# Motives over $\mathbb{F}_p$

J.S. Milne

July 22, 2006

**Abstract**

In April, 2006, Kontsevich asked me whether the category of motives over $\mathbb{F}_p$ ($p$ prime), has a fibre functor over a number field of finite degree since he had a conjecture that more-or-less implied this. This article is my response. Unfortunately, since the results are generally negative or inconclusive, they are of little interest except perhaps for the question they raise on the existence of a cyclic extension of $\mathbb{Q}$ having certain properties (see Question 6.5).

Let $k$ be a finite field. Starting from any suitable class $\mathcal{S}$ of algebraic varieties over $k$ including the abelian varieties and using the correspondences defined by algebraic cycles modulo numerical equivalence, we obtain a graded tannakian category $\mathsf{Mot}(k)$ of motives. Let $\mathsf{Mot}_0(k)$ be the subcategory of motives of weight 0 and assume that the Tate conjecture holds for the varieties in $\mathcal{S}$.

For a simple motive $X$, $D = \mathrm{End}(X)$ is a division algebra with centre the subfield $F = \mathbb{Q}[\pi_X]$ generated by the Frobenius endomorphism $\pi_X$ of $X$ and

$$\mathrm{rank}(X) = [D\colon F]^{\frac{1}{2}} \cdot [F\colon \mathbb{Q}].$$

Therefore, $D$ can act on a $\mathbb{Q}$-vector space of dimension $\mathrm{rank}(X)$ only if it is commutative. Since this is never the case for the motive of a supersingular elliptic curve or of the abelian variety obtained by restriction of scalars from such a curve, there cannot be a $\mathbb{Q}$-valued fibre functor on the full category $\mathsf{Mot}(k)$. Let $k = \mathbb{F}_q$. Then, for each prime $v$ of $F$,

$$\mathrm{inv}_v(D) = \begin{cases} 1/2 & \text{if } v \text{ is real and } X \text{ has odd weight} \\ \dfrac{\mathrm{ord}_v(\pi_X)}{\mathrm{ord}_v(q)} \cdot [F_v : \mathbb{Q}_p] & \text{if } v|p \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

(Tate's formula; see Milne 1994, 2.16). When $q = p$, $\mathrm{ord}_v(p)$ is the ramification index $e(v/p)$, which divides the local degree $[F_v\colon \mathbb{Q}_p]$. Thus, for $k = \mathbb{F}_p$ and $X$ a motive of weight 0 (modulo 2), $D$ is commutative, and so the endomorphism algebras provide no obstruction to $\mathsf{Mot}_0(\mathbb{F}_p)$ being neutral. In this note, we examine whether it is, in fact, neutral.

Before stating our results, we need some notations. Let $K$ be a CM subfield of $\mathbb{C}$, finite and galois over $\mathbb{Q}$, and let $n$ be a sufficiently divisible positive integer. Define $W^K(p,n)$ to be the group of algebraic numbers $\pi$ in $\mathbb{C}$ such that

- $|\pi'| = 1$ for all conjugates $\pi'$ of $\pi$ in $\mathbb{C}$;
- $p^N \pi$ is an algebraic integer for some $N$;

- $\pi^n \in K$, and for every $p$-adic prime of $w$ of $K$, $\frac{\mathrm{ord}_w(\pi^n)}{n \cdot \mathrm{ord}_w(p)}[K_w\colon\mathbb{Q}_p] \in \mathbb{Z}$.

Define $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ to be the category of motives over $\mathbb{F}_p$ whose Weil numbers lie in $W^K(p,n)$. Let $m$ be the order of $\mu(K)$. We prove the following.

**(3.3)** There exists a $\mathbb{Q}_l$-valued fibre functor on $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ for every prime $l$ of $\mathbb{Q}$ (including $p$ and $\infty$).

**(5.2)** There exists a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ if and only if there exists a cyclic field extension $L$ of $\mathbb{Q}$ of degree $mn$ such that

(a) $(p)$ remains prime[1] in $L$;

(b) $\pi$ is a local norm at every prime $v$ of $\mathbb{Q}[\pi^{mn}]$ that ramifies in $\mathbb{Q}(\pi^{mn}) \otimes_{\mathbb{Q}} L$.

Moreover, we show that the generalized Riemann hypothesis sometimes implies that there exists such an $L$.

Now consider the full category $\mathsf{Mot}_0(\mathbb{F}_p)$ of motives of weight 0 over $\mathbb{F}_p$. Then

$$\mathsf{Mot}_0(\mathbb{F}_p) = \bigcup\nolimits_{K,n} \mathsf{Mot}_0^K(\mathbb{F}_p, n),$$

but the existence of a $\mathbb{Q}$-valued fibre functor on each of the categories $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ does not imply that there exists a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0(\mathbb{F}_p)$. In fact, we give a heuristic argument (due to Kontsevich) to show that there does not exist such a fibre functor.

*Throughout the article, we fix a class $\mathcal{S}$ of smooth projective varieties[2] over $k$, closed under the formation of products, disjoint sums, and passage to a connected component, and containing the abelian varieties, projective spaces, and varieties of dimension zero. Except in the last section, we assume that the Tate conjecture holds for the varieties in $\mathcal{S}$.*

# 1 The cohomology of groups of multiplicative type

Let $M$ be a finitely generated $\mathbb{Z}$-module with a continuous action of $\Gamma = \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ (discrete topology on $M$), and let $T = D(M)$ be the corresponding algebraic group of multiplicative type over $\mathbb{Q}$. Thus

$$X^*(T) \overset{\mathrm{def}}{=} \mathrm{Hom}(T_{\mathbb{Q}^{\mathrm{al}}}, \mathbb{G}_m) = M.$$

For $m \in M$, let $\mathbb{Q}[m]$ be the fixed field of $\Gamma_m \overset{\mathrm{def}}{=} \{\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}) \mid \sigma m = m\}$, so that

$$\Sigma_m \overset{\mathrm{def}}{=} \mathrm{Hom}(\mathbb{Q}[m], \mathbb{Q}^{\mathrm{al}}) \simeq \Gamma/\Gamma_m.$$

Let $(\mathbb{G}_m)_{\mathbb{Q}[m]/\mathbb{Q}}$ be the torus over $\mathbb{Q}$ obtained from $\mathbb{G}_m$ by (Weil) restriction of scalars from $\mathbb{Q}[m]$ to $\mathbb{Q}$, so that

$$X^*((\mathbb{G}_m)_{\mathbb{Q}[m]/\mathbb{Q}}) \simeq \mathbb{Z}[\Sigma_m]$$

(free $\mathbb{Z}$-module on $\Sigma_m$ with $\tau \in \Gamma$ acting by $\tau(\sum n_\sigma \sigma) = \sum n_\sigma \tau \circ \rho$). The map

$$\sum\nolimits_\sigma n_\sigma \sigma \mapsto \sum\nolimits_\sigma n_\sigma \cdot \sigma m\colon \mathbb{Z}[\Sigma_m] \to M, \tag{2}$$

defines a homomorphism $T \to (\mathbb{G}_m)_{\mathbb{Q}[m]/\mathbb{Q}}$ and hence a homomorphism

$$\alpha_m\colon H^2(\mathbb{Q}, T) \to H^2(\mathbb{Q}, (\mathbb{G}_m)_{\mathbb{Q}[m]/\mathbb{Q}}) \simeq \mathrm{Br}(\mathbb{Q}[m]). \tag{3}$$

---

[1] By this I mean that the ideal generated by $p$ in $\mathcal{O}_L$ is prime.

[2] By a variety, I mean a geometrically reduced scheme of finite type over the ground field.

PROPOSITION 1.1 *Let $c \in H^2(\mathbb{Q}, T)$. If $\alpha_m(c) = 0$ for all $m \in M$, then $c$ lies in the kernel of*

$$H^2(\mathbb{Q}, T) \to H^2(\mathbb{Q}_l, T)$$

*for every prime $l$ of $\mathbb{Q}$ (including $l = \infty$).*

PROOF. Let $c$ be an element of $H^2(\mathbb{Q}, T)$ such that $\alpha_m(c) = 0$ for all $m \in M$, and fix a finite prime $l$ of $\mathbb{Q}$. To show that $c$ maps to zero in $H^2(\mathbb{Q}_l, T)$, it suffices to show that the family of homomorphisms

$$\alpha_{m,l}\colon H^2(\mathbb{Q}_l, T) \to H^2(\mathbb{Q}_l, (\mathbb{G}_m)_{\mathbb{Q}[m]/\mathbb{Q}}), \quad m \in M,$$

is injective. Choose an extension of $l$ to $\mathbb{Q}^{\mathrm{al}}$, and let $\Gamma(l) \subset \Gamma$ be the corresponding decomposition group. A standard duality theorem (Milne 1986, I 2.4) shows that the $\alpha_{m,l}$ is obtained from the homomorphism

$$\mathbb{Z}[\Sigma_m]^{\Gamma(l)} \to M^{\Gamma(l)} \tag{4}$$

by applying the functor $\mathrm{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$. Thus it suffices to prove that the family of homomorphisms (4), indexed by $m \in M$, is surjective. Let $m \in M^{\Gamma(l)}$. Because the group $\Gamma(l)$ fixes $m$, it is contained in $\Gamma_m$, and so it fixes the inclusion $\sigma_0\colon \mathbb{Q}[m] \hookrightarrow \mathbb{Q}^{\mathrm{al}}$. Thus $\sigma_0$ is an element of $\mathbb{Z}[\Sigma_m]^{\Gamma(l)}$, and it maps to $m$.

The proof with $l = \infty$ is similar (apply Milne 1986, I 2.13b). □

NOTES The proposition is abstracted from Milne 1994 (proof of Theorem 3.13).

## 2 Review of the category of motives over $\mathbb{F}$

Let $q = p^n$. Recall that a ***Weil $q$-number of weight*** $m$ is an algebraic number $\pi$ such that

- $|\pi'| = q^{m/2}$ for all conjugates $\pi'$ of $\pi$ in $\mathbb{C}$ and
- $q^N\pi$ is an algebraic integer for some $N$.

The first condition implies that $\pi \mapsto q^m/\pi$ defines an automorphism $\iota'$ of $\mathbb{Q}[\pi]$ such that $\sigma \circ \iota' = \iota \circ \sigma$ for all $\sigma\colon \mathbb{Q}[\pi] \to \mathbb{C}$. Therefore, $\mathbb{Q}[\pi]$ is totally real or CM. Note that, because $q^N\pi$ is an algebraic integer and $(q^N \cdot \pi)(q^N \cdot \iota'\pi) = q^{2N+m}$, the ideal $(\pi)$ is divisible only by $p$-adic primes.

Fix a CM-subfield $K$ of $\mathbb{Q}^{\mathrm{al}}$, finite and galois over $\mathbb{Q}$, and let $W_0^K(q)$ denote the set of Weil $q$-numbers of weight 0 in $K$ such that

$$n_w(\pi) \overset{\text{def}}{=} \frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)}[K_w\colon \mathbb{Q}_p]$$

lies in $\mathbb{Z}$ for all $p$-adic primes $w$ of $K$. Note that the torsion subgroup of $W_0^K(q)$ is $\mu(K)$, the group of roots of 1 in $K$. Let $X$ and $Y$ be the sets of $p$-adic primes of $K$ and of its largest real subfield $F$. Write $f_K$ for the common inertia degree[3] of the $p$-adic prime ideals of $K$ and $h_K$ for their common order in the class group of $K$.

[3]The inertia degree of a prime $\mathfrak{p}$ of $K$ is the degree $f(\mathfrak{p}/p) = [\mathcal{O}_K/\mathfrak{p}\colon \mathbb{F}_p]$ of the field extension $\mathcal{O}_K/\mathfrak{p} \supset \mathbb{F}_p$.

PROPOSITION 2.1 *For any $n$ divisible by $f_K h_K$, the sequence*

$$0 \longrightarrow W_0^K(p^n)/\mu(K) \xrightarrow{\pi \mapsto \sum_{w|p} n_w(\pi) w} \mathbb{Z}^X \xrightarrow{\sum a_w w \mapsto \sum a_w w|F} \mathbb{Z}^Y \longrightarrow 0 \qquad (5)$$

*is exact.*

PROOF. Everything is obvious except that every element in the kernel of the second map is in the image of the first.

Let $\Gamma = \mathrm{Hom}(K, \mathbb{Q}^{\mathrm{al}}) = \mathrm{Gal}(K/\mathbb{Q}^{\mathrm{al}})$. The group $I_0(K)$ of infinity types of weight 0 on $K$ is the subgroup of $\mathbb{Z}[\Gamma]$ consisting of the sums $\sum n_\sigma \sigma$ such that $n_\sigma + n_{\iota\sigma} = 0$ for all $\sigma$. Fix a $p$-adic prime $w_0$ of $\mathbb{Q}^{\mathrm{al}}$. As $\Gamma$ acts transitively on $X$, the sequence

$$I_0(K) \xrightarrow{\sum n_\sigma \sigma \mapsto \sum n_\sigma \sigma w_0} \mathbb{Z}^X \xrightarrow{\sum a_w w \mapsto \sum a_w w|F} \mathbb{Z}^Y \longrightarrow 0$$

is exact. Because $n/f_K$ is divisible by $h_K$, there exists an element $\varpi$ of $\mathcal{O}_K$ such that $\mathfrak{p}_{w_0}^{n/f_K} = (\varpi)$, i.e., such that for $w$ a finite prime of $K$,

$$\mathrm{ord}_w(\varpi) = \begin{cases} n/f_K & \text{if } w = w_0 \\ 0 & \text{otherwise.} \end{cases}$$

For $\chi = \sum n_\sigma \sigma \in I_0(K)$ and $a \in K^\times$, let

$$\chi(a) = \textstyle\prod_{\sigma \in \Gamma} (\sigma a)^{n_\sigma}.$$

Then $\chi(a) = 1$ for $a \in F^\times$. As the group of units in $F$ has finite index in the group of units in $K$, this shows that $\pi \stackrel{\text{def}}{=} \chi(\varpi)$ is independent of the choice of $\varpi$ up to an element of $\mu(K)$. It lies in $W_0^K(p^n)$, and the diagram

$$\begin{array}{ccc} I_0(K) & & \\ \downarrow{\scriptstyle\chi} & \searrow & \\ & & \mathbb{Z}^X \\ & \nearrow & \\ W_0^K(p^N) & & \end{array}$$

commutes, which completes the proof. □

If $n|n'$, then $\pi \mapsto \pi^{n'/n}$ is a homomorphism $W^K(p^n) \to W^K(p^{n'})$; we define $W^K(p^\infty) = \varinjlim W^K(p^n)$. Similarly, $W_0^K(p^\infty) = \varinjlim W_0^K(p^n)$. Thus, an element of $W_0^K(p^\infty)$ is represented by a pair $(\pi, n)$ with $n \in \mathbb{N}^\times$ and $\pi \in W_0^K(p^n)$.

COROLLARY 2.2 *When $n$ divides $n'$ and both are divisible by $f_K h_K$,*

$$W_0^K(p^n)/\mu(K) \simeq W_0^K(p^{n'})/\mu(K) \simeq W_0^K(p^\infty).$$

*The sequence*

$$0 \to W^K(p^\infty) \to \mathbb{Z}^X \to \mathbb{Z}^Y \to 0$$

*is exact.*

PROOF. The diagram

$$\begin{array}{ccc} W_0^K(p^n) & \longrightarrow & \mathbb{Z}^X \\ {\scriptstyle \pi\mapsto\pi^{n/n'}}\downarrow & & \| \\ W_0^K(p^{n'}) & \longrightarrow & \mathbb{Z}^X \end{array}$$

commutes, and so this follows from (5). □

Let $P^K(p^n)$ be the algebraic group of multiplicative type over $\mathbb{Q}$ with character group $X^*(P^K(p^n)) = W^K(p^n)$.

COROLLARY 2.3 *Let $m = |\mu(K)|$. For any $n$ divisible by $f_K h_K$, there are exact sequences*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathbb{G}_m)_{F/\mathbb{Q}} & \longrightarrow & (\mathbb{G}_m)_{K/\mathbb{Q}} & \longrightarrow & P^K(p^\infty) & \longrightarrow & 0 \\ & & & & & & \| & & \\ & & & & 0 & \longrightarrow & P^K(p^\infty) & \longrightarrow & P^K(p^n) \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0 \end{array}$$

PROOF. Obvious from (2.1) and (2.2). □

PROPOSITION 2.4 *(a) The family of maps $H^1(\mathbb{Q}, P_0^K(p^\infty)) \to H^1(\mathbb{Q}_l, P_0^K(p^\infty))$, with $l$ running over the primes of $\mathbb{Q}$, is injective.*

*(b) $H^2(\mathbb{Q}, P_0^K(p^\infty)) \simeq \bigoplus_l H^2(\mathbb{Q}_l, P_0^K(p^\infty))$ (sum over all primes of $\mathbb{Q}$).*

PROOF. This follows from the cohomology sequence of the upper exact sequence in (2.3) and class field theory (Milne 1994, 3.11). □

PROPOSITION 2.5 *The family of maps $H^2(\mathbb{Q}, P_0^K(p^\infty)) \to \mathrm{Br}(\mathbb{Q}[\pi])$, $\pi \in W_0^K(p^\infty)$, (see (3)) is injective.*

PROOF. Apply Proposition 1.1 and (b) of Proposition 2.4. □

Let $X$ be a simple object in $\mathsf{Mot}_0^K(\mathbb{F})$, and let $\pi_X$ be its Frobenius endomorphism.

PROPOSITION 2.6 *The map $H^2(\alpha_{\pi_X})\colon H^2(\mathbb{Q}, P_0^K(p^\infty)) \to \mathrm{Br}(\mathbb{Q}[\pi_X])$ sends the class of $\mathsf{Mot}_0^K(\mathbb{F})$ in $H^2(\mathbb{Q}, P_0^K(p^\infty))$ to the class of $\mathrm{End}(X)$ in $\mathrm{Br}(\mathbb{Q}[\pi_X])$.*

PROOF. This can be proved by the same argument as in Saavedra Rivano 1972, VI 3.5.3. □

REMARK 2.7 Let $W_0(p^\infty) = \varinjlim_n W_0(p^n)$ and $P_0(p^\infty) = \varprojlim_K P_0^K(p^\infty)$; thus $P_0(p^\infty)$ is the pro-torus with character group $W_0(p^\infty)$. Proposition 2.5 shows that the family of maps $H^2(\mathbb{Q}, P_0(p^\infty)) \to \mathrm{Br}(\mathbb{Q}[\pi])$, $\pi \in W_0(p^\infty)$, has kernel $\varprojlim^1_K H^1(\mathbb{Q}, P_0^K(p^\infty))$, which is zero (Milne 2003, 3.8).

NOTES This section reviews results from Langlands and Rapoport 1987; Wei 1993; Milne 1994, 2003.

# 3 The category of motives over $\mathbb{F}_p$

As before, fix a (large) CM-subfield $K$ of $\mathbb{Q}^{\text{al}}$, finite and galois over $\mathbb{Q}$. Let $W_0^K(p,n)$ be the group of Weil $p$-numbers $\pi$ in $\mathbb{Q}^{\text{al}}$ of weight 0 such that $\pi^n \in W_0^K(p^n)$. Note that, $W_0^K(p,1) = W_0^K(p)$, but otherwise the elements of $W_0^K(p,n)$ need not lie in $K$.

LEMMA 3.1 *For any $n$ divisible by $f_K h_K$, there is an exact sequence*

$$0 \longrightarrow \mu_{mn} \longrightarrow W_0^K(p,n) \xrightarrow{\pi\mapsto[\pi^n,n]} W_0^K(p^\infty) \longrightarrow 0.$$

*where $m = |\mu(K)|$ and $\mu_{mn} = \mu_{mn}(\mathbb{Q}^{\text{al}})$.*

PROOF. According to (2.2), an element of $W_0^K(p^\infty)$ is represented by a $\pi \in W_0^K(p^n)$. Now any $n$th root $\pi^{\frac{1}{n}}$ of $\pi$ in $\mathbb{Q}^{\text{al}}$ lies in $W_0^K(p,n)$ and maps to $\pi$.

If $\pi \in W_0^K(p,n)$ is such that $\pi^n$ represents 1 in $W_0^K(p^\infty)$, then $\pi^n \in W_0^K(p^n)_{\text{tors}} = \mu(K)$. Therefore $(\pi^n)^m = 1$. Conversely, if $\pi^{mn} = 1$, then $\pi \in W_0(p,n)$ and maps to 1 in $W_0^K(p^\infty)$. □

Let $P_0^K(p,n)$ be the group of multiplicative type over $\mathbb{Q}$ such that $X^*(P_0^K(p,n)) = W_0^K(p,n)$.

PROPOSITION 3.2 *For any $n$ divisible by $f_K h_K$, there is an exact sequence*

$$0 \to P_0^K(p^\infty) \to P_0^K(p,n) \to \mathbb{Z}/nm\mathbb{Z} \to 0. \tag{6}$$

PROOF. Immediate from the lemma. □

Recall that the isomorphism classes of simple objects in $\mathsf{Mot}(\mathbb{F}_p)$ are classified by the conjugacy classes of elements of $W(p)$ (Weil $p$-numbers in $\mathbb{Q}^{\text{al}}$) (see, for example, Milne 1994, 2.6). Let $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ be the category of motives over $\mathbb{F}_p$ whose Weil $p$-numbers lie in $W_0^K(p,n)$.

PROPOSITION 3.3 *The category $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ has a $\mathbb{Q}_l$-valued fibre functor for all primes $l$ of $\mathbb{Q}$ (including $p$ and $\infty$).*

PROOF. As we noted in the introduction, the endomorphism algebras of simple objects in $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ are commutative, and so this follows from Propositions 2.6 and 1.1. □

# 4 Cyclic algebras

Let $F$ be field.

DEFINITION 4.1 A ***cyclic semifield over*** $F$ is an étale $F$-algebra $E$ together with an action of a cyclic group $C$ such that $C$ acts simply transitively on $\operatorname{Hom}_{F\text{-algebra}}(E, F^{\text{al}})$. In other words, it is a galois $F$-algebra with cyclic galois group (in the sense of Grothendieck).

PROPOSITION 4.2 *Let $E$ be a cyclic field extension of $F$ with generating automorphism $\sigma_0$. Then $(E^m,\sigma)$, with $\sigma(a_1,\ldots,a_m) = (\sigma_0 a_m, a_1,\ldots,a_{m-1})$, is a cyclic semifield over $F$, and every cyclic semifield over $F$ is isomorphic to one of this form.*

PROOF. Routine application of galois theory (in the sense of Grothendieck). □

We denote $(E^m, \sigma)$ by $(E, \sigma_0)^m$.

EXAMPLE 4.3 Let $(E, \sigma)$ be a cyclic field over $F$. Let $F'$ be a field containing $F$, and let $EF'$ be the composite of $E$ and $F'$ in some common larger field. Let $m$ be the least positive integer such that $\sigma^m$ fixes $E \cap F'$. Then

$$\langle \sigma^m \rangle = \mathrm{Gal}(E/E \cap F') \simeq \mathrm{Gal}(EF'/F'),$$

and so $(EF', \sigma^m)$ is a cyclic field over $F$. Clearly, $(E \otimes_F F', \sigma) \approx (EF', \sigma^m)^m$.

Let $(E, \sigma)$ be a cyclic semifield over $F$. For any element $a \in F^\times$, define

$$B(E, \sigma, a) = E \cdot 1 + E \cdot x + \cdots + Ex^{n-1}$$

with the multiplication determined by

$$x^n = a, \quad x \cdot e = \sigma(e) \cdot x \text{ for } b \in E.$$

Then $B(E, \sigma, a)$ is a central simple $F$-algebra (Albert 1939, VII). Algebras of this form are called ***cyclic***.[4] Because $E$ is a maximal étale subalgebra of $B$, it splits $B$, and so $B(E, \sigma, a)$ represents a class in $\mathrm{Br}(E/F)$.

PROPOSITION 4.4 *With the notations of (4.2),*

$$B(E^m, \sigma, a) \approx B(E, \sigma_0, a) \otimes_F M_m(F).$$

PROOF. See Albert 1939, VII 1, Theorem 1. □

COROLLARY 4.5 *Let $(E, \sigma)$ be a cyclic field over $F$. Let $F'$ be a field containing $F$, and let $a \in F^\times$. With the notations of (4.3),*

$$[B(E \otimes_F F', \sigma, a)] = [B(E, \sigma, a) \otimes_F F'] = [B(EF', \sigma^m, a)]$$

*(equality of classes in $\mathrm{Br}(F')$). More generally, when $a \in F'^\times$, one still has*

$$[B(E \otimes_F F', \sigma, a)] = [B(EF', \sigma^m, a)]$$

PROOF. Apply the proposition to $(E \otimes_F F', \sigma) \approx (EF', \sigma^m)^m$. See also Reiner 2003, 30.8, for the case where $a \in F^\times$. □

4.6 For a fixed $(E/F, \sigma)$, the map

$$a \mapsto [B(E, \sigma, a)] \colon F^\times \to \mathrm{Br}(E/F)$$

has the following cohomological description. The choice of the generator $\sigma$ for the galois group of $E/F$ determines an isomorphism of the Tate cohomology groups $H^0(E/F, E^\times) \to H^2(E/F, E^\times)$, i.e., an isomorphism

$$F^\times / \mathrm{Nm}\, E^\times \to \mathrm{Br}(E/F) \tag{7}$$

(periodicity of the cohomology of cyclic groups; see, for example, Milne 1997, II 2.11). This isomorphism maps $a \in F^\times$ to the class of $B(E, \sigma, a)$. When $F$ is a local or global field, it is known that every element of $\mathrm{Br}(F)$ is split by a cyclic extension, and so is represented by a cyclic algebra.

[4] Classically, they were called "generalized cyclic algebras", and "cyclic algebra" was reserved for those with $E$ is a field.

EXAMPLE 4.7 Let $F$ be a finite extension of $\mathbb{Q}_p$ and let $E$ be an unramified field extension of $F$ of degree $n$. Choose $\sigma$ to be the Frobenius element. For any $a \in F^{\times}$, $B(E,\sigma,a)$ has invariant $\mathrm{ord}_K(a)/n$ (cf. Milne 1997, IV 4.2). Here $\mathrm{ord}_K$ is normalized to map onto $\mathbb{Z}$.

We now fix $(F,a)$ and give a cohomological description of

$$(E,\sigma) \mapsto [B(E,\sigma,a)]\colon H^1(F,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{Br}(F). \tag{8}$$

Let $F[x] = F[X]/(X^n - a)$. The inclusion $F^{\times} \hookrightarrow F[x]^{\times}$ defines a homomorphism $\mathbb{G}_m \to (\mathbb{G}_m)_{F[x]/F}$, and we let $T$ be the cokernel. The class of $x$ in $F[x]^{\times}/F^{\times} \subset T(\mathbb{Q})$ has order dividing $n$, and the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & (\mathbb{G}_m)_{F[x]/F} & \longrightarrow & T & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle 1\mapsto[x]} & & \\ & & & & & & \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

of groups of multiplicative type gives rise to a diagram of cohomology groups

$$\begin{array}{ccccc} H^1(F,T) & \longrightarrow & \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(F[x]) \\ \uparrow & & & & \\ H^1(F,\mathbb{Z}/n\mathbb{Z}) & & & & \end{array}$$

LEMMA 4.8 *The composite of the maps*

$$H^1(F,\mathbb{Z}/n\mathbb{Z}) \to H^1(F,T) \to \mathrm{Br}(F)$$

*is the map (8).*

PROOF. Omitted (for the moment). □

PROPOSITION 4.9 *Let $L$ be an unramified cyclic field extension of $\mathbb{Q}_p$ of degree $n$, and let $\sigma$ be the Frobenius automorphism of $L$ over $\mathbb{Q}_p$. For any finite extension $F$ of $\mathbb{Q}_p$ and $a \in F$,*

$$\mathrm{inv}_v\, B(L \otimes_{\mathbb{Q}_p} F, \sigma, a) = \frac{\mathrm{ord}_F(a)}{n \cdot \mathrm{ord}_F(p)} \cdot [F\colon \mathbb{Q}_p]. \tag{9}$$

PROOF. Let $e$ and $f$ be the ramification and inertia indices of $p$ in $F$. The composite $LF$ of $L$ and $F$ in some common larger field is an unramified extension of $F$ of degree $n/f$ with Frobenius element $\sigma^f$. Thus (see 4.5, 4.7),

$$\begin{aligned} \mathrm{inv}_F\, B(L \otimes_{\mathbb{Q}_p} F, \sigma, a)) &= \mathrm{inv}_F(B(LF, \sigma^f, a) \\ &= \frac{\mathrm{ord}_F(a)}{n/f}. \end{aligned}$$

Since $\mathrm{ord}_F(p) = e$, this gives (9). □

# 5 The $\mathbb{Q}$-valued fibre functors on $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$

As before, $K$ is a CM subfield of $\mathbb{Q}^{\mathrm{al}}$, finite and galois over $\mathbb{Q}$, and $n$ is an integer divisible by $f_K h_K$.

LEMMA 5.1 *Let $\pi \in W_0^K(p,n)$, and let $\overline{\pi}$ be the image of $\pi$ in $W_0(p^\infty)$. Let $X(\overline{\pi})$ be the simple motive over $\mathbb{F}$ corresponding to $\overline{\pi}$. Then the centre of $\mathrm{End}(X(\overline{\pi}))$ is $\mathbb{Q}[\pi^{mn}]$.*

PROOF. Recall that $\overline{\pi}$ is represented by $\pi^n \in W_0^K(p^n)$. The centre of $\mathrm{End}(X(\overline{\pi}))$ is $\mathbb{Q}[\overline{\pi}]$ (notations as in §1, i.e., $\mathbb{Q}[\overline{\pi}]$ is the fixed field of the subgroup of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ fixing $\overline{\pi}$). An element $\sigma$ of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ fixes $\overline{\pi}$ if and only if it fixes its image in $\mathbb{Z}^X$ (notation as in §2), but this equals the image $\pi^n$ in $\mathbb{Z}^X$, which is fixed by $\sigma$ if and only if $\sigma$ fixes $(\pi^n)^m$. □

THEOREM 5.2 *There exists a $\mathbb{Q}$-valued fibre functor $\omega$ on $\mathsf{Mot}_0^K(p,n)$ if and only if there exists a cyclic field extension $L$ of $\mathbb{Q}$ of degree $mn$ such that*
(a) *$(p)$ remains prime in $L$;*
(b) *$\pi^{mn}$ is a local norm at every prime $v$ of $\mathbb{Q}[\pi^{mn}]$ that ramifies in $\mathbb{Q}[\pi^{mn}] \otimes_{\mathbb{Q}} L$.*

PROOF. Consider the diagram arising from (6) and (8)

$$\begin{array}{ccccc}
H^1(\mathbb{Q}, \mathbb{Z}/mn\mathbb{Z}) & \xrightarrow{\alpha} & H^2(\mathbb{Q}, P_0^K(p^\infty)) & \xrightarrow{\beta} & H^2(\mathbb{Q}, P_0^K(p,n)) \\
& \searrow^{\gamma} & \downarrow{\scriptstyle \text{injective}} & & \\
& \prod_{\pi \in W_0^K(p,n)} & \mathrm{Br}(\mathbb{Q}[\pi^{mn}]) & &
\end{array}$$

The map $\beta$ sends the cohomology class of $\mathsf{Mot}_0^K(\mathbb{F}_p)$ to that of $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$. Thus, $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ is neutral if and only if the cohomology class of $\mathsf{Mot}_0^K(\mathbb{F}_p)$ is in the image of $\alpha$. Since $\gamma$ sends an element $(L,\sigma)$ of $H^1(\mathbb{Q}, \mathbb{Z}/mn\mathbb{Z})$ to the class of $B(L \otimes_{\mathbb{Q}} \mathbb{Q}[\pi^{mn}], \sigma, \pi^{mn})$ in $\mathrm{Br}(\mathbb{Q}[\pi^{mn}])$ (cf. 4.8), we see that $\mathsf{Mot}_0^K(p,n)$ is neutral if and only if there exists a cyclic field extension $(L,\sigma)$ of degree dividing $mn$ such that, for all $\pi \in W_0^K(p,n)$ and all primes $v$ of $\mathbb{Q}[\pi^{mn}]$,

$$\mathrm{inv}_v(B(L \otimes_{\mathbb{Q}} \mathbb{Q}[\pi^{mn}], \sigma, \pi^{mn})) = \begin{cases} \dfrac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(p^{mn})} \cdot [\mathbb{Q}[\pi^{mn}]_v : \mathbb{Q}_p] & \text{if } v|p \\ 0 & \text{otherwise} \end{cases} \qquad (10)$$

Let $L$ be a cyclic field extension of $\mathbb{Q}$ of degree $mn$ satisfying the conditions (a) and (b) and let $\sigma = (p, L/\mathbb{Q})$. Condition (a) implies that (10) holds for the primes $v$ dividing $p$ (apply Proposition 4.9 with $L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for $L$, $\mathbb{Q}[\pi^{mn}]_v$ for $F$, $\pi^{mn}$ for $a$), and condition (b) implies that (10) holds for the primes not dividing $p$ (see (4.6)).

Conversely, let $(L,\sigma)$ be a cyclic extension of $\mathbb{Q}$ of degree dividing $mn$ satisfying (10). By considering the primes dividing $p$ and applying Proposition 4.9, one sees that $L$ has degree $mn$, that $(p)$ remains primes in $L$, and $\sigma = (p, L/K)$. On the other hand, the invariant at a prime not dividing $p$ vanishes automatically unless the prime ramifies in $\mathbb{Q}[\pi^{mn}]$, in which case it vanishes if and only if (b) holds (by 4.6). □

THEOREM 5.3 *Let $F$ be a the field generated over $\mathbb{Q}$ by the elements of $W_0^K(p,n)$ — it is a finite galois extension of $\mathbb{Q}$. The generalized Riemann hypothesis implies that there exists a field $L$ satisfying the conditions (a) and (b) of (5.2) provided $p$ is not an $r$th power in $F \cdot \mathbb{Q}^{\mathrm{ab}}$ for any $r$ dividing $mn$.*

PROOF. Note that $F$ is generated over $\mathbb{Q}$ by any set of generators for the abelian group $W_0^K(p,n)$, which can be chosen to be finite and stable under the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$, which shows that $F$ is finite and galois over $\mathbb{Q}$. Note that condition (b) is implied by the stronger condition:

(b′) every prime $l \neq p$ ramifying in $L$ splits in $F$.

(Because then $\pi \in \mathbb{Q}[\pi^{mn}]_v = \mathbb{Q}_l$, and so $\pi^{mn}$ is an $mn$th power *inside* $\mathbb{Q}[\pi^{mn}]_v$.) A natural place to look for such an extension $L$ is inside $\mathbb{Q}[\zeta_l]$ for some prime $l$. Since only $l$ ramifies in $\mathbb{Q}[\zeta_l]$, it will contain an $L$ satisfying (a) and (b′) if

(c) $(\mathbb{Z}/l\mathbb{Z})^\times$ has a quotient of order $mn$ generated by the class of $p$,

(d) $l$ splits in $F$.

We show in the next section that the generalized Riemann hypothesis implies that, under our hypothesis on $p$, $r$, and $F$, there are always infinitely many primes satisfying these conditions (c,d). □

REMARK 5.4 We can make the relation between the $\mathbb{Q}$-valued fibre functors on $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ and the cyclic field extensions of $\mathbb{Q}$ more precise. The base change functor

$$\beta\colon \mathsf{Mot}_0^K(\mathbb{F}_p,n) \to \mathsf{Mot}_0^K(\mathbb{F})$$

realizes the second category as a normal quotient of the first category (in the sense of Milne 2005, §2). The objects of $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ becoming trivial in $\mathsf{Mot}_0^K(\mathbb{F},n)$ are exactly the Artin motives. Let $\omega^\beta$ be the fibre functor on $\mathsf{Art}^K(\mathbb{F}_p,n)$ defined by $\beta$ (ib. §2). Note that the fundamental group of $\mathsf{Art}^K(\mathbb{F}_p,n)$ is $\mathbb{Z}/mn\mathbb{Z}$, and that the motive $X_{mn}$ of $\mathbb{F}_{p^{mn}}$ lies in $\mathsf{Art}^K(\mathbb{F}_p,n)$.

Now let $\omega$ be a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$, and let $\wp = \underline{\mathrm{Hom}}^\otimes(\omega|,\omega^q)$ where $\omega|$ is the restriction of $\omega$ to $\mathsf{Art}^K(\mathbb{F}_p,n)$. Then $\wp$ is a $\mathbb{Z}/mn\mathbb{Z}$-torsor whose class in $H^1(\mathbb{Q},\mathbb{Z}/mn\mathbb{Z})$ maps to the class of $\mathsf{Mot}_0^K(\mathbb{F})$ in $H^2(\mathbb{Q},P_0^K(p^\infty))$ (ib. 2.11). On the other hand, one sees easily that the class of $\wp$ in $H^1(\mathbb{Q},\mathbb{Z}/mn\mathbb{Z})$ is represented by $L=\omega(X_{mn})$.

We have seen that each $\mathbb{Q}$-valued fibre functor $\omega$ on $\mathsf{Mot}_0^K(\mathbb{F}_p)$ gives rise to a cyclic extension $L=\omega(X_{mn})$ of $\mathbb{Q}$, and we have characterized the cyclic extensions that arise in this way. To complete the classification, we have to describe the set of fibre functors giving rise to the same field.

THEOREM 5.5 *Let $\omega$ be a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0^K(p,n)$. The isomorphism classes of pairs consisting of a $\mathbb{Q}$-valued fibre functor $\omega'$ and an isomorphism $\omega(X_{mn}) \to \omega'(X_{mn})$ are classified by $\mathrm{Br}(E/F)$ where $E$ is the fixed field of the decomposition group of a $p$-adic prime of $K$ and $F$ is its largest real subfield.*

PROOF. Let $\wp(\omega')$ be the set of isomorphisms $\omega \to \omega'$ inducing the given isomorphism on $X_{mn}$. Then $\wp(\omega')$ is a torsor for $P_0^K(p^\infty)$ (cf. Milne 2004, 1.6), and $\wp(\omega') \approx \wp(\omega'')$ if and only if $\omega' \approx \omega''$. Therefore, the pairs modulo isomorphism are classified by $H^1(\mathbb{Q},P_0^K(p^\infty))$, which equals $\mathrm{Br}(E/F)$ (Milne 1994, 3.10). □

# 6 The existence of the field $L$

Let $a \neq \pm 1$ be a square-free integer, let $k$ be a second integer, and let $F$ be a finite galois extension of $\mathbb{Q}$. Consider the set $M$ of prime numbers $p$ such that

- $p$ does not divide $a$,
- $p$ splits in $F$,
- the index in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ of the subgroup of generated by the class of $a$ divides $k$.

For each prime number $l$, let $q(l)$ be the smallest power of $l$ not dividing $k$, and let $L_l = \mathbb{Q}[\zeta_{q(l)}, a^{1/q(l)}]$ be the splitting field of $X^{q(l)} - a$ over $\mathbb{Q}$. If $p$ does not divide $a$, then

$$p \text{ splits in } L_l \iff \begin{cases} l \mid p-1, \text{ and} \\ a \text{ is a } q(l)\text{th power modulo } p. \end{cases}$$

Therefore, a necessary condition for $M$ to be nonempty is that none of the fields $L_l$ be contained in $F$.

THEOREM 6.1 *If the generalized Riemann hypothesis holds for each field $L_l$ and no $L_l$ is contained in $F$, then the set $M$ is infinite.*

PROOF. When $k = 1$ and $F = \mathbb{Q}$, the statement becomes Artin's primitive root conjecture: every square-free integer $a \neq \pm 1$ is a primitive root for infinitely many prime numbers $p$. That this follows from the generalized Riemann hypothesis for the fields $L_l$ was proved by Hooley (1967). The general case is proved in Lenstra 1977, 4.6.[5] □

LEMMA 6.2 *Let $a \neq \pm 1$ be a square-free integer, and let $F$ be a finite galois extension of $\mathbb{Q}$. Then there exists an integer $N$ such that, if $a$ is an $m$th power in $F \cdot \mathbb{Q}^{\mathrm{ab}}$, then $m \mid N$.*

PROOF. For odd primes $l$, the galois group of $X^l - a$ is never commutative, and so $a$ is not an $l$th power in $\mathbb{Q}^{\mathrm{ab}}$. It follows that, for any odd $m$, $X^m - a$ is irreducible over $\mathbb{Q}^{\mathrm{ab}}$ (e.g., Lang 2002, VI Theorem 9.1, p297). Therefore, if $a$ is an $m$th power in $\mathbb{Q}^{\mathrm{ab}}$, then $m \mid [F\mathbb{Q}^{\mathrm{ab}} \colon \mathbb{Q}^{\mathrm{ab}}]$.

The proof for even $m$ is similar. □

THEOREM 6.3 *Let $a \neq \pm 1$ be a square-free integer, let $n$ be a positive integer, and let $F$ be a finite galois extension of $\mathbb{Q}$. Let $M$ be the set of prime numbers $p$ such that*

- *$p$ does not divide $a$,*
- *$p$ splits in $F$, and*
- *$(\mathbb{Z}/p\mathbb{Z})^{\times}$ has a quotient of order $n$ generated by the class of $a$.*

*The set $M$ is empty if $a$ is an $m$th power in $F$ for some $m > 1$ dividing $n$, and it is infinite if $a$ is not an $m$th power in $F \cdot \mathbb{Q}^{\mathrm{ab}}$ for any $m$ dividing $n$.*

PROOF. Suppose $p \in M$. If $a$ is an $m$th power in $F$ for some $m$ dividing $n$, then, because $p$ splits in $F$, $a$ is an $m$th power in $\mathbb{Q}_p$. Therefore, it is an $m$th power in $(\mathbb{Z}/p\mathbb{Z})^{\times}$, and in any cyclic quotient $C_n$ of $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Therefore, it can't generate $C_n$.

For the converse statement, the condition on $a$ implies that there exists a $k$ relatively prime to $n$ such that $a$ is not a $q(l)$th power in $F \cdot \mathbb{Q}^{\mathrm{ab}}$ for any prime $l$ (with $q(l)$ defined as above). Then none of the fields $L_l$ is contained in $F[\zeta_{kn}]$, and so there exist infinitely many primes $p$ such that

- $p$ does not divide $a$,
- $p$ splits in $F[\zeta_{nk}]$,
- the index in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ of the subgroup of generated by the class of $a$ divides $k$.

[5] Note that Lenstra frequently muddles his quantifiers. For example, his condition "$a_n \neq 0$ for all $n$" should read "no $a_n$ is zero".

Because $p$ splits in $\mathbb{Q}[\zeta_{kn}]$, $kn$ divides $p-1$, and so $(\mathbb{Z}/p\mathbb{Z})^\times$ has a quotient $C_n$ of order $n$. Because $k$ and $n$ are relatively prime, the image of $a$ in $C_n$ generates it. □

COROLLARY 6.4 *Theorem 5.3 holds.*

PROOF. Apply the theorem with $(a,n)$ replaced by $(p,mn)$. □

QUESTION 6.5 Does there exist a field $L$ satisfying conditions (a) and (b) of Theorem 5.2 for each pair $(K,n)$?

I don't see how to remove the proviso in Theorem 5.3 much less the appeal to the generalized Riemann hypothesis. In fact, I suspect that the answer to the question is no. Here are two comments:

- Let $L=\mathbb{Q}[\zeta_l]$, and let $a\in\mathbb{Z}$ be relatively prime to $l$. When is $a$ local norm at $l$? As $l$ is totally ramified in $L$, the local Galois group is $(\mathbb{Z}/l\mathbb{Z})^\times$, and so this is true if and only if $a\equiv 1$ modulo $l$. Similarly, $a$ is a local norm from the subextension of $\mathbb{Q}[\zeta_l]$ of degree $m$ if and only if $a$ is an $m$th power in $(\mathbb{Z}/l\mathbb{Z})^\times$.
- See Wei 1993 for a description of the subfields of a CM-field generated by Weil numbers.

# 7 Fibre functors on $\mathsf{Mot}^K(\mathbb{F}_p, n)$

PROPOSITION 7.1 *If there exists a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$, then*

(a) there exists a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}^K_{\text{even}}(\mathbb{F}_p,n)$, and
(b) for a number field $L$, there exists an $L$-valued fibre functor on $\mathsf{Mot}^K(\mathbb{F}_p,n)$ if and only if the local degrees of the real and $p$-adic primes of $L$ are even.

PROOF. Omitted (for the present). □

# 8 Explicit description of the categories of motives

In this section, we assume there exists an $L$ as in Theorem and give explicit descriptions of various categories of motives.

## The category $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$

The choice of a fibre functor $\omega$ on defines an equivalence $X\mapsto\omega(X)$ from $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ to the tannakian category whose objects are the pairs $(V,F)$ with $V$ a finite-dimensional vector space over $\mathbb{Q}$ and $F$ a semisimple endomorphism of $V$ whose eigenvalues lie in $W_0^K(p,n)$.

## The category $\mathsf{Mot}_0^K(\mathbb{F})$

The realization of $\mathsf{Mot}_0^K(\mathbb{F})$ as a quotient of $\mathsf{Mot}_0^K(\mathbb{F}_p,n)$ defines an equivalence from $\mathsf{Mot}_0^K(\mathbb{F})$ to the tannakian category whose objects are pairs $(V,F)$ as before together with an action $L\overset{\text{def}}{=}\omega(X_{mn})$ such that

$$F(av)=\sigma a\cdot Fv,\quad a\in L, v\in V$$

(cf. Milne 2005, 2.3 and 2.12 et seq.).

### The category $\mathsf{Mot}^K(\mathbb{F}_p, n)$

Let $F$ be a quadratic extension of $\mathbb{Q}$ such that the local degrees at $p$ and $\infty$ are both 2. Then $\mathsf{Mot}^K(\mathbb{F}_p, n)$ has an explicit description as an $F$-linear category with a descent datum.

### The category $\mathsf{Mot}^K(\mathbb{F})$.

Again, realize $\mathsf{Mot}^K(\mathbb{F})$ as a quotient of $\mathsf{Mot}^K(\mathbb{F}_p, n)$.

## 9 Fibre functors on $\mathsf{Mot}_0(\mathbb{F}_p)$.

If each of $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ is neutral, does this imply that $\mathsf{Mot}_0(\mathbb{F}_p) = \bigcup_{K,n} \mathsf{Mot}_0^K(\mathbb{F}_p, n)$ is neutral? Let $\omega$ be a $\mathbb{Q}$-valued fibre functor on $\mathsf{Mot}_0(\mathbb{F}_p)$. Then $\omega$ restricts to a $\mathbb{Q}$-valued fibre on $\mathsf{Mot}_0^K(\mathbb{F}_p, n)$ for each $K, n$.

> (Kontsevich email, May 7, 2006). The tower structure means that we have an epimorphism
> $$\widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times.$$
> One cannot get $\mathbb{Z}_p$ factor in the image if one uses only unramified at $p$ extensions; also if one ignores $\mathbb{Z}_p$ component there will be still something wrong: we should get an epimorphism
> $$\textstyle\prod_{l \neq p} \mathbb{Z}_l^\times/(\mathbb{Z}/(l-1)\mathbb{Z}) \twoheadrightarrow \prod_{l \neq p} \mathbb{Z}_l$$
> which splits the inclusion of the closure of the subgroup generated by the element $p$. There is a well-known conjecture, 100% solid by probabilistic reasons, that for any prime $p$ there are infinitely many primes $l$ such that $p^{l-1} = 1 \bmod l^2$, hence $p$ generates a proper closed subgroup in $\mathbb{Z}_l^\times/(\mathbb{Z}/(l-1)\mathbb{Z} = \mathbb{Z}_l$ by the logarithmic map.

We look at this more generally. Let $\mathsf{M}$ be a tannakian category over $k$ that is a countable union $\mathsf{M} = \bigcup \mathsf{M}_n$, $\mathsf{M}_n \subset \mathsf{M}_{n+1}$, of neutral algebraic tannakian subcategories.

Suppose first that $k$ is algebraically closed, and chose a $k$-valued fibre functor $\omega_n$ on each $\mathsf{M}_n$. Because $k$ is algebraically closed, $\omega_{n+1}|\mathsf{M}_n \approx \omega_n$. In fact, given $\omega_n$, we can modify $\omega_{n+1}$ so that $\omega_{n+1}|\mathsf{M}_n = \omega_n$. Thus, there exists a fibre functor $\omega$ on $\mathsf{M}$ such that $\omega|\mathsf{M}_n = \omega_n$.

When we try to do this with $k$ not algebraically closed, then we obtain a sequence of torsors $\underline{\mathrm{Hom}}^\otimes(\omega_n, \omega_{n+1}|\mathsf{M}_n)$. Of course, by making a different choice of fibre functors, we get a different sequence of torsors, but if, for example, the fundamental groups $P_n$ of the $\mathsf{M}_n$ are commutative, then we get in this way a well-defined element of $\varprojlim^1 H^1(k, P_n)$, which is the obstruction to $\mathsf{M}$ being neutral.[6]

[6] Recall that for an inverse system $(A_n, u_n)$ of abelian groups indexed by $(\mathbb{N}, \leq)$, $\varprojlim A_n$ and $\varprojlim^1 A_n$ are the kernel and cokernel respectively of

$$(\ldots, a_n, \ldots) \mapsto (\ldots, a_n - u_{n+1}(a_{n+1}), \ldots)\colon \prod_n A_n \xrightarrow{1-u} \prod_n A_n. \tag{11}$$

# 10 A replacement for the Tate conjecture

Let $\mathbb{A}^{p,\infty}$ be the restricted product of the $\mathbb{Q}_l$ for $l \neq p, \infty$, and let $\mathbb{A}$ be the product of $\mathbb{A}^{p,\infty}$ with the field of fractions of the ring of Witt vectors with coefficients in the ground field.

DEFINITION 10.1 Suppose that for each variety $X$ in $\mathcal{S}$ and each integer $r$ we have a $\mathbb{Q}$-structure $T^r(X)$ on the $\mathbb{A}$-module $\mathcal{T}^r(X)$ of Tate classes. We call the family $(T^r(X))_{X,r}$ a ***theory of rational Tate classes on*** $\mathcal{S}$ if

(a) for each variety $X$ in $\mathcal{S}$, $T^*(X) \stackrel{\text{def}}{=} \bigoplus_r T^r(X)$ is a $\mathbb{Q}$-subalgebra of $\mathcal{T}^*(X)$;
(b) for every regular map $f\colon X \to Y$ of abelian varieties, $f_*$and $f^*$ preserve the $\mathbb{Q}$-structures;
(c) every divisor class on $X$ lies in $T^1(X)$.

The elements of $T^*(X)$ will then be called the rational Tate classes on $X$ (for the particular theory).

Now let $\mathcal{S}$ be the smallest class satisfying the conditions in the introduction, and assume there exists a theory of rational Tate classes. Then we can define categories of motives using the varieties in $\mathcal{S}$ with the rational Tate classes as the correspondences, and everything in the preceding sections holds true. If, moreover, algebraic classes are rational Tate classes, then there is an exact tensor functor from the category of motives defined by algebraic classes to the category of motives defined by rational Tate classes. In particular, a fibre functor on the latter gives rise to a fibre functor on the former.

# References


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

HOOLEY, C. 1967. On Artin's conjecture. *J. Reine Angew. Math.* 225:209–220.

LANG, S. 2002. Algebra, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

LANGLANDS, R. P. AND RAPOPORT, M. 1987. Shimuravarietäten und Gerben. *J. Reine Angew. Math.* 378:113–220.

LENSTRA, JR., H. W. 1977. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.* 42:201–224.

MILNE, J. S. 1986. Arithmetic duality theorems, volume 1 of *Perspectives in Mathematics*. Academic Press Inc., Boston, MA.

MILNE, J. S. 1994. Motives over finite fields, pp. 401–459. *In* Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI.

MILNE, J. S. 1997. Class field theory. Available at www.jmilne.org.

MILNE, J. S. 2003. Gerbes and abelian motives. Preprint available at www.jmilne.org/math/ (also arXiv:math.AG/0301304).

MILNE, J. S. 2004. Periods of abelian varieties. *Compos. Math.* 140:1149–1175.

MILNE, J. S. 2005. Quotients of tannakian categories and rational Tate classes. Preprint, available at www.jmilne.org/math/; also arXiv:math.CT/0508479.

REINER, I. 2003. Maximal orders, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, Oxford.

SAAVEDRA RIVANO, N. 1972. Catégories Tannakiennes. Springer-Verlag, Berlin.

WEI, W. 1993. Weil numbers and generating large field extensions. PhD thesis, University of Michigan.