THE THEOREM OF HONDA AND TATE

KIRSTEN EISENTRÄGER

1. Motivation

Consider the following theorem of Tate (proved in [Mum70, Theorems 2–3, Appendix I]):

Theorem 1.1. *Let A and B be abelian varieties over a finite field k of size q, and let f_A, $f_B \in \mathbb{Z}[T]$ be the characteristic polynomials of their q-Frobenius endomorphisms, so f_A and f_B have degrees $2 \cdot \dim A$ and $2 \cdot \dim B$ with constant terms $q^{\dim A}$ and $q^{\dim B}$ respectively. The following statements are equivalent:*

(1) *B is k-isogenous to an abelian subvariety of A.*
(2) *$f_B | f_A$ in $\mathbb{Q}[T]$.*

In particular, A is k-isogenous to B if and only if $f_A = f_B$. Moreover, A is k-simple if and only if f_A is a power of an irreducible polynomial in $\mathbb{Q}[T]$.

Recall that the roots of f_A in $\mathbb{C}$ are "Weil q-integers": algebraic integers whose images in $\mathbb{C}$ all have absolute value $q^{1/2}$. By Theorem 1.1 to describe the isogeny classes of abelian varieties over finite fields we would like to know for which Weil q-integers π in $\mathbb{C}$ we can find a k-simple abelian variety A/k such that π is a root of f_A. We will show that for each π, we can find a k-simple abelian variety A and an embedding $\mathbb{Q}[\pi] \hookrightarrow \mathrm{End}_k^0(A)$ such that π is the q-Frobenius endomorphism of A. We will follow the discussion in [Tat68] and [MW71]. Brian Conrad heavily revised Section 8 to simplify the computation of the invariant $\mathrm{inv}_v(E)$ for $v \mid p$ and he provided the proofs for Theorem 8.3 and the results in the appendix.

2. Setup

Let k be a finite field with $q = p^a$ elements. We will work in the *category $M(k)$ of abelian varieties up to isogeny* over k: $M(k)$ is the category whose objects are abelian varieties over k with the set of morphisms between two abelian varieties A and B given by $\mathrm{Hom}_k(A, B) \otimes \mathbb{Q}$. Two abelian varieties are isomorphic in $M(k)$ if

and only if they are isogenous over k. The category $M(k)$ is a $\mathbb{Q}$-linear category.

Our goal is to describe the category $M(k)$. Since every object in $M(k)$ is a direct sum of a finite number of simple objects, it suffices to list the isomorphism classes of simple objects and, for each class, the endomorphism algebra. The theorems of Honda and Tate allow us to do this, as we shall see.

Notation: For an abelian variety A over k, π_A will denote the q-Frobenius endomorphism. For abelian varieties A and B we use $\mathrm{Hom}_k^0(A,B)$ to denote $\mathrm{Hom}_k(A,B)\otimes\mathbb{Q}$.

Let A be an abelian variety over k, so π_A commutes with all endomorphism of A and hence lies in the center of $\mathrm{End}_k^0(A)$. If A is simple, then $\mathrm{End}_k^0(A)$ is a division algebra. Therefore, when A is simple the subring $\mathbb{Q}[\pi]$ is a number field. An isogeny $A\to B$ of simple abelian varieties over k defines an isomorphism $\mathrm{End}_k^0(A)\to\mathrm{End}_k^0(B)$ carrying π_A into π_B and hence mapping $\mathbb{Q}[\pi_A]$ isomorphically onto $\mathbb{Q}[\pi_B]$. We also know that π_A is an algebraic integer whose absolute value is $q^{1/2}$ under every embedding into $\mathbb{C}$. This motivates the following definition.

Definition 2.1. A *Weil q-integer* in a field of characteristic 0 is an algebraic integer π such that for every embedding $\sigma:\mathbb{Q}[\pi]\hookrightarrow\mathbb{C}$, $|\sigma\pi|=q^{1/2}$.

Let $W(q)$ be the set of Weil q-integers in $\mathbb{C}$.

Definition 2.2. Two Weil q-integers π and π' are *conjugate*, $\pi\sim\pi'$, if there exists an isomorphism of $\mathbb{Q}[\pi]\to\mathbb{Q}[\pi']$ carrying π into π'.

Equivalently, π and π' have the same minimal polynomial over $\mathbb{Q}$.

Let A be a simple abelian variety defined over k. We will describe the division algebra $\mathrm{End}_k^0(A)$ in terms of π_A. To do this, we first need to review the classification of division algebras over number fields.

3. Review: division algebras over global fields

Definition 3.1. A *central simple algebra* over a field F is an F-algebra R such that

(1) R is finite dimensional over F.
(2) F is the center of R.
(3) R is a simple ring.

If R is also a division algebra, we call it a *central division algebra* over F.

Notation: We will denote the $r\times r$ matrix algebra over a field F by $M_r(F)$.

Lemma 3.2. *If R and S are central simple algebras over F, then so is $R \otimes_F S$. For any field F'/F, $R \otimes_F F'$ is a central simple algebra over F'.*

Proof. For the first part see [Rei03, (7.6) Theorem], for the second statement see [Rei03, (7.8) Corollary]. □

Proposition 3.3 (Wedderburn's Theorem)**.** *Every central simple algebra over F is isomorphic to $\mathrm{End}_E(E^{\oplus r}) = M_r(E)$ for some $r \geq 1$ and some central division algebra E over F. Moreover, r is uniquely determined by R, and E is uniquely determined up to F-isomorphism.*

Proof. See [Rei03, p. 91]. □

Definition 3.4 (Brauer group)**.** Let A and B be finite dimensional central simple algebras over a field F. We say that A and B are *similar*, $A \sim B$, if $A \otimes_F M_n(F) \cong M_n(A)$ is F-isomorphic to $B \otimes_F M_m(F) \cong M_m(B)$ for some $m, n \geq 1$. Define the *Brauer group* of F, $\mathrm{Br}(F)$, to be the set of similarity classes of central simple algebras over F, and write $[A]$ for the similarity class of A. For classes $[A]$ and $[B]$, define

$$[A][B] := [A \otimes_F B].$$

This is well defined and makes $\mathrm{Br}(F)$ into an abelian group with $[A]^{-1} = A^{\mathrm{opp}}$, where A^{opp} is the "opposite algebra".

By Proposition 3.3, each element in $\mathrm{Br}(F)$ is represented (up to isomorphism) by a unique central division algebra over F.

We now need to clear up any possible confusion concerning sign conventions for local invariants of Brauer classes for non-archimedean local fields. Upon choosing a separable closure F_{s} of an arbitrary field F, there are two natural procedures to define a functorial isomorphism $\mathrm{Br}(F) \simeq \mathrm{H}^2(F_{\mathrm{s}}/F, F_{\mathrm{s}}^{\times})$: a conceptual method via non-abelian cohomology as in [Ser79, Ch. X, §5] and an explicit method via crossed-product algebras. By [Ser79, Ch. X, §5, Exer. 2], these procedures are negatives of each other. We choose to use the conceptual method of non-abelian cohomology. In case F is a non-archimedean local field with residue field κ and F^{un} denotes its maximal unramified subextension within F_{s} (with $\overline{\kappa}$ the residue field of F^{un}) it is known from local class field theory that the natural map $\mathrm{H}^2(F^{\mathrm{un}}/F, F^{\mathrm{un}\times}) \to \mathrm{H}^2(F_{\mathrm{s}}/F, F_{\mathrm{s}}^{\times})$ is an isomorphism, and the normalized valuation mapping $F^{\mathrm{un}\times} \to \mathbb{Z}$ induces an isomorphism

$$\mathrm{H}^2(F^{\mathrm{un}}/F, F^{\mathrm{un}\times}) \simeq \mathrm{H}^2(F^{\mathrm{un}}/F, \mathbb{Z}) \overset{\delta}{\simeq} \mathrm{H}^1(\mathrm{Gal}(F^{\mathrm{un}}/F), \mathbb{Q}/\mathbb{Z}).$$

There now arises the question of choice of topological generator for $\mathrm{Gal}(\overline{\kappa}/\kappa)$: arithmetic or geometric Frobenius? We choose to follow

Deligne's convention and work with geometric Frobenius; in [CF86, p. 130] and [Ser79, p. 193] the arithmetic Frobenius generator is used instead. Via evaluation on the chosen topological generator, our conventions lead to a composite isomorphism

$$\mathrm{inv}_F : \mathrm{Br}(F) \simeq \mathbb{Q}/\mathbb{Z}$$

for non-archimedean local fields F. If one uses the arithmetic Frobenius convention, then by adopting the crossed-product algebra method to define the isomorphism $\mathrm{Br}(F) \simeq \mathrm{H}^2(F_{\mathrm{s}}/F, F_{\mathrm{s}}^{\times})$ one gets the *same* composite isomorphism inv_F since the two sign differences cancel out in the composite. (**Warning**: In [CF86] and [Ser79] the Brauer group of F is *defined* to be $\mathrm{H}^2(F_{\mathrm{s}}/F, F_{\mathrm{s}}^{\times})$, and so the issue of choosing between non-abelian cohomology or crossed-product algebras does not arise in the foundational aspects of the theory; however, it implicitly arises in comparison with central simple algebras, such as in [CF86, pp. 137-8] where the details are omitted.)

Since $\mathrm{Br}(\mathbb{R})$ is cyclic of order 2 and $\mathrm{Br}(\mathbb{C})$ is trivial, for archimedean local fields F there is a unique injective homomorphism $\mathrm{inv}_F : \mathrm{Br}(F) \hookrightarrow \mathbb{Q}/\mathbb{Z}$.

By [CF86, Thm. 3, p. 131], for a finite extension F'/F of non-archimedean local fields, composition with the natural map $\mathrm{Br}(F) \to \mathrm{Br}(F')$ carries $\mathrm{inv}_{F'}$ to $[F' : F] \cdot \mathrm{inv}_F$. By [Ser79, p. 194, Cor. 3], $\mathrm{inv}_F(E)$ has order $\sqrt{[E : F]}$ for any central division algebra E over F. These assertions are trivially verified to also hold for archimedean local fields F.

Theorem 3.5. *Let F be a global field. There is an exact sequence*

$$0 \to \mathrm{Br}(F) \to \bigoplus_{v \in M_F} \mathrm{Br}(F_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0,$$

where M_F denotes the set of nonequivalent nontrivial absolute values of F and F_v denotes the completion of F at v. The first map is defined via the maps $\mathrm{Br}(F) \to \mathrm{Br}(F_v)$ given by extension of scalars, and the second map is given by summing the local invariants.

Proof. This is [CF86, §9.7, §11.2]. □

For a global field F and a central division algebra E over F, write $\mathrm{inv}_v(E)$ for $\mathrm{inv}_{F_v}(E \otimes F_v)$. The theorem says that a central division algebra E over a global field F is uniquely determined up to isomorphism by its invariants $\mathrm{inv}_v(E)$, and that these may be arbitrarily assigned subject to the condition $\mathrm{inv}_v(E) = 0$ for all but finitely many v and $\sum \mathrm{inv}_v(E) = 0$. Moreover, the order of $[E]$ in $\mathrm{Br}(F)$ is the least common "denominator" of the $\mathrm{inv}_v(E) \in \mathbb{Q}/\mathbb{Z}$.

If K is any field then for a class $c \in \mathrm{Br}(K)$ its *period* is its order and its *index* is $\sqrt{[\Delta : K]}$ with Δ the unique central division algebra over K representing the class c. It is a classical fact that the period divides that index and that these integers have the same prime factors (see [Ser79, X.5], especially Lemma 1 and Exercise 3), but in general equality does not hold. (There are function fields of complex 3-folds for which some order-2 elements in the Brauer group cannot be represented by a quaternion algebra, and counterexamples with less interesting fields were first discovered by Brauer.) We have noted above that over local fields there is equality of period and index (the archimedean case being trivial). We need one more theorem that gives such a result over global fields:

Theorem 3.6. *For a central division algebra E over a global field F, the order of $[E]$ in $\mathrm{Br}(F)$ is $\sqrt{[E : F]}$.*

As a special (and very important) case, elements of order 2 in $\mathrm{Br}(F)$ are precisely the Brauer classes of quaternion division algebras for a global field F; as noted above, this fails for more general fields. We shall require this special case for $\mathbb{Q}$ and real quadratic fields in our study of k-simple A for which f_A has a real root. Since Theorem 3.6 does not seem to be explicitly stated in any of the standard modern references on class field theory (though it is cryptically alluded to in [AT68, p. 105]), we give a proof below.

Proof. Let E have degree n^2 over F and let d be the order of $[E]$ in $\mathrm{Br}(F)$, so $d|n$. Note that d is the least common multiple of the local orders d_v of $[E \otimes_F F_v] \in \mathrm{Br}(F_v)$ for each place v of F, with $d_v = 1$ for complex v, $d_v|2$ for real v, and $d_v = 1$ for all but finitely many v. Using these formal properties of the d_v's, we may call upon the full power of global class field theory via Theorem 5 in [AT68, Ch. X] to infer the existence of a cyclic extension L/F of degree d such that $[L_{v'} : F_v]$ is a multiple of d_v for every v of F (here, v' is any place on L over v, and the constraint on the local degree is only non-trivial for $d_v > 1$). In the special case $d = 2$ (the only case we will require) one only needs weak approximation and Krasner's Lemma rather than class field theory: take L to split a separable quadratic polynomial over F that closely approximates ones that define quadratic separable extensions of F_v for each v such that $d_v = 2$.

Since restriction maps on local Brauer groups induce multiplication by the local degree on the local invariants, it follows that $E \otimes_F L$ is locally split at all places of L, whence by the injectivity of the map from the global Brauer group into the direct sum of the local ones (for L) we

conclude that the Galois extension L/F *of degree* d splits E. (The existence of cyclic splitting fields for all Brauer classes is proved for number fields in Tate's article in [CF86] and is proved in general in Weil's "Basic Number Theory", but neither reference seems to exert much control on the degree of the global cyclic extension.) By a general result concerning Brauer groups of arbitrary fields [Ser79, Ch. X, §5, Lemma 1], every Brauer class split by a Galois extension of degree r is represented by a central simple algebra with degree r^2. Applying this fact from algebra in our situation, $[E] = [C]$ for a central simple algebra C of degree d^2 over F. But each Brauer class is represented by a unique central division algebra, and so C must be F-isomorphic to a matrix algebra over E. Since $[C : F] = d^2$ and $[E : F] = n^2$ with $d|n$, this forces $d = n$ as desired. □

4. Statement of Theorem

We will keep the notation of Section 2.

Theorem 4.1.

(1) *Let k be a finite field of size $q = p^a$. The map $A \mapsto \pi_A$ defines a bijection from the set of k-isogeny classes of simple abelian varieties over k to the set $W(q)/(conjugacy)$.*

Let $A \in M(k)$ be simple. Let $E := \mathrm{End}_k^0(A)$ and let $F := \mathbb{Q}[\pi_A] \subseteq E$. Then E is a division algebra whose center is F.

(2) *The division algebra E does not split at any real place of F, and E splits at all finite places of F not dividing $p = \mathrm{char}(k)$. For a place v of F dividing p we have*

$$\mathrm{inv}_v(E) = \frac{v(\pi_A)}{v(q)} \cdot [F_v : \mathbb{Q}_p] \mod 1, \tag{4.1}$$

where F_v denotes the completion of F at v. We have

$$2 \cdot \dim A = [E : F]^{1/2} \cdot [F : \mathbb{Q}]. \tag{4.2}$$

The injectivity of the map $A \mapsto \pi_A$ was proved by Tate, and the surjectivity of this map was proved by Honda [Hon68]. Part(2) of the theorem was proved by Tate in [Tat66]. An interesting consequence of (4.2) is that if $K \subseteq E$ is a maximal commutative subfield over F (so $[K : F] = \sqrt{[E : F]}$) then $[K : \mathbb{Q}] = 2\dim A$. Hence, every k-simple abelian variety over a finite field k is of CM type *over* k.

5. Examples

Let $\pi \in W(q) \subseteq \mathbb{C}$ be a Weil q-integer in $\mathbb{C}$. Grant Theorem 4.1.

5.1. **Real Case:** Assume $F = \mathbb{Q}[\pi]$ has a real embedding, and fix such an embedding $\mathbb{Q}[\pi] \overset{\phi}{\hookrightarrow} \mathbb{R} \subseteq \mathbb{C}$. Then $\phi(\pi) = \overline{\phi(\pi)}$. In this case $\phi(\pi^2) = \phi(\pi) \cdot \overline{\phi(\pi)} = q = p^a$, so $\pi^2 = p^a$. Of course, $\pm\sqrt{q}$ is a Weil q-integer for any q, so by Theorem 4.1(1) it does arise from a k-simple A that is unique up to k-isogeny. There are two possible cases to consider.

(1) When a is even, we have $F = \mathbb{Q}$. There is only one real place v, and for this place we have $\mathrm{inv}_v(E) = 1/2$, which implies that E must be ramified at p as well with $\mathrm{inv}_p(E) = 1/2$. This implies that the order of E in $\mathrm{Br}(\mathbb{Q})$ is 2, and so (Theorem 3.6) E is a quaternion division algebra over $\mathbb{Q}$ which is ramified at ∞ and p. The formula $2 \dim A = [E : F]^{1/2}[F : \mathbb{Q}]$ implies that $\dim A = 1$. Hence, the characteristic polynomial of $f_A \in \mathbb{Z}[T]$ with a factor $T - p^{a/2}$ has degree 2 and constant term $q = p^a$, so it must be $(T - p^{a/2})^2$.

Since $a_p(A) = 2p^{a/2} \in p\mathbb{Z}$, A is a supersingular elliptic curve. For any abelian variety X over any field K, the faithfulness of $V_\ell(X)$ as a $\mathbb{Q}_\ell \otimes \mathrm{End}^0_K(X)$-module for any prime $\ell \neq \mathrm{char}(K)$ ensures that $\dim_{\mathbb{Q}} \mathrm{End}^0_K(X) \leq (2\dim X)^2$. Thus, for $\mathbb{Q}$-dimension reasons $E = \mathrm{End}^0_k(A) = \mathrm{End}_{\overline{k}}(A) \otimes \mathbb{Q}$, *i.e.* all $\overline{k}$-endomorphisms are already defined over k. Note that the surjectivity in Theorem 4.1(1) ensures conversely that this case really does occur over any k! Conversely, we know from the theory of supersingular elliptic curves that if A is a supersingular elliptic curve over k whose $\overline{k}$-endomorphisms are defined over k then $E = \mathrm{End}^0_k(A)$ is a quaternion division algebra over $\mathbb{Q}$, so the central subfield $F = \mathbb{Q}(\pi) \subseteq E$ must be $\mathbb{Q}$.

(2) When a is odd, we have $F = \mathbb{Q}(\pi) \cong \mathbb{Q}(p^{1/2})$. In F we have two real places, and the invariant of E at those two places is $1/2$ by the theorem. Since there is only one place v of F dividing p, this means that E is not ramified at $v \mid p$. The division algebra E has order 2 in $\mathrm{Br}(F)$, so $[E : F] = 4$ by Theorem 3.6. By formula (4.2), $\dim A = 2$. The characteristic polynomial f_A of π_A in $\mathbb{Z}[T]$ is therefore a quartic with $\pm p^{a/2}$ as a root. By Theorem 1.1, f_A is a power of an irreducible polynomial in $\mathbb{Q}[T]$ since A is k-simple, so $f_A = (T^2 - p^a)^2$. Thus, the characteristic polynomial of the q^2-Frobenius for A over a degree 2 extension k' of k is $(T - p^a)^4$. By the existence aspect in the "real case" (1) applied over the field k' with size p^{2a}, there exists a supersingular elliptic curve A_0 over k' with characteristic polynomial $(T - p^a)^2$. By Theorem 1.1 all choices of A_0 are k'-isogenous, and in (1) we saw that such A_0 are precisely the supersingular

elliptic curves over k' whose "geometric" endomorphisms are defined over k'.

The characteristic polynomial of the q^2-Frobenius of $A_0 \times A_0$ is $(T - p^a)^4$, so $A_{/k'}$ is k'-isogenous to $A_0 \times A_0$. Thus, this is the case of an abelian surface that is k-simple but is isogenous over k' to $A_0 \times A_0$ for some (equivalently, any) supersingular elliptic curve A_0 over k' whose "geometric" endomorphisms are all defined over k'. Observe that necessarily A is k'-isogenous to $\mathrm{Res}_{k'/k}(A_0)$. By the surjectivity aspect of Theorem 4.1(1) such a case must always occur. (That is, this restriction of scalars must be k-simple for any finite field k of size p^a with odd a and "the" quadratic extension k'/k.)

5.2. **"General" case: $F = \mathbb{Q}(\pi)$ is totally imaginary.** For any embedding $\phi : \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$ we have $\phi(\pi)\overline{\phi(\pi)} = q$, so $\overline{\phi(\pi)} = q/\phi(\pi) = \phi(q/\pi)$. Thus, $\phi(F) \subseteq \mathbb{C}$ is stable under complex conjugation with $\phi^{-1}(\overline{\phi(x)})$ independent of ϕ since this is true for $x = \pi$. Then F is a CM-field, *i.e.* a quadratic totally imaginary extension of a totally real field F_0. Let $\overline{x} = \phi^{-1}(\overline{\phi(x)})$ for any $x \in F$, so $\overline{\pi} = q/\pi$. Thus, $F_0 = \mathbb{Q}(\pi + \overline{\pi})$ is the totally real subfield of F. The division algebra E splits at each place v which does not divide p. (There are no real places.) For a place v dividing p, in $\mathbb{Q}/\mathbb{Z}$ we have

$$\mathrm{inv}_v(E) + \mathrm{inv}_{\overline{v}}(E) = 0 \text{ , if } \overline{v} \neq v, \tag{5.1}$$

$$\mathrm{inv}_v(E) = 0 \text{ , if } \overline{v} = v. \tag{5.2}$$

Formula (5.1) follows from $\pi\overline{\pi} = q$, $v(\pi) + v(\overline{\pi}) = v(q)$, and the formula for the invariant in (4.1) since $[F_{\overline{v}} : \mathbb{Q}_p] = [F_v : \mathbb{Q}_p]$. Equation (5.2) follows from formula (4.1) of the theorem and the fact that $[F_v : \mathbb{Q}_p]$ is even when $v = \overline{v}$.

If k is the prime field, $k = \mathbb{F}_p$, then E is split everywhere since $v(\pi)/v(p)$ is an integral multiple of $1/e_v$ and $e_v | [F_v : \mathbb{Q}_p]$ (so for any prime v dividing p, formula (4.1) of the theorem shows that $\mathrm{inv}_v(E) = 0$ in $\mathbb{Q}/\mathbb{Z}$). Thus, $E = F$ and hence $\mathrm{End}_k(A)$ is commutative (recall $k = \mathbb{F}_p$).

5.3. **The remaining possibilities when $\dim A = 1$.** If $\dim A = 1$, then $2 = [E : F]^{1/2}[F : \mathbb{Q}]$. The case $F = \mathbb{Q}$ has been settled, as has the case of real quadratic F (with A necessarily an abelian surface). Thus, if A is either an ordinary elliptic curve or a supersingular elliptic curve whose "geometric" endomorphism ring (a quaternion division algebra over $\mathbb{Q}$ ramified at precisely p and ∞) is strictly larger than E then $E = F$ is an imaginary quadratic field. By Theorem 4.1 this exhausts

all cases with $E = F$ and F imaginary quadratic. Since $F = \mathbb{Q}(\pi)$, we conclude (via §5.1) that these are precisely the elliptic curves over finite fields of size q such that the q-Frobenius is *not* multiplication by a rational integer.

6. Injectivity of the map $A \mapsto \pi_A$

Injectivity proof. Let A and B be two k-simple abelian varieties such that $\pi_A = \pi_B$ in $W(q)$ modulo conjugacy. Let f_A and f_B be the characteristic polynomials of π_A and π_B, respectively. Since A is simple, f_A is a power of an irreducible polynomial $h \in \mathbb{Q}[T]$, say $f_A = h^m$ with $m \geq 1$. Since $\pi_A = \pi_B$ and B is simple, $f_B = h^n$ with $n \geq 1$. By relabeling we may assume $m \geq n$, so f_B divides f_A. Then by Theorem 1.1 we see that B is isogenous to an abelian subvariety of A over k. Since A and B are k-simple, this inclusion must be an isogeny. □

7. Surjectivity of the map $A \mapsto \pi_A$

To prove surjectivity we have to construct sufficiently many simple abelian varieties over k to exhaust all the conjugacy classes of Weil q-integers. But we cannot easily write down abelian varieties of dimension greater than 2 over k, so how to proceed? We will construct abelian varieties with complex multiplication over $\mathbb{C}$, realize them over number fields that we embed in finite extensions of $\mathbb{Q}_p$, and then reduce them to obtain abelian varieties over finite fields.

Notation: We will call a Weil q-integer π *effective* if π is conjugate to the q-Frobenius of a simple abelian variety over k. (That is, there exists a k-simple abelian variety A and an embedding $\mathbb{Q}[\pi] \hookrightarrow \mathrm{End}_k^0(A)$ carrying π to π_A.)

So our goal is to prove that all Weil q-integers are effective. We will first prove the following lemma.

Lemma 7.1. *Let N be an integer, $N \geq 1$. If π^N is effective, then π is effective as well.*

Proof. Let k' be an extension of k of degree N. Let A' be an abelian variety over k' such that π^N is conjugate to $\pi_{A'}$. Let A be the abelian variety over k which is the restriction of scalars of A'.

Let ℓ be a prime, $\ell \neq p$. From the functorial characterization of Weil restriction of scalars, as $\mathbb{Q}_\ell[G_k]$-modules (with $G_k = \mathrm{Gal}(\overline{k}/k)$ for a separable closure $\overline{k}/k'$) we have

$$V_\ell A = \mathrm{Ind}_{G_{k'}}^{G_k} V_\ell A'.$$

From this one can see that the characteristic polynomial f_A of π_A and the characteristic polynomial $f_{A'}$ of $\pi_{A'}$ are related via $f_A(T) = f_{A'}(T^N)$ (Lemma 9.1 in the Appendix) . Since π is a root of f_A, this implies that π is conjugate to the Frobenius π_{A_1} of one of the k-simple factors A_1 of A. □

Let π be a Weil q-integer. In the following let E be the division algebra obtained from π and the information in part (2) of Theorem 4.1; *i.e.*, E is the central division algebra over $F = \mathbb{Q}(\pi)$ whose local invariants are as in the theorem and so are completely determined by π. (Explicitly, $\mathrm{inv}_v(E) = 1/2$ for real places v of F, if any exist, and for non-archimedean v the fraction $v(\pi)[F_v : \mathbb{Q}_p]/v(q)$ represents $\mathrm{inv}_v(E) \in \mathbb{Q}/\mathbb{Z}$; this vanishes for such v not over p since π is a Weil q-integer.) By Theorem 3.5, such an E indeed exists and is unique up to isomorphism.

Lemma 7.2. *There exists a CM field L containing $F = \mathbb{Q}(\pi)$ such that L splits E and such that $[L : F] = [E : F]^{1/2}$.*

Proof. Since π is a Weil q-integer, F is a totally real or CM field. In the totally real case, as in §5.1 we must have $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{p})$ with $[E : F]^{1/2} = 2$, so $L = F(\sqrt{-p})$ works. If F is CM with maximal totally real subfield F_0, then we take $L = F \otimes_{F_0} L_0$ with L_0/F_0 a totally real extension of degree $[E : F]^{1/2}$ such that for all places v_0 of F_0 over p we have two properties: (i) there is exactly one place w_0 of L_0 over v_0, and (ii) w_0 is unramified (resp. totally ramified) over v_0 if the quadratic extension F/F_0 is ramified (resp. unramified) over v_0. Such an L_0 can be found by weak approximation, and by construction for each place w of L over p with restrictions to L_0, F, and F_0 denoted w_0, v, and v_0, we have

$$[L_w : F_v] = [L_{0,w_0} : F_{0,v_0}] = [L_0 : F_0] = [E : F]^{1/2}.$$

Hence, $L \otimes_F E$ is everywhere locally split over L, so it is split. □

Definition 7.3. Let A be an abelian variety over a field K. Let L be a number field. We say that A is *of type* (L) if there is a ring map $i : L \to \mathrm{End}^0_K(A)$ such that $[L : \mathbb{Q}] = 2 \dim A$.

Lemma 7.4. *Let L be a CM field containing $F = \mathbb{Q}(\pi)$ and such that L splits E. Then there exists an abelian variety A of type (L) over a finite extension of $\mathbb{Q}_p$ such that A has good reduction and such that the Frobenius of its reduction is conjugate to a power π^N of π.*

We will prove Lemma 7.4 in the next subsection. The three lemmas together clearly show that any given Weil q-integer π is effective.

7.1. **Proof of Lemma 7.4.** Let L be a CM field with $[L : \mathbb{Q}] = 2 \dim A$. Let ρ be the automorphism of L of order 2 which is induced by complex conjugation for each embedding $L \hookrightarrow \mathbb{C}$. Intrinsically, ρ is the unique nontrivial automorphism of L over its maximal totally real subfield. Let C be an algebraically closed field of characteristic 0. Let Φ be a CM type for L, *i.e.* Φ is a subset of $\mathrm{Hom}_{\mathbb{Q}-\mathrm{alg}}(L, C)$ such that

$$\Phi \cap \Phi\rho = \emptyset \text{ and} \tag{7.1}$$

$$\Phi \cup \Phi\rho = \mathrm{Hom}(L, C). \tag{7.2}$$

Definition 7.5. An abelian variety A over a subfield $F \subseteq C$ is *of type* (L, Φ), if A is of type L over F and the action of $C \otimes_{\mathbb{Q}} L$ on the tangent space t_{A_C} is through the quotient $\prod_{\phi \in \Phi} C_\phi$ (where L acts on $C_\phi = C$ through ϕ).

Lemma 7.6. *There exists an abelian scheme of type* (L, Φ) *defined over the ring of integers of a number field contained in* C.

Proof. This is proved in the notes for Tong Liu's talks in the seminar. □

From now on let us assume that C is an algebraic closure of $\mathbb{Q}_p$. For each place w of L such that $w \mid p$, let L_w be the completion of L with respect to w.

We identify $\mathrm{Hom}_{\mathbb{Q}_p}(L_w, C)$ with its image in $\mathrm{Hom}(L, C)$ and denote this image by H_w. Let $\Phi_w := \Phi \cap H_w$. We have a decomposition

$$\mathbb{Q}_p \otimes L = \prod_{w|p} L_w \tag{7.3}$$

and the disjoint unions

$$\mathrm{Hom}(L, C) = \bigcup_{w|p} H_w \tag{7.4}$$

$$\Phi = \bigcup_{w|p} \Phi_w. \tag{7.5}$$

Lemma 7.7. *Let* A *be an abelian scheme of type* (L, Φ) *defined over the ring of integers* $\mathcal{O}$ *of a finite extension of* $\mathbb{Q}_p$. *Let* k_0 *be the residue field of* $\mathcal{O}$, *and let* $q_0 = \mathrm{Card}(k_0)$. *Let* A_0 *be the reduction of* A *modulo the maximal ideal of* $\mathcal{O}$. *Then there exists an element* $\pi_0 \in L$ *such that* $i(\pi_0) \in \mathrm{End}(A)$ *induces the Frobenius* $\pi_{A_0} \in \mathrm{End}_k^0(A_0)$, *and we have*

$$\frac{w(\pi_0)}{w(q_0)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w).} \tag{7.6}$$

for each $w \mid p$.

Proof. This was proved by Shimura and Taniyama and will be presented in the seminar by Brian Conrad. □

Now we can prove Lemma 7.4.

Proof of Lemma 7.4. Let π, q, F, E as before, and assume that L satisfies the hypotheses of Lemma 7.4. Let $z \mapsto z^\rho$ be the complex conjugation on L. We will now show how we can choose the set Φ such that we have

$$\frac{w(\pi)}{w(q)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w)} \text{ for each place } w \text{ of } L \text{ with } w \mid p. \tag{7.7}$$

Let w be one such place, and let v be the place of F such that $w \mid v$. Let us put

$$n_w = \frac{w(\pi)}{w(q)} \cdot \mathrm{Card}(H_w) = \frac{w(\pi)}{w(q)} \cdot [L_w : \mathbb{Q}_p] = \frac{v(\pi)}{v(q)} \cdot [L_w : F_v] \cdot [F_v : \mathbb{Q}_p].$$

By functoriality of the local invariants and the hypothesis on $\mathrm{inv}_v(E)$, $\mathrm{inv}_w(L \otimes_F E) = [L_w : F_v]\frac{v(\pi)}{v(q)}[F_v : \mathbb{Q}_p] = n_w$ in $\mathbb{Q}/\mathbb{Z}$. The fact that L splits E implies that n_w is an integer for each w. We also clearly have

$$n_w \geq 0, \tag{7.8}$$

and since $\pi\pi^\rho = q$ we can conclude

$$n_w + n_{\rho w} = \mathrm{Card}\, H_w = \mathrm{Card}\, H_{\rho w}. \tag{7.9}$$

We will now choose the CM type Φ by choosing suitable sets Φ_w and then letting $\Phi := \bigcup_w \Phi_w$. Given integers n_w satisfying conditions (7.8) and (7.9) we can see that we can choose subsets $\Phi_w \subset H_w$ such that their union $\Phi := \bigcup_w \Phi_w$ satisfies conditions (7.1) and (7.2) and $n_w = \mathrm{Card}\, \Phi_w$. Let us make such a choice of Φ. Then condition (7.7), namely

$$\frac{w(\pi)}{w(q)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w)}$$

is satisfied by construction. By Lemma 7.6 there exists an abelian scheme of type (L, Φ) defined over the ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_p$, and by Lemma 7.7 there exists $\pi_0 \in L$ such that

$$\frac{w(\pi)}{w(q)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w)} = \frac{w(\pi_0)}{w(q_0)}. \tag{7.10}$$

Here π_0 is a Weil q_0-integer, with $\pi_0 \in L$, which is conjugate to the Frobenius of the reduction A_0 of A. Now we are almost finished. If we replace the ring $\mathcal{O}$ in Lemma 7.7 by an unramified extension of degree N_0 we replace π_0 by $\pi_0^{N_0}$. We can now finish the proof of Lemma 7.4 with the following lemma. □

Lemma 7.8. *Let π be a Weil q-integer in L and π_0 a Weil q_0-integer in L which satisfy $\frac{w(\pi)}{w(q)} = \frac{w(\pi_0)}{w(q_0)}$ for all w. Then there exist positive integers N and N_0 such that $\pi^N = \pi_0^{N_0}$.*

Proof. By replacing π and π_0 by powers we may assume that $q = q_0$. Then $w(\pi) = w(\pi_0)$ for each place w of L such that $w \mid p$. At the other finite places π and π_0 are units, because they divide a power of p. At the infinite places π and π_0 have the same absolute value, namely $q^{1/2}$. Hence π/π_0 has absolute value 1 at each place of L, which implies that π/π_0 is a root of unity. Hence some power of π/π_0 is equal to 1, and the lemma follows. □

8. Proof of part 2 of Theorem 4.1

In this section we will prove the end of Theorem 4.1(1) and Theorem 4.1(2).

8.1. **Statement of result and preliminary arguments.** Let A be a simple abelian variety over a finite field k with size q. Let π_A be the q-Frobenius of A. Let $E := \mathrm{End}_k^0(A)$. Then E is a division algebra. Let us recall Theorem 4.1(2) and the end of Theorem 4.1(1):

Theorem 8.1.

(1) *The center of E is $F = \mathbb{Q}(\pi)$.*
(2) *E splits at every finite place v of F such that v does not divide p.*
(3) *E does not split at any real place.*
(4) *The invariant $\mathrm{inv}_v(E)$ for a place $v \mid p$ is given by the formula*

$$\mathrm{inv}_v(E) = \frac{v(\pi_A)}{v(q)}[F_v : \mathbb{Q}_p] \bmod 1. \tag{8.1}$$

(5) *We have $2 \cdot \dim A = [E : F]^{1/2}[F : \mathbb{Q}]$.*

Formula (8.1) will be proved separately. Everything else will be proved now.

Proof. Part (1): We know that E is a division algebra, so its center is a field. Let $G_k := \mathrm{Gal}(\overline{k}/k)$. For a prime $\ell \neq p$ let $T_\ell A$ be the ℓ-adic Tate module and let $V_\ell(A) := T_\ell A \otimes \mathbb{Q}_\ell$. Let $F_\ell := \mathbb{Q}_\ell \otimes F$, and let $E_\ell := E \otimes \mathbb{Q}_\ell$. Let $S := \mathrm{End}\, V_\ell(A)$, and $T := F_\ell$. From Tate's isogeny theorem we have $E \otimes \mathbb{Q}_\ell \cong \mathrm{End}_{G_k}(V_\ell A)$, so the centralizer of T in S is E_ℓ because G_k is topologically generated by the q-Frobenius. Since E_ℓ is semisimple, we can apply the double centralizer theorem and conclude that the centralizer of E_ℓ in $\mathrm{End}\, V_\ell(A)$ is F_ℓ. So F_ℓ is the center of E_ℓ and hence F is the center of E. □

Part (5): If A is a k-simple abelian variety, then the characteristic polynomial f_A of π_A is a power of a $\mathbb{Q}$-irreducible monic polynomial h_A. Then $\deg h_A = [F : \mathbb{Q}]$. Say $f_A = {h_A}^e$. This implies that $2 \dim A = \deg f_A = e \cdot \deg h_A = e \cdot [F : \mathbb{Q}]$. We also have $[E : \mathbb{Q}] = e^2 \cdot [\mathbb{Q}(\pi_A) : \mathbb{Q}]$. This comes from the dimension computation in the proof that $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathrm{End}_{G_k}(V_\ell A)$ in [Tat66]. (Alternatively, see [Mum70, Thm. 2(a), Appendix I] for a proof.)

Part (2): Since $f_A = h_A^e$ with h_A irreducible over $\mathbb{Q}$ and since $V_\ell A$ is a semisimple $F \otimes \mathbb{Q}_\ell$-module, for a prime ℓ different from p, the Tate module is a free module of rank e over $F_\ell = F \otimes \mathbb{Q}_\ell$. By Tate's theorem, we have $F_\ell \otimes_F E = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} E = E_\ell$ is isomorphic to $\mathrm{End}_{F_\ell} V_\ell(A)$, that is, to the algebra of $e \times e$ matrices over F_ℓ. Since $F_\ell = \prod_{v|\ell} F_v$ it follows that $E_v = F_v \otimes_{\mathbb{Q}} E$ is a matrix algebra over F_v for $v \mid \ell$. That means E splits at all primes $v \mid \ell$.

Part (3): Let A be a simple abelian variety over k. Assume that $F = \mathbb{Q}(\pi)$ has a real place v. We may then view π as a real number, which has absolute value $q^{1/2}$, where $q = \mathrm{Card}(k)$. Consequently π is a root of the polynomial $T^2 - q$.

- If q is a square, then π is rational, $F = \mathbb{Q}$, and since we already proved that the formula $2 \dim A = [E : F]^{1/2}[F : \mathbb{Q}]$ holds, we can rule out the possibility that $E = F = \mathbb{Q}$. Hence E is non-split. We also proved that F is the center of E, and that E splits at every finite place v of F that does not divide p. By Theorem 3.5, E must be non-split at p and ∞, and the invariant must be $1/2$ at those two places. This implies $[E : F] = 4$, so E is a quaternion division algebra which does not split at p and the real place $v = \infty$. That means that the reasoning in §5.1 applies, and so A is a supersingular elliptic curve over k whose $\overline{k}$-endomorphisms are all defined over k (and necessarily $f_A = (T - q^{1/2})^2$).
- If q is not a square in $\mathbb{Q}$, then $F \cong \mathbb{Q}(\sqrt{p})$ is a real quadratic field. Also, since f_A must be a power of an irreducible polynomial over $\mathbb{Q}$, we must have $f_A = (T^2 - q)^e$ for some $e \geq 1$. Over a quadratic extension k'/k, $A' = A_{/k'}$ therefore has associated q^2-Frobenius polynomial $f_{A'} = (T - q)^{2e}$, so by the case just treated we see that A' is k'-isogenous to $A_0 \times A_0$ for a supersingular elliptic curve A_0 over k' whose "geometric" endomorphisms are all defined over k'. By the previous case, the k'-endomorphism algebra of A_0 is the quaternion division algebra D_p over $\mathbb{Q}$ that is ramified at exactly p and ∞. Let E' be the k'-endomorphism ring of A'. Then E' is a 2×2 matrix

algebra over D_p. Since $F = \mathbb{Q}[\pi]$, E is the centralizer of F in E'. By the remark after Theorem 9.2 in the appendix we have that $E \sim E' \otimes_{\mathbb{Q}} F \sim D_p \otimes_{\mathbb{Q}} F$ in $\mathrm{Br}(F)$. Since D_p does not split over $\mathbb{R}$ it follows that E does not split at either of the real primes of F.

□

The rest of §8 is devoted to the computation of $\mathrm{inv}_v(E)$ for the case $v \mid p$. We will follow the method of Tate as explained in [MW71], except that we cut down on the input from non-commutative ring theory.

8.2. **Dieudonné modules.** To compute $\mathrm{inv}_v(E)$ for $v \mid p$ we have to replace the ℓ-adic Tate module by a suitable object.

Notation: Let k be a perfect field of characteristic $p > 0$. Let W be the Witt vectors of k; *e.g.,* if k is finite of size $q = p^a$ then W is the ring of integers in the unramified extension of $\mathbb{Q}_p$ of degree a. Let σ be the unique automorphism of W which reduces to the map $x \mapsto x^p$ on the residue field k. Let $D_k := W[\mathcal{F}, \mathcal{V}]$, where $\mathcal{F}, \mathcal{V}$ are indeterminates subject to the relations

(1) $\mathcal{F}\mathcal{V} = \mathcal{V}\mathcal{F} = p$
(2) $\mathcal{F}\alpha = \alpha^\sigma \mathcal{F}$ and $\alpha\mathcal{V} = \mathcal{V}\alpha^\sigma$ for $\alpha \in W$.

Elements of the "Dieudonné ring" D_k have unique expressions as finite sums

$$a_0 + \sum_{j>0} a_j \mathcal{F}^j + \sum_{j>0} b_j \mathcal{V}^j$$

with coefficients in W, so the center of D_k is clearly $\mathbb{Z}_p[\mathcal{F}^a, \mathcal{V}^a]$ if k has finite size p^a and it is $\mathbb{Z}_p$ otherwise (i.e., if k is infinite). Some of the main conclusions in classical Dieudonné theory, as developed from scratch in [Fon77, Ch. I–III], are summarized in the following theorem:

Theorem 8.2. *There is an additive anti-equivalence of categories $G \rightsquigarrow \mathbb{D}(G)$ from the category of finite commutative k-group schemes of p-power order to the category of left D_k-modules of finite length (or equivalently, of finite W-length). Moreover,*

(1) *A group scheme G has order $p^{\ell_W(\mathbb{D}(G))}$.*
(2) *If $k \to k'$ is an extension of perfect fields with associated extension $W \to W'$ of Witt rings (e.g., the absolute Frobenius automorphism of k) then the functor $W' \otimes_W (\cdot)$ on Dieudonné modules is naturally identified with the base-change functor on finite commutative group schemes. In particular, $\mathbb{D}(G^{(p)}) \simeq \sigma^*(\mathbb{D}(G))$ as W-modules.*

(3) *Let $F_G : G \to G^{(p)}$ be the relative Frobenius morphism. The σ-semilinear action on $\mathbb{D}(G)$ induced by $\mathbb{D}(F_G)$ with respect to the isomorphism $\mathbb{D}(G^{(p)}) \simeq \sigma^*(\mathbb{D}(G))$ equals the action of $\mathcal{F}$, and G is connected if and only if $\mathcal{F}$ is nilpotent on $\mathbb{D}(G)$.*

Let A be an abelian variety over k with dimension $g \geq 1$. Let $A[p^n]$ be the finite commutative p^n-torsion group scheme of rank $(p^n)^{2g}$. We associate with A the p-divisible group $A[p^\infty]$ of height $2g$. Rather generally, for any p-divisible group $G = (G_n)_{n\geq 1}$ over k with height $h \geq 1$, we let $\mathbb{D}(G)$ denote the D_k-module $\varprojlim \mathbb{D}(G_n)$. Then by the same style of arguments used to work out the $\mathbb{Z}_\ell$-module structure of Tate modules of abelian varieties in characteristic $\neq \ell$ (resting on knowledge of the size of the ℓ-power torsion subgroups of geometric points), we use W-length to replace counting to infer that $\mathbb{D}(G)$ is a free right W-module of rank h with

$$\mathbb{D}(G)/p^r\mathbb{D}(G) \xrightarrow{\sim} \mathbb{D}(G_r)$$

for all $r \geq 1$. The p-divisible group G is connected if and only if $\mathcal{F}$ is topologically nilpotent on $\mathbb{D}(G)$ (since this is equivalent to nilpotence of $\mathcal{F}$ on each $\mathbb{D}(G_r)$).

In analogy with the ℓ-adic case we will now write T_pG for $\mathbb{D}(G)$ and T_pA for the case $G = A[p^\infty]$. The D_k-module T_pG will be the replacement for the ℓ-adic Tate module in the "classical" case, even though it is contravariant in A; its D_k-action is the analogue of the Galois action on ℓ-adic Tate modules, though this Dieudonné structure remains non-trivial when k is algebraically closed (whereas the Galois action on Tate modules is trivial for such k).

More Notation: Let L be the fraction field of W. For any p-divisible group G over k, let $V_pG := T_pG \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (and write V_pA for $G = A[p^\infty]$). Then V_pG is an L-module of rank equal to the height h of G, and it also has a left module structure over the "Laurent polynomial ring" $D_k[1/p] = L[\mathcal{F}, 1/\mathcal{F}]$ that is non-commutative if $k \neq \mathbb{F}_p$.

Here is the analogue of Tate's isogeny theorem for V_pA:

Theorem 8.3. *For any abelian variety A over k, with p-divisible group denoted $A[p^\infty]$, the $\mathbb{Q}_p$-algebra map*

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}_k^0(A) \to \mathrm{End}_k^0(A[p^\infty])$$

is an injection, and if k is finite then it is an isomorphism.

Proof. By Theorem 8.2 this is $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} (-)$ applied to the map

$$\mathbb{Z}_p \otimes \mathrm{End}_k(A) \to \mathrm{End}_k(A[p^\infty])$$

and this latter map is proved to be injective exactly as in the ℓ-adic case for $\ell \neq p$, by working with (contravariant) Dieudonné modules instead of the ℓ-adic Tate modules. As for surjectivity for finite k, we first note that the q-Frobenius endomorphism π acting $W(k)$-linearly on $\mathbb{D}(A[p^\infty])$ has the same characteristic polynomial (in $\mathbb{Z}[T]$) as it does as a $\mathbb{Z}_\ell$-linear endomorphism of the ℓ-adic Tate module of A for any $\ell \neq p$; this is true more generally for any element of $\mathrm{End}_k(A)$, and its proof is given by using Dieudonné modules in the role of Tate modules in the proof of [Mum70, Thm. 4, p. 180]. Hence, we may copy Tate's proof of surjectivity essentially verbatim (say, as in Appendix 1 of [Mum70]) by replacing ℓ-adic Tate modules with Dieudonné modules throughout, except that [Mum70, Lemma 6, App. 1] only applies to compute the L-dimension of the centralizer of the semisimple L-linear endomorphism $\mathcal{F}^a = V_p(\pi)$ acting on the L-vector space $V_p(A)$. (That is, we can compute $\dim_L \mathrm{End}_{L[\mathcal{F}^a]}(V_p(A))$.) In order to conclude the proof, it is necessary and sufficient to prove that this L-dimension is equal to the $\mathbb{Q}_p$-dimension of $\mathrm{End}_k^0(A[p^\infty]) = \mathrm{End}_{D_k[1/p]}(V_p(A))^{\mathrm{opp}}$.

The central subalgebra $F = \mathbb{Q}[\pi]$ in the finite-dimensional semisimple $\mathbb{Q}$-algebra $\mathrm{End}_k^0(A)$ must be semisimple and hence a finite product of fields; we do not assume A to be k-simple, so in particular F may not be a field. Consider the decomposition of A and $A[p^\infty]$ (in the isogeny sense) according to the idempotents of F. The action by F on $V_p(A)$ (through its action on A in the isogeny category of abelian varieties over k) commutes with the action by $D_k[1/p]$ on $V_p(A)$, and $\mathcal{F}^a \in D_k[1/p]$ acts as $V_p(\pi)$ on $V_p(A)$. Since there are no nonzero k-maps among the factor abelian varieties or p-divisible groups over k on which the central subalgebra F acts through distinct quotient fields, we may reduce the proof of Tate's theorem to the case when F is a field.

Let $m \in \mathbb{Z}[T]$ be the common characteristic polynomial for $V_\ell(\pi)$ on the $\mathbb{Q}_\ell$-vector spaces $V_\ell(A)$ (for all $\ell \neq p$) and for $V_p(\pi)$ on the L-vector space $V_p(A)$, so by the faithfulness of $V_p(A)$ as a $\mathbb{Q}_p \otimes_{\mathbb{Q}} F$-module we see that $\mathrm{rad}(m)$ is the minimal polynomial of $\pi \in F$ over $\mathbb{Q}$. Hence, $\mathbb{Q}_p \otimes_{\mathbb{Q}} F \simeq \prod_{v|p} F_v$ with $F_v \simeq \mathbb{Q}_p[T]/(m_v)$ for the monic irreducible factors $m_v \in \mathbb{Z}_p[T]$ of m over $\mathbb{Q}_p$. Each $m_v(0)$ divides $m(0) = q^{\dim A}$, so all m_v's have nonzero constant term. Since $\mathbb{Q}_p \otimes_{\mathbb{Q}} F$ acts $D_k[1/p]$-linearly on $V_p(A)$, we get a decomposition of $D_k[1/p]$-modules $V_p(A) \simeq \prod_{v|p} V_p(G_v)$ where $\prod_{v|p} G_v$ is the isogeny decomposition of $A[p^\infty]$ with respect to the idempotents of $\mathbb{Q}_p \otimes_{\mathbb{Q}} F$. Since the central element $m_v(\mathcal{F}^a) \in D_k$ acts on G_v through the element $m_v(\pi) = 0$ in F_v, $V_p(G_v)$ is a left module over the quotient algebra $C_v = D_k[1/p]/D_k[1/p]m_v(\mathcal{F}^a)$.

Using the compatible decompositions (as L-algebras and $\mathbb{Q}_p$-algebras respectively)

$$\mathrm{End}_{L[\mathcal{F}^a]}(V_p(A)) \simeq \prod_{v|p} \mathrm{End}_{L[\mathcal{F}^a]}(V_p(G_v))$$

and

$$\mathrm{End}_{D_k[1/p]}(V_p(A)) \simeq \prod_{v|p} \mathrm{End}_{C_v}(V_p(G_v)),$$

we are reduced to proving

$$\dim_L \mathrm{End}_{L[\mathcal{F}^a]}(M_v) \stackrel{?}{=} \dim_{\mathbb{Q}_p} \mathrm{End}_{C_v}(M_v)$$

for any $v|p$ and any left C_v-module M_v with finite $\mathbb{Q}_p$-dimension (e.g., $M_v = V_p(G_v)$). This general equality is valid when C_v is replaced with $D_k[1/p]/D_k[1/p]h(\mathcal{F}^a)$ for any $h \in \mathbb{Q}_p[T]$ that is a monic irreducible with nonzero constant term; a proof will be given in Corollary 8.7 as a consequence of some general calculations in non-commutative algebra (having no logical dependence on abelian varieties or p-divisible groups). □

8.3. **Restatement via left $D_k[1/p]$-modules.** Take k to be finite of size q, and A a k-simple abelian variety over k with endomorphism algebra E, so E is a central simple algebra over the subfield $F = \mathbb{Q}[\pi]$. Under the decomposition $E \otimes \mathbb{Q}_p \simeq \prod_{v|p} E_v$ with $E_v = E \otimes_F F_v$, we get a corresponding decomposition of $A[p^\infty]$ in the isogeny category of p-divisible groups over k, as a product of *nonzero* p-divisible groups G_v on which $F \otimes \mathbb{Q}_p$ acts through its quotients F_v (here we use the elementary injectivity aspect of Theorem 8.3 to know that each G_v is nonzero).

Since the Dieudonné functor is fully faithful and contravariant, and the map in Theorem 8.3 is an isomorphism for finite k, we may identify the central $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$-algebra $E \otimes \mathbb{Q}_p$ with the opposite $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$-algebra to $\mathrm{End}_{D_k[1/p]}(V_p A)$, where $F = \mathbb{Q}(\pi)$ acts through functoriality via its action on A in the isogeny category over k. In particular, $V_p(\pi)$ is the action of the central element $\mathcal{F}^a \in D_k[1/p]$, and so we get

$$E_v \simeq \mathrm{End}_k^0(G_v) \simeq \mathrm{End}_{D_k[1/p]}(V_p G_v)^{\mathrm{opp}}.$$

as finite-dimensional F_v-algebras. We conclude that the right side is a central simple F_v-algebra, and our problem is to compute its invariant.

8.4. **Passage to a central simple F_v-algebra quotient of $D_k[1/p]$.** We continue with the notation and hypotheses as in §8.3. Since π in the ring of integers of F acts on A as the q-Frobenius over k, on the finite-dimensional $\mathbb{Q}_p$-vector space $V_p(G_v)$ the $\mathbb{Q}_p$-linear operator $\mathcal{F}^a = V_p(\pi)$ acts with a characteristic polynomial that divides the common characteristic polynomial $m \in \mathbb{Q}[T] \subseteq \mathbb{Q}_p[T]$ for the q-Frobenius on each $V_\ell(A)$ over $\mathbb{Q}_\ell$ (for $\ell \neq p$) and $V_p(A)$ over L. (Explicitly, for all $n \in \mathbb{Z}$ the integer $m(n)$ is the degree of $n - \pi$ acting on A.) As we noted in the proof of Theorem 8.3, m is a power of the minimal polynomial of $\pi \in F$ over $\mathbb{Q}$, and so the decomposition $F \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{v|p} F_v$ corresponds to the pairwise distinct monic irreducible factors m_v of m over $\mathbb{Q}_p$. That is, $F_v = \mathbb{Q}_p(\pi)$ with $\pi \in F_v$ having minimal polynomial m_v over $\mathbb{Q}_p$. In particular, $m_v(0)$ divides $m(0) = q^{\dim A}$, so all m_v's have nonzero constant term.

For each $v|p$, the F_v-action on the nonzero $V_p(G_v)$ commutes with the $D_k[1/p]$-action (as it arises from an action of F_v on the p-divisible group G_v in the isogeny category over k), and the central element $m_v(\mathcal{F}^a) \in D_k[1/p]$ acts as multiplication by the element $m_v(\pi) \in F_v$ that is zero. In other words, $V_p(G_v)$ is a nonzero module over the ring

$$C_v := D_k[1/p]/D_k[1/p]m_v(\mathcal{F}^a).$$

Recall that $q = p^a$.

Theorem 8.4. *Let $h \in \mathbb{Q}_p[T]$ be a monic irreducible with $h \neq T$, and let $K = \mathbb{Q}_p[T]/(h)$. The central K-algebra $C = D_k[1/p]/D_k[1/p]h(\mathcal{F}^a)$ (with T acting as $\mathcal{F}^a$) is central simple.*

In order to prove Theorem 8.4, we require some preparations. Recall that L denotes the fraction field of $W(k)$. We have $\dim_L C = \deg(h(T^a)) = a[K : \mathbb{Q}_p]$ due to:

Lemma 8.5. *Let $\lambda \in L[T]$ be monic with positive degree d and non-vanishing constant term. Every $g \in D_k[1/p]$ can be uniquely written*

$$g = h \cdot \lambda(\mathcal{F}) + (c_0 + c_1\mathcal{F} + \cdots + c_{d-1}\mathcal{F}^{d-1})$$

with $c_0, \ldots, c_{d-1} \in L$ and $h \in D_k[1/p]$. In particular, the left $D_k[1/p]$-module $D_k[1/p]/D_k[1/p]\cdot\lambda(\mathcal{F})$ has dimension d as a left L-vector space.

Proof. The uniqueness is easily proved by chasing "least-degree" coefficients (when things are nonzero). For existence it suffices to treat the cases $g = \mathcal{F}^r$ with $r \geq d$ and $r < 0$. These go as in the commutative case (for $r < 0$ we use the non-vanishing of the constant term of λ). □

Since C is an $L \otimes_{\mathbb{Q}_p} K$-module with finite $\mathbb{Q}_p$-dimension, we obtain $\dim_K C = a[L : \mathbb{Q}_p]$. Let $(L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}]$ denote the K-algebra defined

by the relations $\mathcal{F}^a = 1 \otimes \pi$ (for $\pi \in K$) and $\mathcal{F} \cdot x = (\sigma \otimes 1)(x) \cdot \mathcal{F}$ for $x \in L \otimes_{\mathbb{Q}_p} K$, with $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$ the absolute Frobenius. This is easily checked to be a central K-algebra with dimension $a[L : \mathbb{Q}_p] = a^2$. There is a unique map of central K-algebras

$$(L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}] \to C$$

sending $\mathcal{F}$ to $\mathcal{F}$ and L to L by the identity map, and this is clearly surjective. By consideration of K-dimensions, it is an isomorphism. Theorem 8.4 therefore will follow from:

Theorem 8.6. *The central K-algebra $(L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}]$ is K-isomorphic to a matrix algebra over a cyclic K-algebra.*

Remark. Cyclic algebras are a special class of central simple algebras, studied by Dickson before the advent of the general theory.

Proof. We first construct the cyclic K-algebra Δ over which the K-algebra $(L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}]$ will be proved to be a matrix algebra. Let f be the absolute residue degree of K, and let $g := \gcd(f, a)$. Let $L \cap K \subseteq K$ denote the maximal unramified subextension of K that embeds into L (over $\mathbb{Q}_p$), so $g = [L \cap K : \mathbb{Q}_p]$. We arbitrarily choose one of the g embeddings $L \cap K \to L$ as cyclic extensions of $\mathbb{Q}_p$, and let LK denote the resulting linearly disjoint compositum $L \otimes_{L \cap K} K$.

Clearly LK/K is unramified with degree a/g. Let

$$\theta : L \otimes_{\mathbb{Q}_p} K \to LK$$

be the resulting projection map. Let Δ be the central K-algebra $(LK)[\mathcal{F}']$ defined with relations $(\mathcal{F}')^{a/g} = \pi \in K$ and $\mathcal{F}' \cdot x' = \sigma'(x') \cdot \mathcal{F}'$ where $\sigma' : LK \simeq LK$ is the $L \cap K$-automorphism of order a/g induced by σ^g on L and the identity on K. Thus, $\sigma'(\theta(x)) = \theta((\sigma^g \otimes 1)(x))$ for $x \in L \otimes_{\mathbb{Q}_p} K$, and we have a natural isomorphism of K-algebras

$$L \otimes_{\mathbb{Q}_p} K \simeq \prod_{j=1}^{g} LK$$

defined by

$$x \mapsto (\theta(x), \theta((\sigma \otimes 1)(x)), \ldots, \theta((\sigma^{g-1} \otimes 1)(x))).$$

The central K-algebra Δ is a cyclic K-algebra; in classical notation, $\Delta = (LK/K, \sigma', \pi)$, where LK is a cyclic (unramified) extension of K and σ' is a chosen generator of its Galois group.

Now consider the natural map of central K-algebras

$$\xi : (L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}] \to M_g(\Delta)$$

defined by

$$x \mapsto \begin{pmatrix} \theta(x) & 0 & \dots & 0 \\ 0 & \theta((\sigma \otimes 1)(x)) & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \theta((\sigma^{g-1} \otimes 1)(x)) \end{pmatrix}$$

for $x \in L \otimes_{\mathbb{Q}_p} K$ and

$$\mathcal{F} \mapsto \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & 0 & \dots & \ddots & \vdots \\ \vdots & \vdots & 0 & \dots & 1 \\ \mathcal{F}' & 0 & 0 & \dots & 0 \end{pmatrix}$$

The map ξ is obviously a well-defined K-algebra homomorphism, and it is easy to check that both sides have the same $\mathbb{Q}_p$-dimension. To prove that ξ is an isomorphism, it suffices to check surjectivity.

The decomposition of $L \otimes_{\mathbb{Q}_p} K$ as a product of copies of LK shows that the image of ξ contains the diagonal matrices whose entries are elements of $LK \subseteq \Delta$. Moreover, $\xi(\mathcal{F}^g)$ is the diagonal matrix whose diagonal entries are all equal to $\mathcal{F}' \in \Delta$. Thus, by the definition of Δ we see that the image of ξ contains all diagonal matrices in $M_g(\Delta)$. Left-multiplication by $\xi(\mathcal{F})$ carries the set of diagonal matrices onto the set of matrices of the form

$$\begin{pmatrix} 0 & \delta_2 & 0 & \dots & 0 \\ 0 & 0 & \delta_3 & \dots & 0 \\ \vdots & 0 & \dots & \ddots & \vdots \\ \vdots & \vdots & 0 & \dots & \delta_g \\ \mathcal{F}'\delta_1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

with arbitrary $\delta_1, \dots, \delta_g \in \Delta$, and so since $\mathcal{F}' \in \Delta$ has a multiplicative inverse (as $(\mathcal{F}')^{a/g} = \pi \in K^\times$) it follows that the image of ξ contains the matrix

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & 0 & \dots & \ddots & \vdots \\ \vdots & \vdots & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Powers of this matrix, together with arbitrary diagonal matrices in $M_g(\Delta)$, generate $M_g(\Delta)$ under the operations of multiplication and addition. This establishes surjectivity. □

Remark. For later purposes, it is convenient to describe the cyclic algebra Δ in terms of an arithmetic Frobenius generator ϕ of the Galois group of the unramified extension LK/K. With notation as used above, we claim that $\Delta = (LK/K, \sigma', \pi)$ is K-isomorphic to the cyclic K-algebra $(LK/K, \phi, \pi^{f/g})$. This amounts to checking that ${\sigma'}^{f/g} = \phi$ in $\mathrm{Gal}(LK/K)$, and so we just have to compare these on the residue field of L (viewed inside that of LK). Since σ' reduces to $x \mapsto x^{p^g}$ on the residue field of L, ${\sigma'}^{f/g}$ reduces to $x \mapsto x^{p^f}$ on this residue field. But f is the residual degree for K over $\mathbb{Q}_p$, so we are done.

It is an elementary result in the theory of simple rings that (up to isomorphism) there is a unique simple module over such a ring and that all finite modules are isomorphic to a direct sum of copies of this simple module. Thus, up to isomorphism there is a unique simple $D_k[1/p]$-module V killed by the central element $h(\mathcal{F}^a)$, and so for any nonzero left C-module M with finite $\mathbb{Q}_p$-dimension we have $M \simeq V^{\oplus r}$ for some $r \geq 1$ (with C denoting the quotient of $D_k[1/p]$ modulo the central element $h(\mathcal{F}^a)$). In particular, $\mathrm{End}_{D_k[1/p]}(M)$ is a matrix algebra over the division ring $D = \mathrm{End}_C(V)$. Since there is an isomorphism of left C-modules $C \simeq V^{\oplus r_0}$ for some $r_0 \geq 1$, so $M_{r_0}(D) = \mathrm{End}_C(C) = C^{\mathrm{opp}}$, D has center K and in the Brauer group of K we have $D \sim C^{\mathrm{opp}}$. Hence, the class of $\mathrm{End}_{D_k[1/p]}(M)^{\mathrm{opp}}$ in $\mathrm{Br}(K)$ is the same as that of C for any nonzero finitely generated left C-module M. For any such M we have the following result that completes the final step in the proof of Theorem 8.3:

Corollary 8.7. *Let $h \in \mathbb{Q}_p[T]$ be a monic irreducible with $h \neq T$, and let $C = D_k[1/p]/D_k[1/p]h(\mathcal{F}^a)$. For any finite left C-module M,*

$$\dim_L \mathrm{End}_{L[\mathcal{F}^a]}(M) = \dim_{\mathbb{Q}_p} \mathrm{End}_C(M). \tag{8.2}$$

Since $L[\mathcal{F}, 1/\mathcal{F}] = D_k[1/p]$ and $\mathrm{End}_C(M) = \mathrm{End}_{L[\mathcal{F}]}(M)$ ($\mathcal{F}$ acts invertibly on M, as $h(0) \in \mathbb{Q}_p^\times$), the equality $[L : \mathbb{Q}_p] = a$ suggests the possibility that one may be able to deduce (8.2) by some general nonsense with Galois descent. However, it seems that the proof requires fine structural information concerning C.

Proof. Let V be a simple left C-module and let $K = \mathbb{Q}_p[T]/(h)$. We have $M \simeq V^{\oplus r}$ for some $r \geq 0$. The two sides of (8.2) for M are each r^2 times the two sides of (8.2) for V in the role of M. Hence, the truth of (8.2) is independent of the choice of r, so it suffices to verify this identity for one $M \neq 0$. We choose $M = C$. Since $\mathrm{End}_C(C) = C^{\mathrm{opp}}$ (with action through right multiplications on C),

$$\dim_{\mathbb{Q}_p} \mathrm{End}_C(C) = [L : \mathbb{Q}_p] \dim_L(C^{\mathrm{opp}}) = [L : \mathbb{Q}_p] \deg h(T^a)$$

by Lemma 8.5 (with $\lambda = h(T^a)$ satisfying $\lambda(0) \neq 0$ since the irreducible monic h is not T). Because $\deg h = [K : \mathbb{Q}_p]$ and $[L : \mathbb{Q}_p] = a$ we may rewrite this as

$$\dim_{\mathbb{Q}_p} \mathrm{End}_C(C) = \frac{[L \otimes_{\mathbb{Q}_p} K : \mathbb{Q}_p]a^2}{[L : \mathbb{Q}_p]},$$

and so by expressing an L-dimension as $[L : \mathbb{Q}_p]^{-1}$ times a $\mathbb{Q}_p$-dimension it is equivalent to prove

$$\dim_{\mathbb{Q}_p} \mathrm{End}_{L[\mathcal{F}^a]}(C) = [L \otimes_{\mathbb{Q}_p} K : \mathbb{Q}_p]a^2.$$

It therefore suffices to show that $\mathrm{End}_{L[\mathcal{F}^a]}(C)$ is isomorphic as a $\mathbb{Q}_p$-algebra to an $a \times a$ matrix algebra over $L \otimes_{\mathbb{Q}_p} K$.

Let $t \in K = \mathbb{Q}_p[T]/(h)$ denote the residue class of T, so $K = \mathbb{Q}_p[t]$. We saw above Theorem 8.6 that as $L[\mathcal{F}^a]$-algebras $C \simeq (L \otimes_{\mathbb{Q}_p} K)[\mathcal{F}]$ where the right side has relations $\mathcal{F}^a = 1 \otimes t$ and $\mathcal{F} \cdot x = (\sigma \otimes 1)(x)$ for all $x \in L \otimes_{\mathbb{Q}_p} K$. Hence, the $L[\mathcal{F}^a]$-endomorphism ring of C is the same as the $L \otimes_{\mathbb{Q}_p} K$-endomorphism ring of C, and this in turn is indeed an $a \times a$ matrix algebra over $L \otimes_{\mathbb{Q}_p} K$. □

8.5. **Computing with a cyclic algebra.** We now return to our original problem of computing $\mathrm{inv}_v(E_v)$ where $E_v = F_v \otimes_F \mathrm{End}^0_k(A)$ for a k-simple abelian variety A and $F = \mathbb{Q}(\pi)$ is the central subfield of $\mathrm{End}^0_k(A)$ generated by the q-Frobenius endomorphism. By Theorem 8.4 (with $h = m_v$ and $K = F_v$), $C_v = D_k[1/p]/D_k[1/p]m_v(\mathcal{F}^a)$ is a central simple F_v-algebra. Writing V_v to denote a simple left C_v-module (unique up to isomorphism) we have $V_p(G_v) \simeq V_v^{\oplus r_v}$ as left $D_k[1/p]$-modules for some $r_v \geq 1$, so the F_v-algebra $\mathrm{End}_{D_k[1/p]}(V_p(G_v))$ is a matrix algebra over the division ring $D_v^{\mathrm{opp}} = \mathrm{End}_{D_k[1/p]}(V_v)$. For any $N \geq 1$, the F_v-algebra $\mathrm{End}_{D_k[1/p]}(V_v^{\oplus N})$ is a matrix algebra over the division ring $\mathrm{End}_{D_k[1/p]}(V_v)$ (as F_v-algebras), and so its class in $\mathrm{Br}(F_v)$ is independent of N (and is opposite the class of E_v). But C_v is $D_k[1/p]$-isomorphic to a finite direct sum of copies of V_v as left $D_k[1/p]$-modules, so the F_v-algebra $\mathrm{End}_{D_k[1/p]}(C_v)$ also lies in this same Brauer class. This endomorphism ring is the central simple F_v-algebra C_v^{opp} via C_v acting on itself through right multiplications. Thus, in $\mathrm{Br}(F_v)$,

$$E_v \simeq \mathrm{End}_{D_k[1/p]}(V_p(G_v))^{\mathrm{opp}} \sim \mathrm{End}_{D_k[1/p]}(C_v)^{\mathrm{opp}} = (C_v^{\mathrm{opp}})^{\mathrm{opp}} \simeq C_v.$$

By the Remark following the proof of Theorem 8.6 (with $K = F_v$) this class is represented by the cyclic F_v-algebra

$$\Delta_v = (LF_v/F_v, \phi, \pi^{f_v/g_v})$$

that rests on the generator ϕ of $\mathrm{Gal}(LF_v/F_v)$ and the element π^{f_v/g_v} in $F_v^\times$ (where $f_v = f(v|p)$ and $g_v = \gcd(f_v, a)$). Since $[LF_v : F_v] = a/g_v$,

by the formula in Theorem 9.4 for local invariants of certain cyclic algebras over non-archimedean local fields we get the formula

$$\mathrm{inv}_v(\Delta_v) = \frac{1}{a/g_v} \cdot v(\pi^{f_v/g_v}) = (f_v/g_v) \cdot v(\pi) g_v/a = (f_v/a) \cdot v(\pi).$$

Let e_v be the ramification index of F_v over $\mathbb{Q}_p$. Then $e_v f_v = [F_v : \mathbb{Q}_p]$. We have

$$v(q) = a \cdot v(p) = a \cdot e_v,$$

so $a = v(q)/e_v$. This implies that

$$\mathrm{inv}_v(\Delta_v) = \frac{f_v}{a} \cdot v(\pi) = \frac{e_v f_v}{v(q)} \cdot v(\pi) = \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p].$$

9. Appendix

In this appendix we treat two topics: the interaction of Frobenius endomorphisms with Weil restriction for abelian varieties, and the formula for the local invariant of certain cyclic algebras over a local field.

Let k'/k be an extension of finite fields with respective sizes q' and q. Let A' be an abelian variety over k', and $A = \mathrm{Res}_{k'/k}(A)$ its Weil restriction to k (an abelian variety of dimension $[k' : k] \dim A$ over k). Let $R' \subseteq \mathrm{End}^0_{k'}(A')$, $R \subseteq \mathrm{End}^0_k(\mathrm{Res}_{k'/k} A')$ be the $\mathbb{Q}$-subalgebras generated by the q'-Frobenius π' and the q-Frobenius π for A' and A respectively.

Lemma 9.1. *Via* $\mathrm{Res}_{k'/k} : \mathrm{End}^0_{k'}(A') \to \mathrm{End}^0_k(\mathrm{Res}_{k'/k} A')$ *we have* $\pi' \mapsto \pi^{[k':k]}$. *That is,* $\mathrm{Res}_{k'/k}(\pi') = \pi^{[k':k]}$.

Proof. On the ℓ-adic Tate modules, this says $\mathrm{Ind}^k_{k'}(\pi')$ on $\mathrm{Ind}^k_{k'}(V_\ell A')$ is $\pi^{[k':k]}$. This is clear since $G_k, G_{k'}$ are commutative and

$$\begin{pmatrix} 0 & 0 & \dots & 0 & \pi' \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}^{[k':k]} = \begin{pmatrix} \pi' & \dots & 0 \\ 0 & \ddots & \vdots \\ 0 & \dots & \pi' \end{pmatrix}$$

as block matrices. □

Using the lemma, we have a map of $\mathbb{Q}$-algebras

$$\phi : R \otimes_{R'} \mathrm{End}^0_{k'}(A') \to \mathrm{End}^0_k(\mathrm{Res}_{k'/k} A'),$$

where $R' \to R$ via $\pi' \mapsto \pi^{[k':k]}$. (Since R is in the center of the target.)

Theorem 9.2. *The map* ϕ *is an isomorphism.*

Proof. Apply $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} (-)$ to convert it into the natural map

$$\mathbb{Q}_\ell[\pi] \otimes_{\mathbb{Q}_\ell[\pi']} \mathrm{End}_{\mathbb{Q}_\ell[\pi']}(V_\ell A') \to \mathrm{End}_{\mathbb{Q}_\ell[\pi]}(\mathrm{Ind}_{G_{k'}}^{G_k} V_\ell A').$$

We view $V_\ell A'$ as a $\mathbb{Q}_\ell[T']$-module with T' acting as π'. We have

$$\begin{aligned} \mathrm{Ind}_{G_{k'}}^{G_k} T_\ell A' &\cong \mathrm{Ind}_{\mathbb{Z}_\ell[T',T'^{-1}]}^{\mathbb{Z}_\ell[T,T^{-1}]} T_\ell A' \\ &= \mathbb{Z}_\ell[T,T^{-1}] \otimes_{\mathbb{Z}_\ell[T',T'^{-1}]} T_\ell A' \\ &= \mathbb{Z}_\ell[T] \otimes_{\mathbb{Z}_\ell[T']} T_\ell A'. \end{aligned}$$

Thus, $\mathrm{Ind}_{G_k}^{G_{k'}} V_\ell A' \cong \mathbb{Q}_\ell[T] \otimes_{\mathbb{Q}_\ell[T']} V_\ell A'$. We can apply $\overline{\mathbb{Q}}_\ell \otimes_{\mathbb{Q}_\ell} (-)$, so we want to study the natural $\overline{\mathbb{Q}}_\ell[T]$- algebra map

$$\overline{\mathbb{Q}}_\ell[\pi] \otimes_{\overline{\mathbb{Q}}_\ell[\pi']} \mathrm{End}_{\overline{\mathbb{Q}}_\ell[T']}(M') \to \mathrm{End}_{\overline{\mathbb{Q}}_\ell[T]}(\overline{\mathbb{Q}}_\ell[T] \otimes_{\overline{\mathbb{Q}}_\ell[T']} M')$$

for $\overline{\mathbb{Q}}_\ell[T']$-modules M' with π' acting as T' and $\pi \mapsto T$. Note that $M' = V_\ell A'$ is a semisimple $\overline{\mathbb{Q}}_\ell[T']$-module on which $T' = \pi'$ invertibly. Consider any semisimple $\overline{\mathbb{Q}}_\ell[T']$-module M' on which T' acts invertibly. Since $\overline{\mathbb{Q}}_\ell$ is algebraically closed, we have

$$M' \cong \prod_{i=1}^{r} (\overline{\mathbb{Q}}_\ell[T']/(T' - \alpha_i))^{\oplus e_i}$$

as $\overline{\mathbb{Q}}_\ell[T']$-modules for distinct $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}_\ell^\times$. Thus,

$$\overline{\mathbb{Q}}_\ell[T] \otimes_{\overline{\mathbb{Q}}_\ell[T']} M' \cong \prod_{i=1}^{r} (\overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i))^{\oplus e_i}$$

as $\overline{\mathbb{Q}}_\ell[T]$-modules with $f = [k' : k]$. We have, via the Chinese Remainder Theorem and since all $\alpha_i \neq 0$, $\overline{\mathbb{Q}}_\ell[\pi] \xrightarrow{\sim} \prod \overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i)$ as $\overline{\mathbb{Q}}_\ell[\pi]$ is the $\overline{\mathbb{Q}}_\ell$-subalgebra generated by the T-action on $\overline{\mathbb{Q}}[T] \otimes_{\overline{\mathbb{Q}}_\ell[T']} M'$.

Thus, the map of interest is the natural map

$$\prod_i (\overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i)) \otimes_{\overline{\mathbb{Q}}_\ell[T']} M_{e_i}(\overline{\mathbb{Q}}_\ell[T']/(T' - \alpha_i)) \to$$

$$\prod_i M_{e_i}(\overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i)).$$

Since

$$\overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i) \otimes_{\overline{\mathbb{Q}}_\ell[T']} \overline{\mathbb{Q}}_\ell[T']/(T' - \alpha_i) \to \overline{\mathbb{Q}}_\ell[T]/(T^f - \alpha_i)$$

is an isomorphism, we are done. □

Remark. In the special case $A' = k' \otimes_k A$, with $n = [k' : k]$, the q-Frobenius polynomial for $\mathrm{Res}_{k'/k}A'$ is the polynomial

$$\prod_{\zeta^n=1} f_A(\zeta T) \in \mathbb{Q}[T]$$

with degree $n \deg f_A = 2n\dim A$, so if f_A is a polynomial in T^n then this polynomial is $f_A^n = f_{A^n}$. Hence, assuming f_A is a polynomial in T^n we obtain that $\mathrm{Res}_{k'/k}A'$ is k-isogenous to A^n, so this gives us an R-algebra isomorphism of $R \otimes_{R'} \mathrm{End}_{k'}(A')$ to a matrix algebra, $R \otimes_{R'} \mathrm{End}_{k'}(A') \xrightarrow{\sim} M_n(\mathrm{End}_k^0(A))$ where R is identified with the usual $\mathbb{Q}[\pi] \subset \mathrm{End}_k^0 A$ compatibly. The theorem then gives us

$$F \otimes_{F'} \mathrm{End}_{k'}^0(\tilde{A}') \sim \mathrm{End}_k^0(A) \ \text{ in } \mathrm{Br}(F)$$

when A is k-simple if two properties hold: (i) f_A a polynomial in $T^{[k':k]}$, and (ii) there is a *unique* k'-simple factor $\tilde{A}'$ of $k' \otimes_k A$. Here, F and F' are the $\mathbb{Q}$-subalgebras generated by the Frobenius automorphisms π and π' relative to k and k' on A and $\tilde{A}'$ respectively. In fact, (i) implies (ii) for k-simple A. Indeed, if $f_A = h(T^{[k':k]})$ then $f_{k' \otimes_k A} = h^n$, and if moreover A is k-simple then $h = g^m$ for some $m \geq 1$ and irreducible $g \in \mathbb{Q}[T]$, so $f_{k' \otimes_k A} = g^{mn}$. This implies (ii), by Theorem 1.1.

Now we turn to the second topic in this appendix, the computation of the local invariant of certain cyclic algebras over non-archimedean local fields. It is this formula that ultimately provides the explicit determination of the local invariants for the endomorphism algebras of abelian varieties over finite fields. We first record a general lemma:

Lemma 9.3. *Let K be a field and let K'/K be a cyclic extension. Fix a generator s' of $\Gamma = \mathrm{Gal}(K'/K)$. Let $\chi_{s'} : \Gamma \to \mathbb{Q}/\mathbb{Z}$ be the unique homomorphism sending s' to $1/[K' : K]$, and let $\theta_{s'} = \delta(\chi_{s'}) \in \mathrm{H}^2(\Gamma, \mathbb{Z})$.*

(1) *For $c \in K^\times$, the class of the cyclic algebra $(K'/K, s', c)$ in $\mathrm{Br}(K)$ is the image of $c \bmod \mathrm{N}_K^{K'}(K'^\times)$ under the Tate periodicity isomorphism*

$$K^\times/\mathrm{N}_K^{K'}(K'^\times) = \widehat{\mathrm{H}}^0(\Gamma, K'^\times) \overset{\cup\theta_s}{\simeq} \mathrm{H}^2(\Gamma, K'^\times) \subseteq \mathrm{Br}(K).$$

(2) *If K_0'/K is a subextension and $s_0' = s'|_{K_0'}$ then*

$$[(K_0'/K, s_0', c)] = [(K'/K, s', c^{[K':K_0']})]$$

in $\mathrm{Br}(K)$.

Proof. The first part is an explicit cocycle calculation via unwinding definitions and using the cup-product compatibility of the δ-functorial

map $\mathrm{H}^\bullet(\Gamma,\cdot) \to \widehat{\mathrm{H}}^\bullet(\Gamma,\cdot)$ (using Tate cohomology only in non-negative degrees). The second part follows from the first via the commutativity of the diagram

$$\begin{array}{ccc} K^\times/\mathrm{N}(K_0'^\times) & \xrightarrow{\simeq} & \mathrm{H}^2(K_0'/K, K_0'^\times) \\ \downarrow & & \downarrow \mathrm{inf} \\ K^\times/\mathrm{N}(K'^\times) & \xrightarrow[\simeq]{} & \mathrm{H}^2(K'/K, K'^\times) \end{array}$$

(which in turn follows from the definitions of the horizontal isomorphisms and both the δ-functoriality and cup product compatibilities of inflation maps). □

Take K to be a non-archimedean local field, and define

$$\mathrm{inv}_K : \mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$$

as in §3. By Lemma 9.3 and the existence of unramified splitting fields for all Brauer classes of K, it follows that every element of $\mathrm{Br}(K)$ is represented by a cyclic algebra of the form $(K'/K, \phi, c)$ with K'/K a finite unramified extension, $\phi \in \mathrm{Gal}(K'/K)$ the *arithmetic Frobenius* generator, and $c \in K^\times$ an element. (We could also work with geometric Frobenius generators, but for the applications to abelian varieties it is the cyclic algebras resting on arithmetic Frobenius that naturally arise in the analysis of the Dieudonné modules.) The main result is:

Theorem 9.4. *Let K be a non-archimedean local field and K'/K an unramified finite extension. Let $\phi \in \mathrm{Gal}(K'/K)$ be the arithmetic Frobenius element. For any $c \in K^\times$, the cyclic K-algebra $(K'/K, \phi, c)$ has local invariant in $\mathbb{Q}/\mathbb{Z}$ represented by* $\mathrm{ord}_K(c)/[K' : K]$.

Proof. The normalized valuation for K identifies $K^\times/\mathrm{N}_K^{K'}(K'^\times)$ with $\mathbb{Z}/[K' : K]\mathbb{Z}$, so $[(K'/K, \phi, c)] \in \mathrm{Br}(K)$ only depends on the ratio $\mathrm{ord}_K(c)/[K' : K]$. In particular, we may change c by a unit multiple so as to reduce to the case when c is a power of a local uniformizer of K, and by passing to a suitable subextension over K we may reduce to the case when $\mathrm{ord}_K(c)$ is relatively prime to $[K' : K]$. In this case the class of c in $K^\times/\mathrm{N}_K^{K'}(K'^\times)$ has order $[K' : K]$ and so the cyclic K-algebra $(K'/K, \phi, c)$ of degree $[K' : K]^2$ is necessarily a *division algebra* (due to period dividing the index).

A central division algebra D over K admits a unique valuation extending the normalized valuation on K [Ser79, Ch. XII, §2], and there is a classical procedure that uses this valuation to compute $\mathrm{inv}_K([D])$ as follows. Let

$$\mathrm{ord}_D = \mathrm{ord}_K \circ \mathrm{Nrd}_D : D^\times \to \mathbb{Z}$$

(with Nrd_D denoting the reduced norm), so if $[D : K] = n^2$ then $(1/n)\mathrm{ord}_D$ restricts to the normalized valuation on $K^\times$. Since we use the method of non-abelian cohomology (as in [Ser79, Ch. X, §5]) to identify $\mathrm{H}^2(L/K, L^\times)$ with the subgroup of classes in $\mathrm{Br}(K)$ split by a Galois extension L/K and we take arithmetic Frobenius as the preferred topological generator for the Galois group of a finite field, after some explicit unwinding of definitions and calculation with 2-cocycles one finds

$$\mathrm{inv}_K([D]) = -\frac{\mathrm{ord}_D(\gamma)}{n} = -\frac{\mathrm{ord}_D(\gamma^n)}{n^2},$$

where (Skolem–Noether!) $\gamma \in D^\times$ satisfies $\gamma x \gamma^{-1} = \phi^{-1}(x)$ for x in a copy of the degree-n unramified extension K_n/K within D (so $\gamma^n \in K_n^\times$). Taking $D = (K'/K, \phi, c)$ we thereby get

$$\mathrm{inv}_K([D]) = -\frac{\mathrm{ord}_D(1/c)}{n^2} \bmod \mathbb{Z} = \frac{\mathrm{ord}_K(c)}{n} \bmod \mathbb{Z}.$$

□

References

[AT68] E. Artin and J. Tate. *Class field theory*. Addison-Wesley, New York, 1968.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. Reprint of the 1967 original.

[Fon77] Jean-Marc Fontaine. *Groupes p-divisibles sur les corps locaux*. Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48.

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[Lam91] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[MW71] J. S. Milne and W. C. Waterhouse. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, with a foreword by M. J. Taylor.

[Ser79] J-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

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

[Tat68] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini. *Séminaire Bourbaki*, 21:95–110, 1968.