Isomorphism classes of principally polarized abelian varieties over finite fields

Marseglia Stefano

Stockholms Universitet

22 December 2015

Abelian varieties

Definition

An **abelian variety** A over a field k is a connected and complete group variety over k, that is a k-variety A together with morphisms $m : A \times A \to A$ and $\iota : A \to A$ and a identity element $e \in A(k)$ such that the quadruple (A, m, ι, e) is a group in the category of varieties.

It turns out that:

- A is non-singular;
- A is projective;
- the group law on A is commutative;
- a morphism $f : A \to B$ is the composition of homomorphism $h : A \to B$ and a translation t_b, for some $b = -f(e_A) \in B(k)$.

Example

One-dimensional abelian varieties are called **elliptic curves**.

Example

If $\mathrm{char}(k) \neq 2, 3$ consider $\mathcal{C} : y^2 = x^3 + ax + b$, with $4a^3 + 27b^2 \neq 0$.
In this case we can describe explicitly the group law:

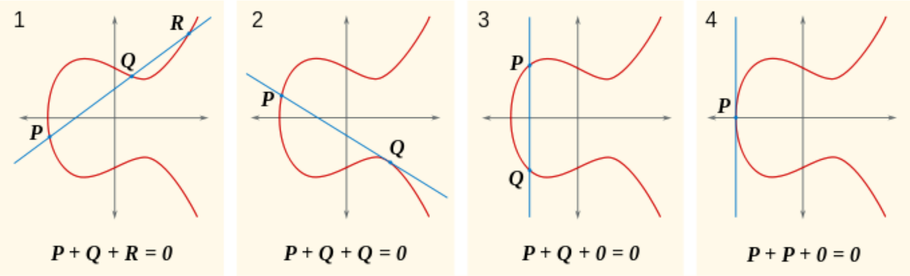

Figure : www.limited-entropy.com

Isogenies

Definition

A homomorphism $f : A \to B$ is called **isogeny** if it is surjective and with finite kernel. The **degree** of f is the degree of the kernel of f (as a finite group scheme).

In particular:

- if $A \simeq B$ then $\dim A = \dim B$;
- $\deg(f \circ g) = \deg(f)\deg(g)$;
- if $\deg(f) = n$ then there exists an isogeny $g : B \to A$ such that $f \circ g = n_A : a \mapsto na$ for every $a \in A(k)$;
- $A \simeq \prod_i A_i^{e_i}$, with the A_i's are **simple** and non-isogenous.

Dual abelian variety

Put: $\mathrm{Pic}^0(A) = \left\{\mathcal{L} \text{ inv. sheaf : } t_a^*\mathcal{L} \approx \mathcal{L} \text{ on } A_{\bar{k}} \text{ for all } a \in A(\bar{k})\right\} / \approx .$

Definition

An abelian variety $A^\vee$ is the **dual** abelian variety of A and an invertible sheaf $\mathcal{P}$ on $A \times A^\vee$ is the **Poincarè** sheaf if:

1. $\mathcal{P}|_{\{e\}\times A^\vee}$ is trivial and $\mathcal{P}|_{A\times\{a\}}$ lies in $\mathrm{Pic}^0(A_{k(a)})$ for all $a \in A^\vee$; and
2. for every k-scheme T and invertible sheaf $\mathcal{L}$ on $A \times T$ such that $\mathcal{L}|_{\{e\}\times A^\vee}$ is trivial and $\mathcal{L}|_{A\times\{t\}}$ lies in $\mathrm{Pic}^0(A_{k(t)})$ for all $t \in T$, there is a unique morphism $f : T \to A^\vee$ such that $(1 \times f)^*\mathcal{P} \approx \mathcal{L}$.

Polarizations

In particular:

- $(A^\vee, \mathcal{P})$ is uniquely determined up to a unique isomorphism;
- $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$ and every element of $\mathrm{Pic}^0(A_{\bar{k}})$ is represented uniquely once in the family $(\mathcal{P}_a)_{a \in A(\bar{k})}$;
- $A^{\vee\vee} = A$.

Definition

A **polarization** λ on A is an isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\bar{k}} = \varphi_{\mathcal{L}} : a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$ for some ample invertible sheaf $\mathcal{L}$ on $A_{\bar{k}}$.
If $\deg(\lambda) = 1$ we say that A is **principally polarized**.

- The automorphism group of (A, λ) is finite.

Over $k = \mathbb{C}$ ...

If $k = \mathbb{C}$ the situation is simpler!
An abelian variety over $\mathbb{C}$ of dimension g is a **complex torus** $A = V/\Lambda$ with a **non-degenarete Riemann form** $H : V \times V \to \mathbb{C}$, where:

- $V =$ a g-dimensional $\mathbb{C}$-vector space;
- $\Lambda =$ a lattice of rank $2g$ (inside V);
- H is Hermitian and $E = \operatorname{Im} H$ is integer valued on Λ.

The **dual** variety is $A^\vee = V^*/\Lambda^*$, where:

- $V^* =$ antilinear functionals on V, and
- $\Lambda^* = \{f \in V^* | \langle f, t\rangle := \operatorname{Im}(f(t)) \in \mathbb{Z} \text{ for all } t \in \Lambda\}$.

A **polarization** is an equivalence class of Riemann forms (containing a non-degenerate one), where $H_1 \sim H_2 \iff \exists n_1, n_2 \in \mathbb{N} : n_1 H_1 = n_2 H_2$.

... and in $\mathrm{char}(k) = p > 0$

- Serre: when $\mathrm{char}(k) = p > 0$ it is **not** possible to functorially attach a free abelian group of rank $2g$ to a g-dimensional abelian variety A.
- Weil: for $l \neq p$: $A[l^m](\bar{k}) \simeq (\mathbb{Z}/l^m\mathbb{Z})^{2g}$;
- but: $A[p^m](\bar{k}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^f$ for some $0 \leq f \leq g$.

Frobenius

Let's move to finite fields:

Definition

Let A be an abelian variety over $\mathbb{F}_q$. The **Frobenius** morphism of A is the morphism $\pi_A : A \to A$ which is the identity on the underlying topological space and is the map $x \mapsto x^q$ on $\mathcal{O}_A$. It is an isogeny of degree q.

Theorem

Let h_A be the **characteristic** polynomial of π_A (on $T_l A := \varprojlim A[l^m](\bar{k})$). Write $h_A(X) = \prod_{i=0}^{2g}(X - \alpha_i)$. The roots α_i are called q-**Weil numbers**. Then

- $h_A(X) \in \mathbb{Z}[X]$;
- $\#A(\mathbb{F}_{q^m}) = \prod(1 - \alpha_i^m)$, for all $m \geq 1$;
- $|\alpha_i| = \sqrt{q}$.

Classification up to isogeny: Honda-Tate theory

Theorem (Tate)

The abelian varieties A and B over $\mathbb{F}_q$ are isogenous if and only if $h_A = h_B$.

Recall: two algebraic numbers α and β are conjugate if and only if $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)$.

Theorem (Honda)

There is a bijection between conjugacy classes of q-Weil numbers and isogeny classes of simple abelian varieties over $\mathbb{F}_q$

Deligne's category

Definition

We say that A is **ordinary** if one of the following equivalent conditions holds:

- $\#A[p](\bar{k}) = p^g$;
- exactly half of the roots of h_A are p-adic units;
- the middle coefficient of h_A is coprime to p.

Definition

Let $\mathcal{D}_q$ be the category of pairs (T, F), with

- T is a free $\mathbb{Z}$-module of even rank and F is an endomorphism of T;
- $F \otimes \mathbb{Q}$ is semi-simple and its eigenvalues have complex-size $\sqrt{q}$;
- half of the roots of the characteristic polynomial of F are p-adic units;
- exists an endomorphism V such that $FV = q$.

Construction of the equivalence

Theorem (Deligne ('69))

There is an equivalence of categories T between the category of ordinary abelian varieties over $\mathbb{F}_q$ and $\mathcal{D}_q$.

- Let $\tilde{A}$ be the canonical Serre-Tate lift of A to the ring of Witt-vectors $W(\overline{\mathbb{F}}_q)$;
- choose and embedding $\varepsilon : W(\overline{\mathbb{F}}_q) \hookrightarrow \mathbb{C}$;
- define $T(A) := H_1(\tilde{A} \otimes_\epsilon \mathbb{C})$ and F the lift of π_A.

Observe: $\mathrm{Rank}(T(A)) = 2\dim(A)$
and $T(\pi_A) = F(A)$.

Dual varieties in $\mathcal{D}_q$

Definition

The **dual** of $(T, F) \in \mathcal{D}_q$ is $(\hat{T}, \hat{F})$, where

- $\hat{T} = \mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Z})$;
- $\hat{F} : \psi \mapsto \psi \circ V$.

Theorem (Howe '95)

Deligne's equivalence respects duality.

Polarizations in $\mathcal{D}_q$

Let $(T, F) \in \mathcal{D}_q$. Put $R = \mathbb{Z}[F, V] \subseteq \mathrm{End}((T, F))$.
Observe: $K = R \otimes \mathbb{Q}$ is a product of CM-fields.
Let v be the p-adic valuation induced by the embedding $\varepsilon : W(\overline{\mathbb{F}}_q) \hookrightarrow \mathbb{C}$.
Define the CM-type $\Phi := \{\varphi : K \to \mathbb{C} | v(\varphi(F)) > 0\}$.
Let $\iota \in K$ such that $\varphi(\iota)$ is positive imaginary for every $\varphi \in \Phi$.
Fact: an isogeny $\lambda : (T, F) \to (\hat{T}, \hat{F})$ induces a pairing $b : T \times T \to \mathbb{Z}$.

Definition

The isogeny λ is a **polarization** if:

- b is alternating, and
- the pairing $(x, y) \mapsto b(\iota x, y)$ on $T \times T$ is symmetric and positive definite.

Theorem (Howe '95)

Deligne's equivalence sends polarizations to polarizations.

When h is irreducible

Fix an irreducible ordinary q-Weil polynomial h and let F be a root.
Let $\mathcal{I}$ be the isogeny class corresponding to h in $\mathcal{D}_q$.
Put $R = \mathbb{Z}[F, V]$. It is an order in the number field $K = \mathbb{Q}[X]/h(X)$.

Proposition (Howe)

$$\{\text{Deligne modules in } \mathcal{I}\} \longleftrightarrow \{\text{Fractional ideals of } R\}$$

Let I be a fractional R-ideal corresponding to a Deligne module (T, F).
Then $(\hat{T}, \hat{F})$ corresponds to $\bar{I}^t$, where $I^t = \left\{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(xI) \subseteq \mathbb{Z}\right\}$ is the **trace dual** of I and $\bar{\cdot}$ is the CM-conjugation of K.
Moreover a **polarization** of (T, F) is $\lambda \in K^*$ such that

- $\lambda I \subseteq \bar{I}^t$;
- λ is totally imaginary;
- $\varphi(\lambda)$ is positive imaginary for every $\varphi \in \Phi$.

Isomorphism classes

Goal: count the isomorphism classes, with polarizations.
We get

$$\left\{\begin{matrix}\text{Isomorphism classes of}\\ \text{abelian varieties in } \mathcal{I}\end{matrix}\right\} \longleftrightarrow \{\textbf{Ideal class monoid} \text{ of } R\}$$

Recall: $I \simeq J \iff \exists x \in K^* : I = xJ$.
Problem: it is not known how to compute efficiently the ICM(R) when R is not maximal (not Dedekind), because there are **non-invertible classes**.
Let $[I] \in ICM(R)$ such that $xI = \bar{I}^t$ for some $x \in K^*$.
If for some $u \in (I : I)^\times$ we have xu is totally imaginary and $\varphi(xu)$ is positive imaginary for every $\varphi \in \Phi$ then $\lambda := xu$ is a polarization of I.

Number of polarizations and automorphisms

Assume that I has a polarization λ. Then:

$$\left\{\begin{matrix}\text{number of non-isomorphic} \\ \text{polarizations on } I\end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in (I : I)^\times\}}{\{v\bar{v} : v \in (I : I)^\times\}}$$

and

$$\mathrm{Aut}((I,\lambda)) \longleftrightarrow \left\{\text{torsion units } u \in (I : I)^\times\right\}$$

Computations

Abelian surfaces over $\mathbb{F}_3$ with **irreducible ordinary (and Clifford)** polynomials:

$$x^4 - 4x^3 + 8x^2 - 12x + 9 = [8] \qquad x^4 - 3x^3 + 5x^2 - 9x + 9 = [2]$$
$$x^4 - 2x^3 + x^2 - 6x + 9 = [6] \qquad x^4 - 2x^3 + 2x^2 - 6x + 9 = [2, 4]$$
$$x^4 - 2x^3 + 4x^2 - 6x + 9 = [2, 2] \qquad x^4 - 2x^3 + 5x^2 - 6x + 9 = [2]$$
$$x^4 - x^3 - 2x^2 - 3x + 9 = [6] \qquad x^4 - x^3 - x^2 - 3x + 9 = [2]$$
$$x^4 - x^3 + 2x^2 - 3x + 9 = [2, 2] \qquad x^4 - x^3 + 5x^2 - 3x + 9 = [2]$$
$$x^4 - 5x^2 + 9 = [4] \qquad x^4 - x^2 + 9 = [2, 2]$$
$$x^4 + x^2 + 9 = [2, 2] \qquad x^4 + x^3 - 2x^2 + 3x + 9 = [6]$$
$$x^4 + x^3 - x^2 + 3x + 9 = [2] \qquad x^4 + x^3 + 2x^2 + 3x + 9 = [2, 2]$$
$$x^4 + x^3 + 5x^2 + 3x + 9 = [2] \qquad x^4 + 2x^3 + x^2 + 6x + 9 = [6]$$

$\dots$

Thank you for your attention.