4. Weil's conjectures

4.1 Endomorphism rings of abelian varieties: Albert classification

Let A be a k-simple abelian variety of dimension g over $\mathbb{F}_q$.

Let $D = \mathrm{End}_k^0(A)$

<u>Wedderburn</u>: D is a division algebra.

- F the centre of D.
- $x \mapsto x^+$ be Rosati involution A.

This is a positive involution. So the fixed field $F^+ = \{x \in D : x^+ = x\}$

is a totally real number field (i.e. every embedding $\sigma : F^+ \hookrightarrow \mathbb{C}$ factors through $\mathbb{R}$)

Clearly, $F^+ \subseteq F$.

- Let $e = [F:\mathbb{Q}]$, $e^+ = [F^+:\mathbb{Q}]$, $[D:F] = d^2$

$d \in \mathbb{Z}_{\geq 0}$.

Theorem (Albert classification)

Keeping the notations above, the algebra D is isomorphic to one of the following types:

(1) Type I: $D = F = F^+$, and the Rosati involution is the identity; in that case, $e \mid g$.

(2) Type II: $F = F^+$ and D is a totally indefinite quaternion algebra over F, i.e $\forall \sigma: F \hookrightarrow \mathbb{R}$, $D \otimes_\sigma \mathbb{R} = M_2(\mathbb{R})$. In that case, $2e \mid g$.

(3) Type III: $F = F^+$ and D is totally definite quaternion algebra (i.e $\forall \sigma: F \hookrightarrow \mathbb{R}$) $D \otimes_\sigma \mathbb{R} \cong \mathbb{H}$, where $\mathbb{H}$ is the Hamilton quaternion algebra.) In that case, $e^2 \mid g$.

(4) Type IV: F is a CM extension of F^+ (i.e. it is totally imaginary quadratic extn of F^+), and D is a division algebra with centre is F. In that case,

* $e^t d^2 \mid g$ if char$(k) \neq 0$
* $e^t d \mid g$ if char$(k) > 0$.

4.2 Zeta functions of abelian varieties

Theorem. . A is an abelian variety $/ \mathbb{F}_q$.

. $\dim A = g$.

. $q = p^n$ $\quad p = \mathrm{char}(\mathbb{F}_p)$, $n \geq 1$.

(i) Every root $\alpha \in \mathbb{C}$ of the characteristic polynomial f_A of π_A has absolute value $|\alpha| = \sqrt{q}$.

(ii) If $\alpha \in \mathbb{C}$ is complex, then so is $\bar{\alpha} = \alpha / q$, and the two roots appear with the same multiplicity.

If $\alpha = \sqrt{q}$ or $-\sqrt{q}$ is a root of f_A, then its occurs with <u>even</u> multiplicity.

Proof: (i) Reduce to the case of a simple abelian variety.

So assume that

$h : A \sim_{\mathbb{F}_q} A' = A_1 \times \cdots \times A_s$, where each A_i is $\mathbb{F}_q$-simple.

The isogeny h induces an isomorphism of Tate modules:

$$V_\ell(h) : V_\ell(A) \cong V_\ell(A') = V_\ell(A_1) \oplus \cdots \oplus V_\ell(A_s)$$

But we have $h \circ \pi_A = \pi_{A'} \circ h$

$$\rightsquigarrow V_\ell(h) \cdot V_\ell(\pi_A) \cdot V_\ell(h)^{-1} = V_\ell(\pi_{A'})$$

But in that case, we see that

$$V_\ell(\pi_{A'}) : V_\ell(A') \longrightarrow V_\ell(A')$$

$$(x_1, \ldots, x_s) \longmapsto (V_\ell(\pi_{A_1})(x_1), \ldots, V_\ell(\pi_{A_s})(x_s))$$

So this implies that

$$f_A = f_{A_1} \cdots f_{A_s}.$$

So enough to consider simple abelian varieties.
Let $\lambda : A \to A^\vee$ and $+$ be the Rosati involution induced by λ. We first show that

$$\pi_A \circ \pi_A^+ = [q]_A$$

But $\pi_A \cdot \pi_A^+ = \pi_A \cdot \lambda^{-1} \cdot \pi_A^\vee \cdot \lambda = \lambda^{-1} \pi_A \cdot \pi_A^\vee \cdot \lambda$

So it is enough to show that $\pi_A \cdot \pi_A^\vee = [q]_{A^\vee}$.
But, by definition

$$\pi_A = F^n_{A/\mathbb{F}_q}$$

By the properties of the Verschiebung map (see next lecture), we have

$$\pi_A^\vee = V_{A^\vee/\mathbb{F}_q}, \text{ and}$$

$$\pi_{A^\vee} \cdot \pi_A^\vee = F^n_{A^\vee/\mathbb{F}_q} \cdot V^n_{A^\vee/\mathbb{F}_q} = [p^n]_{A^\vee} = [q]_{A^\vee}$$

Thus $\pi_A \cdot \pi_A^+ = [q]_A$.

Now, since A is simple, $\mathbb{Q}[\pi_A]$ is a number field. Furthermore, f_A is a power of the

minimal polynomial g of π_A.
So the complex roots of g (and hence f_A) are of the form $\iota(\pi_A)$ where
$\iota : \mathbb{Q}[\pi_A] \hookrightarrow \mathbb{C}$.

The relation $\pi_A \cdot \pi_A^{+} = [q]_A$
$\Rightarrow \mathbb{Q}[\pi_A]$ is stable under the involution $+$.
This is a positive involution.

(a) Totally real case: $\mathbb{Q}[\pi_A]$ is totally real and $+$ is just the identity map.

(b) CM: $\mathbb{Q}[\pi_A]$ is a CM field, i.e.
$\forall\ \iota : \mathbb{Q}[\pi_A] \hookrightarrow \mathbb{C}$, $\overline{\iota(x)} = \iota(x^{+})$
$\forall\ x \in \mathbb{Q}[\pi_A]$.

In either case, we see that $\pi_A \cdot \pi_A^{+} = q$ implies that $\alpha \in \mathbb{C}$ is a root of f_A, then $|\alpha| = \sqrt{q}$.

(ii) The first two assertions are easy to prove (exercise).

Assume that $\alpha = \sqrt{q}$ or $\alpha = -\sqrt{q}$ is a root of f_A. Then $\mathbb{Q}[\pi_A]$ cannot be a CM field. This means that $\mathbb{Q}[\pi_A]$ must be totally real. In that case the only possible roots are $\alpha = \pm\sqrt{q}$ because of the relation $\alpha\bar{\alpha} = q$.

If $\sqrt{q}$ has multiplicity $m \geq 0$, then $-\sqrt{q}$ has multiplicity $2g - m$.

But $f_A(0) = (-1)^m q^g$

$= \deg(\pi_A) = q^g$

$\Rightarrow (-1)^m q^g = q^g \Rightarrow m$ is even. $\square$

Let X be a scheme of finite type over $\mathbb{F}_q$. For any integer $n \geq 0$, let $N_n := \# X(\mathbb{F}_{q^n})$ be the number of $\mathbb{F}_{q^n}$-rational points. The zeta function of X is defined by

$$Z(X;t) := \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} t^n\right) \in \mathbb{Q}[[t]].$$

__Theorem__. Let A be an abelian variety$/\mathbb{F}_q$.
Write $f_A = \prod_{i=1}^{2g}(t-\alpha_i)$ (roots are counted with multiplicity).

(i) $$\# A(\mathbb{F}_{q^n}) = \prod_{i=1}^{2g}(1-\alpha_i^n).$$

(ii) The zeta function is given by
$$Z(A;t) = \frac{P_1 P_3 \cdots P_{2g+1}}{P_0 P_2 \cdots P_{2g}},$$
where each $P_k(t) \in \mathbb{Z}[t]$, $k = 0, \ldots, 2g$, and is given explicitly in terms of the α_i as follows:
$$P_k(t) := \prod_{1 \le i_1 < \cdots < i_k \le 2g} (1 - \alpha_{i_1} \cdots \alpha_{i_k} t).$$

(iii) Functional equation: $Z\left(A; \frac{1}{q^g t}\right) = Z(A;t)$

Jacobian varieties

The functor

X is a complete non singular curve $/k$.

The divisor group of X:

- $\mathrm{Div}(X) := \left\{ \sum_{i=1}^{n} n_i P_i \;:\; n_i \in \mathbb{Z},\ P_i \in X(\bar{k}) \right\}$

- The degree map:

$$D = \sum_{i=1}^{n} n_i P_i \longmapsto \deg(D) := \sum_{i=1}^{n} n_i .$$

- For $f \in \bar{k}(X)$,

$$\mathrm{div}(f) = \sum_{P \in X(\bar{k})} v_P(f)\, P$$

$$\in \mathrm{Div}(X).$$

$$\mathrm{Prin}(X) = \{ D \in \mathrm{Div}(X) : D = \mathrm{div}(f) \text{ for some } f \in \bar{k}(X) \}.$$

$$\mathrm{Pic}(X) = \mathrm{Div}(X)/\mathrm{Princ}(X).$$

$$\mathrm{Div}^0(X) := \{ D \in \mathrm{Div}(X) : \deg D = 0 \}$$

$$\cup\!\!\!\mid$$

$$\mathrm{Prin}(X)$$

Define $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\mathrm{Prin}(X)$

<u>Key fact</u>:

$D \rightsquigarrow \mathcal{L}(D)$ line bundle.

$D \longleftarrow \mathcal{L}$

This correspondence is well-defined, and setting $\deg(\mathcal{L}) = \deg(D)$

This is independent of the choice of D

$\mathcal{L} \longrightarrow D, D' \Rightarrow D' - D = \mathrm{div}(f)$

But $\mathrm{div}(f)$ has degree 0.

We can equally define $\mathrm{Pic}(X)$ and $\mathrm{Pic}^0(X)$ as follows:

$$\mathrm{Pic}(X) := \{\text{Line bundles on } X\} \big/ (\text{isomorphism})$$

$$\mathrm{Pic}^0(X) := \{\mathcal{L} \in \mathrm{Pic}(X) \mid \deg \mathcal{L} = 0\} \big/ \sim .$$

<u>Riemann - Roch Theorem</u>

Euler characteristic $\chi(X, \mathcal{L})$:

$$\chi(X, \mathcal{L}) = \deg(\mathcal{L}) + 1 - g,$$

where g = genus of X.

Take T a connected scheme $/k$.

- $X \times_k T = X \times_{\mathrm{Spec}(k)} T$
- X_t be the fibre of the projection

$$p_T : X \times_k T \longrightarrow T$$

For $\mathcal{L} \in \mathrm{Pic}(X \times_k T)$, then the map

$t \mapsto \chi(X_t, \mathcal{L}_t)$ is locally constant.

$\Longrightarrow$ $\deg(\mathcal{L}_t)$ is independent of t.

Even better, if $T' \longrightarrow T$ is a relative base change, $\deg(\mathcal{L}_t)$ would still be unchanged.

The functor:

$$F(T) := \{\mathcal{L} \in \mathrm{Pic}(X \times T) \mid \deg \mathcal{L}_t = 0 \ \forall t \in T\} \Big/ p_T^* \mathrm{Pic}(T)$$

<u>Theorem</u>. Suppose $X(k) \neq \emptyset$. Then F is representable by an abelian variety of dimension g, called the <u>Jacobian variety of X</u>, denoted by $\mathrm{Jac}(X)$.

The theorem says that there exists a pair $(J, \mathcal{M})$ where J is an abelian variety $/k$, and $\mathcal{M}$ is a line bundle on $X \times J$ such that the following are true:

(a) $\mathcal{M}|_{X \times \{0\}} \cong \mathcal{O}_X$ and $\mathcal{M}|_{\{x\} \times J} \cong \mathcal{O}_J$

(b) $\forall\, T$ (as above), $t \in T$, $\mathcal{L} \in \mathrm{Pic}(X \times T)$ such $\mathcal{L}|_{X \times \{t\}} \cong \mathcal{O}_X$ and $\mathcal{L}|_{\{x\} \times T} \cong \mathcal{O}_T$, there exists a <u>unique</u> morphism $\phi : T \to J$ such that $\phi(t) = 0$ and $\mathcal{L} \cong (1 \times \phi)^* \mathcal{M}$.

<u>Zeta functions of curves</u>

Hasse-Weil-Serre Theorem.

<u>**Proposition**</u> Let X be a complete non-singular over $\mathbb{F}_q$, and $\mathrm{Jac}(X)$ its Jacobian.

Write $f_A = \prod_{i=1}^{2g} (t - \alpha_i)$

(α_i are the roots counted with multiplicity)

For any integer $m \geq 1$,

$$\# X(\mathbb{F}_{q^m}) = 1 - Tr(\pi_J^m) + q^m$$

$$= 1 - \sum_{i=1}^{2g} \alpha_i^m + q^m .$$

<u>Theorem</u>. Let X is a complete nonsingular curve over $\mathbb{F}_q$; $J = Jac(X)$.

$$f_J := \prod_{i=1}^{2g} (t - \alpha_i)$$

Then, we have

(a) $$Z(X;t) = \frac{P_1}{P_0 P_2}, \text{ where}$$

- $P_0 := 1 - t$
- $P_2 := 1 - qt$
- $P_1 := \prod_{i=1}^{2g} (1 - \alpha_i t)$ (reciprocal polynomial of f_J)

(6) $$Z(X;t) = q^{g-1} t^{2g-2} Z\left(X; \frac{1}{qt}\right).$$

<u>Theorem</u>. Let A be an abelian variety of dimension $g/\mathbb{F}_q$. Then, we have

$$|\mathrm{Tr}(\pi_A)| \leq g \lfloor 2\sqrt{q} \rfloor.$$

There is an equality if and only if either

- $\alpha_i + \bar{\alpha_i} = \lfloor 2\sqrt{q} \rfloor, \ \forall i$
- $\alpha_i + \bar{\alpha_i} = -\lfloor 2\sqrt{q} \rfloor, \ \forall i$.

<u>Corollary</u> (H.-W.-S.) Let X be a complete non singular curve $/\mathbb{F}_q$. Then, the number of $\mathbb{F}_q$-rational points of X is bounded by the following inequalities:

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \leq \# X(\mathbb{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$