ABELIAN VARIETIES OVER FINITE FIELDS: PROBLEM SET 2

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]. To this end, we review some crucial background and play around with important constructions. Problems marked $(\star)$, $(\star\star)$, and $(\star\star\star)$ denote beginner, intermediate, and advanced problems, respectively. For the computational problems (⌨) you may use CoCalc or MAGMA's online calculators.

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.

Remark. We don't expect you to solve all the problems in a week. Choose the ones that seem interesting, and save the rest for later!

1. BACKGROUND PROBLEMS

If this is your first encounter with the p-adics, it is worth to spend some time with Problem 1.

Problem 1 $(\star)$

Let p be a prime, and define the *p-adic valuation* $v_p \colon \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ by the unique factorization property of the integers; that is:
$$a = \prod_p p^{v_p(a)}, \text{ for } a \neq 0.$$
In other words, $v_p(a)$ is the largest power of p dividing a, and put $v_p(0) := \infty$. We extend the p-adic valuation to $\mathbb{Q}$ in the usual way by letting $v_p(a/b) := v_p(a) - v_p(b)$ for integers a, b. In this problem, we will establish some of the main properties of v_p.

(1) Show that $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a non-archimedean valuation. That is, prove that:
    (a) $v_p(x) = \infty$ if and only if $x = 0$.
    (b) $v_p(xy) = v_p(x) + v_p(y)$ for every $x, y \in \mathbb{Q}$.
    (c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ for every $x, y \in \mathbb{Q}$.
    (d) $v_p(x + y) = \min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$.

(2) Define the *p-adic absolute value* $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ by $|x|_p := p^{-v_p(x)}$. Show that $|\cdot|_p$ is a non-archimedean absolute value. That is, prove that:
    (a) $|x|_p = 0$ if and only if $x = 0$.
    (b) $|xy|_p = |x|_p |y|_p$ for every $x, y \in \mathbb{Q}$.
    (c) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$ for every $x, y \in \mathbb{Q}$.

(3) Denote by $|\cdot|_\infty$ the usual absolute value of $\mathbb{Q}$. Prove the product formula:
$$|x|_\infty \cdot \prod_p |x|_p = 1, \text{ for any } x \in \mathbb{Q}^\times.$$

(4) Notice that each for each prime $p \leq \infty$, the p-adic absolute value defines a metric on $\mathbb{Q}$ (for $p = \infty$ this is the usual euclidean distance on the rationals). Intuitively, we say a rational number is p-adically small if it is "very" divisible by p. Show that $(\mathbb{Q}, |\cdot|_p)$ is not a complete metric space. That is, give an example of a Cauchy sequence that does not converge in $\mathbb{Q}$.

(5) Show that for two different primes[a] p and ℓ, the identity is not a homeomorphism between $(\mathbb{Q}, |\cdot|_p)$ and $(\mathbb{Q}, |\cdot|_\ell)$.

---

(6) Just as how $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|_\infty$, we define $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. $\mathbb{Z}_p$ is the unit interval of $\mathbb{Q}_p$; that is

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Show that $\mathbb{Z}_p$ is compact and an integral domain.
(7) Convince yourself that you understand why $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

---

[a]Including the prime at infinity!

The next problem allows you to get your hands on some 5-adic numbers. You might want to reflect on Hensel's lemma.

Problem 2 ($\star$)
Show that -1 is a square in $\mathbb{Q}_5$. Manually calculate one of the square roots to 3 digits of 5-adic precision. (⌨) Use your favorite computer algebra system to calculate both roots to 100 digits of 5-adic precision.

The following problem introduces key concepts and theorems about semisimple algebras, as needed in the proof of Tate's isogeny theorem.

Problem 3 ($\star\star$)
Let K be a field. A K-algebra over K is called semi-simple if any left ideal admits a direct complement. By a central simple algebra over K, we mean a finite-dimensional K-algebra which is simple and for which the center is exactly K. By a central division algebra, we mean a central simple algebra which is also a division algebra.
(1) Show that a matrix algebra over K is a central simple algebra. If a central simple algebra is isomorphic to a matrix algebra, then we say that it is a split central simple algebra.
(2) (Wedderburn's theorem) Show that every central simple algebra is isomorphic to a matrix algebra of some central division algebra.
(3) (Skolem-Noether theorem) Show that every automorphism of a central simple algebra is an inner automorphism.
(4) (Double centralizer theorem) Let A be a semisimple subalgebra of a finite dimensional central simple algebra B over a field K. Then, show that

$$C_B(C_B(A)) = A.$$

Also show the dimension formula

$$[B : K] = [A : K][C_B(A) : K].$$

(5) Assume that A is a semisimple algebra over a field K, with a finite-dimensional faithful representation V over K. Then, show that

$$C_{\mathrm{End}(V)}(C_{\mathrm{End}(V)}(A)) = A.$$

(6) Let A be a central division algebra over K. Use the double centralizer theorem to show that $[A : K]$ is a square. If A is a division algebra over $\mathbb{Q}$, we can define its reduced degree over $\mathbb{Q}$ as $[A : \mathbb{Q}]_{\mathrm{red}} := [A : \mathcal{Z}(A)]^{\frac{1}{2}}[\mathcal{Z}(A) : \mathbb{Q}]$, where $\mathcal{Z}(A) = C_A(A)$ is the center of A.

In the next problem we classify central simple algebras over local fields using the cohomological interpretation of the Brauer group.

Problem 4 ($\star\star\star$)
Let K be a field. Recall that a central simple algebra over K is a simple K-algebra with center equal to K. Let $\mathrm{Br}(K)$ be the Brauer group over K, the group[a] of equivalence classes of central simple algebras over K. For any field extension L/K, let $\mathrm{Br}(L/K)$ denote the subgroup of classes of central simple algebras over K that split over L. That is, $[B] \in \mathrm{Br}(K)$ is in $\mathrm{Br}(L/K)$ if and only if $B \otimes_K L \cong M_n(L)$ for some

$n \geq 1$. We have a functorial isomorphism
$$\varphi_K : \mathrm{Br}(K) \cong H^2(G_K, (K^{\mathrm{sep}})^{\times})$$
inducing an isomorphism
$$\varphi_{L/K} : \mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^{\times}),$$
for any finite separable extension L/K. Furthermore, $\varphi_K([A \otimes_K B]) = \varphi_K(A) + \varphi_K(B)$.

(1) Show that $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and that the non-trivial element can be represented by $\mathbb{H}$; Hamilton's original quaternion algebra over $\mathbb{R}$. We define the Hasse-invariant of the representatives such that $\mathrm{inv}_{\infty}([\mathbb{R}]) = 0$ and $\mathrm{inv}_{\infty}([\mathbb{H}]) = \frac{1}{2}$.

Now let K_v be a non-archimedean local field. We can describe the composition
$$\mathrm{inv}_v : \mathrm{Br}(K_v) \cong H^2(G_{K_v}, (K_v^{\mathrm{un}})^{\times}) \cong \mathbb{Q}/\mathbb{Z}$$
as follows. Given a central division algebra D over K_v, let $K_v \subseteq L \subseteq D$ be its maximal subfield. L is an unramified extension of K_v of degree $n := [D : K_v]^{\frac{1}{2}}$.

(2) Let $\sigma \in \mathrm{Gal}(L/K_v)$ be the q-Frobenius automorphism on L, where q is the size of the residue field of K_v. Use the Skolem-Noether theorem to show that there exists $\alpha \in D$, unique up to a multiple in L, such that for every $\beta \in L, \sigma(\beta) = \alpha\beta\alpha^{-1}$.

(3) Let π be a uniformizer of K_v. Show that $\alpha^n = u\pi^r$ for some $u \in \mathcal{O}_L^{\times}$ and $r \in \mathbb{Z}$. Then we define the Hasse-invariant of D to be $\mathrm{inv}_v(D) := r/n \mod \mathbb{Z}$. Show that $\mathrm{inv}_v(D)$ is well-defined. That is, it does not depend on the choice of α.

(4) Let $\mathbb{Q}_{p^h}$ be the unique unramified extension of $\mathbb{Q}_p$ of degree h. For a pair of integers (m, h) such that $h \geq 1, m \geq 0, \gcd(h, m) = 1$, consider $D_{p,h,m}$. It is the division algebra generated by $\mathbb{Q}_{p^h}$ and an element α, with multiplication defined such that for $\beta \in \mathbb{Q}_{p^h}, \alpha\beta = \beta^{\sigma}\alpha$, and $\alpha^h = p^m$. Here, $\sigma \in \mathrm{Gal}(\mathbb{Q}_{p^h}/\mathbb{Q}_p)$ is the p-Frobenius automorphism of $\mathbb{Q}_{p^h}$.

   (a) Verify that $D_{p,h,m}$ is a central division algebra over $\mathbb{Q}_p$ and $\mathbb{Q}_{p^h}$ is a maximal subfield. Compute its Hasse-invariant $\mathrm{inv}_p(D_{p,h,m})$ as an element of $\frac{1}{h}\mathbb{Z}/\mathbb{Z}$. Determine the valuation on D that extends the p-adic valuation on $\mathbb{Q}_{p^h}$.

   (b) Notice that inside D, we have an order $\mathcal{O}$ generated by $\mathbb{Z}_{p^h}$ and α, where $\mathbb{Z}_{p^h}$ is the ring of integers in $\mathbb{Q}_{p^h}$. Determine the pairs (m, h) for which $\mathcal{O}$ is a maximal order.[b]

---

[a]It is not obvious that this set forms a group. Think about what the group operations are!
[b]Hint: notice that $\mathcal{O} \subseteq \mathcal{O}_D := \{x \in D : v(x) \geq 0\}$.

2. Endomorphism Algebras of Abelian Varieties

Let's start by calculating some endomorphism rings! You may use the LMFDB, or your favorite computer algebra system to verify your answers.

Problem 5 ($\star\star$)

Let $\mathbb{Z}_{(3)}$ be the localization of $\mathbb{Z}$ at the prime ideal (3), and E be the elliptic curve over $\mathbb{Z}_{(3)}$ defined by
$$y^2 z = x^3 - xz^2.$$
In PSET 1, Problem 3, we computed the endomorphism ring of $E_{\mathbb{F}_{3^2}}$. Now compute the endomorphism rings $\mathrm{End}(E_{\mathbb{F}_3})$, $\mathrm{End}(E_{\mathbb{Q}(i)})$, $\mathrm{End}(E_{\mathbb{Q}})$, and compare them. Here, i is a root of $T^2 + 1 \in \mathbb{Q}[T]$.[a]

---

[a]Remark: Recall that the endomorphism ring of an elliptic curve E over a field k is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If $\mathrm{char}(k) = 0$, only the first two are possible. [Sil09, Corollary III.9.4]

Section §3.2 of the lecture notes defines the isogeny category of abelian varieties over a field k and states that it is a semisimple abelian category. Let's unpack this idea.

Problem 6 (⋆⋆)

Let k be a field.

(1) Justify why: $A \sim B$ if and only if A is isogenous to B, is an equivalence relation on the set of abelian varieties over k.

(2) Show that for every simple abelian variety A, the endomorphism algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$.

(3) Reality check: $\mathrm{End}(A)$ is an order in $\mathrm{End}^0(A)$.

(4) If A is not necessarily simple, conclude that $\mathrm{End}^0(A)$ is a semisimple algebra over $\mathbb{Q}$.

In the next problem, we sketch a proof of Lenstra [Len96] of a fundamental theorem of Deuring [Deu41].

Problem 7 (⋆⋆)

Let E be an elliptic curve defined over a field k of characteristic p, and suppose that $\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E) = 4$. Then $B := \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞. To prove this, denote by $\mathcal{O} := \mathrm{End}\, E \subset B$, and follow the following steps:

(1) Let n be prime to p. Recall that $\mathrm{End}\, E[n] \cong M_2(\mathbb{Z}/n\mathbb{Z})$.

(2) Show that $\mathcal{O}/n\mathcal{O} \to \mathrm{End}\, E[n]$ is injective.

(3) Show that $\#\mathcal{O}/n\mathcal{O} = n^4$ and conclude that $\mathcal{O}/n\mathcal{O} \to \mathrm{End}\, E[n]$ is an isomorphism.

(4) Show that for every prime $\ell \neq p$ we have that $\mathcal{O}_\ell \cong M_2(\mathbb{Z}_\ell)$ as $\mathbb{Z}_\ell$-algebras.

(5) Argue why B is ramified at ∞.

(6) Recall the fundamental exact sequence from class field theory

$$(2.1) \qquad 0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0$$

where the first map is given by $B \to \bigoplus_v B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ and the second map is given by $(B_v)_v \to \sum_v \mathrm{inv}_v(B_v)$. Use Equation 2.1 to show B is ramified at exactly ∞ and p.[a]

(7) Show that $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong D_{p,2,1}$, where $D_{p,2,1}$ is defined as in 4. [b]

---

[a]See [Voi21, Example 14.2.13] for an explicit description of these quaternion algebras.
[b]Hint: Show that they have the same Hasse-invariant.

Problem 8 (⋆⋆)

Let A be a simple g-dimensional abelian variety defined over $\mathbb{F}_q$. From Problem 6 we have that $\mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$. Recall that for a division algebra D, we defined its reduced degree by $[D : \mathbb{Q}]_{\mathrm{red}} := [D : \mathcal{Z}(D)]^{1/2}[\mathcal{Z}(D) : \mathbb{Q}]$. We say that A has complex multiplication if the reduced degree $[\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}}$ is equal to $2g$.

Let L be the maximal commutative sub-algebra of $D = \mathrm{End}^0(A)$. Show that A has complex multiplication if and only if $[L : \mathbb{Q}] = 2g$.[a]

---

[a]Hint: Use the double centralizer theorem.

Recall the definition and notation of the q-Frobenius endomorphism ϕ_q from PSET 1, Problem 4.

Problem 9 (⋆)

Consider an ordinary elliptic curve E over $\mathbb{F}_q$.

(1) Show that $L = \mathbb{Q}(\phi_q)$ has $[L : \mathbb{Q}] = 2$. Conclude that E has complex multiplication.

(2) Show $\mathbb{Q}(\phi_q)$ is a quadratic imaginary extension of $\mathbb{Q}$.[a]

(3) Show that for every element $\alpha \in \mathrm{End}^0(E)$, α commutes with ϕ_q^r for some $r \geq 1$.

(4) Show that for any $m \geq 1$, $\phi_q^m = a\phi_q + b$ for some $a, b \in \mathbb{Z}$ with $a \neq 0$.

(5) Show that α commutes with ϕ_q and that $\alpha \in \mathbb{Q}(\phi_q)$. Conclude that $\text{End}^0(E)$ is a quadratic imaginary extension of $\mathbb{Q}$.

---

[a]Hint: See [Sil09][V.1.1] for Hasse bound.

3. THE TATE MODULE OF AN ABELIAN VARIETY

Recall from Lecture 2 the existence of a Weil pairing on the Tate module of an abelian variety. In the case of elliptic curves, we can use the Weil pairing to deduce useful formulas for the trace and determinant of the map on the Tate module of E induced by an isogeny.

Problem 10 ($\star\star$)

Let E be an elliptic curve defined over a field k, and ℓ be a prime different from the characteristic of k. Let $T_\ell E$ be the ℓ-adic Tate module of E. The Weil pairing

$$e : T_\ell E \times T_\ell E \to T_\ell \mu$$

is a bilinear, alternating, non-degenerate, Galois-invariant pairing.[a] Here $T_\ell \mu := \varprojlim \mu_{\ell^n}$, where μ_{ℓ^n} is the group of ℓ^n-th roots of unity in $\bar{k}$. Moreover, for $\phi \in \text{End}(E)$ and $T_\ell(\phi) \in \text{End}(T_\ell E)$, the adjoint of $T_\ell(\phi)$ with respect to e corresponds to the dual isogeny $\hat{\phi}$. That is,

$$e(T_\ell(\phi)(P), Q) = e(P, T_\ell(\hat{\phi})(Q)).$$

Using the existence of e and the fact that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$, show that

- $\det(T_\ell(\phi)) = \deg(\phi)$, and
- $\text{tr}(T_\ell(\phi)) = 1 + \deg(\phi) - \deg(1 - \phi)$.

---

[a]See [Sil09][III.8].

Problem 11 ($\star\star$)

Here are some facts about the q-Frobenius endomorphism ϕ_q of an elliptic curve $E/\mathbb{F}_q$:

(a) ϕ_q is a purely inseparable isogeny of degree q.

(b) Its dual isogeny $\hat{\phi}_q$ is the unique isogeny satisfying $\phi_q \circ \hat{\phi}_q = \hat{\phi}_q \circ \phi_q = [q]$.

(c) The isogeny $[m] + [n]\phi_q$ is separable if and only if $p \nmid m$. In this case, we have that

$$\# \ker([m] + [n]\phi_q) = \deg([m] + [n]\phi_q).$$

Let $\ell \neq p$ be a prime and $T_\ell E$ be the ℓ-adic Tate module of E.

(1) Denote by $P_E(T)$ the characteristic polynomial of $T_\ell(\phi_q)$, the so-called characteristic polynomial of Frobenius. Show that $P_E(T) = T^2 - aT + q$, where $a = q + 1 - \#E(\mathbb{F}_q)$. Let $\alpha, \overline{\alpha} \in \mathbb{C}$ be the roots of $P_E(T)$. Show that

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \overline{\alpha}^n,$$

for every positive integer n.

(2) The zeta function attached to E is the formal power series[a]

$$Z(E/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

Show that[b] $Z(E/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$.

---

[a]If we let $T = q^{-s}$, then $\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q, q^{-s})$ is a holomorphic function with variable s, and it is the analogue of $\zeta_{\mathbb{F}_q[t]}(s)$ in PSET 0, Problem 8.

[b]This is the rationality part of the Weil conjectures for $E/\mathbb{F}_q$.

Problem 12 ($\star$)

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 13 ($\star\star$)

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
$$\operatorname{Hom}(A, B) \otimes \mathbb{Z}_\ell \to \operatorname{Hom}(T_\ell(A), T_\ell(B))$$
$$\alpha \otimes c \mapsto c T_\ell \alpha$$
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 nontrivial element of M^{div}.

Problem 14 ($\star$)

Combine Problem 13 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 15 ($\star\star$)

(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 16 ($\star\star$)

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

(4.1) $$\mathrm{Hom}(A, B) \to \mathrm{Hom}_{G_{\mathbb{F}_q}}(T_\ell A, T_\ell B)$$

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

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

(2) Show that bijectivity of Equation 4.2 is equivalent to the bijectivity of

(4.3) $$\mathrm{End}(A) \otimes \mathbb{Q}_\ell \to \mathrm{End}_{G_{\mathbb{F}_q}}(V_\ell A)$$

for every abelian variety $A/\mathbb{F}_q$.

(3) Consider now the commuting subalgebras of $\mathrm{End}_{G_{\mathbb{F}_q}}(V_\ell A)$ defined by
  - E_ℓ is the image of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ by Equation 4.3, and
  - F_ℓ is the subalgebra of $\mathrm{End}_{G_{\mathbb{F}_q}}(V_\ell A)$ 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 4.3 is equivalent to the fact that F_ℓ is the commutant of E_ℓ in $\mathrm{End}(V_\ell A)$.

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

Problem 17 ($\star\star\star$)

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

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

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

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

(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 $P_A(T)$.

References

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR 5125

[Len96] H. W. Lenstra, Jr., *Complex multiplication structure of elliptic curves*, J. Number Theory **56** (1996), no. 2, 227–241. MR 1373549

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

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

[Voi21] John Voight, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, [2021] ©2021. MR 4279905