Chapter 1

Abelian Varieties

These are notes for BUNTES Fall 2017, the topic is Abelian varieties, they were last updated December 8, 2017. We are using Milne's abelian varieties notes primarily, for more details see the webpage. These notes are by Alex, feel free to email me at `alex.j.best@gmail.com` to report typos/suggest improvements, I'll be forever grateful.

1.1 Introduction (Angus)

1.1.1 Definitions

Definition 1.1.1 (Abelian varieties)**.** An **abelian variety** is a complete connected algebraic group.

Definition 1.1.2 (Algebraic groups)**.** An **algebraic group** is an algebraic variety G along with regular maps $m\colon G \times G \to G$, $e\colon * \to G$, $\mathrm{inv}\colon G \to G$ such that the following diagrams commute.

Identity

$$\begin{tikzcd}
* \times G \arrow[r, "e\times\mathrm{id}"] \arrow[dr, "\sim"'] & G \times G \arrow[d, "m"] & G \times * \arrow[l, "\mathrm{id}\times e"'] \arrow[dl, "\sim"] \\
& G &
\end{tikzcd}$$

Inverse

$$\begin{tikzcd}
G \arrow[r, "{\mathrm{inv},\mathrm{id}}"] \arrow[d] & G \times G \arrow[d, "m"] & G \arrow[l, "{\mathrm{id},\mathrm{inv}}"'] \arrow[d] \\
* \arrow[r, "e"'] & G & * \arrow[l, "e"']
\end{tikzcd}$$

Associativity

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times\mathrm{id}"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"'] & G
\end{tikzcd}$$

Definition 1.1.3 (Complete varieties)**.** A variety X is **complete** if every projection map

$$X \times Y \to Y$$

is closed.

Example 1.1.4 (Abelian varieties)**.**

- Elliptic curves.
- Weil restriction $\mathrm{Res}_{K/\mathbf{Q}} E$ of an elliptic curve E.
- Jacobian varieties of curves.

Plan:

- Some motivation via elliptic curves.
- Gathering some material about "completeness".
- Prove that abelian varieties are abelian.

1.1.2 Elliptic curves ($\mathrm{char}(k) \neq 2, 3$)

Theorem 1.1.5. *TFAE for a projective curve E over k.*

1. *E is given by $Y^2Z = X^3 + aXZ^2 + bZ^3$, $4a^3 + 27b^2 \neq 0$.*
2. *E is nonsingular of genus 1 with a distinguished point P_0.*
3. *E is nonsingular with an algebraic group structure.*
4. *(if $k \subseteq \mathbf{C}$) such that $E(\mathbf{C}) = \mathbf{C}/\Lambda$ for some lattice $\Lambda \subseteq \mathbf{C}$.*

Proof. Strategy: Item 1 $\iff$ Item 2 $\iff$ Item 3 and Item 2 $\implies$ Item 4 $\implies$ Item 1.

Item 1 $\implies$ Item 2 is done.

Item 2 $\implies$ Item 1: Riemann-Roch states that $l(D) = l(K-D)+\deg(D)+1-g$ so here $l(D) = l(K - D) + \deg(D)$ further is $D > 0$ then $l(K - D) = 0$ in which case $l(D) = \deg(D)$. Consider $L(nP_0)$ for $n > 0$ Riemann-Roch implies that $l(nP_0) = n$ then it always contains the constants.

$$L(P_0) = k$$
$$L(2P_0) = k \oplus kx$$
$$L(3P_0) = k \oplus kx \oplus ky$$
$$\vdots$$
$$L(6P_0) = k \oplus kx \oplus ky \oplus kx^2 \oplus ky^2 \oplus kxy \oplus kx^3/\sim$$

so we must have a relation which after manipulation is of the desired form. We get an embedding

$$E \hookrightarrow \mathbf{P}^2$$
$$P \mapsto (x(P) : y(P) : 1)\,(P \neq P_0)$$
$$P_0 \mapsto (0 : 1 : 0)$$

and thus E is of the desired form. ◻

Definition 1.1.6 (Elliptic curves)**.** An **elliptic curve** over k is any/all of that 5.

Which of the above characterisations generalise to abelian varieties?

1. No, in general we don't know that the equations look like.
2. One could possibly replace "genus" with a condition on the dimension of cohomology groups.
3. Yes, this is essentially the definition.
4. Yes, stay tuned!

1.1.3 Complete varieties

Idea: if $X \times Y$ had product topology (instead of its Zariski topology) then complete is equivalent to compact.

We'd like to gather a few results about complete varieties we can use to access properties of abelian varieties (like abelianness).

Proposition 1.1.7. *Let V be a complete variety. Given any morphism $\phi \colon V \longrightarrow W$ $\phi(V)$ is closed.*

Proof. Let $\Gamma_\phi = \{(v, \phi(v))\} \subseteq V \times W$ be the graph of ϕ. Its a closed subvariety of $V \times W$. Under the projection $V \times W \longrightarrow W$, the image of Γ_ϕ is $\phi(V)$ and thus closed. $\square$

Corollary 1.1.8. *If V is complete and connected, any regular function on V is constant.*

Proof. A regular function is a morphism $f \colon V \longrightarrow \mathbf{A}^1$. By the above $f(V) \subseteq \mathbf{A}^1$ is closed, and this is a finite set of points. But connected implies we just have one point. $\square$

Corollary 1.1.9. *Let V be a complete connected variety. Let W be an affine variety. Given $\phi \colon V \longrightarrow W$, then $\phi(V)$ is a point.*

Proof. We have an embedding $W \hookrightarrow \mathbf{A}^n$. On $\mathbf{A}^n$ we have the coordinate functions $\mathbf{A}^n \xrightarrow{x_i} \mathbf{A}^1$. The composition

$$V \xrightarrow{\phi} W \hookrightarrow \mathbf{A}^n \longrightarrow \mathbf{A}^1$$

be the above is constant. Thus the coordinates of $\phi(V)$ are constant, so $\phi(V) = \{\mathrm{pt}\}$. $\square$

A final result of interest that I won't prove today:

Theorem 1.1.10. *Projective varieties are complete.*

The main goal of this section is to prove the following theorem:

Theorem 1.1.11 (Rigidity). *Let V, W be varieties such that V is complete and $V \times W$ is geometrically irreducible. Let $\alpha \colon V \times W \longrightarrow U$ be a morphism such that $\exists u_0 \in U(k), v_0 \in V(k), w_0 \in W(k)$ with $\alpha(V \times \{w_0\}) = \alpha(\{v_0\} \times W) = \{u_0\}$. Then $\alpha(V \times W) = \{u_0\}$.*

Proof. Since $V \times W$ is geometrically irreducible, V must be connected. Denote the projection $q \colon V \times W \longrightarrow W$. Let $U_0 \ni u_0$ be an open neighborhood. We consider the set

$$Z = \{w \in W : \alpha((v, w)) \notin U_0 \text{ for some } v \in V\} = q(\alpha^{-1}(U \setminus U_0))$$

Since q is closed, $Z \subseteq W$ is closed. Since $w_0 \in W \setminus Z$, $W \setminus Z$ is a nonempty open subset of W.

Consider $w \in W \setminus Z$. Since $V \times \{w\} \cong V$ it is complete and connected. Thus

$$\alpha(V \times \{w\}) = \{\mathrm{pt}\} = \alpha((v_0, w)) = \{u_0\}$$

which implies that

$$\alpha(V \times (W \setminus Z)) = \{u_0\}$$

Since $V \times (W \setminus Z) \subseteq V \times W$ is open and $V \times W$ is irreducible, it is dense. So $\alpha(V \times W) = \{u_0\}$. $\square$

Proposition 1.1.12. *Let A, B be abelian varieties. Every morphism $\alpha\colon A \to B$ is the composition of a homomorphism and a translation.*

Proof. First compose by a translation on B such that $\alpha(0) = 0$. Consider the map

$$\begin{aligned}\phi\colon A \times A &\to B\\ (a, a') &\mapsto \alpha(a + a') - \alpha(A) - \alpha(a')\end{aligned}$$

Then

$$\begin{aligned}\phi(A \times \{0\}) &= \alpha(a + 0) - \alpha(a) - \alpha(0) = 0\\ \phi(\{0\} \times A) &= \alpha(0 + a) - \alpha(0) - \alpha(a) = 0.\end{aligned}$$

By the rigidity theorem 11 $\phi(A \times A) = \{0\}$ hence $\alpha(a + a') = \alpha(a) + \alpha(a')$. ☐

Corollary 1.1.13. *Abelian varieties are abelian.*

Proof. The inversion map $a \mapsto -a$ sends 0 to 0, thus is a homomorphism. Therefore

$$a + b - a - b = a + b - (a + b) = 0$$

and so

$$a + b = b + a.$$

☐

1.2 Abelian varieties over C (Alex)

The goal of this talk is to understand what abelian varieties look like over $\mathbf{C}$. The goal for me is to understand what a (principal) polarisation is and why it is important.

First immediate question: why study complex theory at all? The most classical field, algebraically closed, archimidean, characteristic 0.

Recall/rapidly learn the picture for elliptic curves, given E an elliptic curve we have for some Λ a rank 2 lattice in $\mathbf{C}$

$$\begin{aligned}\mathbf{C}/\Lambda &\xrightarrow{\sim} E(\mathbf{C}) \subseteq \mathbf{P}^2(\mathbf{C})\\ z &\mapsto (\wp(z) : \wp'(z) : 1)\\ 0 &\mapsto (0 : 1 : 0)\end{aligned}$$

where

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \smallsetminus \{0\}} \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2}.$$

This is a meromorphic function whose image lands in

$$y^2 = 4x^3 - g_2 x - g_3.$$

So the $\mathbf{C}$ points of an elliptic curve are topologically a torus.

Naturally one asks: does this generalise? Let A be an abelian variety over $\mathbf{C}$, what does $A(\mathbf{C})$ look like? Another torus?

Proposition 1.2.1. *$A(\mathbf{C})$ is a compact, connected, complex lie group.*

Proposition 1.2.2. *Let A be an abelian variety of dimension g over $\mathbf{C}$. Then we have*

$$A(\mathbf{C}) \cong V/\Lambda$$

where V is a g dimensional complex vector space and Λ is a full rank lattice of V (i.e Λ is a discrete subgroup of V s.t. $\mathbf{R} \otimes \Lambda = V$).

Proof. Differential geometry gives us a map of complex manifolds, the exponential map

$$\exp\colon \operatorname{Tgt}_0(A(\mathbf{C})) \to A(\mathbf{C})$$

this is holomorphic. And since $A(\mathbf{C})$ is abelian, this is a homomorphism also. In general this is locally an isomorphism around 0.

Claim: exp is injective. There exists a neighborhood $U \supseteq 0$ s.t. $\exp(U) \cong U$. Consider the image $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$. For $x \in \exp(\operatorname{Tgt}_0 A(\mathbf{C}))$, $\{U + x\}$ are all open and give a cover. Thus $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is open. Since $A(\mathbf{C})$ is connected we are thus reduced to showing $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is closed also. Since exp is a homomorphism, the image is a subgroup. So its complement is the union of its non-trivial cosets, which is open. Thus $\exp(\operatorname{Tgt}_0 A(\mathbf{C}))$ is closed. Giving $\exp(\operatorname{Tgt}_0 A(\mathbf{C})) = A(\mathbf{C})$, which proves the claim.

exp is a local isomorphism, which gives that ker(exp) is discrete, i.e. a lattice. We now have

$$A(\mathbf{C}) \cong \operatorname{Tgt}_0 A(\mathbf{C})/\ker(\exp)$$

so as $A(\mathbf{C})$ is compact we cannot have a kernel which is not full rank, as otherwise the quotient could not be compact. □

Definition 1.2.3. We call any such V/Λ a **complex torus**.

From the above isomorphism we can now read off properties of $A(\mathbf{C})$ as a group.

Proposition 1.2.4. *$A(\mathbf{C})$ is divisible, and $A(\mathbf{C})[n] \cong (\mathbf{Z}/n\mathbf{Z})^{2g}$.*

Proof.

$$A(\mathbf{C}) \cong V/\Lambda \cong (\mathbf{R}/\mathbf{Z})^{2g}$$

isomorphisms as groups, thus $A(\mathbf{C})$ is divisible. Further, $(\mathbf{R}/\mathbf{Z})[n] = (\frac{1}{n}\mathbf{Z})/\mathbf{Z}$. □

Question: Given a complex torus V/Λ, does there exist an abelian variety A such that $A(\mathbf{C}) \cong V/\Lambda$?

Example 1.2.5.

- $$\mathbf{C}/\Lambda \cong E(\mathbf{C}) \text{ always in dim } 1$$
- $$\mathbf{C}^2/\Lambda^2 \cong (E \times E)(\mathbf{C}) \text{ sometimes yes in higher dimension}$$
- $$\mathbf{C}^2/\langle (i,0), (i\sqrt{p}, i), (1,0), (0,1)\rangle_{\mathbf{Z}}$$

  for p prime??? (I guess not, see Mumford)

Theorem 1.2.6 (Chow)**.** *If X is an analytic submanifold of $\mathbf{P}^n(\mathbf{C})$ then X is an algebraic subvariety.*

By this theorem it is enough to analytically imbed $V/\Lambda \hookrightarrow \mathbf{P}^m$. We can try and do this by mimicing the elliptic curve strategy, find enough functions $\theta\colon V/\Lambda \to \mathbf{C}$.

Proposition 1.2.7. *Let $X = V/\Lambda$. Then*

$$H^r(X, \mathbf{Z}) \cong \{\textit{alternating } r\textit{-forms } \Lambda \times \cdots \times \Lambda \to \mathbf{Z}\}.$$

Proof. $\pi\colon V \to V/\Lambda$ is a universal covering map, so

$$\Lambda = \pi^{-1}(0) \cong \pi_1(X, 0).$$

Because all these spaces are nice

$$H^1(X, \mathbf{Z}) \cong \mathrm{Hom}(\pi_1(X), \mathbf{Z}) \cong \mathrm{Hom}(\Lambda, \mathbf{Z}).$$

To extend to $r \neq 1$ use the Künneth formula:

$$\begin{tikzcd}
\bigwedge^r(H^1(X_1 \times X_2, \mathbf{Z})) \arrow[rr, equal] \arrow[d, equal, "\text{Künneth}"] & & H^r(X_1 \times X_2, \mathbf{Z}) \arrow[dd, equal, "\text{Künneth}"] \\
\bigwedge^r(H^1(X_1, \mathbf{Z}) \otimes H^1(X_2, \mathbf{Z})) \arrow[d, equal] & & \\
\bigoplus_{p+q=r}(\bigwedge^p(H^1(X_1, \mathbf{Z})) \otimes \bigwedge^q(H^1(X_2, \mathbf{Z}))) \arrow[rr, equal] & & \bigoplus_{p+q=r}(H^p(X_1, \mathbf{Z}) \otimes H^q(X_2, \mathbf{Z}))
\end{tikzcd}$$

Since we know the proposition for $S^1 = \mathbf{R}/\mathbf{Z}$ by taking products and applying the above we get it for all complex tori V/Λ. ◻

Proposition 1.2.8. *There is a correspondence*

$$\{\textit{Hermitian forms } H \textit{ on } V\} \leftrightarrow \{\textit{Alternating forms } E\colon V \times V \to \mathbf{R},\ E(iu, iv) = E(u, v)\}$$

$$H \mapsto \operatorname{im} H$$

$$E(iu, v) + iE(u, v) \leftarrow\!\shortmid E.$$

Now we will consider line bundles on $X = V/\Lambda$, that is

$$L \xrightarrow{\pi} X$$

such that for any $x \in X$ there exists $U \ni x$ with $\pi^{-1}(U) \cong \mathbf{C} \times U$. We can obtain these from hermitian forms and some auxilliary data as follows.

Definition 1.2.9. If H is a hermitian form on V such that $E(\Lambda \times \Lambda) \subseteq \mathbf{Z}$ there exists a map

$$\alpha\colon \Lambda \to \mathbf{C}^* = \{z \in \mathbf{C}^* : |z| = 1\}$$

such that

$$\alpha(u + v) = e^{i\pi E(u,v)}\alpha(u)\alpha(v).$$

Further, there is a line bundle $L(H, \alpha)$ on X which is defined by quotienting $\mathbf{C} \times V$ by Λ which acts via

$$\phi_u(\lambda, v) = (\alpha(u)e^{\pi H(v,u) + \frac{1}{2}\pi H(u,u)}\lambda, v + u) \text{ for } u \in \Lambda,$$

we'll denote by e_u the factor $\alpha(u)e^{\pi H(v,u)+\frac{1}{2}\pi H(u,u)}$ for brevity.

Theorem 1.2.10 (Appell-Humbert)**.** *Any line bundle on X is of the form $L(H, \alpha)$ for some H, α as above. Further*

$$L(H_1, \alpha_1) \otimes L(H_2, \alpha_2) = L(H_1 + H_2, \alpha_1\alpha_2).$$

In fact we have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}(\Lambda, \mathbf{C}) \arrow[r] \arrow[d] & \{\textit{data } (H, \alpha)\} \arrow[r] \arrow[d] & \{\textit{gp. of Herm. } H \textit{ w/ } E(\Lambda \times \Lambda) \subseteq \mathbf{Z}\} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Pic}^0(X) \arrow[r] & \mathrm{Pic}(X) \arrow[r, "c"'] & \ker(H^2(X, \mathbf{Z}) \to H^2(X, \mathcal{O}_X)) \arrow[r] & 0
\end{tikzcd}$$

where $\mathrm{Pic}(X)$ *is the group of all line bundles on* X *and* Pic^0 *is the subgroup of those which are topologically trivial.*

We wanted functions $X \to \mathbf{C}$. Now we can instead consider sections s of $L(H,\alpha) \xrightarrow{\pi} X$ i.e. maps $s\colon X \to L(H,\alpha)$ with $\pi \circ s = \mathrm{id}$. Denote the space of such sections $H^0(X, L(H,\alpha))$.

Definition 1.2.11 (Theta functions)**.** The sections of $L(H,\alpha)$ correspond to holomorphic functions

$$\theta\colon V \to \mathbf{C}$$

such that $\theta(z+u) = e_u\theta(z)$, we will call such a θ a **theta function** for (H,α).

If H is not positive definite the space of such functions is 0!

Proposition 1.2.12. *If H is positive definite, then the dimension of $H^0(X, L(H,\alpha))$ is $\sqrt{\det E}$ where we really mean the determinant of a matrix for E with respect to an integral basis.*

Theorem 1.2.13 (Lefschetz)**.** *Given a positive definite H, there exists an imbedding $X \hookrightarrow \mathbf{P}^m$.*

Proof. Sketch: Let $L = L(H,\alpha)$, consider $L(H,\alpha)^{\otimes 3} = L(3H, \alpha^3)$, take a basis of $\theta_0, \dots, \theta_d$ of $H^0(X, L^{\otimes 3})$.

Claim: $\Theta\colon z \mapsto (\theta_0(z) : \cdots : \theta_d(z)) \subseteq \mathbf{P}^d$ is an embedding.

To see that this is well defined, we must give a section of $L^{\otimes 3}$ not vanishing at z for all $z \in X$. Let $\theta \in H^0(X,L) \smallsetminus \{0\}$. Then pick a, b such that the section of $L^{\otimes 3}$ given by

$$\theta(z-a)\theta(z-b)\theta(z+a+b)$$

does not vanish. This is possible and thus we have a nonvanishing section of $L^{\otimes 3}$.

For injectivity, show that if the above section has the same values on z_1, z_2 then it is a theta function for some sublattice. Almost all sections aren't theta functions for a sublattice (this uses Proposition 12).

Something similar must be done for tangent vectors. □

Definition 1.2.14 (Riemann forms)**.** A **Riemann form** is $E\colon \Lambda \times \Lambda \to \mathbf{Z}$ alternating such that

$$E_{\mathbf{R}}\colon V \times V \to \mathbf{R}$$

has the property that $E(iu, iv) = E(u,v)$ and the corresponding Hermitian form is positive definite.

Definition 1.2.15 (Polarizable tori)**.** A complex torus $X = V/\Lambda$ is **polarizable** if there exists a Riemann form E on Λ.

Example 1.2.16 (Proposition)**.** Every $\mathbf{C}/\Lambda$ where $\Lambda = \langle 1, \tau\rangle_{\mathbf{Z}}$ is polarizable.

To see this take

$$E(u,v) = \frac{uv}{\operatorname{im}\tau}$$

as a Riemann form.

Putting everything together we have obtained an equivalence of categories

$$\{\text{abelian varieties over } \mathbf{C}\} \leftrightarrow \{\text{polarizable complex tori}\}.$$

Definition 1.2.17 (Isogenies of complex tori)**.** An **isogeny** of complex tori is a homomorphism $V/\Lambda \to V'/\Lambda'$ with finite kernel.

Definition 1.2.18 (Dual vector spaces)**.** Given V a complex vector space, let

$$V^* = \{f\colon V \to \mathbf{C} : f(u+v) = f(u) + f(v),\ f(\alpha v) = \bar{\alpha} f(v)\}$$

and given $\Lambda \subset V$ a lattice, let

$$\Lambda^* = \{f \in V^* : f(\lambda) \in \mathbf{Z}\, \forall \lambda \in \Lambda\}.$$

Definition 1.2.19 (Dual tori)**.** If $X = V/\Lambda$, $X^\vee = V^*/\Lambda^*$ is the **dual torus**.

Proposition 1.2.20 (Existence of Weil pairing)**.**

$$X \times X^\vee \to \mathbf{C}$$

so

$$X[n] \times X^\vee[n] \to \left(\frac{1}{n^2}\mathbf{Z}/\frac{1}{n}\mathbf{Z}\right) \cong \mathbf{Z}/n\mathbf{Z}$$

this is called the ***Weil pairing****.*

Can a complex torus be isogenous to its own dual? If X is polarizable then

$$\begin{aligned} X &\to X^\vee \\ v &\mapsto H(v,-) \end{aligned}$$

is an isogeny.

Definition 1.2.21. A **polarization** is an isogeny $X \to X^\vee$.

1.3 Rational Maps into Abelian Varieties (Maria)

Note all varieties are irreducible today.

1.3.1 Rational maps

V, W varieties $/K$. Consider pairs (U, ϕ_U), where $\emptyset \neq U \subset V$ an open subset so U is dense, and $\phi_U\colon U \to W$ is a regular map.

Definition 1.3.1 (Rational maps)**.** (U, ϕ_U), $(U', \phi_{U'})$ are equivalent if ϕ_U and $\phi_{U'}$ agree on $U \cap U'$. An equivalence class ϕ of $\{(U, \phi_U)\}$ is a **rational map** $\phi\colon V \dashrightarrow W$ If $\phi\colon V \dashrightarrow W$ is defined at $v \in V$ if $v \in U$ for some $(U, \phi_U) \in \phi$.

Note 1.3.2. The set $U_1 = \bigcup U$ where ϕ is defined is open and $(U_1, \phi_1) \in \phi$ where $\phi_1\colon U_1 \to W$ restricts to ϕ_U on U.

Example 1.3.3.

1. Let $\emptyset \neq W \subseteq V$ be open. Then the rational map $V \dashrightarrow W$ induced by $\mathrm{id}\colon W \to W$ will not extend to V. To avoid this, assume W is complete (so $W = V$).

2. $C\colon y^2 = x^3$, then $\alpha\colon \mathbf{A}^1 \to C$, $a \mapsto (a^2, a^3)$ is a regular map, restricting to an isomorphism $\mathbf{A}^1 \setminus \{0\} \to C \setminus \{0\}$. The inverse of $\alpha|_{\mathbf{A}^1 \setminus \{0\}}$ represents $\beta\colon C \dashrightarrow \mathbf{A}^1$ which does not extend to C. This corresponds on function fields to

$$K(t) \to K(x,y)$$
$$t \mapsto y/x$$

which does not send $K[y]_{(t)}$ to $K[x,y]_{(x,y)}$.

3. Given a nonsingular surface V, $P \in V$ then $\exists \alpha \colon W \to V$ regular that induces an isomorphism $\alpha \colon W \setminus \alpha^{-1}(P) \to V \setminus P$, but $\alpha^{-1}(P)$ is a projective line. The rational map represented by α^{-1} is not regular on V (where to send P?).

Theorem 1.3.4 (Milne 3.1)**.** *A rational map $\phi \colon V \dashrightarrow W$ from a nonsingular variety V to a complete variety W is defined on an open subset $U \subseteq V$ whose complement has codimension ≥ 2.*

Proof. (V a curve) V nonsingular curve, $\emptyset \neq U \subseteq V$ open, $\phi \colon U \to W$ a regular map.

$$\begin{tikzcd} & V & \\ U \arrow[ur] \arrow[r] \arrow[dr] & U' \subseteq Z \subseteq V \times W \ni (v, w) \arrow[u, "p"] \arrow[d, "q"'] & \\ & W \ni w & \end{tikzcd}$$

U' is the image of U, $Z = \overline{U'}$. W is complete, Z closed implies $p(Z) \subseteq V$ is closed. Also, $U \subseteq p(Z) \implies p(Z) = V$.

$$U \xrightarrow{\sim} U' \to U$$

so

$$U' \xrightarrow{\sim} U$$

$$Z \twoheadrightarrow V$$

this implies $Z \xrightarrow{\sim} V$. Then $q|_Z \colon Z \to W$ is the extension of ϕ to V. □

Theorem 1.3.5 (Milne 3.2)**.** *A rational map $\phi \colon V \dashrightarrow A$ from a nonsingular variety V to an abelian variety W, extends to all of V.*

Proof. Theorem 4 Lemma 6 □

Lemma 1.3.6. *Let $\phi \colon V \dashrightarrow G$ be a map from a nonsingular variety to a group variety. Then either ϕ is defined on all of V or the set where ϕ is not defined is closed of pure codimension 1.*

Proof. Fix $(U, \phi_U) \in \phi$ and consider

$$\Phi \colon V \times V \dashrightarrow G$$

represented by

$$U \times U \xrightarrow{\phi_U \times \phi_U} G \times G \xrightarrow{\mathrm{id} \times \mathrm{inv}} G \times G \xrightarrow{m} G$$

$$(x, y) \mapsto \phi_U(x)\phi_U(y)^{-1}$$

Check ϕ is defined at x iff Φ is defined at (x, x) (and in this case $\Phi(x, x) = e$). This is equivalent to the map $\Phi^* \colon \mathcal{O}_{G,e} \to K(V \times V)$ induced by Φ satisfying $\mathrm{im}(\mathcal{O}_{G,e}) \subseteq \mathcal{O}_{V \times V,(x,x)}$ For a nonzero function f on $V \times V$, write $\mathrm{div}(f) = \mathrm{div}(f)_0 - \mathrm{div}(f)_\infty$ which are effective divisors. Then

$$\mathcal{O}_{V \times V,(x,x)} = \{0\} \cup \{f \in K(V \times V) : \mathrm{div}(f)_\infty \text{ does not contain } (x, x)\}.$$

Suppose ϕ is not defined at x, then there exists $f \in \mathrm{im}(\mathcal{O}_{G,e})$ s.t. $(x, x) \in \mathrm{div}(f)_\infty$. Then Φ is not defined at any $(y, y) \in \Delta \cap \mathrm{div}(f)_\infty = \mathrm{div}(f^{-1})_0$, which is a pure codimension 1 subset of Δ by Milne's AG thm 9.2. The corresponding subset in V is of pure codimension 1, and ϕ is not defined there. □

Theorem 1.3.7 (Milne 3.4)**.** *Let $\alpha\colon V\times W\to A$ be a morphism from a product of nonsingular varieties into an abelian variety. If $\alpha(V\times\{w_0\})=\{a_0\}=\alpha(\{v_0\}\times W)$ for some $a_0\in A$, $v_0\in W$, $w_0\in W$, then $\alpha(V\times W)=\{a_0\}$.*

Corollary 1.3.8 (Milne 3.7)**.** *Every rational map $\alpha\colon G\dashrightarrow A$ from a group variety into an abelian variety is the composition of a homomorphism and a translation in A.*

Proof. Since group varieties are nonsingular, $\alpha\colon G\to A$ is a regular map by Theorem 5. The rest is as proof of Corollary 1.2. □

1.3.2 Dominating and birational maps

Definition 1.3.9 (Dominating maps)**.** $\phi\colon V\dashrightarrow W$ is **dominating** if $\operatorname{im}(\phi_U)$ is dense in W for a representative $(U,\phi_U)\in\phi$.

Exercise: A dominating $\phi\colon V\dashrightarrow W$ defines a homomorphism $K(W)\to K(V)$ and any such homomorphism arises from a unique dominating rational map.

Definition 1.3.10. $\phi\colon V\dashrightarrow W$ is **birational** if the corresponding $K(W)\to K(V)$ is an isomorphism or, equivalently if there exists $\psi\colon W\dashrightarrow V$ s.t. $\phi\circ\psi$ and $\psi\circ\phi$ are the identity wherever they are defined. In this case we say V and W are **birationally equivalent**.

Note 1.3.11. In general birational equivalence does not imply isomorphic. E.g. V a variety $\emptyset\neq W\subsetneq V$ an open subset, or $V=\mathbf{A}^1$, $W\colon y^2=x^3$.

Theorem 1.3.12 (Milne 3.8)**.** *If two abelian varieties are birationally equivalent then they are isomorphic as abelian varieties.*

Proof. A,B abelian varieties with $\phi\colon A\dashrightarrow B$ a birational map with inverse ψ. Then by Theorem 5 ϕ,ψ extend to regular maps $\phi\colon A\to B$, $\psi\colon B\to A$ and $\phi\circ\psi,\psi\circ\phi$ are the identity everywhere. This implies that ϕ is an isomorphism of algebraic varieties and after composition with a translation, ϕ is also a group isomorphism. □

Proposition 1.3.13 (Milne 3.9)**.** *Any rational map $\mathbf{A}^1\dashrightarrow A$ or $\mathbf{P}^1\dashrightarrow A$, for A an abelian variety is constant.*

Proof. Theorem 5 implies $\alpha\colon\mathbf{A}^1\dashrightarrow A$ extends to $\alpha\colon\mathbf{A}^1\to A$ and we may assume $\alpha(0)=e$. $(\mathbf{A}^1,+)$: $\alpha(x+y)=\alpha(x)+\alpha(y)$ for all $x,y\in\mathbf{A}^1(K)=K$. $(\mathbf{A}^1\setminus\{0\},\cdot)$: $\alpha(xy)=\alpha(x)+\alpha(y)+c$ for all $x,y\in K^\times$. These can only hold at the same time if α is constant. $\mathbf{P}^1\dashrightarrow A$ is constant, since its constant on affine patches. □

Definition 1.3.14. $V/\overline{K}$ is **unirational** if there is a dominating map $\mathbf{A}^n\dashrightarrow V$, where $n=\dim_{\overline{K}}V$. V/K is unirational if $V/\overline{K}$ is.

Proposition 1.3.15 (Milne 3.10)**.** *Every rational map $V\dashrightarrow A$ from V unirational to A abelian is constant.*

Proof. Wlog $K=\overline{K}$. Since V is unirational we get $\beta\colon\mathbf{P}^1\times\cdots\times\mathbf{P}^1\dashrightarrow V\dashrightarrow A$, which extends to $\beta\colon\mathbf{P}^1\times\cdots\times\mathbf{P}^1\to A$. Then by Milne corollary 1.5, there exist regular maps $\beta_i\colon\mathbf{P}^1\to A$ s.t. $\beta(x_1,\dots,x_n)=\sum\beta_i(x_i)$ and by Proposition 13 each β_i map is constant. □

1.4 Theorem of the Cube (Ricky)

1.4.1 Crash Course in Line Bundles

Consider $\mathbf{R}^2$, $f: \mathbf{R} \to \mathbf{R}$, $f(x,y) = x^2 + y^2 - 1$, now $S = \{f = 0\} \subseteq \mathbf{R}^2$ is a closed submanifold (in fact a circle). Question: Do all closed submanifolds arise in this way? Lets switch to $\mathbf{C}$ better analogies with AG.

Example 1.4.1. Let $X \in \mathbf{P}^n(\mathbf{C})$, the answer here is no! (Because $f: X \to \mathbf{C}^1$ is constant!) Want to define functions locally that give us level sets, but gluing such will give us a global section. Instead glue in a different way (i.e. into different "copies" of $\mathbf{C}$) so that this doesn't happen.

Example 1.4.2. $X \in \mathbf{P}^1_{\mathbf{C}}$, $\mathcal{O}_X$ the structure sheaf.

$$X = U_0 \cup U_1 = (\mathbf{A}^1, t) \cup (\mathbf{A}^1, s)$$

on $U_0 \cap U_1$, $t = s^{-1}$. What is a global section of $\mathcal{O}_X$, a section of U_0 and a section of U_1 that glue. $\mathcal{O}_X(U_0) = k[t], \mathcal{O}_X(U_1) = k[s]$ so given $f(t), g(s)$ these glue to a global section iff $f(t) = g(1/t)$ so f, g must be constant.

Definition 1.4.3 (Line bundles)**.** A **line bundle** on X is a locally free $\mathcal{O}_X$-module of rank 1, i.e. $\exists\{U_i\}$ open cover along with isomorphisms $\phi_i\colon \mathcal{L}|_{U_i} \xrightarrow{\sim} \mathcal{O}_X|_{U_i}$.

Exercise 1.4.4. Alternative definition: A line bundle on X is equivalent to the following data:

- An open cover of X.
- Transition maps $\tau_{ij} \in \mathrm{GL}_1(\mathcal{O}_X(U_i \cap U_j))$ satisfying $\tau_{ij}\tau_{jk} = \tau_{ik}$ and $\tau_{ii} = \mathrm{id}$.

Example 1.4.5. On $X = \mathbf{P}^n_k$, we have line bundles $\mathcal{O}(d)$ for all $d \in \mathbf{Z}$. Just have to give cover and transition functions, use usual open cover $\{U_i\}$ with $U_i \cong \mathbf{A}^n$. Then τ_{ji} is given by multiplication by $(x_i/x_j)^d$.

Exercise 1.4.6.

$$H^0(X, \mathcal{O}(d))(= \Gamma(X, \mathcal{O}(d)))$$

$= k$vector space spanned by deg. d homogenous polynomials in $k[x_0, \ldots, x_n]$.

Exercise 1.4.7. All line bundles on $\mathbf{P}^n$ are isomorphic to some $\mathcal{O}(d)$.

We say a line bundle $\mathcal{L}$ on X is trivial if $\mathcal{L} \cong \mathcal{O}_X$. Given $\mathcal{L}_1$ and $\mathcal{L}_2$ on X (line bundles) we can create a new line bundle $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$. So isomorphism classes of line bundles on X with $\otimes$ form a group, denoted $\mathrm{Pic}(X)$ with identity $\mathcal{O}_X$ and inverses $\mathcal{L}^{-1} = \mathrm{Hom}(\mathcal{L}, \mathcal{O}_X)$.

Example 1.4.8. By previous exercise $\mathrm{Pic}(\mathbf{P}^n_k) \cong \mathbf{Z}$ since $\mathcal{O}_X(d_1) \otimes \mathcal{O}_X(d_2) \cong \mathcal{O}_X(d_1 + d_2)$.

Fact 1.4.9. *If $f: X \to Y$, then given $\mathcal{L}$ on Y we can pullback to a line bundle $f^*\mathcal{L}$ on X, definition is complicated. We also know that f^* commutes with $\otimes$ so in fact (as $f^*\mathcal{O}_Y = \mathcal{O}_X$) we get a homomorphism $f^*\colon \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$.*

1.4.2 Relation to (Weil) divisors

Let X be a normal variety, call $Z \subseteq X$, a closed subvariety of codimension 1, a **prime divisor**. Then a divisor on X is a formal sum

$$D = \sum_{Z \subseteq X} n_Z \cdot Z$$

of prime divisors.

Let $K = K(X)$ be the function field of X. Given $f \in K^\times$ we can define

$$\operatorname{div}(f) = \sum v_Z(f) \cdot Z.$$

Given $D \in \operatorname{Div}(X)$, we can define a line bundle $\mathcal{L}(D)$ on X via

$$\mathcal{L}(D)(U) = \{f \in K^\times : (D + \operatorname{div}(f))|_U \geq 0\} \cup \{0\}$$

where $D|_U = \sum_{Z \cap U \neq \emptyset} n_Z \cdot (Z \cap U)$.

Proposition 1.4.10. *The map*

$$\operatorname{Cl}(X) = \operatorname{Div}(X)/\operatorname{Princ}(X) \xrightarrow{\mathcal{L}(\cdot)} \operatorname{Pic}(X)$$

is an isomorphism.

1.4.3 Onto cubes

Theorem 1.4.11 (Theorem of the cube)**.** *Let U, V, W be complete varieties. If $\mathcal{L}$ is a line bundle on $U \times V \times W$ s.t. $\mathcal{L}|_{\{u_0\} \times V \times W}, \mathcal{L}|_{U \times \{v_0\} \times W}, \mathcal{L}|_{U \times V \times \{w_0\}}$ are all trivial then $\mathcal{L}$ is trivial.*

Corollary 1.4.12 (Milne 5.2)**.** *Let A be an abelian variety. Let $p_i \colon A \times A \times A \to A$ be the projection onto the ith coordinate. $p_{ij} = p_i + p_j$, $p_{123} = p_1 + p_2 + p_3$. Then for any $\mathcal{L}$ on A, the line bundle*

$$\mathcal{M} = p_{123}^* \mathcal{L} \otimes p_{12}^* \mathcal{L}^{-1} \otimes p_{23}^* \mathcal{L}^{-1} \otimes p_{13}^* \mathcal{L}^{-1} \otimes p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \otimes p_3^* \mathcal{L}$$

is trivial.

Proof. Let $m \colon A \times A \to A$ be multiplication (addition?) and p, q the projections $A \times A \to A$. Then the composites of the maps $\phi \colon A \times A \to A \times A \times A$, $\phi(x, y) = (x, y, 0)$ with $p_{123}, p_{12}, p_{23}, p_{13}, p_1, p_2, p_3$ are respectively $m, m, q, p, p, q, 0$. Hence the restriction of $\mathcal{M}$ to $A \times A \times \{0\}$ is

$$m^* \mathcal{L} \otimes m^* \mathcal{L}^{-1} \otimes q^* \mathcal{L}^{-1} \otimes p^* \mathcal{L}^{-1} \otimes p^* \mathcal{L} \otimes q^* \mathcal{L} \otimes \mathcal{O}_{A \times A}$$

this is trivial by tensor commuting with pullback. Similarly $\mathcal{M}$ restricts to a trivial bundle on $A \times \{0\} \times A$ and $\{0\} \times A \times A$. So by theorem of the cube 11 $\mathcal{M}$ is trivial. □

Corollary 1.4.13 (Milne 5.3)**.** *Let $f, g, h \colon V \to A$ (A abelian). Then for any $\mathcal{L}$ on A the bundle*

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

is trivial.

Proof. $\mathcal{M}$ is the pullback of the line bundle of Corollary 12 via the map $(f, g, h) \colon V \to A \times A \times A$. □

On A we have $n_A : A \to A$ be $n_A(a) = a + \cdots + a$ (n times) for $n \in \mathbf{Z}$.

Corollary 1.4.14 (Milne 5.4)**.** *For $\mathcal{L}$ on A we have*

$$n_A^* \mathcal{L} \cong \mathcal{L}^{(n^2+n)/2} \otimes (-1)_A^* \mathcal{L}^{(n^2-n)/2}$$

In particular if $(-1)^* \mathcal{L} = \mathcal{L}$ (symmetric) then $n_A^* \mathcal{L} = \mathcal{L}^{n^2}$. And if $(-1)^* \mathcal{L} = \mathcal{L}^{-1}$ (antisymmetric) then $n_A^* \mathcal{L} = \mathcal{L}^n$.

Proof. Use Corollary 13 with $f = n_A, g = 1_A, h = (-1)_A$. So the line bundle

$$(n)^* \mathcal{L} \otimes (n+1)^* \mathcal{L}^{-1} \otimes (n-1)^* \mathcal{L}^{-1} \otimes (1-1)^* \mathcal{L}^{-1} \otimes n^* \mathcal{L} \otimes 1^* \mathcal{L} \otimes (-1)^* \mathcal{L}$$

is trivial i.e.

$$(n+1)^* \mathcal{L} = (n-1)^* \mathcal{L}^{-1} \otimes n^* \mathcal{L}^2 \otimes \mathcal{L} \otimes (-1)^* \mathcal{L}$$

in statement $n = 1$ is clear, so use $n = 1$ in the above to get

$$2_A^* \mathcal{L} \cong \mathcal{L}^2 \otimes \mathcal{L} \otimes (-1)_A^* \mathcal{L} \cong \mathcal{L}^3 \otimes (-1)_A^* \mathcal{L}.$$

Then induct on n in above. □

Theorem 1.4.15 (Theorem of the square (Milne 5.5))**.** *Let $\mathcal{L}$ be an invertible sheaf (line bundle) on A. Let $t_a : A \to A$ be translation by $a \in A(k)$. Then*

$$t_{a+b}^* \mathcal{L} \otimes \mathcal{L} \cong t_a^* \mathcal{L} \otimes t_b^* \mathcal{L}.$$

Proof. Use Corollary 13 with $f = \mathrm{id}$, $g(x) = a, h(x) = b$ to get

$$t_{a+b}^* \mathcal{L} \otimes t_a^* \mathcal{L}^{-1} \otimes t_b^* \mathcal{L}^{-1} \otimes \mathcal{L}$$

is trivial. □

Remark 1.4.16. Tensor by $\mathcal{L}^{-2}$ in the above equation to get

$$t_{a+b}^* \mathcal{L} \otimes \mathcal{L}^{-1} \cong (t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}) \otimes (t_b^* \mathcal{L} \otimes \mathcal{L}^{-1}).$$

This gives a group homomorphism

$$A(k) \to \mathrm{Pic}(A)$$

via

$$a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

for any $\mathcal{L} \in \mathrm{Pic}(A)$.

1.5 The Adventures of BUNTES (Sachi)

1.5.1 In which we are introduced to an important homomorphism, review some concepts and our story begins

Abelian variety X, we know this is a complete group variety, our goal is to give an embedding $X \to \mathbf{P}^N$ for some N. This motivates the study of line bundles.

Last time Ricky proved theorem of cube 1.4.11 and square 1.4.15. For any line bundle L on X, there is a group homomorphism $\Phi_L : X \to \mathrm{Pic}(X)$ via $x \mapsto T_x^* L \otimes L^{-1}$. Be careful T_x^* is $-x$, convention, who knows why.

Example 1.5.1. Let $X = E$ an elliptic curve, $L = L((0))$, $x \mapsto (x) - (0)$, in this case this is in $\mathrm{Pic}^0(E) \cong E \cong \widehat{E}$,

Proposition 1.5.2. *This is translation invariant.*

Proof. Translate by $q \in E$. $(x+q) - (q)$ take p to be the third point on the line with x, q, $(x) + (q) + (p) \cong 3(0)$ and $(x+q) + (p) \cong 2(0)$ subtracting these gives $(x) - (x+q) + (q) \cong (0)$ or $(x) - (0) \cong (x+q) - (q)$. □

What about the converse of this, what can we say about translation invariant line bundles

$$K(L) = \{x \in X : T_x^* L \cong L\}?$$

Proposition 1.5.3. *$K(L)$ is Zariski closed in X.*

Proof. Consider $m^* L \otimes p_2^* L^{-1}$ on $X \times X$, then

$$\{x : \text{this is trivial on } \{x\} \times X\}$$

is closed. See-saw 1.6.6 implies restriction is pullback

$$T_x^* L \otimes L^{-1}$$

so this is $K(L)$. □

1.5.2 In which Pooh discovers our main theorem

Proposition 1.5.4. *Let X be an abelian variety and L a line bundle, $L = L(D)$ then TFAE:*

1. *$H(D) = \{x \in X : T_x^* D = D\}$ is finite.*
2. *$K(L) = \{x \in X : T_x^* L \cong L\}$ is finite.*
3. *$|2D|$ is basepoint free and defines a finite morphism $X \longrightarrow \mathbf{P}^N$.*
4. *L is ample.*

Proof. *3. to 4.*. Is algebraic geometry.

2. to 1.. Follows as being equal is stronger than being linearly equivalent.

4. to 2.. Section 3

3. to 4.. Section 4 □

1.5.3 In which Owl proves the ampleness of L implies finiteness of $K(L)$

4. to 2. Assume L ample and $K(L)$ is infinite. Let Y be the connected component at 0 of $K(L)$, $\dim Y > 0$. Show trivial bundle is ample on Y implies Y is affine, But Y is closed and therefore complete so this is a contradiction. $L|_Y$ ample $[-1]^* L|_Y$ is ample. $L|_Y \otimes [-1]^* L|_Y$ is ample, consider

$$\begin{aligned} d \colon Y &\longrightarrow Y \times Y \\ y &\longmapsto (y, -y) \end{aligned}$$

$m \circ d =$ constant, $d^* m^*(L) = \mathcal{O}_Y$, LHS is $L|_Y \otimes [-1]^* L|_Y$.

1.5.4 In which Rabbbit sets out on a long journey to prove finiteness of $H(D)$ implies $|2D|$ is basepoint free and gives a finite map $X \to \mathbf{P}^N$

Note 1.5.5. $|2D|$ is always basepoint free.

Apply the theorem of the square 1.4.15: $T^*_{x+y}D + D \cong T^*_x D + T^*_y D$, let $y = -x$, $2D \cong T^*_x D + T^*_{-x}D$. ($D$ effective) For any $y \in X$, choose some x s.t. RHS doesn't contain y. $E = 2D$

$$\psi_E \colon X \to \mathbf{P}^N$$

can we make this finite? If ψ_E is not finite then $\psi(C) = \mathrm{pt}$ for some irreducible curve C (Zariski's main theorem). For each divisor in $|E|$ either it contains C or fails to intersect C by changing E if necessary, assume $E \cap C = \emptyset$.

Claim 1.5.6. *$T^*_x E \cap C = \emptyset$ or all of C for all $x \in X$.*

Proof. Intersection numbers are constant. □

Proof. $\mathcal{O}(T^*_x E)|_{\widetilde{C}}$, when $x = 0$ this is trivial so deg $= 0$. So deg $= 0$ for all line bundles. E effective implies $C \cap T^*_x E = \emptyset$ for all x s.t. $\cap$ is not in C. □

Claim 1.5.7. *E is invariant by translation by $x - y$ for $x, y \in C$.*

Proof. If $e \in E$, $T^*_{x-e}(E) \cap C \neq \emptyset$. This is as x is in it, $x - (x - e) = e$, because it is nonempty it's all of C. So y is in it. So $y - (x - e) \in E$. This is also $e - (x - y) \in E$, so E is invariant under T^*_{x-y} □

Now assume $H(E) = \{x \in X : T^*_x E = E\}$ is finite. But if $\psi_E(C) = \mathrm{pt}$ then $T^*_{x-y}(E) = E$ for all $x, y \in C$. So H is not finite, a contradiction. So ψ_E can't collapse a curve so ψ_E is finite.

1.5.5 In which Piglet discovers a corollary

Corollary 1.5.8. *Abelian varieties are projective.*

Proof. Let X be an abelian variety, $U \subseteq X$ be an open affine set, $0 \in U$, $X \setminus U = D_1 \cup \cdots \cup D_t$ irreducible divisors. Let $D = \sum D_i$, then claim: $H(D) = \{x \in X : T^*_x D = D\}$ is finite. If $H \subseteq U$, U affine, then H closed subvariety of an abelian variety, hence complete, so its finite. If $x \in H$ then $-x \in H$. Now claim that if $x \in H$ then T^*_x preserves U, if not let $u \in U$. Suppose $u - x = d$ for some $d \in D$ then $u = d + x$ which is d translated by $-x$ so $d + x \in D$ so $u \in D$. But contradiction, oh no! So T^*_x preserves U, for all $x \in H$, as $0 \in U$, for all $x \in H$ we have $0 - x \in U$ and $0 + x \in U$ so $H \subseteq U$. □

Corollary 1.5.9. *Abelian varieties are divisible. $X[n]$ is finite for $n \geq 1$.*

Proof. $[n] \colon X \to X$ and $X[n]$ is the kernel of this. Note that for $x \in X[n]$

$$[n] \circ T_x = [n]$$

$y \in X$, then $n(y - x) = ny - nx = ny$ so for all $L \in \operatorname{Pic} X$

$$T^*_x([n]^*L) \cong ([n]^*L)$$

which implies

$$K([n]^*L) \supseteq X[n]$$

and we just need to find L s.t. this is finite. X projective implies there exists an ample L. The theorem of the cube 1.4.11 implies

$$[n]^*L \cong L^{\frac{n^2+n}{2}} \otimes L^{\frac{n^2-n}{2}}$$

where both terms on the right are ample, hence the left is also. □

1.5.6 Epilogue: In which we might discuss isogenies

Definition 1.5.10. $f\colon X \to Y$ a morphism of varieties, get a field extension $k(X)/f^*k(Y)$, if $\dim X = \dim Y$ and f is surjective. Then this is a finite field extension and $\deg f$ is $d = [k(X) : f^*k(Y)]$ and $d = \#f^{-1}(y)$ for almost all y.

Definition 1.5.11. A homomorphism of abelian varieties $f\colon X \to Y$ is an **isogeny** if f is surjective with finite kernel.

Corollary 1.5.12. *Degree of $[n]$ is n^{2g}, if n is prime to the characteristic of k, $k = \overline{k}$, $g = \dim X$.*

Proof. Let D be an ample symmetric divisor, e.g.

$$D = D' + [-1]^*D'$$

know $[n]^*D \sim n^2 D$

$$\deg([n]^*(D \cdot \ldots \cdot D)) = ([n]^*D \cdot \ldots \cdot [n]^*D) = (n^2D \cdot \ldots \cdot n^2D) = n^{2g}(D \cdot \ldots \cdot D). \quad \square$$

1.6 Line Bundles and the Dual Abelian Variety (Angus)

Meta-goal Understand line bundles on abelian varieties.

Setup A an abelian variety $/k$.

Last time For L a line bundle on A we get a map

$$\begin{aligned} \phi_L\colon A(K) &\longrightarrow \mathrm{Pic}(A) \\ a &\longmapsto t_a^*L \otimes L^{-1} \end{aligned}$$

where

$$\mathrm{Pic}(A) = \{\text{line bundles on } A\}/\sim.$$

This a is a group homomorphism (by the theorem of the square 1.4.15). We define

$$K(L)(k) = \ker(\phi_L) = \{a \in A(k) : t_a^*L \simeq L\}.$$

Today We are going to package these into a big map

$$\begin{aligned} \phi\colon\ \mathrm{Pic}(A) &\longrightarrow \mathrm{Hom}(A(k), \mathrm{Pic}(A)) \\ L &\longmapsto \phi_L. \end{aligned}$$

Proposition 1.6.1.

1. *ϕ is a group homomorphism*

2. $$\phi_{t_a^*L} = \phi_L$$

Proof. 1.

$$\begin{aligned}\phi_{L\otimes M}(a) &= t_a^*(L\otimes M)\otimes(L\otimes M)^{-1}\\ &= t_a^*L\otimes L^{-1}t_a^*M\otimes M^{-1}\\ &= \phi_L\otimes\phi_M\end{aligned}$$

2.

$$\begin{aligned}\phi_{t_b^*L}(a) &= t_a^*(t_b^*L)\otimes(t_b^*L)^{-1}\\ &= t_{a+b}^*L\otimes(t_b^*L)^{-1}\\ &= t_a^*L\otimes t_b^*L\otimes L^{-1}\otimes(t_b^*L)^{-1}\\ &= \phi_L(a)\end{aligned}$$

by the theorem of the square 1.4.15 □

Definition 1.6.2.

$$\begin{aligned}\mathrm{Pic}^0(A) &= \ker(\phi)\\ &= \{L\in\mathrm{Pic}(A):\phi_L=0\}\\ &= \{L\in\mathrm{Pic}(A):t_a^*L\simeq L\ \forall a\in A(k)\}\\ &= \{\text{translation invariant line bundles}\}/\sim\end{aligned}$$

Goals Study $\mathrm{Pic}^0(A)$, give it an abelian variety structure, solve a moduli problem, demonstrate some duality.

1.6.1 Aside: alternate description of $\mathrm{Pic}^0(A)$

Definition 1.6.3 (Algebraic Equivalence)**.** Two line bundles L_1, L_2 on an abelian variety are **algebraically equivalent** if there exists a variety Y with line bundle L on $A\times Y$ and points $y_1 y_2\in Y$ s.t. $L|_{A\times\{y_1\}}\simeq L_1, L|_{A\times\{y_2\}}\simeq L_2$.

Remark 1.6.4. This looks like homotopy.

Proposition 1.6.5.

$$\mathrm{Pic}^0(A) = \{\textit{line bundles which are alg. equiv to } \mathcal{O}_A\}$$

Proof. [26]. □

1.6.2 See-Saws

Theorem 1.6.6 (See-saw theorem)**.** *Let X, T be varieties X complete, let L be a line bundle on $X\times T$, let $T_1=\{t\in T: L|_{X\times\{t\}}$ is trivial$\}$ then T_1 is closed in T. Further let $p_2\colon X\times T_1\longrightarrow T_1$, then $L|_{X\times T_1}\cong p_2^*M$ for some line bundle M on T_1.*

Remark 1.6.7. In fact $M = p_{2*}L$.

Corollary 1.6.8 (that no one states/only Milne)**.** *Let X, T be as above and let L, M be line bundles on $X\times T$ s.t.*

$$L|_{X\times\{t\}}\cong M|_{X\times\{t\}}\forall t\in T$$

$$L|_{\{t\}\times X}\cong M|_{\{t\}\times X}\textit{ for some } x\in X$$

then $L\cong M$.

1.6.3 Properties of $\mathrm{Pic}^0 A$

Lemma 1.6.9. *$L \in \mathrm{Pic}^0(A)$ and $m, p_1, p_2 \colon A \times A \to A$*

1. $$m^*L \cong p_1^*L \otimes p_2^*L$$
2. *Given $f, g \colon X \to A$*
$$(f+g)^*L \cong f^*L \otimes g^*L$$
3. $$[n]^*L \cong L^{\otimes n}$$
4. $$\phi_L(A(k)) \subseteq \mathrm{Pic}^0(A)$$
for $L \in \mathrm{Pic}(A)$.

Proof. 1.
$$(m^*L \otimes (p_1^*l)^{-1} \otimes (p_2^*l)^{-1})|_{A\times\{a\}} = t_a^*L \otimes L^{-1} = \mathcal{O}_A$$
$$(m^*L \otimes (p_1^*l)^{-1} \otimes (p_2^*l)^{-1})|_{\{a\}\times A} = t_a^*L \otimes L^{-1} = \mathcal{O}_A$$
by see-saw 6 whole thing is trivial on $A \times A$.

2.
$$(f+g)^*L \cong (f\times g)^*m^*L \cong (f\times g)^*(p_1^*L \otimes p_2^*L) \cong f^*L \otimes g^*L$$

3. Induction of 3.

4.
$$\phi_{\phi_L(a)} = \phi_{t_a^*L} \otimes L^{-1} = \phi_{t_a^*L} \otimes L^{-1} = \phi_L \otimes \phi_{L^{-1}} = 0$$
□

Proposition 1.6.10. *If L is nontrivial in $\mathrm{Pic}^0(A)$ then $H^i(A, L) = 0\ \forall i$.*

Proof. If $H^0(A, L) \neq 0$, we would have a nontrivial section s of L then $[-1]^*s$ is a nontrivial section of $[-1]^*L = L^{-1}$. But if both L and L^{-1} have a nontrivial section then $L \cong \mathcal{O}_A$. So since L is nontrivial $H^0(A, L) = 0$. Now assume $H^i(A, L) = 0$ for all $i < j$. Consider
$$A \xrightarrow{\mathrm{id}\times 0} A \times A \xrightarrow{m} A$$
$$a \mapsto (a, 0) \mapsto a$$
this gives
$$H^j(A, L) \to H^j(A \times A, m^*L) \to H^j(A, L)$$
which composes to the identity.
$$H^j(A \times A, m^*L) = H^j(A \times A, p_1^*L \otimes p_2^*L) = \bigoplus_{i=0}^{j} H^i(A, L) \otimes H^{j-i}(A, L)$$
by Künneth. The RHS is 0 by the inductive hypothesis. So the identity on $H^j(A, L)$ factors through 0, hence the group is 0. □

We now think of ϕ_L as a map $\phi_L \colon A(k) \to \mathrm{Pic}^0(A)$ with kernel $K(L)(k)$.

Theorem 1.6.11. *If $K(L)(k)$ is finite then ϕ_L is surjective.*

Proof. Idea is to study
$$\Lambda(L) = m^*L \otimes (p_1^*L)^{-1} \otimes (p_2^*L)^{-1}.$$
□

Given an ample line bundle L on A we now have an isomophism of groups
$$A(k)/K(L)(k) \cong \mathrm{Pic}^0(A)$$
the LHS allows us to put an abelian variety structure on $\mathrm{Pic}^0(A)$.

1.6.4 The Dual Abelian Variety

Theorem 1.6.12. *Let A be an abelian variety and L an ample line bundle on A, then the quotient scheme $A/K(L)$ exists and is an abelian variety of the same dimension as A.*

Proof. (Sketch) (characteristic 0) Cover A by affine opens $U_i = \operatorname{Spec} R_i$ such that for all $a \in A$ the orbit $K(L)a \subseteq U_i$ for some i. We can do this because abelian varieties are projective. Then we say $U_i/K(L) = \operatorname{Spec}(R_i^{K(L)})$ then glue. (details in Mumford, II sec, 6 appendix). Since we are in characteristic 0, the quotient scheme is in fact a variety. □

Definition 1.6.13 (Dual abelian varieties)**.** The **dual abelian variety** is

$$\hat{A} = A/K(L).$$

Remark 1.6.14.

- $$\hat{A}(K) = \operatorname{Pic}^0(A)$$
- We have an isogeny
$$\phi_L : A \to \hat{A}.$$

Theorem 1.6.15. *There is a unique line bundle $\mathcal{P}$ on $A \times \hat{A}$ called the* ***Poincaré bundle*** *such that*

1. $$\mathcal{P}|_{A\times\{x\}} \in \operatorname{Pic}^0(A) \text{ for all } x \in \hat{A}$$
2. $$\mathcal{P}|_{0\times\hat{A}} = 0$$
3. *If Z is a scheme with a line bundle R on $A \times Z$ satisfying 1., 2., there exists a unique*
$$f : Z \to \hat{A}$$
s.t.
$$(\mathrm{id} \times f)^* \mathcal{P} = R.$$

That is $(\hat{A}, \mathcal{P})$ represents the functor

$$Z \mapsto \left\{ L \in \operatorname{Pic}(A \times Z) : {}^{L|_{A\times\{z\}} \in \operatorname{Pic}^0(A) \forall z \in Z}_{L|_{0\times Z} = 0} \right\} /\sim .$$

1.6.5 Dual morphisms

Let $f : A \to B$ be a homomorphism of abelian varieties. Let $\mathcal{P}_A, \mathcal{P}_B$ be the Poincaré bundles on A and B. Consider $M = (F \times \mathrm{id}_{\hat{B}})^* \mathcal{P}_B$ on $A \times \hat{B}$, then

1. $$M|_{A\times\{x\}} \in \operatorname{Pic}^0(A)$$
2. $$M|_{\{0\}\times\hat{B}} = 0$$

thus by the universal property we get a unique morphism

$$\hat{f}\colon \hat{B} \to \hat{A}$$

satisfying

$$(\mathrm{id}_A \times \hat{f})^* \mathcal{P}_A = (f \times \mathrm{id}_{\hat{B}})^* \mathcal{P}_B\,.$$

Definition 1.6.16 (Dual morphisms)**.** $\hat{f}$ as above is called the **dual morphism**.

Remark 1.6.17.

- $$\hat{f}\colon \hat{B} = \mathrm{Pic}^0(B) \to \hat{A}(k) = \mathrm{Pic}^0(A)$$
  $$L \mapsto f^* L$$
- $$[\hat{n_A}] = [n_{\hat{A}}]$$

Consider the Poincaré bundle $\mathcal{P}_{\hat{A}}$ on $\hat{A} \times \hat{\hat{A}}$, now think of $\mathcal{P}_A$ as living on $\hat{A} \times A$. By the universal property of $\mathcal{P}_{\hat{A}}$ get a unique morphism

$$\mathrm{can}_A\colon A \to \hat{\hat{A}}.$$

Theorem 1.6.18. can_A *is an isomorphism.*

Lemma 1.6.19.

$$\phi_{f^*L} = \hat{f} \circ \phi_L \circ f.$$

Proposition 1.6.20. *If $f\colon A \to B$ is an isogeny, then $\hat{f}\colon \hat{B} \to \hat{A}$ is an isogeny. Further if $N = \ker f$, then $\hat{N} = \ker \hat{f}$ is the Cartier dual of N.*

Definition 1.6.21 (Symmetric morphisms, (principal) polarizations)**.** A morphism $f\colon A \to \hat{A}$ is **symmetric** if $f = \hat{f} \circ \mathrm{can}_A$

A **polarization** is a symmetric isogeny $f\colon A \to \hat{A}$ s.t. $f = \phi_L$ for some ample line bundle L on A.

A **principal polarization** is a polarization of degree 1, i.e. an isomorphism.

Remark 1.6.22. Elliptic curves always admit principal polarization.

If one wishes to mimic the theory of elliptic curves, one should study principally polarized abelian varieties.

1.7 Endomorphisms and the Tate module (Berke)

Motivation

$$f\colon\ \mathbf{P}^n \subseteq V_1 \to V_2 \subseteq \mathbf{P}^m,\ V_i = V(I_i)$$
$$P \mapsto \cdots$$

$$f = [f_1 : \cdots : f_m],\ f_i \in \overline{K}(V_1)$$

this feels quite restrictive, an isogeny is even more so, rational, regular, homomorphism, surjective, finite kernel. It feels like there won't be too many but we have multiplication by n etc. so we should ask how many are there that will surprise us? I.e. what is

$$\mathrm{rank}_{\mathbf{Z}} \mathrm{Hom}(A, B) =?$$

1.7.1 Poincaré's complete reducibility theorem

Theorem 1.7.1 (Poincaré's complete reducibility theorem)**.** *Let $B \subseteq A$ then there is $C \subseteq A$ s.t. $B \cap C$ is finite and $B + C = A$. I.e. $B \times C \longrightarrow A$, $(b, c) \mapsto b + c$ is an isogeny.*

Proof. Choose $\mathcal{L}$ ample on A

$$\begin{tikzcd} B \arrow[r, "i"] \arrow[d, "\phi_{i^*\mathcal{L}}"'] & A \arrow[d, "\phi_{\mathcal{L}}", "\sim"'] \\ \hat{B} & \hat{A} \arrow[l, "\hat{i}"'] \end{tikzcd}$$

C is defined to be the connected component of $\phi_{\mathcal{L}}^{-1}(\ker \hat{i})$ in A

$$\dim C = \dim \ker \hat{i} \geq \dim \hat{A} - \dim \hat{B} = \dim A - \dim B.$$

$B \cap C$ finite, $z \in B$, $z \in B \cap \phi_{\mathcal{L}^{-1}}(\ker \hat{i}) = T_z^* \mathcal{L} \otimes \mathcal{L}^{-1}|_B$ is trivial if and only if $z \in K(\mathcal{L}|_B)$. So $\mathcal{L}|_B$ ample implies $K(\mathcal{L}|_B)$ finite and so $B \cap C$ is finite. So $B \times C \longrightarrow A$ has finite kernel and

$$\dim(B \times C) = \dim B + \dim C \geq \dim A$$

and surjective implies its an isogeny. □

Definition 1.7.2 (Simple abelian varieties)**.** A is called **simple** if there does not exists $B \subseteq A$ other than $B = 0, A$.

Corollary 1.7.3.

$$A \sim A_1^{n_1} \times \cdots \times A_k^{n_k}$$

$A_i \nsim A_j$ for $i \neq j$ and A_i simple.

Corollary 1.7.4. *$\alpha \in \mathrm{Hom}(A, B)$ for A, B simple then α is an isogeny or 0.*

Proof. $\alpha(A) \subseteq B$ which implies $\alpha(A) = B$ or 0. The connected component of 0 of $\ker \alpha$ will be an abelian subvariety of A, denote it C If $C = 0$ then $\ker \alpha$ is finite, if $C = A$ then $\alpha = 0$. So α is an isogeny or 0. □

Corollary 1.7.5. *If A, B are simple and $A \nsim B$ then $\mathrm{Hom}(A, B) = 0$.*

Definition 1.7.6.

$$\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbf{Q}.$$

Lemma 1.7.7. *If $\alpha\colon A \longrightarrow B$ is an isogeny, then there exists $\beta\colon B \longrightarrow A$ s.t. $\beta \circ \alpha = n_A$ for some $n \geq 1$.*

Proof. α an isogeny implies $\ker \alpha$ is finite. So there exists n with $n \ker \alpha = 0$. $\ker \alpha \subseteq \ker n_A$

$$\begin{tikzcd} & A \arrow[r, "n_A"] \arrow[dl, "\alpha"'] \arrow[d] & A \\ B \arrow[r, "\sim"'] \arrow[urr, bend right] & A/\ker \alpha \arrow[ur, "\circ"'] \arrow[d, "\exists|\beta"] & \\ & A/n_A & \end{tikzcd}$$

so $\beta \circ \alpha = n_A$, also $\alpha \circ \beta = n_B$. □

Corollary 1.7.8. *A is simple then $\mathrm{End}^0(A)$ is a division ring, $\alpha^{-1} = \beta \otimes \frac{1}{n}$.*

Corollary 1.7.9 (to Poincaré reducibility theorem)**.** *If*

$$A \sim A_1^{n_1} \times \cdots \times A_k^{n_k}$$

then

$$\mathrm{End}^0(A) \simeq \prod \mathrm{End}^0(A_i)^{n_i^2}.$$

Proof.

$$\begin{aligned}
\mathrm{End}(A) \otimes \mathbf{Q} &\simeq \prod_{i,j} \mathrm{Hom}(A_i^{n_i}, A_j^{n_j}) \otimes \mathbf{Q} \\
&\simeq \prod_i \mathrm{End}(A_i)^{n_i^2} \otimes \mathbf{Q} \\
&\simeq \prod_i \mathrm{End}^0(A_i)^{n_i^2}
\end{aligned}$$

□

Theorem 1.7.10 (7.2)**.** *If $\dim A = g$ then $\deg n_A = n^{2g}$.*

Corollary 1.7.11. *$\mathrm{char}\, k \nmid n$ implies $\ker(n_A) \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.*

Proof. If $m|n$ then $|\ker(m_A)| = m^{2g}$, then use structure theorem. □

In particular if we let $A[l^n] = A(k^{\mathrm{sep}})[l^n]$, then $A[l^n] \simeq (\mathbf{Z}/l^n)^{2g}$ Define

$$T_l(A) = \varprojlim_n A[l^n],\ A[l^{n+1}] \xrightarrow{l} A[l]$$

Proposition 1.7.12.

$$T_l \simeq (\mathbf{Z}_l)^{2g}$$

$\alpha \colon A \longrightarrow B$ induces

$$\begin{gathered}
T_l\alpha \colon T_l(A) \longrightarrow T_l(B) \\
(a_1, a_2, \ldots) \longmapsto (\alpha(a_1), \alpha(a_2), \ldots)
\end{gathered}$$

Lemma 1.7.13.

$$\mathrm{Hom}(A, B) \hookrightarrow \mathrm{Hom}(T_l(A), T_l(B))$$

Proof. Let $\alpha \in \mathrm{Hom}(A, B)$ and assume $T_l\alpha = 0$ then

$$\ker(\alpha|_{A_i}) \supseteq A_i[l^n] \forall n$$

for any simple component A_i of A so $\alpha = 0$ on each A_i and hence $\alpha = 0$ on A. □

Corollary 1.7.14. *$\mathrm{Hom}(A, B)$ is torsion free.*

Recall we are interested in knowing about $\mathrm{rank}_{\mathbf{Z}} \mathrm{Hom}(A, B)$ =?, can we bound this? If we could show that

$$\mathrm{Hom}(A, B) \otimes \mathbf{Z}_l \hookrightarrow \mathrm{Hom}(T_l(A), T_l(B))$$

we could conclude, so:

$$\begin{tikzcd}
\mathrm{Hom}(A, B) \otimes \mathbf{Z}_l \arrow[r, hook] \arrow[d, "\sim"'] & \mathrm{Hom}(T_lA, T_lB) \arrow[d, "\sim"'] \\
\prod_{i,j} (\mathrm{Hom}(A_i, B_j) \otimes \mathbf{Z}_l) \arrow[r, hook] & \prod_{i,j} \mathrm{Hom}(T_lA_i, T_lB_j)
\end{tikzcd}$$

$A_i + B_j = 0$, $A_i \sim B_j$ $\mathrm{Hom}(A_i, B_j) \hookrightarrow \mathrm{End}(A_i)$. Assume $A = B$ and A simple, then $\mathrm{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \mathrm{End}(T_l(A))$.

Definition 1.7.15. V/k then $f\colon V \to k$ is called a (homogenous) polynomial function of degree d if $\forall\{v_1, \cdots, v_m\} \subseteq V$ linearly independent.

$$f(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m)$$

is given by a homogenous polynomial of degree d in λ_i i.e.

$$f(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m) = P(\lambda_1, \ldots, \lambda_m)$$

for some $P \in k[X_m]$ homogenous of degree d.

$$\deg\colon \operatorname{End}(A) \to \mathbf{Z}$$

α an isogeny iff $\deg \alpha$, α not an isogeny iff 0.

Theorem 1.7.16. $\deg$ *uniquely extends to a polynomial function of degree* $2g$ *on* $\operatorname{End}^0(A) \to \mathbf{Q}$.

Proof. (of above continued)

$$\operatorname{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \operatorname{End}(T_l(A))$$

for A simple iff for any finitely generated $M \subseteq \operatorname{End}(A)$

$$M \otimes \mathbf{Z}_l \hookrightarrow \operatorname{End}(T_l(A))$$

Claim:

$$M^{\mathrm{div}} = \{f \in \operatorname{End}(A) : nf \in M \text{ for some } n \geq 1\}$$

is finitely generated.

Proof: $M^{\mathrm{div}} = (M \otimes \mathbf{Q}) \cap \operatorname{End}(A)$ $\deg\colon M \otimes \mathbf{Q} \to \mathbf{Q}$ is a polynomial so it is continuous.

$$U = \{\phi \in M \otimes \mathbf{Q} : \deg \phi < 1\}$$

is open in $M \otimes \mathbf{Q}$ but $U \cap M^{\mathrm{div}} = 0$ so M^{div} is a discrete subgroup of the finite dimensional $\mathbf{Q}$-vector space $M \otimes \mathbf{Q}$ so M^{div} is finitely generated. $M \hookrightarrow M^{\mathrm{div}}$ so $M \otimes \mathbf{Z}_l \hookrightarrow M^{\mathrm{div}} \otimes \mathbf{Z}_l$ so we may assume $M = M^{\mathrm{div}}$.

Let $f_1, \ldots, f_r$ be a $\mathbf{Z}$-basis for M and suppose that $\sum a_i T_l(f_i) = 0$ for some $a_i \in \mathbf{Z}_l$ not all 0. We can assume not all a_i are divisible by l. Choose $a_i' \in \mathbf{Z}$ s.t. $a_i' = a_i \pmod{l}$

$$f = \sum a_i' f_i \in \operatorname{End}(A)$$

we then have

$$f = \sum a_i' T_l f_i$$

is 0 on the first coordinate of T_l. So $A[l] \subseteq \ker f$ so there exists g with $f = lg$ $f \in M$ implies $g \in M^{\mathrm{div}} = M$ so $g = \sum b_i f_i$ and $f = \sum l b_i f = \sum a_i f_i$ hence $l \mid a_i$ for all i a contradiction. So $\operatorname{End}(A) \otimes \mathbf{Z}_l \hookrightarrow \operatorname{End}(T_l(A))$.

Therefore

$$\operatorname{Hom}(A, B) \otimes \mathbf{Z}_l \hookrightarrow \operatorname{Hom}(T_l(A), T_l(B))$$

$$\operatorname{rank}_{\mathbf{Z}} \operatorname{Hom}(A, B) \leq 4 \dim A \dim B.$$

□

1.8 Polarizations and Étale cohomology (Alex)

Plan: polarizations, a little cohomological warmup and a cool finiteness result. Étale cohomology.

1.8.1 Polarizations

Definition 1.8.1 (Polarizations)**.** A **polarization** of an abelian variety A/k is an isogeny

$$\lambda\colon A \to \hat{A}$$

such that

$$\lambda \simeq_{\overline{k}} \lambda_{\mathcal{L}} : a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

for an ample invertible sheaf $\mathcal{L}$ on $A_{\overline{k}}$.

We then have a notion of degree, polarizations of degree 1 (i.e. isomorphisms $A \to \hat{A}$) are called **principal polarizations**.

Remark 1.8.2. This is in fact equivalent to the previous definition 1.6.21 see [33].

Natural questions: what does the line bundle $\mathcal{L}$ tell us about the polarization? Can we tell principality?

To answer this we must (rapidly) recall (Zariski) sheaf cohomology. But this will help us in the next section too.

A line bundle (or indeed any sheaf) defines for us for any open subset $U \hookrightarrow X$ an abelian group of sections $\mathcal{L}(U)$.

However taking (global) sections doesn't play well exact sequences!

Example 1.8.3 (Classic example)**.** Let $X = \mathbf{C}^*$ and consider

$$0 \to \mathbf{Z} \hookrightarrow \mathcal{O}_X \xrightarrow{e^{2\pi i -}} \mathcal{O}_X^* \to 0$$

but

$$0 \to \mathbf{Z} \to \mathcal{O}_X(X) \to \mathcal{O}_X^*(X)$$

is not surjective on the right, for example $f(z) = z$ is a nowhere vanishing meromorphic function on X but its not exp of anything. Upshot: maps of sheaves can be surjective (by being so locally) but not globally.

To understand/control this phenomenon we introduce $H^1(X, \mathcal{F})$ fitting into the above and so on.

Explicitly: for a sheaf $\mathcal{F}$ we fix an injective resolution

$$0 \to \mathcal{F} \to \mathcal{I}_0 \to \mathcal{I}_1 \to \cdots$$

which we then take global sections of to get a chain complex

$$0 \to \Gamma(X, \mathcal{F}) \to \Gamma(X, \mathcal{I}_0) \to \Gamma(X, \mathcal{I}_1) \to \cdots$$

and we truncate and take cohomology of this to measure "failure of exactness"

$$H^0(X, \mathcal{F}), H^1(X, \mathcal{F}), H^2(X, \mathcal{F}), \ldots.$$

Definition 1.8.4 (Euler-Poincaré characteristic)**.** Define the **Euler-Poincaré characteristic** of a line bundle $\mathcal{L}$ to be

$$\chi(\mathcal{L}) = \sum (-1)^i \dim_k H^i(A, \mathcal{L}).$$

Theorem 1.8.5 (Riemann-Roch)**.** *Let A be an abelian variety of dimension g then*

1. *The degree of $\lambda_{\mathcal{L}}$ is $\chi(\mathcal{L})^2$.*
2. *If $\mathcal{L} = \mathcal{L}(D)$ then $\chi(\mathcal{L}) = (D^g)/g!$, this is the g-fold self intersection number of D.*

Theorem 1.8.6 (Vanishing)**.** *If $\#K(\mathcal{L}) < \infty$ then there is a unique integer $0 \le i(\mathcal{L}) \le g$ with $H^i(A, \mathcal{L}) \neq 0$ and $H^p(A, \mathcal{L}) = 0$ for all $p \neq i$. Moreover $i(\mathcal{L}^{-1}) = g - i(\mathcal{L})$.*

Recall Subsection 1.5.3: So for ample $\mathcal{L}$ we have $K(\mathcal{L})$ finite, so the vanishing theorem applies. Additionally for very ample $\mathcal{L}$ we know $H^0(A, \mathcal{L}) \neq 0$ so in this case we get vanishing of higher cohomology.

Theorem 1.8.7 (Finiteness)**.** *Let k be a finite field, and $g, d \ge 1$ integers. Up to isomorphism there are only finitely many abelian varieties A/k of dimension g and with a polarization of degree d^2.*

Proof. (Super sketch)

Over a finite field implies there is an ample $\mathcal{L}$ with $\lambda_{\mathcal{L}}$ a polarization of degree d^2, then using above $\chi(\mathcal{L}^3) = 3^g d$ and $\mathcal{L}^3$ is very ample hence $\dim H^0(A, \mathcal{L}^3) = 3^g d$ so we get an embedding into $\mathbf{P}^{3^g d - 1}$.

The degree of A in $\mathbf{P}^{3^g d-1}$ is $((3D)^g) = 3^g d(g!)$. It is determined by its Chow form, which by these formulae has some (large) bounded degree, as we are over a finite field however there are only finitely many such. ◻

1.8.2 Étale Cohomology of Abelian Varieties

See [24] or [32].

Recall for abelian varieties over $A/\mathbf{C}$ we considered singular cohomology of the complex points $A(\mathbf{C})$. Indeed this theory was strongly connected to the lattice Λ defining $A(\mathbf{C})$.

We saw that in fact $\pi_1(A, 0) = \pi^{-1}(0) = \Lambda \subseteq V$ which was the universal covering space of $A(\mathbf{C})$. We want to emulate this over a general field.

We want to allow multiplication by n to define finite covers for our abelian varieties as they did before.

Problem: Zariski topology is too coarse: we can't find an open U set around $0 \in A$ such that $[2]\colon U \to A$ is an isomorphism onto its image. Isogenies are not local isomorphisms for the Zariski topology.

How on earth do we "allow" maps which are clearly not local isomorphisms to become such? First what do we mean by local isomorphism?

$$\begin{tikzcd} f^{-1}(U) \arrow[r, "\sim"] \arrow[d] & U \arrow[d, hook, "i"] \\ X \arrow[r, "f"'] & Y \end{tikzcd} .$$

There exists an open subset U such that the base change $X \times_Y U$ is isomorphic with $\coprod U$ of several copies of U in a compatible way with the map to U.

So let's cheat, the best isomorphism is the identity map

$$\begin{tikzcd} X \arrow[r, "\sim"] \arrow[d] & X \arrow[d, "f"] \\ X \arrow[r, "f"'] & Y \end{tikzcd}$$

if we define an "open set" U to be a morphism $X \to Y$ with the properties we want, then all such become local isomorphisms.

By taking our *topology* to be given by some maps we decide are decent covering maps we can circumvent these difficulties.

What is the correct class of morphisms to take here, we feel like our $[n]$

maps should count. Taking inspiration from differential geometry perhaps, we are led to the notion of a local diffeomorphism, an étale map.

Definition 1.8.8. Let X, Y be nonsingular varieties over $k = \overline{k}$. Then $f\colon X \to Y$ is étale at a point $P \in X$ if

$$\mathrm{d}f\colon \operatorname{Tgt}_P(X) \to \operatorname{Tgt}_{f(P)}(Y)$$

is an isomorphism.

Proposition 1.8.9. *Let $f\colon \mathbf{A}^m \to \mathbf{A}^m$ then f is étale at $(a_1, \cdots, a_m)$ iff*

$$\left(\frac{\partial(X_i \circ f)}{\partial Y_j}|_{(a_k)}\right)$$

is nonsingular.

Example 1.8.10 (A non-étale map)**.** Consider the map

$$\mathbf{A}^2 \to \mathbf{A}^2$$
$$(x, y) \mapsto (x^3, x^2 + y)$$

we can see that the image of $y = 0$ is the nodal cubic ($Y^3 = X^2$), which is messed up (singular) at $(0, 0)$. The jacobian is

$$\begin{pmatrix} 3x^2 & 0 \\ 2x & 1 \end{pmatrix}$$

so this matrix is singular exactly when $x = 0$ (unless characteristic 3). So the map is not étale at these points.

Proposition 1.8.11. *The maps $[n]$ are étale on an abelian variety A/k for all* char $k \nmid n$

Proof. Key point $\mathrm{d}(\alpha + \beta)_0 = (\mathrm{d}\alpha)_0 + (\mathrm{d}\beta)_0$. So the map on tangent spaces is simply multiplication by n. □

Definition 1.8.12 (Étale morphisms)**.** A morphism $f\colon X \to Y$ of schemes is **étale** if it is flat and unramified.

Flatness for finite morphisms of varieties is equivalent to each fibre $f^{-1}(t)$ being of equal cardinality, counting multiplicities.

All isogenies are finite and flat.

Definition 1.8.13. Let FEt/X be the category of finite étale maps $\pi\colon Y \to X$ (i.e. finite étale coverings of X).

Then after picking a basepoint $x \in X$ we can map

$$F\colon \mathrm{FEt}/X \to \mathrm{Set}$$
$$\pi \mapsto \operatorname{Hom}_X(x, Y) \approx \pi^{-1}(x).$$

This is in fact pro-representable, i.e. there exists a system

$$\tilde{X} = (X_i)_{i \in I}$$

with

$$F(Y) = \operatorname{Hom}(\tilde{X}, Y) = \varinjlim_i \operatorname{Hom}(X_i, Y).$$

We then define

$$\pi_1(X, x) = \operatorname{Aut}_X(\tilde{X}) = \varprojlim_i \operatorname{Aut}_X(X_i).$$

So we need to understand étale covers of abelian varieties. Following [33]:

Proposition 1.8.14 (surprising proposition)**.** *Let X be a complete variety over a field k with $e \in X(k)$ and $m\colon X \times X \to X$ s.t. $m(e,x) = m(x,e) = x$ for all $x \in X$. Then (X, m, e) is an abelian variety.*

Proof. (Sketch)

Let

$$\tau\colon X \times X \to X \times X$$

$$\tau(x,y) = (xy, y)$$

so $\tau^{-1}(e,e) = (e,e)$. Some exercise in Hartshorne implies $\operatorname{im}\tau$ has dimension $2\dim X$.

Reduce to algebraically closed case.

Let

$$\tau^{-1}(\{e\} \times X) = \{(x,y) : xy = e\} = \Gamma \subseteq X \times X$$

as τ is surjective we get $p_2\colon \Gamma \to X$ is also so pick an irreducible $\Gamma_1 \subseteq \Gamma$ with $p_2(\Gamma_1) = X$. This also implies $p_1(\Gamma_1) = X$.

Let

$$f\colon \Gamma_1 \times X \times X \to X$$

$$f((x,y),z,w) = x((yz)w)$$

then

$$f(\Gamma_1 \times \{e\} \times \{e\}) = \{eee\} = \{e\}$$

so a version of rigidity 1.1.11 gives

$$x((yz)w) = zw \ \forall (x,y) \in \Gamma_1,\ z,w \in X$$

So letting $w = e$ we get

$$x(yz) = z.$$

Fix $y \in X(k)$, and then by surjectivity we can find $x, z \in X(k)$ with $(x,y) \in \Gamma_1 \ni (y,z)$. So we get

$$x = x(yz) = ze = z$$

and so y has both a left and right inverse. We then multiply above by y to get

$$y(zw) = y(x((yz)w)) = (yz)w$$

so $X(k)$ is associative. □

Theorem 1.8.15 (Lang-Serre)**.** *Let X/k be an abelian variety and Y/k a variety with $e_Y \in Y(k)$ s.t. $f\colon Y \to X$ is an étale covering where $f(e_Y) = e_X$. Then Y can be given the structure of an abelian variety so that f is a separable isogeny.*

Proof. Must construct a group law on Y:

Take the graph of $m\colon X \times X \to X$

$$\Gamma_X \subseteq X \times X \times X$$

and pullback along $f \times f \times f$ to

$$\Gamma'_Y \subseteq Y \times Y \times Y$$

fix the connected component Γ_Y containing (e_Y, e_Y, e_Y).

Call the projections from Γ_Y q_I. Now we must show that $q_{12}\colon \Gamma_Y \to Y \times Y$ is an isomorphism, then $m_Y\colon Y \times Y \to Y$ can be defined as $q_3 \circ q_{12}^{-1}$. q_{12} has sections s_1, s_2 over $\{e_Y\} \times Y$, $Y \times \{e_Y\}$ respectively given by $s_1(e_Y, y) = (e_Y, y, y)$

and $s_2(y, e_y, y) = (y, e_y, y)$. So m_Y satisfies the conditions of the surprising proposition.

$$\begin{tikzcd} \Gamma_Y \arrow[r] \arrow[d, "q_{12}"'] & \Gamma_X \arrow[d, "p_{12}"] \\ Y \times Y \arrow[r, "f \times f"'] & X \times X \end{tikzcd}$$

the horizontal maps are étale coverings and the rightmost an isomorphism so q_{12} is an étale covering. The projection $p_2 \circ q_{12} = q_2 \colon \Gamma_Y \to Y$ is smooth proper. Fact: all fibres of q_2 are irreducible. So $Z = q_2^{-1}(e_Y) = q_{12}^{-1}(Y \times \{e_Y\})$ is irreducible. Moreover q_{12} restricts to an étale covering $Z \to Y = Y \times \{e_Y\}$ of the same degree, but s_2 is a section of this covering, hence it is an isomorphism. Hence q_{12} has degree 1 and is therefore an isomorphism as required. □

So we have some control over the finite étale maps, what does the covering space look like? Last week we saw that for an isogeny $\alpha \colon B \to A$ we could find $\beta \colon A \to B$ with $\beta \circ \alpha = [n] \colon A \to A$. This means we can take our universal covering space to be

$$(A)_{i \in I}$$

with multiplication by n maps.

So we find

$$\pi_1^{\text{et}}(A, 0) = \varprojlim_n \operatorname{Aut}_A(A \xrightarrow{[n]} A) = \varprojlim_n A[n].$$

Theorem 1.8.16.

$$H^1_{\text{et}}(A, \mathbf{Z}_l) = \operatorname{Hom}(\pi_1(A, 0), \mathbf{Z}_l) = \operatorname{Hom}(T_l, \mathbf{Z}_l)$$

Theorem 1.8.17.

$$H^r(A_{\text{et}}, \mathbf{Z}_l) = \bigwedge^r H^1(A_{\text{et}}, \mathbf{Z}_l)$$

Note that Milne gives a combined proof of the above two statements, this relies on some theorems on Hopf algebras such as [8].

1.9 Weil pairings (Maria)

1.9.1 Weil pairings on elliptic curves

Start with elliptic curves, later repeat for abelian varieties. E/k an elliptic curve, ≥ 2, if $\operatorname{char}(k) = p > 0$ $(m, p) = 1$. The Weil e_m-pairing $e_m \colon E[m] \times E[m] \to \mu_m$ is defined as follows Fix $T \in E[m]$ then $f \in \bar{k}(E)$ s.t. $\operatorname{div}(f) = m(T) - m(0)$. Fix $T' \in E$ with $mT' = T$ and $g \in \bar{k}(E)$ s.t. $\operatorname{div}(g) = [m]^*(T) = [m]^*(0) = \sum_{R \in E[m]}(T + R) - (R)$. Check $\operatorname{div}(f \circ [m]) = \operatorname{div}(g^m)$, hence

$$f \circ [m] = c g^m$$

so can assume $f \circ [m] = g^m$. For $s \in E[m]$, $x \in E$:

$$g(x + s) = f([m]x + [m]s) = f([m]x) = g(x)^m$$

$$\frac{g(\cdot + s)^m}{g(\cdot)} \colon E \to \mathbf{P}^1$$

is then a constant function, since not surjective. So we define

$$\begin{aligned} e_m\colon E[m]\times E[m] &\to \mu_m \\ (s,t) &\mapsto \frac{g_t(x+s)}{g_t(x)} \end{aligned}$$

will state many properties later, but for now. e_m is compatible:

$$e_{mm'}(a,a')^{m'} = e_m(m'a, m'a')\ \forall a,a' \in E[mm']$$

so for any $l \neq \mathrm{char}(k)$ prime we can combine e_{l^n}-pairings into an l-adic Weil pairing on $T_l E$

$$e\colon T_l E \times T_l E \to T_l \mu = \mathbf{Z}_l(1)$$

1.9.2 Weil pairings on abelian varieties

Story will be broadly similar to before but we must use the dual, which doesn't appear in the presentation for elliptic curves.

Let A/k be an abelian variety $k = \overline{k}$. We construct a Weil e_m-pairing

$$\begin{aligned} e_m\colon A[m]\times A^\vee[m] &\to \mu_m \\ (a,a') &\mapsto \frac{g\circ t_a(x)}{g(x)} = \frac{g(x+a)}{g(x)} \end{aligned}$$

Fix $a \in A[m]$, $a' \in A^\vee[m]$ say a' corresponds to $\mathcal{L}$ and a divisor D then $\mathcal{L}^m$ and $m_A^*\mathcal{L}$ are trivial so $\exists f,g \in k(A)$ s.t.

$$\mathrm{div}(f) = mD$$

$$\mathrm{div}(g) = m_A^* D$$

again we have

$$\begin{aligned} \mathrm{div}(f\circ m_A) &= \mathrm{div}(g^m) \\ g(x+a)^m &= g(x)^m \end{aligned}$$

Proposition 1.9.1. *The Weil e_m-pairing has the following properties*

1. *e_m is bilinear*
$$\begin{aligned} e_m(a_1+a_2,a') &= e_m(a_1,a')e_m(a_2,a') \\ e_m(a,a_1'+a_2') &= e_m(a,a_1')e_m(a,a_2') \end{aligned}$$

2. *e_m is non-degenerate: if $e_m(a,a') = 1 \forall a \in A[m]$ then $a' = 0$ (and likewise for the reverse).*

3. *e_m is Galois-invariant... but we assume $\overline{k} = k$ so we ignore this.*

4. *e_m is compatible*
$$e_{mm'}(a,a')^{m'} = e_m(m'a, m'a')\ \forall a \in A[mm'], a' \in A^\vee[mm']$$
$(mm', \mathrm{char}\, k) = 1$

Corollary 1.9.2. *There exists a bilinear non-degenerate (Galois invariant) pairing*

$$e_l = e\colon T_l A \times T_l A^\vee \to T_l \mu$$

$$((a_n),(a_n')) \mapsto (e_{l^n}(a, a_n'))$$

For a homomorphism $\lambda\colon A \to A^\vee$ we define

$$e_m^\lambda\colon A[m] \times A[m] \to \mu_m$$
$$(a, a') \mapsto e_m(a, \lambda(a'))$$
$$e_m\colon T_l A \times T_l A \to T_l \mu$$
$$(a, a') \mapsto e_m(a, \lambda(a')).$$

Proposition 1.9.3. *For a homomorphism $\alpha\colon A \to B$*

1.
$$e(a, \alpha^\vee(b)) = e(\alpha(a), b) \forall a \in T_l A,\ b \in T_l B$$

2.
$$e^{\alpha^\vee \lambda \alpha}(a, a') = e^\lambda(\alpha(a), \alpha(a'))$$
for $a, a' \in T_l(A)$, $\lambda \in \mathrm{Hom}(B, B^\vee)$.

3.
$$e^{\alpha^* \mathcal{L}}(a, a') = e^{\mathcal{L}}(\alpha(a), \alpha(a'))$$
$a, a' \in T_l A$ $\mathcal{L} \in \mathrm{Pic}(B)$.

4.
$$\mathrm{Pic}\, A \to \mathrm{Hom}(\bigwedge^2 T_l A, T_l \mu)$$
$$\mathcal{L} \mapsto e^{\mathcal{L}}$$
is a homomorphism (in particular $e^{\mathcal{L}}$ is skew-symmetric).

Proof.

1. $a = (a_n) \in T_l A$ $b \in (b_n) \in T_l B^\vee$ fix a divisor D on B representing b_n and $g \in k(B)$ s.t. $\mathrm{div}(h) = (l_B^n)^* D$. Then $\alpha^* D$ represents $\alpha^\vee(b_n)$ so:
$$\mathrm{div}(g \circ \alpha) = \alpha^* \mathrm{div}(g) = \alpha^*(l_B^n)^* D = (l_A^n)^* \alpha^* D.$$
So

2.
$$e^{\alpha^\vee \lambda \alpha}(a, a') = e(a, \alpha^\vee \lambda \alpha(a')) = e(\alpha(a), \lambda(\alpha(a'))) = e^\lambda(\alpha(a), \alpha(a')).$$

3.
$$\lambda_{\alpha^* \mathcal{L}} = \alpha^\vee \lambda_{\mathcal{L}} \alpha$$

4. Follows from $\lambda_{\mathcal{L} \otimes \mathcal{L}'} = \lambda_{\mathcal{L}} + \lambda_{\mathcal{L}'}$.

□

Example 1.9.4 (Computation over $\mathbf{C}$). $A/\mathbf{C}$ be an abelian variety

$$0 \to \mathbf{Z} \to \mathcal{O}_A \xrightarrow{e^{2\pi i(\cdot)}} \mathcal{O}^\times \to 0$$

induces

$$H^1(A(\mathbf{C}), \mathbf{Z}) \to H^1(A(\mathbf{C}), \mathcal{O}) \to H^1(A(\mathbf{C}), \mathcal{O}^\times) \simeq \mathrm{Pic}\, A \to H^2(A(\mathbf{C}), \mathbf{Z})$$

and

$$H^1(A(\mathbf{C}), \mathcal{O})/H^1(A(\mathbf{C}), \mathbf{Z}) \simeq A^\vee(\mathbf{C}) = \mathrm{Pic}^0(A)$$

so we get an exact sequence

$$0 \to \mathrm{NS}(A) \to H^2(A(\mathbf{C}), \mathbf{Z}) \to H^2(A(\mathbf{C}), \mathcal{O}_A)$$

$$\lambda \mapsto E_\lambda$$

then we can regard E_λ as a skew-symmetric 2-form on $H_1(A(\mathbf{C}), \mathbf{Z})$. Mumford pg. 237 proves

$$\begin{tikzcd} H_1(A(\mathbf{C}), \mathbf{Z}) \times H_1(A(\mathbf{C}), \mathbf{Z}) \arrow[r] \arrow[d] & \mathbf{Z} \ni m \arrow[d] \\ T_l \times T_l \arrow[r] & T_l\mu \ni \zeta^m \end{tikzcd}$$

commutes with - sign so $e^\lambda(a, a') = \zeta^{-E(a,a')}$

1.9.3 Results about polarizations

$k = \overline{k}$ $p = \mathrm{char}(k) \geq 0$.

Theorem 1.9.5 (13.4). *Let $\alpha: A \to B$ be an isogeny of degree prime to $\mathrm{char}\, k$ and $\lambda \in \mathrm{NS}(A)$ then $\lambda = \alpha^*\lambda'$ for $\lambda' \in \mathrm{NS}(B)$ $\iff$ $\forall l | \deg(\alpha)$ l prime there exists a skew-symmetric form $f: T_lB \times T_lB \to T_l\mu$ s.t. $e^\lambda(a, a') = f(\alpha(a), \alpha(a'))$ for all $a, a' \in T_l(A)$.*

Proof. Milne 1986 16.4 □

Corollary 1.9.6 (13.5). *$l \neq \mathrm{char}(k)$ $\lambda \in \mathrm{NS}(A)$ is divisible by l^n $\iff$ e^λ is divisible by l^n in $\mathrm{Hom}(\bigwedge^2 T_lA, T_l\mu)$.*

Proof. Apply theorem 13.4 with $\alpha = l^n$. □

Lemma 1.9.7 (13.7). *Let $\mathcal{P}$ be the Poincaré sheaf on $A \times A^\vee$ then*

$$e^{\mathcal{P}}((a, b), (a', b')) = \frac{e(a, b')}{e(a', b)}$$

for all $a, a' \in T_lA$, $b, b' \in T_lA^\vee$.

Proof. Milne 1986 16.7. Use:

$$(1 + \lambda_{\mathcal{L}})^*\mathcal{P} \cong m^*\mathcal{L} \otimes p^*\mathcal{L}^{-1} \otimes q^*\mathcal{L}^{-1}$$ □

Proposition 1.9.8 (13.6). *Assume $\mathrm{char}\, k \neq l, 2$ then a homomorphism $\lambda: A \to A^\vee$ is $\lambda = \lambda_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}\, A$ iff e^λ is skew-symmetric.*

Proof. Clear.

e^λ is skew-symmetric, define $\mathcal{L} = (1 \times \lambda)^*\mathcal{P}$ then $\forall a, a' \in T_lA$

$$e(a, \lambda_{\mathcal{L}}(a')) = e^{\mathcal{L}}(a, a') = e^{(1\times\lambda)^*\mathcal{P}}(a, a') = e^{\mathcal{P}}((a, \lambda(a)), (a', \lambda(a'))) = \frac{e(a, \lambda(a'))}{e(a', \lambda(a))}$$

$$= \frac{e^\lambda(a, a')}{e^\lambda(a', a)} = (e^\lambda(a, a'))^2 = e(a, 2\lambda(a'))$$

so $2\lambda = \lambda_{\mathcal{L}}$. So by corollary 13.5 $\lambda_{\mathcal{L}} = 2\lambda_{\mathcal{L}'}$ for some $\mathcal{L}' \in \mathrm{Pic}\, A$ so $\lambda = \lambda_{\mathcal{L}'}$. □

Definition 1.9.9. For a polarization $\lambda\colon A \to A^\vee$ define

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

$$(a,a') \mapsto e_m(a,\lambda(b))$$

where m kills $\ker(\lambda)$ and $b \in A$ s.t.$mb = a'$.

Check: this is well defined.

Note 1.9.10. e^λ is skew-symmetric.

Proposition 1.9.11 (13.8)**.** *$\alpha\colon A \to B$ is an isogeny of degree prime to p, $\lambda\colon A \to A^\vee$ polarization then $\lambda = \alpha^*\lambda'$, $\lambda'\colon B \to B^\vee$ polarization iff*

$$\ker(\alpha) \subset \ker\lambda$$

$$e^\lambda \textit{ is trivial on } \ker(\alpha)\times\ker(\alpha)$$

Note 1.9.12. If $\lambda = \alpha^*\lambda'$ then

$$\deg(\lambda) = \deg(\lambda')\deg(\alpha)^2.$$

Corollary 1.9.13 (13.10)**.** *A an abelian variety, $\lambda\colon A \to A^\vee$ is a polarization with $(\deg(\lambda),p) = 1$ then A is isogenous to a principally polarized abelian variety.*

Proof. Fix $l|\deg(\lambda)$ prime. Choose a subgroup $N \subseteq \ker\lambda$ of order l let $\alpha\colon A \to A/N = B$ N is cyclic and e^λ is skew-symmetric so e^λ is trivial on $N\times N$ so B has a polarization of degree $\deg(\lambda)/l^2$ by 13.8. ◻

Corollary 1.9.14 (13.11)**.** *Let λ be a polarization of A s.t. $\ker(\lambda) \subseteq A[m]$ for some $(m,p) = 1$. If $\exists\alpha\colon A \to A$ s.t. $\alpha(\ker(\lambda)) \subseteq \ker(\lambda)$ and $\alpha^\vee\lambda\alpha = -\lambda$ on $A[m^2]$ then $A\times A^\vee$ is principally polarized.*

Theorem 1.9.15 (13.12 (Zarhin's trick))**.** *For any abelian variety A $(A\times A^\vee)^4$ is principally polarized.*

Proof. Fix $\lambda\colon A \to A^\vee$ polarization, assume $\ker(\lambda) \subseteq A[m]$ $(m,p) = 1$ there exists $a,b,c,d \in \mathbf{Z}$ s.t. $a^2+b^2+c^2+d^2 = m^2-1 = -1 \pmod{m^2}$ then

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

works. ◻

Corollary 1.9.16 (13.13)**.** *Let k be a finite field, then for each $g \in \mathbf{Z}$ there exist only finitely many isomorphism classes of abelian varieties of dimension g over k.*

Proof. A/k an abelian variety of dimension g, so $(A\times A^\vee)^4$ is an abelian variety of dimension $8g$ with a principal polarization so using theorem 11.2 there are finitely many (up to $\simeq$) of those. Also $(A\times A^\vee)^4$ has finitely many direct factors (theorem 15.3). ◻

1.10 The Rosati involution (Alex)

Let A/k be an abelian variety and $f \in \mathrm{End}(A)$. Via pullback we get $\hat{f} \in \mathrm{End}(\hat{A})$, in the case where A is polarized i.e. we have an isogeny $\phi\colon A \to \hat{A}$ we might wonder what the relation is between $\hat{f}$ and f. E.g. $\hat{\mathrm{id}} = \mathrm{id}$ but here we have $\hat{\phi}\mathrm{id}\phi = [\deg\phi]$, this is a little ugly, depends on the degree of our polarization. If we work with $\mathrm{Hom}^0(A,B) = \mathrm{Hom}(A,B)\otimes\mathbf{Q}$ rather than $\mathrm{Hom}(A,B)$ we have a bona fide inverse ϕ^{-1} of an isogeny ϕ. So now we can ask precisely, what is the relationship of the endomorphism $f^\dagger = \phi^{-1}\circ\hat{f}\circ\phi \in \mathrm{End}^0(A)$ with f?

What sort of properties does this map $f \mapsto f^\dagger$ have?

Definition 1.10.1 (The Rosati involution)**.** The map $\phi^{-1}\hat{-}\phi = -^\dagger\colon \mathrm{End}^0(A) \to \mathrm{End}^0(A)$ is called the **Rosati involution**.

Proposition 1.10.2. $-^\dagger$ *is* $\mathbf{Q}$*-linear*

Proposition 1.10.3. $-^\dagger$ *is an anti-homomorphism i.e.*

$$(fg)^\dagger = g^\dagger f^\dagger$$

Proposition 1.10.4. *Recall the l-adic Weil pairing for $l \neq \mathrm{char}(k)$, fix $a, a' \in V_lA = T_lA\otimes\mathbf{Q}$, then*

$$e_l^\phi(fa,a') = e_l^\phi(a, f^\dagger a').$$

Proof.

$$e_l^\phi(fa,a') = e_l(fa,\phi a') = e_l(a,\hat{f}\phi a') = e_l(a,\phi\phi^{-1}\hat{f}\phi a') = e_l^\phi(a,f^\dagger a') \qquad \square$$

Proposition 1.10.5. $-^\dagger$ *is an involution, i.e.*

$$\alpha^{\dagger\dagger} = \alpha.$$

Proof. We apply the previous proposition and skew-symmetry of a polarization (over some extension)

$$e_l^\lambda(\alpha a,a') = e_l^\lambda(a,\alpha^\dagger a') = e_l^\lambda(\alpha^{\dagger\dagger}a,a')$$

for all $a, a' \in V_lA$. □

So we have a weird algebra with a weird operation, what can we do? Perhaps inspired by the killing form of a lie algebra:

We can form a bilinear form using the trace

$$\mathrm{End}^0(A)\times\mathrm{End}^0(A) \to \mathbf{Q}$$

$$(f,g) \mapsto \mathrm{tr}(fg^\dagger).$$

Proposition 1.10.6. *This is positive definite. In fact*

$$\mathrm{tr}(ff^\dagger) = 2g\frac{(D^{g-1}\cdot f^*(D))}{(D^g)}$$

for $\phi = \phi_{\mathcal{L}(D)}$.

So given a simple abelian variety we have a division algebra $/\mathbf{Q}$ equipped with a positive definite involution.

Definition 1.10.7 (Albert algebras?)**.** A division algebra D finite over $\mathbf{Q}$ with an involution $'$ such that $\mathrm{tr}_{D/\mathbf{Q}}(xx') > 0\ \forall x \in D^\times$ is called an **Albert algebra**.

Such algebras were studied by Albert who proved an important classification theorem.

Theorem 1.10.8 (Albert (1934/5))**.** *Let $(D,')$ be an Albert algebra, let K be the center of D and K_0 the subfield fixed by $'$. Then we have the following classification*

1. *Type I: $D = K = K_0$ a totally real number field and $'$ is the identity.*
2. *Type II: D is a quaternion algebra over $K = K_0$ a totally real field, that is split at all infinite places and $'$ is defined by letting starting with the standard quaternion algebra conjugation for which $x + x^* = \mathrm{tr}(x)$ and then letting $x' = ax^*a^{-1}$ for some $a \in D$ for which $a^2 \in K$ and is totally negative.*
3. *Type III: D is a quaternion algebra over $K = K_0$ a totally real field, that is ramified at all infinite places and $'$ is the standard quaternion algebra conjugation as above.*
4. *Type IV: D is a division algebra over a CM field K and K_0 is the maximal totally real subfield. Additionally if v is a finite place with $v = \bar{v}$ we have $\mathrm{Inv}_v(D) = 0$ and $\mathrm{Inv}_v(D) + \mathrm{Inv}_{\bar{v}}(D) = 0$ for all places v.*

There is a fascinating table in Mumford, page 200 or something.

As one might hope, changing the polarization does not change the type of the algebra + involution pair.

One might wonder which endomorphisms are invariant under this process? I.e. what is

$$\{f \in \mathrm{End}^0(A) : f^\dagger = f\}.$$

Equivalently, for which f is the dual given by conjugating by our polarization.

We can map

$$\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{NS}(X) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{Pic}\, X/\mathrm{Pic}^0\, X \to \mathrm{Hom}(A, \hat{A})$$

$$\mathcal{M} \mapsto \phi_{\mathcal{M}},$$

however we also have an isomorphism

$$\mathrm{Hom}^0(A, \hat{A}) \xrightarrow{\sim} \mathrm{End}^0(A)$$

$$\phi \mapsto \lambda^{-1}\phi$$

for some fixed polarization λ, hence we can view $\mathrm{NS}(A) \otimes \mathbf{Q}$ inside $\mathrm{End}^0(A)$.

Proposition 1.10.9. *Assume k algebraically closed. The image of*

$$\mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{NS}(X) \to \mathrm{End}^0(A)$$

is the fixed subspace

$$\{f \in \mathrm{End}^0(A) : f^\dagger = f\}.$$

Proof. Fix $\alpha \in \mathrm{End}^0(A)$ and $l \neq \mathrm{char}(k)$ odd. Applying Proposition 1.9.8 we see that $\lambda\alpha = \phi_{\mathcal{L}}$ for some $\mathcal{L}$ iff $e_l^{\lambda\alpha}$ is skew-symmetric, but we also have

$$e_l^{\lambda\alpha}(a, a') = e_l^{\lambda}(a, \alpha a') = -e_l^{\lambda}(\alpha a', a) = -e_l(a', \hat{\alpha}\lambda a)$$

for all $a, a' \in V_l A$ this is the same as requiring $\lambda\alpha = \hat{\alpha}\lambda$ i.e. $\alpha = \alpha^\dagger$. . ◻

Another cool result we can now prove (in fact this was the reason Weil introduced the notion of a polarization).

Theorem 1.10.10. *The automorphism group of a polarized abelian variety is finite.*

Proof. Let α be an automorphism of (A, λ) i.e. $\lambda = \hat{\alpha}\lambda\alpha$, then $\alpha^\dagger\alpha = 1$ and so

$$\alpha \in \mathrm{End}(A) \cap \{\beta \in \mathrm{End}(A) \otimes \mathbf{R} : \mathrm{Tr}(\alpha^\dagger\alpha) = 2g\}$$

but $\mathrm{End}(A)$ is discrete inside the compact RHS. ◻

1.11 Abelian Varieties over finite fields (Ricky)

Set $q = p^m$, p prime. Given $X/\mathbf{F}_q$ have geometric Frobenius $\pi_X \colon X \to X$ which acts as id on $|X|$ and sends $f \to f^q$ for $f \in \mathcal{O}_X(U)$.

Example 1.11.1. $X \hookrightarrow \mathbf{P}^n$ then $\pi_X(a_0 : \cdots : a_n) = (a_0^q : \cdots : a_n^q)$.

We also have absolute Frobenius

$$F \colon X \to X^{(p)}.$$

Example 1.11.2.

$$X \colon y^2 = x^3 + i/\mathbf{F}_q$$
$$X^{(p)} \colon y^2 = x^3 + i^3 = x^3 - i/\mathbf{F}_q$$

We see that $X^{(p^m)} = X$ and $F^m = \pi_X$.

$$\begin{tikzcd}
X \arrow[dr] \arrow[drr] \arrow[ddr] & & \\
& X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\
& \mathbf{F}_q \arrow[r, "p"'] & \mathbf{F}_q
\end{tikzcd}$$

If $f \colon X \to Y$ of $\mathbf{F}_q$-schemes then $\pi_Y \circ f = f \circ \pi_X$. Now let X be an abelian variety over $\mathbf{F}_q$. From above, we have π_X commutes with all elements of $\mathrm{End}^0(X) = \mathrm{End}^0(X) \otimes \mathbf{Q}$. Let f_X be the characteristic polynomial of $T_l(\pi_X) \colon V_l(X) \to V_l(X)$ for $l \neq p$.

An alternative definition is to take $f_X \in \mathbf{Z}[X]$ monic of degree $2g$, $g = \dim X$ s.t.

$$f_X(n) = \deg([n] - \pi_X),$$

see 12.8.

Proposition 1.11.3 (16.3)**.** *Assume X is elementary, (i.e. its isogenous to A^n for some A simple). Then $\mathbf{Q}[\pi_X] \subseteq \mathrm{End}^0(X)$ is a field and f_X is a power of the minimal polynomial of π_X over $\mathbf{Q}$.*

Proof. Since X is elementary $Z(\mathrm{End}^0(X))$ is a field containing $\mathbf{Q}[\pi_X]$. Let g be the minimal polynomial of π_X over $\mathbf{Q}$. Let α be a root of f. Then $g(\alpha)$ is an eigenvalue of $g(V_l(\pi_X)) = V_l(g(\pi_X)) = V_l(0) = 0$. Hence $g(\alpha) = 0$. □

Theorem 1.11.4 (16.4)**.** *Let $g = \dim(X)$.*

1. *Every root of f_X $\alpha \in \mathbf{C}$ satisfies $|\alpha| = q^{1/2}$.*

2. *If α is a root of f_X, then $\bar{\alpha}$ with the same multiplicity. In particular if $\alpha = \pm\sqrt{q}$ then it occurs with even multiplicity.*

We need some facts before proving this: Ref 5.20, 5.21

- There exists

  $$V \colon X^{(p)} \to X$$

  such that

  $$V \circ F = [p]_X$$

  and

  $$F \circ V = [p]_{X^{(p)}}.$$

  Using $\deg F = p^g$ get $\deg V = p^g$

- By induction $[p^m] = V^m \circ F^m$.

We also need some facts about F and V relative to $X^\vee$.

$$F_X^\vee = V_{X^\vee} \colon (X^\vee)^{(p)} \to X^\vee$$

identifying $(X^\vee)^{(p)} = (X^{(p)})^\vee$, Ref 7.33, 7.34.

Proof. Reduce to the case where X is simple, we have

$$h \colon X \to X_1 \times X_2 \times \cdots \times X_s$$

an isogeny with X_i simple, then h induces an isomorphism

$$h \colon V_l(X) \xrightarrow{\sim} \bigoplus_i V_l(X_i)$$

so $f_X = f_{X_1} \cdots f_{X_s}$. Hence we can assume X is simple.

Let $\lambda \colon X \to X^\vee$ be a polarization of X and $\dagger$ be the corresponding Rosati involution on $\mathrm{End}^0(X)$ we will show that $\pi_X \pi_X^\dagger = q$.

$$\pi_X \pi_X^\dagger = \pi_X \lambda^{-1} \pi_X^\vee \lambda = \lambda^{-1} \pi_{X^\vee} \pi_X^\vee \lambda = \lambda^{-1}[q]\lambda = [q]$$

To see $\pi_{X^\vee} = \pi_X^\vee = q$ we use $\pi_X = F^m$ and $\pi_X^\vee = V^m$. So $\pi_{X^\vee}\pi_X^\vee = F^M V^M = p^m = q$. As X is simple $\mathbf{Q}[\pi_X]$ is a field. Thus f_X is a power of g, the minimal polynomial of $\pi_X/\mathbf{Q}$. So the complex roots of f_X are $\iota(\pi_X)$ for every embedding $\mathbf{Q}[\pi_X] \hookrightarrow \mathbf{C}$. since $\pi_X^\dagger = q/\pi_X$, we see that

$$\mathbf{Q}[\pi_X] \subseteq \mathrm{End}^0(X)$$

is stable under $\dagger$. We have two cases for such a $K = \mathbf{Q}[\pi_X]$

1. K is totally real and $\dagger = \mathrm{id}$.
2. K is a CM field and $\dagger = \bar{\cdot}$.

hence we get

$$\iota(\pi_X \pi_X^\dagger) = \iota(\pi_X)\overline{\iota(\pi_X)} = q$$

for any $\iota \colon K \to \mathbf{C}$.

If $\pm\sqrt{q}$ is a root of f_X then we are in the case of K totally real. If $\sqrt{q}$ has multiplicity n. Then $-\sqrt{q}$ has multiplicity $2g - n$. Thus $f_X(0) = (-1)^n q^g$. But also $f_X(0) = \deg(0 - \pi_X) = q^g$. Hence n is even. ∎

Honda-Tate The correspondence between isogeny classes of $X/\mathbf{F}_q$ and conjugacy classes of q-Weil numbers is a bijection. (i.e. algebraic integers α s.t. $|\iota\alpha| = \sqrt{q}$ for all $\iota \colon \mathbf{Q}(\alpha) \hookrightarrow \mathbf{C}$).

Using relations between a curve $C/\mathbf{F}_q$ and its Jacobian $J(C)$, one can show:

Theorem 1.11.5 (Hasse-Weil-Serre bound)**.**

$$q + 1 - g\lfloor 2\sqrt{q}\rfloor \leq \#C(\mathbf{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q}\rfloor$$

where $g = g(C)$.

Proof. Hint: Use Lefschetz trace and $H^1(C, \mathbf{Q}_l) \simeq H^1(J(C), \mathbf{Q}_l)$. ∎

Application: Let $J = J_0(103) = J(X_0(103))$. $J \sim J_+ \times J_-$.

$$J_\pm = \mathrm{im}(w \pm \mathrm{id})$$

w Atkin-Lehner. $\dim J = 8$ and $\dim(J_-) = 6$. In fact $\exists f \in S_2(\Gamma_0(103))$ an eigenform s.t. if

$$f = \sum_{n \geq 1} a_n q^n$$

then $[\mathbf{Q}(a_n)_{n\geq 1} : \mathbf{Q}] = 6$ and $\mathrm{tr}(F_{J_-,p}; T_l(J_-)) = \mathrm{tr}_{K/\mathbf{Q}}(a_p)$ for $l \neq p, p \neq 103$ We can compute $\mathrm{tr}_{K/\mathbf{Q}}(a_2) = 4$. This implies that $J_- \times \mathbf{F}_2$ is not the Jacobian of a curve $/\mathbf{F}_2$, if it were, then if $J_- \times \mathbf{F}_2 = J(C)$ then via Lefschetz trace formula

$$\#C(\mathbf{F}_2) = 2 + 1 - 4 = -1$$

similar thing at 17.

1.12 Tate's Isogeny Theorem (Sachi)

1.12.1 The Theorem

Theorem 1.12.1 (Tate)**.** *Let $A, B/\mathbf{F}_q = k$, $q = p^n$, $l \neq p$ be abelian varieties and $G = \mathrm{Gal}(k^s/k)$, then*

$$\mathrm{Hom}_k(A,B) \otimes \mathbf{Z}_l \to \mathrm{Hom}_G(T_lA, T_lB) = \mathrm{Hom}_{\mathbf{Z}_l}(T_lA, T_lB)^G$$

(where the G action on $\mathrm{Hom}_{\mathbf{Z}_l}(T_lA, T_lB)$ is $(gf)(x) = gf(g^{-1}x)$) is an isomorphism.

Remark 1.12.2. Tate's theorem is also true for function fields over finite fields (Zarhin) and fields that are finitely generated over their prime field (Faltings), e.g. number fields. Not true over algebraically closed fields though.

1.12.2 Motivation

Let π_A and π_B be the (relative) Frobenii on $V_l(A), V_l(B)$

$$\mathrm{Hom}_k(A,B) \otimes \mathbf{Q}_l \to \mathrm{Hom}_G(V_lA, V_lB)$$

P_A, P_B characteristic polynomials of π_A, π_B.

Toy Weil conjectures: P_A, P_B have $\mathbf{Z}$-coefficients, don't depend on the choice of l. Provided that induced action of Frobenii are semisimple, we can find a number $r(P_A, P_B)$ then Tate implies

$$r(P_A, P_B) = \dim_{\mathbf{Q}_l} \mathrm{Hom}_G(V_l(A), V_l(B)) = \mathrm{rank}\,\mathrm{Hom}_k(A,B)$$

Corollary 1.12.3. *Let A, B be abelian varieties over $\mathbf{F}_q$ and P_A, P_B as above*

1. $$\mathrm{rank}\,\mathrm{Hom}_k(A,B) = r(P_A, P_B)$$

2. *TFAE*
   - *(a) B is k-isogenous to an abelian subvariety of A*
   - *(b) V_lB is G-isomorphic to a G-subrepresentation of V_lA for $l \neq \mathrm{char}\, k$*
   - *(c)* $$P_B | P_A$$

we also have similar statements for equivalence, but get a nice statement about counting points over all extensions determining an abelian variety.

Proof.

$$\alpha\colon V_l(B) \hookrightarrow V_l(A)$$

the surjectivity in Tate's theorem means we can choose $u \in \operatorname{Hom}_k(B,A) \otimes \mathbf{Q}_l$. $V_l(u) = \alpha$. Choose $u \in \operatorname{Hom}_k(B,A) \otimes \mathbf{Q}$ arbitrarily close to α. Lower semicontinuity implies if $V_l(u)$ is close enough to α, can ensure $V_l(u)$ is injective ($\ker(V_l(u)) = 0$) take multiple to get $u \in \operatorname{Hom}_k(B,A)$. Since $T_l(u)$ is injective u is an isogeny to an abelian subvariety. □

1.12.3 Isogeny category

Recall: The isogeny category, Theorem 1.7.1, Corollary 1.7.3. So we have a category $\mathcal{I}\int\wr\}$ of abelian varieties with

$$\operatorname{Hom}_{\mathcal{I}\int\wr\}}(A,B) = \operatorname{Hom}_{\mathcal{AV}}(A,B) \otimes \mathbf{Q}.$$

Now if $f\colon A \to B$ there exists $g\colon B \to A$ an isogeny and $n \in \mathbf{Z}_{\geq 1}$ s.t. $gf = [n]$. So $\frac{1}{n}g$ is an inverse for $f \in \mathcal{I}\int\wr\}$ so isogenies are isomorphisms in $\mathcal{I}\int\wr\}$.

$\mathcal{I}\int\wr\}$ is a semisimple abelian category. The simples are simple abelian varieties.

1. Decomposition up to isogeny into a product of simple abelian varieties is unique.

2. If A is simple $\operatorname{End} A \otimes \mathbf{Q}$ is a division algebra over $\mathbf{Q}$. Reason: If A is simple in an abelian category, if $\operatorname{End} A \supseteq k$ a field implies it's a division algebra.

1.12.4 Reductions

Lemma 1.12.4.

1. $$\mathbf{Z}_l \otimes \operatorname{Hom}_{\mathcal{AV}}(A,B) \to \operatorname{Hom}_H(T_l, T_l B)$$

   is an isomorphism if and only if

   $$\mathbf{Q}_l \otimes \operatorname{Hom}_{\mathcal{AV}}(A,B) \to \operatorname{Hom}_G(V_l A, V_l B)$$

   is an iso

2. *If for every C,*

   $$\mathbf{Q}_l \otimes \operatorname{End}_{\mathcal{AV}}(C) \to \operatorname{End}_G(V_l C)$$

   is an isomorphism then the above is an isomorphism for every pair A, B.

Proof.

1. The first map is always injective, the cokernel is torsion free, hence free. It's an isomorphism if and only if $\mathbf{Q}_l \otimes \operatorname{coker} = 0$ As $\mathbf{Q}_l$ is flat over $\mathbf{Z}_l$ the second map injective and its cokernel is $\mathbf{Q}_l\otimes$ the cokernel of the first map.

2.
$$C = A \times B$$
then
$$\mathrm{End}^0(C) = \mathrm{End}^0(A) \oplus \mathrm{Hom}^0(A, B) \oplus \mathrm{Hom}^0(B, A) \oplus \mathrm{End}^0(B)$$
and
$$\mathrm{End}_G(V_l C) = \mathrm{End}_G(V_l A) \oplus \mathrm{Hom}_G(V_l A, V_l B) \oplus \mathrm{Hom}_G(V_l B, V_l A) \oplus \mathrm{End}_G(V_l B)$$
which the injection above preserves, in particular if the last map is an isomorphism, so are the rest.

□

One more reduction!

$$E_l = \mathrm{End}_k(A) \otimes \mathbf{Q}_l \subseteq \mathrm{End}_{\mathbf{Q}_l}(V_l A)$$
$$F_l = \mathbf{Q}_l[G] \subseteq \mathrm{End}_{\mathbf{Q}_l}(V_l A)$$
automorphisms of $V_l(A)$ coming from G.

Note 1.12.5. E_l coming from k-rational endomorphisms commute with the Galois action
$$F_l \subseteq C_{\mathrm{End}_{\mathbf{Q}_l}(V_l(A))}(E_l)$$
want equality.

Lemma 1.12.6.

1. *The last map of the reduction lemma is an isomorphism if and only if*
$$C(C(E_l)) = \mathrm{End}_G(V_l(A))$$
2. *If F_l is semisimple the map is an isomorphism if and only if*
$$C(E_l) = F_l$$

Proof.

1. Double centralizer theorem, if E_l is semisimple then $C(C(E_l)) = E_l$. Poincaré reducibility implies
$$A \sim \prod A_i^{m_i}$$
$$\mathrm{End}^0(A) = \mathrm{End}^0(\prod A_i^{m_i}) = \prod \mathrm{Mat}_{m_i}(\mathrm{End}^0(A_i))$$
a finite dimensional division algebra $/\mathbf{Q}$. A matrix algebra over a finite dimensional division algebra is semisimple.
2. If F_l is semisimple
$$C(E_l) = F_l \iff E_l = C(C(E_l))$$
so
$$E_l = C(F_l) = \mathrm{End}_G(V_l(A)).$$
□

1.12.5 Proof of Tate using finiteness

We introduce a hypothesis: $\mathrm{Hyp}(k, A, l)$ there exist only finitely many (up to k-isomorphism) abelian varieties B s.t. there is a k-isogeny of l-power degree from $B \to A$.

$D = C(E_l)$ want that $C(D) = \mathrm{End}_G(V_l(A))$ know $C(D) \subseteq E_l \subseteq \mathrm{End}_G(V_l(A))$ want $C(D) \supseteq \mathrm{End}_G(V_l(A))$. Let $\alpha \in \mathrm{End}_G(V_l(A))$ show that it commutes with everything in D. Equivalently let W be the graph of α

$$W = \{(x, \alpha x) \in V_l(A) \times V_l(A)\} \subseteq V_l(A) \times V_l(A)$$

note $g \in G$ then $g \circlearrowleft (x, \alpha x) = (gx, g\alpha x) = (gx, \alpha(gx))$.

$$\alpha \in C(D) \iff \forall x \in V_l(A), d \in D$$

$$\alpha dx = d\alpha x \iff (d \oplus d)W \subseteq W \forall d \in D$$

$$W \ni (dx, d\alpha x) = (dx, \alpha dx)$$

Lemma 1.12.7 (Technical lemma)**.** *If $W \subseteq V_l(A)$ is G-stable subspace then there exists $u \in E_l$ s.t. $uV_l(A) = W$.*

Proof. For $n \in \mathbf{Z}_{\geq 0}$ let $U_n = (W \cap T_l(A)) + l^n T_A$ which is a G-stable lattice in $V_l A$,

$$l^n T_l A \subseteq U_n \subseteq T_l A$$

let $\mathcal{K}_n \subseteq A[l^n](k^s) = T_l A / l^n T_l A$ be the image of U_n. $\mathcal{K}_n$ is stable under G-action on $A[l^n](k^s)$ which implies $\mathcal{K}_n = K_n(k^s)$. Let $\pi_n \colon A \to B_n = A/K_n$, $\iota_n \colon B_n \to A$ unique isogeny s.t.

$$\iota_n \circ \pi_n = [[l^n]_A$$

then $T_l B \cong U_n$ as $\mathbf{Z}_l$-modules with G-action. As $T_l(\iota_n) \colon U_n = T_l B \to T_l A$ is the inclusion map. Assuming $\mathrm{Hyp}(k, A, l)$ we can find $n = n_1 < n_2 < \cdots$ s.t. we have

$$\alpha_i \colon B_n \xrightarrow{\sim} B_{n_i}$$

$$\begin{tikzcd} B_n \arrow[r, "\alpha_i"] & B_{n_i} \arrow[d, "\iota_{n_i}"] \\ A \arrow[u, "\pi_n"] \arrow[r, dashed, "u_i"'] & A \end{tikzcd}$$

$u_i = \iota_{n_i} \circ \alpha_i \circ \pi_n$ is an endomorphism of A on Tate modules $T_l(u_i)$ is induced map

$$T_l A \xrightarrow{[l^n]} U_n \xrightarrow{T_l \alpha_i} U_{n_i} \hookrightarrow T_l A$$

because $\mathbf{Z}_l \otimes \mathrm{End}\, A$ is a free $\mathbf{Z}_l$-module of finite rank compact in l-adic topology subsequence of $u_i \to u$ in $\mathbf{Z}_l \otimes \mathrm{End}\, A$

$$U_{n_1} \supseteq U_{n_2} \supseteq \cdots$$

the endomorphism of $T_l u$ maps $T_l A$ to $\bigcap_{i=1}^{\infty} U_{n_i} = W \cap T_l A$ passing to $\mathbf{Q}_l$-coefficients, note $\mathbf{Q}_l(W \cap T_l A) = \mathbf{Q}_l(l^n(W \cap T_l A)) = W$ so $\mathrm{im}(V_l(u)) = W$. □

Why does the hypothesis hold.

Fact 1.12.8. *There exists a moduli space of d-polarised abelian varieties of* $\dim = g$ *$A_{g,d}$ which is a stack of finite type $/k$.*

$$A_{g,d}(k) = \{(A, \lambda) : A, \lambda \colon A \to A^\vee, \ \deg d\}$$

Zahrin's trick: A abelian variety $(A \times A^\vee)^4$ is principally polarized. Finiteness of direct factors $B \subseteq A$ $A \simeq B \times C$.

Corollary 1.12.9. *If* $k = \mathbf{F}_q$ *exists only finitely many isogeny classes of abelian varieties of* dim g.

Proof. A is a direct factor $(A \times A^\vee)^4 \in A_{8g,1}$. □

Proof. of Tate.

Apply technical lemma to $V_l(A \times A)$ and W so

$$(d \oplus d)W = (d \oplus d)uV_l(A \times A) = u(d \oplus d)V_l(A \times A) \subseteq uV_l(A \times A) = W$$

$$\implies C(D) \supseteq \mathrm{End}_G(V_l(A)).$$ □

1.13 The Honda Tate Theorem (Angus)

$q = p^n$, A a simple abelian variety over $\mathbf{F}_q$, π_A the frobenius on A, $\mathrm{End}^0(A) = \mathbf{Q} \otimes \mathrm{End}(A)$, f_A is the charpoly of A (i.e. of π_A).

Fact 1.13.1.

- $\mathrm{End}^0(A)$ *is a division ring.*
- $\mathbf{Q}[\pi]$ *is a field.*
- $Z(\mathrm{End}^0(A)) = \mathbf{Q}[\pi_A]$

Lemma 1.13.2 (The Weil Conjectures)**.** *The roots of* f_A *all have absolute value* $\sqrt{q}$. *Alternatively, under all embeddings*

$$\iota \colon \mathbf{Q}[\pi_A] \hookrightarrow \mathbf{C}, \ |\iota(\pi_A)| = \sqrt{q}.$$

Definition 1.13.3 (q-Weil numbers)**.** A q-**Weil number** is an algebraic integer π s.t.

$$\forall \iota \colon \mathbf{Q}[\pi] \hookrightarrow \mathbf{C}, \ |\iota(\pi)| = \sqrt{q}$$

we say that two q-Weil numbers are conjugate if they have the same minimal polynomial over $\mathbf{Q}$, and write $\pi \sim \pi'$.

From the facts so far we have a map

$$\{\text{simple AVs}/\mathbf{F}_q\} \to \{q\text{-Weil numbers}\}$$

$$A \mapsto \pi_A$$

Theorem 1.13.4. *We have a bijection*

$$\{\textit{isogeny classes of simple AVs}/\mathbf{F}_q\} \xrightarrow{\sim} \{\textit{conjugacy classes of } q\textit{-Weil numbers}\}$$

$$A \mapsto \pi_A.$$

We need to show this is well-defined, injectivity and surjectivity.

1.13.1 Honda-Tate map

Recall:

Corollary 1.13.5. *Let A, B be abelian varieties over $\mathbf{F}_q$ with rational Tate modules $V_l A, V_l B$ then*

$$A \sim_{isog} B \iff V_l A \simeq V_l B \forall l \neq p.$$

Corollary 1.13.6.

$$A \sim_{isog} B \iff f_A = f_B$$

Proof. By above $V_l A \simeq V_l B$ for all $l \neq p$ but f_A (resp. f_B) is the charpoly of π_a (π_B) on $V_l A$ ($V_l(B)$).

The Galois modules $V_l A$ and $V_l B$ are semisimple. The Brauer-Nesbitt theorem says $f_A = f_B \implies V_l A \simeq V_l B$ for $l \neq p$. □

Recalling that f_A is a power of the minimal polynomial of π_A,

$$A \sim_{\text{isog}} B \implies f_A = f_B \implies \pi_A \sim \pi_B.$$

So the Honda-Tate map is well defined.

This doesn't quite give injectivity because a priori f_A and f_B could be powers of the minpolys of π_A, π_B.

1.13.2 Injectivity and Brauer groups

From last time:

Proposition 1.13.7. *There exists a certain quantity $r(f_A, f_B)$ such that*

$$r(f_A, f_B) = \operatorname{rank} \operatorname{Hom}(A, B).$$

Corollary 1.13.8. *Let $d = [\operatorname{End}^0(A) : \mathbf{Q}(\pi_A)]^{1/2}$, let $h_A = \operatorname{minpoly}_{\mathbf{Q}}(\pi_A)$ then $f_A = h_A^d$.*

Proof. Study the formula for $r(f_A, f_A)$ Edixhoven-van der Geer-Moonen 16.22. □

So the next step is to try and recover $\operatorname{End}^0(A)$ form π.

Definition 1.13.9. A **central simple algebra** B/k is a k-algebra B with no two-sided ideals and $Z(B) = k$.

Theorem 1.13.10 (Artin-Wedderburn)**.** *Any such algbera is isomorphic to $M_n(D)$ for D a division ring over k.*

Definition 1.13.11 (Brauer groups)**.** The **Brauer group** of k $\operatorname{Br}(k)$ is the set of central simple algebras under $\otimes$ module the algebras $M_n(k)$.

Fact 1.13.12.

- *If $k = \overline{k}$,* $\operatorname{Br}(k) = 0$.
- *k complete nonarchimidean* $\operatorname{Br}(k) = \mathbf{Q}/\mathbf{Z}$
- $\operatorname{Br}(\mathbf{R}) = \mathbf{Z}/2\mathbf{Z}$

Given a place v of k we get a map

$$\mathrm{Br}(k) \longrightarrow \mathrm{Br}(k_v)$$

$$D \mapsto D \otimes k_v$$

in fact we get an injection

$$\mathrm{Br}(k) \hookrightarrow \prod_v \mathrm{Br}(k_v) \simeq \prod_{v \text{ nonarch}} \mathbf{Q}/\mathbf{Z} \times \prod_{v \text{ real}} \mathbf{Z}/2\mathbf{Z}$$

$$D \mapsto (\mathrm{inv}_v(D))_v$$

these $\mathrm{inv}_v(D)$ *are called the* ***local invariants****.*

Proposition 1.13.13. *Let $A/\mathbf{F}_q$ be an elementary abelian variety. Let $K = \mathbf{Q}(\pi_A)$ then*

$$\mathrm{inv}_v(\mathrm{End}^0(A)) = \begin{cases} \frac{v(\pi_A)}{v(q)}[k_v : \mathbf{Q}_p], & v|p \\ \frac{1}{2}, & v \text{ real} \\ 0, & \text{else} \end{cases}$$

Proof. Edixhoven-van der Geer-Moonen 16.30. □

Proposition 1.13.14. *Let $d = [\mathrm{End}^0(A) : \mathbf{Q}(\pi_A)]^{1/2}$ then d is the least common denominator of all the* $\mathrm{inv}_v(\mathrm{End}^0(A))$.

Corollary 1.13.15.

$$\pi_A \sim \pi_B \iff f_A = f_B.$$

Proof. $\Leftarrow$ done.

$\Rightarrow$ Let D_{π_A}, D_{π_B} be the division rings with invariants specified as in Proposition 13. $\pi_A \sim \pi_B \implies D_{\pi_A} \simeq D_{\pi_B} \implies f_A = \mathrm{minpoly}(\pi_A)^d = f_B$. □

1.13.3 Surjectivity and CM theory

We need to sow that for aπ a q-Weil number there exists an abelian variety $A/\mathbf{F}_q$ such that $\pi_A \sim \pi$.

Definition 1.13.16. Such a q-Weil number π is called effective.

Proposition 1.13.17. *A q-Weil number π is effective if and only if π^N is effective for some $N \in \mathbf{Z}_{\geq 1}$.*

Proof. $\Rightarrow$ clear.

$\Leftarrow$ By assumption we have A'/k a simple abelian variety s.t. $\pi_{A'} \sim \pi^N$ for k a degree N extension of $\mathbf{F}_q$. Let

$$A = \mathrm{Res}_{k/\mathbf{F}_q}(A')$$

on the rational Tate modules we have

$$V_l A = \mathrm{Ind}_{G_k}^{G_{\mathbf{F}_q}}(V_l A')$$

where

$$G_k = \mathrm{Gal}(\overline{\mathbf{F}_q}/k)$$

$$G_{\mathbf{F}_q} = \mathrm{Gal}(\overline{\mathbf{F}_q}/k)$$

since $G_k, G_{\mathbf{F}_q}$ are abelian, by studying the induced action, one can see

$$\mathrm{Ind}_{G_k}^{G_{\mathbf{F}_q}}(\pi_{A'}) = \pi_A^N$$

in particular $f_A(T) = f_{A'}(T^N)$. Choosing a simple factor A_i one gets $\pi_{A_i} \sim \pi$. □

So it is sufficient to show π^N is effective.
Strategy for proving surjectivity

1. Construct a division algebra D_π.
2. Choose a CM field L splitting D_π.
3. Find an abelian variety $A/\mathbf{C}$ of type (L, Φ).
4. In fact A is defined over a number field K and has good reduction at $v|p$.
5. Apply the Shimura-Taniyama formula to relate π_A to Φ.
6. Choose Φ wisely (in retrospect in 3) to relate π to π_A.
7. Show $\pi_A^N = \pi^{N'}$.

D_π is given by the invariants described by π (and $K = \mathbf{Q}(\pi)$).

Proposition 1.13.18. *There exists a CM field $L/\mathbf{Q}(\pi)$ such that L splits D_π and further*

$$[L : \mathbf{Q}(\pi)] = [D_\pi : \mathbf{Q}(\pi)]^{1/2}$$

Proof. Two cases:

1. $\mathbf{Q}(\pi)$ is totally real, in which case $\mathbf{Q}(\pi) = \mathbf{Q}$ or $\mathbf{Q}(\sqrt{p})$.
2. $\mathbf{Q}(\pi)$ is a CM field with totally real subfield $\mathbf{Q}(\pi + q/\pi)$.

In the case

1. Choose $L = \mathbf{Q}(\pi)(\sqrt{-p})$.
2. Let $d = [D_\pi : \mathbf{Q}(\pi)]^{1/2}$. This L splits D_π.

□

For a CM field L all the embeddings

$$\iota \colon L \hookrightarrow \mathbf{C}$$

come in complex conjugate pairs, choosing an embedding for each pair defines a subset $\Phi \subseteq \mathrm{Hom}(L, \mathbf{C})$ such that

$$\Phi \cup \overline{\Phi} = \mathrm{Hom}(L, \mathbf{C})$$

$$\Phi \cap \overline{\Phi} = \emptyset$$

such a choice of Φ is called a CM type.

Let $A/\mathbf{C}$ be an abelian variety with CM by L i.e.

$$L \hookrightarrow \mathrm{End}^0(A)$$

then

$$\mathbf{C} \otimes L = \prod_\iota \mathbf{C}$$

acts on the tangent space at the origin $\mathrm{Lie}(A)$.

Proposition 1.13.19. *The action of $\mathbf{C} \otimes L$ factors through the quotient $\prod_{\iota \in \Phi} \mathbf{C}$ for some CM type Φ. We then say $A/\mathbf{C}$ is of type (L, Φ).*

Theorem 1.13.20. *For any CM type* (L, Φ) *there exists an abelian variety* $A/\mathbf{C}$ *of type* (L, Φ).

Proof. Found in Shimura-Taniyama. ◻

The fact that A is in fact defined over a number field K is also in Shimura-Taniyama.

Theorem 1.13.21. *Let* A/K *be an abelian variety which admits CM. Then* A/K *admits potentially good reduction at all places* v *of* K.

Proof. Highly nontrivial, Neron models, Chevalley decomposition, Neron-Ogg-Shafarevich criterion, result of Grothendieck on potentially stable reduction. ◻

After passing to a finite extension we will assume A/K has good reduction at places $v|p$. So we have a reduction $A_{\mathbf{F}_{q'}}/\mathbf{F}_{q'}$. For a place $w|p$ of L let

$$\Sigma_w = \mathrm{Hom}(L_w, \mathbf{C}_p)$$

$$\Phi_w = \Phi \cap \Sigma_w.$$

Theorem 1.13.22 (Shimura-Taniyama formula)**.** *For all places* $w|p$ *of* L,

$$\frac{w(\pi_{A_{\mathbf{F}_{q'}}})}{w(q')} = \frac{\#\Phi_w}{\#\Sigma_w}$$

Proof. Tate has a proof using CM theory of p-divisible groups. ◻

Recall we fixed π and from this we deterministically formed $\mathbf{Q}(\pi), D_\pi, L$ however we have no restriction on our choice of Φ.

Lemma 1.13.23. *We can choose* Φ *such that for all places* $w|p$ *of* L,

$$\frac{w(\pi)}{w(q)} = \frac{\#\Phi_w}{\#\Sigma_w}$$

Proof. Let $v = w|_{\mathbf{Q}(\pi)}$ be the place of $\mathbf{Q}(\pi)$ below w. Let

$$n_w = \frac{w(\pi)}{w(q)}\#\Sigma_w = \frac{w(\pi)}{w(q)}[L_w : \mathbf{Q}_p]$$

$$= \frac{w(\pi)}{w(q)}[L_w : \mathbf{Q}(\pi)_v][\mathbf{Q}(\pi)_v : \mathbf{Q}_p]$$

by recalling the formula for the local invariants of D_π we get

$$n_w = \mathrm{inv}_w(D_\pi \otimes_{\mathbf{Q}(\pi)} L).$$

But L splits D_π so $n_w \in \mathbf{Z}$, further

$$n_w + n_{\overline{w}} = \left(\frac{w(\pi)}{w(q)} + \frac{\overline{w}(\pi)}{\overline{w}(q)}\right)\#\Sigma_w$$

$$= \left(\frac{w(\pi\overline{\pi})}{w(q)}\right)\#\Sigma_w = \#\Sigma_w$$

check the CM type $\Phi = \bigcup_w \Phi_w$ where for each w $\#\Phi_w = n_w$. Then the formula follows. ◻

Combining the previous result with the Shimura-Taniyama formula we get tahat for all places $w|p$

$$\frac{w(\pi_{A_{\mathbf{F}_{q'}}})}{w(q')} = \frac{w(\pi)}{w(q)}.$$

Taking the correct power,

$$w\left(\frac{\pi^m_{A_{\mathbf{F}_{q'}}}}{\pi^{m'}}\right) = 0\forall w|p$$

$$\pi, \pi_{A_{\mathbf{F}_{q'}}}|q^{m'}$$

$$\implies w(\cdots) = 0\forall w \nmid p$$

since $|\pi^{m'}|_w = |\pi^m_{A_{\mathbf{F}_{q'}}}|_w = (q^{m'})^{1/2}\forall$ infinite places

$$\pi_{A_{\mathbf{F}_{q'}}}/\pi_A^{m'}$$

is a root of unity $\pi^N_{A_{\mathbf{F}_{q'}}} = \pi^{N'}$.