BUNTES

Sachi Hashimoto
Dec 1, 2017

Tate's Isogeny Theorem

Theorem [Tate]

Let A, B be abelian varieties over a finite field $k = \mathbb{F}_q$, and let $\ell \neq \mathrm{char}(\mathbb{F}_q)$ be a prime.
Let $G = \mathrm{Gal}(k^s/k)$.
Then

$$\mathrm{Hom}_k(A,B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_G(T_\ell A, T_\ell B)$$
$$= \left(\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)\right)^G$$

is an isomorphism. where G acts by $(gf)(x) = g \cdot f(g^{-1}(x))$

Remark: Tate's theorem is also true for function fields over finite fields (Zarhin) and fields that are finitely generated over their prime fields, like number fields (Faltings).

Motivation: Let π_A and π_B be the (relative) Frobenius endomorphisms $(x \mapsto x^q)$ on $V_\ell(A)$, $V_\ell(B)$:

$$\mathrm{Hom}_k(A,B) \otimes \mathbb{Q}_\ell \longrightarrow \mathrm{Hom}_G(V_\ell(A), V_\ell(B))$$

P_A, P_B characteristic polynomials of π_A, π_B.

Tate Weil Conjectures: P_A, P_B have $\mathbb{Z}$-coefficients, and they don't depend on the choice of ℓ.

Provided the induced action of Frob are semisimple, we can find a number $r(P_A, P_B)$ which computes $\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_G(V_\ell A, V_\ell B)$.

Tate $\Rightarrow$ $r(P_A, P_B) = \mathrm{rank}\ \mathrm{Hom}_k(A, B)$

Corollary: Let A, B be abelian varieties over $\mathbb{F}_q$, and P_A, P_B as above.

(a) $\mathrm{rank}\ \mathrm{Hom}_k(A, B) = r(P_A, P_B)$

(b) TFAE

(i) B is k-isogenous to an abelian subvariety of A.

(ii) $V_\ell B$ is G-isomorphic to a G-subrepresentation of $V_\ell A$ for $\ell \neq \mathrm{char}(k)$

(iii) $P_B \mid P_A$

Pf: (bii) $\Rightarrow$ (bi): $\alpha : V_\ell B \hookrightarrow V_\ell A$

Tate $\otimes \mathbb{Q}_\ell \Rightarrow$ Find $u \in \mathrm{Hom}_k(B, A) \otimes \mathbb{Q}_\ell$ such that $V_\ell(u) = \alpha$.

Now choose u' in $\mathrm{Hom}_k(B, A) \otimes \mathbb{Q}_\ell$ arbitrarily close to u.

Lower semicontinuity $\Rightarrow$ If $V_\ell(u')$ is close enough to α, can ensure $V_\ell(u')$ is injective

Multiply by scalars to get $u'' \in \mathrm{Hom}_k(B, A)$

Since $T_\ell u''$ is injective, then u'' is an isogeny to an abelian subvariety.

This follows since $2\dim \ker(u) = \dim(V_\ell(\ker u)) = \dim(\ker(V_\ell u))$. $\square$

Recall: The Isogeny Category

Theorem [Poincaré Reducibility]

Let A be an abelian variety, B an abelian subvariety.
There exists C an abelian subvariety such that $B \cap C$ is finite and there exists an isogeny

$$B \times C \longrightarrow A.$$

Corollary: Up to isogeny, all abelian varieties are a product of simple abelian varieties.

"General Nonsense": A category Isog, objects: abelian varieties

morphisms: $\mathrm{Hom}_{\mathrm{Isog}}(A,B) = \mathrm{Hom}_{\mathrm{AV}}(A,B) \otimes \mathbb{Q}$

Recall: Given $f: A \longrightarrow B$ an isogeny, there exists an isogeny $g: B \longrightarrow A$ and $n \in \mathbb{Z}_{\geq 0}$ such that

$$gf = [n].$$

$\Rightarrow \frac{1}{n} g$ is an inverse for f in Isog

$\Rightarrow$ isogenies are isomorphisms in Isog.

Poincaré Reducibility $\Rightarrow$ Isog is a semisimple abelian category, where the simple objects are simple abelian varieties.

① Decomposition into a product of simple AVs is unique (up to isogeny)

② If A is simple, $\mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$

Reason: If A is simple in a semisimple abelian category and $\mathrm{End}(A) \supseteq k$ a field, then $\mathrm{End}(A)$ is a division algebra.

Reductions

Lemma: ① $\mathbb{Z}_\ell \otimes \mathrm{Hom}_{AV}(A,B) \xrightarrow{(*)} \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$ is an isomorphism

$\iff$

$\mathbb{Q}_\ell \otimes \mathrm{Hom}_{AV}(A,B) \xrightarrow{(**)} \mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell A, V_\ell B)$ is an isomorphism.

② If for every C, $\mathbb{Q}_\ell \otimes \mathrm{End}_{AV}(C) \xrightarrow{(***)} \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell C)$ is an isomorphism, then $(**)$ is an isomorphism for every pair A, B.

Proof: (i) $(*)$ is always injective.

$\operatorname{coker}(*)$ is torsion-free $\Rightarrow$ free.

It's an isogeny iff $\mathbb{Q}_\ell \otimes \operatorname{coker}(*) = 0$.

$\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$, so $(**)$ is injective, and

$\operatorname{coker}(**) = \mathbb{Q}_\ell \otimes \operatorname{coker}(*)$.

(ii) $C = A \times B$

Then

$$\begin{array}{ccccccccc} \mathrm{End}^0(C) & = & \mathrm{End}^0(A) & \oplus & \mathrm{Hom}^0(A,B) & \oplus & \mathrm{Hom}^0(B,A) & \oplus & \mathrm{End}^0(B) \\ \downarrow (***) & & \| & & \| & & \| & & \| \\ \mathrm{End}_G(V_\ell C) & = & \mathrm{End}_G(V_\ell A) & \oplus & \mathrm{Hom}_G(V_\ell A, V_\ell B) & \oplus & \mathrm{Hom}_G(V_\ell B, V_\ell A) & \oplus & \mathrm{End}_G(V_\ell B) \end{array}$$

In particular, if $(***)$ is an isomorphism, then so are the rest. □

A further reduction, let

$$E_\ell = \mathrm{End}_k(A) \otimes \mathbb{Q}_\ell \subseteq \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$$

$$F_\ell = \mathbb{Q}_\ell[G] \subseteq \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A), \quad \text{automorphisms of } V_\ell A \text{ coming from } G.$$

Note: E_ℓ are the k-rational endomorphisms, so they commute with the Galois action, so

$$F_\ell \subseteq C_{\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)}(E_\ell) \qquad \text{(the centralizer)}$$

Want: $F_\ell = C_{End_{\mathbb{Q}_\ell}(V_\ell A)}(E_\ell)$

Lemma: (i) $(***)$ is an isomorphism iff

$$C(C(E_\ell)) = End_{\mathbb{Q}}(V_\ell A)$$

(ii) If F_ℓ is semisimple, $(***)$ is an isomorphism $\iff C(E_\ell) = F_\ell$.

Proof: (i) The Double Centralizer Theorem states that if E_ℓ is semisimple, then $C(C(E_\ell)) = E_\ell$.

Poincaré reducibility $\Rightarrow A \overset{\text{isogeny}}{\sim} \prod_i A_i^{m_i}$

$$\Rightarrow End^\circ(A) = End^\circ\left(\prod_i A_i^{m_i}\right) = \prod_i End^\circ\left(A_i^{m_i}\right)$$

$$= \prod_i Mat_{m_i}\left(\underbrace{End^\circ(A_i)}_{\text{finite dim division algebra over } \mathbb{Q}}\right)$$

A matrix algebra over a division algebra is semisimple.

(ii) If F_ℓ is semisimple, $C(E_\ell) = F_\ell \iff E_\ell = C(C(E_\ell))$ (?)

$$\| \qquad\qquad (?)$$

$$C(F_\ell) = End_{\mathbb{Q}}(V_\ell A)$$

□

Proof of Tate using finiteness:

We will prove the theorem under the following hypothesis

$\mathrm{Hyp}(k, A, \ell)$: There exist only finitely many (up to k-isomorphism) abelian varieties B such that there is a k-isogeny of ℓ-power degree from $B \to A$.

Let $D = C(E_\ell)$.

Want to show: $C(D) = \mathrm{End}_G(V_\ell A)$

Certainly $C(D) \subseteq E_\ell \subseteq \mathrm{End}_G(V_\ell A)$

Want $C(D) \supseteq \mathrm{End}_G(V_\ell A)$.

Let $\alpha \in \mathrm{End}_G(V_\ell A)$.

We will show this commutes with anything in D.

Equivalently, let W be the graph of α,

$$W := \{ (x, \alpha x) \in V_\ell(A \times A) \} \subseteq V_\ell(A \times A)$$

[Note: $g \in G$ acts by $g \cdot (x, \alpha x) = (gx, g(\alpha x)) = (gx, \alpha(gx))$.]

$\alpha \in C(D) \iff \forall x \in V_\ell(A)$ and $d \in D$, $\alpha d x = d \alpha x$

$\iff (d \oplus d) W \subseteq W \quad \forall d \in D$

since this states $(dx, d\alpha x) = (dx, \alpha dx)$.

[Technical Lemma: If $W \subseteq V_\ell(A)$ is a G-stable subspace, then there exists $u \in E_\ell$ such that $u V_\ell(A) = W$.]

Applying this to $V_\ell(A \times A)$, W we see

$$\begin{aligned}(d \oplus d) W &= (d+d) u V_\ell(A \times A) \\ &= u(d+d) V_\ell(A \times A) \subseteq u V_\ell(A \times A) = W\end{aligned}$$

Thus $C(D) \geq \mathrm{End}_G(V_\ell A)$ □

Proof of Technical Lemma: For $n \in \mathbb{Z}_{\geq 0}$, let $U_n = (W \cap T_\ell A) + \ell^n T_\ell A$, which is a G-stable lattice in $V_\ell A$.

$$\ell^n T_\ell A \subseteq U_n \subseteq T_\ell A$$

Let $K_n \subseteq A[\ell^n](k^s) = T_\ell A / \ell^n T_\ell A$ be the image of U_n.

K_n is stable under G-action on $A[\ell^n](k^s)$

$\Rightarrow K_n = K_n(k^s)$

Let $\pi_n : A \longrightarrow B_n := A/K_n$.

Let $\iota_n : B_n \longrightarrow A$ be the unique isogeny such that $\iota_n \circ \pi_n = [\ell^n]_A$.

Then $T_\ell B \simeq U_n$ as $\mathbb{Z}_\ell$-modules with G-action.

As $T_\ell(z_n) : U_n = T_\ell B \longrightarrow T_\ell A$ is the inclusion map, assuming $\mathrm{Hyp}(k, A, \ell)$, we can find $n = n_1 < n_2 < \cdots$ such that we have isomorphisms $\alpha_i : B_i \xrightarrow{\sim} B_i$

$$\begin{array}{ccc} B_n & \xrightarrow[\alpha_i]{\sim} & B_{n_i} \\ {\scriptstyle \pi_n}\uparrow\downarrow{\scriptstyle z_n} & & \downarrow{\scriptstyle z_{n_i}} \\ A & \xrightarrow{u_i} & A \end{array}$$

$u_i = z_{n_i} \circ \alpha_i \circ \pi_n$ is an endomorphism of A.

On Tate modules, $T_\ell(u_i)$ is the induced map

$$T_\ell A \xrightarrow{[\ell^n]} U_n \xrightarrow{T_\ell \alpha_i} U_{n_i} \longrightarrow T_\ell A$$

Because $\mathbb{Z}_\ell \otimes \mathrm{End}\, A$ is a free $\mathbb{Z}_\ell$-module of finite rank, it's compact in the ℓ-adic topology.
$\Rightarrow$ Subsequence of u_i converges to some u in $\mathbb{Z}_\ell \otimes \mathrm{End}\, A$.

$$U_{n_1} \supseteq U_{n_2} \supseteq U_{n_3} \supseteq \cdots$$

The endomorphism $T_\ell(u)$ maps $T_\ell A$ to $\bigcap_{i=1}^{\infty} U_{n_i} = W \cap T_\ell A$

Passing to $\mathbb{Q}_\ell$-coefficients, note $\mathbb{Q}_\ell(W \cap T_\ell A) = \mathbb{Q}_\ell(\ell^n(W \cap T_\ell A)) = W$.

So $\mathrm{image}(V_\ell(u)) = W$. □

Why does $\mathrm{Hyp}(k, A, \ell)$ hold?

Fact: There exists a moduli space of d-polarized abelian varieties of dimension g $\mathcal{A}_{g,d}$ which is a stack of finite type $/k$.

$$\mathcal{A}_{g,d}(k) = \left\{ (A, \lambda) \;\middle|\; \begin{array}{l} A \text{ is an abelian variety } /k, \\ \lambda : A \longrightarrow A^\vee, \text{ deg } d \text{ polarization} \end{array} \right\}$$

Zarhin's trick: Given an abelian variety A, $(A \times A^\vee)^4$ is principally polarized.

Finiteness of direct factors $B \subseteq A$, $A \simeq B \times C$.

Corollary: If $k = \mathbb{F}_q$, there exists only finitely many non isogenous abelian varieties of dimension g.

Proof: A is a direct factor of $(A \times A^\vee)^4 \in \mathcal{A}_{8g,1}$. □