On the second Tate–Shafarevich group
of a 1-motive

Peter Jossen

msp

On the second Tate–Shafarevich group of a 1-motive

Peter Jossen

We prove finiteness results for Tate–Shafarevich groups in degree 2 associated with 1-motives. We give a number-theoretic interpretation of these groups, relate them to Leopoldt's conjecture, and present an example of a semiabelian variety with an infinite Tate–Shafarevich group in degree 2. We also establish an arithmetic duality theorem for 1-motives over number fields, which complements earlier results of Harari and Szamuely.

Introduction and overview

Let k be a number field, and let X be a commutative group scheme over k. The Tate–Shafarevich group $\mathrm{III}^i(k, X)$ of X is the subgroup of the étale cohomology group $H^i(k, X)$ consisting of those elements that restrict to zero over each completion of k. These groups are among the most fundamental invariants associated with commutative group schemes over number fields, and their vanishing is by definition the obstruction to various local-to-global principles.

If the group scheme X is given by a finitely generated discrete group with continuous Galois action, or if X is a group of multiplicative type, then $\mathrm{III}^i(k, X)$ is finite for all i [Milne 1986, Theorem I.4.20; Neukirch et al. 2000, Theorem 8.6.8]. It

is widely conjectured that if A is an abelian variety over k, then the group $\text{III}^1(k, A)$ is finite, and it is known that for $i \neq 1$ the group $\text{III}^i(k, A)$ is trivial. This is a nontrivial statement for $i = 2$; indeed, the proof of Corollary I.6.24 in [Milne 1986] shows that the vanishing of $\text{III}^2(k, A)$ is essentially equivalent to the positive answer to the congruence subgroup problem for the abelian variety dual to A, given by Serre [1964; 1971].

An evident generalisation of these finiteness results would be to show that $\text{III}^i(k, G)$ is finite for semiabelian varieties G over k, i.e., when G is an extension of an abelian variety A by a torus. A simple dévissage shows that $\text{III}^1(k, G)$ is finite [Harari and Szamuely 2005, Lemma 4.11], provided $\text{III}^1(k, A)$ is finite. The situation is more complicated for $i = 2$, and surprisingly, it turns out that the groups $\text{III}^2(k, G)$ are not always finite.

Theorem 1. *There exists a semiabelian variety G over $\mathbb{Q}$ such that the group $\text{III}^2(\mathbb{Q}, G)$ contains a subgroup isomorphic to $\mathbb{Q}/\mathbb{Z}$ and in particular is infinite.*

A 1-motive M over a number field k is a two-term complex of group schemes $M = [Y \to G]$ over k placed in degrees -1 and 0, where Y is given by a finitely generated free discrete group with continuous Galois action and where G is a semiabelian variety. It was asked in [Harari and Szamuely 2005, Remark 4.13] whether for all 1-motives M the group $\text{III}^2(k, M)$ is finite. By Theorem 1, we already know that this is not always the case even for 1-motives of the form $[0 \to G]$ over $\mathbb{Q}$. Our second result shows that even for very simple 1-motives it might be difficult to decide whether $\text{III}^2(k, M)$ is finite (assuming the conservation law of difficulty).

Theorem 2. *If the group $\text{III}^2(k, M)$ is finite for all 1-motives of the form $M = [\mathbb{Z}^r \to \mathbb{G}_m^s]$ over k, then Leopoldt's conjecture holds for k (and all prime numbers).*

The converse to this statement is not true: there exist 1-motives of this particular form over number fields for which Leopoldt's conjecture is known to hold such that $\text{III}^2(k, M)$ is infinite. Our third result provides conditions on a 1-motive that ensure that $\text{III}^2(k, M)$ is finite. It is most conveniently expressed as a duality theorem. Classical global arithmetic duality theorems are statements about the existence and nondegeneracy of canonical pairings between certain Tate–Shafarevich groups. Let X be a group of multiplicative type over k, and denote by $X^\vee$ its group of characters. The Poitou–Tate duality theorem states that there is a natural, perfect pairing of finite groups

$$\text{III}^i(k, X) \times \text{III}^{3-i}(k, X^\vee) \to \mathbb{Q}/\mathbb{Z}$$

[Milne 1986, Theorem I.4.20; Neukirch et al. 2000, Theorem 8.6.8]. The analogue of this duality theorem for abelian varieties is the Cassels–Tate duality theorem. It states that for an abelian variety A over k with dual $A^\vee$, there is a canonical pairing

$$\text{III}^i(k, A) \times \text{III}^{2-i}(k, A^\vee) \to \mathbb{Q}/\mathbb{Z}$$

whose left and right kernels are the maximal divisible subgroups [Milne 1986, Theorem I.6.26]. Conjecturally, it is a perfect pairing of finite groups.

The idea to unify and generalise these arithmetic duality theorems to duality theorems for 1-motives appeared first in [Harari and Szamuely 2005]. Deligne constructed for each 1-motive M a dual 1-motive $M^\vee$. Harari and Szamuely show that for a 1-motive M over a number field k there is a canonical pairing

$$\text{III}^1(k, M) \times \text{III}^1(k, M^\vee) \to \mathbb{Q}/\mathbb{Z}$$

that is nondegenerate modulo divisible subgroups and generalises the Cassels–Tate pairing. They also construct a pairing between a certain modification of $\text{III}^0(k, M)$ and $\text{III}^2(k, M^\vee)$ and show that it is nondegenerate modulo divisible subgroups. However, this modified $\text{III}^0(k, M)$ remains somehow uncontrollable, and the resulting generalised pairing does not seem to be very useful (the statement of [Harari and Szamuely 2005, Theorem 0.2] was rectified in [Harari and Szamuely 2009]).

Theorem 3. *Let k be a number field, and let $M = [u : Y \to G]$ be a 1-motive over k with dual $M^\vee$. There exists a natural pairing*

$$\text{III}^0(k, M) \times \text{III}^2(k, M^\vee) \to \mathbb{Q}/\mathbb{Z} \qquad (*)$$

generalising the Poitou–Tate pairing for finitely generated Galois modules and tori. The group $\text{III}^0(k, M)$ is finite, and the pairing $(*)$ is nondegenerate on the left. If the semiabelian variety G is an abelian variety or a torus, such that the $\mathbb{Q}$-algebra $\text{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras, then the pairing $(*)$ is a perfect pairing of finite groups.

It was already shown in [Harari and Szamuely 2005] that $\text{III}^0(k, M)$ is finite. The finiteness results stated in the second part of the theorem are new and are also the essential part of the theorem. Equivalently, the condition on G is that over an algebraic closure of k either G is the multiplicative group or an abelian variety isogenous to a product of pairwise nonisogenous simple abelian varieties. Our proof uses techniques developed by Serre [1964; 1971] in his work on the congruence subgroup problem for abelian varieties.

Overview. In Section 1, we rehearse 1-motives and ℓ-adic realisations, which will play a prominent role throughout this paper. In Section 2, we construct a duality pairing that relates the ℓ-adic realisation of a 1-motive with the second Tate–Shafarevich group of its dual and obtain the pairing $(*)$ of Theorem 3. In Section 3, we compute the cohomology of some ℓ-adic Lie groups associated with 1-motives, and in Section 4, we use these computations to prove the finiteness statements in Theorem 3. We conclude the proof of Theorem 3 in Section 5. In

Sections 6 and 7, we prove Theorems 2 and 1, respectively. There remain several open questions and unsolved problems, which I state in the last section.

1. About 1-motives and their realisations

In this section, we rehearse the relevant facts about classical 1-motives and their realisations defined by Deligne [1974, §10].

1.1. Throughout this section, S is a noetherian regular scheme, $\mathscr{F}_S$ stands for the category of sheaves of commutative groups on the small fppf site over S and $\mathscr{D}\mathscr{F}_S$ for the derived category of $\mathscr{F}_S$. We identify commutative group schemes over S with objects of $\mathscr{F}_S$ via the functor of points. In particular, we say that an fppf sheaf on S is an abelian scheme, a torus, or a finite flat group scheme if it can be represented by such. By a *lattice over S*, we mean an object of $\mathscr{F}_S$ that is locally isomorphic to a finitely generated free $\mathbb{Z}$-module. Notice that if S is the spectrum of a field, then Y may be regarded as a finitely generated group on which the absolute Galois group acts continuously.

Definition 1.2. A 1-*motive* over S is a diagram

$$M = \left[\begin{array}{c} Y \\ {}_u\!\downarrow \\ 0 \to T \to G \to A \to 0 \end{array} \right]$$

in the category $\mathscr{F}_S$, where Y is a lattice, T a torus, and A an abelian scheme. A morphism of 1-motives is a morphism between diagrams. The *complex associated with M* is the complex of fppf-sheaves $[M] := [Y \to G]$, placed in degrees -1 and 0. We denote by $\mathcal{M}_{1,S}$ the category of 1-motives over S.

1.3. Observe that the sheaf G is representable. Indeed, we may look at it as a T-torsor over A, and since T is affine, representability follows from [Milne 1980, Theorem III.4.3a]. Later on, 1-motives will often be given by their associated complexes and morphisms accordingly by commutative squares. This is also customary in the literature and justified by the fact that there are no nonzero morphisms from a torus to an abelian scheme.

1.4. We say that a sequence of morphisms of 1-motives $0 \to M_1 \to M_2 \to M_3 \to 0$ is a *short exact sequence* if the induced sequences of lattices, tori, and abelian schemes are exact in $\mathscr{F}_S$. Such a short exact sequence of 1-motives yields then an exact triangle

$$[M_1] \to [M_2] \to [M_3] \to [M_1][1]$$

in the derived category $\mathscr{D}\mathscr{F}_S$. With a 1-motive M over S are naturally associated several short exact sequences coming from the *weight filtration* on M. This is the

natural three-term filtration given by $W_i M = 0$ if $i \leq -3$ and $W_i M = M$ if $i \geq 0$ and

$$W_{-2}M := \begin{bmatrix} 0 \\ \downarrow \\ 0 \to T = T \to 0 \to 0 \end{bmatrix} \quad \text{and} \quad W_{-1}M := \begin{bmatrix} 0 \\ \downarrow \\ 0 \to T \to G \to A \to 0 \end{bmatrix}.$$

Although 1-motives do not form an abelian category, the quotients $M/W_i M$ make sense in the obvious way.

Definition 1.5. Let M be a 1-motive over S, and let ℓ be a prime number that is invertible on S. The *ℓ-adic Tate module* and the *ℓ-divisible Barsotti–Tate group* associated with M are the smooth ℓ-adic sheaf

$$\mathrm{T}_\ell(M) := \lim_{i \geq 0} H^1([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z})$$

and the smooth ℓ-divisible group

$$\mathrm{B}_\ell(M) := \mathrm{colim}_{i \geq 0} H^1([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}),$$

both over S, where the derived tensor product is taken in the derived category $\mathscr{DF}_S$.

1.6. By construction, $\mathrm{T}_\ell M$ only depends on the complex $[M] = [Y \xrightarrow{u} G]$ up to quasi-isomorphism, and the assignment $M \mapsto \mathrm{T}_\ell M$ is functorial. Using the flat resolution $\mathbb{Z} \xrightarrow{\ell^i} \mathbb{Z}$ of $\mathbb{Z}/\ell^i\mathbb{Z}$, we see that the object $[M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}$ of $\mathscr{DF}_S$ is given by the bounded complex

$$\cdots \to 0 \to Y \xrightarrow{y \mapsto (\ell^i y, u(y))} Y \oplus G \xrightarrow{(y,g) \mapsto u(y) - \ell^i g} G \to 0 \to \cdots$$

supported in degrees 0, 1, and 2. For $n \neq 1$, we have $H^n([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}) = 0$ because Y is torsion-free and G is divisible as a sheaf. Hence, the object $[M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}$ of $\mathscr{DF}_S$ is homologically concentrated in degree 1. Given a category $\mathscr{C}$ and a functor $F : \mathscr{DF}_S \to \mathscr{C}$, we write

$$F(\mathrm{T}_\ell M) := \lim_{i \geq 0} F([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}[-1]),$$
$$F(\mathrm{B}_\ell M) := \mathrm{colim}_{i \geq 0} F([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}[-1]),$$

and interpret these expressions as either limit systems in $\mathscr{C}$ or actual objects of $\mathscr{C}$, provided limits and colimits exist in $\mathscr{C}$. This is only a notation, and we do not need or claim that F commutes with limits or colimits.

1.7. Suppose S is connected, and let $\mathrm{spec}(\bar{k}) = \bar{s} \to S$ be a geometric point where $\bar{k}$ is an algebraic closure of the residue field k at the scheme point underlying $\bar{s}$. We can describe the finite, locally constant group schemes $H^1([M] \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z})$ in terms

of finite $\pi_1 := \pi_1^{\text{ét}}(S, \bar{s})$-modules as follows. The underlying group is given by

$$\frac{\{(y, P) \in Y(\bar{k}) \times G(\bar{k}) \mid \ell^i P = u(y)\}}{\{(\ell^i y, u(y)) \mid y \in Y(\bar{k})\}},$$

and the action of π_1 is induced by the action of π_1 on $\bar{k}$. Taking the limit over $i \geq 0$, we find the description of the ℓ-adic sheaf $\mathrm{T}_\ell M$ as a π_1-module. The short exact sequence of 1-motives coming from the weight filtration

$$0 \to [0 \to G] \to M \to [Y \to 0] \to 0$$

induces a sequence of ℓ-adic sheaves and one of continuous π_1-representations

$$0 \to \mathrm{T}_\ell G \to \mathrm{T}_\ell M \to Y \otimes \mathbb{Z}_\ell \to 0,$$

which is exact because $G(\bar{k})$ is an ℓ-divisible group. Observe that, given $y \in Y$, a preimage of $y \otimes 1$ in $\mathrm{T}_\ell M$ is given by a sequence $(y, P_i)_{i \geq 0}$ with $P_0 = u(y)$ and $\ell P_i = P_{i-1}$ for $i \geq 1$.

1.8. Let A be a commutative group. We consider the following four operations on A relative to the prime ℓ:

$$A \widehat{\otimes} \mathbb{Z}_\ell := \lim_{i \geq 0} A/\ell^i A, \qquad\qquad \mathrm{T}_\ell A := \lim_{i \geq 0} A[\ell^i],$$

$$A[\ell^\infty] := \operatorname{colim}_{i \geq 0} A[\ell^i], \qquad A \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell := \operatorname{colim}_{i \geq 0} A/\ell^i A.$$

These are the ℓ-adic completion, the ℓ-adic Tate module, extraction of ℓ-torsion, and tensorisation with $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. These four operations are related, as follows. Given a short exact sequence of commutative groups $0 \to A \to B \to C \to 0$, there is a long exact sequence of $\mathbb{Z}_\ell$-modules

$$0 \to \mathrm{T}_\ell A \to \mathrm{T}_\ell B \to \mathrm{T}_\ell C \to A \widehat{\otimes} \mathbb{Z}_\ell \to B \widehat{\otimes} \mathbb{Z}_\ell \to C \widehat{\otimes} \mathbb{Z}_\ell \to 0$$

coming from the snake lemma, identifying $- \widehat{\otimes} \mathbb{Z}_\ell$ with the first right derived functor of the Tate module functor $\mathrm{T}_\ell(-)$ and vice versa. Similarly, there is a six-term exact sequence of ℓ-torsion groups

$$0 \to A[\ell^\infty] \to B[\ell^\infty] \to C[\ell^\infty] \to A \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to B \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to C \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to 0$$

identifying $(-)[\ell^\infty]$ with the first left derived functor of $- \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$ and vice versa. Given a bilinear pairing of commutative groups $A \times B \to \mathbb{Q}/\mathbb{Z}$, these operations induce pairings

$$A \widehat{\otimes} \mathbb{Z}_\ell \times B[\ell^\infty] \to \mathbb{Q}/\mathbb{Z} \quad \text{and} \quad \mathrm{T}_\ell A \times (B \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell) \to \mathbb{Q}/\mathbb{Z}.$$

If the original pairing was nondegenerate, these are nondegenerate pairings as well. Most of the time, we shall deal with commutative groups on which the multiplication-by-ℓ has finite kernel and cokernel. For such a group A, the $\mathbb{Z}_\ell$-modules $A \widehat{\otimes} \mathbb{Z}_\ell$

and $T_\ell A$ are finitely generated, and the torsion groups $A \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$ and $A[\ell^\infty]$ are of cofinite type (meaning that their Pontryagin duals are finitely generated as $\mathbb{Z}_\ell$-modules), and there is an isomorphism of finite groups $(A \widehat{\otimes} \mathbb{Z}_\ell)[\ell^\infty] \cong A[\ell^\infty] \widehat{\otimes} \mathbb{Z}_\ell$. Nondegenerate pairings of such groups induce perfect pairings of topological groups.

Proposition 1.9. *Let* $F : \mathscr{D}\mathscr{F}_S \to \mathscr{D}\mathscr{A}b$ *be a triangulated functor, and let* M *be a 1-motive over* S. *There are canonical short exact sequences of* $\mathbb{Z}_\ell$-*modules*

$$0 \to H^{i-1}F(M) \widehat{\otimes} \mathbb{Z}_\ell \to H^i F(T_\ell M) \to T_\ell H^i F(M) \to 0$$

and short exact sequences of ℓ-*torsion groups*

$$0 \to H^{i-1}F(M) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to H^i F(B_\ell M) \to H^i F(M)[\ell^\infty] \to 0$$

both natural in M *and* F.

Proof. The short exact sequence of constant sheaves $0 \to \mathbb{Z} \xrightarrow{\ell^i} \mathbb{Z} \to \mathbb{Z}/\ell^i\mathbb{Z} \to 0$ induces a long exact sequence of groups, from where we can cut out the short exact sequences

$$0 \to H^i F(M) \otimes \mathbb{Z}/\ell^i\mathbb{Z} \to H^i F(M \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}) \to H^{i+1}F(M)[\ell^i] \to 0.$$

The limit system of commutative groups $(H^i F(M) \otimes \mathbb{Z}/\ell^i\mathbb{Z})_{i=0}^\infty$ has the Mittag–Leffler property, and the short exact sequences in the proposition are then obtained by taking limits or colimits, respectively, over $i \geq 0$. $\square$

Corollary 1.10. *Let* k *be a number field, let* ℓ *be a prime number, and let* $M = [u : Y \to G]$ *be a 1-motive over* k. *Set* $Z := H^{-1}(M) = \ker u$. *The morphism of* $\mathbb{Z}_\ell$-*modules*

$$H^i(k, Z \otimes \mathbb{Z}_\ell) \to H^i(k, T_\ell M)$$

induced by the morphism of 1-motives $[Z \to 0] \to [Y \to G]$ *is an isomorphism for* $i = 0$ *and injective for* $i = 1$.

Proof. Proposition 1.9 applied to the functor $R\Gamma(k, -)$ yields a short exact sequence of $\mathbb{Z}_\ell$-modules

$$0 \to H^{-1}(k, M) \widehat{\otimes} \mathbb{Z}_\ell \to H^0(k, T_\ell M) \to T_\ell H^0(k, M) \to 0.$$

Since $Z(k) = H^{-1}(k, M)$ is a finitely generated group, we can identify $Z(k) \widehat{\otimes} \mathbb{Z}_\ell$ with $Z(k) \otimes_\mathbb{Z} \mathbb{Z}_\ell$, so to get the statement for $i = 0$, it remains to show that the last group in this sequence vanishes. Write $\mathbb{O}_k$ for the ring of integers of k, and choose a sufficiently small open subscheme $U \subseteq \operatorname{spec} \mathbb{O}_k$ such that M extends to a 1-motive over U and such that ℓ is invertible on U. We have then $Z(U) = Z(k)$ and $H^0(U, T_\ell M) = H^0(k, T_\ell M)$, so we may as well show that $T_\ell H^0(U, M)$ vanishes. Indeed, it follows by dévissage from the Mordell–Weil theorem, Dirichlet's unit theorem, and finiteness of $H^1(U, Y)$ that $H^0(U, M)$ is a finitely generated group

[Harari and Szamuely 2005, Lemma 3.2], so its Tate module is trivial. For the case $i = 1$, we consider the triangle

$$[Z \to 0] \to [Y \to G] \to [Y/Z \to G]$$

and observe that if we quotient both terms of the complex $[Y/Z \to G]$ by the finite torsion part of Y/Z, we get a quasi-isomorphic complex, which is the complex of a 1-motive $M' = [u' : Y' \to G']$ where now u' is injective. By the first part, we have $H^0(k, \mathrm{T}_\ell M') = 0$, and the statement can be read in the long exact cohomology sequence associated with $0 \to Z \otimes \mathbb{Z}_\ell \to \mathrm{T}_\ell M \to \mathrm{T}_\ell M' \to 0$. $\qquad\square$

The statement of Corollary 1.10 remains true over any field k that is finitely generated over its prime field and prime number ℓ different from the characteristic of k. It is wrong in general for local fields.

We now come to the dual 1-motive: with each 1-motive M over a noetherian regular scheme S is functorially associated a dual 1-motive $M^\vee$ over S so that we get an involution of the category $\mathcal{M}_{1,S}$ of 1-motives over S. The duals of tori, lattices, and abelian schemes, if seen as 1-motives, are the usual duals, and the duality functor is compatible with the weight filtration. This is the content of the following theorem:

Theorem 1.11. *There exists an antiequivalence of categories* $(-)^\vee : \mathcal{M}_{1,S} \to \mathcal{M}_{1,S}$ *such that for every* 1*-motive M over S the following hold*:

(1) *There are canonical and natural isomorphisms of* 1*-motives*

$$(M/W_{-i}(M))^\vee \cong W_{i-3}(M^\vee)$$

   for each i.

(2) *There is a natural isomorphism*

$$[M^\vee] \cong \mathrm{R}\,\mathcal{H}om(M, \mathbb{G}_m[1])_{\leq 0}$$

   in the derived category $\mathcal{DF}_S$, where $(-)_{\leq 0}$ means truncation in degree 0.

(3) *There is a natural isomorphism of* 1*-motives $\epsilon_M : M \to M^{\vee\vee}$ such that the induced morphism of complexes coincides with the canonical evaluation morphism in the derived category of $\mathcal{F}_S$ (explained below).*

Properties (1), (2), *and* (3) *characterise* $(-)^\vee$ *up to an isomorphism of functors.*

For every object X of $\mathcal{DF}_S$, we have a natural morphism $X \to \mathrm{R}\,\mathcal{H}om(\mathrm{R}\,\mathcal{H}om(X, \mathbb{G}_m[1]), \mathbb{G}_m[1])$ (see [SGA 5, Exposé 1] after Proposition 1.6) as well as $X \to X_{\leq 0}$. Together, these yield the natural morphism

$$X_{\leq 0} \to \mathrm{R}\,\mathcal{H}om(\mathrm{R}\,\mathcal{H}om(X, \mathbb{G}_m[1])_{\leq 0}, \mathbb{G}_m[1])_{\leq 0},$$

which is the one we consider for $X = X_{\leq 0} = [M]$ in part (3) of the theorem.

1.12. The uniqueness of the functor $(-)^\vee$ can be shown by a simple dévissage argument. Its existence is in essence the construction of the dual 1-motive of [Deligne 1974, §10.2.11] combined with the following observations (1) and (2):

(1) If X is either a finite flat group scheme, a torus, or a lattice over S, then the sheaf $\mathscr{H}om(X, \mathbb{G}_m)$ is represented by the Cartier dual of X, and $\mathscr{E}xt^1(X, \mathbb{G}_m) = 0$.

(2) If A is an abelian scheme over S, the sheaves $\mathscr{H}om(A, \mathbb{G}_m)$ and $\mathscr{E}xt^2(A, \mathbb{G}_m)$ are trivial, and $\mathscr{E}xt^1(A, \mathbb{G}_m)$ is represented by the dual abelian scheme $A^\vee$.

(3) For all $i \geq 2$, the sheaves $\mathscr{E}xt^i(X, \mathbb{G}_m)$ and $\mathscr{E}xt^i(A, \mathbb{G}_m)$ are torsion. If ℓ is invertible on S, these sheaves contain no ℓ-torsion.

In the case X is a finite flat group scheme, the statements of (1) can be found in [Oort 1966, Theorem III.16.1]. For locally constant group schemes and tori, these follow from [SGA 3 II, Exposé XIII, Corollaire 1.4] and [SGA 7 I, Exposé VIII, Proposition 3.3.1], respectively. In (2), we have $\mathscr{H}om(A, \mathbb{G}_m) = 0$ because A is proper and geometrically connected, and $\mathbb{G}_m$ is affine. The isomorphism $\mathscr{E}xt^1(A, \mathbb{G}_m) \cong A^\vee$ is given by the classical Barsotti–Weil formula [Oort 1966, Theorem III.18.1].[1] It is shown in [Breen 1969a] that (over a noetherian regular base scheme as we suppose S to be) the sheaves $\mathscr{E}xt^i(A, \mathbb{G}_m)$ are torsion for all $i > 1$. Using the second statement of (1), we see that for $n \neq 0$ the multiplication-by-n map on $\mathscr{E}xt^2(A, \mathbb{G}_m)$ is injective; hence, $\mathscr{E}xt^2(A, \mathbb{G}_m) = 0$. Finally, the torsion sheaves $\mathscr{E}xt^i(X, \mathbb{G}_m)$ and $\mathscr{E}xt^i(A, \mathbb{G}_m)$ contain no ℓ-torsion because if F is a finite flat group scheme over S annihilated by ℓ, then $\mathscr{E}xt^i(F, \mathbb{G}_m) = 0$ for all $i \geq 1$. Indeed, such a group scheme is locally constant and locally presented as $0 \to \mathbb{Z}^r \to \mathbb{Z}^r \to F \to 0$, and the functor $\mathscr{H}om(\mathbb{Z}^r, -)$ is exact.

The reason why we need the truncation operations in Theorem 1.11(1) is that in general we do not know whether the sheaves $\mathscr{E}xt^i(F, \mathbb{G}_m)$ vanish for $i > 1$ if F is a finite flat group scheme over S that is not locally constant. This is presumably not the case, as an explicit example of Breen [1969b] suggests (he works with sheaves for the étale topology, but it seems that his example also works in the fppf setting). Over a field of characteristic 0, or after inverting all residual characteristics of S, the truncation is not needed.

---

[1]The additional hypothesis that either A is projective over S or that S is artinian is superfluous. The trouble is caused only by Oort's Proposition I.5.3, where representability of the Picard functor $T \mapsto \operatorname{Pic} A/T$ is known just in these cases. This problem has been overcome by M. Raynaud [Faltings and Chai 1990, Theorem 1.9].

Oort proves that the Barsotti–Weil formula over a general scheme holds if it holds over all of its residue fields. He then says that the formula is known to hold over any field and quotes Serre's *Groupes algébriques et corps de classes*, VII.16, Théorème 6. But Serre makes right at the beginning of Chapter VII the hypothesis that the ground field is algebraically closed. Hence, as long as all residue fields of S are perfect, Oort's proof is fine. The general case follows by checking that Serre's arguments also work verbatim over separably closed fields.

Proposition 1.13. *Let M be a 1-motive over S with dual $M^\vee$, and let $n \geq 1$ be an integer that is invertible on S. The Cartier dual of the finite flat group scheme $H^1([M] \otimes^{\mathbb{L}} \mathbb{Z}/n\mathbb{Z})$ is naturally isomorphic to $H^1([M^\vee] \otimes^{\mathbb{L}} \mathbb{Z}/n\mathbb{Z})$. In particular, there is a canonical, natural isomorphism $\mathrm{T}_\ell(M^\vee) \cong \mathscr{H}om(\mathrm{T}_\ell M, \mathbb{Z}_\ell(1))$ of ℓ-adic sheaves on S for every prime number ℓ invertible on S.*

Proof. This follows from Theorem 1.11 and the statement (3) of Section 1.12. □

2. The pairing between $\mathrm{III}^0(k, M)$ and $\mathrm{III}^2(k, M^\vee)$

We fix number field k with algebraic closure $\bar{k}$ and write Ω for the set of all places of k. For $v \in \Omega$, we denote by k_v the completion of k at v. After recalling the definition of Tate–Shafarevich groups, we use the Poitou–Tate duality theorem for finite Galois modules to identify the ℓ-torsion part of $\mathrm{III}^2(k, M^\vee)$ with the dual of $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ for any 1-motive $M = [Y \to G]$ over k. Then we show that the group $\mathrm{III}^0(k, M)$ is finite and that its ℓ-part canonically injects into $\mathrm{III}^1(k, \mathrm{T}_\ell M)$.

2.1. Let C be a bounded complex of continuous $\mathrm{Gal}(\bar{k}|k)$-modules. The Tate–Shafarevich groups $\mathrm{III}^i(k, C)$ of C are defined by

$$\mathrm{III}^i(k, C) := \ker\left(H^i(k, C) \to \prod_{v \in \Omega} H^i(k_v, C) \right),$$

where H^i is continuous cochain cohomology with the convention that for archimedean v the group $H^i(k_v, C) = H^i(\mathrm{Gal}(\mathbb{C}|k_v), C)$ stands for Tate modified cohomology [Neukirch et al. 2000, I§2]. The Tate–Shafarevich groups $\mathrm{III}^i(k, M)$ of a 1-motive $M = [Y \to G]$ over k are those of the complex of discrete Galois modules $Y(\bar{k}) \to G(\bar{k})$ placed in degrees -1 and 0.

Proposition 2.2. *Let M be a 1-motive over k, and let ℓ be a prime number. There is a canonical, perfect pairing of topological groups*

$$\mathrm{III}^1(k, \mathrm{T}_\ell M) \times \mathrm{III}^2(k, M^\vee)[\ell^\infty] \to \mathbb{Q}/\mathbb{Z}$$

where $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ is profinite and $\mathrm{III}^2(k, M^\vee)[\ell^\infty]$ is discrete. In particular, $\mathrm{III}^2(k, M^\vee)[\ell^\infty]$ is finite or zero if and only if $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ is so.

Proof. By Poitou–Tate duality for finite Galois modules [Neukirch et al. 2000, Theorem 8.6.8], we have a natural, perfect duality between finite groups

$$\mathrm{III}^1(k, M \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i \mathbb{Z}) \times \mathrm{III}^2(k, M^\vee \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i \mathbb{Z}) \to \mathbb{Q}/\mathbb{Z},$$

noting Proposition 1.13. The functor $\mathrm{III}^2(k, -)$ commutes with arbitrary colimits, and $\mathrm{III}^1(k, -)$ commutes with limits of finite Galois modules by [Serre 1964,

Proposition 7]. We obtain thus, without violating the notational conventions from Section 1.6, a perfect pairing of topological groups

$$\text{III}^1(k, \text{T}_\ell M) \times \text{III}^2(k, \text{B}_\ell M^\vee) \to \mathbb{Q}/\mathbb{Z},$$

and it remains to show that $\text{III}^2(k, \text{B}_\ell M^\vee)$ is canonically isomorphic to the ℓ-part of the torsion group $\text{III}^2(k, M^\vee)$. Indeed, from Proposition 1.9 we get the following commutative diagram of torsion groups with exact rows:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(k, M^\vee) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell & \longrightarrow & H^2(k, \text{B}_\ell M^\vee) & \longrightarrow & H^2(k, M^\vee)[\ell^\infty] & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \displaystyle\prod_{v \in \Omega} H^1(k_v, M^\vee) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell & \to & \displaystyle\prod_{v \in \Omega} H^2(k_v, \text{B}_\ell M^\vee) & \to & \displaystyle\prod_{v \in \Omega} H^2(k_v, M^\vee)[\ell^\infty] & \to & 0
\end{array}
$$

Because $H^1(k, M^\vee)$ and $H^1(k_v, M^\vee)$ are torsion, the first terms of both rows are zero; hence, the canonical isomorphism $\text{III}^2(k, \text{B}_\ell M^\vee) \cong \text{III}^2(k, M^\vee)[\ell^\infty]$, as required. $\square$

2.3. Let M be a 1-motive over k, and let ℓ be a prime number. From Proposition 1.9, we get a commutative diagram of $\mathbb{Z}_\ell$-modules with exact rows:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(k, M) \widehat{\otimes} \mathbb{Z}_\ell & \longrightarrow & H^1(k, \text{T}_\ell M) & \longrightarrow & \text{T}_\ell H^1(k, M) & \longrightarrow & 0 \\
& & {\scriptstyle \alpha_\ell}\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \displaystyle\prod_{v \in \Omega} H^0(k_v, M) \widehat{\otimes} \mathbb{Z}_\ell & \longrightarrow & \displaystyle\prod_{v \in \Omega} H^1(k_v, \text{T}_\ell M) & \longrightarrow & \displaystyle\prod_{v \in \Omega} \text{T}_\ell H^1(k_v, M) & \longrightarrow & 0
\end{array}
$$

The kernel of the rightmost vertical map is the Tate module of $\text{III}^1(k, M)$, which is torsion free, and even trivial if $\text{III}^1(k, M)$ is finite (which conjecturally is always the case; compare [Harari and Szamuely 2005, Corollary 4.9]). In any case, the map $\ker \alpha_\ell \to \text{III}^1(k, \text{T}_\ell M)$ is an isomorphism on torsion elements. The kernel of α_ℓ contains $\text{III}^0(k, M) \otimes \mathbb{Z}_\ell$ and hence an injection

$$\text{III}^0(k, M) \otimes \mathbb{Z}_\ell \to \text{III}^1(k, \text{T}_\ell M). \tag{$\dagger$}$$

In [Harari and Szamuely 2005, Section 5], a profinite group $\text{III}^0_\wedge(k, M)$ was introduced. Its pro-ℓ part is $\ker \alpha_\ell$ and hence equal to $\text{III}^1(k, \text{T}_\ell M)$ in the case $\text{III}^1(k, A)$ is finite. This relates Proposition 5.1 of [loc. cit.] to our Proposition 2.2. There is a canonical isomorphism $\text{III}^0(k, M) \otimes \mathbb{Z}_\ell \cong \text{III}^0(k, M)[\ell^\infty]$ because $\text{III}^0(k, M)$ is finite as we shall see in Proposition 2.5. These observations yield the following corollary to Proposition 2.2:

Corollary 2.4. *The pairing of Proposition 2.2 induces a pairing*

$$\text{III}^0(k, M)[\ell^\infty] \times \text{III}^2(k, M^\vee)[\ell^\infty] \to \mathbb{Q}/\mathbb{Z},$$

which is nondegenerate on the left. Its right kernel is divisible if and only if the map (†) *induces an isomorphism* $\text{III}^0(k, M) \otimes \mathbb{Z}_\ell \to \text{III}^1(k, T_\ell M)_{\text{tor}}$, *and this pairing is a perfect pairing of finite groups if and only if the map* (†) *is an isomorphism.*

We end the section with the following proposition, which explains the group $\text{III}^0(k, M)$ and shows that it is finite [Harari and Szamuely 2005, Lemma 4.11]:

Proposition 2.5. *Let $M = [u : Y \to G]$ be a 1-motive over k, and set $Z := \ker u$. The morphism of 1-motives $[Z \to 0] \to [Y \to G]$ induces an isomorphism of finite groups*

$$\text{III}^1(k, Z) \xrightarrow{\cong} \text{III}^0(k, M).$$

For any prime number ℓ, there are canonical isomorphisms of finite groups

$$\text{III}^1(k, Z)[\ell^\infty] \cong \text{III}^1(k, Z) \otimes \mathbb{Z}_\ell \cong \text{III}^1(k, Z \otimes \mathbb{Z}_\ell) \cong \text{III}^1(k, T_\ell[Z \to 0]).$$

All these groups are annihilated by the order of any finite Galois extension $k' | k$ over which Z is constant.

Proof. By diagram chase, using one finite place $v \in \Omega$, we see that the map $\text{III}^0(k, M) \to \text{III}^1(k, Y)$ is injective. It follows in particular that $\text{III}^0(k, M)$ is zero if the Galois action on Y is trivial. In general, let $k' | k$ be a finite Galois extension such that $\text{Gal}(\bar{k} | k')$ acts trivially on Y, and let Ω' be the set of places of k'. For $w \in \Omega'$ lying over $v \in \Omega$, we write k'_w for the completion of k' at w and k_w for the completion of k at v. As a Galois module, $Z := \ker(u)$ can be interpreted as $Z = H^{-1}(k', M)$. From the Hochschild–Serre spectral sequence, we get then a commutative diagram with exact rows:

$$
\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\text{Gal}(k'|k), Z) & \longrightarrow & H^0(k, M) & \longrightarrow & H^0(k', M) \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_{w \in \Omega'} H^1(\text{Gal}(k'_w | k_w), Z) & \longrightarrow & \prod_{w \in \Omega'} H^0(k_w, M) & \longrightarrow & \prod_{w \in \Omega'} H^0(k'_w, M)
\end{array}
$$

Because $\text{Gal}(\bar{k} | k')$ acts trivially on Y, we have $\text{III}^0(k', M) = 0$ by our previous observation; hence,

$$\text{III}^0(k, M) \cong \ker\left(H^1(\text{Gal}(k'|k), Z) \to \prod_{w \in \Omega'} H^1(\text{Gal}(k'_w | k_w), Z) \right),$$

the product running over all $w \in \Omega'$ or alternatively over all decomposition subgroups of $\text{Gal}(k'|k)$. The finiteness statement follows as $H^1(\text{Gal}(k'|k), Z)$ is finite and

annihilated by the order of $\text{Gal}(k'|k)$ [Weibel 1994, Theorem 6.5.8 and Corollary 6.5.10]. Repeating the arguments for the 1-motive $[Z \to 0]$ yields the first isomorphism of the proposition.

Now let ℓ be a prime number. The first isomorphism from the left exists for any finite commutative group in place of $\text{III}^1(k, Z)$. For the next one, choose a finite Galois extension $k'|k$ such that Z is constant over k'. We can proceed as before in order to express $\text{III}^1(k, Z)$ and $\text{III}^1(k, Z \otimes \mathbb{Z}_\ell)$ in terms of cohomology groups of the finite group $\text{Gal}(k'|k)$ and its subgroups. It remains to show that, given a finite group Γ acting on Z, the canonical map $H^1(\Gamma, Z) \otimes \mathbb{Z}_\ell \to H^1(\Gamma, Z \otimes \mathbb{Z}_\ell)$ is an isomorphism. This is indeed so for any flat $\mathbb{Z}$-algebra in place of $\mathbb{Z}_\ell$ by the universal coefficient theorem. The last isomorphism holds because $Z \otimes \mathbb{Z}_\ell \cong \lim Z/\ell^i Z$ and because limits are left exact and commute with continuous H^1. $\qquad\square$

3. Lie algebra cohomology of the Tate module

We fix a number field k with algebraic closure $\bar{k}$ and a prime number ℓ. With every 1-motive M over k is associated a continuous $\mathbb{Q}_\ell$-linear representation $V_\ell M = T_\ell M \otimes \mathbb{Q}_\ell$ of $\text{Gal}(\bar{k}|k)$. The image of $\text{Gal}(\bar{k}|k)$ in $\text{GL}(V_\ell M)$ is an ℓ-adic Lie group L^M, whose Lie algebra we denote by $\mathfrak{l}^M$. An idea going back to Serre and Tate, used by Serre [1964] to solve the congruence subgroup problem for abelian varieties over number fields, is to consider the vector space $H^1_*(\mathfrak{l}^M, V_\ell M)$ consisting of those elements of $H^1(\mathfrak{l}^M, V_\ell M)$ that restrict to zero on each one-dimensional subalgebra of $\mathfrak{l}^M$. Our goal is to describe $H^1_*(\mathfrak{l}^M, V_\ell M)$.

We will work only with 1-motives $M = [Y \to G]$ where G is either an abelian variety or a torus rather than a general semiabelian variety. This brings considerable simplifications in both statements and proofs. I will comment at the end of Section 3.11 on this hypothesis and on the modifications that are necessary in order to compute $H^1_*(\mathfrak{l}^M, V_\ell M)$ for general 1-motives. The following theorem is the crucial ingredient for our finiteness results:

Theorem 3.1. *Let $M = [u := Y \to G]$ be a 1-motive over k where G is an abelian variety or a torus. Set $E_\ell := \text{End}_{\bar{k}}(G) \otimes \mathbb{Q}_\ell$ and $X_\ell := \text{im}(u) \otimes \mathbb{Q}_\ell$, denote by D_ℓ the E_ℓ-submodule of $G(\bar{k}) \otimes \mathbb{Q}_\ell$ generated by X_ℓ, and define*

$$\overline{X}_\ell := \{x \in D_\ell \mid f(x) \in f(X_\ell) \text{ for all } f \in \text{Hom}_{E_\ell}(D_\ell, V_\ell G)\}.$$

There is a canonical isomorphism of $\mathbb{Q}_\ell$-vector spaces $\overline{X}_\ell/X_\ell \cong H^1_*(\mathfrak{l}^M, V_\ell M)$.

The proof of this theorem relies on a structure result for the Lie algebra $\mathfrak{l}^M$, which in turn relies on Faltings's theorems on endomorphisms of abelian varieties over number fields. Observe that the object $\overline{X}_\ell/X_\ell$ can be calculated by means of ordinary linear algebra. The statement of the theorem is wrong for general semiabelian varieties G.

3.2. We recall some definitions and results from [Serre 1964]. Let L be a profinite group, and let T be a continuous L-module. We write $H^1(L, T)$ for the group of continuous cocycles $L \to T$ modulo coboundaries and define

$$H^1_*(L, T) := \ker\Big(H^1(L, T) \to \prod_{x \in L} H^1(\langle x \rangle, T) \Big),$$

where $\langle x \rangle$ denotes the closed subgroup of L generated by x. If N is a closed normal subgroup of L acting trivially on T, then the inflation map induces an isomorphism $H^1_*(L/N, T) \to H^1_*(L, T)$ [loc. cit., Proposition 6]. If T is a profinite L-module, say $T = \lim T_i$ where the T_i are finite discrete L-modules, then the canonical map $H^1(L, T) \to \lim H^1(L, T_i)$ is an isomorphism [loc. cit., Proposition 7]. Because the limit functor is left exact, also the canonical map $H^1_*(L, T) \to \lim H^1_*(L, T_i)$ is an isomorphism in that case.

For a Lie algebra $\mathfrak{l}$ acting on a vector space V, we denote by $H^1_*(\mathfrak{l}, V)$ the subspace of $H^1(\mathfrak{l}, V)$ consisting of those elements that restrict to zero in $H^1(\langle x \rangle, V)$ for every one-dimensional subalgebra $\langle x \rangle$ of $\mathfrak{l}$.

Lemma 3.3. *Let L be a compact ℓ-adic Lie group with Lie algebra $\mathfrak{l}$ acting on a finite-dimensional $\mathbb{Q}_\ell$-vector space V. For any open subgroup N of L, we have*

$$H^1_*(L, V) = \ker\Big(H^1(L, V) \to \prod_{x \in N} H^1(\langle x \rangle, V) \Big).$$

If N is normal, there is a canonical isomorphism $H^1_*(L, V) \cong H^1_*(N, V)^{L/N}$. If N is sufficiently small, there is a canonical isomorphism $H^1_*(N, V) \cong H^1_*(\mathfrak{l}, V)$.

Proof. Let N be an open subgroup of L, and let c be an element of $H^1(L, V)$ restricting to zero in $H^1(\langle x \rangle, V)$ for each $x \in N$. Fix an element $x \in L$, and let us show that c restricts to zero in $H^1(\langle x \rangle, V)$. Because $\langle x \rangle$ is compact, the quotient $\langle x \rangle / (N \cap \langle x \rangle)$ is finite. By a restriction-corestriction argument and using that V is uniquely divisible, we see that the restriction map $H^1(\langle x \rangle, V) \to H^1(\langle x \rangle \cap N, V)$ is injective, hence the first claim. Now suppose that N is open and normal. Since L is compact, the quotient L/N is finite and we have $H^i(L/N, V) = 0$ for all $i > 0$, and the Hochschild–Serre spectral sequence yields an isomorphism $H^1(L, V) \cong H^1(N, V)^{L/N}$. We must show that in the diagram

$$
\begin{array}{ccccccc}
0 & \longrightarrow & H^1_*(L, V) & \longrightarrow & H^1(L, V) & \longrightarrow & \prod\limits_{x \in L} H^1(\langle x \rangle, V) \\
& & \downarrow & & {\scriptstyle \cong}\big\downarrow \ \ \ {\scriptstyle \delta} & & \downarrow \\
0 & \longrightarrow & H^1_*(N, V)^{L/N} & \longrightarrow & H^1(N, V)^{L/N} & \longrightarrow & \prod\limits_{x \in N} H^1(\langle x \rangle, V)
\end{array}
$$

the leftmost vertical map is an isomorphism, i.e., that the kernel of the diagonal map δ is exactly $H^1_*(L, V)$. But this is again the first statement of the lemma. Finally, if N is sufficiently small, we have an isomorphism $H^1(N, V) \cong H^1(\mathfrak{l}, V)$ by a well-known theorem of Lazard [1965, V.2.4.10], from which the last statement follows. $\qquad\square$

3.4. Let $M = [u : Y \to G]$ be a 1-motive over k where G is an abelian variety or a torus. The Tate module $\mathrm{T}_\ell M$ of M is an extension of $Y \otimes \mathbb{Z}_\ell$ by the Tate module $\mathrm{T}_\ell G$ of G as we have seen in Section 1.7, so we get an extension continuous of Galois representations

$$0 \to \mathrm{V}_\ell G \to \mathrm{V}_\ell M \to Y \otimes \mathbb{Q}_\ell \to 0.$$

We denote by $\mathfrak{l}^M$ and $\mathfrak{l}^G$ the Lie algebras of the image of $\Gamma := \mathrm{Gal}(\bar{k} \,|\, k)$ in the groups $\mathrm{GL}(\mathrm{V}_\ell M)$ and $\mathrm{GL}(\mathrm{V}_\ell G)$, respectively. The Galois group Γ acts continuously on these Lie algebras by conjugation, and we have a canonical surjection $\mathfrak{l}^M \to \mathfrak{l}^G$. Let $\mathfrak{n}^M$ denote its kernel, so $\mathfrak{n}^M$ consists of those elements of $\mathfrak{l}^M$ that act trivially on $\mathrm{V}_\ell G$. The Lie algebra $\mathfrak{n}^M$ is commutative, and we can identify it with a linear subspace of $\mathrm{Hom}(Y \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G)$ via the map

$$\vartheta : \mathfrak{n}^M \to \mathrm{Hom}_{\mathbb{Q}_\ell}(Y \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G)$$

given by $\vartheta(x)(y) = x.v$ where $v \in \mathrm{V}_\ell M$ is any element mapping to $y \in Y \otimes \mathbb{Q}_\ell$. Routine checking shows that this map is well-defined, injective, and Γ-equivariant. We can describe the image of ϑ as follows. Look at u as being a k-rational point on the abelian variety or torus $\mathcal{H}om(Y, G)$, and denote by B the connected component of the smallest algebraic subgroup of $\mathcal{H}om(Y, G)$ containing u. Then B is also an abelian variety or a torus, and we have an inclusion

$$\mathrm{V}_\ell B \subseteq \mathrm{V}_\ell \, \mathcal{H}om(Y, G) \cong \mathrm{Hom}_{\mathbb{Q}_\ell}(Y \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G).$$

The following theorem is a special case of [Jossen 2013b, Theorem 6.2]. In the case G is an abelian variety, it goes back to a result of Ribet [1976] (see [Hindry 1988, Appendix 2]).

Theorem 3.5. *The map ϑ induces an isomorphism of Galois representations* $\vartheta : \mathfrak{n}^M \overset{\cong}{\Longrightarrow} \mathrm{V}_\ell B$.

In particular, it follows that the dimension of $\mathfrak{n}^M$ is independent of ℓ. If G is an abelian variety, it is still unknown whether the dimension of $\mathfrak{l}^G$ is independent of ℓ.

Lemma 3.6. *Let $M = [u : Y \to G]$ be a 1-motive over k where G is an abelian variety or a torus. Denote by D the $\mathrm{End}_{\bar{k}}(G)$ submodule of $G(\bar{k})$ generated by* $\mathrm{im}(u)$, *and define $B \subseteq \mathcal{H}om(Y, G)$ as in Section 3.4. The linear map*

$$h : \mathrm{Hom}_{\bar{k}}(B, G) \otimes \mathbb{Q} \to G(\bar{k}) \otimes \mathbb{Q}$$

given by $h(\psi \otimes 1) = \psi(nu) \otimes n^{-1}$, *where* $n \geq 1$ *is any integer such that* $nu \in B(k)$, *induces an isomorphism* $\mathrm{Hom}_{\bar{k}}(B, G) \otimes \mathbb{Q} \cong D \otimes \mathbb{Q}$.

Proof. The homomorphism h is injective. Indeed, if $\psi : B \to G$ is such that $h(\psi) = 0$, then $\ker \psi$ is a subgroup of B containing a nonzero multiple of u; hence, $\ker \psi = B$ by minimality of B. By Poincaré's complete reducibility theorem [Mumford 1970, IV.19, Theorem 1], the inclusion $B \subseteq \mathscr{H}om(Y, G)$ induces a surjection

$$Y \otimes \mathrm{End}_{\bar{k}}(G) \cong \mathrm{Hom}_{\bar{k}}(\mathscr{H}om(Y, G), G) \xrightarrow{\mathrm{res}} \mathrm{Hom}_{\bar{k}}(B, G)$$

sending $y \otimes \varphi$ to the unique homomorphism $\psi : B \to G$ with $\psi(nu) = n\varphi(u(y))$ where $n \geq 1$ is sufficiently big that $nu \in B(k)$, so the remaining statements follow. $\square$

Lemma 3.7. *Let the* 1-*motive* $M = [Y \to G]$, *the subgroup* $D \subseteq G(\bar{k})$, *and the algebraic subgroup* $B \subseteq G$ *be as in Lemma 3.6. There is a commutative diagram*

$$
\begin{array}{ccccc}
Y \otimes \mathbb{Q}_\ell & \xrightarrow{u \otimes \mathrm{id}} & D \otimes \mathbb{Q}_\ell & \xrightarrow[\cong]{(1)} & \mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell B, \mathrm{V}_\ell G) \\
\Big\downarrow{\cong} & & {(2)}\Big\downarrow{\cong} & & {\cong}\Big\downarrow{\vartheta^*} \\
H^0(\mathfrak{l}^M, Y \otimes \mathbb{Q}_\ell) & \xrightarrow{\partial} & H^1(\mathfrak{l}^M, \mathrm{V}_\ell G) & \xrightarrow[\cong]{\mathrm{res}} & \mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{n}^M, \mathrm{V}_\ell G)
\end{array}
$$

with canonical isomorphisms where indicated.

Proof. We start with the left-hand square. The leftmost vertical isomorphism is tautological because $\mathfrak{l}^M$ acts trivially on $Y \otimes \mathbb{Q}_\ell$. The map ∂ is the connecting morphism in the long exact cohomology sequence coming from the weight filtration of M. The vector spaces $D \otimes \mathbb{Q}_\ell$ and $H^1(\mathfrak{l}^M, \mathrm{V}_\ell G)$ are naturally E_ℓ-modules, where $E_\ell := \mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}_\ell$ — the first one by definition and the second one via the canonical action of E_ℓ on $\mathrm{V}_\ell G$. The map (2) is then given by E_ℓ-linearity and sending $u(y) \otimes 1$ to $\partial(y \otimes 1)$ for all $y \in Y$. By definition of D, this indeed describes a unique map such that the left-hand square commutes. We will see in a moment that it is well-defined and an isomorphism.

We now come to the right-hand square, starting with the description of the map (1). Every element of $D \otimes \mathbb{Q}_\ell$ is a linear combination of elements of the form $\psi(u) \otimes 1$ for some $\psi \in \mathrm{Hom}_{\bar{k}}(B, G)$ by Lemma 3.6. The map (1) is given by linearity and sends $\psi(u) \otimes 1$ to the $\mathfrak{l}^G$-equivariant map $\mathrm{V}_\ell \psi : \mathrm{V}_\ell B \to \mathrm{V}_\ell G$. This map is an isomorphism by Lemma 3.6 and by Faltings's theorem on homomorphisms of abelian varieties. The rightmost vertical map is given by precomposition with the isomorphism ϑ, hence an isomorphism. The lower horizontal map is given by restriction of cocycles and an isomorphism because $H^i(\mathfrak{l}^G, \mathrm{V}_\ell G)$ vanishes for $i = 1, 2$ [Serre 1971, Théorème 2].

By definition of ϑ, the big square commutes. Moreover, the isomorphisms (1) and ϑ^* and the inverse of res are all isomorphisms of E_ℓ-modules. Hence, so is their

composition, which is then an isomorphism of E_ℓ-modules $D \otimes \mathbb{Q}_\ell \to H^1(\mathfrak{l}^M, V_\ell G)$, which must coincide with (2). $\qquad\square$

Proposition 3.8 [Jossen 2013a, Corollary 2.19]. *The Lie algebra extension*

$$0 \to \mathfrak{n}^M \to \mathfrak{l}^M \to \mathfrak{l}^G \to 0$$

is split. There exist a Lie algebra section $\sigma : \mathfrak{l}^G \to \mathfrak{l}^M$ *and a* $\mathbb{Q}_\ell$*-linear section* $s : Y \otimes \mathbb{Q} \to V_\ell M$ *such that the action of* $\mathfrak{l}^M$ *on* $V_\ell M$ *is given by*

$$(f + \sigma(g)).(v + s(y)) = g.v + f.y$$

for all $f \in \mathfrak{n}^M$, *all* $g \in \mathfrak{l}^G$, *all* $v \in V_\ell A$, *and* $y \in Y \otimes \mathbb{Q}_\ell$.

Proof. This is essentially a consequence of Theorem 3.5, semisimplicity of $V_\ell G$ as $\mathfrak{l}^G$-module (by the assumption on G and [Faltings 1983]), and the vanishing of $H^i(\mathfrak{l}^G, V_\ell G)$ for $i = 1, 2$ [Serre 1971, Théorème 2]. $\qquad\square$

Lemma 3.9. *Let* $M = [u := Y \to G]$ *be a 1-motive over* k *where* G *is an abelian variety or a torus. In order that an element* $h \in H^1(\mathfrak{l}^M, V_\ell G)$ *belongs to* $H^1_*(\mathfrak{l}^M, V_\ell M)$, *it suffices that it maps to zero in* $H^1(\mathfrak{c}, V_\ell M)$ *for each one-dimensional subalgebra* $\mathfrak{c}$ *of* $\mathfrak{n}^M$.

Proof. Represent $h \in H^1(\mathfrak{l}^M, V_\ell G)$ by a cocycle $c : \mathfrak{l}^M \to V_\ell G \subseteq V_\ell M$, and choose a linear section $s : Y \otimes \mathbb{Q}_\ell \to V_\ell M$ and a Lie algebra section $\sigma : \mathfrak{l}^G \to \mathfrak{l}^M$ as in Proposition 3.8. Since $H^1(\mathfrak{l}^G, V_\ell G)$ vanishes [Serre 1971, Théorème 2], the cocycle $c \circ \sigma$ is a coboundary. Thus, changing c by a coboundary, we may suppose that $c \circ \sigma = 0$. Let $\mathfrak{c}$ be a one-dimensional subalgebra of $\mathfrak{l}^M$ generated by an element $x \in \mathfrak{l}^M$. We have to show that there exists an element $v \in V_\ell M$ such that $c(x) = x.v$. We can write x as $x = f + \sigma(g)$ for some $f \in \mathfrak{n}^M$ and $g \in \mathfrak{l}^G$. By hypothesis, there exists an element $v \in V_\ell M$ with $c(f) = f.v$. We can write v as $v = v' + s(y)$ for some $v' \in V_\ell G$ and $y \in Y \otimes \mathbb{Q}_\ell$. We then have

$$c(x) = c(f + \sigma(g)) = c(f) = f.v = f.s(y) = (\sigma(g) + f).s(y) = x.s(y),$$

and this proves the lemma. $\qquad\square$

Lemma 3.10. *Let* $M = [u : Y \to G]$ *be a 1-motive over* k *where* G *is an abelian variety or a torus. Denote by* D *the* $E := \mathrm{End}_{\bar{k}}(G)$ *submodule of* $G(\bar{k})$ *generated by* $X := \mathrm{im}(u)$. *The isomorphism* $D \otimes \mathbb{Q}_\ell \to H^1(\mathfrak{l}^M, V_\ell G)$ *from Lemma 3.7 induces an isomorphism between the kernels of the maps*

$$D \otimes \mathbb{Q}_\ell \to \prod_{h \in H} V_\ell G / h(X \otimes \mathbb{Q}_\ell) \quad \text{and} \quad H^1(\mathfrak{l}^M, V_\ell G) \to \prod_{\mathfrak{c} \subseteq \mathfrak{l}^M} H^1(\mathfrak{c}, V_\ell M)$$

where the leftmost product runs over all $h \in H := \mathrm{Hom}_{E \otimes \mathbb{Q}_\ell}(D \otimes \mathbb{Q}_\ell, V_\ell G)$.

Proof. Lemma 3.9 shows that if on the right side we let the product only run over $\mathfrak{c} \in \mathfrak{n}^M$ we still get the same kernel. For every $\mathfrak{c} = \langle x \rangle \subseteq \mathfrak{n}^M$, we have

$$H^1(\mathfrak{c}, \mathrm{V}_\ell M) \cong \frac{\mathrm{V}_\ell M}{\{x.v \mid v \in \mathrm{V}_\ell M\}} = \frac{\mathrm{V}_\ell M}{\mathrm{im}(\vartheta(x))},$$

where $\vartheta : \mathfrak{n} \to \mathrm{Hom}(Y \otimes \mathbb{Q}, \mathrm{V}_\ell G)$ is as defined in Section 3.4. The map

$$H^1(\mathfrak{l}^M, \mathrm{V}_\ell G) \to \mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{n}^M, \mathrm{V}_\ell G)$$

given by restriction of cocycles is an isomorphism; thus, we have to show that the kernels of the maps

$$D \otimes \mathbb{Q}_\ell \to \prod_{h \in H} \mathrm{V}_\ell G / h(X \otimes \mathbb{Q}_\ell) \quad \text{and} \quad \mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{n}^M, \mathrm{V}_\ell G) \to \prod_{x \in \mathfrak{n}^M} \mathrm{V}_\ell G / \mathrm{im}(\vartheta(x))$$

correspond under the isomorphism $D \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{n}^M, \mathrm{V}_\ell G)$ sending $\psi(u) \otimes 1$ to $\mathrm{V}_\ell \psi \circ \vartheta$ for all $\psi \in \mathrm{Hom}_{\bar{k}}(B, G)$. Here, $B \subseteq \mathscr{H}om(Y, G)$ is defined as in Theorem 3.5. The map on the right sends an $\mathfrak{l}^G$-module homomorphism $c : \mathfrak{n}^M \to \mathrm{V}_\ell G$ to the class of $c(x)$ in the factor corresponding to x. As for the map on the left, by Lemma 3.7, we may as well take $\mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell B, \mathrm{V}_\ell G)$ in place of $D \otimes \mathbb{Q}_\ell$ as the domain. Then we must show that the kernels of the maps

$$\mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell B, \mathrm{V}_\ell G) \to \prod_h \mathrm{V}_\ell G / f(X \otimes \mathbb{Q}_\ell)$$

and

$$\mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{n}^M, \mathrm{V}_\ell G) \to \prod_{x \in \mathfrak{n}^M} \mathrm{V}_\ell G / \mathrm{im}(\vartheta(x))$$

correspond to each other via composition with the isomorphism $\vartheta : \mathfrak{n}^M \to \mathrm{V}_\ell B$, the first of these products now running over all $E \otimes \mathbb{Q}_\ell$-module morphisms $h : \mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell B, \mathrm{V}_\ell G) \to \mathrm{V}_\ell G$. The canonical map

$$\mathrm{V}_\ell B \xrightarrow{\cong} \mathrm{Hom}_{E \otimes \mathbb{Q}_\ell}(\mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell B, \mathrm{V}_\ell G), \mathrm{V}_\ell G), \qquad v \mapsto [f \mapsto f(v)]$$

is an isomorphism by Schur's lemma, so all these $E \otimes \mathbb{Q}_\ell$-module homomorphisms h are given by evaluation in an element $v \in \mathrm{V}_\ell B$. If h is the evaluation in $v = \vartheta(x)$ for some $x \in \mathfrak{n}^M$, then $h(X \otimes \mathbb{Q}_\ell) = \mathrm{im}\,\vartheta(x)$, hence the claim of the lemma. $\square$

Proof of Theorem 3.1. We consider the following diagram, where the exact row is induced by the weight filtration on the $\mathfrak{l}^M$-module $\mathrm{V}_\ell M$ and where the column is exact by definition:

$$H^1_*(\mathfrak{l}^M, V_\ell M)$$

$$H^0(\mathfrak{l}^M, Y \otimes \mathbb{Q}_\ell) \xrightarrow{\partial} H^1(\mathfrak{l}^M, V_\ell G) \longrightarrow H^1(\mathfrak{l}^M, V_\ell M) \longrightarrow H^1(\mathfrak{l}^M, Y \otimes \mathbb{Q}_\ell)$$

$$\prod_{\mathfrak{c} \subseteq \mathfrak{l}^M} H^1(\langle x \rangle, V_\ell M)$$

The upper diagonal map is zero because $\mathfrak{l}^M$ acts trivially on $Y \otimes \mathbb{Q}_\ell$; hence, $H^1_*(\mathfrak{l}^M, Y \otimes \mathbb{Q}_\ell)$ is trivial. This shows that every element of $H^1_*(\mathfrak{l}^M, V_\ell M)$ comes from an element in $H^1(\mathfrak{l}^M, V_\ell G)$, so we find an isomorphism

$$\ker \delta / \operatorname{im} \partial \cong H^1_*(\mathfrak{l}^M, V_\ell M)$$

induced by the inclusion $V_\ell G \subseteq V_\ell M$. Lemmas 3.7 and 3.10 respectively show that the isomorphism $D \otimes \mathbb{Q}_\ell \to H^1(\mathfrak{l}^M, V_\ell G)$ induces isomorphisms $X \otimes \mathbb{Q}_\ell \cong \operatorname{im} \partial$ and

$$\overline{X}_\ell := \left\{ x \in D \otimes \mathbb{Q}_\ell \mid f(x) \in f(X \otimes \mathbb{Q}_\ell) \text{ for all } f \in \operatorname{Hom}_{E \otimes \mathbb{Q}_\ell}(D \otimes \mathbb{Q}_\ell, V_\ell G) \right\}$$
$$\cong \ker \delta,$$

as needed. $\qquad\square$

3.11. Throughout this section, we have always supposed that the semiabelian variety G is either an abelian variety or a torus. Most statements and constructions, notably Theorems 3.1 and 3.5, remain true if G is isogenous to a product of an abelian variety and a torus, and the proofs require only small additional arguments, but the statements are wrong for general semiabelian varieties. The main problem here is that a general semiabelian variety G is not a semisimple object, so the analogue of Poincaré's complete reducibility theorem fails, and the Galois representation $V_\ell G$ is not semisimple either.

In a general setting, the Lie algebra $\mathfrak{n}^M$ should be replaced by the subalgebra of $\mathfrak{l}^M$ consisting of those elements of which act trivially on $V_\ell A$ and $V_\ell T$, where A and T are respectively the abelian and torus parts of M. This is then in general not a commutative but just a nilpotent Lie algebra. The generalisation of Theorem 3.5 is [Jossen 2013b, Theorem 6.2]. The subgroup D of $G(\bar{k})$ has to be replaced by the group of so-called *deficient points* [loc. cit., Definition 6.2], and the generalisation of Lemma 3.6 is [loc. cit., Theorem 8.10]. Finally, E-linearity should be reformulated in terms of derivations. With these settings, it should be possible to generalise Theorem 3.1 to arbitrary 1-motives.

4. Finiteness results

In this section, we prove the finiteness statements of Theorem 3 stated in the introduction. We fix a number field k with algebraic closure $\bar{k}$ and a prime number ℓ and write $\Gamma := \mathrm{Gal}(\bar{k}\,|\,k)$ for the absolute Galois group of k and Ω for the set of all places of k. For a 1-motive M over k, we write $V_\ell M := T_\ell M \otimes \mathbb{Q}_\ell$ and denote by L^M the image of Γ in $\mathrm{GL}(T_\ell M)$ and by $\mathfrak{l}^M \subseteq \mathrm{End}(V_\ell M)$ the Lie algebra of L^M.

Theorem 4.1. *Let $M = [u : Y \to G]$ be a 1-motive over k. The $\mathbb{Z}_\ell$-module $\mathrm{III}^1(k, T_\ell M)$ is finitely generated. If G is an abelian variety or a torus, such that $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras, then $\mathrm{III}^1(k, T_\ell M)$ is finite.*

Observe that if G is an abelian variety, then $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras precisely if $G_{\bar{k}}$ is isogenous to a product of pairwise nonisogenous simple abelian varieties over $\bar{k}$. If G is a torus, then $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras precisely if G is of dimension ≤ 1.

The plan of this section is as follows. First we show that for every 1-motive M over k there is a canonical injection of $\mathrm{III}^1(k, T_\ell M)$ into $H^1_*(L^M, T_\ell M)$. We continue with some elementary linear algebra and prove, using Theorem 3.1, that the group $H^1_*(L^M, T_\ell M)$, and hence $\mathrm{III}^1(k, T_\ell M)$, is finite for all ℓ if M is a 1-motive satisfying the condition in the theorem.

Proposition 4.2. *Let M be a 1-motive over k. There is a canonical injective $\mathbb{Z}_\ell$-linear map $\mathrm{III}^1(k, T_\ell M) \to H^1_*(L^M, T_\ell M)$. The $\mathbb{Z}_\ell$-module $H^1_*(L^M, T_\ell M)$ is finitely generated, and its rank is bounded by the dimension of $H^1_*(\mathfrak{l}^M, V_\ell M)$.*

Proof. For every finite Galois module F, the subgroup $\mathrm{III}^1(k, F)$ of $H^1(k, F) = H^1(\Gamma, F)$ is contained in $H^1_*(\Gamma, F)$ by [Serre 1964, Proposition 8], which is essentially a consequence of Chebotarev's density theorem. Because $H^1(k, -)$ commutes with limits of finite Galois modules and by left exactness of the limit functor, we can deduce that $\mathrm{III}^1(k, T_\ell M)$ is contained in $H^1_*(\Gamma, T_\ell M)$, and $H^1_*(\Gamma, T_\ell M)$ is isomorphic to $H^1_*(L^M, T_\ell M)$ by [Serre 1964, Proposition 6], hence the canonical injection. By [loc. cit., Proposition 9], the $\mathbb{Z}_\ell$-module $H^1(L^M, T_\ell M)$ is finitely generated, and we have an isomorphism of finite-dimensional vector spaces

$$H^1(L^M, T_\ell M) \otimes \mathbb{Q}_\ell \cong H^1(L^M, V_\ell M).$$

This identifies $H^1_*(L^M, T_\ell M) \otimes \mathbb{Q}_\ell$ with a subspace of $H^1_*(L^M, V_\ell M)$, which in turn is a subspace of $H^1_*(\mathfrak{l}^M, V_\ell M)$ by Lemma 3.3. □

Lemma 4.3. *Let $K_1 | K_0$ be an extension of fields (think of $\mathbb{Q}_\ell | \mathbb{Q}$). Let E_0 be a K_0-algebra, let D_0 and V_0 be E_0-modules, and let X_0 be a K_0-linear subspace of D_0. Denote by E_1, D_1, V_1, and X_1 the corresponding objects obtained by tensoring*

with K_1. *Define*

$$\overline{X}_0 := \{x \in D_0 \mid f(x) \in f(X_0) \text{ for all } f \in \operatorname{Hom}_{E_0}(D_0, V_0)\},$$
$$\overline{X}_1 := \{x \in D_1 \mid f(x) \in f(X_1) \text{ for all } f \in \operatorname{Hom}_{E_1}(D_1, V_1)\}.$$

Then, the inclusion $\overline{X}_1 \subseteq \overline{X}_0 \otimes K_1$ *holds. In particular, if the equality* $X_0 = \overline{X}_0$ *holds, then the equality* $X_1 = \overline{X}_1$ *holds as well.*

Proof. Let x be an element of $\overline{X}_1 \subseteq D_1$, and let us show that x belongs to $\overline{X}_0 \otimes K_1$. Every E_0-linear map $D_0 \to V_0$ gives rise by K_1-linear extension to an E_1-linear map $D_1 \to V_1$, so by definition of $\overline{X}_1$, there exists in particular for every $f \in \operatorname{Hom}_{E_0}(D_0, V_0)$ an element $x^f \in X_1$ such that $f(x) = f(x^f)$. Let $(t_i)_{i \in I}$ be a K_0-basis of K_1, so we can write x and x^f as sums

$$x = \sum_{i \in I} x_i \otimes t_i \quad \text{and} \quad x^f = \sum_{i \in I} x_i^f \otimes t_i$$

for unique elements $x_i \in D_0$ and $x_i^f \in X_0$, almost all zero. We have to show that the x_i belong to $\overline{X}_0$ for all $i \in I$. The equality $f(x) = f(x^f)$ reads

$$\sum_{i \in I} f(x_i) \otimes t_i = \sum_{i \in I} f(x_i^f) \otimes t_i.$$

Linear independence of the t_i over K_0 implies that we have in fact $f(x_i) = f(x_i^f)$ for all i. Hence, for every $i \in I$ and every $f \in \operatorname{Hom}_{E_0}(D_0, V_0)$, we have $f(x_i) \in f(X_0)$, that is, $x_i \in \overline{X}_0$ as we wanted to show. As for the additional statement, if we have $X_0 = \overline{X}_0$, then the inclusions

$$X_0 \otimes K_1 \stackrel{\text{def}}{=} X_1 \subseteq \overline{X}_1 \subseteq \overline{X}_0 \otimes K_1$$

must all be equalities. $\square$

Lemma 4.4. *Let K be a field of characteristic 0, let E be a finite product of finite-dimensional division algebras over K, let D and V be finite-dimensional E-modules, and suppose that V is faithful. Let X be a K-linear subspace of D. An element $v \in D$ belongs to X if and only if $f(v)$ belongs to $f(X)$ for all E-linear maps $f : D \to V$.*

Proof. We only show the case where E is a division algebra over K; the proof of the general case is similar. That V is faithful means then just that V is nonzero, and without loss of generality, we may suppose that V is E, so we are considering E-linear forms $f : D \to E$. Let $\operatorname{tr}_{E|K} : E \to K$ be a trace map, which for our purpose can be just any K-linear map with the property that

$$\operatorname{tr}_{E|K}(yx) = 0 \text{ for all } y \in E \implies x = 0.$$

Such a trace map always exists (see, e.g., [Gille and Szamuely 2006, Section 2.6]). Consider then the K-linear map

$$\mathrm{Hom}_E(D, E) \to \mathrm{Hom}_K(D, K), \quad f \mapsto \mathrm{tr}_{E|K} \circ f.$$

We claim that this is an isomorphism of K-vector spaces. We only have to show injectivity; surjectivity follows then by dimension-counting. To show injectivity, we can suppose that $D = E$. The above map sends then an E-linear endomorphism of E, which is just multiplication on the right by some $x \in E$, to the K-linear map $y \mapsto \mathrm{tr}(yx)$. If this map is zero, then x must be zero by the above property of the trace, hence injectivity. The hypothesis on v implies that

$$\mathrm{tr}_{E|K} \ f(v) \in \mathrm{tr}_{E|K} \ f(X)$$

for all $f \in \mathrm{Hom}_E(D, E)$; hence, $f(v) \in f(X)$ for all $f \in \mathrm{Hom}_K(D, K)$; hence, $v \in X$ by standard linear algebra. $\qquad \square$

Proof of Theorem 4.1. By Proposition 4.2, it is enough to show that the vector space $H^1_*(\mathfrak{l}^M, V_\ell M)$ is trivial. Set $E_\ell := \mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}_\ell$ and $X_\ell := \mathrm{im}(u) \otimes \mathbb{Q}_\ell$, denote by D_ℓ the E_ℓ-submodule of $G(\bar{k}) \otimes \mathbb{Q}_\ell$ generated by X_ℓ, and define

$$\overline{X}_\ell := \{x \in D_\ell \mid f(x) \in f(X_\ell) \text{ for all } f \in \mathrm{Hom}_{E_\ell}(D_\ell, V_\ell G)\}.$$

By Theorem 3.1, we have to check that the equality $X_\ell = \overline{X}_\ell$ holds. Fix an embedding of k into the field of complex numbers $\mathbb{C}$. Set $V_0 G := H_1(G(\mathbb{C}), \mathbb{Q})$ and $E_0 := \mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ and $X_0 := \mathrm{im}(u) \otimes \mathbb{Q}$, and denote by D_0 the E_0-submodule of $G(\bar{k}) \otimes \mathbb{Q}$ generated by X_0. Note that $V_0 G$ is a faithful E_0-module and that there is a natural isomorphism $V_\ell G \cong V_0 G \otimes \mathbb{Q}_\ell$. By Lemma 4.3, it is now enough to check the equality $X_0 = \overline{X}_0$ for

$$\overline{X}_0 := \{x \in D_0 \mid f(x) \in f(X_0) \text{ for all } f \in \mathrm{Hom}_{E_0}(D_0, V_0 G)\}.$$

By hypothesis, the $\mathbb{Q}$-algebra E_0 is a product of division algebras; hence, the equality $X_0 = \overline{X}_0$ indeed holds by Lemma 4.4. $\qquad \square$

4.5. One can think of other linear algebra conditions on the objects E, D, V, and X than those in Lemma 4.4 that ensure the equality $X = \overline{X}$. For instance, the conclusion of the lemma holds true for any finite-dimensional semisimple algebra E over K and faithful V if X is of dimension ≤ 1 or if X is an E-submodule or D. One can conclude along the same lines that if $M = [u : Y \to G]$ is a 1-motive where G is an abelian variety or a torus, such that the image of u generates an $\mathrm{End}_{\bar{k}} \otimes \mathbb{Q}$-submodule of $G(\bar{k}) \otimes \mathbb{Q}$ or such that $u(Y)$ is of rank ≤ 1, then $\mathrm{III}^1(k, T_\ell M)$ is finite.

4.6. Our strategy of proving finiteness of $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ consisted of showing that the a priori larger group $H^1_*(L^M, \mathrm{T}_\ell M)$ is finite. This strategy does not succeed always; indeed, there exist 1-motives M such that the group $H^1_*(L^M, \mathrm{T}_\ell M)$ is infinite, yet $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ is finite. The point here is that $H^1_*(\Gamma, \mathrm{T}_\ell M)$ only sees the primes at which $\mathrm{T}_\ell M$ is unramified, whereas $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ sees all primes.

5. The torsion of $\mathrm{III}^1(k, \mathrm{T}_\ell M)$

In this section, we complete the proof of Theorem 3 by examining the finite torsion part of the group $\mathrm{III}^1(k, \mathrm{T}_\ell M)$. The key ingredient for this is the following lemma:

Lemma 5.1. *Let T be a finitely generated free $\mathbb{Z}_\ell$-module, and set $V := T \otimes \mathbb{Q}_\ell$. Let $D \subseteq L \subseteq \mathrm{GL}(T)$ be Lie subgroups with Lie algebras $\mathfrak{d}$ and $\mathfrak{l}$, respectively. If*

(1) *the set $\{\pi \circ x \mid x \in \mathfrak{l},\ \pi \in V^*\}$ is a linear subspace of V^* and*

(2) *for all open subgroups $H \subseteq L$ containing D the equality $T^H = T^L$ holds,*

then the map $r : H^1_*(L, T) \to H^1_*(D, T)$ given by restriction of cocycles is injective on torsion elements.

This generalises Lemma 4.1 in [Jossen 2013a], which we get back by taking for D the trivial group. In our application, T will be $\mathrm{T}_\ell M$ for a 1-motive M, L will be L^M, i.e., the image of $\Gamma := \mathrm{Gal}(\bar{k} \mid k)$ in $\mathrm{GL}(\mathrm{T}_\ell M)$, and D will be the image in $\mathrm{GL}(\mathrm{T}_\ell M)$ of a decomposition group $D_v \subseteq \Gamma$.

Proof of Lemma 5.1. Let $c : L \to T$ be a cocycle representing an element of order ℓ in $\ker(r)$, and let us show that c is a coboundary. Because c represents a torsion element in $H^1(L, T)$, its image in $H^1(L, V)$ is trivial. Thus, identifying T with a subset of V, there exists $v \in V$ such that $c(g) = gv - v$ for all $g \in L$. The cocycle c is a coboundary if v belongs to $v \in V^L + T$. In fact, we will show that

$$v \in (T + V^D) \cap (T + V^{\mathfrak{l}}). \tag{$\ddagger$}$$

Since the restriction of c to D is a coboundary, there exists $t \in T$ such that $c(g) = gt - t$ for all $g \in D$; hence, $v - t \in V^D$, and so $v \in T + V^D$ as needed. To say that the cohomology class of c belongs to $H^1_*(L, T)$ is to say that for each $g \in L$ there exists an element $t_g \in T$ such that $c(g) = gt_g - t_g$. Let N be an open normal subgroup of $\mathfrak{l}$ on which the exponential map $\exp : N \to \mathfrak{l}$ is defined so that $V^{\langle g \rangle} = \ker(\exp(g))$ for all $g \in N$. We then have

$$v \in \bigcap_{g \in L}(T + V^{\langle g \rangle}) \subseteq \bigcap_{g \in N}(T + V^{\langle g \rangle}) = \bigcap_{x \in \mathfrak{l}}(T + \ker(x)).$$

Because of the hypothesis (1), Lemma 4.4 of [Jossen 2013a] applies, which yields $v \in T + \bigcap_{x \in \mathfrak{l}} \ker(x) = T + V^{\mathfrak{l}}$ and completes the proof of ($\ddagger$).

By modifying v by an element of T, we may suppose without loss of generality that v belongs to V^D and in particular to $V^{\mathfrak{d}}$. The finite group $G := D/(N \cap D)$ acts on $V^{\mathfrak{d}}$ as well as on $V^{\mathfrak{l}}$. By Maschke's theorem, there exists a $\mathbb{Q}_\ell$-linear, G-equivariant retraction map $r : V^{\mathfrak{d}} \to V^{\mathfrak{l}}$ of the inclusion $V^{\mathfrak{l}} \to V^{\mathfrak{d}}$. Restricting r to $V^{\mathfrak{l}} + (T \cap V^{\mathfrak{d}})$, we find a decomposition of G-modules

$$V^{\mathfrak{l}} + (T \cap V^{\mathfrak{d}}) = V^{\mathfrak{l}} \oplus (\ker r \cap (T \cap V^{\mathfrak{d}})).$$

Writing $v = v_1 + t_1$ with $v_1 \in V^{\mathfrak{l}}$ and $t_1 \in \ker r \cap T \cap V^{\mathfrak{d}}$ according to this decomposition, we see that v_1 (and also t_1) is fixed under G because v is so; hence, we have

$$v \in (V^{\mathfrak{l}} \cap (V^{\mathfrak{d}})^G) + T = (V^N \cap V^D) + T = V^{ND} + T.$$

The subgroup ND of L is open and contains D; hence, $v \in V^L + T$ by hypothesis (2). $\qquad\square$

Lemma 5.2. *Let $M = [u : Y \to G]$ be a 1-motive where G is an abelian variety or a torus such that $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras. If the Galois action on Y is trivial, then $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ is trivial.*

Proof. For every finite Galois extension $k' | k$, we have

$$H^0(k, \mathrm{T}_\ell M) = H^0(k', \mathrm{T}_\ell M) \cong H^{-1}(M) \otimes \mathbb{Z}_\ell$$

by Corollary 1.10. Hence, we have $(\mathrm{T}_\ell M)^{L^M} = (\mathrm{T}_\ell M)^U$ for all open subgroups U of L^M. It follows from [Jossen 2013a, Propositions 3.1 and 3.2], which use the hypothesis on $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ that the image of the bilinear map

$$\mathfrak{l}^M \times (\mathrm{V}_\ell M)^* \to (\mathrm{V}_\ell M)^*, \qquad (x, \pi) \mapsto \pi \circ x$$

is a linear subspace of $(\mathrm{V}_\ell M)^*$. The hypotheses of Lemma 5.1 are thus satisfied, and taking for D the trivial group, it shows that $H^1_*(L^M, \mathrm{T}_\ell M)$ is torsion-free. By Theorem 4.1, this group is also finite, hence trivial, and we conclude by Proposition 4.2. $\qquad\square$

Proof of Theorem 3. Let $M = [u : Y \to G]$ be a 1-motive over k. We have constructed the pairing of the theorem and shown in Corollary 2.4 that it is nondegenerate on the left and in Proposition 2.5 that $\mathrm{III}^0(k, M)$ is finite. Suppose then that G is an abelian variety or a torus such that $\mathrm{End}_{\bar{k}}(G) \otimes \mathbb{Q}$ is a product of division algebras. By Corollary 2.4, it remains to prove that the canonical map

$$\mathrm{III}^0(k, M) \otimes \mathbb{Z}_\ell \to \mathrm{III}^1(k, \mathrm{T}_\ell M) \qquad\qquad (\star)$$

constructed in Section 2.3 is an isomorphism. We define $Z := H^{-1}(M) = \ker u$ and use Proposition 2.5 to identify $\mathrm{III}^1(k, M) \otimes \mathbb{Z}_\ell$ with $\mathrm{III}^1(k, Z \otimes \mathbb{Z}_\ell)$. Fix a finite Galois extension $k' | k$ over which Z is constant. For every place w of k', we write

k_w for the completion of k at the restriction of w to k, and $D_w := \operatorname{Gal}(k'_w \,|\, k_w)$. From the Hochschild–Serre spectral sequence, we get a commutative diagram with exact rows

$$
\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\operatorname{Gal}(k'\,|\,k), Z \otimes \mathbb{Z}_\ell) & \longrightarrow & H^1(k, \mathrm{T}_\ell M) & \longrightarrow & H^1(k', \mathrm{T}_\ell M) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_w H^1(G_w, H^0(k'_w, \mathrm{T}_\ell M)) & \longrightarrow & \prod_w H^1(k_w, \mathrm{T}_\ell M) & \longrightarrow & \prod_w H^1(k'_w, \mathrm{T}_\ell M)
\end{array}
$$

The rightmost vertical map is injective by Lemma 5.2; hence, every element of $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ comes from a unique element of $H^1(\operatorname{Gal}(k'\,|\,k), Z \otimes \mathbb{Z}_\ell)$, hence from $H^1(k, Z \otimes \mathbb{Z}_\ell)$. It remains to show that this element is in $\mathrm{III}^1(k, Z \otimes \mathbb{Z}_\ell)$. To this end, we consider the diagram

$$
\begin{array}{ccccc}
0 & \longrightarrow & H^1(k, Z \otimes \mathbb{Z}_\ell) & \longrightarrow & H^1(k, \mathrm{T}_\ell M) \\
 & & \downarrow & \overset{\delta}{\dashrightarrow} & \downarrow \\
 & & \prod H^1(k_v, Z \otimes \mathbb{Z}_\ell) & \longrightarrow & \prod H^1(k_v, \mathrm{T}_\ell M)
\end{array}
$$

where the horizontal maps are induced by the morphism of 1-motives $[Z \to 0] \to [Y \to G]$. Injectivity of the top horizontal map follows from Corollary 1.10. We have thus $\ker \delta \cong \mathrm{III}^1(k, \mathrm{T}_\ell M)$ and must show that every element of $\ker \delta$ maps already to zero in $H^1(k_v, Z \otimes \mathbb{Z}_\ell)$ for all $v \in \Omega$; that is, $\ker \delta = \mathrm{III}^1(k, Z \otimes \mathbb{Z}_\ell)$.

Fix an element x of $\mathrm{III}^1(k, \mathrm{T}_\ell M)$ and a place v, and let D_v be a decomposition group for v. We know that x comes via inflation from an element z of the finite group $H^1_*(L^M, \mathrm{T}_\ell M)$. Write D for the image of D_v in $\operatorname{GL}(\mathrm{T}_\ell M)$. This D is a Lie subgroup of L^M, and by hypothesis, z restricts to zero in $H^1(D, \mathrm{T}_\ell M)$. By Lemma 5.1 (using again [Jossen 2013a, Propositions 3.1 and 3.2]), we conclude that there is an open subgroup U of L^M containing D such that z is already zero in $H^1(U, \mathrm{T}_\ell M)$. This shows as well that there is an open subgroup Γ' of Γ containing D_v such that x maps to zero in $H^1(\Gamma', \mathrm{T}_\ell M)$. Consider then the diagram

$$
\begin{array}{ccccc}
0 & \longrightarrow & H^1(\Gamma, Z \otimes \mathbb{Z}_\ell) & \longrightarrow & H^1(\Gamma, \mathrm{T}_\ell M) \\
 & & \downarrow & \overset{\delta'}{\dashrightarrow} & \downarrow{\scriptstyle x \mapsto 0} \\
0 & \longrightarrow & H^1(\Gamma', Z \otimes \mathbb{Z}_\ell) & \longrightarrow & H^1(\Gamma', \mathrm{T}_\ell M) \\
 & & \downarrow & & \downarrow \\
 & & H^1(D_v, Z \otimes \mathbb{Z}_\ell) & \longrightarrow & H^1(D_v, \mathrm{T}_\ell M)
\end{array}
$$

We know that the element $x \in \mathrm{III}^1(k, \mathrm{T}_\ell M)$ comes from an element of $\ker \delta'$. The middle row is exact by Corollary 1.10 and because Γ' is the Galois group

of a number field so that this element maps to zero in $H^1(\Gamma', Z \otimes \mathbb{Z}_\ell)$, hence in $H^1(D_v, Z \otimes \mathbb{Z}_\ell)$. $\square$

6. Tate 1-motives and Leopoldt's conjecture

In this section, we study the pairing of Theorem 3 in the case where M is a *Tate 1-motive* over k, that is, a 1-motive of the form $M = [\mathbb{Z}^r \to \mathbb{G}_m^s]$. I will show the following sharper version of Theorem 2 stated in the introduction:

Theorem 6.1. *Let k be a number field with ring of integers $\mathbb{O}_k$, and let ℓ be a prime number. If for every 1-motive of the form $M = [\mathbb{Z}^r \to \mathbb{G}_m^2]$ over $\mathrm{spec}(\mathbb{O}_k)$ the group $\mathrm{III}^2(k, M^\vee)[\ell^\infty]$ is trivial, then the statement of Leopoldt's conjecture is true for k and ℓ.*

6.2. We work with the following formulation of Leopoldt's conjecture [Neukirch et al. 2000, Theorem 10.3.6(iii)]. For a finite prime $\mathfrak{p}$ of k, let $\mathbb{O}_{k,\mathfrak{p}}$ denote the ring of integers of the completion of k at $\mathfrak{p}$. There is a canonical map

$$i_\ell : \mathbb{O}_k^* \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \prod_{\mathfrak{p}|\ell} \mathbb{O}_{k,\mathfrak{p}}^* \, \widehat{\otimes} \, \mathbb{Z}_\ell,$$

which on each component $i_\mathfrak{p} : \mathbb{O}_k^* \otimes \mathbb{Z}_\ell \to \mathbb{O}_{k,\mathfrak{p}} \, \widehat{\otimes} \, \mathbb{Z}_\ell$ is obtained by applying $- \, \widehat{\otimes} \, \mathbb{Z}_\ell$ to the inclusion $\mathbb{O}_k^* \subseteq \mathbb{O}_{k,\mathfrak{p}}^*$. Leopoldt's conjecture asserts that the map i_ℓ is injective. Note that i_ℓ is injective on torsion elements and injective if $\mathbb{O}_k^*$ is of rank ≤ 1.

Proof of Theorem 6.1. We suppose Leopoldt's conjecture is false for k and ℓ, so there exists a nontorsion element $z \in \ker(i_\ell) \subseteq \mathbb{O}_k^* \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which we may write as

$$z = \sum_{i=1}^n \varepsilon_i \otimes \lambda_i,$$

where $n \geq 2$ is the rank of $\mathbb{O}_k^*$ and $\varepsilon_1, \ldots, \varepsilon_n$ are $\mathbb{Z}$-linearly independent elements of $\mathbb{O}_k^*$. By reordering the ε_i and replacing ε_1 by ε_1^{-1} if necessary, we may as well assume $\lambda_1 + \lambda_2 \neq 0$. We will now construct a 1-motive M of the form $M = [u : \mathbb{Z}^{2n-1} \to \mathbb{G}_m^2]$ over $\mathrm{spec}(\mathbb{O}_k)$ such that the group $\mathrm{III}^1(k, T_\ell M)$ is infinite. The 1-motive dual to M is then of the form $M^\vee = [\mathbb{Z}^2 \to \mathbb{G}_m^{2n-1}]$, and $\mathrm{III}^2(k, M^\vee)$ will be infinite by Proposition 2.2. Let $Y \simeq \mathbb{Z}^{2n-1}$ be the group matrices

$$y = \begin{pmatrix} y_{11} & y_{12} & y_{13} & \cdots & y_{1n} \\ y_{21} & y_{22} & y_{23} & \cdots & y_{2n} \end{pmatrix}$$

with integer coefficient satisfying $y_{11} + y_{22} = 0$, and define the morphism u by

$$u(y) = \begin{pmatrix} y_{11}\varepsilon_1 + y_{12}\varepsilon_2 + y_{13}\varepsilon_3 + \cdots + y_{1n}\varepsilon_n \\ y_{21}\varepsilon_1 + y_{22}\varepsilon_2 + y_{23}\varepsilon_3 + \cdots + y_{2n}\varepsilon_n \end{pmatrix} \in \mathbb{G}_m^2(\mathbb{O}_k),$$

where we decided to write the group $\mathbb{G}_m(\mathbb{O}_k) = \mathbb{O}_k^*$ additively. So if ε denotes the column vector of the ε_i, we have just $u(y) = y\varepsilon$. We will prove the following lemma later:

Lemma 6.3. *For each $1 \leq i \leq n$, there exists $y \in Y$ such that $\binom{\varepsilon_i}{\varepsilon_i} \equiv u(y)$ mod $\mathfrak{p}$ holds in $\mathbb{G}_m^2(\kappa_\mathfrak{p})$, where $\kappa_\mathfrak{p} = $ is the residue field at $\mathfrak{p}$.*

Set $U := \mathrm{spec}(\mathbb{O}_k[\ell^{-1}])$, and denote by c_i and c, respectively, the images of $\binom{\varepsilon_i}{\varepsilon_i} \otimes 1$ and $\binom{z}{z}$ under the composite map

$$\mathbb{G}_m^2(U) \otimes \mathbb{Z}_\ell \to H^0(U, M) \otimes \mathbb{Z}_\ell \to H^1(U, T_\ell M)$$

where the first map is induced by the projection $\mathbb{G}_m^2(U) \to \mathbb{G}_m^2(U)/u(Y) \cong H^0(U, M)$ and the second map is the injection defined in Proposition 1.9. The $\mathbb{Z}_\ell$-submodules of $\mathbb{G}_m^2(\mathbb{O}_k) \otimes \mathbb{Z}_\ell$ generated by $\binom{z}{z}$ and by $u(Y)$ intersect trivially because $\lambda_1 + \lambda_2 \neq 0$; hence, c is of infinite order in $H^1(U, T_\ell M) \subseteq H^1(k, T_\ell M)$. I claim that c belongs to $\mathrm{III}^1(k, T_\ell M)$. Fix a place $\mathfrak{p}$ of k of residual characteristic p, and let us show that the restriction of c to $H^1(k_\mathfrak{p}, T_\ell M)$ is zero. In the case $p = \ell$, this is true by construction, considering the commutative diagram

$$
\begin{array}{ccc}
(\mathbb{O}_k^*)^2 \otimes \mathbb{Z}_\ell & \longrightarrow & H^1(U, T_\ell M) \\
\downarrow & & \downarrow \\
(\mathbb{O}_{k,\mathfrak{p}}^*)^2 \widehat{\otimes} \mathbb{Z}_\ell & \longrightarrow & H^1(k_\mathfrak{p}, T_\ell M)
\end{array}
$$

and that the image of $\binom{z}{z}$ is already zero in $(\mathbb{O}_{k,\mathfrak{p}}^*)^2 \widehat{\otimes} \mathbb{Z}_\ell$. Suppose now that $p \neq \ell$, so $T_\ell M$ is unramified at $\mathfrak{p}$. Because $c = \lambda_1 c_1 + \cdots + \lambda_n c_n$, it suffices to show that the restriction of each c_i to $H^1(\kappa_\mathfrak{p}, T_\ell M)$ is zero. In view of the commutative diagram

$$
\begin{array}{ccc}
(\mathbb{O}_k^*)^2 \otimes \mathbb{Z}_\ell & \longrightarrow & H^1(U, T_\ell M) \\
\downarrow & & \downarrow \\
Y \otimes \mathbb{Z}_\ell \xrightarrow{u \bmod \mathfrak{p}} (\kappa_\mathfrak{p}^*)^2 \otimes \mathbb{Z}_\ell & \longrightarrow & H^1(\kappa_\mathfrak{p}, T_\ell M)
\end{array}
$$

this amounts to show that there exists $y \in Y$ such that $\binom{\varepsilon_i}{\varepsilon_i} \equiv u(y)$ mod $\mathfrak{p}$ holds in $\mathbb{G}_m^2(\kappa_\mathfrak{p})$, which is what we claimed in Lemma 6.3. Hence, c belongs indeed to $\mathrm{III}^1(k, T_\ell M)$ and is of infinite order, and thus, $\mathrm{III}^1(k, T_\ell M)$ is infinite. $\qquad\square$

Proof of Lemma 6.3. Fix $1 \leq i \leq n$ and a maximal ideal $\mathfrak{p}$ of $\mathbb{O}_k$ with residue field $\kappa_\mathfrak{p}$. We have to find a matrix $y \in Y$ such that $\binom{\varepsilon_i}{\varepsilon_i}$ is congruent to $u(y)$ modulo $\mathfrak{p}$. For $i \neq 1, 2$, such a y exists trivially. Let $J_1 \subseteq \mathbb{Z}$ be the ideal consisting of those $m \in \mathbb{Z}$ such that $m\varepsilon_1$ mod $\mathfrak{p}$ is in the subgroup of $\kappa_\mathfrak{p}^*$ generated by ε_2, and let $a_1 \geq 1$ be the

positive generator of J_1. Similarly, define J_2 and a_2. There exist $b_1, b_2 \in \mathbb{Z}$ such that the linear dependence relations

$$a_1 \varepsilon_1 + b_2 \varepsilon_2 = 1 \quad \text{and} \quad b_1 \varepsilon_1 + a_2 \varepsilon_2 = 1$$

hold in the finite group $\kappa_{\mathfrak{p}}^*$, written additively. Note that b_i is a multiple of a_i. We claim that the integers a_1 and a_2 are coprime. Indeed, suppose there exists a prime ℓ dividing a_1 and a_2 so that we can write $a_i = \ell a_i'$ and $b_i = \ell b_i'$. Let Z be the subgroup of κ_ℓ^* generated by ε_1 and ε_2. Since $\kappa_{\mathfrak{p}}^*[\ell]$ is cyclic of order ℓ, we may suppose that $\kappa_{\mathfrak{p}}^*[\ell] \cap Z$ is contained in the subgroup of κ_ℓ^* generated by, say, ε_2. Thus, the point

$$T := a_1' \varepsilon_1 + b_2' \varepsilon_2 \in \kappa_{\mathfrak{p}}^*[\ell] \cap Z$$

can be written as $T = c \varepsilon_2$, and we get the relation $a_1' \varepsilon_1 + (b_2' - c) \varepsilon_2 = 1$, which contradicts the minimality of a_1. Therefore, a_1 and a_2 are coprime as claimed, and we can choose integers c_1 and c_2 such that $a_1 c_1 + a_2 c_2 = 1$. The matrices

$$y_1 = \begin{pmatrix} 1 - a_1 c_1 & -c_1 b_2 & 0 & \cdots & 0 \\ 1 - c_2 b_1 & -a_2 c_2 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad y_2 = \begin{pmatrix} -a_1 c_1 & 1 - c_1 b_2 & 0 & \cdots & 0 \\ -c_2 b_1 & 1 - a_2 c_2 & 0 & \cdots & 0 \end{pmatrix}$$

belong to Y, and we have $\binom{\varepsilon_i}{\varepsilon_i} \equiv u(y_i) \bmod \mathfrak{p}$ as desired. $\qquad \square$

Remark 6.4. If k is a number field whose group of global units $\mathbb{O}_k^*$ has rank ≤ 1, one can show that $\text{III}^1(k, T_\ell M) = 0$ holds for every Tate 1-motive M over k. On the other hand, a construction analogous to the one used in the next section produces Tate 1-motives over particular number fields k with infinite $\text{III}^1(k, T_\ell M)$.

7. A semiabelian variety with infinite III^2

In this section, we prove Theorem 1 by producing a semiabelian variety G over $\mathbb{Q}$ such that $\text{III}^2(\mathbb{Q}, G)$ contains $\mathbb{Q}/\mathbb{Z}$ as a subgroup and hence in particular is infinite. The technique is similar to that in the previous paragraph, and here we exploit now that for elliptic curves of sufficiently big rank the statement analogue to Leopoldt's conjecture trivially fails.

7.1. Let E be an elliptic curve over $\mathbb{Q}$ of rank at least 3, and let $P_1, P_2, P_3 \in E(\mathbb{Q})$ be $\mathbb{Z}$-linearly independent rational points. Let us write A for the abelian threefold E^3 over $\mathbb{Q}$ and Y for the group of 3×3 matrices of trace 0 with integer coefficients. Looking at $Y \simeq \mathbb{Z}^8$ as a Galois module with trivial Galois action, we consider the 1-motive

$$M = [u : Y \to A], \qquad u(y) = y P = \begin{pmatrix} y_{11} P_1 + y_{12} P_2 + y_{13} P_3 \\ y_{21} P_1 + y_{22} P_2 + y_{23} P_3 \\ y_{31} P_1 + y_{32} P_2 + y_{33} P_3 \end{pmatrix} \in E(\mathbb{Q})^3 = A(\mathbb{Q}).$$

The map u is injective, and I will use X as a shorthand for the group $u(Y) \subseteq A(\mathbb{Q})$. This 1-motive M is of special interest because it produces a counterexample to the so-called *problem of detecting linear dependence*: although $P \notin X$ and even $nP \notin X$ for all $n \neq 0$, there exists for every prime p where E has good reduction an element $x \in X$ such that P is congruent to x modulo p. The verification of this is similar to the proof of Lemma 6.3; see [Jossen and Perucca 2010]. Using Theorem 3.1, one shows that $H^1_*(\mathfrak{l}^M, \mathrm{V}_\ell M)$ is nontrivial — this is what makes the counterexample work and also how it was found in the first place.

7.2. I claim that the Tate–Shafarevich group in degree 2 of the semiabelian variety dual to the 1-motive M constructed in the previous paragraph contains a subgroup isomorphic to $\mathbb{Q}/\mathbb{Z}$. By Proposition 2.2, this amounts to say that for each prime number ℓ the Tate–Shafarevich group

$$\mathrm{III}^1(\mathbb{Q}, \mathrm{T}_\ell M)$$

is of rank ≥ 1 as a $\mathbb{Z}_\ell$-module. Fix a prime ℓ, and let us denote by $[c_P]$ the cohomology class of $P \otimes 1$ via the injection $H^0(\mathbb{Q}, M) \otimes \mathbb{Z}_\ell \to H^1(\mathbb{Q}, \mathrm{T}_\ell M)$ from Proposition 1.9. A cocycle c_P representing $[c_P]$ is explicitly given by

$$c_P(\sigma) = (\sigma P_i - P_i)_{i=0}^\infty,$$

where $(P_i)_{i=0}^\infty$ are elements of $A(\overline{\mathbb{Q}})$ such that $P_0 = P$ and $\ell P_i = P_{i-1}$. Up to a coboundary, c_P does not depend on the choice of the division points P_i. As the class $[P]$ of P in $H^0(\mathbb{Q}, M) \cong A(\mathbb{Q})/X$ is of infinite order, the element $[c_P] \in H^1(\mathbb{Q}, \mathrm{T}_\ell M)$ is of infinite order too. We claim that $n[c_P]$ belongs to $\mathrm{III}^1(\mathbb{Q}, \mathrm{T}_\ell M)$ for some integer $n \geq 1$ (depending on ℓ). To check this, we must show that for every finite place p of $\mathbb{Q}$ the restriction of nc_P to a decomposition group D_p is a coboundary. In the case where $\ell = 2$ and $p = \infty$, we should also demand that the restriction of $n[c_P]$ to $H^1(\mathrm{Gal}(\mathbb{C}|\mathrm{R}), \mathrm{T}_\ell M)$ is zero, but we can ignore this by choosing n to be even. So from now on, we will stick to finite primes p only.

Lemma 7.3. *Let p be a prime, and let $D_p \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ be a decomposition group at p. The restriction of c_P to D_p is a coboundary if and only if the class of P in $A(\mathbb{Q}_p)/X = H^0(\mathbb{Q}_p, M)$ is ℓ-divisible.*

Proof. Choose an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ in such a way that the given decomposition group D_p equals $\mathrm{Gal}(\overline{\mathbb{Q}}|(\overline{\mathbb{Q}} \cap \mathbb{Q}_p))$. Consider the commutative diagram with exact rows

$$
\begin{array}{ccccc}
0 & \longrightarrow & H^0(\mathbb{Q}, M) \otimes \mathbb{Z}_\ell & \longrightarrow & H^1(\mathbb{Q}, \mathrm{T}_\ell M) \\
& & \downarrow & & \downarrow \\
0 & \longrightarrow & H^0(\mathbb{Q}_p, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell & \longrightarrow & H^1(\mathbb{Q}_p, \mathrm{T}_\ell M)
\end{array}
$$

The restriction of c_P to D_p is a coboundary if and only if $[P] \otimes 1 \in H^0(\mathbb{Q}, M) \otimes \mathbb{Z}_\ell$ maps to zero in $H^0(\mathbb{Q}_p, M) \widehat{\otimes} \mathbb{Z}_\ell$, that is, if and only if the class of P in $H^0(\mathbb{Q}_p, M)$ is ℓ-divisible. $\square$

Lemma 7.4. *For every prime p, the closure of X in $A(\mathbb{Q}_p)$ for the p-adic topology is an open subgroup of $A(\mathbb{Q}_p)$ of finite index.*

Proof. Because $E(\mathbb{Q}_p)$ has the structure of a compact p-adic Lie group of dimension 1, there exists an open subgroup of $E(\mathbb{Q}_p)$ isomorphic to $\mathbb{Z}_p$, and because $E(\mathbb{Q}_p)$ is compact, any such subgroup has finite index [Silverman 1986, Proposition 6.3]. We find thus a short exact sequence of profinite groups

$$0 \to \mathbb{Z}_p^3 \to A(\mathbb{Q}_p) \to F \to 0$$

for some finite group F. Let $m \geq 1$ be an integer annihilating F so that mX is contained in $\mathbb{Z}_p^3$. The elements

$$\begin{pmatrix} 0 \\ mP_1 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 0 \\ mP_2 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} mP_3 \\ 0 \\ 0 \end{pmatrix}$$

of $mX \subseteq \mathbb{Z}_p^3 \subseteq A(\mathbb{Q}_p)$ are linearly independent over $\mathbb{Z}_p$ because each $mP_i \in \mathbb{Z}_p$ is nonzero. The closure of mX in $\mathbb{Z}_p^3$ contains the $\mathbb{Z}_p$-submodule generated by these three points, hence is of finite index in $\mathbb{Z}_p^3$. We conclude that the closure of X in $A(\mathbb{Q})$ has finite index. Every closed subgroup of finite index is also open. $\square$

7.5. We now come to the proof of the claims made in Section 7.2. First of all, let us choose an integer $n \geq 1$ such that the following conditions are met:

  (0) If $\ell = 2$, then n is even.

  (1) For every prime $p \neq \ell$ where E has bad reduction, the point nP is ℓ-divisible in $A(\mathbb{Q}_p)$.

  (2) For $p = \ell$, the point nP belongs to the closure of X in $A(\mathbb{Q}_p)$ for the p-adic topology.

Such an integer n exists. Indeed, start with, say, $n = 2$, so condition (0) is satisfied. We have already observed that $A(\mathbb{Q}_p)$ is an extension of a finite discrete group F by $\mathbb{Z}_p^3$, so by replacing n by some sufficiently high multiple of n, we can assure that nP belongs to the subgroup $\mathbb{Z}_p^3$ of $A(\mathbb{Q}_p)$, which is ℓ-divisible. We do this for all the finitely many primes of bad reduction, so condition (1) is met. As for the last condition, we know that the closure of X in $A(\mathbb{Q}_p)$ has finite index by Lemma 7.4, so we again replace n by some sufficiently high multiple if necessary. In order to show that $n[c_P]$ belongs to $\text{III}^1(\mathbb{Q}, T_\ell M)$, it remains to show by Lemma 7.3 that for each prime p the class of nP in $H^0(\mathbb{Q}, M) = A(\mathbb{Q}_p)/X$ is ℓ-divisible. In other words, we must show:

Claim. *For every $i \geq 0$, there exist elements $Q_i \in A(\mathbb{Q}_p)$ and $x_i \in X$ such that $\ell^i Q_i + x_i = nP$.*

We have already ruled out the case $p = \infty$, and for finite p, we will distinguish three cases: first, the case where p is a place of good reduction for E and $p \neq \ell$, second, the case where p is a place of bad reduction and $p \neq \ell$, and finally, the case $p = \ell$. All but finitely many primes p fall in the first case. For the finitely many primes that remain, the claim will hold by our particular choice of n.

<u>Case 1</u> (good reduction at p and $p \neq \ell$). In this case, we can consider the surjective reduction map $\mathrm{red}_p : E(\mathbb{Q}_p) \to E(\mathbb{F}_p)$. Its kernel is isomorphic to $\mathbb{Z}_p$, so we get a short exact sequence

$$0 \to \mathbb{Z}_p^3 \to A(\mathbb{Q}_p) \xrightarrow{\mathrm{red}_p} A(\mathbb{F}_p) \to 0.$$

By [Jossen and Perucca 2010], there exists an element $x \in X$ such that $\mathrm{red}_p(P) = \mathrm{red}_p(x)$ in $A(\mathbb{F}_p)$. Because $\mathbb{Z}_p$ is uniquely ℓ-divisible, we can define $Q_i := \ell^{-i} n(P - x)$ and get $\ell^i Q_i + nx = nP$.

<u>Case 2</u> (bad reduction at p and $p \neq \ell$). Condition (1) in Section 7.5 ensures that nP is ℓ-divisible in $A(\mathbb{Q}_p)$ for bad $p \neq \ell$, so the class of P in $A(\mathbb{Q}_p)/X$ is ℓ-divisible as well.

<u>Case 3</u> ($p = \ell$). For all $i \geq 0$, the subgroup $p^i A(\mathbb{Q}_p)$ is open in $A(\mathbb{Q}_p)$; hence, by condition (2) in Section 7.5, the intersection $X \cap (nP + p^i A(\mathbb{Q}_p))$ is nonempty. But that means that there exists an element $Q_i \in A(\mathbb{Q}_p)$ and an element $x_i \in X$ such that $p^i Q_i + x_i = nP$, just as needed.

8. Open questions and problems

I present three open arithmetic questions and an elementary problem in linear algebra, which so far have defied all attempts of being solved. The first question is about how far finitely generated subgroups of a Mordell–Weil group are detectable by reduction maps. It is a sharpened version of the problem that in the literature is named the problem of *detecting linear dependence*.

Question 8.1. Let G be a semiabelian variety defined over a number field k, and let X be a finitely generated subgroup of $G(k)$. Denote by $\overline{X} \subseteq G(k)$ the subgroup of those points P such that for almost all finite primes $\mathfrak{p}$ of k the reduction $P \bmod \mathfrak{p}$ belongs to $X \bmod \mathfrak{p}$ in $G(\kappa_{\mathfrak{p}})$. Let $M = [u : Y \to G]$ be a 1-motive where Y is constant and $X = u(Y)$. Is it true that the map

$$\overline{X}/X \otimes \mathbb{Z}_\ell \to H^1_*(k, \mathrm{T}_\ell M)$$

induced by the injection $H^0(k, M) \otimes \mathbb{Z}_\ell \to H^1(k, \mathrm{T}_\ell M)$ is an isomorphism?

A positive answer to this question was given in [Jossen 2013a] in the case where G is a geometrically simple abelian variety. In this case, we know that $H^1_*(k, T_\ell M)$ is trivial and get a nice local-global principle for subgroups of Mordell–Weil groups. Apart from a few other isolated examples, the question remains open, even in the cases where G is an abelian variety or a torus. The second question is similar in nature, but we impose a stronger local condition.

Question 8.2. Let G be a semiabelian variety defined over a number field k, let X be a finitely generated subgroup of $G(k)$, and let $P \in G(k)$ be a rational point. Suppose that for *all* finite primes $\mathfrak{p}$ of k the point P belongs to the closure of X in $G(k_\mathfrak{p})$ for the p-adic topology on $G(k_\mathfrak{p})$. Does then P belong to X?

We know the answer to be positive if G is a simple abelian variety and in some other scattered examples. If we could choose the integer n in Section 7.5 *independently of* ℓ, the answer to the question would be negative. Thirdly, I would like to ask for a converse to Theorem 6.1.

Question 8.3. Let k be a number field for which the statement of Leopoldt's conjecture holds. For which 1-motives $M = [Y \to G]$, where G is a torus, is the pairing

$$\text{III}^0(k, M) \times \text{III}^2(k, M^\vee) \to \mathbb{Q}/\mathbb{Z}$$

of Theorem 3 a perfect pairing of finite groups? In general, can we compute the dimension of $\text{III}^1(k, V_\ell M)$? How does this dimension vary with ℓ?

The second part of this question can as well be formulated for general mixed Artin–Tate motives. At last, motivated by the proof of Theorem 4.1, let me state a problem in linear algebra that any first-year student can understand.

Problem. Let K be a field, and write E for the K-algebra of $n \times n$ matrices with coefficients in K. Denote by V and V_0 the E-modules of $n \times m$ and $n \times m_0$ matrices, respectively. Finally, let W be a K-linear subspace of V, and define

$$\overline{W} := \{v \in V \mid f(v) \in f(W) \text{ for all } f \in \text{Hom}_E(V, V_0)\},$$

so $\overline{W}$ is a linear subspace of V containing W. Observe that elements of $\text{Hom}_E(V, V_0)$ are just $m \times m_0$ matrices by Schur's lemma. The problem is to compute $\overline{W}$. This means find an algorithm that takes as an input a K-basis of W (this will be some finitely many $n \times m$ matrices) and provides a basis of $\overline{W}$ or equivalently provides some finitely many $f_1, \ldots, f_r \in \text{Hom}_E(V, V_0)$ such that

$$\overline{W} = \{v \in V \mid f_i(v) \in f_i(W) \text{ for } i = 1, 2, \ldots, r\}.$$

Changing scalars from K to a bigger field may result in a smaller dimensional $\overline{W}$ (i.e., the inclusion of Lemma 4.3 may be strict). Yet, I don't know of a solution to the problem even in the case where K is algebraically closed.

Acknowledgements

References

[Breen 1969a] L. Breen, "Extensions of abelian sheaves and Eilenberg–MacLane algebras", *Invent. Math.* **9** (1969), 15–44. MR 41 #3488 Zbl 0181.26401

[Breen 1969b] L. S. Breen, "On a nontrivial higher extension of representable abelian sheaves", *Bull. Amer. Math. Soc.* **75** (1969), 1249–1253. MR 41 #211 Zbl 0184.46602

[Deligne 1974] P. Deligne, "Théorie de Hodge, III", *Inst. Hautes Études Sci. Publ. Math.* 44 (1974), 5–77. MR 58 #16653b Zbl 0237.14003

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Faltings and Chai 1990] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **22**, Springer, Berlin, 1990. MR 92d:14036 Zbl 0744.14031

[Gille and Szamuely 2006] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press, 2006. MR 2007k:16033 Zbl 1137.12001

[Harari and Szamuely 2005] D. Harari and T. Szamuely, "Arithmetic duality theorems for 1-motives", *J. Reine Angew. Math.* **578** (2005), 93–128. MR 2006f:14053 Zbl 1088.14012

[Harari and Szamuely 2009] D. Harari and T. Szamuely, "Corrigenda for: Arithmetic duality theorems for 1-motives", *J. Reine Angew. Math.* **632** (2009), 233–236. MR 2010i:14079 Zbl 1172.14029

[Hindry 1988] M. Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94**:3 (1988), 575–603. MR 89k:11046 Zbl 0638.14026

[Jossen 2013a] P. Jossen, "Detecting linear dependence on an abelian variety via reduction maps", *Comment. Math. Helv.* **88**:2 (2013), 323–352. MR 3048189 Zbl 06176450

[Jossen 2013b] P. Jossen, "On the Mumford–Tate conjecture for 1-motives", *Inventions Math.* (2013).

[Jossen and Perucca 2010] P. Jossen and A. Perucca, "A counterexample to the local-global principle of linear dependence for abelian varieties", *C. R. Math. Acad. Sci. Paris* **348**:1-2 (2010), 9–10. MR 2011c:11094 Zbl 1219.11089

[Lazard 1965] M. Lazard, "Groupes analytiques *p*-adiques", *Inst. Hautes Études Sci. Publ. Math.* 26 (1965), 389–603. MR 35 #188 Zbl 0139.02302

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980. MR 81j:14002 Zbl 0433.14012

[Milne 1986] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics **1**, Academic, Boston, 1986. MR 88e:14028 Zbl 0613.14019

[Mumford 1970] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1970. MR 44 #219 Zbl 0223.14022

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2000. MR 2000j:11168 Zbl 0948.11001

[Oort 1966] F. Oort, *Commutative group schemes*, Lecture Notes in Mathematics **15**, Springer, Berlin, 1966. MR 35 #4229 Zbl 0216.05603

[Ribet 1976] K. A. Ribet, "Dividing rational points on Abelian varieties of CM-type", *Compositio Math.* **33**:1 (1976), 69–74. MR 54 #12781 Zbl 0331.14020

[Serre 1964] J.-P. Serre, "Sur les groupes de congruence des variétés abéliennes", *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 3–20. MR 28 #3994 Zbl 0128.15601

[Serre 1971] J.-P. Serre, "Sur les groupes de congruence des variétés abéliennes, II", *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 731–737. MR 44 #6702 Zbl 0222.14025

[SGA 3 II] A. Grothendieck et al., *Séminaire de géométrie algébrique du Bois-Marie* 1962/64: *Schémas en groupes (SGA 3), II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, reprinted as Lecture Notes in Mathematics **152**, Springer, Berlin, 1970. MR 43 #223b Zbl 0209.24201

[SGA 5] A. Grothendieck et al., *Séminaire de géométrie algébrique du Bois-Marie* 1965–66: *Cohomologie ℓ-adique et fonctions L (SGA 5)*, reprinted as Lecture Notes in Mathematics **589**, Springer, Berlin, 1977. MR 58 #10907 Zbl 0345.00011

[SGA 7 I] A. Grothendieck et al., *Séminaire de géométrie algébrique du Bois-Marie* 1967–1969: *Groupes de monodromie en géométrie algébrique (SGA 7 I)*, reprinted as Lecture Notes in Mathematics **288**, Springer, Berlin, 1972. MR 50 #7134 Zbl 0237.00013

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, 1994. MR 95f:18001 Zbl 0797.18001

peter.jossen@gmail.com   *CNRS, UMR 8628, Mathématiques, Université Paris-Sud, Bâtiment 425, 91450 Orsay, France*

Algebra & Number Theory

msp.org/ant

Algebra & Number Theory