On the Tate and Standard Conjectures over Finite Fields (version 1.1)

J. S. Milne

July 23, 2019

Abstract

For an abelian variety over a finite field, Clozel (1999) showed that l-homological equivalence coincides with numerical equivalence for infinitely many l, and the author (1999) gave a criterion for the Tate conjecture to follow from Tate's theorem on divisors. We generalize both statements to motives, and apply them to other varieties including $K3$ surfaces.

Contents

Let X be a motive for rational equivalence over $\mathbb{F}_q$, and let ω be the fibre functor defined by a standard Weil cohomology theory. Assume that the Frobenius element π_X of X acts semisimply on $\omega(X)$. Then $\mathbb{Q}[\pi_X]$ has a unique positive involution $\alpha \mapsto \alpha'$, and we let S denote the algebraic group over $\mathbb{Q}$ such that $S(\mathbb{Q}) = \{a \in \mathbb{Q}[\pi] \mid a \cdot a' = 1\}$.

We let $\bigotimes V$ denote the tensor algebra $\bigoplus_{n\in\mathbb{N}} V^{\otimes n}$ of a finite-dimensional vector space V and $\langle X\rangle^{\otimes}$ the pseudo-abelian rigid tensor subcategory generated by a motive X and the Tate object.

THEOREM 0.1. *Let X be a motive of weight m over $\mathbb{F}_q$ whose Frobenius element π_X acts semisimply on $\omega(X)$.*

(a) *The $\mathbb{Q}$-algebra $(\bigotimes \omega(X))^S$ is generated by $\omega(X^{\otimes 2})^S$:*

$$(\bigotimes \omega(X))^S = \mathbb{Q}[\omega(X^{\otimes 2})^S].$$

(b) *If $X^{\otimes 2}(m)$ satisfies the Tate conjecture and S is generated by $\pi_X/q^{m/2}$, then the Tate conjecture holds for all motives in $\langle X\rangle^{\otimes}$.*

In fact, we prove a more general statement (Theorem 3.7).

Our next theorem generalizes the theorem of Clozel 1999 (see also Deligne 2009). Let X be a motive over $\mathbb{F}_q$ for rational equivalence and X_l (resp. X_{num}) the image of X in the category of motives for l-adic homological equivalence (resp. for numerical equivalence).

THEOREM 0.2. *Let X be a motive of weight m over $\mathbb{F}_q$. If $X^{\otimes 2}(m)$ satisfies the full Tate conjecture, then there exists an infinite set of prime numbers $P(X)$, depending only on the centre of* $\mathrm{End}(X_{\mathrm{num}})$*, such that the functor*

$$\langle X_l \rangle^{\otimes} \to \langle X_{\mathrm{num}} \rangle^{\otimes}$$

is fully faithful for all $l \in P(X)$.

In fact, we prove a stronger statement (Theorem 4.3 et seq.).

On applying these statements to h^1 of an abelian variety, we recover the theorems of Clozel and the author mentioned above. On applying Theorem 0.1 to the motive of a $K3$ surface V of height 1, we find that the Tate conjecture holds for all powers of V, thereby recovering a theorem of Zarhin. On applying Theorem 0.2 to the motive of a general $K3$ surface V, we find that there exist infinitely many primes l such that l-homological equivalence coincides with numerical equivalence for all powers of V.

ASIDE 0.3. Our proof of Theorem 0.1 follows the proof for abelian varieties in Milne 1999. However, our proof of Theorem 0.2 is simpler than the proofs for abelian varieties in Clozel 1999 and Deligne 2009; in particular, it avoids using the standard conjecture of Lefschetz type.

ASIDE 0.4. There is the following general procedure for producing infinite sequences of new theorems. Take a theorem about abelian varieties and restate and prove it for motives. Now apply the motivic result to the motive of *any* variety to obtain a new theorem. In practice, this process does not work well because much more is known to be true about abelian varieties and their motives than about general motives. Nevertheless, in this article, we show that it can yield new results.

Notation and Conventions

All algebraic varieties are smooth and projective. Complex conjugation on $\mathbb{C}$ and its subfields is denoted by ι. The field of q elements, q a power of the prime p, is denoted by $\mathbb{F}_q$. The symbol l always denotes a prime number, possibly p. For a perfect field k, we let $W(k)$ denote the ring of Witt vectors of k and $B(k)$ the field of fractions of $W(k)$. For tensor categories, we follow the conventions of Deligne and Milne 1982.

1 Statement of the Tate conjecture for motives

Categories of motives

We refer the reader to Scholl 1994 for the basic formalism of motives. In particular, a motive over a field k is a triple (V, e, m) with V a variety over k, e an algebraic correspondence such that $e^2 = e$, and m an integer. When the Künneth components p_i of the diagonal are algebraic, we use them to modify the commutativity constraint. We write $h^i(V)(m)$ for (V, p_i, m). The category of motives over a field k defined by an admissible equivalence relation $\sim$ is denoted by $\mathsf{Mot}_{\sim}(k)$. It is a pseudo-abelian rigid tensor category with $\mathrm{End}(\mathbb{1}) = \mathbb{Q}$, and if V is of pure dimension d, then the motive dual to (V, e, m) is

$$(V, e, m)^{\vee} = (V, e^t, d - m)$$

(Saavedra Rivano 1972, VI, 4.1.3.5). We let γ denote the functor

$$X \rightsquigarrow \mathrm{Hom}(\mathbb{1}, X)\colon \mathsf{Mot}_{\sim}(k) \to \mathsf{Vec}_{\mathbb{Q}}.$$

For example, if $X = (V, e, m)$, then $\gamma(X) = eA^m_{\sim}(V)$ (algebraic cycles of codimension m modulo $\sim$ with $\mathbb{Q}$-coefficients). Similarly, $\gamma(X^\vee) = e^t A^{d-m}_{\sim}(V)$, and the intersection product $A^m_{\sim}(V) \times A^{d-m}_{\sim}(V) \to \mathbb{Q}$ defines an intersection product

$$\gamma(X) \times \gamma(X^\vee) \to \mathbb{Q}.$$

We write rat for rational equivalence, num for numerical equivalence, and hom(l) (or just l) for the equivalence relation defined by the standard l-adic Weil cohomology theory, We have categories of motives and tensor functors

$$X \rightsquigarrow X_l \rightsquigarrow X_{\mathrm{num}}\colon \mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q) \to \mathsf{Mot}_{\mathrm{hom}(l)}(\mathbb{F}_q) \to \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q).$$

The category $\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$ is tannakian (Jamsen 1992).

The Tate conjectures

Let X be a motive in $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$ and l a prime number. The standard l-adic Weil cohomology theory $V \rightsquigarrow H^*_l(V)$ is crystalline cohomology if $l = p$ and étale cohomology if $l \neq p$. Let Q denote its coefficient field; thus $Q = B(\mathbb{F}_q)$ if $l = p$ and $\mathbb{Q} = \mathbb{Q}_l$ if $l \neq p$. Let ω_l denote the tensor functor $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q) \to \mathsf{Vec}_Q$ defined by H^*_l. The vector space $\omega_l(X)$ is equipped with a Q-linear Frobenius operator $\pi = \pi_X$. For example, if $l = p$, then $\omega_l(X)$ is an F-isocrystal, and $\pi_X = F^n$, where $q = p^n$.

The functor ω_l defines a $\mathbb{Q}$-linear map

$$\gamma(X) \overset{\mathrm{def}}{=} \mathrm{Hom}(\mathbb{1}, X) \xrightarrow{\omega_l} \mathrm{Hom}(\omega_l(\mathbb{1}), \omega_l(X)) \simeq \omega_l(X), \tag{1}$$

and we let $A_l(X)$ denote its image. Thus $A_l(X)$ is a $\mathbb{Q}$-subspace of $\omega_l(X)$ canonically isomorphic to $\gamma(X_l)$. The inclusion $A_l(X) \subset \omega_l(X)$ extends to a Q-linear map

$$c \otimes a \mapsto ca\colon Q \otimes_{\mathbb{Q}} A_l(X) \to \omega_l(X)^{\pi_X}. \tag{2}$$

Let $(X^\vee, \mathrm{ev})$ be the dual motive. The morphism $\mathrm{ev}\colon X^\vee \otimes X \to \mathbb{1}$ induces a perfect pairing $\omega_l(X^\vee) \times \omega_l(X) \to Q$, compatible with the Frobenius maps, which restricts to pairings

$$\begin{array}{ccccc} \omega(X^\vee)^\pi & \times & \omega(X)^\pi & \longrightarrow & Q \\ \cup & & \cup & & \cup \\ A_l(X^\vee) & \times & A_l(X) & \longrightarrow & \mathbb{Q}. \end{array} \tag{3}$$

The lower pairing is intersection product.

There are the following conjectural statements.

$T(X, l)$: The map (2) is surjective, i.e., $Q \cdot A_l(X) = \omega_l(X)^{\pi_X}$.

$I(X, l)$: The map (2) is injective, i.e., $Q \otimes A_l(X) \hookrightarrow \omega_l(X)$.

$D(X, l)$: The right kernel $N(X)$ of the pairing $A_l(X^\vee) \times A_l(X) \to \mathbb{Q}$ is zero; equivalently, the map $\gamma(X_l) \to \gamma(X_{\mathrm{num}})$ is an isomorphism.

$S(X,l)$: The eigenvalue 1 of π_X on $\omega_l(X)$ is semisimple (i.e., not a multiple root of the minimum polynomial of π_X).

REMARK 1.1. (a) When $X = h^{2j}(V)(j)$, these become the statements in Tate 1994.

(b) If X is of weight $m \neq 0$, then these statements are trivially true because $\gamma(X_l) = 0 = \gamma(X_l^\vee)$ and 1 is not an eigenvalue of π_X on $\omega_l(X)$.

(c) Let X have weight $2m$. Once we have chosen an isomorphism $Q \to Q(1)$, we can identify (2) with a map

$$Q \otimes_{\mathbb{Q}} A_l(X(m)) \to \omega_l(X(m)) \simeq \omega_l(X).$$

Then $T(X(m),l)$ becomes the statement that $Q \cdot A_l(X) = \omega_l(X)^{\pi_X/q^m}$.

THEOREM 1.2. *Let X be a motive of weight $2m$ over $\mathbb{F}_q$, and let l be a prime number (possibly p). The following statements are equivalent:*

(a) $\dim_{\mathbb{Q}} A_l(X(m))/N = \dim_Q \omega_l(X)^{\pi/q^m}$;
(b) $T(X(m),l) + D(X(m),l)$;
(c) $T(X(m),l) + T(X^\vee(-m),l) + S(X(m),l)$;
(d) $T(X(m),l) + T(X^\vee(-m),l) + D(X(m),l) + D(X^\vee(-m),l) + I(X(m),l) + I(X^\vee(-m),l) + S(X(m),l) + S(X^\vee(-m),l)$;
(e) *the order of the pole of the zeta function $Z(X,t)$ at $t = q^{-m}$ is equal to the dimension of the $\mathbb{Q}$-vector space $\gamma(X(m)_{\mathrm{num}})$.*

PROOF. The hard Lefschetz theorem for l-adic cohomology shows that $\omega_l(X)$ and $\omega_l(X^\vee)$ are isomorphic together with their Frobenius operators, and so

$$\omega_l(X)^{\pi_X/q^m} \approx \omega_l(X^\vee)^{\pi_{X^\vee}/q^m}.$$

In particular, they have the same dimension. We can now apply the arguments in Tate 1994, §2, to the diagram

$$\begin{tikzcd}
Q \otimes A_l(X(m)) \arrow[r, "b"] \arrow[d, "a"] & \omega_l(X(m))^{\pi/q^m} \arrow[r, "c"] & (\omega_l(X(-m)^\vee)^{\pi/q^m})^* \arrow[d, "d"] \\
Q \otimes (A_l(X(m))/N) \arrow[r, hook, "f"] & Q \otimes \mathrm{Hom}_{\mathbb{Q}}(A_l(X(-m)^\vee), \mathbb{Q}) & (Q \otimes A_l(X(-m)^\vee))^*. \arrow[l, hook', "e"']
\end{tikzcd}$$

Here $(-)^* = \mathrm{Hom}_Q(-,Q)$, b is the map (2), and d is the linear dual of the similar map for $X^\vee$. The maps e and f are defined by the pairings in (3), and the maps a and e are obvious. $\square$

Statement (e) of the theorem is independent of l, and so

$$T(X(m),l) + D(X(m),l) \text{ for one } l \iff T(X(m),l) + D(X(m),l) \text{ for all } l.$$

We call $T(X(m),l)$ the *Tate conjecture* (for $X(m),l$), and equivalent statements of the theorem the *full Tate conjecture* (for $X(m)$).

REMARK 1.3. All four conjectures are stable under passage to direct sums, direct summands, and duals (but not tensor products or Tate twists).

For example, we show that $T(X,l)$ implies $T(X^\vee,l)$. Because T is stable under passage to direct sums and direct summands, it suffices to do this for $X = h^{2i}(V)(i)$. From the hard Lefschetz theorem for the l-adic Weil cohomology, we get a diagram

$$\begin{tikzcd} Q\otimes A_l(X) \arrow[r] \arrow[d, "\text{onto}"] & Q\otimes A_l(X^\vee) \arrow[d] \\ H_l^{2i}(V)(i)^\pi \arrow[r, "\simeq"] & H_l^{2d-2i}(V)(d-i)^\pi, \end{tikzcd}$$

from which the statement follows.

Let X be a motive; if one of the conjectures holds for all motives $X^{\otimes r}(m)$, $r\in\mathbb{N}$, $m\in\mathbb{Z}$, of weight 0, then it holds for all objects of $\langle X\rangle^{\otimes}$.

Characteristic polynomials

Let $(\mathsf{C},\otimes)$ be a pseudo-abelian rigid tensor category with $\mathrm{End}(\mathbb{1})=\mathbb{Q}$. Every object X of C admits a dual $(X^\vee,\mathrm{ev})$, and we have maps

$$\underline{\mathrm{Hom}}(X,X)\simeq X^\vee\otimes X\xrightarrow{\mathrm{ev}}\mathbb{1}.$$

On applying the functor $\mathrm{Hom}(\mathbb{1},\ )$ to the composite of these maps, we obtain the trace map

$$\alpha\mapsto\mathrm{Tr}(\alpha|X)\colon\mathrm{End}(X)\to\mathrm{End}(\mathbb{1})=\mathbb{Q}.$$

The rank of X is defined to be $\mathrm{Tr}(\mathrm{id}_X|X)$. These constructions commute with tensor functors. If $(\mathsf{C},\otimes)$ is tannakian, then, for every fibre functor $\omega\colon\mathsf{C}\to\mathsf{Vec}_Q$ (Q a field containing $\mathbb{Q}$), we have

$$\begin{aligned}\mathrm{Tr}(\alpha|X)&=\mathrm{Tr}(\omega(\alpha)\mid\omega(X))\\ \mathrm{rank}(X)&=\dim_Q(\omega(X))\in\mathbb{N}.\end{aligned}$$

From now on, we assume that $(\mathsf{C},\otimes)$ admits a tensor functor to a tannakian category with $\mathrm{End}(\mathbb{1})=\mathbb{Q}$. For an object X and integer $r\geq 0$, there is a morphism

$$a(r)=\sum_{\sigma\in S_r}\mathrm{sgn}(\sigma)\cdot\sigma\colon X^{\otimes r}\to X^{\otimes r},\quad S_r=\text{symmetric group}.$$

Then $a(r)/r!$ is an idempotent in $\mathrm{End}(X^{\otimes r})$, and we define $\bigwedge^r X$ to be its image. The characteristic polynomial of an endomorphism α of X is

$$P_\alpha(X,t)=c_0+c_1t+\cdots+c_{r-1}t^{r-1}+t^r,\quad r=\mathrm{rank}(X),$$

where

$$c_{r-i}=(-1)^i\,\mathrm{Tr}(\alpha\mid\textstyle\bigwedge^i X)=(-1)^i\,\mathrm{Tr}(\frac{a(i)}{i!}\circ\alpha^{\otimes i}\mid X^{\otimes i}).\qquad None$$

This definition commutes with tensor functors.

2 Weil numbers and tori

Invariants of torus actions

Let Q be a field of characteristic zero with algebraic closure Q^{al}, and let S be a group of multiplicative type over Q acting on a Q-vector space V. For a character χ of S, let V_χ denote the subspace of $V_{Q^{\mathrm{al}}}$ on which S acts through χ. Then

$$V_{Q^{\mathrm{al}}} = \bigoplus_{\chi \in X^*(S)} V_\chi, \quad X^*(S) \stackrel{\text{def}}{=} \mathrm{Hom}_{Q^{\mathrm{al}}}(S, \mathbb{G}_m),$$

and the χ for which $V_\chi \neq 0$ are called the weights of S in V.

LEMMA 2.1. *If the weights of S in V can be numbered $\xi_1, \ldots, \xi_{2m}, \ldots, \xi_{2m+r}$ in such a way that the $\mathbb{Z}$-module of relations among the ξ_i is generated by the relations*

$$\begin{aligned} \xi_i + \xi_{m+i} &= 0, \quad i = 1, \ldots, m, \\ 2\xi_{2m+i} &= 0, \quad i = 1, \ldots, r, \end{aligned}$$

then $\left(\bigotimes V\right)^S$ is generated as a Q-algebra by $(V^{\otimes 2})^S$.

PROOF. Clearly $Q[(V^{\otimes 2})^S] \subset \left(\bigotimes V\right)^S$. It suffices to prove that the two become equal after tensoring with Q^{al} (because forming invariants commutes with passing to a field exension). Therefore, we may suppose that Q is algebraically closed. Fix an integer $n \geq 1$. For a $2m+r$-tuple $\Sigma = (n_1, \ldots, n_{2m}, \ldots, n_{2m+r})$ of nonnegative integers with sum n, let $[\Sigma]$ denote the character $\sum_{i=1}^{2m+r} n_i \xi_i$ of S, and let $V(\Sigma) = \bigotimes_{i=1}^{2m+r} V_{\xi_i}^{\otimes n_i}$. Then $V^{\otimes n} = \bigoplus_\Sigma V(\Sigma)$, and S acts on $V(\Sigma)$ through the character $[\Sigma]$. Therefore, $(V^{\otimes n})^S = \bigoplus_{[\Sigma]=0} V(\Sigma)$. By assumption, a character $[\Sigma]$ is zero if and only if

$$\begin{aligned} n_i &= n_{m+i}, \quad i = 1, \ldots, m, \\ n_i &\text{ is even} \quad i = 1, \ldots, r. \end{aligned}$$

and so

$$[\Sigma] = 0 \implies V(\Sigma) = \bigotimes_{i=1}^{m} (V_{\xi_i} \otimes V_{\xi_{m+i}})^{\otimes n_i} \otimes \bigotimes_{i=1}^{r} (V_{2m+i}^{\otimes 2})^{\otimes n_i/2}.$$

But $V_{\xi_i} \otimes V_{\xi_{m+i}} \subset (V^{\otimes 2})^S$ because $\xi_i + \xi_{m+i} = 0$ in $X^*(T)$, and $V_{2m+i}^{\otimes 2} \subset (V^{\otimes 2})^S$ because $2\xi_{2m+i} = 0$. It follows that $\left(\bigotimes^n V\right)^S \subset Q\,[(V^{\otimes 2})^S]$. □

An involution $a \mapsto a'$ of a $\mathbb{Q}$-algebra F is said to be positive if $\mathrm{Tr}_{F/\mathbb{Q}}(a\,a') > 0$ for all nonzero a in F. A commutative finite $\mathbb{Q}$-algebra F admits a positive involution if and only if it is a product of totally real fields and CM fields, in which case, the involution acts as the identity map on each real factor and as complex conjugation on each CM factor; in particular, it is unique.

PROPOSITION 2.2. *Let $(F, ')$ be a finite commutative $\mathbb{Q}$-algebra with positive involution, and let S denote the algebraic group (of multiplicative type) such that*

$$S(R) = \{a \in (F \otimes R)^\times \mid a \cdot a' = 1\}, \quad R \text{ a } \mathbb{Q}\text{-algebra.}$$

Let Q be a field containing $\mathbb{Q}$, and let V be a free $F \otimes_{\mathbb{Q}} Q$-module of finite rank. Then $\left(\bigotimes V\right)^S$ is generated as a Q-algebra by $(V^{\otimes 2})^S$:

$$\left(\bigotimes V\right)^S = Q[(V^{\otimes 2})^S].$$

PROOF. If F is a CM field, then S is a torus. Every embedding $\sigma: F \hookrightarrow Q^{\mathrm{al}}$ defines a character ξ_σ of S, and the character group of S is the quotient of $\bigoplus \mathbb{Z}\xi_\sigma$ by the subgroup generated by the elements $\xi_\sigma + \xi_{\iota\circ\sigma}$ (recall that ι denotes complex conjugation). As V is a free $F \otimes Q$-module, the weights of S on $V \otimes_Q Q^{\mathrm{al}}$ are precisely the characters ξ_σ, $\sigma \in \mathrm{Hom}(F, Q^{\mathrm{al}})$, and each has the same multiplicity. Choose a CM type $\{\varphi_1, \ldots, \varphi_m\}$ for F. Then the character group of S has generators $\{\xi_{\varphi_1}, \ldots, \xi_{\varphi_m}, \xi_{\iota\circ\varphi_1}, \ldots, \xi_{\iota\circ\varphi_m}\}$ and defining relations

$$\xi_{\varphi_i} + \xi_{\iota\circ\varphi_i} = 0, \quad i = 1, \ldots, m.$$

Thus the statement follows from the lemma.

If F is a totally real field, then $S = \mu_2$, and the element -1 of $\mu_2(\mathbb{Q})$ acts on V as multiplication by -1. Therefore $V_{\mathbb{Q}^{\mathrm{al}}} = V_\xi$ where ξ is the nonzero element of $X^*(S)$. Therefore $X^*(S)$ has generator ξ and defining relation $2\xi = 0$. Thus the statement follows from the lemma.

In the general case, F is a product of CM fields and totally real fields, and the same arguments as in the last two paragraphs apply. □

REMARK 2.3. Let $(F,')$ be as in 2.2. It follows from the definition of S, that the involution $a \mapsto a'$ acts on the algebraic group S by sending each element to its inverse. Therefore, it acts on $X^*(S)$ as -1.

Application to the tori attached to Weil numbers

By an algebraic number, we mean an element of a field algebraic over $\mathbb{Q}$. We let $\mathbb{Q}^{\mathrm{al}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

DEFINITION 2.4. An algebraic number π is said to be a Weil q-number of weight m if

(a) for every embedding $\rho: \mathbb{Q}[\pi] \hookrightarrow \mathbb{Q}^{\mathrm{al}}$, $|\rho(\pi)| = q^{m/2}$;

(b) for some n, $q^n\pi$ is an algebraic integer.

Let π be Weil q-number of weight m. Condition (a) implies that $\pi \mapsto \pi' = q^m/\pi$ defines an involution $\alpha \mapsto \alpha'$ of $\mathbb{Q}[\pi]$ such that $\rho(\alpha') = \iota(\rho(\alpha))$ for all embeddings $\rho: \mathbb{Q}[\pi] \hookrightarrow \mathbb{Q}^{\mathrm{al}}$. Therefore $\mathbb{Q}[\pi]$ is a CM-field or a totally real field (according as $\pi' \neq \pi$ or $\pi' = \pi$).

2.5. Let $\mathbb{Q}[\pi]$ be a finite $\mathbb{Q}$-algebra that can be written as a product of fields

$$\mathbb{Q}[\pi] = \prod\nolimits_i \mathbb{Q}[\pi_i], \quad \pi \leftrightarrow (\pi_1, \ldots, \pi_r),$$

with each π_i a Weil q-number of weight m. Let $'$ be the (unique) positive involution of $\mathbb{Q}[\pi]$ and S the algebraic group attached to $(\mathbb{Q}[\pi], ')$ as in 2.2. Note that $\pi/q^{m/2} \in S(\mathbb{Q}^{\mathrm{al}})$. We say that $\pi/q^{m/2}$ ***generates*** S if there does not exist a proper algebraic subgroup H of S such that $\pi/q^{m/2} \in H(\mathbb{Q}^{\mathrm{al}})$. Note that, if S_i is the group attached to $\mathbb{Q}[\pi_i]$, then $S = \prod S_i$, and $\pi/q^{m/2}$ generates S if and only if $\pi_i/q^{m/2}$ generated S_i for all i.

PROPOSITION 2.6. *Let Q be a field containing $\mathbb{Q}$, and let V be a free $\mathbb{Q}[\pi] \otimes_{\mathbb{Q}} Q$-module of finite rank. If $\pi/q^{m/2}$ generates S, then*

$$(\bigotimes V)^{\pi/q^{m/2}} = Q[(V^{\otimes 2})^S].$$

PROOF. According to Proposition 2.2, $(\bigotimes V)^S = Q[(V^{\otimes 2})^S]$, and so it remains to show that $(\bigotimes V)^{\pi/q^{m/2}} = (\bigotimes V)^S$. As $\pi/q^{m/2} \in S(\mathbb{Q}^{\mathrm{al}})$, certainly $(\bigotimes V)^{\pi/q^{m/2}} \supset (\bigotimes V)^S$. Conversely, let $v \in (\bigotimes V)^{\pi/q^{m/2}}$, and let H be the algebraic subgroup of GL_V of elements fixing v. Then $\pi/q^{m/2} \in H(\mathbb{Q}^{\mathrm{al}})$, and so $S \subset H$ because $\pi/q^{m/2}$ generates S. We conclude that S fixes v. □

ASIDE 2.7. Let $\mathbb{Q}[\pi]$ and S be as in 2.5, and assume that π has no real conjugates. Let $\pi_1, \iota\pi_1, \ldots, \pi_g, \iota\pi_g$ be the conjugates of π in $\mathbb{Q}^{\mathrm{al}}$. The following conditions are equivalent:

(a) S is generated by $\pi/q^{m/2}$;

(b) if
$$\pi_1^{n_1} \cdots \pi_g^{n_g} = q^n, \quad n_i, n \in \mathbb{Z},$$
then $n_1 = \cdots = n_g = 0 = n$;

(c) if
$$\pi_1^{n_1} \cdot \iota\pi_1^{n_1'} \cdot \cdots \cdot \pi_g^{n_g} \cdot \iota\pi_g^{n_g'} = q^n, \quad n_i, n_i', n \in \mathbb{Z},$$
then $n_i = n_i'$ for all i and $m(n_1 + \cdots + n_g) = n$.

Weil numbers π such that $\pi/q^{m/2}$ generates S.

Let $\mathbb{Q}[\pi] = \prod \mathbb{Q}[\pi_i]$ and S be as in 2.5. We give some examples where $\pi/q^{m/2}$ generates S (following Kowalski 2006, Lenstra and Zarhin 1993, and Zarhin 1991).

We (ambiguously) write ι for the unique positive involution of $\mathbb{Q}[\pi]$ (so $\rho \circ \iota = \iota \circ \rho$ for all $\rho \colon \mathbb{Q}[\pi] \to \mathbb{Q}^{\mathrm{al}}$). By a p-adic prime of $\mathbb{Q}[\pi]$ we mean a prime ideal of the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\pi]$ lying over p. Thus $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}[\pi] \simeq \prod \mathbb{Q}[\pi]_v$ where v runs over the p-adic primes of $\mathbb{Q}[\pi]$ and each field $\mathbb{Q}[\pi]_v$ is the completion of some $\mathbb{Q}[\pi_i]$ at a p-adic prime of it. The degree of v is $[\mathbb{Q}[\pi]_v \colon \mathbb{Q}_p]$.

EXAMPLE 2.8. Assume that there exists a p-adic prime v_1 of $\mathbb{Q}[\pi]$ of degree 1 and such that
$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q^m)} = \begin{cases} 0 & \text{if } v = v_1 \\ 1/2 & \text{if } v \neq v_1, \iota v_1 \\ 1 & \text{if } v = \iota v_1. \end{cases}$$
For a homomorphism $\rho \colon \mathbb{Q}[\pi] \to \mathbb{Q}^{\mathrm{al}}$ and a p-adic prime w of $\mathbb{Q}^{\mathrm{al}}$, we have
$$\frac{\mathrm{ord}_w(\rho(\pi/q^{m/2}))}{\mathrm{ord}_w(q^m)} = \begin{cases} -1/2 & \text{if } \rho^{-1}(w) = v_1 \\ 0 & \text{if } \rho^{-1}(w) \neq v_1, \iota v_1 \\ 1/2 & \text{if } \rho^{-1}(w) = \iota v_1. \end{cases}$$
Let $\chi = \sum n(\rho)\rho$ be a character of $(\mathbb{G}_m)_{\mathbb{Q}[\pi]/\mathbb{Q}}$. For a p-adic prime w of $\mathbb{Q}^{\mathrm{al}}$,
$$\mathrm{ord}_w(\chi(\pi/q^{m/2})) = \frac{\mathrm{ord}_{v_1}(q^m)}{2}(-n(\rho) + n(\iota \circ \rho)),$$
where ρ is the unique embedding of $\mathbb{Q}[\pi]$ into $\mathbb{Q}^{\mathrm{al}}$ such that $\rho^{-1}(w) = v_1$ (the uniqueness uses that v_1 has degree 1). Therefore, $\chi(\pi/q^{m/2}) = 1$ if and only if $\chi = \iota \circ \chi$, i.e., if and only if χ is trivial on S. This shows that $\pi/q^{m/2}$ generates S.

EXAMPLE 2.9. Assume that there exists a p-adic prime v_1 of $\mathbb{Q}[\pi]$ with decomposition group $\{1,\iota\}$ and such that

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q^m)} = \begin{cases} 1/2 & \text{if } v = v_1 \\ 0 \text{ or } 1 & \text{otherwise.} \end{cases}$$

Then $\pi/q^{m/2}$ generates S (see, for example, Milne 2001, A.9).

Let π be a Weil q-number of weight $m > 0$ with no real conjugates. We say that π is ***ordinary*** if its characteristic polynomial

$$X^{2g} + a_1 X^{2g-1} + \cdots + a_g X^g + \cdots + q^{gm}$$

has middle coefficient a_g a p-adic unit. From the theory of Newton polygons, this means that, for each p-adic prime v of $\mathbb{Q}[\pi]$, either $\mathrm{ord}_v(\pi) = 0$ (hence $\mathrm{ord}_v(\iota\pi) = m\,\mathrm{ord}_v(q)$) or $\mathrm{ord}_v(\iota\pi) = 0$. An ordinary Weil q-number is an algebraic integer.

EXAMPLE 2.10. Let π be an ordinary Weil q-number of weight $m > 0$ and degree $2g$, and let L be the splitting field in $\mathbb{Q}^{\mathrm{al}}$ of the characteristic polynomial of π. Assume that, for each complex conjugate pair π', $\iota\pi'$ of conjugates of π in L, there exists an element of $\mathrm{Gal}(L/\mathbb{Q})$ fixing π' and $\iota\pi'$ and acting as ι on the remaining conjugates of π in L. This condition holds, for example, if $\mathrm{Gal}(L/\mathbb{Q})$ is the full group of permutations of the set of conjugates of π preserving the subsets $\{\pi',\iota\pi'\}$.

We claim that $\pi/q^{m/2}$ generates S. To prove this, we fix a p-adic prime v of L and we normalize ord_v so that $\mathrm{ord}_v(q) = 1$. We number the conjugates of π in L so that $\mathrm{ord}_v(\pi_i) = m$ and $\mathrm{ord}_v(\iota\pi_i) = 0$ for $i = 1,\ldots,g$. We may suppose that $g > 1$ as the case $g = 1$ is trivial.

Suppose that there is a relation

$$\pi_1^{n_1}\cdots\pi_g^{n_g} = q^n, \quad n_i, n \in \mathbb{Z}, \tag{4}$$

in L. Let $\alpha = \pi_1^{n_1}\cdots\pi_g^{n_g}$. Then $\alpha\bar{\alpha} = q^{2n}$, and so

$$m(n_1 + \cdots + n_g) = 2n.$$

Let σ_i be the element of $\mathrm{Gal}(L/\mathbb{Q})$ fixing π_i and $\iota\pi_i$ and interchanging π_j and $\iota\pi_j$ for $j \neq i$. On applying σ_i to (4) and then ord_v, we find that

$$mn_i = n.$$

As this is true for all i, we deduce that $n_1 = \cdots = n_g = 0$, i.e., (4) is the trivial relation. It follows from this that if

$$\pi_1^{n_1}\cdot\iota\pi_1^{n_1'}\cdot\cdots\cdot\pi_g^{n_g}\cdot\iota\pi_g^{n_g'} = q^n,$$

then

$$n_i = n_i', \text{ for all } i.$$

Let ρ_i be the homomorphism $\mathbb{Q}[\pi] \to L$ sending π to π_i, and let $\chi = \sum_{i=1}^{g}(n_i\rho_i + n_i'(\iota\circ\rho_i))$ be a cocharacter of $(\mathbb{G}_m)_{\mathbb{Q}[\pi]/\mathbb{Q}}$. Then

$$\chi(\pi/q^{m/2}) = \pi_1^{n_1}\cdot\iota\pi_1^{n_1'}\cdot\cdots\cdot\pi_g^{n_g}\cdot\iota\pi_g^{n_g'}\cdot q^{-n}$$

with $n = (n_1 + n_1' + \cdots + n_g + n_g')m/2$. Therefore,

$$\chi(\pi/q^{m/2}) = 1 \iff n_i = n_i' \text{ for all } i \iff \chi = \iota\circ\chi \iff \chi \text{ is trivial on } S.$$

This shows that $\pi/q^{m/2}$ generates S.

3 Proof of Theorem 0.1

We begin with an easy lemma.

LEMMA 3.1. *Let a and b be eigenvalues of endomorphisms α and β of vector spaces V and W. If the eigenvalue ab of $\alpha \otimes \beta$ on $V \otimes W$ is semisimple and $b \neq 0$, then a is semisimple.*

EXAMPLE 3.2. Let α be an endomorphism of a k-vector space V. Let q be an element of k, and suppose that the eigenvalues of α on V occur in pairs (a, a') with $aa' = q$. If the eigenvalue q of $\alpha \otimes \alpha$ on $V \otimes V$ is semisimple, then α acts semisimply on V.

We fix a standard Weil cohomology H on the varieties over $\mathbb{F}_q$, and we let $\mathsf{Mot}_H(\mathbb{F}_q)$ denote the corresponding category of motives. It is a pseudo-abelian rigid tensor category such that $\mathrm{End}(\mathbb{1}) = \mathbb{Q}$ (Saavedra 1972, 4.1.3.5). By a motive, we shall mean an object of $\mathsf{Mot}_H(\mathbb{F}_q)$. We let Q denote the field of coefficients of H and ω the tensor functor $\mathsf{Mot}_H(\mathbb{F}_q) \to \mathsf{Vec}_Q$ defined by H.

The category $\mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$ of numerical motives is a semisimple tannakian category, and there is a (quotient) tensor functor $q\colon \mathsf{Mot}_H(\mathbb{F}_q) \to \mathsf{Mot}_{\mathrm{num}}(\mathbb{F}_q)$. For a motive X, the kernel of $\mathrm{End}(X) \to \mathrm{End}(qX)$ is a nilpotent ideal N equal to the Jacobson radical of $\mathrm{End}(X)$ (Jannsen 1992, Thm 1, Cor. 1). In particular, $\mathrm{End}(X)/N$ is separable over $\mathbb{Q}$, and so the $\mathbb{Q}$-bilinear pairing

$$\mathrm{End}(X) \times \mathrm{End}(X) \to \mathbb{Q}, \quad \alpha, \beta \mapsto \mathrm{Tr}(\alpha \circ \beta) \tag{5}$$

has left and right kernels equal to N.

LEMMA 3.3. *Let $M \subset \mathrm{End}(X)$ be a $\mathbb{Q}$-subspace such that $M \cap N = 0$. Then the map $Q \otimes M \to \mathrm{End}(\omega(X))$ is injective, and its image is a direct summand of $\mathrm{End}(\omega(X))$ (as a Q-vector space with a Frobenius operator).*

PROOF. As $M \cap N = 0$, there exists a $\mathbb{Q}$-subspace E of $\mathrm{End}(X)$ such that M and E are dual under the pairing (5). The orthogonal space to $Q \cdot E$ is a complementary submodule to $Q \cdot M$ in $\mathrm{End}(\omega_H(X))$. □

Let X be a motive. The characteristic polynomial $P_\alpha(X, t) = \det(1 - \alpha t | X)$ of an endomorphism α of X is monic with coefficients in $\mathbb{Q}$, and its degree is equal to $\mathrm{rank}\, X$. Moreover, $P_\alpha(X, t)$ is equal to the characteristic polynomial $\det(1 - \omega(\alpha)t \mid \omega(X))$ of $\omega(\alpha)$ acting on the Q-vector space $\omega(X)$. See §1.

LEMMA 3.4. *Let X be a motive and F a subfield of $\mathrm{End}(X)$. The $F \otimes Q$-module $\omega(X)$ is free of rank $\frac{\mathrm{rank}(X)}{[F:\mathbb{Q}]}$.*

PROOF. If $F \otimes Q$ is again a field, then $\omega(X)$ is certainly free. Otherwise it will decompose into a product of fields $F \otimes Q = \prod_i F_i$, and correspondingly $\omega(X) \simeq \bigoplus_i W_i$ with W_i an F_i-vector space of dimension $m_i \geq 0$. Our task is to show that the m_i are all equal (in fact, to $\mathrm{rank}(X)/[F:\mathbb{Q}]$).

Let α be such that $F = \mathbb{Q}[\alpha]$, and let $P_\alpha(F/\mathbb{Q}, t)$ (resp. $P_\alpha(F_i/Q, t)$) denote the characteristic polynomial of α in the field extension $F/\mathbb{Q}$ (resp. F_i/Q). From the decomposition $F \otimes Q = \prod_i F_i$, we find that

$$P_\alpha(F/\mathbb{Q}, t) = \prod_i P_\alpha(F_i/Q, t) \tag{6}$$

in $Q[t]$. The polynomial $P_\alpha(F/\mathbb{Q},t)$ is irreducible in $\mathbb{Q}[t]$, and (6) is its factorization into irreducible polynomials in $Q[t]$.

From the isomorphism of $F\otimes Q$-modules $\omega(X)\simeq\bigoplus_i W_i$, we find that

$$P_\alpha(X,t)=\prod\nolimits_i P_\alpha(F_i/Q,t)^{m_i}.$$

The two equations show that every monic irreducible factor of $P_\alpha(X,t)$ in $\mathbb{Q}[t]$ shares a root with $P_\alpha(F/\mathbb{Q},t)$, and therefore equals it. Hence $P_\alpha(X,t)=P_\alpha(F/\mathbb{Q},t)^m$ for some integer m, and each $m_i=m$. On equating the degrees, we find that $\operatorname{rank}X=m[L\colon\mathbb{Q}]$. □

3.5. According to Wedderburn's Principal Theorem (Albert 1939, III, Theorem 23), the homomorphism of $\mathbb{Q}$-algebras $\mathrm{End}(X)\to\mathrm{End}(X)/N$ admits a section, unique up to conjugation. Choose one, and let $\mathrm{End}(X)'$ be its image; thus

$$\mathrm{End}(X)=N\oplus\mathrm{End}(X)'.$$

Let π denote the image of π_X in $\mathrm{End}(X)'$ — it is independent of the choice of the section because π_X lies in the centre of $\mathrm{End}(X)$. As $\mathrm{End}(X)'$ is separable and π is contained in its centre, $\mathbb{Q}[\pi]$ is a product of fields. Moreover, as π is the image of π_X under a homomorphism of $\mathbb{Q}$-algebras, it satisfies $P_{\pi_X}(X,t)$. Thus we are in the situation of 2.5 with m equal to the weight of X. Let S be the algebraic group defined by $\mathbb{Q}[\pi]$, as in 2.2. According to Lemma 3.3, the map $Q\otimes\mathbb{Q}[\pi]\to\mathrm{End}(\omega(X))$ is injective.

LEMMA 3.6. *Let X be a motive of weight m in $\mathsf{Mot}_{\mathrm{hom}(l)}(\mathbb{F}_q)$. The following conditions are equivalent:*

(a) $Q\cdot A_l(X^{\otimes 2}(m))=\omega(X^{\otimes 2})^{\pi/q^{m/2}}$;

(b) $T(X^{\otimes 2}(m),l)+S(X^{\otimes 2}(m),l)$;

(c) $T(X^{\otimes 2}(m),l)$ *and* π_X *acts semisimply on* $\omega(X)$.

Each statement implies

(d) $Q\cdot A_l(X^{\otimes 2}(m))\supset\omega(X^{\otimes 2})^S$,

and is equivalent to it if $\pi/q^{m/2}$ *generates* S.

PROOF. (a) $\iff$ (b). We have

$$Q\cdot A_l(X^{\otimes 2}(m))\subset\omega(X^{\otimes 2})^{\pi_X/q^{m/2}}\subset\omega(X^{\otimes 2})^{\pi/q^{m/2}}.$$

The first inclusion is an equality if and only if $T(X^{\otimes 2}(m),l)$ holds, and the second inclusion is an equality if and only if 1 is a semisimple eigenvalue of $\pi_X/q^{m/2}$ on $\omega(X)$.

(b) $\iff$ (c). From 3.2 we see that π_X acts semisimply on $\omega(X)$ if and only if q^m is a semisimple eigenvalue of $\pi_X\otimes\pi_X$ on $\omega(X^{\otimes 2})$..
For the final statement, note that $\omega(X^{\otimes 2})^{\pi/q^{m/2}}\supset\omega(X^{\otimes 2})^S$ because $\pi/q^{m/2}\in S(\mathbb{Q}^{\mathrm{al}})$, and equals it if $\pi/q^{m/2}$ generates S. □

THEOREM 3.7. *Let X be a motive of weight m in $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$, and let π and S be as in 3.5.*

(a) *The Q-algebra $(\bigotimes\omega(X))^S$ is generated by $\omega(X^{\otimes 2})^S$:*

$$\left(\bigotimes\omega(X)\right)^S=Q[\omega(X^{\otimes 2})^S].$$

(b) *If $\omega(X^{\otimes 2})^S$ consists of algebraic classes and S is generated by $\pi_X/q^{m/2}$, then the Tate conjecture holds for $X^{\otimes n}(\frac{mn}{2})$ for all $n \in \mathbb{N}$ with mn even.*

PROOF. (a) Lemma 3.4 allows us to apply Proposition 2.6 to the $\mathbb{Q}$-algebra $\mathbb{Q}[\pi]$ acting on the Q-vector space $V = \omega(X)$.

(b) From the hypotheses, we find that

$$\left(\bigotimes \omega(X)\right)^{\pi/q^{m/2}} = \left(\bigotimes \omega(X)\right)^S \subset Q[A_l(X^{\otimes 2}(m))] \subset \bigoplus\nolimits_n Q \cdot A_l(X^{\otimes n}(m))$$

which implies that, for all n with mn even,

$$\omega(X^{\otimes n})^{\pi/q^{m/2}} \subset Q \cdot A_l(X^{\otimes n}(\tfrac{mn}{2})).$$

□

We now prove Theorem 0.1. When π_X actx semisimply on $\omega(X)$, statement (a) of Theorem 3.7 becomes statement (a) of Theorem 0.1. On the other hand, Lemma 3.6 shows that statement (b) of Theorem 3.7 implies statement (b) of Theorem 0.1.

4 Proof Theorem 0.2

LEMMA 4.1. *Let S be a diagonalizable group acting on a Q-vector space V, and let G be the group of Q-linear automorphisms of V commuting with the action of S. For every character χ of S, the action of G on V_χ is irreducible.*

PROOF. Because S is diagonalizable,

$$V = \bigoplus_{\chi \in X^*(S)} V_\chi, \quad G = \prod_{\chi \in X^*(S)} \mathrm{GL}(V_\chi),$$

from which the statement is obvious. □

Let H be a standard Weil cohomology theory, and let Q be its field of coefficients. By a motive, we shall mean an object of $\mathsf{Mot}_H(\mathbb{F}_q)$. For a motive Y of weight $2m$ and a field Q' containing Q, we say that an element of $Q' \otimes_Q \omega(Y)$ is algebraic if it is in the image of the map

$$Q' \otimes_{\mathbb{Q}} \gamma(Y(m)) \to Q' \otimes_Q \omega(Y)$$

(cf. 1.1(c)).

Let X be a motive of weight m, and let π and S be as in 3.5. Let ι_π denote the unique positive involution of $\mathbb{Q}[\pi]$. Then ι_π acts on $X^*(S)$ as -1 (see 2.3).

LEMMA 4.2. *Assume that the elements of $\omega(X^{\otimes 2})^S$ are algebraic, and let $n \in \mathbb{N}$. If a Q-linear map $\alpha\colon \omega(X^{\otimes n}) \to \omega(X^{\otimes n})$ commutes with the action of S, then it maps algebraic classes to algebraic classes.*

PROOF. As $(\bigotimes \omega(X))^S$ is generated as a Q-algebra by $\omega(X^{\otimes 2})^S$ (see 2.6), it consists of algebraic classes. It follows that the graph of the map α is algebraic, and so it maps algebraic classes to algebraic classes. □

Let $Y = X^{\vee}$, and let $\bar{Q}$ be a finite Galois extension of Q splitting $\mathbb{Q}[\pi]$ (i.e., such that $Q' \otimes_{\mathbb{Q}} \mathbb{Q}[\pi]$ is a product of copies of Q'). From the pairing $\mathrm{ev}\colon Y \otimes X \to \mathbb{1}$, we get a pairing

$$Y^{\otimes n} \times X^{\otimes n} \to \mathbb{1},$$

which in turn gives us a nondegenerate pairing

$$\omega(Y^{\otimes n}) \times \omega(X^{\otimes n}) \to Q. \tag{7}$$

This is S-equivariant, and so its restriction to

$$\omega(Y^{\otimes n})_{\chi_1} \times \omega(X^{\otimes n})_{\chi_2} \to \bar{Q}$$

is nondegenerate if $\chi_1 + \chi_2 = 0$ and zero otherwise.

THEOREM 4.3. *Let $\bar{Q}$ be a finite Galois extension of Q splitting $\mathbb{Q}[\pi]$. Assume*

(a) *there exists an involution ι_Q of $\bar{Q}/Q$ such that $\rho \circ \iota_\pi = \iota_Q \circ \rho$ for all homomorphisms $\rho\colon \mathbb{Q}[\pi] \to \bar{Q}$, and*
(b) *$\omega(X^{\otimes 2})^S$ consists of algebraic classes.*

Then, for all n with mn even, the pairing

$$\gamma(Y^{\otimes n}(-\tfrac{mn}{2}) \times \gamma(X^{\otimes n}(\tfrac{mn}{2})) \to \mathbb{Q} \tag{8}$$

induced by $Y^{\otimes n} \times X^{\otimes n} \to \mathbb{1}$ is nondegenerate.

PROOF. Fix an n, and let $V = \bar{Q} \otimes_Q \omega(X^{\otimes n})$ and $W = \bar{Q} \otimes \omega(Y^{\otimes n})$. Let G be the group of $\bar{Q}$-linear automorphisms of V commuting with the action of S. According to Lemma 4.2, the action of G on $\omega(X^{\otimes n})$ preserves the algebraic classes. Let χ be a character of S over $\bar{Q}$. As V_χ is a simple G-module (4.1), either $V_\chi \cap \bar{Q} \cdot A_H(X^{\otimes n}(\frac{mn}{2}))$ is the whole of V_χ or it is zero. If $V\chi$ consists of algebraic classes, so also does $\iota_Q V_\chi$ because $\bar{Q} \cdot A_H(X^{\otimes n}(\frac{mn}{2}))$ is stable under the action of $\mathrm{Gal}(\bar{Q}/Q)$. Now

$$\iota_Q V_\chi = V_{\iota_Q \circ \chi} = V_{\chi \circ \iota_\pi} \overset{(2.3)}{=} V_{-\chi}.$$

The hard Lefschetz theorem shows that if $V_{-\chi}$ consists of algebraic classes, then so also does $W_{-\chi}$. It follows that the pairing

$$\bar{Q} \cdot A_H(Y^{\otimes n}(-\tfrac{mn}{2})) \times \bar{Q} \cdot A_H(X^{\otimes n}(\tfrac{mn}{2})) \to \bar{Q}$$

induced by the pairing $W \times V \to \bar{Q}$ is nondegenerate, and this implies that the pairing

$$A_H(Y^{\otimes n}(-\tfrac{mn}{2})) \times A_H(X^{\otimes n}(\tfrac{mn}{2})) \to \mathbb{Q}$$

is nondegenerate. This is isomorphic to the required pairing (8). □

COROLLARY 4.4. *Under the hypotheses of the theorem, the functor*

$$\langle X \rangle^{\otimes} \to \langle X_{\mathrm{num}} \rangle^{\otimes}$$

is an equivalence of categories.

PROOF. Immediate consequence of the theorem. □

COROLLARY 4.5. *Under the hypotheses of the theorem, the maps*

$$Q \otimes A_H(X^{\otimes n}(\tfrac{mn}{2})) \to \omega(X^{\otimes n})$$

are injective.

PROOF. Let $e_1, e_2, \ldots$ be $\mathbb{Q}$-linearly independent elements of $A_H(X(\frac{m}{2})^{\otimes n})$. According to the theorem, there exist elements $f_1, f_2, \ldots$ of $A_H(Y^{\otimes n}(mn/2))$ such that $\langle e_i, f_j\rangle = \delta_{ij}$. Suppose that $\sum a_i \otimes e_i$, $a_i \in Q$, maps to zero in $\omega(X^{\otimes n})$. Then $0 = \langle \sum a_i e_i, f_j\rangle = a_j$. □

REMARK 4.6. Let X be a motive over $\mathbb{F}_q$ for l-adic homological equivalence.

(a) Let F be the Galois closure of the conjugates of the centre of $\mathrm{End}(X_{\mathrm{num}})$ in $\mathbb{Q}^{\mathrm{al}}$. If complex conjugation in $\mathrm{Gal}(F/\mathbb{Q})$ lies in the decomposition group of (l), then hypothesis (a) of the theorem holds.

(b) If the Tate conjecture holds for $X^{\otimes 2}(m)$ and π_X acts semisimply on $\omega(X)$, then hypothesis (b) of the theorem holds (see Lemma 3.6).

We now prove Theorem 0.2. Let X be a motive of weight m in $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$, and assume the full Tate conjecture for $X^{\otimes 2}(m)$. According to Lemma 3.6, this implies that hypotheses (b) of Theorem 4.3 holds for X_l for all prime numbers l. Thus, it remains to show that hypothesis (a) holds for an infinite set of primes, but the Chebotarev density theorem (even the Frobenius density theorem) implies this (see 4.6a).

ASIDE 4.7. It would be interesting to see whether Deligne's proof of Clozel's theorem (Deligne 2009) can be transferred to motives. It may yield a theorem with different hypotheses.

5 Examples

By a motive in this section, we mean an object of $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$.

Motives with semisimple Frobenius

We say that a motive X has semisimple Frobenius if the action of π_X on $\omega(X)$ is semisimple. For example, the motives of curves, abelian varieties, and $K3$ surfaces have semisimple Frobenius (Weil, Deligne, Piatetski-Shapiro and Shafarevich). The property is preserved by passage to direct sums, direct summands, tensor products, and duals, and so the motives with semisimple Frobenius form a pseudo-abelian rigid tensor subcategory of $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$. For such a motive X, $\mathbb{Q}[\pi_X]$ satisfies the conditions in 2.5, and we let S denote the associated algebraic group. We say that π_X is ***regular*** if S is generated by $\pi_X/q^{m/2}$.

THEOREM 5.1. *Let X be motive of weight m over $\mathbb{F}_q$ with semisimple Frobenius.*

(a) *The $\mathbb{Q}$-algebra $(\bigotimes \omega(X))^S$ is generated by $\omega(X^{\otimes 2})^S$.*

(b) *If $X^{\otimes 2}(m)$ satisfies the Tate conjecture and π_X is regular, then the full Tate conjecture holds for all motives in $\langle X\rangle^{\otimes}$.*

(c) *If $X^{\otimes 2}(m)$ satisfies the Tate conjecture, then, for infinitely many prime numbers l, the functor $\langle X_l\rangle^{\otimes} \to \langle X_{\mathrm{num}}\rangle^{\otimes}$ is faithful.*

PROOF. These statements are special cases of Theorems 0.1 and 0.2. □

REMARK 5.2. Let V be a variety of even dimension d. After possibly extending the base field, we may suppose that

$$H_l^d(V)(\tfrac{d}{2}) = H_l^d(V)(\tfrac{d}{2})^{\pi_V} \oplus H_l^d(V)(\tfrac{d}{2})_{\mathrm{trans}},$$

where the eigenvalues of π_V on $H_l^d(V)(\frac{d}{2})_{\mathrm{trans}}$ are not roots of 1. Assume that these eigenvalues are all distinct. Then the subspace

$$\left(H_l^d(V) \otimes H_i^d(V)(d)\right)^{\pi}$$

of $H_l^{2d}(V \times V)(d)^{\pi}$ is generated by $H_l^d(V)(\frac{d}{2})^{\pi} \otimes H_i^d(V)(\frac{d}{2})^{\pi}$ and the cohomology classes of the graphs of the powers of π_V (Zarhin 1996, 4.4). Sometimes this can be used to show that the Tate conjecture holds for $V \times V$ if it holds for V.

For example, if V is a $K3$ surface, then the characteristic polynomial of π_V on $H_l^2(V)(1)_{\mathrm{trans}}$ is a power Q^r of an irreducible polynomial $Q \in \mathbb{Q}[t]$ and r divides the height of V (Yu and Yui 2008). If $r = 1$, then the Tate conjecture holds for $V \times V$ and the only "new" algebraic cycles on $V \times V$ are the graphs of the powers of π_V.

Abelian motives

A motive in $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$ is said to be abelian (or of abelian type) if it isomorphic to a motive (A, e, m) with A an abelian variety. The category of abelian motives is the smallest pseudo-abelian rigid tensor subcategory of $\mathsf{Mot}_{\mathrm{rat}}(\mathbb{F}_q)$ containing the motives of curves.

The standard conjecture of Lefschetz type holds for abelian motives, and so an abelian motive X and its dual $X^{\vee}$ are isomorphic. Thus, the full Tate conjecture holds for X if $T(X,l)$ and $S(X,l)$ hold for some l (see 1.2).

THEOREM 5.3. *Let X be an abelian motive of weight m over $\mathbb{F}_q$ such that $X^{\otimes 2}(m)$ satisfies the Tate conjecture (e.g., $X = h^1A$ for A an abelian variety).*

(a) *If π_X is regular, then the full Tate conjecture holds for all motives in $\langle X\rangle^{\otimes}$.*
(b) *For infinitely many prime numbers l, the functor $\langle X_l\rangle^{\otimes} \to \langle X_{\mathrm{num}}\rangle^{\otimes}$ is faithful.*

PROOF. These statements are special cases of Theorems 0.1 and 0.2. □

$K3$ surfaces

Recall that the Tate conjecture is known for $K3$ surfaces over finite fields (Artin and Swinnerton Dyer 1973 for elliptic $K3$ surfaces; Nygaard 1983 for $K3$ surfaces of height 1;Nygaard and Ogus 1985 for $K3$ of finite height and $p \neq 2,3$; Charles 2013 and Maulik 2014 independently for supersingular $K3$ surfaces and $p \neq 2,3$; Madapusi Pera 2015 for all $K3$ surfaces and $p \neq 2$; Madupusi Pera and Kim 2018 for all $K3$ surfaces and $p = 2$). More recently, the Tate conjecture has been proved for the square $V \times V$ of a $K3$ surface V (Ito et al. 2018).

THEOREM 5.4. *Let V be a $K3$ surface over a finite field.*

(a) *If π_V is regular, then the full Tate conjecture holds for all powers of V.*

(b) *There exists an infinite set of prime numbers l such that l-homological equivalence coincides with numerical equivalence for all powers of V.*

PROOF. These statements are special cases of Theorems 0.1 and 0.2. □

It follows from Example 2.8 that π_V is regular if V has height 1.

References

ALBERT, A. A. 1939. Structure of Algebras. American Mathematical Society Colloquium Publications, vol. 24. American Mathematical Society, New York.

CLOZEL, L. 1999. Equivalence numérique et équivalence cohomologique pour les variétés abéliennes sur les corps finis. *Ann. of Math. (2)* 150:151–163.

DELIGNE, P. 2009. Equivalence numérique, équivalence cohomologique, et théorie de Lefschetz des variétés abéliennes sur les corps finis (written by L. Clozel). *Pure Appl. Math. Q.* 5:495–506.

DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics 900. Springer-Verlag, Berlin.

ITO, K., ITO, T., AND KOSHIKAWA, T. 2018. CM liftings of K3 surfaces over finite fields and their applications to the Tate conjecture. arXiv:1809.09604.

KOWALSKI, E. 2006. Weil numbers generated by other Weil numbers and torsion fields of abelian varieties. *J. London Math. Soc. (2)* 74:273–288.

LENSTRA, JR., H. W. AND ZARHIN, Y. G. 1993. The Tate conjecture for almost ordinary abelian varieties over finite fields, pp. 179–194. *In* Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ. Oxford Univ. Press, New York.

MILNE, J. S. 1999. Lefschetz classes on abelian varieties. *Duke Math. J.* 96:639–675.

SAAVEDRA RIVANO, N. 1972. Catégories Tannakiennes. Lecture Notes in Mathematics, Vol. 265. Springer-Verlag, Berlin.

SCHOLL, A. J. 1994. Classical motives, pp. 163–187. *In* Motives (Seattle, WA, 1991), volume 55 of *Proc. Sympos. Pure Math.* Amer. Math. Soc.

TATE, J. T. 1994. Conjectures on algebraic cycles in l-adic cohomology, pp. 71–83. *In* Motives (Seattle, WA, 1991), volume 55 of *Proc. Sympos. Pure Math.* Amer. Math. Soc., Providence, RI.

YU, J.-D. AND YUI, N. 2008. $K3$ surfaces of finite height over finite fields. *J. Math. Kyoto Univ.* 48:499–519.

ZARHIN, Y. G. 1991. Abelian varieties of $K3$ type and l-adic representations, pp. 231–255. *In* Algebraic geometry and analytic geometry (Tokyo, 1990), ICM-90 Satell. Conf. Proc. Springer, Tokyo.

ZARHIN, Y. G. 1996. The Tate conjecture for powers of ordinary $K3$ surfaces over finite fields. *J. Algebraic Geom.* 5:151–172.