§ Categorical descriptions of $AV(q)$

- Let $q = p^d$, p a prime.
- Denote by $AV(q)$ the category of ab. var. over $\mathbb{F}_q$.
- Recall that we can associate to each $A \in AV(q)$

  a monic polynomial $h_A(x) \in \mathbb{Z}[x]$ of degree $2 \cdot \dim A$ which identifies A up to isogeny.

  $\left(h_A = \mathrm{char}(\pi_A : T_\ell A \to T_\ell A) \right.$, for any $\left. \ell \neq \mathrm{char}\, \mathbb{F}_q \right)$

- Def $A \in AV(q)$ is called ordinary if one of the following equiv. conditions holds: $\quad g = \dim A$

  ① $A[p](\overline{\mathbb{F}}_q) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^g$ max possible;

  ② half of the roots of $h_A(x)$ in $\overline{\mathbb{Q}}_p$ are p-adic units;

  ③ The coefficients of x^{g+1} in $h_A(x)$ is coprime with p.

- Ex If A is an elliptic curve over $\mathbb{F}_q$ then

$$h_A = x^2 - t_p x + q$$

where t_p is the trace of the Frobenius.

By Hasse-Weil:

$$|t_p| < 2\sqrt{q}$$

If $(t_p, p) = 1$ then A is ordinary.

- **Def**
  - $AV^{ord}(q) = \left\{\begin{array}{l}\text{full subcategory of } AV(q) \text{ consisting} \\ \text{of ordinary ab. var.}\end{array}\right\}$
  - $AV^{cs}(p) = \left\{\begin{array}{l}\text{—— '' —— } AV(p) \text{ ——} \\ \text{of ab. var. } A \text{ s.t. } h_A(\sqrt{p}) \neq 0\end{array}\right\}$ | - over $\mathbb{F}_p$ - no real roots.
  - $\mathcal{M}^{ord}(q)$ = pairs (T, F), where T is a free fin. gen $\mathbb{Z}$-module and F is a $\mathbb{Z}$-linear $F: T \to T$ st
    1. $F \otimes \mathbb{Q}$ is semisimple, w/ eigenvalues of abs. value $\sqrt{q}$
    2. half of the roots of char$(F \otimes \mathbb{Q})$ over $\overline{\mathbb{Q}}_p$ are p-adic units
    3. there exists $V: T \to T$ $\mathbb{Z}$-linear such that $FV = VF = q$
  - $\mathcal{M}^{cs}(p)$ = — (T, F) ——
    1. ———— abs. value $\sqrt{p}$
    2. — char$(F \otimes \mathbb{Q})$ has no real roots ——
    3. — $FV = VF = p$.
  - morphisms in $\mathcal{M}^{ord}(q)$ and $\mathcal{M}^{cs}(p)$ are commutative diagrams

$$\begin{tikzcd} T \arrow[r, "\varphi"] \arrow[d, "F"'] & T' \arrow[d, "F'"] \\ T \arrow[r, "\varphi"'] & T' \end{tikzcd}$$

φ $\mathbb{Z}$-linear.

Thm There is an equivalence of categories

$$\mathcal{F}^{ord} : AV^{ord}(q) \to \mathcal{M}^{ord}(q)$$

and an anti-equivalence

$$\mathcal{F}^{cs} : AV^{cs}(p) \to \mathcal{M}^{cs}(p).$$

Both satisfy :

if $\quad A \mapsto (T(A), F(A))$

then : $\quad rk_{\mathbb{Z}}(T(A)) = 2 \cdot \dim A$

and $\quad F(A)$ is the image of π_A the Frobenius end. of A

Rmk • ①, ② and ①', ②' are conditions on the char and min polynomial of F.

• $AV^{ord}(p) \subseteq AV^{cs}(p)$ <u>Exercise</u>

F^{ord}: - A ord / $\overline{\mathbb{F}}_q$

- denote by $W = W(\overline{\mathbb{F}}_q)$ the ring of Witt vectors over $\overline{\mathbb{F}}_q$.
  and fix an embedding $W \overset{\varepsilon}{\hookrightarrow} \mathbb{C}$.
- since A is ordinary there exists a lift $\tilde{A}$ to W
  satisfying $\mathrm{End}_{\overline{\mathbb{F}}_q}(A) = \mathrm{End}_W(\tilde{A})$
  called the <u>canonical lift</u> of A.
- put $A_{\mathbb{C}} := \tilde{A} \underset{\varepsilon}{\otimes} \mathbb{C}$
- finally set $T(A) = H_1(A_{\mathbb{C}}, \mathbb{Z})$.
- note that every step in the construction is functorial
  so $T(A)$ comes equipped with a Frobenius endomorph.
  which we denote $F(A)$.

<u>Ref</u> Deligne 1969

F^{cs}: Reference: Centeleghe - Stix 2015
"Categories of abelian varieties, I:
Abelian varieties over $\mathbb{F}_p$"

- Let $W(p) = \{ p\text{-Weil numbers} \} \setminus \{\sqrt{p}\}$
- For every finite subset $w \subset W(p)$ they find an abelian variety A_w s.t.

$$A_w \sim \prod_{\pi_B \in w} B$$

and $\mathrm{End}_{\mathbb{F}_p}(A_w)$ is minimal

- Define $$M_w(A) := \mathrm{Hom}_{\mathbb{F}_p}(A, A_w)$$
- "Patch together" the functors M_w (as $w \subset W(p) \setminus \{\sqrt{p}\}$ grows) by choosing appropriate varieties A_w's to obtain the functor $T(A)$.
- All M_w induce anti-eq. $\rightsquigarrow$ also $T(A)$ is an anti-eq.

§ The square-free case

- Let h be an ordinary square-free q-Weil poly
  or a square-free p-Weil poly s.t. $h(\sqrt{p}) \neq 0$.
- $\underline{\underline{\text{i.e}}}$ $h = h_A$ for some $A \in AV^{ord}(q)$
  or $A \in AV^{cs}(p)$

and $A \sim B_1 \times \dots \times B_r$ with B_i simple and pairwise non-isogenous.

- **Rmk**: Here we are using the non-trivial fact that
  for $A \in AV^{ord}(q)$ or $AV^{cs}(p)$

  h_A is irreducible $\Leftrightarrow$ A is simple.

- **Def** - Denote by $AV(h)$ the full sub-category of $AV^{ord}(q)$ (resp. $AV^{cs}(p)$) of abelian varieties A s.t. $h_A = h$.
  - Denote by $\mathcal{M}(h)$ the full sub-category of $\mathcal{M}^{ord}(q)$ (resp. $\mathcal{M}^{cs}(p)$) of pairs (T, F) st $\mathrm{char}(F) = h$.

- **Cor** $\mathcal{F}^{ord}$ (resp $\mathcal{F}^{cs}$) induces an equivalence (resp. antiequiv.)

$$AV(h) \xrightarrow{\sim} \mathcal{M}(h).$$

- Put
$$R = \frac{\mathbb{Z}[x,y]}{(h(x),\, xy-q)}$$
p in the cs case

- R is an order in the étale $\mathbb{Q}$-algebra $\frac{\mathbb{Q}[x]}{(h(x))} = K$
- Denote by $\mathcal{J}(R)$ the category of fractional R-ideals, with R-linear morphisms.

- **Thm** There is an equivalence of categories
$$\mathcal{M}(h) \longrightarrow \mathcal{J}(R)$$

Pf. • for each pair (T,F) in $\mathcal{M}(h)$ we have a canonical isomorphism
$$\mathbb{Z}[F,V] \xrightarrow{\sim} R$$
induced by
$$F \longmapsto x$$
$$V \longmapsto y$$

- Since T is a $\mathbb{Z}[F,V]$-module of rank $\mathrm{rk}_{\mathbb{Z}} T = \deg h = \dim_{\mathbb{Q}} K$ it can be identified with a fractional ideal I of R.
- Conversely, every $I \in \mathcal{J}(R)$ is a free $\mathbb{Z}$-module of rank $\deg h$, hence it is an element of $\mathcal{M}(h)$

- To sum up

$$\mathcal{G} : \underbrace{AV(h) \simeq \mathcal{M}(h) \simeq}_{\sim} \mathcal{J}(R).$$

We understand this category <u>better</u>

- <u>Cor</u> Let A be in $AV(h)$ and put $I = \mathcal{G}(A) \in \mathcal{J}(R)$

then: ① $\mathrm{End}(A) = (I:I)$

② $\mathrm{Aut}(A) = (I:I)^{\times}$

③ $A \simeq B_1 \times \dots \times B_r$ iff

$I = I_1 \oplus \dots \oplus I_r$ iff

$(I:I) = R_1 \oplus \dots \oplus R_r$

Moreover: $AV(h)/_{\simeq} \longleftrightarrow ICM(R)$

<u>Hence</u> we can compute abelian varieties in $AV(h)$ up to isomorphism.

In the talk tomorrow....-

§ Another application of the ICM

- Let U, V be matrices, $m \times m$, with integer coefficients

$$U, V \in \mathcal{M}_{m\times m}(\mathbb{Z}).$$

- Recall that they are conjugate over $\mathbb{Z}$ if $\exists\ X \in GL_m(\mathbb{Z})$ ($\Leftrightarrow \det X = \pm 1$)

st $\quad XUX^{-1} = V \qquad$ Write $U \sim V$

- If $U \sim V$ then they have same characteristic polynomial and minimal polynomial.
- The converse is not true!

'Relation w/ $\mathcal{M}^{ad}(q)$'

- Fix a characteristic poly $h(x)$, assume $h(x)$ square-free
  ($\Rightarrow h(x) =$ minimal poly)

- Thm (Latimer, MacDuffee '33)
  There is a bijection

$$\left\{ U \in \mathcal{M}_{m,m}(\mathbb{Z}) : \underset{\text{char poly}}{h_U(x)} = h(x) \right\} \Big/ \sim_{\mathbb{Z}} \qquad \deg h = m$$

$$\Big\updownarrow$$

$$\mathrm{ICM}\left(\frac{\mathbb{Z}[x]}{(h)} \right)$$

"Pf" idea Write $\frac{\mathbb{Z}[x]}{(h)} = \mathbb{Z}[\alpha]$

for every $I \in \mathcal{J}(\mathbb{Z}[\alpha])$
choose a $\mathbb{Z}$-basis: $I = x_1\mathbb{Z} \oplus \ldots \oplus x_m\mathbb{Z}$
Consider the matrix U_α which represents the mult. by α wrt the chosen basis.

Exercise: fill in the details.