2023/02/07 30 mins

A crash-course on abelian varieties over $\overline{\mathbb{F}_q}$

Def An abelian variety (AV) A over a field k is a
- connected
- projective
- group variety over k.

We have maps

$m : A \times A \to A \qquad \iota : A \to A$

and a rational point $\varepsilon \in A(k)$

s.t

$\leadsto$ $A(\bar{k})$ has a group structure
with operation m,
inverse ι,
neutral elt ε.

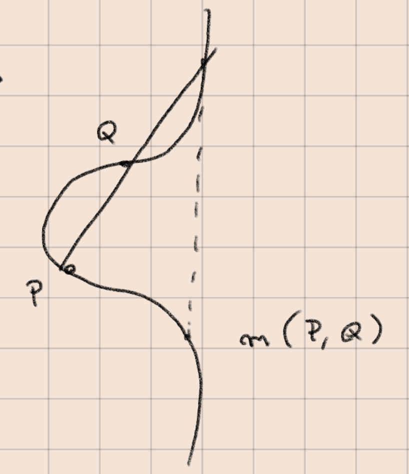
- Facts :
  - the group law is commutative.
  - A is smooth
  - A, B AVs, a morphism of varieties
    $\varphi : A \to B$
    is a homomorphism iff
    $$\varphi(\varepsilon_A) = \varepsilon_B.$$

- Examples 1) Elliptic curve :

$$Y^2 Z = X^3 + AXZ^2 + BZ^3 \qquad \Delta = 4A^3 + 27B^2 \neq 0$$

$\varepsilon = (0:1:0)$

(If $k = \mathbb{R}$ $\leadsto$



2) C a smooth curve of genus g

$\mathrm{Jac}(C)$ is an AV

<u>Def</u> : A hom. $\varphi : A \to B$ is an <u>isogeny</u> if surjective and $\dim A = \dim B$

($\ker \varphi$ is a finite group scheme.)

<u>Fact</u> : Being isogenous is an equivalence relation. $A \sim B$

(reflexive is tricky!)

Warning : All morphisms, hom, isogenis between A and B over k are going to be over k as well !!!

eg
- $\mathrm{Hom}(A,B)$ "=" $\mathrm{Hom}_k(A,B)$
- $A \sim B$ "=" $A \sim_k B$

§ <u>Over $\mathbb{F}_q$</u> $q = p^a$, with p prime

- An AV A over $\mathbb{F}_q$ comes equipped with a special endomorphism : <u>Frobenius</u>

$$\pi : A \to A$$

induced by the ring homomorphism

$$x \mapsto x^q$$

- <u>Fact</u> : π is an isogeny.

(π is very important to describe the isogeny class of A)

(Need some ingredients to get there)

Def For $\ell \neq p$, define the <u>ℓ-adic Tate module</u>:
$$T_\ell A = \varprojlim A[\ell^n]$$
ℓ^n-torsion subgroup of $A(\overline{\mathbb{F}_q})$

- Analogous to $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$

- In fact:
$$T_\ell A \simeq \mathbb{Z}_\ell^{2g}$$
where $g = \dim A$.

- The Frobenius induces a map
$$T_\ell A \xrightarrow{\pi_\ell} T_\ell A$$

- Consider $h_A(x)$ the <u>characteristic polynomial</u> of π:

- <u>Facts</u>:
  - $\deg(h_A) = 2g$
  - the definition of h_A does <u>NOT</u> depend on ℓ !!!
  - $h_A(x) \in \mathbb{Z}[x]$.
  - the complex roots α of $h_A(x)$ satisfy $|\alpha|_{\mathbb{C}} = \sqrt{q}$.

Fix g
q-Weil $=:$ polynomial

- **Thm** (Tate)

Given A, B AVs over $\mathbb{F}_q$. TFAE:

1. $A \sim B$ (over $\mathbb{F}_q$)
2. $h_A(x) = h_B(x)$

- **Def** A is <u>ordinary</u> if the coeff of x^g in h_A is coprime to p.

- $\left\{\begin{array}{c}\text{isogeny classes of} \\ \text{AVs over } \mathbb{F}_q \text{ of} \\ \text{dim } g\end{array}\right\} \longrightarrow \left\{\begin{array}{c}q\text{-Weil} \\ \text{poly of degree} \\ 2g\end{array}\right\}$

$$[A]_{\sim} \longmapsto h_A$$

is injective.

- There is also a "surjectivity" statement (Honda-Tate)

$\forall$ q-Weil poly h [with a few exceptions] ⚠

$\exists$ A s.t. $h_A = h$.