BUNTES

Ricky Magner
Nov 17, 2017

Abelian Varieties over Finite Fields

Set $q = p^m$, p prime.

Given $X/\mathbb{F}_q$, we have the geometric Frobenius

$$\pi_X : X \longrightarrow X$$

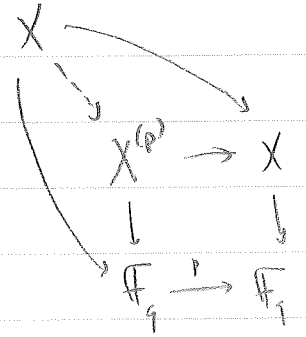
which acts as id on $|X|$ and sends $f \mapsto f^q$ for $f \in \mathcal{O}_X(U)$.

eg. $X \hookrightarrow \mathbb{P}^N_{\mathbb{F}_q}$, then

$$\pi_X((a_0 : \cdots : a_N)) = (a_0^q : \cdots : a_N^q)$$

Have absolute Frobenius, $F : X \longrightarrow X^{(p)}$

$$\left(\text{eg.} \quad \begin{array}{l} X : y^2 = x^3 + i \quad /\mathbb{F}_q \\ X^{(3)} : y^2 = x^3 + i^3 = x^3 - i \end{array} \right)$$



We see that $X^{(p^m)} = X$ and $F^m = \pi_X$.

If $f: X \to Y$ of $\mathbb{F}_q$-schemes, then $\pi_Y \circ f = f \circ \pi_X$.

Now: Let X be an abelian variety over $\mathbb{F}_q$.

By the above, we have π_X commutes with all elements of $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbb{Q}$

Let f_X be the characteristic polynomial of $T_\ell(\pi_X): V_\ell(X) \to V_\ell(X)$ $(\ell \neq p)$.

(Alt dfn: $f_X \in \mathbb{Z}[x]$ monic of deg $2g$, $g = \dim(X)$ such that $f_X(n) = \deg([n] - \pi_X)$.
See 12.18.)

Prop 16.3: Assume X is elementary (i.e. X is isogenous to A^n for A simple).
Then $\mathbb{Q}[\pi_X] \subseteq \mathrm{End}^0(X)$ is a field and f_X is a power of the minimal polynomial of π_X over $\mathbb{Q}$.

Pf: Since X is elementary, $Z(\mathrm{End}^0(X))$ is a field containing $\mathbb{Q}[\pi_X]$.
Let g be the minimal polynomial of π_X over $\mathbb{Q}$.
Let α be a root of f.
Then $g(\alpha)$ is an eigenvalue of $g(V_\ell(\pi_X)) = V_\ell(g(\pi_X)) = V_\ell(0) = 0$

Hence $g(\alpha) = 0$. □

Theorem 16.4

Let $g = \dim(X)$.

(i) Every root of f_X satisfies $|\alpha| = \sqrt{q}$

(ii) If α is a root of f_X, then $\bar{\alpha}$ is a root with the same multiplicity.

In particular, if $\alpha = \pm\sqrt{q}$ is real, then it occurs with even multiplicity.

We need some facts before proving this (ref 5.20, 5.21):

- There exists $V : X^{(p)} \longrightarrow X$ such that $V \circ F = [p]_X$, $F \circ V = [p]_{X^{(p)}}$.
  Using $\deg F = p^g$, get $\deg V = p^g$.
- By induction, $V^m \circ F^m = [p^m]$
  $$V^{m+1} \circ F^{m+1} = V \circ (V^m \circ F^m) \circ F$$
  $$= V \circ [p^m] \circ F = [p^m] \circ [p] = [p^{m+1}]$$

We also need facts about F and V relative to $X^\vee$ (ref 7.33, 7.34).

$$F_X^\vee = V_{X^\vee} : (X^\vee)^{(p)} \longrightarrow X^\vee \quad \text{(identifying } (X^\vee)^{(p)} = (X^{(p)})^\vee\text{)}.$$

Pf of thm 16.4:

(i) Reduce to the case where X is simple.

We have an isogeny $h : X \longrightarrow X_1 \times \cdots \times X_s$ with X_i simple.

Then h induces an isomorphism $h: V_\ell(X) \xrightarrow{\sim} \bigoplus_i V_\ell(X_i)$

So $f_X = f_{X_1} f_{X_2} \cdots f_{X_s}$.

Hence we can assume X is simple.

Let $\lambda: X \longrightarrow X^\vee$ be a polarisation of X, and $\cdot^\dagger$ be the corresponding Rosati involution on $\mathrm{End}^0(X)$.
We will show that

$$\pi_X \cdot \pi_X^\dagger = q.$$

$$\begin{aligned} \pi_X \pi_X^\dagger &= \pi_X \cdot \lambda^{-1} \cdot \pi_X^\vee \cdot \lambda \\ &= \lambda^{-1} \cdot \pi_{X^\vee} \pi_X^\vee \cdot \lambda \qquad (\text{since } \pi_X \in Z(\mathrm{End}^0(X))). \\ &= \lambda^{-1} q \cdot \lambda \\ &= q \end{aligned}$$

To see $\pi_{X^\vee} \pi_X^\vee = q$, recall $\pi_X = F_X^m$.
Then $\pi_X^\vee = (F_X^m)^\vee = (F_X^\vee)^m = V_{X^\vee}^m$.
So

$$\pi_X \pi_X^\vee = F_{X^\vee}^m V_{X^\vee}^m = [p^m]$$

As X is simple, $\mathbb{Q}[\pi_X]$ is a field.
Thus f_X is a power of $g :=$ min poly of π_X / $\mathbb{Q}$.
So the complex roots of f_X are

$$\iota(\pi_X) \text{ for every embedding } \iota: \mathbb{Q}[\pi_X] \longrightarrow \mathbb{C}$$

Since $\pi_X^\dagger = q/\pi_X$, we see that $\mathbb{Q}[\pi_X] \subseteq \mathrm{End}^0(X)$ is stable under $\dagger$.

We have two cases for such a $K = \mathbb{Q}(\pi_x)$

(a) K is a totally real field, and $\cdot^\dagger = id$

(b) K is a CM field, and $\cdot^\dagger = \overline{\cdot}$.

Hence, we get $\iota(\pi_x \cdot \pi_x^\dagger) = \iota(\pi_x)\overline{\iota(\pi_x)} = q$

for any $\iota : K \hookrightarrow \mathbb{C}$.

(iii) If $\pm\sqrt{q}$ is a root of f_x, then we are in the case K totally real.

If $\sqrt{q}$ has multiplicity n, then $-\sqrt{q}$ has multiplicity $2g-n$.

Thus $f_x(0) = (-1)^n q^g$.

However, we also have $f_x(0) = \deg(0 - \pi_x) = q^g$.

Thus n is even. □

Our goal for future talks:

Theorem [Honda-Tate]

We have a bijection

$$\{\text{isogeny classes of } X/\mathbb{F}_q\} \longleftrightarrow \{\text{conjugacy classes of } q\text{-Weil numbers}\}$$

where

q-Weil numbers are algebraic integers α such that $|\iota(\alpha)| = \sqrt{q}$ for all $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.

Using a relation between a curve $C/\mathbb{F}_q$ and its Jacobian $J(C)$, one can show:

Theorem [Hasse-Weil-Serre bound]

$$q^n+1 - g\lfloor 2\sqrt{q}\rfloor \leq \#C(\mathbb{F}_{q^n}) \leq q^n+1 + g\lfloor 2\sqrt{q}\rfloor \quad \text{where } g=g(C).$$

Proof hint: Use Lefschetz trace formula and the fact

$$H^1(C, \mathbb{Q}_\ell) \simeq H^1(J(C), \mathbb{Q}_\ell).$$

□

Application

Let $J = J_0(103) = J(X_0(103))$

Let w be the Atkin-Lehner involution.

Then

$$J \sim J_+ \times J_- \quad \text{where} \quad J_\pm = \mathrm{Im}(w \pm id)$$

$$\dim(J) = 8 \quad \text{and} \quad \dim(J_-) = 6.$$

In fact, $\exists f \in S_2(\Gamma_0(103))$ an eigenform such that if $f = \sum_{n=1}^{\infty} a_n q^n$ then $[K = \mathbb{Q}(a_n)_{n\geq 1} : \mathbb{Q}] = 6$ and

$$\mathrm{Tr}\left(F_{J_-,p}; T_\ell(J_-)\right) = \mathrm{Tr}_{K/\mathbb{Q}}(a_p) \quad \text{for } \ell \neq p,\ p \neq 103$$

We can compute $\mathrm{Tr}_{K/\mathbb{Q}}(a_2) = 4$

This implies that $J_- \times \mathbb{F}_2$ is not the Jacobian of a curve over $\mathbb{F}_2$.

If it were, i.e. $J_- \times \mathbb{F}_2 = J(C)$, then

$$\#C(\mathbb{F}_2) = 2+1-4 = -1, \quad \text{contradiction!} \qquad (*)$$

A similar thing works at 17.

Note: $(*)$ follows from $\#C(\mathbb{F}_{q^n}) = \sum (-1)^i \mathrm{Tr}(F | H^i(C))$.

$$= 1 + q^n - \mathrm{Tr}(F | V_e J(C))$$