ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 3

SANTIAGO ARANGO-PIÑEROS, SEOKHYUN CHOI, ALICE LIN, YUXIN LIN, AND MINGJIA ZHANG

Instructions: The goal of this problem set is to assimilate Tate's isogeny theorem [Tat66, Main Theorem]. Problems marked ($\star$), ($\star\star$), and ($\star\star\star$) denote beginner, intermediate, and advanced problems, respectively.

Notation: As customary, p will be a prime, and q will be a power of p. We use ℓ to denote a prime, usually different from p. For a field K, we will use G_K to denote the absolute Galois group of K.

Problem 1 ($\star$)
Let A and B be abelian varieties over a field k. Choose a prime $\ell \neq \operatorname{char} k$, and let $T_\ell A$ and $T_\ell B$ be their ℓ-adic Tate modules.

(1) Define a natural map
$$T_\ell : \operatorname{Hom}(A, B) \to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B).$$
(2) Show this map is injective.[a]

[a] Hint: Prove this first in the case that A is a simple abelian variety.

Problem 2 ($\star\star$)
Let A, B be simple abelian varieties over a field k. Choose a prime $\ell \neq \operatorname{char} k$. We will show that the natural map
$$\operatorname{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \operatorname{Hom}(T_\ell(A), T_\ell(B))$$
$$\alpha \otimes c \mapsto cT_\ell\alpha$$
is injective, using the following steps.

(1) Let $M \subset \operatorname{Hom}(A, B)$ be a finitely generated subgroup. Let
$$M^{div} := \{\phi \in \operatorname{Hom}(A, B) \ : \ [m] \circ \phi \in M \text{ for some integer } m \geq 1\}.$$
Consider the finite-dimensional vector space $M \otimes \mathbb{R}$ with the natural Euclidean topology from $\mathbb{R}$, and linearly extend the degree mapping on M to $M \otimes \mathbb{R}$. By considering $M^{div} \subset M \otimes \mathbb{R}$, show that M^{div} is a discrete subgroup of $M \otimes \mathbb{R}$.[a] Deduce that M^{div} is finitely generated.
(2) Show that $\operatorname{Hom}(A, B)$ is torsion-free as a $\mathbb{Z}$-module.
(3) Take $\phi \in \operatorname{Hom}(A, B) \otimes \mathbb{Z}_\ell$, and suppose that $T_\ell\phi = 0$. Take $M \subset \operatorname{Hom}(A, B)$ be a finitely generated subgroup such that $\phi \in M \otimes \mathbb{Z}_\ell$. Show that M^{div} is a free finitely generated $\mathbb{Z}$-module, so that we can choose a $\mathbb{Z}$-basis $\{\psi_1, \ldots, \psi_r\}$ of M^{div} and uniquely write ϕ as
$$\phi = \alpha_1\psi_1 + \cdots + \alpha_r\psi_r, \quad \text{for } \alpha_i \in \mathbb{Z}_\ell.$$
(4) Fix $n \geq 1$, and choose $a_1, \ldots, a_r \in \mathbb{Z}$ such that $a_i \cong \alpha_i \bmod \ell^n$ for $i = 1, \ldots, r$. Show that
$$\psi := [a_1] \circ \psi_1 + \cdots + [a_r] \circ \psi_r \in \operatorname{Hom}(A, B)$$
annihilates the subgroup $A[\ell^n]$. Deduce that ψ factors as $\psi = [\ell^n] \circ \lambda$ for some $\lambda \in \operatorname{Hom}(A, B)$.
(5) Deduce that $\lambda \in M^{div}$, and show that $\ell^n \mid a_i$ for $i = 1, \ldots, r$. Since the choice of n was arbitrary, conclude that $\alpha_i = 0$ for $i = 1, \ldots, r$, and thus that $\phi = 0$.

[a] Hint: Find an open neighborhood U of $0 \in M \otimes \mathbb{R}$ which does not contain any nontrival element of M^{div}.

Problem 3 ($\star$)
Combine Problem 2 with PSET 1, Problem 7 to deduce an upper bound on $\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(A, B)$ for abelian varieties A, B over a field k.

Problem 4 ($\star\star$)
(1) Let A be an abelian variety. Suppose the endomorphism algebra $\operatorname{End}^0(A)$ contains a number field K. Let $g = \dim A$ and $f = [K : \mathbb{Q}]$. Show that $V_\ell A := T_\ell A \otimes \mathbb{Q}_\ell$ is a free $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank $2g/f$.
(2) Let E/K be an elliptic curve with complex multiplication over a number field K. Show that for all primes ℓ, the action of G_K on $V_\ell E$ is abelian. In other words, the image of the ℓ-adic representation $\rho_{\ell^\infty} : G_K \to \operatorname{Aut}(V_\ell E)$ is abelian.

Problem 5 ($\star\star$)
Let A, B be abelian varieties defined over $\mathbb{F}_q$. Let ℓ be a prime not dividing q. We have seen that the map

$$\operatorname{Hom}(A, B) \to \operatorname{Hom}_{G_{\mathbb{F}_q}}(T_\ell A, T_\ell B) \tag{0.1}$$

is injective. Tate's Isogeny Theorem states that it is also surjective.
Let $V_\ell A := T_\ell A \otimes \mathbb{Q}_\ell$ be the Tate $\mathbb{Q}_\ell$-vector space.
(1) Show that Tate's Isogeny Theorem is equivalent to the bijectivity of

$$\operatorname{Hom}(A, B) \otimes \mathbb{Q}_\ell \to \operatorname{Hom}_{G_{\mathbb{F}_q}}(V_\ell A, V_\ell B). \tag{0.2}$$

(2) Show that bijectivity of Equation 0.2 is equivalent to the bijectivity of

$$\operatorname{End}(A) \otimes \mathbb{Q}_\ell \to \operatorname{End}_{G_{\mathbb{F}_q}}(V_\ell A) \tag{0.3}$$

for every abelian variety $A/\mathbb{F}_q$.
(3) Consider now the commuting subalgebras of $\operatorname{End}_{G_{\mathbb{F}_q}}(V_\ell A)$ defined by
- E_ℓ is the image of $\operatorname{End}(A) \otimes \mathbb{Q}_\ell$ by Equation 0.3, and
- F_ℓ is the subalgebra of $\operatorname{End}_{G_{\mathbb{F}_q}}(V_\ell A)$ generated by the automorphisms of $V_\ell A$ induced by $G_{\mathbb{F}_q}$.

Prove that if F_ℓ is semisimple, the bijectivity of Equation 0.3 is equivalent to the fact that F_ℓ is the commutant of E_ℓ in $\operatorname{End}(V_\ell A)$.

Here, we will prove some consequences of Tate's Isogeny Theorem, as proved in [Tat66].

Problem 6 ($\star\star\star$)
Let A and B be abelian varieties over a finite field $\mathbb{F}_q$, and let $P_A(T)$ and $P_B(T)$ be the characteristic polynomials of the q-Frobenius endomorphisms ϕ_A and ϕ_B, acting on the corresponding ℓ-adic Tate modules.
(1) Let α and β be absolutely semisimple endomorphisms of two finite-dimensional vector spaces V and W over a field K with characteristic polynomials $P_\alpha(T)$ and $P_\beta(T)$. Factor $P_\alpha(T)$ and $P_\beta(T)$ as products of powers of distinct monic irreducible polynomials $f(T) \in K[T]$.

$$P_\alpha(T) = \prod_f f(T)^{m(f)}, \quad P_\beta(T) = \prod_f f(T)^{n(f)}.$$

Show that the vector space

$$U := \{\psi \in \operatorname{Hom}_K(V, W) \mid \psi \circ \alpha = \beta \circ \psi\}$$

has dimension

$$r(P_\alpha, P_\beta) := \sum_f m(f) n(f) \deg f.$$

(2) Apply item 1 together with Tate's isogeny theorem to conclude that

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{F}_q}(A, B) = r(P_A, P_B).$$

(3) Show that the following are equivalent:
   (a) B is $\mathbb{F}_q$-isogenous to an abelian subvariety of A defined over $\mathbb{F}_q$.
   (b) For some ℓ, $V_\ell B$ is isomorphic to a sub-$G_{\mathbb{F}_q}$-representation of $V_\ell(A)$.
   (c) $P_B(T)$ divides $P_A(T)$.

(4) Show that the following are equivalent.
   (a) A and B are $\mathbb{F}_q$-isogenous.
   (b) $P_A(T) = P_B(T)$.
   (c) The zeta functions of A and B are equal.
   (d) $\#A(\mathbb{F}_{q^n}) = \#B(\mathbb{F}_{q^n})$ for every $n \geq 1$.

References

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 206004