an n prime to p such that $\ker(\lambda^4) \subseteq A^4(k)[n]$ (cf. the remark at the beginning of this section). We need to exhibit an endomorphism $\varphi \in \mathrm{End}(A^4)$ satisfying the assumptions of Corollary 4.6. By the four squares theorem of Lagrance, there are integers a, b, c, d with

$$a^2 + b^2 + c^2 + d^2 \equiv -1 \pmod{n}$$

Consider the endomorphism φ of A^4 given by the matrix

$$\varphi = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

Since $\lambda^4 = \mathrm{diag}(\lambda, \lambda, \lambda, \lambda)$ commutes with φ, we have $\varphi(\ker(\lambda^4)) \subseteq \ker(\lambda^4)$. We can compute $\varphi^\vee$ as the transpose of the matrix and therefore we also have

$$\varphi^\vee \circ \lambda^4 \circ \varphi = \varphi^T \circ \varphi \circ \lambda^4$$

We now readily calculate that

$$\varphi^T \circ \varphi = (a^2 + b^2 + c^2 + d^2) I_4 = -1 \qquad \blacksquare$$

5 The Rosati involution

We fix a polarization $\lambda \colon A \to A^\vee$ on an abelian variety A. Recall that, as an isogeny, it has an "inverse" living in $\mathrm{Hom}^0(A^\vee, A)$. We denote it by λ^{-1}.

Definition 5.1. The **Rosati involution** on $\mathrm{End}^0(A)$ is given by

$$\alpha \mapsto \alpha^\dagger = \lambda^{-1} \circ \alpha^\vee \circ \lambda \qquad \Diamond$$

The fixed points of $(-)^\dagger$ have a nice interpretation. They exactly correspond to algebraic equivalence classes of line bundles on A:

Proposition 5.2 ([Mil08], Proposition I.14.2)**.** *Let $k = \overline{k}$. Then the map*

$$\mathcal{L} \mapsto \lambda^{-1} \circ \lambda_{\mathcal{L}}$$

sends $\mathrm{NS}(A) \otimes \mathbb{Q}$ to the subset of fixed points in $(-)^\dagger$ of $\mathrm{End}^0(A)$.

Observe that the image need not necessarily be a subalgebra of $\mathrm{End}^0(A)$. More precisely, the product $\alpha\beta$ of two fixed $\mathbb{Q}$-endomorphisms α and β may itself not be fixed if $\mathrm{End}^0(A)$ is noncommutative, since

$$(\alpha\beta)^\dagger = \beta^\dagger \alpha^\dagger = \beta\alpha$$

is not equal to $\alpha\beta$ in general.

Using $(-)^\dagger$ we can also define a positive-definite bilinear form on $\mathrm{End}^0(A)$. This will allow us to prove a lot of finiteness results for abelian varieties and polarizations.

Theorem 5.3. *The bilinear form*

$$\mathrm{End}^0(A) \times \mathrm{End}^0(A) \to \mathbb{Q}, \quad (\alpha, \beta) \mapsto \mathrm{tr}(\alpha \circ \beta^\dagger)$$

is positive definite, that is $\mathrm{tr}(\alpha \otimes \alpha^\dagger) > 0$ *for all* $\alpha \neq 0$.

Proposition 5.4. *Let* λ *be a polarization on the abelian variety* A*. Then:*

1. *The group of automorphisms of* (A, λ) *is finite.*
2. *Let* $n \geqslant 3$*. If an automorphism of* (A, λ) *acts as the identity on* $A(\overline{k})[n]$*, then it is the identity.*

6 Finiteness results

We now employ all results of this talk to show the finiteness of various moduli of abelian varieties and their polarizations. Our first result only uses the Poincaré irreducibility theorem.

Theorem 6.1. *Let* k *be a finite field and fix* $g, d > 0$*. There are only finitely many isomorphism classes of abelian varieties of dimension* g *possessing a polarization of degree* d^2*. In particular, there are only finitely many isomorphism classes of principally polarized abelian varieties of each dimension.*

Sketch of proof. Use Hirzebruch–Riemann–Roch to show that A can be embedded in $\mathbb{P}^{3^g d-1}$. Its Chow form is then a homogenous polynomial of degree $3^g d \cdot g!$ and determines the isomorphism class of A. There are only finitely many of these homogeneous polynomials with coefficients in k. ■

Using the Rosati involution and ~~some~~ a lot of algebraic results about orders in semisimple algebras we could prove the following two theorems:

Theorem 6.2 ([Mil08], Theorem I.15.1)**.** *Let* A *be an abelian variety over any field* k *and* d *be an integer. Then there are only finitely many isomorphism classes of polarized abelian varieties* (A, λ) *with* λ *of degree* d*.*

In the finite field case we knew this already, by Theorem 6.1. The difference is that we are over any field now and we only consider (varying) polarizations on a fixed abelian variety.

Definition 6.3 (Direct factor)**.** Let B be an abelian subvariety of an abelian variety A. We say B is a **direct factor** of A if there exists another abelian subvariety $C \subseteq A$ such that

$$B \times C \to A, \quad (b, c) \mapsto b + c$$

is an isomorphism. Two direct factors B and C are **isomorphic** if there exists an automorphism α of A such that $\alpha(B) = C$. ◊

Theorem 6.4 ([Mil08], Theorem I.15.3)**.** *An abelian variety has only finitely many direct factors, up to isomorphism.*

We can now finally conclude the most interesting result:

Proposition 6.5. *Let* k *be a finite field. For each* g *there are only finitely many isomorphism classes of abelian varieties of dimension* g *over* k*.*

Remark 6.6. Observe that we *don't* consider a polarization or its degree anymore. This is a much stronger result than Theorem 6.1. ◊

Proof. We know $(A \times A^\vee)^4$ is principally polarized by Zarhin's trick. Theorem 6.1 implies there are only finitely many isomorphism classes of principally polarized varieties of dimension $8g$ over k. Since each of them only has finitely many direct factors (Theorem 6.4) and A is a direct factor of $(A \times A^\vee)^4$, the result follows. ■

References

[EvGM14] B. Edixhoven, G. van der Geer, and B. Moonen. (2014). Abelian varieties. Last retrieved April 20, 2015, [Online]. Available: `http://gerard.vdgeer.net/AV.pdf`.

[LOZ96] H. W. Lenstra, F. Oort, and Y. G. Zarhin, "Abelian subvarieties," *J. Algebra*, vol. 180, pp. 513–516, 1996.

[Mil08] J. S. Milne. (2008). Abelian varieties. Last retrieved April 20, 2015, [Online]. Available: `http://www.jmilne.org/math/CourseNotes/av.html`.

[Mum08] D. Mumford, *Abelian varieties*. New Delhi: Hindustan Book Agency, 2008.

[Oor66] F. Oort, "Algebraic group schemes in characteristic zero are reduced," *Invent. Math.*, vol. 2, pp. 79–80, 1966.

[Sil10] J. H. Silverman, "A survey of local and global pairings on elliptic curves and abelian varieties," in *Pairing-based cryptography – Pairing 2010*, M. Joye, A. Miyaji, and A. Otsuka, Eds. Springer, 2010, pp. 377–396.