§ Abelian varieties

Let k be a field

- Def A group variety over k is a variety V over k, together with maps
  $$m : V \times V \to V \quad , \quad i : V \to V$$
  and a rational point $\varepsilon \in V(k)$ inducing a group structure on $V(\bar{k})$
  with multiplication m
  inverse i
  unit ε
- Equivalently (V, m, i, ε) is a group object in the category of k-schemes.

- Prop: A group variety is smooth.
  Pf: translate the non-singular locus, which is open.

- Def: A connected and complete group variety $/k$ is called an abelian variety over k
- Prop: - AV are projective
  - The group law is commutative.

Example

An abelian variety of dimension 1 is an elliptic curve:

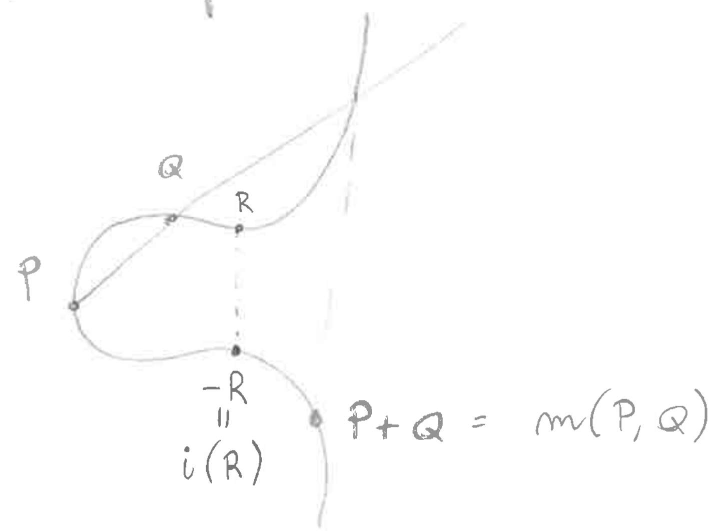
(char $k \neq 2, 3$) $Y^2Z = X^3 + AXZ^2 + BZ^3$ $\Delta = 4A^3 + 27B^2 \neq 0$

smooth

$\mathcal{E} = (0:1:0)$

group law is explicit

if $k = \mathbb{R}$



§ Isogenies

Prop Let $f: A \to B$ be a homomorphism of abelian varieties
TFAE: (1) f is surjective and $\dim(A) = \dim(B)$

(2) $\ker(f)$ is a finite group scheme
and $\dim(A) = \dim(B)$

(3) f is finite (flat) and surjective
superfluous

Def A hom. $f: A \to B$ sat. 1, 2, 3 is an isogeny
The degree of an isogeny is the degree as a morphism of var. i.e.

$$[k(A) : k(B)] = \operatorname{rank}(\ker f)$$

Ex Let $m \in \mathbb{Z}$, and consider

$$[m]_A : A \to A$$
$$P \mapsto mP$$

$[m]_A$ is an isogeny of degree $m^{2\cdot \dim A}$

Prop If $f: A \to B$ is an isogeny of degree d,
then $\exists\, g: B \to A$ isogeny s.t. $g \circ f = [d]_A$
and $f \circ g = [d]_B$

Cor Being isogenous is an eq. relation.

§ Endomorphisms

- Given $f, g : A \to B$ homomorphisms of a.v. over k we can define
$$f + g = m_B \circ (f, g) : A \to B.$$
- This induces an abelian group structure on
$$\mathrm{Hom}_k(A, B)$$
and a ring structure on
$$\mathrm{End}_k(A)$$
- Since for every $n \in \mathbb{Z}$ we have
$$n \cdot f = [n]_B \circ f = f \circ [n]_A$$
and $[n]_A$ is onto we get that
$$\mathrm{Hom}_k(A, B)$$
is <u>torsion-free</u>
- Put $\mathrm{Hom}^\circ_k(A, B) = \mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$
and $\mathrm{End}^\circ_k(A) = \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$
- Observe that isogenies are precisely elements which become invertible in $\mathrm{Hom}^\circ_k(A, B)$.

- **Thm** (Poicaré Splitting thm)
  Let A be an a.v. $/k$ and B an ab. sub-variety of A.
  Then there exists an ab. sub-variety C of A s.t.

$$f: B \times C \longrightarrow A$$
$$(x, y) \longmapsto m(x,y)$$

is an isogeny.

- **Def** An abelian variety A over k is simple (over k) if there are no proper non-trivial abelian sub-varieties of A (over k).

- **Cor** (Poincaré decomp.)
  Given an ab. var. A over k
  there are simple and pair-wise non-isogenous abelian subvar. $B_1, \dots, B_r$ and positive integers $e_1, \dots, e_r$ st

$$A \underset{\text{isogenous}}{\sim} B_1^{e_1} \times \dots \times B_r^{e_r}.$$

- **Rmk** – A simple $/k$ $\overset{\Leftarrow}{\not\Rightarrow}$ A simple over $k' \supsetneq k$.

  – $A \sim B$ $/k$ $\underset{\not\Leftarrow}{\Rightarrow}$ $A \sim B$ $/k' \supsetneq k$

§ Over $\mathbb{C}$

- Let's take a close look to the case $k = \mathbb{C}$.

- A an ab. var. $/ \mathbb{C}$
  then $A(\mathbb{C})$ is a compact connected Lie group.

- Let $T_\varepsilon(A(\mathbb{C}))$ be the tangentspace at the unit ε.

  and consider

$$\begin{array}{rcl} V & & \\ \exp : T_\varepsilon(A(\mathbb{C})) & \longrightarrow & A(\mathbb{C}) \\ v & \longmapsto & (\varphi_v : \mathbb{C} \to A(\mathbb{C}))\big|_1 \end{array}$$

– exp is surjective

– ker(exp) is a discrete subgroup L

$$\Rightarrow \quad \frac{V}{L} \simeq A(\mathbb{C})$$

$+ \; V \simeq \mathbb{C}^g \qquad g = \dim A$

$+ \; L \simeq \mathbb{Z}^{2g}$

$\Rightarrow \; V/L$ is a $\mathbb{C}$-torus
which admits a Riemann form.

- The converse also holds.

- **Thm** There is an eq of categories

$$\{AV / \mathbb{C}\} \longleftrightarrow \left\{ \begin{array}{c} \text{complex tori} \\ + \text{Riemann form} \end{array} \right\}$$

"Pf"

$\longrightarrow$ ok

$\longleftarrow$: use the R.f. $\rightsquigarrow$ Θ-functions $\rightsquigarrow$ proj embedding of the torus

§ positive characteristic

- Example (Serre)
  Let E be a supersing. elliptic curve over $\overline{\mathbb{F}_p}$.
  Then $\mathrm{End}^\circ(E)$ is a quaternion algebra
  which does not admit a 2-dimensional representation

  Hence we cannot have an analogous Thm on the whole category of ab. var.

  "life is hard"

- "On the other hand there's extra structure in char p".
  Let k be a field of characteristic p.

$$0 \to p\mathbb{Z} \to \mathbb{Z} \to k \iff \mathbb{F}_p \hookrightarrow k$$

  eg. $\overline{\mathbb{F}_p}$, $\mathbb{F}_p(t)$, $\mathbb{F}_q$ with $q = p^d$.

- The map $x \mapsto x^p$ is a ring homomorphism
  called the Frobenius of k.

- Let S be a scheme over $\mathbb{F}_p$ (eg. $\mathrm{Spec}(\overline{\mathbb{F}_q})$)

- The <u>absolute Frobenius</u> of S is the morphism

$$F_S : S \to S$$
$$\mathcal{O}_S : x \mapsto x^p$$

Let A be a scheme over S and put $A^{(p)} = A \times_S S$ induced by F_S.

- Define the <u>relative Frobenius</u> $F_{A/S}$ of A as

$$\begin{tikzcd}
A \arrow[dr, dashed, "F_{A/S}"] \arrow[drr, bend left, "F_A"] \arrow[ddr, bend right] & & \\
& A^{(p)} \arrow[r] \arrow[d] & A \arrow[d] \\
& S \arrow[r, "F_S"] & S
\end{tikzcd}$$

- <u>Def</u> Let A be a scheme over $\mathbb{F}_{p^m}$ $\left(A^{(p^m)} \simeq A\right)$
the <u>Frobenius of A</u> is

$$\pi_A : \left(A \xrightarrow{F_{A/S}} A^{(p)} \xrightarrow{F_{A^{(p)}/S}} A^{(p^2)} \to \cdots \to A^{(p^m)} \simeq A\right)$$

- <u>Prop</u>
  - k a field of char$(k) = p$
  - A an abelian variety of dim g on k
  - Then $F_{A/k}$ is an isogeny of degree p^g

  If $k = \mathbb{F}_q$, $q = p^m$ then π_A is an isogeny of degree q^g.

- It follows that there exists an isogeny

$$V_{A/k} : A^{(p)} \to A$$

st $\quad V_{A/k} \circ F_{A/k} = [p]_A$ and $F_{A/k} \circ V_{A/k} = [p]_{A^{(p)}}$

called the <u>relative Verschiebung</u>.

- If $k = \mathbb{F}_{p^m}$, we define the <u>Verschiebung</u> of A as the m-th iterate of rel. Versch.

<u>Ex</u> $\quad S = \operatorname{Spec} A$ an affine scheme over $\mathbb{F}_p$

$$X = \operatorname{Spec} \frac{A[T_1, \dots, T_m]}{I}$$

Then $\quad X^{(p)} = \operatorname{Spec} \dfrac{A[T_1, \dots, T_m]}{I^{(p)}}$

where $\quad I^{(p)} = \left\{ \sum_{\nu \in \mathbb{N}^m} a_\nu^p T^\nu : \sum_{\nu \in \mathbb{N}^m} a_\nu T^\nu \in I \right\}$

The relative Frob

$$F_{X/S} : X \to X^{(p)}$$

is induced by the A-alg. hom. $\quad T_i \to T_i^p$

§ Weil conjectures

- Let V be a smooth projective variety of dimension g defined over $\mathbb{F}_q$, with $q = p^n$
- Let $N_m = \# V(\mathbb{F}_{q^m})$ is finite.
- The Hasse-Weil zeta function of V is

$$\zeta(V, T) = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} T^m\right)$$

- Observe $$N_m = \left(\frac{1}{(m-1)!} \frac{d^m}{d^m T} \log(\zeta(V, T))\right)\Bigg|_{T=0}$$

- **Thm** (Weil conj)

1) (Rationality) $\zeta(V, T) \in \mathbb{Q}(T)$

2) (Riemann hyp)

We can write $$\zeta(V, T) = \frac{P_1(T) P_3(T) \cdots P_{2g-1}(T)}{P_0(T) P_2(T) \cdots P_{2g}(T)}$$

with $P_i \in \mathbb{Z}[T]$ and

$$P_0(T) = (1-T), \quad P_{2g}(T) = (1 - q^g T)$$

and for $1 \leq i \leq 2g-1$

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \quad \text{over } \mathbb{C}$$

for alg. integers α_{ij} with $|\alpha_{ij}| = q^{i/2}$

3) (Functional equation)

Euler char of V

$$\zeta\left(V, \frac{1}{q^g T}\right) = \pm q^{\frac{g\chi}{2}} T^{\chi} \zeta(V, T)$$ L3.11

(Induces symmetries on α_{ij}

eg $\alpha_{2g-1,i} = q^g/\alpha_i$

4) (Betti numbers $\leftrightarrow$ deg P_i)

"Pf by Weil, Dwork, Grothendieck, Deligne, ..."

§ Tate modules

- Let A be an abelian variety of a perfect field k.
- Let ℓ ~~be~~ a prime, $\ell \neq$ char k.

 - $A[\ell^m] = \ker(\ell^m : A \to A)$ finite group scheme of rank $(\ell^m)^{2g}$

 - $A[\ell^m]$ is étale, that is is uniquely determined by its $\bar{k}$-points and the action of $G = Gal(\bar{k}/k)$.

- The group schemes $\ell : A[\ell^{m+1}] \to A[\ell^m]$ form an inverse system

Def The ℓ-Tate module of A is

$$T_\ell A = \varprojlim A[\ell^m](\bar{k})$$

- **Prop**
  - $T_\ell A \simeq \mathbb{Z}_\ell^{2g}$ $\qquad g = \dim A$
  - $A[\ell^m](\bar{k}) \simeq T_\ell A / \ell^m T_\ell A$
  - T_ℓ is a functor:

$$\{AV \text{ over } k\} \to \underline{\mathrm{Mod}}_{\mathbb{Z}_\ell[\mathcal{G}]}$$

- **Thm** (Weil)

A, B ab. var. over k. Then the natural morphism

$$\mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(T_\ell A, T_\ell B)$$

is injective.

It follow that $\mathrm{Hom}_k(A, B)$ is a free $\mathbb{Z}$-module of finite rank.

- Let A be an abelian variety over $\mathbb{F}_q$

Denote by h_A the characteristic polynomial of

$$T_\ell \pi_A : T_\ell A \to T_\ell A$$

- One can prove that

$$h_A = P_1 \in \mathbb{Z}[T] \rightsquigarrow \text{in } \frac{\text{does not depend on } \ell}{\zeta(A, T)}$$

and P_r is the char poly of the action of π_A on $\Lambda^r T_\ell A$.

Def h_A is called the characteristic poly of A

- It follows also that if

$$A \sim B_1^{m_1} \times \dots \times B_r^{m_r} \qquad B_i \text{ simple pairwise non isog.}$$

then

$$\mathrm{End}^0(A) = \prod_{i=1}^{r} \mathrm{End}^0(B_i^{m_i}) \quad \text{with center } \mathbb{Q}(\pi_A) \cong \prod_{i=1}^{r} \mathbb{Q}(\pi_{B_i})$$

and

$$\mathrm{End}^0(B_i^{m_i}) = M_{m_i \times m_i}(\mathrm{End}^0(B_i))$$

- <u>Def</u> $q = p^n$

  A <u>q-Weil number</u> π is an algebraic integer s.t. for every embedding

  $$\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$$

  we have $|\psi(\pi)| = q^{1/2}$

- π_A is a <u>q-Weil number</u> (as it is a root of P_1)

- <u>Thm</u> (Tate) If k is a finite fied, then

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

  is an iso.

- <u>Thm</u> (Tate) TFAE: $\qquad A, B$ a.v. $/ \mathbb{F}_q$
  - $A \underset{\mathbb{F}_q}{\sim} B$
  - $h_A = h_B$
  - $\zeta(A,T) = \zeta(B,T)$

- <u>Thm</u> (Honda - Tate)
There is a bijection

$$\{\text{simple ab. var.}/\mathbb{F}_q\}/\sim_{\mathbb{F}_q} \longleftrightarrow \{q\text{-Weil numbers}\}/\sim$$

isogeny

conjugation
//
Same minimal
poly

$$A \longmapsto \pi_A$$

- If $A \underset{\mathbb{F}_q}{\sim} B_1^{m_1} \times \dots \times B_r^{m_r}$, $\dim A = g$, $q = p^n$
then $\underline{h_A = h_{B_1}^{m_1} \cdots h_{B_r}^{m_r}}$, $\deg h_A = 2g$,
- If B is simple then $\underline{h_B = m_B^e}$
where m_B is the (irreducible) minimal polynomial of π_B
and

$$e = \text{l.c.d.}\left\{ \frac{v_p(g(0))}{n} : g \text{ irreducible factor of } m_B \text{ over } \mathbb{Q}_p \right\}$$

- <u>Hence</u> if we fix a dimension g
we can <u>list</u> all characteric poly's of Frobenius
i.e. we can list all ab. var. of dim g $/\mathbb{F}_q$
up to isogeny.