–

On the arithmetic of 1–motives

Peter Jossen

Submitted to
Central European University
Department of mathematics and its applications

In partial fulfilment of the requirements for the degree of
Doctor of Philosophy in Mathematics

Supervisor: Tamás Szamuely

Committee: David Harari
Gergely Harcos
René Schoof

Chair: Péter Pál Pálfy

Budapest, 2009

Abstract

This thesis deals with arithmetic aspects of 1–motives. We introduce *1–motives with torsion* generalizing Deligne's 1–motives and establish arithmetic duality theorems for them, generalizing earlier work of T.Szamuely and D.Harari.

We generalize results and techniques developed by J.-P.Serre in his work on the congruence subgroup problem for abelian varieties and a theorem of K.Ribet on Kummer fields associated with abelian varieties over number fields. We also generalize G.Faltings's theorem on homomorphisms of abelian varieties over number fields to 1–motives.

Combining duality theorems with Kummer theoretic results, we manage to prove that in some interesting cases the Tate–Shafarevich group $Ш^2(k, M)$ of a 1–motive M over a number field k is finite, answering thus partially a question of Harari and Szamuely.

Finally, we present an application of our techniques to the problem of "detecting linear dependence in a Mordell–Weil group".

The most exciting phrase to hear in science, the one that heralds new discoveries, is not *"Eureka!"* – but *"That's funny..."*.[a]

[a]Isaac Asimov

Introduction and Overview

The idea of *motives* was introduced more than 40 years ago by A. Grothendieck as "a systematic theory of arithmetic properties of algebraic varieties as embodied in their groups of classes of cycles" [**And04**]. Motives should be invariants attached to algebraic varieties that are of cohomological nature, in the sense that all cohomological features that are not specific to a single cohomology theory continue to exist for motives, and with respect to this property, motives should be universal. Such features that are not specific to one single cohomology theory include for example the existence of a cycle class map. Because this exists for deRham, for ℓ–adic and for crystalline cohomology, it must also exist for motives. Others are the existence of a weight filtration and a notion of purity, cup products, and homotopy invariance. To smooth proper varieties are associated pure motives, to general varieties mixed motives.

All this is what motives are supposed to somehow provide. Grothendieck gave a construction of a category of pure motives, and several constructions of categories of mixed motives which should be nontrivial extensions of pure ones have been suggested (e.g. by Voevodsky, Levine and others). However, at present no unconditional construction of mixed motives over a general base with all the expected properties exists.
Although this central problem remains unsolved, many partial steps towards this category have been taken and led to exciting, unconditional results. The most prominent being probably Voevodsky's proof of the Milnor conjecture in 1996, for which motivic cohomology is essential.

Already back as far as in 1974, P. Deligne [**Del74**] made with the introduction of *1–motives* literally a first step towards mixed motives: A 1–motive in the sense of Deligne should be an object of level ≤ 1 in the hypothetical category of mixed motives. And indeed, a theorem of Voevodsky (worked out by Orgogozo and later refined by Barbieri and Kahn, see [**KBV08**], Theorem 2.1.2) states that over a perfect field and up to inverting the exponential characteristic, Deligne's 1–motives generate the part of Voevodsky's triangulated category of mixed motives coming from varieties of dimension at most one. Compared with other more recent constructions, Deligne's is very concrete:

Définition ([**Del74**], 10.1.10). Un *1–motif lisse* M sur un schéma S consiste en:

a) un schéma en groupes Y sur S, qui localement pour la topologie étale est un schéma en groupes constant défini par un $\mathbb{Z}$–module libre de type fini, un schéma abélien A sur S, et un tore T sur S;
b) une extension G de A par T
c) un morphisme $u : Y \longrightarrow G$

Over a field k with algebraic closure $\overline{k}$, the group scheme Y in the definition corresponds to a finitely generated commutative group with a continuous action of the absolute Galois group $\mathrm{Gal}(\overline{k}|k)$. One attaches cohomology groups to a 1–motive M simply by looking at it as a complex of group schemes $[Y \longrightarrow G]$ put in degrees -1 and 0. Abelian schemes, tori and locally constant free $\mathbb{Z}$–modules of finite rank can be seen as special cases of 1–motives, by choosing the other components respectively to be trivial. These are the *pure* 1–motives.

The conjectures on the relations between special values of L–functions and regulators of Deligne, Beilinson and Bloch–Kato, all formulated in the 1980's in terms of motives, are natural generalizations of the Birch–Swinnerton-Dyer conjecture, and of classical results on zeta functions going back to Euler, Riemann and Dedekind. Thus, arithmeticians and number theorists have good reasons to be interested in motives, and particularly in 1–motives, since they present a handy testing ground for these conjectures (see section 4 of [**Jan94**]).

Arithmeticians have found two more reasons (at least) to be interested in 1–motives: First, they provide a natural way to unify and generalize *duality theorems* for the Galois cohomology of commutative group schemes over local and global fields. Secondly, 1–motives are a natural tool for studying *Kummer theory on semiabelian varieties* over a field. My thesis deals with these two aspects of 1–motives, which I shall describe now in some more detail.

Duality theorems. Duality theorems are among the most fundamental results in arithmetic, and the mother of all duality theorems is the theorem of Poitou and Tate for finite groups over a number field ([**Mil08**] Theorem 1.4.10a or [**NSW00**] Theorem 6.8.6). It states that if F is a finite commutative group scheme (Galois module) over a number field k with Cartier dual $F^\vee$, then there is a perfect pairing of finite groups

$$Ш^i(k, F) \times Ш^{3-i}(k, F^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

where $Ш^i(k, F)$ is the group of those cohomology classes in $H^i(k, F)$ that become trivial over every completion of k. In place of the finite group scheme F one can also take other commutative group schemes. For instance, if T is an algebraic torus over k with character group Y then there are canonical perfect pairings of finite groups

$$Ш^i(k, T) \times Ш^{3-i}(k, Y) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

([**NSW00**], Theorem 8.6.8 for i = 1, and [**Mil08**], Theorem I.4.20 for $i = 2$) For an abelian variety A over k, only the group $Ш^1(k, A)$ is interesting. It is a torsion group of finite corank, and it is widely conjectured that it is finite. There is again a canonical pairing

$$Ш^1(k, A) \times Ш^1(k, A^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

A theorem of Cassels (for elliptic curves) and Tate (for general abelian varieties) states that the left and right kernel of this pairing are the maximal divisible subgroups of $Ш^1(k, A)$ and $Ш^1(k, A^\vee)$

respectively ([**Mil08**], Theorem 6.26). In particular, the above is a perfect pairing if $Ш^1(k, A)$ and $Ш^1(k, A^\vee)$ are finite.

We have now stated duality theorems for all cases of pure 1–motives, namely for a torus T, for a locally free and finitely generated group Y and for an abelian variety A. The question that naturally arises, and which has been studied at large by D.Harari and T.Szamuely in [**HS05a**] is whether these duality theorems can be merged to one single duality theorem for 1–motives.
Indeed, for a 1–motive M, Deligne constructs a *dual 1–motive* $M^\vee$ which in the pure cases gives back the duality between tori and character groups, respectively duality for abelian varieties. Theorem 0.2 of [**HS05a**] (see also [**HS05b**]) states that there exist canonical pairings

$$Ш^i(k, M) \times Ш^{2-i}(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

and that these pairings are nondegenerate modulo divisible subgroups, provided one replaces $Ш^0(k, -)$ by a certain modification. It is shown in *loc.cit.* that $Ш^0(k, M)$ is finite, that $Ш^1(k, M)$ is finite provided this holds for the abelian variety coming with M, and it is conjectured that the group $Ш^2(k, M)$ is finite. From this theorem one recovers the duality theorems for tori and character groups, as well as the Cassels–Tate duality theorem.

What is slightly unsatisfactory about the pairings for 1–motives is that they do not generalize the pairings for finite groups, because 1–motives as introduced by Deligne do not contain the class of finite groups. To overcome this, one might try to introduce a category of 1–motives with torsion that contains Deligne's 1–motives as well as finite groups, and to generalize the duality theorem of Harari and Szamuely to this context[1].

This leads to my first main result. I propose a category of 1–motives with torsion $\mathcal{M}_1$ over a (noetherian regular) base scheme S containing Deligne's 1–motives as well as finite group schemes. I associate with every such 1–motive with torsion a dual 1–motive $M^\vee$ so to obtain a contravariant functor $(-)^\vee : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$. This functor extends Deligne's construction of the dual of torsion free 1–motives, as well as Cartier duality for finite flat group schemes[2]. Barbieri and Kahn also suggest a category of 1–motives with torsion in [**KBV08**], different from ours but certainly not unrelated (see [**Rus09**]). I show (Theorems 4.2.6 and 4.3.1)

Duality Theorem. *Let M be a 1–motive with torsion over a number field k, with dual $M^\vee$. There are canonical pairings*

$$Ш^i(k, M) \times Ш^{2-i}(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

These are nondegenerate modulo divisible subgroups and trivial for $i \neq 0, 1, 2$.

This duality theorem generalizes and unifies all arithmetic duality theorems I mentioned so far by making suitable specializations. The proof of the duality theorem is split into two parts, the case $i = 1$, and the case $i = 0, 2$. In the case $i = 1$ it follows classical arguments I have taken over from [**HS05a**], with only a few technical adaptations by myself. The proof in the case $i = 0, 2$ is new.
That $Ш^0(k, M)$ is finite is easy to prove as I already mentioned, and finiteness of $Ш^1(k, M)$ follows

[1]To perform this was the task with which this work originated. Besides, the question arised several times whether one could not generalize the whole theory to *Laumon* 1–motives, containing an additive factor. Probably this can be done, however, from the arithmetic standpoint this seems not to be very interesting since the additive group has trivial cohomology.

[2]Besides that these new 1–motives with torsion provide good duality theorems in arithmetic, this is what they are designed for, they are certainly of independent interest. For example if one studies the largest sub–Hodge structure of type $(0,0), (0,1), (1,0), (1,1)$ of $H^2_{\mathrm{dR}}(X, \mathbb{C})$, where X is a complex surface, 1–motives with torsion naturally arise, due to the fact that the Neron–Severi group of X may have torsion (see [**Car85**]).

from finiteness of $Ш^1(k,A)$ where A is the abelian part of M. That $Ш^1(k,A)$ is finite for all abelian varieties is widely conjectured, as a part of the Birch–Swinnerton-Dyer conjecture. The question remains whether $Ш^2(k,M)$ is finite. This is well–known to be the case for pure 1–motives. We shall set up a machinery that permits us to show finiteness of $Ш^2(k,M)$ also in some interesting mixed cases, for instance

Duality Theorem (bis). *Let $M = [Y \longrightarrow G]$ be a 1–motive over a number field k. If G is either a simple abelian variety, or else a 1–dimensional torus, then the canonical pairing*

$$Ш^0(k,M) \times Ш^2(k,M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups.

This is new, even for classical 1–motives. The general case however remains open for the time being, we do at present not even know whether for a general semiabelian variety G the group $Ш^2(k,G)$ is finite or not. Our method for proving finiteness of $Ш^2(k,M)$ heavily relies on methods developed by Serre in his work on the congruence subgroup problem for abelian varieties. In [**Ser64**] and [**Ser71**][3], Serre shows that if A is an abelian variety over a number field k, then every subgroup of $A(k)$ of finite index contains a subgroup which is defined by finitely many congruence relations. The link between this seemingly unrelated result of Serre and Tate–Shafarevich groups in degree 2 appears in [**Mil08**] (Theorem 6.26 and the remarks preceding it), where it is shown that triviality of $Ш^2(k,A)$ follows from the validity of the congruence subgroup problem for $A^\vee$, the dual of A. This also works for 1–motives.

Going through Serre's arguments with a 1–motive instead of an abelian variety, "mixedness phenomena" cause trouble at nearly every step. For mixed motives, endomorphism rings are not semisimple, Tate modules are no longer semisimple, the eigenvalues of Frobenius have different absolute values, and so on. These problems can often be handled using the nice interrelation between 1–motives and Kummer theory on semiabelian varieties. This leads us to Kummer theory. Step by step, the results I am about to present will lead to a criterion for $Ш^2(k,M^\vee)$ to be finite.

Kummer theory. To give a rational point P on a semiabelian variety G over a scheme U is the same as to give a 1–motive of the form $u : \mathbb{Z} \longrightarrow G$, setting $u(1) = P \in G(U)$. Studying rational points on semiabelian varieties can be translated in studying 1–motives with constant lattice $\mathbb{Z}$. That is of course just a matter of formulating things, but it can be very useful as we shall demonstrate. Probably for the first time this aspect of 1–motives was successfully used by K.Ribet and O.Jacquinot in [**JR87**] and [**Rib87**] in order to investigate so called *deficient* points on a semiabelian variety over a number field.

To explain what is really behind the connection between 1–motives and Kummer theory I need to introduce the ℓ–adic Tate module associated with a 1–motive, also known as the ℓ–adic realization of the given 1–motive. The construction is due to Deligne ([**Del74**] 10.1.10 and 10.1.11) and fits nicely into the big picture of motives and realizations. For a torsion free 1–motive M over a field k of characteristic $\neq \ell$, the ℓ–adic Tate–module is a finitely generated free $\mathbb{Z}_\ell$-module, and the Galois group of k acts continuously on $\mathrm{T}_\ell M$. If T, A and Y are the pure pieces of M, then $\mathrm{T}_\ell M$ is a twofold Galois module extension of the ordinary Tate modules $\mathrm{T}_\ell T$ and $\mathrm{T}_\ell A$, and $Y \otimes \mathbb{Z}_\ell$. In chapter 6 we shall prove

[3] the all–important suggestion to read this material came from David Harari.

Tate Property. *Let M_1 and M_2 be torsion free 1–motives over the number field k. Let $\overline{k}$ be an algebraic closure of k, set $\Gamma := \mathrm{Gal}(\overline{k}|k)$, and let ℓ be a prime number. The natural map*

$$\mathrm{Hom}_k(M_1, M_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_\Gamma(\mathrm{T}_\ell M_1, \mathrm{T}_\ell M_2)$$

is an isomorphism.

This theorem generalizes Falting's theorem on homomorphisms of abelian varieties over number fields ([**Fal83**]). Of course there will be a problem for our new 1–motives with torsion, for what should be the Tate module of a finite group scheme? We will define Tate modules for 1–motives with torsion, and show that the Tate property holds in this context as well. Let us stick to torsion free 1–motives for the introduction.

The relation between Tate modules and Tate–Shafarevich groups in degree 2 is again given by a duality: A simple application of the Poitou–Tate duality theorem for finite Galois modules shows that there is a perfect pairing of topological groups

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

Thus, showing finiteness of $Ш^2(k, M^\vee)$ is essentially the same as showing finiteness of $Ш^1(k, \mathrm{T}_\ell M)$ for all ℓ (and triviality for almost all ℓ). We need thus to understand action of $\Gamma := \mathrm{Gal}(\overline{k}|k)$ on the Tate module $\mathrm{T}_\ell M$, and that is what Kummer theory is all about. Naively, let us choose a $\mathbb{Z}_\ell$–basis $t_1, \ldots, t_r, a_1, \ldots, a_{2g}, y_1, \ldots, y_s$ of $\mathrm{T}_\ell M$ such that the t_i's form a $\mathbb{Z}_\ell$–basis of $\mathrm{T}_\ell T$, the a_i's a $\mathbb{Z}_\ell$–basis of $\mathrm{T}_\ell A$ and the y_i's a $\mathbb{Z}_\ell$–basis of $Y \otimes \mathbb{Z}_\ell$. Using this basis, the effect of an element $\sigma \in \Gamma$ acting on $\mathrm{T}_\ell M$ is given by a 3×3 upper triangular block matrix

$$\sigma = \left(\begin{array}{c|c|c} \sigma_T & * & * \\ \hline 0 & \sigma_A & * \\ \hline 0 & 0 & \sigma_Y \end{array}\right) \qquad\qquad * = \text{something}$$

On the diagonal blocks, we see the action of Γ on the pure parts of M. The extension data is encoded in the strictly upper triangular blocks. For instance, if for a 1–motive M the strictly upper triangular blocks are zero for all $\sigma \in \Gamma$, then $\mathrm{T}_\ell M$ splits into $\mathrm{T}_\ell T$, $\mathrm{T}_\ell A$ and $Y \otimes \mathbb{Z}_\ell$ as a Galois module, hence M itself splits, as you can see from the Tate property.

Let us write $L^M, L^G, L^A, \ldots$ and so on for the image of the Galois group Γ in the groups of $\mathbb{Z}_\ell$–linear automorphisms of $\mathrm{T}_\ell M, \mathrm{T}_\ell G, \mathrm{T}_\ell A, \ldots$ and so on. Then, write L^M_G for the subgroups of L^M consisting of those elements which act trivially on $\mathrm{T}_\ell G$ and $L^M_{T,A,Y}$ for the subgroups of L^M consisting of those elements which act trivially on $\mathrm{T}_\ell T$, $\mathrm{T}_\ell A$ and $Y \otimes \mathbb{Z}_\ell$, and so on. Elements of $L^M_{G,Y}$ for example are then block matrices as above with $\sigma_T = \mathrm{id}$, $\sigma_A = \mathrm{id}$, $\sigma_Y = \mathrm{id}$, and where the middle block in the top row is zero. Such matrices correspond to $\mathbb{Z}_\ell$–linear homomorphisms from $Y \otimes \mathbb{Z}_\ell$ to $\mathrm{T}_\ell G$. We find the so called *Kummer injection*

$$\vartheta : L^M_{G,Y} \longrightarrow \mathrm{Hom}(Y \otimes \mathbb{Z}_\ell, \mathrm{T}_\ell G)$$

It should of course be the case that, in a certain sense, the less M is split the bigger is the image of the Kummer injection. The following theorem indicates that such a principle indeed holds

Algebraicity Theorem. *Let $M = [u : \mathbb{Z}^r \longrightarrow A]$ be a 1–motive over k, where A is an abelian variety. Consider u as a rational point on the abelian variety $\mathcal{H}om(\mathbb{Z}^r, A) \cong A^r$, and let H^M_A be the smallest abelian subvariety of A^r containing a nonzero multiple of u. The image of the Kummer injection*

$$\vartheta : L^M_A \longrightarrow \mathrm{Hom}(\mathbb{Z}^r_\ell, \mathrm{T}_\ell A) \cong \mathrm{T}_\ell A^r \supseteq \mathrm{T}_\ell H^M_A$$

is contained and open in $\mathrm{T}_\ell H^M_A$. In particular, the Lie group L^M_A is algebraic and its dimension is independent of the prime ℓ.

Essentially this theorem is due to K.Ribet [**Rib76, Hin88**]. We prove it here for split semiabelian varieties, making heavy use of Faltings's results on the semisimplicity of the Tate module associated with an abelian variety over k. The statement for a nonsplit semiabelian variety in place of A is wrong in general.

The proof of this Theorem uses besides Faltings's results a powerful theorem of Bogomolov, stating that the group L^A, i.e. the image of Γ in $\mathrm{GL}\,\mathrm{T}_\ell A$ contains an open subgroup of the group of scalar matrices. Together with Bogomolov's theorem on the structure of L^A, we understand sufficiently well the group $H^1(L^M, \mathrm{T}_\ell M)$ in order to compute the following object,

$$H^1_*(L^M, \mathrm{T}_\ell M) := \ker\left(H^1(L^M, \mathrm{T}_\ell M) \longrightarrow \prod_{C \leq L^M} H^1(C, \mathrm{T}_\ell M)\right)$$

the product ranging over all monogenous subgroups of L^M (i.e. those topologically generated by a single element). The explanation what this group $H^1_*(L^M, \mathrm{T}_\ell M)$ is good for brings us back to Tate–Shafarevich groups. Let S be a set of places of the number field k of density 1, and consider

$$H^1_S(k, \mathrm{T}_\ell M) := \ker\left(H^1(k, \mathrm{T}_\ell M) \longrightarrow \prod_{v \in S} H^1(k_v, \mathrm{T}_\ell M)\right)$$

In the case S is the set of all places of k, the group $H^1_S(k, \mathrm{T}_\ell M)$ is nothing but the Tate–Shafarevich group of the Tate–module $\mathrm{T}_\ell M$. As Serre shows in [**Ser64**], it follows essentially from Frobenius's density theorem that there is an injection

$$H^1_S(k, \mathrm{T}_\ell M) \xrightarrow{\subseteq} H^1_*(L^M, \mathrm{T}_\ell M)$$

As O. Gabber pointed out to me, if S does not contain a finite list of "bad" places, this injection is even an equality. This injection is at the heart of Serre's solution to the congruence subgroup problem, and makes things work also for us. We see from it that finiteness of $H^1_*(L^M, \mathrm{T}_\ell M)$ implies finiteness of $H^1_S(k, \mathrm{T}_\ell M)$, hence of $Ш^1(k, \mathrm{T}_\ell M)$. Knowing L^M sufficiently well, we manage under some technical conditions to compute more or less explicitly the group $H^1_*(L^M, \mathrm{T}_\ell M)$, and to give reasonable criteria under which it is finite. For example:

THEOREM. *Let $M = [Y \longrightarrow G]$ be a 1–motive, where G is either a simple abelian variety or the multiplicative group. For every prime ℓ, the group $H^1_*(L^M, \mathrm{T}_\ell M)$ is finite. Hence so are $Ш^1(k, \mathrm{T}_\ell M)$ and $H^1_S(k, \mathrm{T}_\ell M)$, and the pairing*

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

is a perfect pairing of finite groups.

This leads to the additional statement to our duality theorem. The bad news is that working only with sets primes of density 1 and not with all places can not lead to a finiteness theorem valid for all 1–motives. Indeed, we shall give an example of a 1–motive M and a set of places S of density 1, for which $H^1_S(k, \mathrm{T}_\ell M)$ is not finite. For this special 1–motive we check by hand that nevertheless $Ш^1(k, \mathrm{T}_\ell M)$ is finite and even trivial for all ℓ, showing that $Ш^2(k, M^\vee)$ is trivial as well.

But there is also an advantage in working with sets primes of density 1. As a pleasant side result, we can solve to some extent an interesting problem in Kummer theory, often described (for instance in [**BGK05, GG09**] and [**Per08**]) as the problem of "detecting linear dependence in Mordell–Weil groups by reduction mod $\mathfrak{p}$". This is the following question asked by W. Gajda: Given an abelian variety A over a number field k, a subgroup X of $A(k)$ and a rational point $P \in A(k)$, is it true that P belongs to X if and only if the reduction of P belongs to the reduction of X for almost all primes of k? As we shall see, the answer is negative in general. Together with Antonella Perucca we have constructed a counter example, which we shall present it in section 8.3. However, if A is simple, this works:

Theorem. *Let k be a number field and let A be a simple abelian variety over k. Let $X \subseteq A(k)$ be a subgroup and let $P \in A(k)$ be a point. The point P belongs to X if and only if for almost all primes $\mathfrak{p}$ of k the point $(P \bmod \mathfrak{p})$ belongs to $(X \bmod \mathfrak{p})$.*

That such a thing might be true has been conjectured by several people, and the literature on this problem is quite vast. I give a short historical overview in section 8.1.

Description of the chapters

Chapter 1. We define a category of *1–motives with torsion* over a noetherian regular base scheme S and study its elementary properties. This new category of 1–motives with torsion contains the category of 1–motives in the sense of Deligne, and it also contains the category of finite flat group schemes over S. Moreover there exists a canonical duality functor extending both, duality for classical 1–motives as well as Cartier duality for finite flat group schemes.

Chapter 2. One of the very central objects in this work is the ℓ–adic Tate module associated with a 1–motive. In Chapter 2, we provide the necessary foundations that permit us to associate with any reasonable complex of group schemes a complex of ℓ–adic sheaves, which in the simplest cases gives back Tate modules as they are known. We check that these complexes of ℓ–adic sheaves feature what one naturally expects of them, for instance, some exactness properties and the existence of a Weil pairing.

Chapter 3. This chapter is to review some well and not so well–known material on cohomolore. We recall what we need about the interrelation between étale cohomology and Galois cohomology, the construction and elementary properties of compact support cohomology, some structure results for the cohomology of 1–motives, and the definition of Tate–Shafarevich groups and related local–to–global obstructions.
In section 3.5, we generalize duality theorems which are classically known for finite group schemes to bounded complexes of sheaves, whose homology groups are finite group schemes. Among them Theorem 3.5.9, the Poitou–Tate duality theorem for finite Galois modules over a number field.

Chapter 4. We prove the duality theorems. In a first section, we investigate local duality theorems over a p–adic field, generalizing the classical duality theorems of Tate and Nakayama for abelian varieties and tori over a p–adic field. In section 4.2 the duality theorem in the case $i = 0, 2$ as explained, admitting for the time being the Kummer theory results. In section 4.3, we prove the case $i = 1$ of the duality theorem, following the methods of [**HS05a**]. This uses only the generalization of the Poitou–Tate duality theorem to complexes of finite groups, and the local duality theorems.

Chapter 5. We introduce the various Lie groups mentioned in the introduction, and show how they are related. These Lie groups (associated with a 1–motive M over a number field k) act on the Tate module of M and its graded pieces, and we compute some of the arising cohomology. These computations are based on Bogomolov's theorem on the image of the absolute Galois group of k in the automorphism group of $\mathrm{T}_\ell A$ for an abelian variety A. In the last section, we link this Lie group cohomology to Galois cohomology via the functor H^1_* we also already mentioned.

Chapter 6. We prove the Tate property for 1–motives over a number field, as stated in the introduction. The proof makes of course heavy and repeated use of the Tate property for abelian varieties proven by Faltings. It uses also some Lie group computations from Chapter 5 relying on Bogomolov's theorem.

Chapter 7. This chapter mainly deals with Kummer theory on semiabelian varieties and its applications to finiteness theorems for 1–motives. In the first section we prove the algebraicity theorem stated in the introduction (Theorem 7.1.3), and apply it in section 7.2 to answer some Kummer–theoretic questions. In section 7.3 we use our algebraicity theorem to compute the group $H^1_*(L^M, \mathrm{T}_\ell M)$ under some technical assumptions on M. In a last section we present a few reasonable conditions under which the group $H^1_*(L^M, \mathrm{T}_\ell M)$, and hence $Ш^1(k, \mathrm{T}_\ell M)$ is finite for all ℓ. This leads to the additional statement to our duality theorem stated in the introduction.

Chapter 8. We give a brief historical overview on the problem of detecting linear dependence and prove the last theorem stated in the introduction. The last section is devoted to examples.

Acknowledgments

First of all, I would like to thank my supervisor Tamás Szamuely for guiding me through this work. He taught me to keep thinking about the details, to start with something half–way useful that solves some fairly immediate need, and not to get lost in some fancy design. It is thanks to him that there is some meat on the bones of this thesis.

I am very grateful to Grzegorz Banaszak, Luca Barbieri–Viale, David Harari, Wojciech Gajda, Philippe Gille, Cristian David Gonzalez–Avilés and Gisbert Wüstholz, who took their time to correspond with me. They had the patience to read my questions, shared generously their knowledge and gave me many hints on the literature I would not have found by myself.

Discussions with Antonella Perucca have led to considerable improvements and simplifications in chapter 7, and she was also a great help in working out one of the examples in chapter 8. I'm indebted to her and whoever is reading this thesis is, in fact, too.

My most heartfelt thanks go to my fellow students Anna Devic, Catalin Ghinea, Nivaldo de Góes Grulha Jr., Michele Klaus, David Kohler, Caroline Lassueur and Nicola Mazzari. They made travel documents from Iceland to Budapest, provided me with food, coffee, shelter and false identity whenever I needed.

I would like to express my gratitude to the following institutions for their hospitality. The Rényi intézet, the Università degli Studi di Milano where I could stay for a semester in 2007 upon the initiative of Luca Barbieri–Viale, the Ecole polytechnique fédérale de Lausanne, the Universität Regensburg and the École normale superieure where I presented parts of this work in its early state.

At last, I wish to express my sincere appreciation to Mr. Soproni Kékfrankos, and Mr. Egri Bika–Vér. Upon them I could rely when inspiration was missing, it was they who provided solace at the many occasions, and above all they proved to be the very best of companions when something was to be celebrated.

Contents

CHAPTER 1

1–motives with torsion

Throughout the whole chapter, S is a noetherian regular scheme, and $\mathcal{F}_S$ or just $\mathcal{F}$ stands for the category of sheaves of commutative groups on the fppf site over S. We write $\mathcal{DF}$ for the unbounded, and $\mathcal{D}^{\mathrm{b}}\mathcal{F}$ for the bounded derived category of $\mathcal{F}$. We identify the category of commutative group schemes which are locally of finite presentation over S with its essential image in $\mathcal{F}$ via the functor of points.
In particular, we say that a fppf sheaf on S is an abelian scheme or a finite flat group scheme if it can be represented by a such. By a *lattice over* S, we mean an object of $\mathcal{F}_S$ which is locally isomorphic to a free $\mathbb{Z}$–module of finite rank.

1.1. Definition, relation to classical 1–motives

In this section, we define the category of 1–motives with torsion, and discuss how it is related to the category of classical 1–motives in the sense of Deligne.

Definition 1.1.1. A 1*–motive* over S is a diagram

$$M = \left[\begin{tikzcd} & & Y \arrow[d, "u"'] & & \\ 0 \arrow[r] & X \arrow[r] & G \arrow[r] & A \arrow[r] & 0 \end{tikzcd}\right]$$

in the category $\mathcal{F}$ where

(1) the sheaf Y fits into an exact sequence $0 \longrightarrow F \longrightarrow Y \longrightarrow L \longrightarrow 0$, where F is a finite flat group scheme, and L is a lattice.
(2) the sheaf X fits into an exact sequence $0 \longrightarrow T \longrightarrow X \longrightarrow F \longrightarrow 0$ where F is a finite flat group scheme and where T is a torus.
(3) the sheaf A is an abelian scheme.
(4) the sequence $0 \longrightarrow X \longrightarrow G \longrightarrow A \longrightarrow 0$ is exact.

A morphism of 1–motives $\varphi : M_1 \longrightarrow M_2$ is a morphism between diagrams

$$\left[\begin{tikzcd} & & Y_1 \arrow[d] & & \\ 0 \arrow[r] & X_1 \arrow[r] & G_1 \arrow[r] & A_1 \arrow[r] & 0 \end{tikzcd}\right] \xrightarrow{\varphi_Y, \varphi_X, \varphi_G, \varphi_A} \left[\begin{tikzcd} & & Y_2 \arrow[d] & & \\ 0 \arrow[r] & X_2 \arrow[r] & G_2 \arrow[r] & A_2 \arrow[r] & 0 \end{tikzcd}\right]$$

I denote by $\mathcal{M}_{1,S}$ or $\mathcal{M}_1$ the resulting category and call it *category of* 1*–motives over* S.

– 1.1.2. A 1–motive in the sense of Deligne ([**Del74**], Section 10) is defined as in 1.1.1, but where $Y = L$ is a lattice, and where $X = T$ is a torus, so that G becomes a semiabelian scheme. We will call such 1–motives *torsion free*, and write $\mathcal{M}_1^{\mathrm{Del}}$ for the corresponding full subcategory in $\mathcal{M}_1$. In the literature ([**KBV08, Car85, Ram98**] and others), torsion–free 1–motives are often given by two term complexes $[Y \longrightarrow G]$, and morphisms by commutative squares

$$\begin{tikzcd} Y_1 \arrow[r] \arrow[d, "\varphi_Y"'] & G_1 \arrow[d, "\varphi_G"] \\ Y_2 \arrow[r] & G_2 \end{tikzcd}$$

This is no problem, morphisms between semiabelian schemes respect automatically their extension structures because there are no nontrivial morphisms from a torus to an abelian scheme. However, there are nontrivial morphisms from finite flat groups to abelian schemes. A morphism between 1–motives with torsion is thus not described just by its effect on Y_1 and G_1, and so it is essential to us to distinguish between the 1–motive M and the complex $[Y \longrightarrow G]$. In a recent work, H. Russell has introduced a category of 1–motives with unipotent part ([**Rus09**], Definition 2.10), containing our category of 1–motives with torsion.

DEFINITION 1.1.3. Let M be a 1–motive over S, as defined in 1.1.1. The *complex associated with* M is the complex of sheaves $[M] := [Y \longrightarrow G]$, placed in degrees -1 and 0.
I denote $[\mathcal{M}_1]$ the category of *1–motives up to quasi–isomorphism.* Its objects are the complexes $[M]$ where M is a 1–motive, and its morphisms are morphisms of complexes modulo homotopy, localized in the class of quasi–isomorphisms.

– 1.1.4. The class of quasi–isomorphisms is a *localizing class* in the sense of [**MG96**] Definition III.2.6. By Lemma III.2.8 of *loc.cit.*, morphisms $f : [M_1] \longrightarrow [M_2]$ in $[\mathcal{M}_1]$ can be represented by a "hat"

$$\begin{tikzcd} & {[M_2']} & \\ {[M_1]} \arrow[ur, "f'"] & & {[M_2]} \arrow[ul, "\iota"'] \end{tikzcd}$$

where f' is a morphism of complexes, and where ι is a quasi–isomorphism. One usually writes $f = \iota^{-1}f'$. The morphism ι or its formal inverse are isomorphisms in $[\mathcal{M}_1]$. Mind that the functor $[-] : \mathcal{M}_1 \longrightarrow [\mathcal{M}_1]$ is neither full nor faithful, and it happens that $[M] = [M']$ without M and M' being isomorphic.
We usually look at $[\mathcal{M}_1]$ as being a subcategory of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_S$. There is a subtle point to observe. Morphisms $[M_1] \longrightarrow [M_2]$ in $\mathcal{D}^{\mathrm{b}}\mathcal{F}_S$ are represented by hats of the form

$$\begin{tikzcd} & C & \\ {[M_1]} \arrow[ur, "f'"] & & {[M_2]} \arrow[ul, "\iota"'] \end{tikzcd}$$

where C is any bounded complex, not necessarily homotopic to a complex of the form $[M_2']$. Presumably $[\mathcal{M}_1]$ is full in $\mathcal{D}^{\mathrm{b}}\mathcal{F}$, meaning that every hat as the above is equivalent to a hat where $C = [M_2']$ for a 1–motive M_2', but we do not know this for sure.

DEFINITION 1.1.5. A morphism of 1–motives $\varphi : M_1 \longrightarrow M_2$ is called an *isogeny* if the kernels and cokernels of the induced morphisms φ_Y, φ_X and φ_A are all finite.

– 1.1.6. We say that a sequence of morphisms of 1–motives $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ is a *short exact sequence*[1] if the induced sequences of sheaves $0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow Y_3 \longrightarrow 0$ and

[1]For us, this is just a handy terminology. The category $\mathcal{M}_1$ is not an abelian category, and we are not going to claim that this notion of exactness will lead to anything like an *exact structure* on $\mathcal{M}_1$.

$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X_3 \longrightarrow 0$ and $0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$ are exact. Such a short exact sequence of 1–motives yields then an exact triangle

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

in the derived category $\mathcal{D}^{\mathrm{b}}\mathcal{F}_S$. With a 1–motive M over S are naturally associated several short exact sequences coming from the so called *weight filtration* on M. This is a three term filtration given by $W_iM = 0$ if $i \leq -3$ and $W_iM = M$ if $i \geq 0$ and

$$W_{-2}M := \left[\begin{array}{c} \begin{tikzcd} & & 0 \arrow[d] & & \\ 0 \arrow[r] & X \arrow[r, equal] & X \arrow[r] & 0 \arrow[r] & 0 \end{tikzcd} \end{array}\right] \qquad \text{and} \qquad W_{-1}M := \left[\begin{array}{c} \begin{tikzcd} & & 0 \arrow[d] & & \\ 0 \arrow[r] & X \arrow[r] & G \arrow[r] & A \arrow[r] & 0 \end{tikzcd} \end{array}\right]$$

Remark that the filtrations are endofunctors $W_i : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$ such that $W_i \circ W_i = W_i$. Even if $\mathcal{M}_1$ is not an abelian category, the quotients W_iM/W_jM for $i \geq j$ make sense in an obvious way:

$$M/W_{-1}M := \left[\begin{array}{c} \begin{tikzcd} & & Y \arrow[d] & & \\ 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \end{tikzcd} \end{array}\right] \qquad \text{and} \qquad M/W_{-2}M := \left[\begin{array}{c} \begin{tikzcd} & & Y \arrow[d] & & \\ 0 \arrow[r] & 0 \arrow[r] & A \arrow[r, equal] & A \arrow[r] & 0 \end{tikzcd} \end{array}\right]$$

Given a 1–motive M, we will often write M_A for the 1–motive $M/W_{-2}M$. There are natural morphisms of 1–motives which fit into a diagram with exact rows and columns

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & & \\ & W_{-2}M \arrow[r, equal] \arrow[d] & W_{-2}M \arrow[d] & & \\ 0 \arrow[r] & W_{-1}M \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M/W_{-1}M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & W_{-1}M/W_{-2}M \arrow[r] \arrow[d] & M/W_{-2}M \arrow[r] \arrow[d] & M/W_{-1}M \arrow[r] & 0 \\ & 0 & 0 & & \end{tikzcd}$$

These morphisms induce exact triangles $[W_iM] \longrightarrow [M] \longrightarrow [M/W_iM]$. However, it is not true that the functors $W_i : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$ induce functors $[\mathcal{M}_1] \longrightarrow [\mathcal{M}_1]$.

Proposition 1.1.7. *Let M_1 and M_2 be 1–motives, and let $f : [M_1] \longrightarrow [M_2]$ be a morphism of complexes. There exists a 1–motive M_2' and a morphism $\varphi : M_1 \longrightarrow M_2'$ such that $[M_2] = [M_2']$ and $f = [\varphi]$.*

Proof. The 1–motives M_1 and M_2 and the morphism of complexes f yield altogether a commutative diagram (with the obvious notation)

$$\begin{tikzcd} & & & Y_1 \arrow[dl, "u_1"'] \arrow[dd, "f_Y"] & & \\ 0 \arrow[r] & X_1 \arrow[r] & G_1 \arrow[rr] \arrow[dd, "f_G"'] & & A_1 \arrow[r] & 0 \\ & & & Y_2 \arrow[dl, "u_2"] & & \\ 0 \arrow[r] & X_2 \arrow[r] & G_2 \arrow[rr] & & A_2 \arrow[r] & 0 \end{tikzcd}$$

The image of X_1 in A_2 is affine and proper, hence finite. Write A_2' for the quotient of A_2 by this image, and write X_2' for the kernel of $G_2 \longrightarrow A_2'$. Define M_2' to be

$$M_2 = \left[\begin{tikzcd} & & Y_2 \arrow[d, "u_2"'] & & \\ 0 \arrow[r] & X_2' \arrow[r] & G_2 \arrow[r] & A_2' \arrow[r] & 0 \end{tikzcd}\right]$$

By diagram chase, there is a (unique) morphism of 1–motives $\varphi : M_1 \longrightarrow M_2'$ such that $f_Y = \varphi_Y$ and $f_G = \varphi_G$. □

PROPOSITION 1.1.8. *The functor* $[-] : \mathcal{M}_1^{\mathrm{Del}} \longrightarrow [\mathcal{M}_1]$ *is fully faithful.*

PROOF. Let M_1 and M_2 be torsion free 1–motives, and let $\varphi : [M_1] \longrightarrow [M_2]$ be a morphism of complexes. All we have to show is that if φ is a quasi–isomorphism, then it is an isomorphism of complexes. From φ we get a commutative diagram with exact rows and columns

$$\begin{tikzcd} & & 0 \arrow[d] & 0 \arrow[d] & & \\ & & \ker\varphi_Y \arrow[r] \arrow[d] & \ker\varphi_G \arrow[d] & & \\ 0 \arrow[r] & \ker u_1 \arrow[r] \arrow[d, "\cong"'] & Y_1 \arrow[r, "u_1"] \arrow[d, "\varphi_Y"'] & G_1 \arrow[r] \arrow[d, "\varphi_G"] & \operatorname{coker} u_1 \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & \ker u_2 \arrow[r] & Y_2 \arrow[r, "u_2"] \arrow[d] & G_2 \arrow[r] \arrow[d] & \operatorname{coker} u_2 \arrow[r] & 0 \\ & & \operatorname{coker}\varphi_Y \arrow[r] \arrow[d] & \operatorname{coker}\varphi_G \arrow[d] & & \\ & & 0 & 0 & & \end{tikzcd}$$

To say that φ is a quasi–isomorphism is to say that it induces an isomorphism between the kernels and cokernels of u_1 and u_2 as indicated. By diagram chase, this is equivalent to saying that the induced morphisms $\ker\varphi_Y \longrightarrow \ker\varphi_G$ and $\operatorname{coker}\varphi_Y \longrightarrow \operatorname{coker}\varphi_G$ are isomorphisms. But this can not happen unless these kernels and cokernels are trivial. Indeed, on one hand $\ker\varphi_Y$ is a locally constant sheaf locally isomorphic to a finitely generated free group. On the other hand $\ker\varphi_G$ is a subgroup scheme of a semiabelian variety, so its connected component is a semiabelian variety which has finite index in $\ker\varphi_G$. Thus, the only possibility for $\ker\varphi_Y$ and $\ker\varphi_G$ to be isomorphic is that both are trivial. Also, $\operatorname{coker}\varphi$ is locally constant isomorphic to a finitely generated group, whereas $\operatorname{coker}\varphi$ is divisible as a sheaf, since G is so. Again, the only possibility for $\operatorname{coker}\varphi_Y$ and $\operatorname{coker}\varphi_G$ to be isomorphic is that both be trivial. □

1.2. On $\mathcal{E}xt$–sheaves and the Barsotti–Weil formula

We shall recall the statement of the Barsotti–Weil formula and present a mild generalization of it. Then, we collect some useful facts about sheaves of extensions.

– 1.2.1. Let A be an abelian scheme over S, and consider an extension of commutative group schemes $0 \longrightarrow \mathbb{G}_m \longrightarrow G \longrightarrow A \longrightarrow 0$ over S. We can look at G as being a $\mathbb{G}_m$–torsor over A, and get this way an element of $H^1(A, \mathcal{O}_A^*) = \operatorname{Pic}(A/S)$. The Barsotti–Weil formula states that this procedure induces an isomorphism from $\operatorname{Ext}^1_S(A_S, \mathbb{G}_m)$ to $\operatorname{Pic}^0(A/S) = A^\vee(S)$.

THEOREM 1.2.2 ([**Oor66**], III.18.1). *Let A be an abelian scheme over S. There is a canonical and natural isomorphism of groups*

$$\mathrm{Ext}^1_S(A, \mathbb{G}_m) \longrightarrow A^\vee(S)$$

This isomorphism commutes with base change, hence induces a canonical isomorphism $A^\vee \cong \mathcal{E}xt^1(A, \mathbb{G}_m)$ of fppf sheaves.[2]

Now if $\mathbb{Z}$ denotes the constant sheaf with value $\mathbb{Z}$ on S, then we have of course $A^\vee \cong \mathcal{H}om(\mathbb{Z}, A^\vee)$, so that the above isomorphism reads $\mathcal{E}xt^1_S(A, \mathbb{G}_m) \longrightarrow \mathcal{H}om(\mathbb{Z}, A^\vee)$. The generalization we have in mind consists of replacing $\mathbb{G}_m$ by an extension of a finite flat group scheme by a torus, and $\mathbb{Z}$ by its Cartier dual.

PROPOSITION 1.2.3. *Let X be an extension of a finite flat group scheme by a torus, let $X^\vee$ be the Cartier dual of X, and let A be an abelian scheme with dual $A^\vee$. There is a canonical isomorphism*

$$\mathrm{Ext}^1(A, X) \xrightarrow{\cong} \mathrm{Hom}(X^\vee, A^\vee)$$

functorial in A, X and S. In particular, there is an isomorphism $\mathcal{E}xt^1(A, X) \cong \mathcal{H}om(X^\vee, A^\vee)$ of fppf sheaves over S which is functorial in A and X.

The proof is not very difficult once we have some more material at hand. We postpone it until then. What we shall need not only for the proof of 1.2.3, but also on several occasions later is some information about the sheaves of higher extensions $\mathcal{E}xt^i(A, \mathbb{G}_m)$. These sheaves arise as the homology of the derived functor $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$, or alternatively by sheafifying the presheaf

$$(U \xrightarrow{\text{fppf}} S) \quad \longmapsto \quad \mathrm{Ext}^i_U(A_U, \mathbb{G}_{m,U})$$

on S. For $i = 0, 1$ these sheaves are well understood. For $i \geq 2$ we know from works of L.Breen that these are torsion sheaves. We can easily handle their ℓ–primary part whenever ℓ is a prime invertible on S. In contrast, not much is known about their p–primary part when p is any of the residual characteristics of S.

LEMMA 1.2.4. *Let F be a group scheme over S which is locally constant isomorphic to a finitely generated group. Then, $\mathcal{E}xt^i(F, -) = 0$ for all $i \geq 2$. In particular $\mathcal{E}xt^i(F, \mathbb{G}_m) = 0$ for all $i \geq 1$.*

PROOF. It suffices to show that the sheaf $\mathcal{E}xt^i(F, H)$ is trivial on each fppf open $U \longrightarrow S$ on which F is constant. We may thus suppose without loss of generality that F is constant, defined by a commutative group of finite type which we still denote by F. There exists a short exact sequence of groups

$$0 \longrightarrow \mathbb{Z}^s \xrightarrow{\alpha} \mathbb{Z}^r \longrightarrow F \longrightarrow 0$$

which we can regard as a short exact sequence of constant sheaves as well. The functor $\mathcal{H}om(\mathbb{Z}^r, -) : \mathcal{F} \longrightarrow \mathcal{F}$ is obviously exact. Therefore, we have $\mathcal{E}xt^i(\mathbb{Z}^r, H) = 0$ for $i > 0$, hence $\mathcal{E}xt^i(F, H) = 0$ for $i > 1$. For the additional statement, we just need to see that $\mathcal{E}xt^1(F, \mathbb{G}_m) = 0$. This is indeed true for any finite flat group scheme F by [**Oor66**] Theorem III.16.1, and we have already seen that $\mathcal{E}xt^i(\mathbb{Z}^r, \mathbb{G}_m) = 0$. □

[2]Oort makes the additional hypothesis that either A is projective over S, or that S is artinian. The trouble is caused only by Prop. I.5.3 in *loc.cit.*, where representability of the Picard functor $T \longmapsto \mathrm{Pic}\, A/T$ is known just in these cases. This problem has been overcome by M. Raynaud ([**FC90**], Theorem 1.9).

Theorem 1.2.5. *Let X be either a finite flat group scheme, a torus or a lattice over S, and let A and B be abelian schemes over S. The following holds:*

(1) *The sheaf $\mathcal{H}om(X, \mathbb{G}_m)$ is represented by the Cartier dual of X, and $\mathcal{E}xt^1(X, \mathbb{G}_m) = 0$.*
(2) *The sheaves $\mathcal{H}om(A, \mathbb{G}_m)$ and $\mathcal{E}xt^2(A, \mathbb{G}_m)$ are trivial, and $\mathcal{E}xt^1(A, \mathbb{G}_m)$ is represented by $A^\vee$.*
(3) *The sheaf $\mathcal{H}om(A, B)$ is a lattice, and $\mathcal{E}xt^1(A, B)$ is a torsion sheaf.*

For all $i \geq 2$, the sheaves $\mathcal{E}xt^i(X, \mathbb{G}_m)$, $\mathcal{E}xt^i(A, \mathbb{G}_m)$ and $\mathcal{E}xt^i(A, B)$ are torsion. If ℓ is a prime number invertible on S, these sheaves contain no ℓ–torsion.

Proof. In the case X is a finite flat group scheme, the statements of (1) can be found in [**Oor66**], Theorem III.16.1. For constant group schemes and tori, these follow from [**Gro66a**] exp. XIII cor. 1.4 and [**Gro66b**] exp. VIII prop. 3.3.1 respectively.
In (2), we have $\mathcal{H}om(A, \mathbb{G}_m) = 0$ because A is proper and geometrically connected, and $\mathbb{G}_m$ is affine. The isomorphism $\mathcal{E}xt^1(A, \mathbb{G}_m) \cong A^\vee$ is given by the Barsotti–Weil formula 1.2.2. It is shown in [**Bre69**] that (over a noetherian regular base scheme, as we suppose S to be) the sheaves $\mathcal{E}xt^i(A, \mathbb{G}_m)$ are torsion for all $i > 1$. Using the second statement of (1), we see that for $n > 0$, the multiplication by n on $\mathcal{E}xt^2(A, \mathbb{G}_m)$ is injective, hence $\mathcal{E}xt^2(A, \mathbb{G}_m) = 0$.
That $\mathcal{H}om(A, B)$ is a lattice follows from the well known fact that over any field, the group of homomorphisms between two abelian varieties is a finitely generated free group. That the sheaves $\mathcal{E}xt^i(A, B)$ are torsion for $i \geq 1$ is proven in [**Bre69**].
Now let ℓ be a prime number which is invertible on S. Finite flat group schemes over S of exponent ℓ are then étale, hence locally constant. It follows then from Lemma 1.2.4 that $\mathcal{E}xt^i(X, \mathbb{G}_m)$, $\mathcal{E}xt^i(A, \mathbb{G}_m)$ and $\mathcal{E}xt^i(A, B)$ have no ℓ–torsion. □

– 1.2.6. Recall (e.g. from [**KS06**], Definition 12.3.1) that for each $n \in \mathbb{Z}$ there is a canonical truncation functor $(-)_{\leq n} : \mathcal{DF} \longrightarrow \mathcal{DF}$ and a canonical morphism of functors $(-)_{\leq n} \longrightarrow \mathrm{id}_{\mathcal{DF}}$ with the property that for each object C of $\mathcal{D}^{\mathrm{b}}\mathcal{F}$

$$H^i(A_{\leq n}) = \begin{cases} H^i(A) & \text{if } i \leq n \\ 0 & \text{if } i > n \end{cases}$$

Recall (e.g. from [**GBH**$^+$**66**] Exposé I, following Proposition 1.6) that for every two objects A and B of $\mathcal{DF}$, there is a canonical and natural *evaluation* morphism

$$A \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{R}\mathcal{H}om(A, B), B)$$

We consider the functor $(-)^D := \mathbb{R}\mathcal{H}om(-, \mathbb{G}_m[1])_{\leq 0}$ from the category $\mathcal{DF}$ to itself. Combining truncation and evaluation, we find for every object A of $\mathcal{DF}$ a canonical and natural evaluation morphism

$$\epsilon_A : A_{\leq 0} \longrightarrow A^{DD}$$

that is, a functor morphism $\epsilon_{(-)} : (-)_{\leq 0} \longrightarrow (-)^D \circ (-)^D$. Indeed, given an object A of $\mathcal{DF}$, one considers first the morphism

$$A \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{R}\mathcal{H}om(A, \mathbb{G}_m[1]), \mathbb{G}_m[1]) \longrightarrow \mathbb{R}\mathcal{H}om(A^D, \mathbb{G}_m[1])$$

where the first map is the usual evaluation map, and where the second map is induced by the canonical morphism $A^D = \mathbb{R}\mathcal{H}om(A, \mathbb{G}_m[1])_{\leq 0} \longrightarrow \mathbb{R}\mathcal{H}om(A, \mathbb{G}_m[1])$. Then, one applies $(-)_{\leq 0}$ and finds ϵ_A.

PROOF OF 1.2.3. We will construct in a canonical way two isomorphisms, inverse to each other.

$$\mathrm{Hom}(X^\vee, A^\vee) \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathrm{Ext}^1(A, X)$$

Let $f : X^\vee \longrightarrow A^\vee$ be a morphism of sheaves, and let $\xi \in \mathrm{Ext}^1(A, X)$ be an extension of sheaves, represented by an exact sequence $0 \longrightarrow X \longrightarrow E \longrightarrow A \longrightarrow 0$. We find exact triangles in $\mathcal{DF}$

$$\triangle_f := \big[A^\vee \longrightarrow C(f) \longrightarrow X^\vee[1] \longrightarrow A^\vee[1]\big] \qquad \text{and} \qquad \triangle_\xi := \big[X \longrightarrow E \longrightarrow A \xrightarrow{0} X[1]\big]$$

where $C(f) = [X^\vee \xrightarrow{f} A^\vee]$ is the cone of f, placed in degrees -1 and 0. We will now define Φ and Ψ, and show on the way that the triangles $(\triangle_f)^D$ and $(\triangle_\xi)^D$ are exact as well.

Applying $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m[1])$ to the triangle $\triangle_f$ yields the following exact sequence

$$\cdots \longrightarrow 0 \longrightarrow \underbrace{\mathcal{H}om(X^\vee, \mathbb{G}_m)}_{=X^{\vee\vee}\cong X} \longrightarrow \mathcal{E}xt^1(C(f), \mathbb{G}_m) \longrightarrow \underbrace{\mathcal{E}xt^1(A^\vee, \mathbb{G}_m)}_{=A^{\vee\vee}\cong A} \longrightarrow 0 \longrightarrow \cdots$$

By Theorem 1.2.5, the sheaves $\mathcal{H}om(A^\vee, \mathbb{G}_m)$ and $\mathcal{E}xt^1(X^\vee, \mathbb{G}_m)$ are trivial, whence the zeroes in this sequence. The Cartier duality theorem, respectively the duality theorem for abelian schemes states that the evaluation morphism induces isomorphisms of sheaves $X \cong X^{\vee\vee}$ and $A \cong A^{\vee\vee}$ as indicated. Truncating in degree zero, we remain with the exact triangle

$$(\triangle_f)^D = \big[X \longrightarrow C(f)^D \longrightarrow A \xrightarrow{0} X[1]\big]$$

This way we got an extension of A by X, which we denote by $\Phi(f) \in \mathrm{Ext}^1(A, X)$, and one easily checks that this procedure yields in fact a morphism of groups

$$\Phi : \mathrm{Hom}(X^\vee, A^\vee) \longrightarrow \mathrm{Ext}^1(A, X)$$

On the other hand, if we apply $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m[1])$ to the triangle $\triangle_\xi$, we find an exact sequence

$$\cdots \longrightarrow 0 \longrightarrow \mathcal{H}om(E, \mathbb{G}_m) \longrightarrow \underbrace{\mathcal{H}om(X, \mathbb{G}_m)}_{=X^\vee} \xrightarrow{\partial} \underbrace{\mathcal{E}xt^1(A, \mathbb{G}_m)}_{=A^\vee} \longrightarrow \mathcal{E}xt^1(E, \mathbb{G}_m) \longrightarrow 0 \longrightarrow \cdots$$

Again by Theorem 1.2.5, the sheaves $\mathcal{H}om(A, \mathbb{G}_m)$ and $\mathcal{E}xt^1(X, \mathbb{G}_m)$ are trivial, hence the zeroes. We get an exact triangle

$$(\triangle_\xi)^D = \big[A^\vee \longrightarrow C(\partial) \longrightarrow X^\vee[1] \longrightarrow A^\vee[1]\big]$$

where $C(\partial)$ is the cone of the connecting morphism ∂. We write $\Psi(\xi) := \partial \in \mathrm{Hom}(X^\vee, A^\vee)$. This yields a morphism of groups

$$\Psi : \mathrm{Ext}^1(A, X) \longrightarrow \mathrm{Hom}(X^\vee, A^\vee)$$

It remains to show that Φ and Ψ are isomorphisms, inverse to each other. By now, we know that $(\triangle_f)^D$ and $(\triangle_f)^{DD}$ are exact, because applying $(-)^D$ once, and identifying $X = X^{\vee\vee}$ and $A = A^{\vee\vee}$ yields the exact triangle $\triangle_{\Phi(f)}$, and applying $(-)^D$ again yields the exact triangle $\triangle_{\Psi(\Phi(f))}$. Similarly, the triangles $(\triangle_\xi)^D$ and $(\triangle_\xi)^{DD}$ are exact, because applying $(-)^D$ once to $\triangle_\xi$ yields the exact triangle $\triangle_{\Psi(\xi)}$, and applying $(-)^D$ again and identifying $X = X^{\vee\vee}$ and $A = A^{\vee\vee}$ yields the exact triangle $\triangle_{\Phi(\Psi(\xi))}$.

Theorem 1.2.5 and the five Lemma show that the evaluation morphism gives isomorphisms of triangles

$$\triangle_f \xrightarrow{\cong} \triangle_{\Psi(\Phi(f))} \qquad \text{and} \qquad \triangle_\xi \xrightarrow{\cong} \triangle_{\Phi(\Psi(\xi))}$$

Writing out the associated long exact sequences, the left hand isomorphism gives a commutative diagram

$$\begin{tikzcd} X^\vee \arrow[r, "f"] \arrow[d, equal] & A^\vee \arrow[d, equal] \\ X^\vee \arrow[r, "\Psi(\Phi(f))"] & A^\vee \end{tikzcd}$$

showing that $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}(X^\vee, A^\vee)}$, and the right hand side triangle gives a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & X \arrow[r] & \mathcal{E}xt^1(C(\partial), \mathbb{G}_m) \arrow[r] & A \arrow[r] & 0 \end{tikzcd}$$

Here the top row represents ξ, and the bottom row represents $\Phi(\Psi(\xi))$. Thus we find $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Ext}^1(A,X)}$. □

1.3. The dual 1–motive

We shall associate with each 1–motive M a dual 1–motive $M^\vee$. Of course in a functorial way, so that we get involutions in each of the categories $\mathcal{M}_1$ and $[\mathcal{M}_1]$. The dual of a torus, a locally free sheaf of a finite flat group should, if seen as a 1–motive, be the usual Cartier dual, and the dual of an abelian scheme should be the usual dual abelian scheme. Furthermore, the duality functor should be compatible with the weight filtration.

THEOREM 1.3.1. *There exists a functor $(-)^\vee : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$, having the following three properties:*

(1) *The diagram of categories and functors*

$$\begin{tikzcd} \mathcal{M}_1 \arrow[r, "(-)^\vee"] \arrow[d, "{[-]}"'] & \mathcal{M}_1 \arrow[d, "{[-]}"] \\ {[\mathcal{M}_1]} \arrow[r, "(-)^D = \mathbb{R}\mathcal{H}om(-, \mathbb{G}_m[1])_{\leq 0}"] & {[\mathcal{M}_1]} \end{tikzcd}$$

commutes up to a canonical isomorphism of functors.

(2) *Let M be a 1–motive. There are canonical and natural isomorphisms*

$$\epsilon_M : M \longrightarrow M^{\vee\vee}$$

such that $[\epsilon_M] = \epsilon_{[M]}$ is the canonical evaluation morphism.

(3) *Let M be a 1–motive. There are canonical and natural isomorphisms of 1–motives*

$$M/W_i(M) \;\cong\; (W_{1-i}(M^\vee))^\vee$$

for each i.

Furthermore, the above properties (1), (2) *and* (3) *characterize $(-)^\vee$ up to a canonical isomorphism of functors.*

REMARK 1.3.2. The theorem contains an implicit statement: That property (1) makes sense implies that the functor $(-)^D$ sends the subcategory $[\mathcal{M}_1]$ of $\mathcal{DF}$ into itself, i.e. restricts to an endofunctor of $[\mathcal{M}_1]$.
Property (2) implies that $(-)^\vee : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$ as well as $(-)^D : [\mathcal{M}_1] \longrightarrow [\mathcal{M}_1]$ are antiequivalences of categories.

PROOF OF 1.3.1. We begin with the construction of a contravariant functor $(-)^\vee : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$. Let M be a 1–motive given by

$$M = \left[\begin{tikzcd} & & Y \arrow[d, "u"'] \arrow[dr, "v"] & & \\ 0 \arrow[r] & X \arrow[r, "\tau"] & G \arrow[r, "\gamma"] & A \arrow[r] & 0 \end{tikzcd}\right]$$

Write $Y^\vee := \mathcal{H}om(X, \mathbb{G}_m)$ for the character group of X, write $X^\vee := \mathcal{H}om(Y, \mathbb{G}_m)$ for the character group of Y and write $A^\vee := \mathcal{E}xt^1(A, \mathbb{G}_m)$ for the dual abelian scheme of A. Observe that $Y^\vee$ is an extension of a finite flat group scheme by a lattice, and that $X^\vee$ is an extension of a torus by a finite flat group scheme. Consider the exact triangle

$$(*) \qquad [Y \longrightarrow 0] \longrightarrow [Y \xrightarrow{v} A] \longrightarrow [0 \longrightarrow A]$$

Applying $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$ to this triangle and taking Theorem 1.2.5 into account yields the following short exact sequence

$$0 \longrightarrow X^\vee \xrightarrow{\partial =: \tau^\vee} \mathcal{E}xt^1([Y \longrightarrow A], \mathbb{G}_m) \xrightarrow{\partial =: \gamma^\vee} A^\vee \longrightarrow 0$$

Writing $G^\vee := \mathcal{E}xt^1([Y \longrightarrow A], \mathbb{G}_m)$, we get an extension of $A^\vee$ by $X^\vee$ which is, by definition, the one coming from the morphism $v \in \mathrm{Hom}(Y, A)$ via the Barsotti–Weil formula 1.2.3. Observe that the sheaf $G^\vee$ is representable. Indeed, we may look at it as an $X^\vee$–torsor over $A^\vee$, and since $X^\vee$ is affine, representability follows from [**Mil80**], Theorem III.4.3a. Next, consider the exact triangle

$$(**) \qquad [0 \longrightarrow X] \xrightarrow{(0,\tau)} [Y \longrightarrow G] \xrightarrow{(\mathrm{id},\gamma)} [Y \longrightarrow A]$$

Applying $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$, it yields a long exact sequence part of which is

$$\cdots \longrightarrow \mathcal{H}om([Y \longrightarrow G], \mathbb{G}_m) \longrightarrow Y^\vee \xrightarrow{\partial =: u^\vee} G^\vee \longrightarrow \mathcal{E}xt^1([Y \longrightarrow G], \mathbb{G}_m) \longrightarrow \cdots$$

We now may define $M^\vee$ to be the 1–motive

$$M^\vee := \left[\begin{tikzcd} & & Y^\vee \arrow[d, "u^\vee"'] & & \\ 0 \arrow[r] & X^\vee \arrow[r, "\tau^\vee"] & G^\vee \arrow[r, "\gamma^\vee"] & A^\vee \arrow[r] & 0 \end{tikzcd}\right]$$

A morphism of 1–motives $\varphi : M_1 \longrightarrow M_2$ induces morphisms of triangles in $(*)$ and $(**)$, hence a morphism $\varphi^\vee : M_2^\vee \longrightarrow M_1^\vee$. We find a contravariant functor $(-)^\vee$. Let us now verify that this functor satisfies the properties (1), (2) and (3).
(1): This is true by construction. Indeed, applying the functor $(-)^D$ to the exact triangle $(**)$ yields the triangle

$$[Y \longrightarrow A]^D \longrightarrow [M]^D \longrightarrow X^D$$

which is exact, because $\mathcal{E}xt^1(X, \mathbb{G}_m) = 0$. We know that X^D is quasi–isomorphic to $Y^\vee[1]$ via $H^0(-)$, and the same way $[Y \longrightarrow A]^D$ is quasi–isomorphic to $G^\vee$. Thus we get an exact triangle

$$G^\vee \longrightarrow [M]^D \longrightarrow Y^\vee[1] \xrightarrow{v^\vee} G^\vee[1]$$

But to say that this triangle is exact is precisely to say that $[M]^D$ is quasi–isomorphic to $[Y^\vee \longrightarrow G^\vee]$. Thus $[M^\vee] = [M]^D$, and this shows also the implicit statement of the theorem that the functor $(-)^D$ sends objects of $[\mathcal{M}_1]$ to objects of $[\mathcal{M}_1]$.
(2): Repeat the above construction in order to get a 1–motive

$$M^{\vee\vee} = \left[\begin{tikzcd} & & Y^{\vee\vee} \arrow[d] & & \\ 0 \arrow[r] & X^{\vee\vee} \arrow[r] & G^{\vee\vee} \arrow[r] & A^{\vee\vee} \arrow[r] & 0 \end{tikzcd}\right]$$

There are natural isomorphisms $\epsilon_Y : Y \longrightarrow Y^{\vee\vee}$ and $\epsilon_X : X \longrightarrow X^{\vee\vee}$, and also $\epsilon_A : A \longrightarrow A^{\vee\vee}$, induced by the derived evaluation map. The evaluation map $\epsilon_G : G \longrightarrow G^{\vee\vee}$, is also an isomorphism by the five lemma. By naturality of these evaluation maps, we get as requested a canonical and natural isomorphism of 1–motives $\epsilon_M : M \longrightarrow M^{\vee\vee}$. The equality $[\epsilon_M] = \epsilon_{[M]}$ holds by construction.
(3): Is true by construction as well.
Now let $(-)^\flat : \mathcal{M}_1 \longrightarrow \mathcal{M}_1$ be any other functor satisfying (1), (2) and (3), and denote by $Y^\flat$, $X^\flat$,$G^\flat$ and $A^\flat$ the components of $M^\flat$. It follows from the properties (1), (2) and (3) that there are canonical isomorphisms

$$Y^\flat \cong Y^\vee \qquad \text{and} \qquad X^\flat \cong X^\vee \qquad \text{and} \qquad A^\flat \cong A^\vee$$

Indeed, using (all) three properties, we get canonical and natural isomorphisms (in the category $[\mathcal{M}_1]$)

$$[Y^\flat \longrightarrow 0] = [M^\flat / W_{-1}(M^\flat)] \cong [(W_{-2}M)^\flat] \cong [W_{-2}M]^D = [0 \longrightarrow X]^D$$

and thus $Y^\flat = H^0([Y^\flat \longrightarrow 0]) \cong H^0([0 \longrightarrow X]^D) = Y^\vee$, and similarly we find $X^\flat \cong X^\vee$ and $A^\flat \cong A^\vee$. The unicity statement follows now by dévissage. □

CHAPTER 2

Tate modules

For this chapter we keep fixed an integral noetherian scheme S and a prime number ℓ invertible on S. As in the previous chapter we write $\mathcal{F} = \mathcal{F}_S$ for the category of fppf-sheaves of commutative groups on S and identify commutative group schemes over S with their associated sheaves. Recall (e.g. from[**KS06**], Chapter 18) that $\mathcal{F}$ is an abelian category with internal homomorphism functor $\mathcal{H}om$ and tensor product $\otimes$, and that it has enough injectives and flats.

2.1. An ℓ–adic formalism

The goal of this section is to introduce a good formalism of complexes of ℓ–adic and ℓ–divisible sheaves on the base scheme S. The motivation is the following: Given, say, a commutative and geometrically connected group scheme G over S, the ℓ–adic Tate module and the ℓ–divisible (Barsotti–Tate) group of G are defined to be the formal limit and colimit

$$\mathrm{T}_\ell G := \lim_{n\geq 0} G[\ell^n] \qquad \text{and} \qquad \mathrm{B}_\ell G := \operatorname*{colim}_{n\geq 0} G[\ell^n]$$

The Tate module $\mathrm{T}_\ell G$ is an ℓ-adic sheaf in the sense of [**GBH$^+$66**], and the Barsotti–Tate group $\mathrm{B}_\ell G$ is a sheaf of ℓ–divisible groups. We want to associate Tate modules and Barsotti–Tate groups not only with group schemes, but rather with complexes of group schemes, for instance with complexes coming from 1-motives. To give another example, C. Demarche is investigating in his Ph.D. thesis (to appear) two term complexes of tori $[T_1 \longrightarrow T_2]$, to which one would like to associate a Tate module. These of course will not be just ℓ–adic sheaves or sheaves of ℓ–divisible groups, but rather complexes of such. This explains our need for a *derived category of ℓ–adic sheaves.*

When considering a derived category of ℓ–adic sheaves, two problems appear, as pointed out in [**Eke90**]: On one hand, ℓ–adic sheaves are not actual sheaves but rather formal limit systems of such. On the other hand, one wants to pretend that one is dealing with complexes of sheaves and not some more abstract objects.
The most simple minded approach works well for our applications. We will mimick the construction of ℓ–adic sheaves (cf. [**GBH$^+$66**] exp.V). Instead of working with limit systems of sheaves, we work with limit systems of complexes of sheaves up to quasi–isomorphism. As with ℓ–adic sheaves, we define morphisms between such systems in such a way that Artin–Rees equivalent systems become isomorphic.
Most of this section is adapted, inspired or stolen from [**FK87, Jan88, Eke90, Beh03, KS06**] and of course [**GBH$^+$66**].

– 2.1.1. We will write "$\mathbb{Z}$" for the constant sheaf with value $\mathbb{Z}$ on S, and for brevity we write Λ_i for the constant sheaf with value $\mathbb{Z}/\ell^i\mathbb{Z}$ on S.

– 2.1.2. By a *limit system* in a category $\mathcal{C}$ we understand the following data: A collection of objects $(F_i)_{i=0}^{\infty}$ and for each $i \geq j \geq 0$ a morphism $\pi_{ij} : F_i \longrightarrow F_j$, such that

$$\pi_{jk} \circ \pi_{ij} = \pi_{ik}$$

for all $i \geq j \geq k$. Put otherwise, a limit system is a covariant functor $I \longrightarrow \mathcal{C}$, where I is the category having as objects the nonnegative integers. and where the morphism sets are either empty or singletons $\{*\}$ according to the rule

$$\mathrm{Hom}(i,j) = \begin{cases} \{*\} & \text{if } i \geq j \\ \varnothing & \text{if } i < j \end{cases}$$

A *colimit system* in $\mathcal{C}$ is a limit system in the opposite category, or equivalently a contravariant functor $I \longrightarrow \mathcal{C}$. We will usually represent a limit or colimit system by a sequence $(F_i)_{i=0}^{\infty}$ of objects of $\mathcal{C}$, the morphisms $F_i \longrightarrow F_j$ for $i \geq j$ being understood.

– 2.1.3. Given two limit systems $F = (F_i)_{i=0}^{\infty}$ and $G = (G_i)_{i=0}^{\infty}$, we let $\mathrm{Hom}_I(F,G)$ be the set of functor morphisms from F to G, that is, sequences of morphisms $(f_i : F_i \longrightarrow G_i)_{i=0}^{\infty}$ such that the obvious squares commute. In particular, we can consider for every $r \geq 0$ the shifted limit system $F_{+r} = (F_{i+r})_{i=0}^{\infty}$, and the functor morphism $(\pi_{i+r,i} : F_{i+r} \longrightarrow F_i)_{i=0}^{\infty}$. We define the set of *morphisms of limit systems* from F to G by

$$\mathrm{Hom}(F,G) := \operatorname*{colim}_{r\in I} \mathrm{Hom}_I(F_{+r}, G)$$

the colimit being taken in the category of sets. A morphism between limit systems $f : F \longrightarrow G$ is thus given by an integer $r \geq 0$ and a sequence of morphisms $(f_i : F_{i+r} \longrightarrow G_i)_{i=0}^{\infty}$. Two such data $(r, (f_i)_{i=0}^{\infty})$ and $(r', (f_i')_{i=0}^{\infty})$ represent the same morphism of limit systems if there exists an integer $r'' \geq \max(r, r')$ such that $f_i \circ \pi_{r''+i,r+i} = f_i' \circ \pi_{r''+i,r'+i}$ for all $i \geq 0$.

– 2.1.4. Let $\mathcal{C}$ be an additive category. A limit system $F = (F_i)_{i=0}^{\infty}$ in $\mathcal{C}$ is said to be a *null–system* if there is an integer $r \geq 0$ such that the maps $F_{i+r} \longrightarrow F_i$ are zero for all i. In other words, F is a null system if it is isomorphic to the zero system. A morphism of limit systems $f : F \longrightarrow G$ in an abelian category, given by an integer $r \geq 0$ and a sequence of morphisms $(f_i : F_{i+r} \longrightarrow G_i)_{i=0}^{\infty}$ is an isomorphism of limit systems if and only if the systems $(\ker f_i)_{i=0}^{\infty}$ and $(\operatorname{coker} f_i)_{i=0}^{\infty}$ are null systems. Frequently, it is said that f is an *Artin–Rees equivalence.* Recall the following definition ([**FK87**], Definitions 12.6 and 12.9)

Definition 2.1.5. A *locally constant ℓ–adic sheaf on S* is a limit system $F = (F_i)_{i=0}^{\infty}$ in $\mathcal{F}$ such that all for all i the sheaf F_i is locally constant killed by ℓ^i, and such that the morphisms

$$F_i \otimes \Lambda_j \longrightarrow F_j$$

are isomorphisms. A *locally constant ℓ–divisible sheaf on S* is a colimit system $F = (F_i)_{i=0}^{\infty}$ in $\mathcal{F}$ such that all for all i the sheaf F_i is locally constant killed by ℓ^i, and such that the morphisms

$$F_j \longrightarrow \mathcal{H}om(\Lambda_j, F_i)$$

are isomorphisms. A limit or colimit system in $\mathcal{F}$ which is isomorphic (Artin–Rees equivalent) to a limit or colimit system having these properties is then called Artin–Rees ℓ–adic, respectively Artin–Rees ℓ–divisible.

– 2.1.6. In the sequel we will not make the distinction between ℓ–adic sheaves and Artin–Rees ℓ–adic sheaves, and call all these limit systems just ℓ–adic sheaves. Also, we will only consider locally constant ℓ–adic sheaves, and not repeat this all the time. Recall the following stability property for ℓ–adic sheaves ([**FK87**], Proposition 12.11)

Proposition 2.1.7. *The kernel and cokernel of any morphism of ℓ–adic sheaves on S, taken in the category of limit systems, are again ℓ–adic sheaves. Moreover, given an exact sequence of limit systems in $\mathcal{F}$*

$$0 \longrightarrow F \longrightarrow G \longrightarrow H \longrightarrow 0$$

where F and H are ℓ-adic sheaves, the limit system $G = (G_i)_{i=0}^{\infty}$ is an ℓ–adic sheaf as well provided $\ell^{i+r}G_i = 0$ for some suitable r and all i.

Definition 2.1.8. A *complex of locally constant ℓ–adic sheaves* or simply *ℓ–adic complex* is a limit system $F = (F_i)_{i=0}^{\infty}$ in the derived category $\mathcal{DF}$ having the following two properties:

(1) For all but finitely many integers r, the sheaf $H^r(F_i)$ is trivial for all $i \geq 0$.
(2) For all integers r, the limit system $H^r(F_i)_{i=0}^{\infty}$ is an ℓ–adic sheaf.

A morphism of ℓ–adic complexes is a morphism of limit systems. We call the arising category *derived category of locally constant ℓ–adic sheaves on S.*
A *complex of locally constant ℓ–divisible sheaves* or *ℓ–divisible complex* is a colimit system in $\mathcal{DF}$ having property (1) above, and:

(2') For all integers r, the colimit system $H^r(F_i)_{i=0}^{\infty}$ is an ℓ–divisible sheaf.

A morphism of ℓ–divisible complexes is a morphism of colimit systems. We call the arising category *derived category of locally constant ℓ–divisible sheaves on S.*

– 2.1.9. In summary, a limit system $F = (F_i)_{i=0}^{\infty}$ in $\mathcal{DF}$ is a ℓ–adic complex if the F_i's are uniformly bounded in length, and if for each r, the limit system $(H^r(F_i))_{i=0}^{\infty}$ is an ℓ–adic sheaf. We will often write

$$F = \lim_{i \geq 0} F_i$$

The definition is well set, in the sense that if a limit system F is isomorphic to an ℓ–adic complex, then F itself is an ℓ–adic complex. We will give now some justification for it. The upshot is that this derived category of ℓ–adic sheaves presents all features one would expect of a true derived category.

– 2.1.10. Let $\mathcal{F}_\ell$ be the category of ℓ–adic sheaves, and let $\mathcal{D}_\ell$ be the derived category of ℓ–adic sheaves on S as defined in 2.1.8. There exists for each integer m a *shift functor* $(-)[m] : \mathcal{D}_\ell \longrightarrow \mathcal{D}_\ell$ and truncation functors $(-)_{\leq m}$ and $(-)_{>m}$ induced by the shift functor and truncation functors on $\mathcal{DF}$. The natural functor $\natural : \mathcal{F} \longrightarrow \mathcal{D}F$ sending a sheaf to a complex concentrated in degree 0, and the functor $H^0 : \mathcal{D}F \longrightarrow F$ induce functors

$$\begin{tikzcd} \mathcal{F}_\ell \arrow[r, bend left, "\natural"] & \mathcal{D}_\ell \arrow[l, bend left, "H^0"] \end{tikzcd}$$

It follows immediately from the definitions that the functor $\natural$ is fully faithful, and that the composition $H^0 \circ \natural$ is equivalent to the identity functor on $\mathcal{F}_\ell$. There is no need to talk about *quasi–isomorphisms*, since these have already been inverted in $\mathcal{DF}$. We will check that given a morphism of ℓ–adic complexes $f : F \longrightarrow G$, the cone of f taken in the category of limit systems (i.e. "level by level") is also an ℓ–adic complex, and we get canonical morphisms

$$F \xrightarrow{f} G \longrightarrow C(f) \longrightarrow F[1]$$

Taking homology, these induce a long exact sequence of ℓ–adic sheaves. This leads to a triangulated structure on $\mathcal{D}_\ell$, the exact (or distinguished) triangles being those isomorphic to a cone. All axioms of a triangulated category ([**MG96**], IV.1) are immediately satisfied, with the possible exception of the octahedron axiom (we do not care).

– 2.1.11. We now check several things. First, we show that the cone of a morphism of ℓ–adic complexes is again an ℓ–adic complex. Then, we show that the derived category of ℓ–adic sheaves has a tensor product and an internal homomorphism functor, and that these behave as they ought to. Then, we show that the category of ℓ–adic sheaves is antiequivalent to the category of ℓ–divisible sheaves (so we don't have to check everything for ℓ–divisible sheaves again).

PROPOSITION 2.1.12. *Let $F = \lim F_i$ and $G = \lim G_i$ be ℓ–adic complexes and let $f : F \longrightarrow G$ be a morphism of ℓ–adic complexes represented by an integer $r \geq 0$ and a system of morphisms $(f_i : F_{i+r} \longrightarrow G_i)_{i=0}^\infty$ in $\mathcal{F}$. The limit system*

$$\mathrm{Cone}(f) := \mathrm{Cone}(f_i)_{i=0}^\infty$$

depends only on the morphism f and not on the chosen representation. If moreover $\ell^{i+r}\mathrm{Cone}(f_i) = 0$ for some suitable r and all i, then $\mathrm{Cone}(f)$ is an ℓ–adic sheaf as well.

PROOF. We first check independence of the representation of f. Write $\pi_{ij} : F_i \longrightarrow F_j$ for the transition maps that come by definition with the limit system F. We only have to check that for every integer $r'' \geq r$ the morphism given by $(f_i \circ \pi_{i+r'',i+r})_{i=0}^\infty$ yields an isomorphic cone. Indeed, the composition $F_{i+r''} \longrightarrow F_{i+r} \longrightarrow G_i$ yields a triangle of cones (c.f. [**Mil08**], II.0.10)

$$\mathrm{Cone}(\pi_{i+r'',i+r}) \longrightarrow \mathrm{Cone}(f_i \circ \pi_{i+r'',i+r}) \longrightarrow \mathrm{Cone}(f_i) \longrightarrow \mathrm{Cone}(\pi_{i+r'',i+r})[1]$$

But the limit system $(\mathrm{Cone}(\pi_{i+r'',i+r}))_{i=0}^\infty$ is a null–system, hence the desired isomorphism of limit systems. We have for all $r \in \mathbb{Z}$ and $i \geq 0$ a natural exact sequence

$$H^r(F_i) \longrightarrow H^r(G_i) \longrightarrow H^r\mathrm{Cone}(f_i) \longrightarrow H^{r+1}(F_i) \longrightarrow H^{r+1}(G_i)$$

The first and last two terms in this sequence constitute morphisms of ℓ–adic sheaves, hence the middle term by Proposition 2.1.7. $\square$

COROLLARY 2.1.13. *Let $F \longrightarrow G \longrightarrow H \longrightarrow F[1]$ be an exact triangle of limit systems in $\mathcal{DF}$, where F_i, G_i and H_i are killed by ℓ^{i+r} for some suitable r and all i. If two out of these three limit systems are ℓ–adic complexes, so is the third one.*

PROOF. Suppose without loss of generality that F and G are ℓ–adic complexes. The limit system H is quasi–isomorphic (noncanonically) with the cone of the given morphism $F \longrightarrow G$, hence an ℓ–adic complex by the proposition. $\square$

– 2.1.14. Let C be an object of $\mathcal{DF}$ such that for all $r \in \mathbb{Z}$ the sheaf $H^r(C)$ is locally constant killed by some power of ℓ. We can then consider the constant (co)limit system $(C_i)_{i=0}^\infty$ with $C_i = C$ for all i. This is easily seen to be an ℓ–adic complex, respectively an ℓ–divisible complex. We call an ℓ–adic of ℓ–divisible complex *finite* if it is isomorphic to such a constant (co)limit system. There is no danger in identifying finite complexes with such objects of $\mathcal{DF}$ and vice versa.

PROPOSITION 2.1.15. *Let $F = \lim F_i$ and $G = \lim G_i$ be ℓ–adic complexes on S. For all $i \geq 0$, the limit and colimit*

$$F \otimes^{\mathbb{L}} G_i := \lim_{j \geq 0} \big(F_j \otimes^{\mathbb{L}} G_i\big) \qquad \text{and} \qquad \mathbb{R}\mathcal{H}om(F, G_i) := \operatorname*{colim}_{j \geq 0} \mathbb{R}\mathcal{H}om(F_j, G_i)$$

exist in $\mathcal{DF}$. The homology groups of these objects are finite locally constant sheaves killed by ℓ^i. The limit systems

$$F \otimes^{\mathbb{L}} G := \lim_{i \geq 0} \big(F \otimes^{\mathbb{L}} G_i\big) \qquad \text{and} \qquad \mathbb{R}\mathcal{H}om(F, G) := \lim_{i \geq 0} \mathbb{R}\mathcal{H}om(F, G_i)$$

are ℓ–adic sheaves. These are natural in F and G, and null–systems if either F or G is a null–system. Moreover, if H is another ℓ–adic sheaf, then the adjunction formula

$$\mathbb{R}\mathcal{H}om(F \otimes^{\mathbb{L}} G, H) \cong \mathbb{R}\mathcal{H}om(F, \mathbb{R}\mathcal{H}om(G, H))$$

holds. If $\mathbb{Z}_\ell$ denotes the constant ℓ–adic complex $\lim \Lambda_i$, then there are canonical isomorphisms $F \otimes^{\mathbb{L}} \mathbb{Z}_\ell \cong F$ and $\mathbb{R}\mathcal{H}om(\mathbb{Z}_\ell, F) \cong F$.

PROOF. Let us begin with the tensor products. Suppose first that F and G are concentrated in degree 0 only. The derived tensor product $F_j \otimes^{\mathbb{L}} G_i$ is then concentrated in degrees -1 and 0, and we have a canonical and natural triangle

$$H^{-1}(F_j \otimes^{\mathbb{L}} G_i)[1] \longrightarrow F_j \otimes^{\mathbb{L}} G_i \longrightarrow H^0(F_j) \otimes H^0(G_i)$$

The limit system $H^{-1}(F_j \otimes^{\mathbb{L}} G_i)_{j \geq 0}$ is a null system, and $H^0(F_j) \otimes H^0(G_i) \cong H^0(F_i) \otimes H^0(G_i)$ for all $j \geq i$. Hence the limit system $(F_j \otimes^{\mathbb{L}} G_i)_{j \geq 0}$ is canonically isomorphic to the constant system with value $H^0(F_i) \otimes H^0(G_i)$. From this we see that $F \otimes^{\mathbb{L}} G$ is concentrated in degree 0, and given there by the ℓ–adic sheaf

$$H^0(F \otimes G) = \lim_{i \geq 0} \big(H^0(F_i) \otimes H^0(G_i)\big)$$

which viewed as a limit system of complexes concentrated in degree 0 is an ℓ–adic complex. This shows the claims for the tensor products in the case F and G are concentrated in degree 0. The general case follows then by dévissage (first on F and then on G, say) and induction on the length of the complexes. The statements about null systems and the isomorphism $F \otimes^{\mathbb{L}} \mathbb{Z}_\ell \cong F$ are clear. On the way one finds that also the Künneth formula

$$H^r(F \otimes^{\mathbb{L}} G) \cong \bigoplus_{s+t=r} H^s(F) \otimes H^t(G)$$

holds (there are no Tor's). The checking for the derived homomorphisms is similar. First one checks that for F and G concentrated in degree 0 the given colimit system is isomorphic to the constant system with value $\mathcal{H}om(H^0(F_i), H^0(G_i))$. Hence $\mathbb{R}\mathcal{H}om(F, G)$ is equivalently given by the limit

$$\mathbb{R}\mathcal{H}om(F, G) = \lim_{i \geq 0} \mathcal{H}om(H^0(F_i), H^0(G_i))$$

which is an ℓ–adic complex concentrated in degree 0. Then one proceeds by dévissage. The adjunction formula holds as well, because it holds already on finite levels ([**KS06**], 18.6.9). □

PROPOSITION 2.1.16. *The functor $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$ induces an equivalence between the derived category of locally constant ℓ–adic sheaves and the derived category of locally constant ℓ–divisible sheaves.*

PROOF. Let $F = \lim F_i$ be a ℓ–adic complex on S. Applying the contravariant functor $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$ to it yields the colimit system $\mathbb{R}\mathcal{H}om(F_i, \mathbb{G}_m)_{i=0}^{\infty}$. It follows from Lemma 1.2.4 and dévissage that this colimit system is an ℓ–divisible complex. Similarly, applying $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$ to an ℓ–divisible complex yields an ℓ–adic complex. For each i, there is a canonical morphism

$$F_i \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{R}\mathcal{H}om(F_i, \mathbb{G}_m), \mathbb{G}_m)$$

which is an isomorphism by Cartier duality for finite flat group schemes, Lemma 1.2.4 and dévissage. Hence, the functor $\mathbb{R}\mathcal{H}om(-, \mathbb{G}_m)$ is an equivalence in both directions. □

2.2. Tate modules of complexes

In this section, we show how to associate with a reasonably well behaving complex C of sheaves on S an ℓ–adic complex $\mathbb{T}_\ell C$, which we call *ℓ–adic Tate module* of C. We check that these Tate modules have the properties we expect, among them the existence of a Weil pairing (Proposition 2.2.7). This is what ℓ–adic complexes are designed for. We continue working over a noetherian regular base S and a prime ℓ invertible on S. We keep the notation $\Lambda_i := \mathbb{Z}/\ell^i\mathbb{Z}$.

Definition 2.2.1. Let C be an object of $\mathcal{DF}$. We say that C is *moderate* if the kernel and the cokernel of the multiplication–by–ℓ^i map on $H^r(C)$ are locally constant finite group schemes for all $i \geq 0$ and all $r \in \mathbb{Z}$, trivial for all but finitely many $r \in \mathbb{Z}$.

– 2.2.2. The interest of *moderate* complexes of sheaves is that these form a natural and essentially best possible subcategory of $\mathcal{DF}$ on which the Tate module construction makes sense. We will check that the full subcategory of moderate objects of $\mathcal{DF}$ is a triangulated subcategory, stable under $\otimes$ and $\mathbb{R}\mathcal{H}om$, and that finite flat group schemes, abelian schemes, lattices and tori, if seen as objects of $\mathcal{DF}$ are moderate, hence so are all objects in $[\mathcal{M}_1]$.

Definition 2.2.3. Let C be a moderate object of $\mathcal{DF}$. Its *Tate module* and its *Barsotti–Tate group* are the ℓ–adic complex, respectively the ℓ–divisible complex[1]

$$\mathbb{T}_\ell C := \lim_{i\geq 0}\,(C \otimes^{\mathbb{L}} \Lambda_i)[-1] \qquad \text{and} \qquad \mathbb{B}_\ell C := \operatorname*{colim}_{i\geq 0}\,(C \otimes^{\mathbb{L}} \Lambda_i)[-1]$$

The transition maps are those induced by the canonical projections $\Lambda_{i+1} \longrightarrow \Lambda_i$, respectively the canonical injections $\Lambda_i \longrightarrow \Lambda_{i+1}$.

Proposition 2.2.4. *Let C be a moderate object of $\mathcal{DF}$. The limit and colimit systems given in Definition 2.2.3 are indeed an ℓ–adic complex and an ℓ–divisible complex respectively. If $H^r(C) = 0$ for $r < a$ and $r > b$, then $H^r(\mathbb{T}_\ell C) = 0$ and $H^r(\mathbb{B}_\ell C) = 0$ for $r < a$ and $r > b+1$.*

Proof. The complex $[\mathbb{Z} \xrightarrow{\cdot\ell^i} \mathbb{Z}]$ supported in degrees -1 and 0 is a flat resolution of Λ_i. Using this resolution, we can represent $C \otimes^{\mathbb{L}} \Lambda_i$ by the complex

$$[\cdots \longrightarrow 0 \longrightarrow C_{r-1} \oplus C_r \longrightarrow \underbrace{C_r \oplus C_{r+1}}_{\text{degree } r} \xrightarrow{d_r} C_{r+1} \oplus C_{r+2} \longrightarrow \cdots]$$

the differential d_r being given by $d_r(x, y) = (dx + (-1)^r \ell^i y, dy)$. This complex is just the cone of the multiplication–by–ℓ^i map on C. The additional statement in the proposition is now immediate.

[1]We need the shifts for the following reason: Our convention is to put the complexes associated with 1–motives in degree -1 and 0. In particular, an abelian variety if seen as a 1–motive sits in degree 0, and we want its Tate module also to be concentrated in degree 0. The shift ensures precisely this.

It remains to check that $\lim H^r(C \otimes^{\mathbb{L}} \Lambda_i)$ is an ℓ–adic sheaf. For all $r \in \mathbb{Z}$ and all $i \geq j \geq 0$ we have a morphism of short exact sequences of torsion sheaves on S

$$\begin{tikzcd} 0 \arrow[r] & H^r(C) \otimes \Lambda_i \arrow[r] \arrow[d] & H^r(C \otimes^{\mathbb{L}} \Lambda_i) \arrow[r] \arrow[d] & H^{r+1}(C)[\ell^i] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & H^r(C) \otimes \Lambda_j \arrow[r] & H^r(C \otimes^{\mathbb{L}} \Lambda_j) \arrow[r] & H^{r+1}(C)[\ell^j] \arrow[r] & 0 \end{tikzcd}$$

By definition of moderateness, these sequences are trivial for almost all r. The first and last term in each of these sequences is a locally constant sheaf killed by ℓ^i respectively ℓ^j, hence so are the sheaves in the middle. The first vertical map is induced by the projection $\Lambda_i \longrightarrow \Lambda_j$, and the last vertical map is multiplication by ℓ^{i-j}. It remains to show that the limit systems

$$\lim_{i \geq 0}(H^r(C) \otimes \Lambda_i) \qquad \text{and} \qquad \lim_{i \geq 0}(H^{r+1}(C)[\ell^i])$$

are ℓ–adic sheaves. For the first one this is immediate because $\Lambda_i \otimes \Lambda_j = \Lambda_j$ for all $i \geq j \geq 0$. For the second one, observe that there is an integer $m \geq 0$ such that for all integers i and $m' \geq m$ the image of $H^{r+1}(C)[\ell^{i+m'}]$ in $H^{r+1}(C)[\ell^i]$ is the same as the image of $H^{r+1}(C)[\ell^{i+m}]$ just as it is the case for ordinary groups instead of sheaves (mind that S is integral and noetherian). Writing $A := \ell^r H^{r+1}(C)$, the above limit system is thus isomorphic (Artin–Rees equivalent) to the limit system $\lim(A[\ell^i])$. In this system, all transition maps $\ell^{i-j} : A[\ell^i] \longrightarrow A[\ell^j]$ are surjective, hence induce isomorphisms $A[\ell^i] \otimes \Lambda_j \longrightarrow A[\ell^j]$ as required. □

Proposition 2.2.5. *The following holds*

(1) *Let $C_1 \longrightarrow C_2 \longrightarrow C_3 \longrightarrow C_1[1]$ be an exact triangle of moderate objects. The induced triangles*

$$\mathbb{T}_\ell C_1 \longrightarrow \mathbb{T}_\ell C_2 \longrightarrow \mathbb{T}_\ell C_3 \longrightarrow \mathbb{T}_\ell C_1[1] \qquad \textit{and} \qquad \mathbb{B}_\ell C_1 \longrightarrow \mathbb{B}_\ell C_2 \longrightarrow \mathbb{B}_\ell C_3 \longrightarrow \mathbb{B}_\ell C_1[1]$$

are also exact triangles.

(2) *For any two moderate objects C_1 and C_2 the tensor product $C_1 \otimes^{\mathbb{L}} C_2$ is moderate and there is a natural isomorphism*

$$\mathbb{T}_\ell(C_1 \otimes^{\mathbb{L}} C_2)[-1] \cong \mathbb{T}_\ell C_1 \otimes^{\mathbb{L}} \mathbb{T}_\ell C_2$$

(3) *For any two moderate objects C_1 and C_2 the object $\mathbb{R}\mathcal{H}om(C_1, C_2)$ is moderate and there is a natural isomorphism*

$$\mathbb{T}_\ell \mathbb{R}\mathcal{H}om(C_1, C_2)[1] \cong \mathbb{R}\mathcal{H}om(\mathbb{T}_\ell C_1, \mathbb{T}_\ell C_2)$$

Proof. In (1) we can suppose without loss of generality that C_3 is the cone of the given map $f : C_1 \longrightarrow C_2$ and it is enough to show that under this assumption $\mathbb{T}_\ell C_3$ is naturally isomorphic to the cone of the induced morphism $\mathbb{T}_\ell C_1 \longrightarrow \mathbb{T}_\ell C_2$. This holds indeed because of the canonical isomorphism

$$\mathrm{Cone}(f : C_1 \longrightarrow C_2) \otimes^{\mathbb{L}} \Lambda_i \cong \mathrm{Cone}(f \otimes 1 : C_1 \otimes^{\mathbb{L}} \Lambda_i \longrightarrow C_2 \otimes^{\mathbb{L}} \Lambda_i)$$

The same argument works for the ℓ–divisible complexes. For the second statement, it is enough to observe that the limit systems

$$(C_1 \otimes^{\mathbb{L}} C_2 \otimes^{\mathbb{L}} \Lambda_i)_{i=0}^{\infty} \qquad\qquad (C_1 \otimes^{\mathbb{L}} C_2 \otimes^{\mathbb{L}} \Lambda_i \otimes^{\mathbb{L}} \Lambda_i)_{i=0}^{\infty}$$

are isomorphic by the last statement of Proposition 2.1.15. The first one is $\mathbb{T}_\ell(C_1 \otimes^{\mathbb{L}} C_2)$ shifted by 1, the second one is $\mathbb{T}_\ell C_1 \otimes^{\mathbb{L}} \mathbb{T}_\ell C_2$ shifted by 2. The same works for homomorphisms in place of tensor products. □

– 2.2.6. We now come to the Weil pairing. Given moderate objects A, B and C in $\mathcal{D}^{\mathrm{b}}\mathcal{F}$ and a morphism $A \otimes^{\mathbb{L}} B \longrightarrow C$ we get by statement (2) of Proposition 2.2.5 a morphism

$$\mathbb{T}_\ell A \otimes^{\mathbb{L}} \mathbb{T}_\ell B \longrightarrow \mathbb{T}_\ell C[-1]$$

Using the adjunction formula from Proposition 2.1.15, this pairing induces morphisms of ℓ–adic complexes $\mathbb{T}_\ell A \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{T}_\ell B, \mathbb{T}_\ell C)$ and $\mathbb{T}_\ell B \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{T}_\ell A, \mathbb{T}_\ell C)$. We say that the above pairing of ℓ–adic complexes is *perfect* if these are both isomorphisms. We will write $\mathbb{Z}_\ell(1)$ for the Tate module of $\mathbb{G}_m$ put in degree zero.

Proposition 2.2.7. *Let C be a moderate object of $\mathcal{DF}$ and set $C^\vee := \mathbb{R}\mathcal{H}om(C, \mathbb{G}_m)$. The natural "Weil" pairing*

$$\mathbb{T}_\ell C \otimes^{\mathbb{L}} \mathbb{T}_\ell C^\vee \longrightarrow \mathbb{Z}_\ell(1)[-1]$$

is a perfect pairing of ℓ–adic complexes.

Proof. We first show that the adjunction map $\mathbb{T}_\ell C^\vee \longrightarrow \mathbb{R}\mathcal{H}om(\mathbb{T}_\ell C, \mathbb{Z}_\ell(1))$ is an isomorphism. This has to be checked on finite levels. We must show that for all $i \geq 0$, the map

$$\mathbb{R}\mathcal{H}om(C, \mathbb{G}_m) \otimes^{\mathbb{L}} \Lambda_i[-1] \longrightarrow \mathbb{R}\mathcal{H}om(C \otimes^{\mathbb{L}} \Lambda_i[-1], \mathbb{G}_m \otimes \Lambda_i[-1])[-1]$$

is an isomorphism. All shifts cancel, and homomorphisms of $C \otimes^{\mathbb{L}} \Lambda_i$ into $\mathbb{G}_m \otimes \Lambda_i$ are the same as homomorphisms to $\mathbb{G}_m$ because $C \otimes^{\mathbb{L}} \Lambda_i$ is anyway killed by ℓ^i. Hence, the above map reads

$$\mathbb{R}\mathcal{H}om(C, \mathbb{G}_m) \otimes^{\mathbb{L}} \Lambda_i \longrightarrow \mathbb{R}\mathcal{H}om(C \otimes^{\mathbb{L}} \Lambda_i, \mathbb{G}_m)$$

This is indeed an isomorphism, on both sides stands just the cone of the multiplication–by–ℓ^i on $\mathbb{R}\mathcal{H}om(C, \mathbb{G}_m)$. Now let us show that we can exchange the roles of C and $C^\vee$. For this, write $C^{\vee\vee} := \mathbb{R}\mathcal{H}om(C^\vee, \mathbb{G}_m)$ for the bidual of C. There is an evaluation map $C \longrightarrow C^{\vee\vee}$ (cf. 1.2.6). It is enough to show that this morphism induces an isomorphism

$$\mathbb{T}_\ell C \xrightarrow{\cong} \mathbb{T}_\ell C^{\vee\vee}$$

Indeed, we have for all $i \geq 0$

$$C \otimes^{\mathbb{L}} \Lambda_i \cong \mathbb{R}\mathcal{H}om(\mathbb{R}\mathcal{H}om(C \otimes^{\mathbb{L}} \Lambda_i, \mathbb{G}_m), \mathbb{G}_m) \cong \mathbb{R}\mathcal{H}om(\mathbb{R}\mathcal{H}om(C, \mathbb{G}_m), \mathbb{G}_m) \otimes^{\mathbb{L}} \Lambda_i = C^{\vee\vee} \otimes^{\mathbb{L}} \Lambda_i$$

The first isomorphism comes from Lemma 1.2.4 and Cartier duality, and the second isomorphism is obvious because both objects are the cone of the multiplication–by–ℓ^i map on $C^{\vee\vee}$. □

– 2.2.8. Let A be a commutative group. We introduce the following four operations on A relative to the prime ℓ

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

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

These are the ℓ–adic completion, the ℓ–adic Tate module, extraction of ℓ–torsion and tensorization with $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Mind that $A/\ell^i A \cong A \otimes \mathbb{Z}/\ell^i\mathbb{Z}$ and that colimits commute with tensor products. These four operations are closely related, as follows.

Given a short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ of commutative groups, there is a long exact sequence of $\mathbb{Z}_\ell$–modules

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

coming from the snake lemma, identifying $- \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ 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

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

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 $A\times B\longrightarrow\mathbb{Q}/\mathbb{Z}$, these operations induce pairings

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

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 $A\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell$ and $\mathrm{T}_\ell A$ are finitely generated, and the torsion groups $A\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell$ and $A[\ell^\infty]$ are of cofinite type. In this context, nondegenerate pairings of groups induce perfect pairings of topological groups.

Proposition 2.2.9. *Let $F:\mathcal{D}^{\mathrm{b}}\mathcal{F}\longrightarrow\mathcal{D}\mathcal{A}b$ be a triangulated functor. For every moderate object C of $\mathcal{D}^{\mathrm{b}}\mathcal{F}$, there is a canonical short exact sequence of $\mathbb{Z}_\ell$–modules*

$$0\longrightarrow H^{i-1}F(C)\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell\longrightarrow H^iF(\mathbb{T}_\ell C)\longrightarrow\mathrm{T}_\ell H^iF(C)\longrightarrow 0$$

and a short exact sequence of ℓ–torsion groups

$$0\longrightarrow H^{i-1}F(C)\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell\longrightarrow H^iF(\mathbb{B}_\ell C)\longrightarrow H^iF(C)[\ell^\infty]\longrightarrow 0$$

both natural in C and F.

Proof. The short exact sequence of constant sheaves $0\longrightarrow\mathbb{Z}\xrightarrow{\ell^i}\mathbb{Z}\longrightarrow\Lambda_i\longrightarrow 0$ induces a long exact sequence of groups

$$H^{i-1}F(C)\longrightarrow H^{i-1}F(C\otimes^{\mathbb{L}}\Lambda_i)\longrightarrow H^iF(C)\xrightarrow{\ell^i}H^iF(C)\longrightarrow H^iF(C\otimes^{\mathbb{L}}\Lambda_i)\longrightarrow H^{i+1}F(C)$$

From this long sequence, we can cut out the short exact sequences

$$0\longrightarrow H^iF(C)\otimes\mathbb{Z}/\ell^i\mathbb{Z}\longrightarrow H^iF(C\otimes^{\mathbb{L}}\Lambda_i)\longrightarrow H^{i+1}F(C)[\ell^i]\longrightarrow 0$$

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

Remark 2.2.10. This applies in particular to cohomology functors, that is, $F=\mathbb{R}\Gamma(S,-)$ and $H^iF=H^i(S,-)$. The first short exact sequence in the proposition reads then

$$0\longrightarrow H^{i-1}(S,C)\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell\longrightarrow H^i(S,\mathbb{T}_\ell C)\longrightarrow\mathrm{T}_\ell H^i(S,C)\longrightarrow 0$$

and link thus the cohomology of an object C with the cohomology of its Tate module. There is of course a spectral sequence behind this.

2.3. The Tate module of a 1–motive

In this section, we specialize what we discussed about Tate modules of complexes to complexes associated with 1–motives.

Definition 2.3.1. Let M be a 1–motive over S. The *ℓ–adic Tate module* associated with M is the ℓ–adic complex

$$\mathbb{T}_\ell M:=\mathbb{T}_\ell[M]=\lim_{i\geq 0}([M]\otimes^{\mathbb{L}}\Lambda_i)[-1]$$

on S.

– 2.3.2. Because the complex $[M]$ is supported in degrees -1 and 0, the Tate module of M has homology in degrees -1, 0 and 1 by Proposition 2.2.4. However, we have always $H^{-1}(\mathbb{T}_\ell M) = 0$ because the torsion of $H^{-1}(M)$ is finite, and $H^1(\mathbb{T}_\ell M)$ is always finite. If $H^{-1}(M)$ is torsion free, then $H^0(\mathbb{T}_\ell M)$ is torsion free as well, and if $H^0(M)$ is divisible as a sheaf, then $H^1(\mathbb{T}_\ell M)$ is trivial. In particular, if M is a torsion free 1–motive, then the homology of $\mathbb{T}_\ell M$ is concentrated in degree 0 only and is torsion free, hence $\mathbb{T}_\ell M$ can be identified with an ordinary torsion free ℓ–adic sheaf on S. We will then usually write

$$\mathrm{T}_\ell M := H^0(\mathbb{T}_\ell M)$$

The weight filtration on M introduces in 1.1.6 induces a filtration on $\mathbb{T}_\ell M$. The diagram given in 1.1.6, together with Proposition 2.2.5 yields a diagram of ℓ–adic complexes

$$\begin{tikzcd}
\mathbb{T}_\ell T \arrow[r, equal] \arrow[d] & \mathbb{T}_\ell T \arrow[d] & \\
\mathbb{T}_\ell G \arrow[r] \arrow[d] & \mathbb{T}_\ell M \arrow[r] \arrow[d] & \mathbb{T}_\ell Y[1] \arrow[d, equal] \\
\mathbb{T}_\ell A \arrow[r] & \mathbb{T}_\ell M_A \arrow[r] & \mathbb{T}_\ell Y[1]
\end{tikzcd}$$

where all columns and rows are exact triangles. Here, M_A is the 1–motive $M/W_{-2}M$, having associated complex $[Y \longrightarrow A]$.

Proposition 2.3.3. *Let M be a 1–motive over S with dual $M^\vee$. There is a canonical, perfect pairing of ℓ–adic complexes*

$$\mathbb{T}_\ell M \otimes \mathbb{T}_\ell M^\vee \longrightarrow \mathbb{Z}_\ell(1)$$

Proof. This is an immediate consequence of Proposition 2.2.7 and Theorem 1.3.1. Observe that truncating $[M^\vee] \cong \mathbb{R}\mathcal{H}om([M], \mathbb{G}_m[1])_{\leq 0} \longrightarrow \mathbb{R}\mathcal{H}om([M], \mathbb{G}_m[1])$ induces an isomorphism on the level of Tate modules, since multiplication by ℓ is an isomorphism on $\mathcal{E}xt^{i+1}([M], \mathbb{G}_m) = H^i\mathbb{R}\mathcal{H}om([M], \mathbb{G}_m[1])$ for $i \geq 1$ by Theorem 1.2.5. $\square$

– 2.3.4. Let M be a torsion–free 1–motive over a field k with algebraic closure $\overline{k}$. The Tate module of M is then an ℓ–adic sheaf on k, corresponding to a $\mathbb{Z}_\ell$–module with continuous $\Gamma := \mathrm{Gal}(\overline{k}|k)$–action. The above diagram becomes then a diagram of $\mathbb{Z}_\ell$–modules with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mathrm{T}_\ell T \arrow[r, equal] \arrow[d] & \mathrm{T}_\ell T \arrow[d] & & \\
0 \arrow[r] & \mathrm{T}_\ell G \arrow[r] \arrow[d] & \mathrm{T}_\ell M \arrow[r] \arrow[d] & Y \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathrm{T}_\ell A \arrow[r] \arrow[d] & \mathrm{T}_\ell M_A \arrow[r] \arrow[d] & Y \otimes \mathbb{Z}_\ell \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

All of these $\mathbb{Z}_\ell$–modules are torsion free and of finite rank. The rank of $\mathrm{T}_\ell M$ equals the sum of the rank of Y as a $\mathbb{Z}$–module, the dimension of T and twice the dimension of A.

– 2.3.5. Again for a torsion free 1–motive over a field k, the Weil pairing becomes a nondegenerate pairing of torsion free ℓ–adic sheaves on k

$$\mathrm{T}_\ell M \otimes \mathrm{T}_\ell M^\vee \longrightarrow \mathbb{Z}_\ell(1)$$

hence $\mathrm{T}_\ell M^\vee \cong \mathrm{Hom}_k(\mathrm{T}_\ell M, \mathbb{Z}_\ell(1))$. This means that in 2.3.4 the corresponding diagram for the dual 1–motive is obtained by applying $\mathrm{Hom}_k(-, \mathbb{Z}_\ell(1))$ to the given diagram and flipping it around the diagonal.

– 2.3.6. We end this section with an explicit description of the Tate module of a torsion free 1–motive over a field k with algebraic closure $\overline{k}$. Consider the complex of Γ–modules $M(\overline{k}) := [Y(\overline{k}) \longrightarrow G(\overline{k})]$. For $i \geq 0$, the homology of $M(\overline{k}) \otimes^{\mathbb{L}} \Lambda_i$ is computed by the cone of the multiplication–by–ℓ^i on $M(\overline{k})$, which is

$$\cdots \longrightarrow 0 \longrightarrow Y(\overline{k}) \longrightarrow Y(\overline{k}) \oplus G(\overline{k}) \longrightarrow G(\overline{k}) \longrightarrow 0 \longrightarrow \cdots$$

in degrees -2, -1 and 0. The first relevant map sends y to $(\ell^i y, u(y))$, the second one sends (y, P) to $u(y) - \ell^i P$. The homology of this complex is concentrated in degree -1, because $Y(\overline{k})$ is torsion free and $G(\overline{k})$ is divisible. We have

$$H^{-1}(M(\overline{k}) \otimes^{\mathbb{L}} \Lambda_i) \cong \frac{\{(y, P) \in Y(\overline{k}) \times G(\overline{k}) \mid u(y) = \ell^i P\}}{\{(\ell^i y, u(y)) \mid y \in Y\}}$$

which is a finite Galois module, depending naturally on M. For all $j \geq i \geq 0$, we have a natural map of Galois modules $H^{-1}(M(\overline{k}) \otimes^{\mathbb{L}} \Lambda_i) \longrightarrow H^{-1}(M(\overline{k}) \otimes^{\mathbb{L}} \Lambda_j$ sending the class of (y, P) to the class of $(y, \ell^{i-j} P)$. The limit with respect to these maps

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

is the ℓ–adic Tate module of M, seen as a Galois module. Explicitly, an element $x \in \mathrm{T}_\ell M$ is given by a sequence $(y_i, P_i)_{i=0}^\infty$ where the y_i's are elements of $Y(\overline{k})$, the P_i's are elements of $G(\overline{k})$, and where it is required that

$$u(y_i) = \ell^i P_i \qquad \text{and that} \qquad \ell P_i - P_{i-1} = u(z_i) \qquad \text{and} \qquad y_i - y_{i-1} = \ell^{i-1} z_i \quad \text{for some } z_i \in Y$$

Two sequences $(y_i, P_i)_{i=0}^\infty$ and $(y_i', P_i')_{i=0}^\infty$ represent the same element if and only if for each $i \geq 0$, there exists a $z_i \in Y$ such that $\ell^i z_i = y_i - y_i'$ and $u(z_i) = P_i - P_i'$.

CHAPTER 3

Cohomology

3.1. Galois cohomology and étale cohomology

In this section, we briefly review some features in Galois cohomology and étale cohomology over "arithmetic" base schemes, and how these notions interact. By arithmetic base scheme, we mean spectra of local fields, of number fields, or open subschemes of the spectrum of the ring of integers of a number field.

– 3.1.1. Let us start with a p–adic field K, that is, a finite extension of $\mathbb{Q}_p$ for some prime p. Let $\mathcal{O}_K$ be the ring of integers of K, and let κ be the finite residue field of characteristic p. Recall (e.g. from [**Mil08**], Theorem I.2.1) that if F is a finite group over K, then the cohomology groups $H^i(K,F)$ are *finite*, and trivial for $i>2$. For future reference, let us retain

Proposition 3.1.2. *Let ℓ be a prime number and let C be a moderate complex on K. The multiplication–by–ℓ map on $H^i(K,C)$ has finite kernel and cokernel.*

This follows from the long exact cohomology sequence associated with $C \xrightarrow{\cdot\ell} C \longrightarrow C\otimes^{\mathbb{L}}\mathbb{Z}/\ell\mathbb{Z}$, noting that the cohomology of $C\otimes^{\mathbb{L}}\mathbb{Z}/\ell\mathbb{Z}$ is finite.

– 3.1.3. Let again F be a finite group over K, let $\overline{K}$ be an algebraic closure of K, and write K^{un} for the maximal unramified extension of K in $\overline{K}$. If the inertia group $\mathrm{Gal}(\overline{K}|K^{\mathrm{un}})$ acts trivially on $F(\overline{K})$, then F is said to be *unramified*. This is the case if and only if F extends to an étale group scheme over $\operatorname{spec}\mathcal{O}_K$.

– 3.1.4. We now come to p–adic "Henselian" fields which we need for the global theory (this will become apparent in the proof of Proposition 3.2.2). Let v be a finite place of a number field k, corresponding to a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_k$ of k. We write $\mathcal{O}_v^{\mathrm{h}}$ for the henselization of the localization of $\mathcal{O}_k$ at $\mathfrak{p}$, and k_v^{h} for the field of fractions of $\mathcal{O}_v^{\mathrm{h}}$. We write $\mathcal{O}_v$ and k_v for the completions of $\mathcal{O}_k^{\mathrm{h}}$ respectively k_v^{h} with respect to v. So, we have inclusions

$$\mathcal{O}_k \subseteq \mathcal{O}_v^{\mathrm{h}} \subseteq \mathcal{O}_v \qquad \subseteq \qquad k \subseteq k_v^{\mathrm{h}} \subseteq k_v$$

Although the complete field k_v is much bigger than k_v^{h} (the former is an uncountable field and the latter countable), the "cohomological behavior" of the two fields is almost the same. This similarity stems from an approximation theorem of Greenberg, stating the following:

Theorem 3.1.5 ([**Gre66**], Theorem 1). *Let V be a variety (an integral scheme, separated and of finite type) over k_v^{h}. Then, the set $V(k_v^{\mathrm{h}})$ is dense in $V(k_v)$ for the v–adic topology.*

In particular, if V is finite over k_v^{h}, then the sets $V(k_v^{\mathrm{h}})$ and $V(k_v)$ are equal. This shows that k_v^{h} is algebraically closed in k_v, hence that the two fields have isomorphic absolute Galois groups.

Proposition 3.1.6. *Let C be a bounded complex of sheaves on k_v^{h} such that $H^i(C)$ is a finite group scheme for all i. The map $H^i(k_v^{\mathrm{h}}, C) \longrightarrow H^i(k_v, C)$ is an isomorphism of finite groups for all $i \in \mathbb{Z}$.*

Indeed, we can look at C as being a complex of Galois modules over k_v^{h}. The absolute Galois groups of k_v^{h} and k_v being isomorphic, the desired isomorphism of Galois cohomology groups follows (here, we consider an algebraic closure of k_v^{h} embedded in an algebraic closure of k_v). Moreover, we know that the groups $H^i(k_v, C)$ are finite by what we discussed in 3.1.1. In particular, note that the statement of Proposition 3.1.2 holds as well over k_v^{h}. It follows also immediately from the corollary that if T is an ℓ–adic complex on k_v^{h}, then the maps $H^i(k_v^{\mathrm{h}}, T) \longrightarrow H^i(k_v, T)$ are isomorphisms. The same goes for ℓ–divisible complexes.

– 3.1.7. We now come to the global case. Let k be a number field with ring of integers $\mathcal{O}_k$ and let U be an open subscheme of $\operatorname{spec} \mathcal{O}_k$. Write k_U for the maximal extension of k in $\overline{k}$ unramified over U and set $\Gamma_U := \mathrm{Gal}(k_U|k)$. The group Γ_U is the étale fundamental group of U with respect to the base point $\operatorname{spec} \overline{k} \longrightarrow U$. There is an equivalence of categories

$$\left\{\begin{matrix}\text{locally constant } \mathbb{Z}\text{–con-} \\ \text{structible sheaves on } U\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{finitely generated dis-} \\ \text{crete } \Gamma_U\text{–modules}\end{matrix}\right\}$$

given by the functor that sends such a sheaf F on U to the Γ_U–module $F(\overline{k}) = F(k_U)$. Let F be a finite, locally constant group scheme on U of order invertible on U, then the canonical morphism

$$H^i(U, F) \xrightarrow{\cong} H^i(\Gamma_U, F)$$

is an isomorphism of finite groups by [**Mil08**] Proposition II.2.9 and Theorem II.2.13. The same holds then of course for any object C in $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$ such that $H^i(C)$ is finite, locally constant and of order invertible on U. For future reference we state

Proposition 3.1.8. *Let ℓ be a prime invertible on $U \subseteq \operatorname{spec} \mathcal{O}_k$ and let C be a moderate complex on U. The multiplication–by–ℓ map on $H^i(U, C)$ has finite kernel and cokernel.*

Indeed, we already mentioned that finite complexes have finite cohomology groups ([**Mil08**], Theorem II.2.13), so the statement of the proposition follows then by considering the long exact cohomology sequence associated with the Kummer triangle $C \longrightarrow C \longrightarrow C \otimes^{\mathbb{L}} \mathbb{Z}/\ell\mathbb{Z}$.

– 3.1.9. Let k be a number field and let C be a complex of sheaves on $U \subseteq \operatorname{spec} \mathcal{O}_k$ such that each $H^i(C)$ is a finite locally constant group scheme on U of order invertible on U. Let S be a set of places of k containing all places not corresponding to a point of U, in particular the infinite places. We write k_S for the maximal extension of k unramified in S, and $\Gamma_S := \mathrm{Gal}(k_S|k)$. Composing the isomorphisms in the preceding paragraph with the inflation map induced by $\Gamma_S \longrightarrow \Gamma_U$ yields morphisms

$$H^i(U, C) \longrightarrow H^i(\Gamma_S, C)$$

Let $\mathfrak{U}$ be the family of those open subschemes $V \subseteq U$ that contain all closed points of $\operatorname{spec} \mathcal{O}_k$ not corresponding to a place in S. The field k_S is the union of the fields k_V for $V \in \mathfrak{U}$, hence Γ_S is the limit of the groups Γ_V. Group cohomology commutes with limits in the first argument ([**NSW00**], Proposition I.1.2.6), so this yields isomorphisms

$$H^i(\Gamma_S, C) \cong H^i(\lim_{V \in \mathfrak{U}} \Gamma_V, C) \cong \operatorname*{colim}_{V \in \mathfrak{U}} H^i(\Gamma_V, C) \cong \operatorname*{colim}_{V \in \mathfrak{U}} H^i(V, C)$$

In less fancy terms, this means that every element of $H^i(\Gamma_S, C)$ is the image of an element in $H^i(V, C)$ for a sufficiently small V, and that every element of $H^i(U, C)$ that maps to zero in $H^i(\Gamma_S, C)$ maps already to zero in $H^i(V, C)$ for a sufficiently small V. Of course, the open U does not really play a role here, if U' is any open in the family $\mathfrak{U}$, we can replace U by U' and C by the restriction of C to U' and compute $H^i(\Gamma_S, C)$ starting from these data. The way one usually uses this computation is to start with a complex of Γ_S–modules, to extend it to a complex of sheaves on some suitable open $U \subseteq \operatorname{spec} \mathcal{O}_k$, and then compute $H^i(\Gamma_S, C)$ by this limit argument. We just remarked that the outcome will not depend on the chosen U and the chosen extension of C. Our next lemma ensures the existence of such extensions.

LEMMA 3.1.10. *Let S be a set of places of k containing all infinite places and let Γ_S be the Galois group of the maximal extension of k unramified outside S. Let C be a bounded complex of discrete Γ_S–modules such that each $H^i(C)$ is finitely generated as a group. Up to replacing C by a quasi–isomorphic complex, there exists an open subscheme U of* $\operatorname{spec} \mathcal{O}_k$ *containing all closed points of* $\operatorname{spec} \mathcal{O}_k$ *that do not correspond to an element of S and an extension of C to a complex of locally constant group schemes on U.*

PROOF. We shall first show that there is a quasi–isomorphism of bounded complexes of discrete Γ_S–modules $B \longrightarrow C$, where each piece of B is finitely generated as a group, and then use the equivalence of categories explained in 3.1.7 in order to extend B to a complex of group schemes as claimed. The complex C is given, say, by

$$0 \longrightarrow C_0 \xrightarrow{d_0} C_1 \xrightarrow{d_1} \cdots \longrightarrow C_d \longrightarrow 0$$

Suppose that for some $i \leq d$ we have found a quasi–isomorphism of complexes $C' \longrightarrow C$ of the form

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & C_0 \arrow[r] \arrow[d, equal] & \cdots \arrow[r] \arrow[d, equal] & C_{i-1} \arrow[r] \arrow[d, equal] & C'_i \arrow[r, "d'_i"] \arrow[d] & B_{i+1} \arrow[r] \arrow[d] & \cdots \arrow[r] \arrow[d] & B_d \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & C_0 \arrow[r] & \cdots \arrow[r] & C_{i-1} \arrow[r] & C_i \arrow[r] & C_{i+1} \arrow[r] & \cdots \arrow[r] & C_d \arrow[r] & 0
\end{tikzcd}$$

where $B_{i+1}, \ldots, B_d$ are Γ_S–modules finitely generated as groups. For $i = d$ we can just take $C' = C$ and the identity morphism so we can go on reasoning by induction on i. Let X be a finite subset of C'_i such that the subgroup of B_{i+1} generated by $d'_i(X)$ is equal to $\operatorname{im} d'_i$, and such that each element of $H^i(C)$ is represented by an element of X. This is possible, since B_{i+1} and hence $\operatorname{im} d'_i$ is finitely generated, as well as $H^i(C)$. Because Γ_S is compact and acts continuously, the set

$$\Gamma_S X = \{\sigma x \mid \sigma \in \Gamma_S, x \in X\}$$

is finite. Replacing X by $\Gamma_S X$ we may suppose that X is Γ_S–invariant. Let B_i be the subgroup of C'_i generated by X. Because X was Γ_S–invariant, B_i is also a Γ_S submodule of C_i. Let C'_{i-1} be the preimage of B_i in C_{i-1}, so that we get a quasi–isomorphism

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & C_0 \arrow[r] \arrow[d, equal] & \cdots \arrow[r] \arrow[d, equal] & C_{i-2} \arrow[r] \arrow[d, equal] & C'_{i-1} \arrow[r] \arrow[d, "\subseteq"'] & B_i \arrow[r] \arrow[d] & B_{i+1} \arrow[r] \arrow[d] & \cdots \arrow[r] \arrow[d] & B_d \arrow[r] \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & C_0 \arrow[r] & \cdots \arrow[r] & C_{i-2} \arrow[r] & C_{i-1} \arrow[r] & C'_i \arrow[r, "d'_i"] & B_{i+1} \arrow[r] & \cdots \arrow[r] & C_d \arrow[r] & 0
\end{tikzcd}$$

This brings us one step further in the induction process, and so the existence of B is proven. Now, since B is bounded, there exists an open $U \subseteq \operatorname{spec} \mathcal{O}_k$ such that each B_i is unramified in all places corresponding to closed points of U, and since the B_i's are actually Γ_S–modules we can take the complement of S to be in U. In other words, the action of Γ_S factors over Γ_U, the Galois group of the maximal extension of k unramified in U. Hence, the complex B extends to a complex of locally constant group schemes on U. $\square$

– 3.1.11. We have seen in 3.1.9 that we can commute Galois cohomology with limits. Similarly, we can commute étale cohomology and limits in the base. If C is a bounded complex of étale sheaves on U, then we have ([**FK87**], Proposition 4.18)

$$H^i(k,C) \cong \operatorname*{colim}_{V\subseteq U} H^1(V,C)$$

where V runs over the open subschemes of U. Again, this means that every element of $H^i(k,C)$ comes from an element of $H^i(V,C)$ for a sufficiently small V, and that every element of $H^i(U,C)$ that maps to zero in $H^i(k,C)$ maps already to zero in $H^i(V,C)$ for a sufficiently small V.

3.2. Compact support cohomology

In this section we review the construction and some basic properties of *compact support cohomology*, following closely Milne's approach in [**Mil08**]. We fix a number field k with ring of integers $\mathcal{O}_k$, and let U be a nonempty open subscheme of $\operatorname{spec}\mathcal{O}_k$. Recall that $\mathcal{F} = \mathcal{F}_U$ stands for the category of fppf sheaves on U. With "sheaf over U" we always mean a sheaf for the fppf topology.

– 3.2.1. Let C be a bounded complex of sheaves over $U \subseteq \operatorname{spec}\mathcal{O}_k$. For every finite place v of k, let $I(k_v) := \mathbb{R}\Gamma(k_v^{\mathrm{h}}, C)$ be a complex of groups which computes étale cohomology of C over k_v^{h}, and for infinite v, let $I(k_v)$ be a complex of groups which computes the Tate modified cohomology ([**NSW00**], I.2) of C over k_v. We write

$$\mathbb{P}(U,C) := \prod_{v\notin U} I(k_v) \qquad \text{and} \qquad P^i(U,C) := H^i\mathbb{P}(U,C) = \prod_{v\notin U} H^i(k_v,C)$$

the products running over all infinite places of k and those finite places of k not corresponding to a closed point of U. We regard $\mathbb{P}(U,C)$ as an object of the derived category of commutative groups $\mathcal{D}\mathcal{A}b$, where it is well defined up to a unique isomorphism. One has a canonical morphism of triangulated functors

$$\alpha : \mathbb{R}\Gamma(U,-) \longrightarrow \mathbb{P}(U,-)$$

On factors corresponding to a finite place, this morphism is given by the natural morphism $\mathbb{R}\Gamma(U,C) \longrightarrow \mathbb{R}\Gamma(k_v,C)$ induced by the maps $\operatorname{spec} k_v \longrightarrow U$. On factors corresponding to an archimedean place, it is given by composing the natural morphisms $\mathbb{R}\Gamma(U,C) \longrightarrow \mathbb{R}\Gamma(k_v,C)$ and $\mathbb{R}\Gamma(k_v,C) \longrightarrow I(k_v)$, the second one given (say) using standard resolutions. Following Milne, we define *cohomology with compact support* of C by

$$\mathbb{C}(U,-) := \operatorname{Cone}\alpha[-1] \qquad \text{and} \qquad H^i_{\mathrm{c}}(U,C) := H^i\mathbb{C}(U,C)$$

The following proposition ([**Mil08**], Proposition II.2.3) lists the basic features of compact support cohomology. For the sake of completeness, and since it is constructive, we sketch the proof.

Proposition 3.2.2. *Let $U \subseteq \operatorname{spec}\mathcal{O}_k$ be an open subscheme. The following holds:*

(1) *There is an exact triangle $\mathbb{C}(U,C) \longrightarrow \mathbb{R}\Gamma(U,C) \longrightarrow \mathbb{P}(U,C)$ giving rise to a long exact sequence of groups $\cdots \longrightarrow P^{i-1}(U,C) \longrightarrow H^i_{\mathrm{c}}(U,C) \longrightarrow H^i(U,C) \longrightarrow P^i(U,C) \longrightarrow \cdots$ natural in C.*
(2) *An exact triangle $C_1 \longrightarrow C_2 \longrightarrow C_3 \longrightarrow C_1[1]$ in $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$ gives rise to a long exact sequence of groups $\cdots \longrightarrow H^{i-1}_{\mathrm{c}}(U,C_3) \longrightarrow H^i_{\mathrm{c}}(U,C_1) \longrightarrow H^i_{\mathrm{c}}(U,C_2) \longrightarrow H^i_{\mathrm{c}}(U,C_3) \longrightarrow \cdots$*
(3) *Let $i : Z \longrightarrow U$ be a closed immersion, and let C be a sheaf on Z. There is a canonical isomorphism $\mathbb{C}(U,i_*C) \cong \mathbb{R}\Gamma(Z,C)$*

(4) *Let V be an open subscheme of U, write $j : V \longrightarrow U$ for the inclusion and let C be a sheaf on V. There is a canonical isomorphism $\mathbb{C}(U, j_!C) \cong \mathbb{C}(V, C)$.*

(5) *Let $j : V \longrightarrow U$ be an open subscheme of U with complement $i : Z \longrightarrow U$, and let C be a complex of sheaves on U. There is a canonical and natural exact triangle*

$$\mathbb{C}(V, j^*C) \longrightarrow \mathbb{C}(U, C) \longrightarrow \mathbb{R}\Gamma(Z, i^*C)$$

in the derived category of commutative groups. In particular, the first map in this triangle gives rise to canonical and natural morphisms $H^i_{\mathrm{c}}(V, j^*C) \longrightarrow H^i_{\mathrm{c}}(U, C)$.

(6) *Let $\pi : U' \longrightarrow U$ be a finite map, and let C be a sheaf on U'. There is a canonical and natural isomorphism $\mathbb{C}(U, \pi_*C) \cong \mathbb{C}(U', C)$.*

Proof. Assertion (1) holds by definition of the cone, and the (2) stems from the elementary fact that the cone of a morphism of triangulated functors is again triangulated (the snake lemma, that is). For (3), observe that $\mathbb{P}(U, i_*C)$ is trivial, since the stalk of j_*C at the generic point is zero. Thus, we have indeed isomorphisms

$$\mathbb{C}(U, j_*C) \cong \mathbb{R}\Gamma(U, j_*C) \cong \mathbb{R}\Gamma(Z, C)$$

To show (4), let Z be the complement of V in U, and consider the relative cohomology sequence of the pair $V \subseteq U$. This sequence comes from an exact triangle

$$\mathbb{R}\Gamma_Z(U, j_!C) \longrightarrow \mathbb{R}\Gamma(U, j_!C) \longrightarrow \mathbb{R}\Gamma(V, C)$$

where Γ_Z is the functor of sections with closed support on Z. Now, Z is just a finite union of closed points, so that by excision ([**Mil80**], III.1.28) and ([**Mil08**], II.1.1) the above exact triangle becomes the middle horizontal row in the following diagram

$$\begin{tikzcd}
 & \mathbb{C}(U, j_!C) \arrow[r, "\cong"] \arrow[d] & \mathbb{C}(V, C) \arrow[d] \\
\prod_{v \in Z} \mathbb{R}\Gamma(k_v^{\mathrm{h}}, C) \arrow[r] \arrow[d, equal] & \mathbb{R}\Gamma(U, j_!C) \arrow[r] \arrow[d] & \mathbb{R}\Gamma(V, C) \arrow[d] \\
\prod_{v \in Z} \mathbb{R}\Gamma(k_v^{\mathrm{h}}, C) \arrow[r] & \mathbb{P}(U, C) \arrow[r] & \mathbb{P}(V, C)
\end{tikzcd}$$

which shows the claim. For (5), let C be a sheaf on U, write again $j : V \longrightarrow U$ for the inclusion and $i : Z \longrightarrow U$ for the inclusion of the closed complement Z of V. We have then an exact sequence of sheaves on U

$$0 \longrightarrow j_!j^*C \longrightarrow C \longrightarrow i_*i^*C \longrightarrow 0$$

Applying the triangulated functor $\mathbb{C}(U, -)$ yields an exact triangle. Taking (3) and (4) into account, this triangle is the triangle we wanted. For (6) it is enough to observe that we have already natural isomorphisms $\mathbb{R}\Gamma(U, \pi_*C) \cong \mathbb{R}\Gamma(U', C)$ and $\mathbb{P}(U, \pi_*C) \cong \mathbb{P}(U', C)$. □

– 3.2.3. If k has no real places, or else if one is morally prepared to ignore the prime 2, then compact support cohomology is given by $H^i_{\mathrm{c}}(U, C) = H^i(\operatorname{spec} \mathcal{O}_k, j_!C)$, where $j : U \longrightarrow \operatorname{spec} \mathcal{O}_k$ is the inclusion. Indeed, we have in any case an isomorphism $H^i_{\mathrm{c}}(U, C) = H^i_{\mathrm{c}}(\operatorname{spec} \mathcal{O}_k, j_!C)$ (property (4)), and $H^i_{\mathrm{c}}(\operatorname{spec} \mathcal{O}_k, j_!C)$ is by definition the homology of the cone

$$\mathbb{C}(\operatorname{spec} \mathcal{O}_k, j_!C) := \operatorname{Cone}\Big(\alpha : \mathbb{R}\Gamma(\operatorname{spec} \mathcal{O}_k, j_!C) \longrightarrow \prod_{v \text{ infinite}} I(k_v)\Big)[-1]$$

where $I(k_v)$ computes the Tate modified cohomology of C over k_v. If all infinite places of k are complex then the $I(k_v)$ are homotopic to zero, hence $\mathbb{C}(\operatorname{spec} \mathcal{O}_k, j_!C)$ is quasi–isomorphic to

$\mathbb{R}\Gamma(\operatorname{spec}\mathcal{O}_k, j_!C)$ in this case. This, covariant functoriality and the existence of long exact sequences explains why the construction is called compact support cohomology. The following diagram commutes:

$$\begin{array}{ccccccc} P^{i-1}(U,C) & \to & H^i_{\mathrm{c}}(U,C) & \longrightarrow & H^i(U,C) & \longrightarrow & P^i(U,C) \\ \uparrow & & \uparrow & & \downarrow & & \uparrow \\ P^{i-1}(V,C) & \to & H^i_{\mathrm{c}}(V,C) & \longrightarrow & H^i(V,C) & \longrightarrow & P^i(V,C) \end{array}$$

The maps $H^i(U,C) \longrightarrow H^i(V,C)$ are restrictions, the maps $H^i_{\mathrm{c}}(V,C) \longrightarrow H^i_{\mathrm{c}}(U,C)$ are those given by property (5) in Proposition 3.2.2, and the maps $P^i(V,C) \longrightarrow P^i(U,C)$ are the projections. That this diagram commutes follows just by bookkeeping the construction of the contravariant functoriality (property (5)) for compact support cohomology. Ignoring the prime 2, this follows as well from elementary formulae for sheaf pull–back and extension by zero.

Proposition 3.2.4. *Let C be a moderate complex on U. For every prime ℓ invertible on U, the multiplication–by–ℓ map on $H^i_{\mathrm{c}}(U,C)$ has finite kernel and cokernel.*

Proof. We have seen in 3.1.2 and 3.1.8 that the analogous statement holds for the groups $P^i(U,C)$ and $H^i(U,C)$. It holds thus for the groups $H^i_{\mathrm{c}}(U,C)$ as well because of the long exact sequence in (1) of Proposition 3.2.2. □

– 3.2.5. **Trace map:** We briefly explain how to compute the cohomology with compact support of the multiplicative group $\mathbb{G}_m$ over an open $U \subseteq \operatorname{spec}\mathcal{O}_k$ following Milne ([**Mil08**], II.2.6). For simplicity we suppose that $U \neq \operatorname{spec}\mathcal{O}_k$, so that there is at least one finite place of k not corresponding to a closed point of U. Recall that if v is a finite place of k, then there is a canonical trace isomorphism

$$\mathrm{tr}_v : H^2(k_v, \mathbb{G}_m) = \mathrm{Br}(k_v) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}$$

By Hilbert 90 we have $H^1(k_v, \mathbb{G}_m) = 0$, and as k_v is of cohomological dimension 2, we have $H^3(k_v, \mathbb{G}_m) = 0$. If v is a real place of k, then the trace isomorphism is

$$\mathrm{tr}_v : H^2(k_v, \mathbb{G}_m) = \mathrm{Br}(k_v) \xrightarrow{\cong} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

and we have still $H^1(k_v, \mathbb{G}_m) = 0$ by Hilbert 90, and $H^3(k_v, \mathbb{G}_m) = 0$. The relevant part of the long exact sequence 3.2.2(1) now reads

$$\mathrm{Pic}(U) \longrightarrow H^2_{\mathrm{c}}(U, \mathbb{G}_m) \longrightarrow \mathrm{Br}(U) \longrightarrow \bigoplus_{v \notin U} \mathrm{Br}(k_v) \longrightarrow H^3_{\mathrm{c}}(U, \mathbb{G}_m) \longrightarrow H^3(U, \mathbb{G}_m)$$

The group $H^3(U, \mathbb{G}_m)$ is trivial by [**Mil08**], II.2.2. By global class field theory (essentially by the theorem of Brauer, Hasse and Noether) we know that a collection of local Brauer elements $(x_v)_{v \notin U}$ with $x_v \in Br(k_v)$ comes from a global Brauer element $x \in \mathrm{Br}(U)$ if and only if the sum of the traces

$$\sum_{v \notin U} \mathrm{tr}_v(x_v)$$

is zero in $\mathbb{Q}/\mathbb{Z}$. Therefore (unless $U = \operatorname{spec}\mathcal{O}_k$), we see that the local trace isomorphisms induce a canonical global isomorphism

$$\mathrm{tr} : H^3_{\mathrm{c}}(U, \mathbb{G}_m) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}$$

In the case $U = \operatorname{spec}\mathcal{O}_k$ we have still an isomorphism $H^3_{\mathrm{c}}(U, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$ ([**Mil08**] Proposition II.2.6), but that case is not interesting for us.

– 3.2.6. **Pairings:** Let A, B and G be objects of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$, and $\varphi : A \otimes^{\mathbb{L}} B \longrightarrow G$ be a morphism. We shall construct canonical morphisms

$$\mathbb{P}(U,A) \otimes^{\mathbb{L}} \mathbb{P}(U,B) \longrightarrow \mathbb{P}(U,C) \qquad \text{and} \qquad \mathbb{R}\Gamma(U,A) \otimes^{\mathbb{L}} \mathbb{C}(U,B) \longrightarrow \mathbb{C}(U,G)$$

in the derived category of commutative groups $\mathcal{D}\mathcal{A}b$, depending naturally on A, B and G. Observe that for any triangulated functor $F : \mathcal{D}\mathcal{F} \longrightarrow \mathcal{D}\mathcal{A}b$ there is a canonical morphism $F(A) \otimes^{\mathbb{L}} F(B) \longrightarrow F(A \otimes^{\mathbb{L}} B)$ in $\mathcal{D}\mathcal{A}b$ (which is an isomorphism if $F(A)$ or $F(B)$ is flat). From this, one obtains the local pairing by composing

$$\mathbb{P}(U,A) \otimes^{\mathbb{L}} \mathbb{P}(U,B) \longrightarrow \mathbb{P}(U, A \otimes^{\mathbb{L}} B) \longrightarrow \mathbb{P}(U,C)$$

The same way, we get also a morphism $\mathbb{R}\Gamma(U,A) \otimes^{\mathbb{L}} \mathbb{R}\Gamma(U,B) \longrightarrow \mathbb{R}\Gamma(U,C)$. We have a canonical "localization" morphism $\alpha_A : \mathbb{R}\Gamma(U,A) \longrightarrow \mathbb{P}(U,A)$, whose cone shifted by 1 computes compact support cohomology by definition, and similarly we have morphisms α_B and α_C. We consider then the following square

$$\begin{tikzcd}
\mathbb{R}\Gamma(U,A) \arrow[d, equal] & \otimes^{\mathbb{L}} & \mathbb{R}\Gamma(U,B) \arrow[r] \arrow[d, "\alpha_B"] & \mathbb{R}\Gamma(U,C) \arrow[d, "\alpha_C"] \\
\mathbb{R}\Gamma(U,A) & \otimes^{\mathbb{L}} & \mathbb{P}(U,B) \arrow[r] & \mathbb{P}(U,C)
\end{tikzcd}$$

where the lower horizontal map is obtained by composing the local pairing with the map α_C in the first variable. The cones of the vertical maps shifted by one degree yield the desired global pairing. From these considerations follows the all–important

Proposition 3.2.7. *Let A and B be objects of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$, and $\varphi : A \otimes^{\mathbb{L}} B \longrightarrow \mathbb{G}_m[1]$ be a morphism. There are canonical and natural pairings*

$$H^i(U,A) \times H^{2-i}_{\mathrm{c}}(U,B) \longrightarrow \mathbb{Q}/\mathbb{Z} \qquad \textit{and} \qquad P^i(U,A) \times P^{1-i}(U,B) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

These pairings are compatible, meaning that the diagram

$$\begin{tikzcd}
P^{i-1}(U,A) \arrow[r] \arrow[d] & H^i_{\mathrm{c}}(U,A) \arrow[r] \arrow[d] & H^i(U,A) \arrow[r] \arrow[d] & P^i(U,A) \arrow[d] \\
P^{2-i}(U,B)^D \arrow[r] & H^{2-i}(U,B)^D \arrow[r] & H^{2-i}_{\mathrm{c}}(U,B)^D \arrow[r] & P^{1-i}(U,B)^D
\end{tikzcd}$$

commutes. Here, $(-)^D$ means $\mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$.

Proof. In 3.2.6, we have constructed a pairing $\mathbb{R}\Gamma(U,A) \otimes^{\mathbb{L}} \mathbb{C}(U,B) \longrightarrow \mathbb{C}(U,G)$ in the derived category of commutative groups $\mathcal{D}\mathcal{A}b$. Taking homology yields pairings

$$H^i(U,A) \times H^j_{\mathrm{c}}(U,B) \longrightarrow H^{i+j+1}_{\mathrm{c}}(U,\mathbb{G}_m)$$

Via the trace isomorphism $H^3_{\mathrm{c}}(U,\mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$, the desired pairings appear. In the case $U = \operatorname{spec} \mathcal{O}_k$, we can still consider $H^3_{\mathrm{c}}(U,\mathbb{G}_m) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ as a subgroup of $\mathbb{Q}/\mathbb{Z}$. For the local pairings, we consider the composition

$$\mathbb{P}(U,A) \otimes^{\mathbb{L}} \mathbb{P}(U,B) \longrightarrow \mathbb{P}(U,\mathbb{G}_m[1]) \longrightarrow \mathbb{C}(U,\mathbb{G}_m[1])[1]$$

Again taking homology and applying the trace isomorphism yields the desired pairings. Alternatively, we could consider first for each individual place $v \notin U$ the pairing

$$H^i(k_v,A) \times H^{1-i}(k_v,B) \longrightarrow H^2(k_v,\mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z} \quad (\text{or } \tfrac{1}{2}\mathbb{Z}/\mathbb{Z})$$

using the local trace isomorphism, and then define the pairing $P^i(U,A) \times P^{1-i}(U,B) \longrightarrow \mathbb{Q}/\mathbb{Z}$ by summing up. By definition of the global trace isomorphism, this amounts to the same. The compatibilities hold already on the level of complexes, by construction. $\square$

3.3. Structure of the cohomology groups of a 1–motive

In this section we show some structure results for the cohomology groups of 1–motives over an arithmetic scheme, meaning either an open subscheme of the spectrum of the ring of integers of a number field, or the spectrum of a number field, or the spectrum of a local field. We begin by recalling two presumably well–known structure results for commutative groups. In this section, *group* always means *commutative group.*

LEMMA 3.3.1. *Let A be a torsion group. If the multiplication–by–ℓ map on A has finite kernel, then there exists an isomorphism $A[\ell^\infty] \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n \oplus F$ for an integer $n \geq 0$ and a finite ℓ–group F. In particular, the following holds*

(1) *The subgroup of divisible elements of $A[\ell^\infty]$ coincides with its maximal divisible subgroup*[1]*.*
(2) *Every subgroup and every quotient of A has the same property.*
(3) *Let $B_0 \supseteq B_1 \supseteq B_2 \cdots$ be a descending chain of subgroups of A, and let B be their intersection. There exists $i \geq 0$ such that $B[\ell^\infty] = B_i[\ell^\infty]$.*

PROOF. By hypothesis, the group $A[\ell]$ is finite, say isomorphic with $(\mathbb{Z}/\ell\mathbb{Z})^m$ for an integer $m \geq 0$. We can thus choose an injection $A[\ell] \longrightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m$. Because $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m$ is divisible, that is, an injective object in the category of commutative groups ([**Rot95**], Theorem 10.23), there exists a filler f in the diagram

$$\begin{tikzcd} A[\ell] \arrow[d, "\subseteq"'] \arrow[dr, hook] & \\ A[\ell^\infty] \arrow[r, dashed, "f"] & (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m \end{tikzcd}$$

The map f is automatically injective, and identifies thus $A[\ell^\infty]$ with a subgroup of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m$. The subgroups of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^m$ are all of the form $(\mathbb{Q}_p/\mathbb{Z}_p)^n \oplus F$ for some $n \leq m$ and some finite F. This shows that $A[\ell^\infty]$ has the claimed structure. Properties (1) and (2) are immediate from this. To show (3), we can suppose that A and the B_i's are ℓ–torsion groups, say $A \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^n \oplus F$ and $B_i \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{n_i} \oplus F_i$. The sequence of integers $n_i \geq 0$ is decreasing, hence stabilizes for sufficiently big i. We can thus suppose that $B_i \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^r \oplus F_i$ for a fixed integer r. But then, B is of finite index in B_i for all i, so we must indeed have $B = B_i$ for some sufficiently big i. □

– 3.3.2. Our next lemma concerns extensions of finitely generated groups by finitely generated free $\mathbb{Z}_p$–module. Such a group T fits thus into an exact sequence

$$0 \longrightarrow \mathbb{Z}_p^r \longrightarrow T \longrightarrow D \longrightarrow 0$$

where D is finitely generated. We can equip T with a topology by taking on $\mathbb{Z}_p^r$ the usual p–adic topology and declaring $\mathbb{Z}_p^r$ to be open in T, so that D is discrete for the quotient topology. This topology on T is canonical, it does not depend on the way we write T as an extension. What we are going to say about such extensions is best formulated in terms of topological groups, even though the structures condition we impose is a purely algebraic condition. We are thus interested in topological groups satisfying

(∗) *The group T is topologically finitely generated and contains an open subgroup isomorphic to a finitely generated free $\mathbb{Z}_p$–module.*

As a topological space such a group T is locally isomorphic to $\mathbb{Z}_p^r$, and the group law $T \times T \longrightarrow T$ is locally given by addition in $\mathbb{Z}_p^r$. This means, as we shall see in section 5.1, that T is a commutative p–adic Lie group of dimension r, and we shall also see that in fact every commutative p–adic Lie group which is topologically finitely generated has this form. This condition (∗) is interesting for the following, presumably well–known reason:

[1]in general, the maximal divisible subgroup is only contained in the subgroup of divisible elements.

PROPOSITION 3.3.3. *Let G be a semiabelian variety over a p–adic field K. The group of rational points $G(K)$ is an extension of a finitely generated group by a finitely generated free $\mathbb{Z}_p$–module.*

PROOF (SKETCH). For an abelian variety A over K this is a classical result of Mattuck (see *Abelian varieties over p–adic fields*, Ann. of Math. **62** (1955), 92–119). More precisely, $A(K)$ is even compact, that is, an extension of a finite group by a finitely generated free $\mathbb{Z}_p$–module. For the multiplicative group $\mathbb{G}_m$ the result can be shown as in Serre's *Cours d'arithmétique*, II.3. Now is G is a torus over K split over $K'|K$, then $G(K')$ is of the form $(*)$, hence $G(K)$ since it is a closed subgroup of $G(K')$. The claim follows by dévissage. □

LEMMA 3.3.4. *Let T be a topological group satisfying $(*)$. Let X be a finitely generated subgroup of T with closure $\overline{X}$. There is an isomorphism of topological groups*

$$T/X \simeq T/\overline{X} \times \overline{X}/X$$

The group $T/\overline{X}$ satisfies again $(*)$, and $\overline{X}/X$ is divisible, carrying the trivial topology (having only two open sets, the empty set and the whole space).

PROOF. We have a tautological sequence $0 \longrightarrow \overline{X}/X \longrightarrow T/X \longrightarrow T/\overline{X} \longrightarrow 0$ of topological groups and continuous morphisms, which is exact as a sequence of abstract groups. We have to show that $T/\overline{X}$ and $\overline{X}/X$ have the claimed structure, and that this short exact sequence has a continuous section.
Let T' be any closed subgroup of T and let us show that T' and T/T' satisfy $(*)$. Choose an open subgroup $L \subseteq T$ which is a finitely generated free $\mathbb{Z}_p$–module. Since L is open, the quotient $D := T/L$ is discrete and topologically finitely generated, since T is so, hence just finitely generated as a group. Since T' is closed in T and since L is open and closed in T, the intersection $L' := L \cap T'$ is closed in L and open in T'. Every closed subgroup of a finitely generated free $\mathbb{Z}_p$–module is again a finitely generated free $\mathbb{Z}_p$–module. Indeed, by closedness the $\mathbb{Z}$–module structure of the subgroup uniquely extends to a continuous $\mathbb{Z}_p$–module structure on one hand, and on the other hand since $\mathbb{Z}_p$ is a principal ideal ring every submodule of a finitely generated free module is finitely generated and free. Hence, L' is a finitely generated $\mathbb{Z}_p$–module and an open subgroup of T'. Writing D' for the image of T' in D, we can write T' as an extension of the finitely generated group D' by L', hence T' satisfies $(*)$. We can write T/T' as an extension of the finitely generated discrete group D/D' by the finitely generated $\mathbb{Z}_p$–module L/L'. Now L/L' is not necessarily free, but certainly contains a finitely generated free $\mathbb{Z}_p$–module as an open subgroup of finite index, which is then also an open subgroup of T/T'. In particular this shows that $T/\overline{X}$ satisfies $(*)$.
The quotient topology on $\overline{X}/X$ is the trivial topology having only two open sets, the empty set and the whole space, because X is dense in $\overline{X}$. Indeed, the preimage in $\overline{X}$ of any open neighborhood of the identity of $\overline{X}/X$ is an open neighborhood U of the identity of $\overline{X}$ such that $X + U = U$. Since X is dense in $\overline{X}$ the intersection $(x + U) \cap X$ is nonempty for all $x \in \overline{X}$, thus we have $U = \overline{X}$ and hence every open neighborhood of the identity of $\overline{X}/X$ is in fact equal to $\overline{X}/X$. Let us show that the group $\overline{X}/X$ is divisible. Indeed, $\overline{X}$ is topologically finitely generated, and contains a finitely generated free $\mathbb{Z}_p$–module as an open subgroup. In particular, the subgroup $n\overline{X}$ of $\overline{X}$ is open and of finite index for every $n > 0$. Hence $n\overline{X}$ contains an element of X for all $n > 0$, and that precisely means that multiplication–by–n is surjective on $\overline{X}/X$.
Finally, let us show that the exact sequence given at the beginning is topologically split. Indeed, because $\overline{X}/X$ is divisible, there exists ([**Rot95**], Theorem 10.23) an section $T/X \longrightarrow \overline{X}/X$ of the given injection $\overline{X}/X \longrightarrow T/X$. Any such section is necessarily continuous because of the topology given on $\overline{X}/X$. Hence, we have a decomposition $T/X \cong T/\overline{X} \times \overline{X}/X$ as topological groups. □

REMARK 3.3.5. Concerning the structure of the divisible group $\overline{X}/X$ in the above proposition, we can be a bit more precise. Indeed, we have

$$\overline{X}/X \simeq \left(V \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^{e-r} \oplus \bigoplus_{\ell \neq p} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{e-r+d} \right)$$

In this expression V is a uniquely divisible group, i.e. a $\mathbb{Q}$–vector space (either trivial or of uncountable dimension) and the integers e, r and d are

$$e := \operatorname{rank} X \qquad \text{and} \qquad r := \operatorname{rank} \overline{X} \qquad \text{and} \qquad d := \dim \overline{X}$$

meaning that: e is the least integer such that e elements generate X modulo torsion, r is the least integer such that r elements of $\overline{X}$ generate a subgroup with open closure of finite index, and d is the least integer such that d elements of $\overline{X}$ generate a subgroup with open closure. This can be seen as follows. By the classification theorem for divisible groups ([**Rot95**], Theorems 10.28 and 10.29), every divisible group is isomorphic to a group

$$V \oplus \bigoplus_{\ell} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\oplus \alpha(\ell)}$$

for a uniquely divisible group V and unique cardinals $\alpha(\ell)$ for each prime number ℓ. Thus, we just need to show that for each prime ℓ and some $i \geq 0$, multiplication by ℓ^i on $\overline{X}/X$ has a finite kernel, containing $\ell^{i(e-r)}$ elements if $\ell = p$ and $\ell^{i(e-r+d)}$ elements if $\ell \neq p$. Indeed, the snake lemma applied to the multiplication–by–ℓ^i map on the short exact sequence $0 \longrightarrow X \longrightarrow \overline{X} \longrightarrow \overline{X}/X \longrightarrow 0$ yields an exact sequence

$$0 \longrightarrow X[\ell^i] \longrightarrow \overline{X}[\ell^i] \longrightarrow \overline{X}/X[\ell^i] \longrightarrow X/\ell^i X \longrightarrow \overline{X}/\ell^i\overline{X} \longrightarrow 0$$

Let us choose i so big that the ℓ-torsion part of X and $\overline{X}$ (which is finite in both cases) is killed by ℓ^i. From the above sequence we get

$$\#\overline{X}/X[\ell^i] \;=\; \frac{\#X/\ell^i X \cdot \#\overline{X}[\ell^i]}{\#X[\ell^i] \cdot \#\overline{X}/\ell^i\overline{X}} \;=\; \ell^{ie} \cdot \frac{\#\overline{X}[\ell^i]}{\#\overline{X}/\ell^i\overline{X}}$$

The group $\overline{X}$ contains a finitely generated $\mathbb{Z}_p$–module as an open subgroup. The $\mathbb{Z}_p$–rank of any such subgroup is d, and the quotient of $\overline{X}$ by this open subgroup is a finitely generated group of $\mathbb{Z}$–rank $r-d$. Hence, the second factor has indeed $\ell^{i(r-d)}$ elements if $\ell \neq p$, and ℓ^{ir} elements in the case $\ell = p$.

– 3.3.6. We now come to structure results for the cohomology of a 1–motive, starting with the local case. Let K be a p–adic field, i.e. a finite extension of $\mathbb{Q}_p$, and let $M = [u : Y \longrightarrow G]$ be a 1-motive over K. We have a long exact cohomology sequence, starting with

$$0 \longrightarrow H^{-1}(K,M) \longrightarrow Y(K) \longrightarrow G(K) \longrightarrow H^0(K,M) \longrightarrow H^1(K,Y) \longrightarrow H^1(K,G) \longrightarrow \cdots$$

We have seen that $G(K)$ contains an open subgroup isomorphic to a finitely generated free $\mathbb{Z}_p$–module. The group $H^1(K,Y)$ is finite, hence $H^0(K,M)$ is essentially the quotient of $G(K)$ by the image of the finitely generated group $Y(K)$. Lemma 3.3.4 precisely explains the structure of such quotients.

PROPOSITION 3.3.7. *Let M be a 1–motive over the p–adic field K. For all i and all primes ℓ, multiplication–by–ℓ has a finite kernel and cokernel on the cohomology group $H^i(K,M)$. These cohomology groups have the following structure*

(1) *The group $H^{-1}(K,M)$ is finitely generated*
(2) *The group $H^0(K,M)$ is a direct sum of a divisible group and a group which is an extension of a finitely generated group by a finitely generated $\mathbb{Z}_p$–module.*

(3) *The groups $H^1(K,M)$ and $H^2(K,M)$ are torsion groups, and $H^2(K,M)$ is divisible*
(4) *For $i<-1$ or $i>2$, the groups $H^i(K,M)$ are trivial.*

Denote by X the image of $Y(K)$ in $G(K)$, and by $\overline{X}$ the closure of X in the p–adic topology on $G(K)$. Then, the divisible subgroup of $H^0(K,M)$ is canonically isomorphic to $\overline{X}/X$.

Proof. The group $H^{-1}(K,M)$ is a subgroup of $Y(K)$ which is finitely generated. The group $H^0(K,M)$ is an extension of $G(K)/X$ and a subgroup of $H^1(K,Y)$ which is finite. The divisible subgroup of $H^0(K,M)$ is thus the same as the divisible subgroup of $G(K)/X$. By Lemma 3.3.4, we know that this quotient is indeed a sum of the divisible group $\overline{X}/X$ and a group which is an extension of a finitely generated group by a finitely generated $\mathbb{Z}_p$–module. For $i\geq 1$, the cohomology groups $H^i(K,Y)$ and $H^i(K,G)$ are torsion, hence the $H^i(K,M)$. The last statement holds because K is of cohomological dimension 2. □

– 3.3.8. Let k be a number field, let v be a finite place of k of residual characteristic p, and let k_v be the completion of k with respect to v. Let $k_v^{\mathrm{h}}\subseteq k_v$ be the field of fractions of the henselization of the localization of $\mathcal{O}_k$ in v, as in 3.1.4. The next proposition, which is a minor generalization of Lemma 2.7 in [**HS05a**] compares the cohomology of a 1–motive over k_v^{h} with its cohomology over the p–adic field k_v.

Proposition 3.3.9. *Let M be a 1–motive on k_v^{h}. Then, the map $H^0(k_v^{\mathrm{h}},M)\longrightarrow H^0(k_v,M)$ is injective and has a uniquely divisible cokernel, and for all $i\neq 0$ the maps $H^i(k_v^{\mathrm{h}},M)\longrightarrow H^i(k_v,M)$ are isomorphisms.*

Proof. Write $M=[Y\longrightarrow G]$, and let us first consider the case $[0\longrightarrow G]$. By Greenberg's approximation theorem, $G(k_v^{\mathrm{h}})$ is dense in $G(k_v)$ for the v–adic topology. For all integers $n\geq 0$, the subgroup $nG(k_v)$ is open in $G(k_v)$, and so are its cosets. Thus every coset of $nG(k_v)$ contains an element of $G(k_v^{\mathrm{h}})$, what shows that the quotient $G(k_v)/G(k_v^{\mathrm{h}})$ is divisible. On the other hand, if $P\in G(k_v)$ is a point such that nP is in $G(k_v^{\mathrm{h}})$, then already P must be in $G(k_v^{\mathrm{h}})$, since k_v^{h} is algebraically closed in k_v. This shows that $G(k_v)/G(k_v^{\mathrm{h}})$ is uniquely divisible.
The Kummer triangle $G\xrightarrow{\cdot n}G\longrightarrow G\otimes^{\mathbb{L}}\mathbb{Z}/n\mathbb{Z}$ induces commutative diagrams with exact rows

$$\begin{tikzcd}
H^{i-1}(k_v^{\mathrm{h}},G\otimes^{\mathbb{L}}\mathbb{Z}/n\mathbb{Z}) \arrow[r] \arrow[d, "\cong"'] & H^i(k_v^{\mathrm{h}},G) \arrow[r, "\cdot n"] \arrow[d] & H^i(k_v^{\mathrm{h}},G) \arrow[d] \\
H^{i-1}(k_v,G\otimes^{\mathbb{L}}\mathbb{Z}/n\mathbb{Z}) \arrow[r] & H^i(k_v,G) \arrow[r, "\cdot n"] & H^i(k_v,G)
\end{tikzcd}$$

for all $i\in\mathbb{Z}$ and $n>0$. In order to show that the map $H^i(k_v^{\mathrm{h}},G)\longrightarrow H^i(k_v,G)$ is an isomorphism, it is enough to show that the map

$$H^{i-1}(k_v^{\mathrm{h}},G)/nH^{i-1}(k_v^{\mathrm{h}},G)\longrightarrow H^{i-1}(k_v,G)/nH^{i-1}(k_v,G)$$

is an isomorphism for all $n>0$. For $i=1$ we know that already, and for $i>1$, this follows by induction. This settles the proposition for $[0\longrightarrow G]$. The morphisms $H^i(k_v^{\mathrm{h}},Y)\longrightarrow H^i(k_v,Y)$ are isomorphisms for all i, since k_v^{h} is closed in k_v. The general case follows now by dévissage. □

– 3.3.10. We now come to structure results over a global base. Let k be a number field with ring of integers $\mathcal{O}_k$, and let U be a open subscheme of $\operatorname{spec}\mathcal{O}_k$. While the cohomology groups $H^i(k,M)$ for a 1–motive M over k are not very handy (they are in some sense “too big”) the cohomology groups $H^i(U,M)$ for a 1–motive M over U behave nicely, as the next proposition shows.

Proposition 3.3.11. *Let M be a 1–motive over U. Then*

(1) *the groups $H^{-1}(U,M)$, $H^0(U,M)$ and $H^0_c(U,M)$ are finitely generated*
(2) *for $i \geq 1$, the groups $H^i(U,M)$ are torsion groups, and so are $H^i_c(U,M)$ for $i \geq 2$*

If ℓ is a prime number invertible on U, the multiplication by ℓ has a finite kernel and cokernel on $H^i(U,M)$ and $H^i_c(U,M)$.

Proof. That $H^{-1}(U,M)$ is finitely generated is clear, since $H^{-1}(U,M) = \ker(Y(U) \longrightarrow G(U))$. That $H^0(U,M)$ is finitely generated follows from the Mordell–Weil theorem, Dirichlet's unit theorem and dévissage. From this and again dévissage it follows that $H^0_c(U,M)$ is finitely generated. The groups $H^i(U,M)$ are torsion because étale cohomology groups in degree $i > 0$ of any group scheme are torsion. That $H^i_c(U,M)$ is torsion for $i \geq 2$ follows from the long exact sequence relating cohomology with compact support cohomology. The additional statement follows from 3.1.8 and 3.2.4. $\square$

– 3.3.12. For $i \geq 3$, the groups $H^i(U,M)$ are finite groups of exponent 2, depending only on the real places of k and for $i < -1$ they are trivial. Likewise, the groups $H^i_c(U,M)$ are finite groups of exponent 2, depending only on the real places of k for $i \leq 0$, and trivial for $i \geq 3$.

Proposition 3.3.13. *Let $M = [Y \longrightarrow G]$ be a 1–motive over a number field k. Then $H^0(k,M)$ is isomorphic to a direct sum of a free group and a finite group.*
More generally, let $k_0|k$ be a Galois extension with Galois group Γ_0, and write $M(k_0)$ for the complex of Γ_0–modules $[Y(k_0) \longrightarrow G(k_0)]$. Then $H^0(\Gamma_0, M(k_0))$ is isomorphic to a direct sum of a free group and a finite group.

Proof. For brevity, let us call a group *almost free* if it is isomorphic to a direct sum of a free group and a finite group. Write A and T for the abelian, respectively the toric part of G.
The group $A(k)$ is of finite type by the Mordell–Weil theorem, hence almost free. The group $\mathbb{G}_m(k)$, hence any power $\mathbb{G}_m^r(k)$ is almost free, because k^* it is the sum of the finite group of roots of unity of k and a subgroup of the free group of divisors $\mathrm{Div}(k)$. Choose a finite extension k' of k over which T splits. Then, $T(k)$ is a subgroup of the almost free group $T(k')$, and we have an exact sequence

$$0 \longrightarrow T(k) \longrightarrow G(k) \longrightarrow A(k)$$

Thus, in order to show that $G(k)$ is almost free it is enough to show that the class of almost free groups is stable under taking subgroups and extensions. We check this in Proposition 3.3.14 below. There is an exact sequence $Y^\Gamma \longrightarrow G(k) \longrightarrow H^0(\Gamma_0, M) \longrightarrow H^1(\Gamma_0, Y)$. The group Y^Γ is of finite type and $H^1(\Gamma_0, Y)$ is even finite, and we have seen that $G(k)$ is almost free. We shall also check in Proposition 3.3.14 that the quotient of an almost free group by a group of finite type is almost free, hence $H^0(\Gamma_0, M)$ is almost free, as claimed. $\square$

Proposition 3.3.14. *Every quotient of an almost free group by a finitely generated group is almost free, and the class of almost free groups is stable under extensions.*

Proof. Let G be a finitely generated subgroup of the almost free group $L \oplus F$ where L is free and F is finite. Let $(e_i)_{i \in I}$ be a $\mathbb{Z}$–basis of L and let $g_1, \ldots, g_n$ be generators of G. Each g_j can be uniquely written as a sum

$$g_j = f_j + \sum_{i \in I} a_{ij} e_i$$

of an element $f_j \in F$ and a finite $\mathbb{Z}$–linear combination of the e_i's. Let $e_1, \dots, e_m$ be the set of those basis elements of L occurring in these linear combinations. Then we have $L = L' \oplus L''$, where L' is the factor of L generated by $e_1, \dots, e_m$. The group G is a subgroup of $F \oplus L'$, and we have

$$(F \oplus L)/G \cong (F \oplus L')/G \oplus L''$$

But L' and hence $(F \oplus L')/G$ are finitely generated, hence isomorphic to a sum of a free group and a finite group. The first claim follows. Now let E be an extension of two almost free groups, i.e. there exist free groups L_1 and L_2 and finite groups F_1 and F_2 and a short exact sequence

$$0 \longrightarrow L_1 \oplus F_1 \longrightarrow E \longrightarrow L_2 \oplus F_2 \longrightarrow 0$$

We must show that E is isomorphic to the sum of a free group and a finite group. Let E' be the subgroup of E consisting of the elements mapping to the finite group F_2. Then E is an extension of L_2 by E', and since L_2 is free there exists an isomorphism $E \simeq E' \oplus L_2$. It remains to show that E' is almost free. The group E' sits in a short exact sequence

$$0 \longrightarrow L_1 \oplus F_1 \longrightarrow E' \longrightarrow F_2 \longrightarrow 0$$

Let G' be a finitely generated subgroup of E' mapping surjectively onto F_2, and let G be the intersection of G' with $L_1 \oplus F_1$. We have already shown that $E'/G' \cong (L_1 \oplus F_1)/G$ is almost free, hence isomorphic to $L' \oplus F'$, with L' free and F' finite. We find a short exact sequence

$$0 \longrightarrow G' \longrightarrow E' \longrightarrow L' \oplus F' \longrightarrow 0$$

Let E'' be the subgroup of E' consisting of the elements mapping to the finite group F'. Then E' is an extension of L' by E'', and since L' is free there exists an isomorphism $E' \simeq E'' \oplus L'$. But E'' is finitely generated, so in particular almost free. This shows that E', and hence E are almost free. $\square$

Corollary 3.3.15. *Let $M = [u : Y \longrightarrow G]$ be a 1–motive over the number field k, and write $Z := H^{-1}(M) = \ker u$. There is a canonical isomorphism $Z(k) \otimes \mathbb{Z}_\ell \cong H^0(k, \mathbb{T}_\ell M)$.*

Proof. From 2.2.9 we get a short exact sequence

$$0 \longrightarrow Z(k) \otimes \mathbb{Z}_\ell \longrightarrow H^0(k, \mathbb{T}_\ell M) \longrightarrow \mathrm{T}_\ell H^0(k, M) \longrightarrow 0$$

because the torsion subgroup of $H^0(k, M)$ is finite by Proposition 3.3.13, the last group in this sequence vanishes, hence the desired canonical isomorphism. $\square$

3.4. Tate–Shafarevich groups

We introduce two kinds of groups consisting of global cohomology classes that are locally everywhere trivial. Among them, of course, the Tate–Shafarevich groups

Definition 3.4.1. Let S be a set of places of k, and let C be a bounded complex of continuous Γ_S–modules. For $i \in \mathbb{Z}$, we define the *Tate–Shafarevich group* relative to S by

$$Ш^i_S(k, C) := \ker\Big(H^i(\Gamma_S, C) \longrightarrow P^i_S(k, C)\Big)$$

where $P^i_S(k, C)$ is the restricted product of the groups $H^i(k_v^{\mathrm{h}}, C)_{v \in S}$ with respect to the maps $r_v : H^i(\mathcal{O}_v^{\mathrm{h}}, C) \longrightarrow H^i(k_v^{\mathrm{h}}, C)$. In words, an element of $H^i(\Gamma_S, C)$ belongs to $Ш^i_S(k, C)$ if for all places $v \in S$ it maps to zero in $H^i(k_v, C)$, and if for all but finitely many places $v \in S$ where it is unramified it maps to zero already in $H^i(\mathcal{O}_v^{\mathrm{h}}, C)$. In the case S is the set of all places of k, we drop it from the notation.

– 3.4.2. In the case where the maps $H^i(\mathcal{O}_v^{\mathrm{h}}, C) \longrightarrow H^i(k_v^{\mathrm{h}}, C)$ are almost all injective we can forget about the restricted product and have just

$$Ш^i_S(k, C) := \ker \Big(H^i(\Gamma_S, C) \longrightarrow \prod_{v \in S} H^i(k_v^{\mathrm{h}}, C) \Big)$$

We could also define $Ш^i_S(k, C)$ using the groups $H^i(k_v, C)$ rather than $H^i(k_v^{\mathrm{h}}, C)$. Indeed, the Galois cohomology groups $H^i(k_v, C)$ and $H^i(k_v^{\mathrm{h}}, C)$ are isomorphic, as k_v and k_v^{h} have isomorphic absolute Galois groups. We find it nicer to work with the fields k_v^{h} because this fits better with compact support cohomology. We will also have to consider the following integral variant of the Tate–Shafarevich group:

Definition 3.4.3. Let U be an open subscheme of $\operatorname{spec} \mathcal{O}_k$ and let C be a bounded complex of sheaves on U. We write

$$D^i(U, C) := \ker \big(H^i(U, C) \longrightarrow P^i(U, C) \big)$$

where $P^i(U, C)$ is the product of the groups $H^i(k_v^{\mathrm{h}}, C)$ over the finite or infinite places of k not corresponding to a closed point of U (c.f. 3.2.1).

– 3.4.4. The long exact sequence relating cohomology and compact support cohomology shows that

$$D^i(U, C) \cong \operatorname{im} \big(H^i_{\mathrm{c}}(U, C) \longrightarrow H^i(U, C) \big) \cong \operatorname{coker} \big(P^{i-1}(U, C) \longrightarrow H^i_{\mathrm{c}}(U, C) \big)$$

The interest of these groups is that they provide a good approximation to Tate–Shafarevich groups on one hand, and that on the other hand pairings are easily defined for them, as we can see immediately

Proposition 3.4.5. *Let U be an open subscheme of* $\operatorname{spec} \mathcal{O}_k$ *and let C be an object in $\mathcal{D}^{\mathrm{b}} \mathcal{F}_U$. Let S be a set of places of k. There are canonical and natural pairings*

$$D^i(U, C) \times D^{2-i}(U, C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

Proof. From Proposition 3.2.7, definition of $D^i(U, C)$ and the remark following it, we get a diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & D^i(U,C) \arrow[r] \arrow[d, dotted] & H^i(U,C) \arrow[r] \arrow[d] & P^i(U,C) \arrow[d] \\
0 \arrow[r] & D^{2-i}(U,C^\vee)^D \arrow[r] & H^{2-i}_{\mathrm{c}}(U,C^\vee)^D \arrow[r] & P^{1-i}(U,C^\vee)^D
\end{tikzcd}$$

The pairing we wanted is then given by the dotted arrow. Naturality follows from naturality of the pairings in 3.2.7. □

Lemma 3.4.6. *Let S be a set of places of k containing all infinite places, let $V \subseteq U$ be open subschemes of* $\operatorname{spec} \mathcal{O}_k$ *containing all closed points* $\operatorname{spec} \mathcal{O}_k$ *that do not correspond to an element of S, and let C be a complex of sheaves on U. The image of $D^i(V, C)$ in $H^i(\Gamma_S, C)$ is contained in the image of $D^i(U, C)$.*

Proof. By the previous remark, the image if $D^i(U,C)$ in $H^i(\Gamma_S,C)$ is the same as the image of $H^i_{\mathrm{c}}(U,C)$ via the following diagram

$$\begin{tikzcd} H^i_{\mathrm{c}}(U,C) \arrow[r] & H^i(U,C) \arrow[d] \arrow[dr] & \\ H^i_{\mathrm{c}}(V,C) \arrow[r] \arrow[u] & H^i(V,C) \arrow[r] & H^i(\Gamma_S,C) \end{tikzcd}$$

This shows the claimed inclusion. □

3.5. Duality theorems for finite complexes

The goal of this section is to extend three duality theorems which are classically known for finite group schemes to bounded complexes of sheaves, whose homology groups are finite group schemes. These duality theorems are the following, each of which I shall recall at the given place: The Artin–Verdier duality for finite groups over a p–adic field, its global version for finite locally constant group schemes over a finite localization of the ring of integers of a number field, and the Poitou–Tate duality theorem for finite Galois modules over a number field.
That these generalizations hold for the local and global Artin–Verdier dualities is fairly immediate, the thankless task of proving them consists of screwing up the complexes and proceed on induction on their length. To prove the Poitou–Tate duality for complexes is slightly more challenging.

– 3.5.1. **The local duality theorem of Tate and Nakayama.** Let p be a prime number and let K be a p–adic field, that is, a finite extension of $\mathbb{Q}_p$. By local class field theory, we have an isomorphism

$$H^2(K,\mathbb{G}_m) \cong \operatorname{Br} K \cong \mathbb{Q}/\mathbb{Z}$$

Now let F be a finite group scheme over K, with Cartier dual $F^\vee = \mathcal{H}om(F,\mathbb{G}_m)$. The canonical evaluation map $F \otimes F^\vee \longrightarrow \mathbb{G}_m$ yields pairings of cohomology groups $H^i(K,F) \times H^j(K,F^\vee) \longrightarrow H^{i+j}(K,\mathbb{G}_m)$. The local duality theorem ([**NSW00**], Theorem 7.2.9 or [**Mil08**] Theorem I.2.14) states that the pairings

$$H^i(K,F) \times H^{2-i}(K,F^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of finite groups.

Proposition 3.5.2. *Let C be an object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_K$ such that $H^r(C)$ is a finite group over K for all $r \in \mathbb{Z}$, and write $C^\vee := \mathbb{R}\mathcal{H}om(C,\mathbb{G}_m)$. The canonical pairings*

$$H^i(K,C) \times H^{2-i}(K,C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of finite groups for all $i \in \mathbb{Z}$.

Proof. Without loss of generality, we can assume that $H^i(C) = 0$ except for $0 \le i \le n$ for some integer $n \ge 0$. We proceed by induction on n. For $n = 0$ there is nothing to prove, so we assume that $n > 0$, and that the proposition holds for complexes with homology concentrated in degrees $0 \le i < n$. By hypothesis, $F := H^n(C)$ is a finite group scheme over K. Let $C_{\le n-1}$ be the truncation of C at degree $n-1$, so that we get an exact triangle

$$C_{\le n-1} \longrightarrow C \longrightarrow F[-n]$$

The homology of $C^\vee$ is concentrated in degrees $-n \leq i \leq 0$, and applying $\mathbb{R}\mathcal{H}om(-,\mathbb{G}_m)$ to the above triangle yields a triangle

$$F^\vee[n] \longrightarrow C^\vee \longrightarrow (C_{\leq n-1})^\vee$$

where $F^\vee = \mathcal{H}om(F,\mathbb{G}_m)$ is the Cartier dual of F. This uses that K is of characteristic zero and Lemma 1.2.4 which implies that $\mathcal{E}xt^i(F,\mathbb{G}_m) = 0$ for all $i > 0$. The long exact cohomology sequences associated with these triangles fit into a diagram

$$\begin{tikzcd}
\cdots \arrow[r] & H^i(K,C_{\leq n-1}) \arrow[r] \arrow[d, "\alpha_i"'] & H^i(K,C) \arrow[r] \arrow[d, "\beta_i"'] & H^{i-n}(K,F) \arrow[r] \arrow[d, "\gamma_i"'] & \cdots \\
\cdots \arrow[r] & H^{2-i}(K,C_{\leq n-1})^D \arrow[r] & H^{2-i}(K,C)^D \arrow[r] & H^{2-i+n}(K,F^\vee)^D \arrow[r] & \cdots
\end{tikzcd}$$

where $(-)^D = \mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$. The maps α_i and γ_i are isomorphisms by the classical local Artin–Verdier duality theorem and by the induction hypothesis. Hence, the maps β_i are isomorphisms, by the five lemma. □

COROLLARY 3.5.3. *Let C be a moderate object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_K$, and write $C^\vee := \mathbb{R}\mathcal{H}om(C,\mathbb{G}_m)$. The canonical pairings*

$$H^i(K,\mathbb{T}_\ell C) \times H^{2-i}(K,\mathbb{B}_\ell C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of topological groups for all $i \in \mathbb{Z}$.

PROOF. This follows from 3.5.2 and taking limits. □

– 3.5.4. **The Artin–Verdier duality theorem.** Let k be a number field, and let $U \subseteq \operatorname{spec} \mathcal{O}_k$ bs a nonempty open subscheme. By global class field theory, we have an isomorphism $H^3_{\mathrm{c}}(U,\mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$, as we computed in 3.2.5. Let F be a finite locally constant group scheme over U whose order is invertible on U, with Cartier dual $F^\vee$. The canonical adjunction map $F \otimes F^\vee \longrightarrow \mathbb{G}_m$ yields pairings

$$H^i(U,F) \times H^{i-3}_{\mathrm{c}}(U,F^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

The duality theorem of Artin and Verdier ([**Mil08**] Corollary II.3.3.) states that the pairings are perfect pairings of finite groups.

PROPOSITION 3.5.5. *Let C be an object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$ such that $H^r(C)$ is a finite locally constant group scheme over U of order invertible on U for all $r \in \mathbb{Z}$, and write $C^\vee := \mathbb{R}\mathcal{H}om(C,\mathbb{G}_m)$. Then, the canonical pairings*

$$H^i(U,C) \times H^{3-i}_{\mathrm{c}}(U,C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of finite groups for all $i \in \mathbb{Z}$.

PROOF. Same as for 3.5.2. Mind that since the order of F is invertible on U the group scheme F is locally constant, and therefore we have $\mathcal{E}xt^i(F,\mathbb{G}_m) = 0$ for all $i > 0$ by Lemma 1.2.4. □

COROLLARY 3.5.6. *Let C be a moderate object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$, and write $C^\vee := \mathbb{R}\mathcal{H}om(C,\mathbb{G}_m)$. Let ℓ be a prime number invertible on U. Then, the canonical pairings*

$$H^i(U,\mathbb{T}_\ell C) \times H^{3-i}_{\mathrm{c}}(U,\mathbb{B}_\ell C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z} \qquad \text{and} \qquad H^i(U,\mathbb{B}_\ell C) \times H^{3-i}_{\mathrm{c}}(U,\mathbb{T}_\ell C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of topological groups for all $i \in \mathbb{Z}$.

COROLLARY 3.5.7. *Let C be an object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_U$ such that $H^r(C)$ is a finite locally constant group scheme over U of order invertible on U. The canonical pairing*

$$D^i(U,C) \times D^{3-i}(U,C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups.

PROOF. Indeed, this pairing comes by definition from a diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & D^i(U,C) \arrow[r] \arrow[d] & H^i(U,C) \arrow[r] \arrow[d, "\cong"] & P^i(U,C) \arrow[d, "\cong"] \\ 0 \arrow[r] & D^{3-i}(U,C^\vee)^D \arrow[r] & H^{3-i}_{\mathrm{c}}(U,C^\vee)^D \arrow[r] & P^{2-i}(U,C^\vee)^D \end{tikzcd}$$

All groups in this diagram are finite. The second and third vertical map are isomorphisms by 3.5.5 and 3.5.2 respectively. □

– 3.5.8. **The Poitou–Tate duality theorem.** Let k be a number field with fixed algebraic closure, let S be a set of places of k containing the infinite places, and define k_S and Γ_S as in 3.1.9. Let F be a finite continuous Γ_S–module of order in $\mathbb{N}(S)$ and let $F^\vee$ be its dual. The Poitou–Tate duality theorem ([**NSW00**], Theorem 8.6.8) asserts that there exist canonical pairings

$$\text{Ш}^i_S(k,F) \times \text{Ш}^{3-i}_S(k,F^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

and that these are perfect pairings of finite groups for all $i \in \mathbb{Z}$. Except for $i = 1$ of $i = 2$ they are trivial. Again, this continues to hold when we replace F by a finite complex. Recall that to give a finite continuous Γ_S–module is the same as to give a finite k group scheme which is unramified outside S, or else, a finite k–group scheme which extends to an étale group scheme over $\operatorname{spec} \mathcal{O}_v$ for all $v \notin S$, where $\mathcal{O}_v$ is the ring of integers of the local field k_v.

THEOREM 3.5.9. *Let C be a complex in $\mathcal{D}^{\mathrm{b}}\mathcal{F}_k$ such that each $H^i(C)$ is finite of order in $\mathbb{N}(S)$ and unramified outside S for all i, and write $C^\vee := \mathbb{R}\mathcal{H}om(C, \mathbb{G}_m)$. There are canonical, perfect pairings finite groups*

$$\text{Ш}^i_S(k,C) \times \text{Ш}^{3-i}_S(k,C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

– 3.5.10. The proof of this is less straightforward since we can not use dévissage anymore by lack of any apparent exactness properties of the functor $\text{Ш}^i_S(k,-)$. The proof of 3.5.9 consists rather of combining the already proven duality theorems for finite complexes. We give a complete proof for the case when S contains all infinite places as we suppose, and indicate then briefly how one can get rid of this hypothesis. We need two preparatory lemmas, generalizing Lemmas 4.6 and 4.7 of [**HS05a**].

LEMMA 3.5.11. *Let R be a henselian discrete valuation ring with field of fractions K of characteristic zero and finite residue field κ of characteristic $p > 0$, and let C be a bounded complex of fppf sheaves on R such that $H^i(C)$ is a finite group scheme on R of order prime to p for all i. The restriction map $H^i(R,C) \longrightarrow H^i(K,C)$ is injective for all i.*

PROOF. Let F be a finite locally constant group scheme on R of order prime to p. Because F is proper, equality $F(R) = F(K)$ holds. The restriction $H^1(R,F) \longrightarrow H^1(K,F)$ is injective. Indeed, the kernel of this map corresponds to F–torsors on R that have a K–point, and by properness such a torsor has already a R–point. For $i > 1$, the group $H^i(R,F)$ is trivial, because $H^i(R,F) \cong H^i(\kappa,F)$ by Proposition II.1.1 of [**Mil08**]. This shows the lemma in the case C is concentrated in one degree.

We continue by induction. Suppose C is concentrated in degrees $0 \leq i \leq n$ and suppose that the lemma holds for shorter complexes. Set $F := H^n(C)$. The truncation triangle

$$C_{<n} \longrightarrow C \longrightarrow F[-n] \longrightarrow C_{<n}[1]$$

induces an exact sequences for cohomology over R and over K. In degrees $i < n$ the cohomology of $F[-n]$ is trivial, hence the statement of the lemma holds in these degrees. In degree $n+1$, we have $H^{n+1}(R, C_{<n}) = 0$, hence an isomorphism $H^{n+1}(R, C) \cong H^1(R, F)$, and $H^1(R, F)$ injects to $H^1(K, F)$ as we already have seen. Hence injectivity of $H^{n+1}(R, C) \longrightarrow H^{n+1}(K, C)$. In degrees $i > n+1$ everything is trivial, so it remains to discuss the case $i = n$. The relevant part of the long exact sequences reads

$$\begin{tikzcd}
0 \arrow[r] & H^n(R, C_{<n}) \arrow[r] \arrow[d, hook] & H^n(R, C) \arrow[r] \arrow[d] & F(R) \arrow[d, equal] \\
0 \arrow[r] & H^n(K, C_{<n}) \arrow[r] & H^n(K, C) \arrow[r] & F(K)
\end{tikzcd}$$

By induction hypothesis the left hand vertical map is injective and the right vertical map is an isomorphism by properness of F, hence of injectivity the vertical map in the middle. □

Lemma 3.5.12. *Let $U \subseteq \operatorname{spec} \mathcal{O}_k$ be an open subscheme, let S be a set of places of k containing all places not corresponding to a closed point of U and let Γ_S be the Galois group of the maximal extension of k unramified outside S. Let C be a bounded complex of group schemes on U such that each $H^i(C)$ is finite of order invertible on U.*[2]
For every sufficiently small open subscheme $V \subseteq U$ containing the complement of S the image of $D^i(V, C)$ in $H^i(\Gamma_S, C)$ is exactly $Ш^i_S(k, C)$.

Proof. Let $\mathfrak{U}$ be the family of those open subschemes $V \subseteq U$ that contain all closed points $\operatorname{spec} \mathcal{O}_k$ not corresponding to an element of S. For an open $V \in \mathfrak{U}$, write $\mathcal{D}^i(V, C)$ for the image of $D^i(V, C)$ in $H^i(\Gamma_S, C)$. We claim that the equality

$$Ш^i_S(k, C) = \bigcap_{V \in \mathfrak{U}} \mathcal{D}^i(V, C)$$

holds. If we show this we are done, since all groups $\mathcal{D}^i(V, C)$ are finite, hence equality $Ш^i_S(k, C) = \mathcal{D}^i(V, C)$ must hold for sufficiently small V by Lemma 3.4.6. We check both inclusions.
$\subseteq$: Take $x \in Ш^i_S(k, C) \subseteq H^i(\Gamma_S, C)$, let $V \in \mathfrak{U}$, and let us show that $x \in \mathcal{D}^i(V, C)$. As explained in 3.1.9 there exists an open $W \in \mathfrak{U}$ contained in V and such that x is the image of some $y \in H^i(W, C)$. If v is any place of k, then the image of y in $H^i(k_v, C)$ is the same as the image of x in $H^i(k_v, C)$ which is zero by definition of $Ш^i_S(k, C)$. As this holds in particular for all v that do not correspond to a closed point of W, we see that y is in $D^i(W, C)$, and hence $x \in \mathcal{D}^i(W, C)$. But as $\mathcal{D}^i(W, C) \subseteq \mathcal{D}^i(V, C)$, we have also $x \in \mathcal{D}^i(V, C)$.
$\supseteq$: Take $x \in H^i(\Gamma_S, C)$ such that $x \in \mathcal{D}^i(V, C)$ for all V. If v is a place of S, then we can choose an open $V \in \mathfrak{U}$ not containing v as a closed point. As $x \in \mathcal{D}^i(V, C)$, there is $y \in D^i(V, C)$ having x as image. But the image of y in $H^i(k_v, C)$ is zero by definition of $D^i(V, C)$. The image of x in $H^i(k_v, C)$ is thus zero. Together with Lemma 3.5.11, this shows that x is in $Ш^i_S(k, C)$. □

[2]So in particular if we regard C as a complex of Γ_S–modules, then the order of $H^i(C)$ is in $\mathbb{N}(S)$. Reciprocally, we have shown in Lemma 3.1.10 that if we start with a bounded complex of Γ_S–modules with each $H^i(C)$ of order in $\mathbb{N}(S)$, then up to replacing C by a quasi–isomorphic complex we may extend C to a complex of group schemes on a sufficiently small open $U \subseteq \operatorname{spec} \mathcal{O}_k$ containing the complement of S.

Proof of Theorem 3.5.9. We suppose that S contains all infinite places. By Lemmas 3.1.10 and 3.5.12, we can (replacing C by a quasi–isomorphic complex if necessary) choose an open $U \subseteq \operatorname{spec} \mathcal{O}_k$ containing all closed points $\operatorname{spec} \mathcal{O}_k$ that do not correspond to an element of S and an extension of C to a complex on U such that the image of $D^i(U,C)$ in $H^i(\Gamma_S, C)$ is exactly $Ш^i_S(k,C)$. Because $D^i(U,C)$ is finite, we can choose an open subscheme V of U containing the complement of S, such that every element of $D^i(U,C)$ that maps to zero in $H^i(\Gamma_S, C)$ maps already to zero in $H^i(V,C)$. The image of $D^i(V,C)$ in $H^i(\Gamma_S, C)$ is then $Ш^i_S(k,C)$ as well. We claim that the image of $D^i(U,C)$ in $H^i(V,C)$ equals $D^i(V,C)$. Indeed, we have the following two diagrams

$$\begin{tikzcd} H^i_{\mathrm{c}}(U,C) \arrow[r] \arrow[dr, dotted] & H^i(U,C) \arrow[d, "\alpha"] \\ H^i_{\mathrm{c}}(V,C) \arrow[u] \arrow[r] & H^i(V,C) \end{tikzcd} \qquad \begin{tikzcd} D^i(V,C) \arrow[r, "\subseteq"] \arrow[dr] & \alpha D^i(U,C) \arrow[d, "\cong"] \\ & Ш^i_S(k,C) \end{tikzcd}$$

The groups $D^i(U,C)$ and $D^i(V,C)$ are the image of the horizontal maps in the left hand diagram, hence $\alpha D^i(U,C)$, which is the image of the dotted arrow, contains $D^i(V,C)$. This explains then the inclusion in the right hand diagram. The vertical map in this diagram is an isomorphism by choice of U and V. Hence, in fact all maps in the right hand diagram are isomorphisms.
Altogether, we have shown that the inflation $H^i(\Gamma_V, C) \longrightarrow H^i(\Gamma_S, C)$ induces an isomorphism

$$D^i(V,C) \xrightarrow{\cong} Ш^i_S(k,C)$$

Choosing V smaller if necessary, we may suppose that the analogous isomorphism holds for $C^\vee$ in degree $3-i$. The desired pairing is then the perfect pairing from Corollary 3.5.7 via these isomorphisms. This yields the theorem in the case S contains all infinite places. □

Corollary 3.5.13. *Let C be a moderate object of $\mathcal{D}^{\mathrm{b}}\mathcal{F}_k$, and write $C^\vee := \mathbb{R}\mathcal{H}om(C, \mathbb{G}_m)$. Let ℓ be a prime number invertible on U. Then, the canonical pairings*

$$Ш^i_S(k, \mathbb{T}_\ell C) \times Ш^{3-i}_S(k, \mathbb{B}_\ell C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of topological groups for all $i \in \mathbb{Z}$.

Proof. That follows from 3.5.9 and taking limits. □

– 3.5.14. We end this section with a brief discussion on how to prove Theorem 3.5.9 in the case S does not contain all infinite places. The idea is the following. Let S_∞ be the set of infinite places in S. Instead of considering the groups $D^i(U,C)$, one considers

$$D^i_+(U,C) := \ker\left(H^i(U,C) \longrightarrow \prod_{v \notin U \text{ finite}} H^i(k_v, C) \times \prod_{v \in S_\infty} H^i(k_v, C)\right)$$

Again, there is a perfect pairing of finite groups

$$D^i_+(U,C) \times D^{3-i}_+(U, C^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

Along the same lines as in the proof of Theorem 3.5.9 one identifies $D^i_+(U,C)$ with $Ш^i_S(k,C)$ for sufficiently small U and gets the desired pairing of Tate–Shafarevich groups.

CHAPTER 4

Arithmetic duality theorems

In this chapter we prove the duality theorem stated in the introduction. The first section deals with local duality theorems. In the second section we investigate the pairing between $Ш^0(k, M)$ and $Ш^2(k, M^\vee)$, anticipating some results we show only later, and in the third and last section we investigate the pairing between $Ш^1(k, M)$ and $Ш^1(k, M^\vee)$, generalizing the classical duality theorem of Tate and Cassels for abelian varieties. In all of this chapter, if not explicitly mentioned otherwise, *1–motive* means *1–motive with torsion*.

4.1. Local duality theorems

Let K be a finite extension of $\mathbb{Q}_p$, and let ℓ be a prime number not necessarily distinct from p. The goal of this section is to investigate the pairings

$$H^i(K, M) \times H^{1-i}(K, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

for a 1–motive (with torsion) M over K. Mind that, since everything is in characteristic 0, the finite parts are étale. Because K is of cohomological dimension 2, these pairings are trivial except for $i = -1, 0, 1, 2$. Later on we shall see what happens if we replace K by a henselian field, or what happens over the reals. Our starting point is Corollary 3.5.3 and Proposition 2.2.9. Recall from Corollary 3.5.3 that for all $i \in \mathbb{Z}$, the canonical pairings

$$H^i(K, \mathbb{T}_\ell M) \times H^{2-i}(K, \mathbb{B}_\ell M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are perfect pairings of topological groups. The group $H^i(K, \mathbb{T}_\ell M)$ is a finitely generated $\mathbb{Z}_\ell$–module, and accordingly $H^{2-i}(K, \mathbb{B}_\ell M^\vee)$ is a ℓ–torsion group of finite corank (a finite power of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ plus a finite ℓ–group). These pairings are also trivial except for $i = -1, 0, 1, 2$.

Theorem 4.1.1. *Let M be a 1–motive with dual $M^\vee$ over the p–adic field K and let ℓ be a prime number.*

(1) *The group $H^2(K, M^\vee)$ is a torsion group, and its ℓ–part is canonically isomorphic to $H^2(K, \mathbb{B}_\ell M^\vee)$ hence a canonical pairing of topological groups*

$$H^0(K, \mathbb{T}_\ell M) \times H^2(K, M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

(2) *The group $H^1(K, M^\vee)$ is a torsion group. There is a canonical pairing of topological groups*

$$H^0(K, M) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \times H^1(K, M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

Proof. We have already seen in Proposition 3.3.7 that $H^1(K, M^\vee)$ and $H^2(K, M^\vee)$ are torsion groups. Proposition 2.2.9 yields a short exact sequence of torsion groups

$$0 \longrightarrow H^1(K, M) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^2(K, \mathbb{B}_\ell M) \longrightarrow H^2(K, M)[\ell^\infty] \longrightarrow 0$$

Since $H^1(K, M)$ is torsion, the first term of this sequence vanishes, and we remain with the claimed isomorphism. The pairing of statement (1) is then given via these isomorphisms by Corollary 3.5.3.

Again from Proposition 2.2.9 and by Corollary 3.5.3 we get a morphism of short exact sequences of $\mathbb{Z}_\ell$–modules

$$\begin{tikzcd} 0 \arrow[r] & H^0(K,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & H^1(K,\mathbb{T}_\ell M) \arrow[r] \arrow[d, "\cong"'] & \mathrm{T}_\ell H^1(K,M) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & H^1(K,M^\vee)[\ell^\infty]^D \arrow[r] & H^1(K,\mathbb{B}_\ell M^\vee)^D \arrow[r] & \big(H^0(K,M^\vee)\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell\big)^D \arrow[r] & 0 \end{tikzcd}$$

The pairing of statement (2) is given by the left hand vertical map, which is injective, and we have to show that it is an isomorphism. We do this by dévissage. Write

$$M = \left[\begin{tikzcd} & & Y \arrow[d, "u"'] & & \\ 0 \arrow[r] & T \arrow[r] & G \arrow[r] & A \arrow[r] & 0 \end{tikzcd}\right]$$

as in chapter 1, where A and T are the abelian, respectively the multiplicative part of G. We have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & T(K)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & G(K)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d] & A(K)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & H^1(K,T)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[d, "\cong"'] \\ 0 \arrow[r] & H^2(K,Y^\vee)[\ell^\infty]^D \arrow[r] & H^1(K,M_A^\vee)[\ell^\infty]^D \arrow[r] & H^1(K,A^\vee)[\ell^\infty]^D \arrow[r] & H^1(K,Y^\vee)[\ell^\infty]^D \end{tikzcd}$$

The first, third and fourth vertical map are isomorphisms by the local duality theorems of Tate and Nakayama ([**Mil08**], Corollary I.2.4 and Corollary I.3.4). That the top row is exact follows from finiteness of $H^1(K,T)$ and $A(K)[\ell^\infty]$ (indeed, given a long exact sequence of groups all having trivial ℓ–adic Tate module, the sequence obtained by applying $-\,\widehat{\otimes}\,\mathbb{Z}_\ell$ to it is again exact. This can be seen from the long exact sequences given in 2.2.8). Also the bottom row is exact, for $(-)[\ell^\infty]$ is an exact functor on torsion groups, and $(-)^D = \mathrm{Hom}(-,\mathbb{Q}/\mathbb{Z})$ is exact because $\mathbb{Q}/\mathbb{Z}$ is divisible, i.e. an injective object in the category of groups. It follows that the second vertical map in the above diagram is an isomorphism as well. Now, consider

$$\begin{tikzcd} A^\vee(K)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & H^0(K,M_A^\vee)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & H^1(K,Y^\vee)[\ell^\infty] \arrow[r] \arrow[d, "\cong"'] & H^1(K,A^\vee)[\ell^\infty] \arrow[d, "\cong"'] \\ H^1(K,A)[\ell^\infty]^D \arrow[r] & H^1(K,G)[\ell^\infty]^D \arrow[r] & H^1(K,T)[\ell^\infty]^D \arrow[r] & (H^0(K,A)\,\widehat{\otimes}\,\mathbb{Z}_\ell)^D \end{tikzcd}$$

First, the rows in this diagram make sense, because $H^1(K,Y^\vee)$ is finite, hence $H^1(K,Y^\vee)\,\widehat{\otimes}\,\mathbb{Z}_\ell$ is canonically isomorphic to $H^1(K,Y^\vee)[\ell^\infty]$, and the same goes for $H^1(K,G)$. The first, third and fourth vertical map are isomorphisms again by the classical local dualities. That the top row is exact follows from finiteness of $H^1(K,Y^\vee)$ and right exactness of $-\,\widehat{\otimes}\,\mathbb{Z}_\ell$. The bottom row is also exact, the second vertical map is thus an isomorphism. Finally, consider

$$\begin{tikzcd} G(K)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & H^0(K,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & H^1(K,Y)[\ell^\infty] \arrow[r] \arrow[d, "\cong"'] & H^1(K,G)[\ell^\infty] \arrow[d, "\cong"'] \\ H^1(K,M_A^\vee)[\ell^\infty]^D \arrow[r] & H^1(K,M)[\ell^\infty]^D \arrow[r] & H^1(K,T^\vee)[\ell^\infty]^D \arrow[r] & (H^0(K,M_A^\vee)\,\widehat{\otimes}\,\mathbb{Z}_\ell)^D \end{tikzcd}$$

As before, these rows are well defined and exact. We have shown that the first and last vertical map is an isomorphism, and the third map is an isomorphism by Tate–Nakayama. This proves the second part of the theorem. $\square$

Corollary 4.1.2. *The statements of Theorem 4.1.1 hold as well if one replaces the p–adic field K by k_v^{h}, the field of fractions of the henselization of $\mathcal{O}_v$, where $\mathcal{O}_v$ is the localization of the ring of integers of a number field k at some place v.*

Proof. Let $K = k_v$ be the completion of k_v^{h}. The restriction $H^i(k_v^{\mathrm{h}}, -) \longrightarrow H^i(K, -)$ induces isomorphisms for all ingredients of the theorem by Proposition 3.1.6 and Proposition 3.3.9. □

Proposition 4.1.3. *Let $M = [Y \longrightarrow G]$ be a 1–motive over $\mathbb{R}$, and denote by $H^i_T(\mathbb{R}, M)$ the Tate modified cohomology of the complex of* $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$*–modules $[Y(\mathbb{C}) \longrightarrow G(\mathbb{C})]$. The cup product pairing induces a perfect pairings of finite groups of exponent 2*

$$H^i_T(\mathbb{R}, M) \times H^{1-i}_T(\mathbb{R}, M^\vee) \longrightarrow \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

Proof. This is well known for finite groups, lattices, tori and abelian varieties over the reals ([**Mil08**], I.2.13 and I.3.7), and follows from these cases by dévissage. □

– 4.1.4. Recall that for an open $U \subseteq \operatorname{spec} \mathcal{O}_k$ and a 1–motive M over U we have set

$$P^i(U, M) := \prod_{v \notin U} H^i(k_v^{\mathrm{h}}, M)$$

where the product ranges over the places of k not corresponding to a closed point of U, with the convention that for archimedean places v, the piece of notation $H^i(k_v^{\mathrm{h}}, M)$ stands for Tate modified cohomology groups. These are finite 2–groups as in Proposition 4.1.3 if v is real, and trivial if v is complex. From Corollary 4.1.2 and Proposition 4.1.3 one obtains perfect pairings of topological groups

$$P^0(U, \mathbb{T}_\ell M) \times P^2(U, M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z} \qquad \text{and} \qquad P^0(U, M) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \times P^1(U, M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

In the sequel, it is only in this form we shall make use of these local pairings.

4.2. The pairing between $Ш^0(k, M)$ and $Ш^2(k, M^\vee)$

In this section we prove a part of the duality theorem stated in the introduction concerning the case where $i = 0, 2$. We fix once and for all a number field k, an algebraic closure $\overline{k}$ of k, and write $\Gamma := \mathrm{Gal}(\overline{k}|k)$ and Ω for the set of all places of k. Given a 1–motive M over k, we write $Ш^i(k, M)$ for the Tate–Shafarevich group in degree i of the Γ–module complex $[Y(\overline{k}) \longrightarrow G(\overline{k})]$ as defined in 3.4.1.

– 4.2.1. The main results of this section are as follows: We first establish a perfect pairing of topological groups

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

This is actually an easy consequence of our version of the Poitou–Tate duality theorem for complexes of finite Galois modules, or rather its Corollary 3.5.13. We show then that there is a canonical injection $Ш^0(k, M) \otimes \mathbb{Z}_\ell \longrightarrow Ш^1(k, \mathbb{T}_\ell M)$. In order to proceed, we shall use a fact we prove only much later, namely that this injection yields an isomorphism

$$Ш^0(k, M) \otimes \mathbb{Z}_\ell \xrightarrow{\cong} Ш^1(k, \mathbb{T}_\ell M)_{\mathrm{tor}}$$

and that $Ш^1(k, \mathbb{T}_\ell M)$ is finitely generated as a $\mathbb{Z}$–module. Admitting this for the moment, we show that there is a canonical pairing

$$Ш^0(k, M) \times Ш^2(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

nondegenerate on the left, and with divisible right kernel, obtained by stitching together the former pairings for all primes ℓ.

PROPOSITION 4.2.2. *Let $M = [u : Y \longrightarrow G]$ be a 1–motive over k and set $Z := \ker u$. There is a canonical isomorphism of finite groups*

$$Ш^1(k, Z) \xrightarrow{\cong} Ш^0(k, M)$$

In particular, $Ш^0(k, M)$ is annihilated by the order of any finite Galois extension $k'|k$ over which Z is constant.

PROOF. First, observe that if Y is constant, then $Ш^0(k, M)$ is trivial. Indeed, it follows from a simple diagram chase using only one single finite place $v \in \Omega$ that the map $Ш^0(k, M) \longrightarrow Ш^1(k, Y)$ is injective, and the latter group is trivial by Frobenius's density theorem (trivially if Y is torsion free). Now let $k'|k$ be a finite Galois extension such that $\mathrm{Gal}(\overline{k}|k')$ acts trivially on Y, and let Ω' be the set of places of k'. We write Γ and Γ' for the absolute Galois groups of k and k' and $G := \Gamma'/\Gamma$ and for $w \in \Omega'$ lying over $v \in \Omega$ we write k_w for the completion of k at v, and $G_w := \mathrm{Gal}(k'_w|k_w)$. Because Y is constant over k', we have

$$Z := \ker u = H^{-1}(k', M)$$

From the Hochschild–Serre spectral sequence we get a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^1(G, Z) \arrow[r] \arrow[d] & H^0(\Gamma, M) \arrow[r] \arrow[d] & H^0(\Gamma', M) \arrow[d] \\
0 \arrow[r] & \prod H^1(G_w, Z) \arrow[r] & \prod H^0(k_w, M) \arrow[r] & \prod H^0(k'_w, M)
\end{tikzcd}$$

in the lower line we take the product over all places $w \in \Omega'$ (so there are "repetitions" in the first and second product). Because k' acts trivially on Y we have $Ш^0(k', M) = 0$ by our previous observation, hence

$$Ш^0(k, M) \cong \ker \left(H^1(G, Z) \longrightarrow \prod_{w \in \Omega'} H^1(G_w, Z) \right)$$

the product running over all $w \in \Omega'$. The finiteness statement follows, as $H^1(G, Z)$ is obviously finite. Repeating the arguments for the 1–motive $[Z \longrightarrow 0]$ yields the same expressions again, and shows the proposition. $\square$

– 4.2.3. Let $S \subseteq \Omega$ be a set of places of k of density 1, and write $H^0_S(k, M)$ for the group of those elements of $H^0(k, M)$ which restrict to zero in $H^0(k_v, M)$ for each $v \in S$. The same proof shows that there is a canonical isomorphism of finite groups

$$H^1_S(k, Z) \xrightarrow{\cong} H^1_S(k, M)$$

Since S is of density 1, every cyclic subgroup of G occurs as one of the G_w's by Frobenius's density theorem. The difference between $Ш^0(k, M)$ and $H^0_S(k, M)$ depends entirely on the primes v that ramify in k'. This shows that if we are given Z in terms of a finitely generated $\mathbb{Z}$–module upon which $G = \mathrm{Gal}(k'|k)$ acts, then we can compute it effectively.

PROPOSITION 4.2.4. *Let M be a 1–motive over k and let ℓ be a prime number. There is a canonical, perfect pairing of topological groups*

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

In particular, $Ш^2(k, M^\vee)[\ell^\infty]$ is finite if and only if $Ш^1(k, \mathbb{T}_\ell M)$ is.

Proof. By Corollary 3.5.13, we have a natural, perfect pairing of topological groups

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

The proof now simply consists of showing that $Ш^2(k, \mathbb{B}_\ell M^\vee)$ is canonically isomorphic to the ℓ–part of the torsion group $Ш^2(k, M^\vee)$. Indeed, from Proposition 2.2.9 we get the following commutative diagram of torsion groups with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^1(k, M^\vee) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \arrow[r] \arrow[d] & H^2(k, \mathbb{B}_\ell M^\vee) \arrow[r] \arrow[d] & H^2(k, M^\vee)[\ell^\infty] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod H^1(k_v, M^\vee) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \arrow[r] & \prod H^2(k_v, \mathbb{B}_\ell M^\vee) \arrow[r] & \prod H^2(k_v, M^\vee)[\ell^\infty] \arrow[r] & 0
\end{tikzcd}$$

the products running over $v \in \Omega$. Because $H^1(\Gamma, M^\vee)$ and $H^1(k_v, M^\vee)$ are torsion, the first terms of both rows are zero, hence the canonical isomorphism $Ш^2(k, \mathbb{B}_\ell M^\vee) \cong Ш^2(k, M^\vee)[\ell^\infty]$ as required. □

– 4.2.5. Let M be a 1–motive over k and let ℓ be a prime number. Again from Proposition 2.2.9 we get a commutative diagram of $\mathbb{Z}_\ell$–modules with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^0(k, M) \widehat{\otimes} \mathbb{Z}_\ell \arrow[r] \arrow[d, "\alpha_\ell"'] & H^1(k, \mathbb{T}_\ell M) \arrow[r] \arrow[d] & \mathrm{T}_\ell H^1(k, M) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod H^0(k_v, M) \widehat{\otimes} \mathbb{Z}_\ell \arrow[r] & \prod H^1(k_v, \mathbb{T}_\ell M) \arrow[r] & \prod \mathrm{T}_\ell H^1(k_v, M) \arrow[r] & 0
\end{tikzcd}$$

The kernel of the right hand vertical map is the Tate module of $Ш^1(k, M)$, which is torsion free, and even trivial if $Ш^1(k, M)$ is finite. Hence, in any case the map $\ker \alpha \longrightarrow Ш^1(k, \mathbb{T}_\ell M)$ is an isomorphism on torsion elements. Clearly, $Ш^0(k, M) \otimes \mathbb{Z}_\ell$ is a subgroup of $\ker \alpha_\ell$, hence an injection

$$(*) \qquad Ш^0(k, M) \otimes \mathbb{Z}_\ell \longrightarrow Ш^1(k, \mathbb{T}_\ell M)_{\mathrm{tor}}$$

Observe that there is a canonical isomorphism $Ш^0(k, M) \otimes \mathbb{Z}_\ell \cong Ш^0(k, M)[\ell^\infty]$ just because $Ш^0(k, M)$ is finite. We shall prove later (Theorem 5.5.1) that this injection $(*)$ is actually an isomorphism.

Theorem 4.2.6. *Let M be a 1–motive over k and let ℓ be a prime number. There is a canonical pairing of topological groups*

$$Ш^0(k, M)[\ell^\infty] \;\times\; Ш^2(k, M^\vee)[\ell^\infty] \;\longrightarrow \mathbb{Q}/\mathbb{Z}$$

which is nondegenerate on the left and has divisible right kernel. Provided the group $Ш^1(k, \mathbb{T}_\ell M)$ is finite, this is even a perfect pairing of finite groups, trivial for all but finitely many ℓ.

Proof. That this pairing is nondegenerate on the left follows immediately from Proposition 4.2.4. The right kernel of this pairing is, again by Proposition 4.2.4, the Pontryagin dual of the quotient of $Ш^1(k, \mathbb{T}_\ell M)$ by $Ш^0(k, M)[\ell^\infty]$. By what we claim above this quotient is torsion free, hence its dual is divisible. The additional statement is clear from Propositions 4.2.4 and 4.2.2. □

This has the following interesting consequence:

Corollary 4.2.7. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. Suppose that $Ш^1(k, \mathbb{T}_\ell M)$ is finite for all primes ℓ. Then, $Ш^1(k, \mathbb{T}_\ell M)$ is even trivial for all but finitely many ℓ, and the canonical pairing*

$$Ш^0(k, M) \times Ш^2(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups. If $\ker u$ is constant, then these groups are trivial.

PROOF. Indeed, if $Ш^1(k,\mathbb{T}_\ell)$ is finite, then we have $Ш^0(k,M)[\ell^\infty] \cong Ш^1(k,\mathbb{T}_\ell M)$ by $(*)$ above. Since $Ш^0(k,M)$ is finite, we have $Ш^1(k,\mathbb{T}_\ell M)=0$ and hence $Ш^2(k,M^\vee)=0$ for all but finitely many ℓ. The pairing of the corollary is then obtained from the pairing of Proposition 4.2.4 by taking products over all ℓ. The additional statement follows from Proposition 4.2.2. □

We shall give in section 7.4 (Theorem 7.4.1) a few criteria under which the hypothesis of this corollary is indeed satisfied.

4.3. The Cassels–Tate pairing for 1–motives

In this section we prove the second half of the duality theorem in the introduction, that is, the case $i=1$.

THEOREM 4.3.1. *Let M be a 1–motive over k with dual $M^\vee$. The left and right kernel of the canonical pairing*

$$Ш^1(k,M) \ \times \ Ш^1(k,M^\vee) \ \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are the subgroups of divisible elements. If the abelian part A of M is such that $Ш^1(k,A)$ is finite, this is a perfect pairing of finite groups.

– 4.3.2. All essential steps of the proof are already in [**HS05a**], where Theorem 4.3.1 is proven for torsion free 1–motives. The presence of torsion makes just things technically a bit more complicated, but the arguments remain the same. These are as follows. The starting point is the pairing

$$H^i(U,M)[\ell^\infty] \times H^{2-i}_{\mathrm{c}}(U,M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

for a fixed prime number ℓ. A purely formal argument shows that this pairing is nondegenerate modulo divisible subgroups (Proposition 4.3.4, corresponding to Theorem 3.4 of [**HS05a**]). Adapting a computation of Milne, we can then show that even the pairing

$$D^1(U,M)[\ell^\infty] \times D^1(U,M)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is nondegenerate modulo divisible subgroups (Proposition 4.3.7, corresponding to Corollary 3.5 in *loc.cit.*). Harari and Szamuely proceed then by showing that for sufficiently small U, the group $D^1(U,M)[\ell^\infty]$ can be identified with $Ш^1(U,M)[\ell^\infty]$ via the restriction map $H^1(U,M) \longrightarrow H^1(k,M)$. For torsion free 1–motives, this map is injective on ℓ–torsion provided again that U is sufficiently small. This fails for 1–motives with torsion, we can't get anything better than a map with finite kernel. But this is already good enough. As in the proof of the Poitou–Tate duality for complexes, we can then choose a small $V \subseteq U$ such that the image of $D^1(U,M)$ in $H^1(V,M)$ is isomorphic to $Ш^1(k,M)$ on ℓ–parts. Once we have a pair $V \subseteq U$ at hand where this holds for M and also for the dual of M, we can conclude as in the finite case.
It is widely conjectured that for abelian varieties A over k, the Tate–Shafarevich group $Ш^1(k,A)$ is finite. If this is the case, the group $Ш^1(k,M)$ as well as $D^1(U,M)$ for small U are finite as well. We end the section with showing this implication.

– 4.3.3. Let $U \subseteq \operatorname{spec}\mathcal{O}_k$ be an open subscheme, let ℓ be a prime invertible on U and let M be a 1–motive over U. By Proposition 3.3.11, we know that $H^1(U,M)$ is a torsion group, and that the multiplication–by–ℓ map on $H^1(U,M)$ has a finite kernel and cokernel. Lemma 3.3.1 gives us a clear picture what such groups look like.

Proposition 4.3.4. *Let M be a 1–motive over U with dual $M^\vee$, and let ℓ be a prime number invertible on U. The left and right kernel of the canonical pairing*

$$H^1(U,M)[\ell^\infty] \times H^1_{\mathrm{c}}(U,M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are the subgroups of divisible elements.

Proof. Since this is a pairing of torsion groups, its kernels must contain the subgroups of divisible elements. What we have to show is that after modding out the divisible subgroups, we get a perfect pairing. In other words, we must prove that the induced pairing

$$(*) \qquad H^1(U,M)[\ell^\infty] \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \times H^1_{\mathrm{c}}(U,M^\vee)[\ell^\infty] \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is perfect. (This is a pairing of finite groups.) By Corollary 3.5.6, we have for all $i \in \mathbb{Z}$ a perfect pairing of topological groups

$$H^1(U,\mathbb{B}_\ell M) \times H^2_{\mathrm{c}}(U,\mathbb{T}_\ell M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

inducing perfect pairings of finite groups

$$H^1(U,\mathbb{B}_\ell M) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \times H^2_{\mathrm{c}}(U,\mathbb{T}_\ell M)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

We will identify the groups in this pairing with those in $(*)$. First, by Proposition 2.2.9, we have a short exact sequence of torsion groups

$$0 \longrightarrow H^0(U,M) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^1(U,\mathbb{B}_\ell M) \longrightarrow H^1(U,M)[\ell^\infty] \longrightarrow 0$$

Applying the right exact functor $-\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell$ to this sequence yields an isomorphism $H^1(U,\mathbb{B}_\ell M)\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell \cong H^1(U,M)[\ell^\infty]\mathbin{\widehat{\otimes}}\mathbb{Z}_\ell$ because the first group in the above sequence is divisible. Again by Proposition 2.2.9, we have a short exact sequence of profinite groups

$$0 \longrightarrow H^1_{\mathrm{c}}(U,M^\vee) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \longrightarrow H^2_{\mathrm{c}}(U,\mathbb{T}_\ell M^\vee) \longrightarrow \mathrm{T}_\ell H^2_{\mathrm{c}}(U,M^\vee) \longrightarrow 0$$

Taking torsion parts yields an isomorphism $H^1_{\mathrm{c}}(U,M^\vee)[\ell^\infty] \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \cong H^2_{\mathrm{c}}(U,\mathbb{T}_\ell M^\vee)[\ell^\infty]$ because the last group in the above sequence is torsion free. □

– 4.3.5. We need a preliminary computation, analogous to Milne's Lemma I.6.15 in [**Mil08**], and to the lemma in [**HS05b**], concerning the local pairing

$$P^1(U,\mathbb{T}_\ell M) \times P^1(U,\mathbb{B}_\ell M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

Let $S(U,M^\vee)$ be the preimage of $D^1(U,M)[\ell^\infty]$ under the map $H^1(U,\mathbb{B}_\ell M^\vee) \longrightarrow H^1(U,M^\vee)[\ell^\infty]$. Put otherwise, $S(U,M^\vee)$ is the kernel of the map s in the diagram

$$\begin{tikzcd}
0 \arrow[r] & S(U,M^\vee) \arrow[r] & H^1(U,\mathbb{B}_\ell M^\vee) \arrow[r, "s"] \arrow[d] & P^1(U,M^\vee)[\ell^\infty] \\
& & P^1(U,\mathbb{B}_\ell M^\vee) \arrow[ur] &
\end{tikzcd}$$

Lemma 4.3.6. *Every element $c \in P^1(U,\mathbb{T}_\ell M)$ which is orthogonal to the image of $S(U,M^\vee)$ in $P^1(U,\mathbb{B}_\ell M^\vee)$ is the sum of the coboundary of an element in $P^0(U,M) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ and of the restriction of an element in $H^1(U,\mathbb{T}_\ell M)$.*

Proof. Pick such an element $c \in P^1(U, \mathbb{T}_\ell M)$. Dualizing the diagram in 4.3.5 using the local pairings as given in 4.1.4 and the pairings for Tate modules and Barsotti–Tate groups (Corollary 3.5.3 and Corollary 3.5.6) yields

$$\begin{tikzcd}
0 & S(U,M^\vee)^D \arrow[l] & H^2_c(U,\mathbb{T}_\ell M) \arrow[l] & P^0(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[l, "s^D"'] \arrow[dl, "\delta"] \\
 & & P^1(U,\mathbb{T}_\ell M) \arrow[u, "\gamma"] &
\end{tikzcd}$$

and our hypothesis is that c maps to zero in $S(U, M^\vee)^D$. By exactness of the top row, $\gamma(c) = s^D(b)$ for some element $b \in P^1(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$. We have $c = \delta b + (c - \delta b) \in \operatorname{im}\delta + \ker\gamma$, and $\ker\gamma$ is the image of the restriction map $H^1(U, \mathbb{T}_\ell M) \longrightarrow P^1(U, \mathbb{T}_\ell M)$. □

Proposition 4.3.7. *Let M be a 1–motive over U with dual $M^\vee$, and let ℓ be a prime number invertible on U. The left and right kernel of the canonical pairing*

$$D^1(U,M)[\ell^\infty] \times D^1(U,M)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

are the subgroups of divisible elements.

Proof. We already know that this is a pairing of torsion groups, its kernels must thus contain the subgroups of divisible elements. What we have to show is that the left and right kernels of the are divisible. Fix an element $a \in D^1(U, M)[\ell^\infty]$ orthogonal to $D^1(U, M^\vee)[\ell^\infty]$.
Let b be any preimage of a in $H^1_c(U, M)$. By Proposition 4.3.4, the element a is divisible in $H^1(U, M)$, hence maps to zero in $H^1(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$. Consider the following commutative diagram

$$\begin{tikzcd}
P^0(U,M) \arrow[r, "\partial"] \arrow[d] & H^1_c(U,M) \arrow[r, "b\mapsto a"] \arrow[d] & H^1(U,M) \arrow[d, "a\mapsto 0"] \\
P^0(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] & H^1_c(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] & H^1(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell
\end{tikzcd}$$

The top row is exact, but the bottom row may not be. However, *if* there exists a $c \in P^0(U, M) \widehat{\otimes} \mathbb{Z}_\ell$ mapping to the image of b in $H^1_c(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$ then we are done. Indeed, for every $n \geq 0$, let c_n be an element of $P^0(U, M)$ whose class in $P^0(U, M)/\ell^n P^0(U, M)$ equals the class of c, and set $b_n := b - \partial c_n$. This b_n is then divisible by ℓ^n, and maps to a in $H^1_c(U, M)$, what shows that a is divisible by ℓ^n, hence ℓ–divisible because n was arbitrary[1].
It remains to show that we can indeed find an element $c \in P^0(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$ mapping to the image of b in $H^1(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$. For this, consider the diagram

$$\begin{tikzcd}
 & P^0(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & H^1_c(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & H^1(U,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell \arrow[d, hook] \\
H^1(U,\mathbb{T}_\ell M) \arrow[r] & P^1(U,\mathbb{T}_\ell M) \arrow[r] & H^2_c(U,\mathbb{T}_\ell M) \arrow[r] & H^2(U,\mathbb{T}_\ell M)
\end{tikzcd}$$

The lower row is exact, so there is a $c \in P^1(U, \mathbb{T}_\ell M)$ mapping to the image of b in $H^2_c(U, \mathbb{T}_\ell M)$. If we can write c as a sum of an element coming from $P^0(U, M) \,\widehat{\otimes}\, \mathbb{Z}_\ell$ and an element coming from $H^1(U, \mathbb{T}_\ell M)$ then we are done. By Lemma 4.3.6, it suffices to show that c is orthogonal to the image of $S(U, M^\vee)$ in $P^1(U, \mathbb{B}_\ell M^\vee)$. We check this. Let a' be an element of $S(U, M^\vee)$. The image of a' in $H^1(U, M^\vee)[\ell^\infty]$ is in $D^1(U, M^\vee)$, hence orthogonal to a by hypothesis on a. Therefore, $a' \in H^1(U, \mathbb{B}_\ell M^\vee)$ is orthogonal to the image of b in $H^2_c(U, \mathbb{T}_\ell M)$ by choice of b. This in turn implies that the image of a' in $P^1(U, \mathbb{B}_\ell M^\vee)$ is orthogonal to c, and we are done. □

[1]We do not know whether a comes from a divisible element in $H^1_c(U, M)$.

LEMMA 4.3.8. *Let M be a 1–motive over U. For almost all places v of k corresponding to a closed point of U, the restriction maps $H^1(\mathcal{O}_v, M) \longrightarrow H^1(k_v, M)$ are injective.*

PROOF. Let G° be the connected component of G, and set $F := G/G^\circ$. Choosing U smaller if necessary, we may suppose that F is locally constant on U, and that also the torsion part of Y is locally constant. We will show that under this hypothesis the restriction maps $H^i(\mathcal{O}_v, M) \longrightarrow H^i(k_v, M)$ are injective for all v corresponding to a closed point of U. Set $M^\circ := [0 \longrightarrow G^\circ]$ and $M' := [Y \longrightarrow F]$ so that we get a short exact sequence

$$0 \longrightarrow M^\circ \longrightarrow M \longrightarrow M' \longrightarrow 0$$

That the restrictions $H^1(\mathcal{O}_v, M') \longrightarrow H^1(k_v, M')$ are injective can be seen by dévissage, as in the proof of Lemma 3.5.11 where we showed the analogous statement for complexes with finite homology groups. The above exact sequence yields the following diagram with exact rows

$$\begin{tikzcd} 0 = H^1(\mathcal{O}_v, G^\circ) \arrow[r] \arrow[d] & H^1(\mathcal{O}_v, M) \arrow[r, hook] \arrow[d] & H^1(\mathcal{O}_v, M') \arrow[d, hook] \\ H^1(k_v, G^\circ) \arrow[r] & H^1(k_v, M) \arrow[r] & H^1(k_v, M') \end{tikzcd}$$

As indicated, the group $H^1(\mathcal{O}_v, G^\circ)$ is trivial. Indeed, this follows from Lang's theorem and the canonical isomorphism $H^1(\mathcal{O}_v, G^\circ) \cong H^1(\kappa_v, G^\circ)$ ([**Mil08**], II.1.1), where κ_v is the residue field at v. From this, injectivity of $H^1(\mathcal{O}_v, M) \longrightarrow H^1(k_v, M)$ follows. □

LEMMA 4.3.9. *Let $M = [Y \longrightarrow G]$ be a 1–motive over U. For every sufficiently small open $V \subseteq U$, the image of $D^1(V, M)[\ell^\infty]$ in $H^1(k, M)[\ell^\infty]$ equals $Ш^1(k, M)[\ell^\infty]$.*

PROOF. For every open $V \subseteq U$, write $\mathcal{D}^1(V, M)$ for the image of $D^1(V, M)$ in $H^1(k, M)$. By Lemma 3.4.6, we know that for every two opens $W \subseteq V$ the inclusion $\mathcal{D}^1(W, M) \subseteq \mathcal{D}^1(V, M)$ holds. Using property (3) of Lemma 3.3.1, it is enough to show that equality

$$Ш^1(k, M) = \bigcap_{V \subseteq U} \mathcal{D}^1(V, M)$$

holds. We check both inclusions.
$\subseteq$: Take $x \in Ш^1(k, M) \subseteq H^1(k, M)$, let $V \subseteq U$, and let us show that $x \in \mathcal{D}^1(V, M)$. There exists an open $W \subseteq V$ such that x is the image of some $y \in H^1(W, M)$. If v is any place of k, then the image of y in $H^1(k_v, M)$ is the same as the image of x in $H^1(k_v, M)$ which is zero by definition of $Ш^1(k, M)$. As this holds in particular for all v that do not correspond to a closed point of W, we see that y is in $D^1(W, M)$, and hence $x \in \mathcal{D}^1(W, M)$. But as $\mathcal{D}^1(W, M) \subseteq \mathcal{D}^1(V, M)$, we have also $x \in \mathcal{D}^1(V, M)$.
$\supseteq$: Take $x \in H^1k, M)$ such that $x \in \mathcal{D}^1(V, M)$ for all $V \subseteq U$. If v is a place of k, then we can choose an open V of U not containing v as a closed point. As $x \in \mathcal{D}^1(V, M)$, there is $y \in D^1(V, M)$ having x as image. But the image of y in $H^1(k_v, M)$ is zero by definition of $D^1(V, M)$. The image of x in $H^1(k_v, M)$ is thus zero. Together with Lemma 4.3.8, this shows that x is in $Ш^1(k, M)$. □

LEMMA 4.3.10. *Let M be a 1–motive over U. The restriction $H^1(U, M)[\ell^\infty] \longrightarrow H^1(k, M)[\ell^\infty]$ has a finite kernel.*

PROOF. The proof goes by dévissage. Write $M = [Y \longrightarrow G]$, and write G as an extension of an abelian scheme A by T, where the connected component of T is a torus. Observe that it is enough to show that this kernel is killed by some power of ℓ, because the multiplication by ℓ^n has a finite kernel already on $H^1(U, M)$.
For a finite group scheme F over U, the groups $H^i(U, F)$ are themselves finite, and the $H^i(k, F)$ are

of finite exponent. Also, the groups $H^1(U, Y)$ and $H^1(U, T)$ are finite, and $H^1(k, Y)$ and $H^1(k, T)$ are of finite exponent. For an abelian scheme A over U, the restriction $H^1(U, A) \longrightarrow H^1(k, A)$ is always injective on the ℓ–parts by Lemma 5.5 of [**Mil08**]. Writing out the necessary long exact sequences, and using that $A(V) = A(k)$, one finds that the restriction $H^1(U, G) \longrightarrow H^1(k, G)$ has finite kernel on ℓ–parts. From dévissage one sees then that in order to prove the statement of the Lemma it suffices to show that the map $H^2(U, Y) \longrightarrow H^2(k, Y)$ is has a finite kernel on ℓ–parts. We can suppose that Y is torsion free. But then, using Proposition II.2.9 of [**Mil08**], this restriction map can be identified with the inflation map

$$H^1(\Gamma_U, Y(k_U) \otimes \mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(\Gamma, Y(\bar{k}) \otimes \mathbb{Q}/\mathbb{Z})$$

in Galois cohomology (on ℓ–parts), which is injective by Hochschild–Serre. Here, k_U is the maximal extension of k unramified in U, and $\Gamma_U := \mathrm{Gal}(k_U|k)$. □

Proof of Theorem 4.3.1. We are given a 1–motive M over k with dual $M^\vee$. Because $Ш^1(k, M)$ and $Ш^1(k, M^\vee)$ are torsion groups, it is enough to construct a pairing

$$Ш^1(k, M)[\ell^\infty] \times Ш^1(k, M^\vee)[\ell^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

for every prime number ℓ and prove that this pairing is nondegenerate modulo divisible subgroups. Fix any ℓ, and choose a model of the given 1–motive M over an open subscheme $U \subseteq \operatorname{spec} \mathcal{O}_k$ of over k. Taking U small enough, we can assume that ℓ is invertible on U, and, by Lemma 4.3.10, that the restriction map

$$H^1(U, M)[\ell^\infty] \longrightarrow H^1(k, M)[\ell^\infty]$$

have finite kernel. By Lemma 4.3.9, we can as well suppose that the ℓ–part of the image of $D^1(U, M)$ in $H^1(k, M)$, which is the same as the image of $H^1_c(U, M)[\ell^\infty] \longrightarrow H^1(k, M)[\ell^\infty]$ equals the ℓ–part of the Tate–Shafarevich group, so that we have a surjective map with finite kernel

$$D^1(U, M)[\ell^\infty] \longrightarrow Ш^1(k, M)[\ell^\infty]$$

Every element of this kernel maps already to zero on some open subscheme of U, and since this kernel contains only finitely many elements we see that for every sufficiently small open V of U the image of $D^1(U, M)[\ell^\infty]$ in $H^1(V, M)$ is isomorphic to $Ш^1(k, M)[\ell^\infty]$ via the restriction map $H^1(V, M) \longrightarrow H^1(k, M)$. Consider again (as in the proof of Poitou–Tate duality for complexes) the diagrams

$$\begin{tikzcd} H^1_c(U, M) \arrow[r] \arrow[dr, dotted] & H^i(U, M) \arrow[d, "\alpha"] \\ H^1_c(V, M) \arrow[u] \arrow[r] & H^1(V, M) \end{tikzcd} \qquad \begin{tikzcd} D^1(V, M)[\ell^\infty] \arrow[r, "\subseteq"] \arrow[dr] & \alpha D^1(U, M)[\ell^\infty] \arrow[d, "\cong"] \\ & Ш^1(k, M)[\ell^\infty] \end{tikzcd}$$

The groups $D^1(U, M)$ and $D^1(V, M)$ are the image of the horizontal maps in the left hand diagram, and from this we see that $D^1(V, M)$ is contained in $\alpha D^1(U, M)$. Hence the inclusion in the right hand diagram, which then shows that the restriction from V to k induces an isomorphism $D^1(V, M)[\ell^\infty] \longrightarrow Ш^1(k, M)[\ell^\infty]$.
Restricting V further if necessary, we may suppose that the same holds for the dual 1–motive $M^\vee$. For such a V, we can identify the pairing of Proposition 4.3.7 with the pairing we were searching for.
It remains to show the additional statement of the theorem, that finiteness of $Ш^1(k, A)$ implies finiteness of $Ш^1(k, M)$. We formulate this in a separate proposition. □

Proposition 4.3.11. *Let M be a 1–motive over k with abelian part A. If $Ш^1(k, A)$ is finite, then $Ш^1(k, A^\vee)$, $Ш^1(k, M)$ and $Ш^1(k, M^\vee)$ are finite as well.*

Proof. We work again over an open $U \subseteq \operatorname{spec} \mathcal{O}_k$ and a model of M over U. If $Ш^1(k, A)$ is finite, then $D^1(U, A)$ and $D^1(U, A^\vee)$ are finite as well by [**Mil08**] Lemma 5.5 and Theorem 5.6b. From the proof of 4.3.9, one can see that finiteness of $Ш^1(k, M)$ follows from finiteness of $D^1(U, M)$. It is thus enough to show that finiteness of $D^1(U, A)$ implies finiteness of $D^1(U, M)$. This can be done by dévissage. First, we consider the diagram

$$\begin{array}{ccccc} H^1(U,T) & \to & H^1(U,G) & \to & H^1(U,A) \\ \downarrow & & \downarrow & & \downarrow \\ P^1(U,T) & \to & P^1(U,G) & \to & P^1(U,A) \end{array}$$

The groups $H^1(U, T)$ and $P^1(U, T)$ are both finite, and the left hand vertical map has finite kernel $D^1(U, A)$. Hence $D^1(U, G)$, the kernel of the middle vertical map, is finite as well. Next, consider the diagram

$$\begin{array}{ccccccc} H^1(U,Y) & \to & H^1(U,G) & \to & H^1(U,M) & \to & H^2(U,Y) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ P^1(U,Y) & \to & P^1(U,G) & \to & P^1(U,M) & \to & P^2(U,Y) \end{array}$$

The groups $H^1(U, Y)$ and $P^1(U, Y)$ are both finite, and $D^2(U, Y)$ is finite as well since it is dual to $D^1(U, Y^\vee)$ where $Y^\vee := \mathcal{H}om(Y, \mathbb{G}_m)$. Hence, finiteness of $D^1(U, M)$ follows by diagram chase. $\square$

CHAPTER 5

Lie groups associated with 1–motives

In this chapter we introduce several Lie groups and Lie algebras associated with a torsion free 1–motive M and show some of the more immediate properties of these objects. These Lie groups act on the Tate module of M, and we compute some of the arising cohomology. In the last section we relate this Lie group cohomology with Galois cohomology.
All vector spaces, Lie algebras, Lie algebra modules et cetera are understood to be finite dimensional over their field of definition. We will only work with torsion free 1–motives[1], always defined over a number field k with fixed algebraic closure $\overline{k}$ and absolute Galois group $\Gamma := \mathrm{Gal}(\overline{k}|k)$.

5.1. Summary of ℓ–adic Lie theory

In this section, we review some topics in ℓ–adic Lie theory and Lie algebra cohomology.

– 5.1.1. An ℓ–adic Lie group L is a group–object in the category of analytic $\mathbb{Q}_\ell$–varieties. This means that L is a topological group, equipped with an atlas, i.e. a family of local homeomorphisms (charts) from open subsets of L to open subsets of $\mathbb{Q}_\ell^d$ for a fixed integer d, called the dimension of L, with analytic transition maps. Analytic means locally given by an absolutely converging power series. Such an atlas yields an analytic structure on L, and also on $L \times L$, and one asks that the maps

$$L \times L \xrightarrow{\text{multiplication}} L \qquad \text{and} \qquad L \xrightarrow{\text{inversion}} L$$

are analytic. The standard examples of ℓ–adic Lie groups are the additive groups $\mathbb{Z}_\ell^r$ and $\mathbb{Q}_\ell^r$, linear groups like $\mathrm{GL}(\mathbb{Q}_\ell^r)$ or $\mathrm{SL}(\mathbb{Z}_\ell^r)$ and so on. If G is any (topological) group and L a (open) subgroup of G, then there exists a unique Lie group structure on G making L an open Lie subgroup of G (follows from [**Bou72**], Ch.III, §1, no.9, proposition 18 taking $U = V = L$, or by reasoning directly on the local nature of analyticity). In particular, the groups we considered in 3.3.2 are such, because they contain $\mathbb{Z}_\ell^r$ as an open subgroup. Finally, let us mention without proof that if $K|\mathbb{Q}_p$ is a p-adic field and G a commutative group scheme over K, then the group $G(K)$ with its p–adic topology is a p–adic Lie group.

– 5.1.2. As explained in [**Hoo42**], one associates with an ℓ–adic Lie group L a Lie algebra $\mathfrak{l}$ over $\mathbb{Q}_\ell$ in the usual way. The exponential map $\mathfrak{l} \longrightarrow L$ is defined in a neighborhood of 0 in $\mathfrak{l}$, and has the usual properties. Two Lie groups L and L' have the same Lie algebra if and only if there is a Lie group L'' which is isomorphic to an open subgroup of L and to an open subgroup of L'. From this one can see that every ℓ–adic Lie group admits a system of open neighborhoods of unity consisting of open subgroups. In particular, a commutative ℓ–adic Lie group contains an open subgroup isomorphic to a power of $\mathbb{Z}_\ell$, because in the commutative case the exponential is even a homomorphism.

[1]The reason for this is that on one hand this makes things technically much easier and on the other hand Proposition 5.2.5 suggests that we don't lose too much of the general case.

Every closed subgroup of an ℓ–adic Lie group is an ℓ–adic Lie group ([**Hoo42**], Theorem 8, or [**Bou72**], Ch.III, §2, no.2, théorème 2), and every continuous morphism between ℓ–adic Lie groups is analytic, i.e. a morphism of Lie groups ([**Bou72**], Ch.III, §8, no.1, théorème 1).

– 5.1.3. This has the following important consequence: Let k be a field with absolute Galois group Γ, and let T be a finitely generated $\mathbb{Z}_\ell$ module on which Γ acts continuously. Typically T could be the Tate module of an algebraic group or a 1–motive over k. The group $\mathrm{GL}\,T$ is a compact ℓ–adic Lie group, and since Γ is compact, the image of Γ in $\mathrm{GL}\,T$ is closed, hence a compact ℓ–adic Lie group itself. We shall demonstrate that it is very desirable to understand the structure of so arising Lie groups and their Lie algebras.

Proposition 5.1.4 ([**Ser64**], Proposition 2). *Let L be a compact ℓ–adic Lie group. As a topological group, L is a profinite group and topologically finitely generated, that is to say, there exists a finite subset of L which generates a dense subgroup.*

Proof. As a topological space, L is Hausdorff and totally disconnected, since every analytic $\mathbb{Q}_\ell$–variety is. A totally disconnected compact topological group is profinite ([**Sha72**] §1, Theorem 2). Let $\mathfrak{l}$ be the Lie algebra of L and let $x_1, \ldots, x_n$ be a $\mathbb{Q}_\ell$–basis of $\mathfrak{l}$, such that $g_i := \log x_i$ is defined for all i. The elements $g_i \in L$ generate then a subgroup of L whose closure has finite index. If $g_{n+1}, \ldots, g_N \in L$ are representatives of the left cosets of this closure, then the elements $g_1, \ldots, g_N$ generate a dense subgroup of L. $\square$

– 5.1.5. Here is a quick review of Lie algebra cohomology. A more detailed introduction is provided by the lecture notes [**Bur05**]. For additional material see chapter 7 of [**Wei94**], or J.L. Koszul's thesis [**Kos50**]. Let K be a field of characteristic zero, let $\mathfrak{l}$ be a Lie algebra over K, and let V be a $\mathfrak{l}$–module. This means that we are given a Lie algebra map $\mathfrak{l} \longrightarrow \mathfrak{gl}_K V$, or in other terms, an action $\mathfrak{l} \times V \longrightarrow V$ which is K–bilinear and satisfies the rule

$$[x, y].v = x.(y.v) - y.(x.v) \qquad \text{for all } x, y \in \mathfrak{l},\ \ v \in V$$

We write $V^{\mathfrak{l}} := \{v \in V \,|\, xv = 0 \text{ for all } x \in \mathfrak{l}\}$ and call this K–vector space the *space of invariants* of V under the given action of $\mathfrak{l}$. If V and W are $\mathfrak{l}$–modules, then $V \otimes_K W$ and $\mathrm{Hom}_K(V, W)$ inherit natural $\mathfrak{l}$–module structures, given by

$$x.(v \otimes w) = x.v \otimes w + v \otimes x.w \qquad \text{and} \qquad (x.f)(v) = x.f(v) - f(x.v)$$

The invariants of $\mathrm{Hom}_K(V, W)$ are of course $\mathrm{Hom}_{\mathfrak{l}}(V, W)$, the set of $\mathfrak{l}$–module homomorphisms from V to W. There is a natural action of $\mathfrak{l}$ on itself given by $x.y = [x, y]$. This is called the *adjoint representation.*

Now we come to cohomology. Of course, the fixed point functor from the category of $\mathfrak{l}$–modules to the category of K–vector spaces is left exact, has a right derivative, and its homology groups $H^i(\mathfrak{l}, V)$ are what we call *cohomology groups of* $\mathfrak{l}$ *with coefficients in* V. In order to compute, we shall need a more explicit construction, as follows: For $n \geq 0$, we call

$$C^n(\mathfrak{l}, V) := \mathrm{Hom}_K\left(\textstyle\bigwedge^n \mathfrak{l},\ V\right) = \left\{\text{Multilinear, alternating maps } \mathfrak{l} \times \cdots \times \mathfrak{l} \longrightarrow V\right\}$$

the space of n*–cochains*, and define coboundary maps $\partial : C^n(\mathfrak{l}, V) \longrightarrow C^{n+1}(\mathfrak{l}, V)$ by the formula

$$(\partial f)(x_0 \wedge \cdots \wedge x_n) = \sum_{0 \leq i \leq j \leq n} (-1)^{i+j} f([x_i, x_j] \wedge x_0 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge \widehat{x_j} \wedge \cdots \wedge x_n)$$
$$+ \sum_{i=0}^{n} (-1)^i x_i.f(x_0 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_n)$$

where $\hat{x}_i$ means omission of the term x_i. It is a computational, although not entirely trivial matter to show that $\partial^2 = 0$. Once this is established, we can set

$$H^n(\mathfrak{l}, V) := \frac{\ker\left(\partial : C^n(\mathfrak{l}, V) \longrightarrow C^{n+1}(\mathfrak{l}, V)\right)}{\operatorname{im}\left(\partial : C^{n-1}(\mathfrak{l}, V) \longrightarrow C^n(\mathfrak{l}, V)\right)} = \frac{n\text{–cocycles}}{n\text{–coboundaries}}$$

This cochain construction computes indeed the derived functor cohomology (Corollary 7.7.3 of [**Wei94**]). The natural action of $\mathfrak{l}$ on n–cochains is explicitly given by the linear map $\rho : \mathfrak{l} \longrightarrow \mathfrak{gl}(C^n(\mathfrak{l}, V))$ defined by the formula

$$(\rho(x)f)(x_1 \wedge \cdots \wedge x_n) = x.f(x_1 \wedge \cdots \wedge x_n) - \sum_{i=1}^{n} f(x_1 \wedge \cdots \wedge [x, x_i] \wedge \cdots \wedge x_n)$$

valid for every $x \in \mathfrak{l}$ and $f \in C^n(\mathfrak{l}, V)$. This action commutes with the coboundary operator ∂, and hence induces an action on the space of cocycles, on coboundaries, and on the cohomology spaces. The *insertion operator* $i(x) : C^n(\mathfrak{l}, V) \longrightarrow C^{n-1}(\mathfrak{l}, V)$ is given by

$$(i(x)f)(x_1 \wedge \cdots \wedge x_{n-1}) = f(x \wedge x_1 \wedge \cdots \wedge x_{n-1})$$

On $C^0(\mathfrak{l}, V)$ one defines $i(x)$ to be the zero map. These maps are related by the so called Cartan homotopy formula, which reads

$$\rho(x) = i(x)\partial + \partial i(x)$$

This formula shows in particular that the action of $\mathfrak{l}$ on $H^n(\mathfrak{l}, V)$ is trivial. This fact has the following well–known analogue group cohomology (see [**Wei94**], Theorem 6.7.8): If G is a group and M a G–module and $x \in G$, then the maps $g \longmapsto x^{-1}gx$ and $m \longmapsto xm$ are compatible and induce maps $H^n(G, M) \longrightarrow H^n(G, M)$, whence an action of G on $H^n(G, M)$. This action is the trivial action. These observations yield the following useful lemma (analogous to Sah's Lemma in group cohomology):

LEMMA 5.1.6. *Let $\mathfrak{l}$ be a Lie algebra, and let V be an $\mathfrak{l}$–module. If there exists a central element $x \in Z(\mathfrak{l})$ such that $v \longmapsto x.v$ is an automorphism of V, then $H^n(\mathfrak{l}, V) = 0$ for all $n \geq 0$.*

PROOF. As x is central, the map $m_x : v \longmapsto x.v$ is a $\mathfrak{l}$–module endomorphism of V, inducing therefore endomorphisms $H^n(m_x) : H^n(\mathfrak{l}, V) \longrightarrow H^n(\mathfrak{l}, V)$. On n–cochains, these are given by $f \longmapsto m_x \circ f$. Because since x is central, the sum in the expression for $\rho(x)f$ vanishes, so that we remain with

$$(\rho(x)f)(x_1 \wedge \cdots \wedge x_n) = x.f(x_1 \wedge \cdots \wedge x_n) = (m_x \circ f)(x_1 \wedge \cdots \wedge x_n)$$

that is to say $\rho(x)f = m_x \circ f$. The Cartan formula shows that the action of $\mathfrak{l}$ on the cohomology spaces is trivial, that is, if f is a cocycle then $\rho(x)f$ is a coboundary. Thus $H^n(m_x)$ is the zero map on $H^n(\mathfrak{l}, V)$. But the very same map induces by hypothesis an automorphism of $H^n(\mathfrak{l}, V)$. Therefore, $H^n(\mathfrak{l}, V)$ is trivial. □

– 5.1.7. Let L be an ℓ–adic Lie group with Lie algebra $\mathfrak{l}$, and let V be a $\mathbb{Q}_\ell$ vector space on which L acts continuously. This action is then analytic, hence induces an action of $\mathfrak{l}$ on V, and one can introduce continuous cohomology $H^n_{\mathrm{c}}(L, V)$ using continuous cochains, analytical cohomology $H^n_{\mathrm{an}}(L, V)$ using analytical cochains, and Lie algebra cohomology $H^n(\mathfrak{l}, V)$. These cohomology groups compare as follows. The natural morphisms

$$H^n_{\mathrm{an}}(L, V) \longrightarrow H^n_{\mathrm{c}}(L, V)$$

are isomorphisms ([**Laz65**], V.2.3.10). We will write just $H^i(L, V)$ for these groups. The Lie algebra cohomology groups $H^i(\mathfrak{l}, V)$ are naturally isomorphic to *stable cohomology* defined by

$$H^n_{\mathrm{st}}(L, V) := \operatorname*{colim}_{U \subseteq L} H^n(U, V)$$

where the colimit runs over all open subgroups U of L. On the other hand, L acts on $H^i(\mathfrak{l}, V)$, and the fixed points of this action can be identified with $H^i(L, V)$ ([**Laz65**], V.2.4.10). In particular, if $H^i(\mathfrak{l}, V)$ is trivial, then $H^i(L, V)$ is trivial as well.
Often, we will be given a Lie group L acting on a finitely generated $\mathbb{Z}_\ell$–module T, which we can extend by linearity to an action of L on $V := T \otimes \mathbb{Q}_\ell$. We can compare $H^i(L, T)$ with $H^i(L, V)$ using the following proposition:

PROPOSITION 5.1.8. *Let T be a finitely generated $\mathbb{Z}_\ell$–module, and let L be a topological group acting continuously and linearly on T and set $V := T \otimes \mathbb{Q}_\ell$. The canonical $\mathbb{Q}_\ell$–linear maps*

$$\alpha_n : H^n(L, T) \otimes \mathbb{Q}_\ell \longrightarrow H^n(L, V)$$

are isomorphisms for $n = 0$ and $n = 1$. If L is topologically finitely generated, then $H^n(L, T)$ is a finitely generated $\mathbb{Z}_\ell$–module, finite if T is so, and $H^n(L, V)$ is a finite dimensional $\mathbb{Q}_\ell$–vector space for all $n \geq 0$. The maps α_n are all isomorphisms in that case.

PROOF. We work with continuous cochain cohomology. Let $Z^n(L, T)$ and $B^n(L, T)$ be the sets of continuous n–cocycles and n–coboundaries respectively.
That α_0 is an isomorphism is trivial, and that α_1 is an isomorphism follows from [**Ser64**], Proposition 9. Now suppose that L is topologically generated, i.e. that there exists a finite subset X of L such that the subgroup of L generated by X is dense in L. A continuous n–coboundary $f : L^n \longrightarrow T$ is uniquely determined by the values it takes on X^n. Therefore $Z^n(L, T)$ is finitely generated as a $\mathbb{Z}_\ell$–module, hence $H^n(L, T)$. If T is finite, then $Z^n(L, T)$ is finite, hence $H^n(L, T)$, and the same argument shows that $Z^n(L, V)$ is a finite dimensional vector space, hence $H^n(L, V)$. Moreover, we have $Z^n(L, T \otimes \mathbb{Q}_\ell) \cong Z^n(L, T) \otimes \mathbb{Q}_\ell$ and $B^n(L, T \otimes \mathbb{Q}_\ell) \cong B^n(L, T) \otimes \mathbb{Q}_\ell$, hence the desired isomorphisms. □

This shows in particular that if L is a Lie group acting on a finitely generated $\mathbb{Z}_\ell$–module T, then $H^1(L, T)$ is finite if and only if $H^1(L, V)$ is trivial.

PROPOSITION 5.1.9. *Let T be a finitely generated $\mathbb{Z}_\ell$–module, and set $T_i := T/\ell^i T$, so that $T \cong \lim T_i$. Let L be a topological group acting continuously and linearly on T. The canonical maps*

$$\alpha_n : H^n(L, T) \longrightarrow \lim_{i \geq 0} H^n(L, T_i)$$

are isomorphisms for $n = 0$ and $n = 1$. If L is topologically finitely generated, then the maps α_n isomorphisms for all $n \geq 0$.

PROOF. That α_0 is an isomorphism is trivial, and that α_1 is an isomorphism follows from Proposition 7 of [**Ser64**]. Suppose then that L is topologically finitely generated, so that by Proposition 5.1.8 the exact triangles $T \longrightarrow T \longrightarrow T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}$ yield short exact sequences of finite groups

$$0 \longrightarrow H^n(L, T)/\ell^i H^n(L, T) \longrightarrow H^n(L, T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}) \longrightarrow H^{n+1}(G, T)[\ell^i] \longrightarrow 0$$

Taking limits over i, we find a short exact sequence of topological groups

$$0 \longrightarrow H^n(L, T) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \longrightarrow \lim_{i \geq 0} H^n(L, T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}) \longrightarrow \mathrm{T}_\ell H^{n+1}(G, T) \longrightarrow 0$$

Now, because $H^n(L, T)$ and $H^{n+1}(G, T)$ are finitely generated $\mathbb{Z}_\ell$–modules, this sequence yields in fact an isomorphism

$$H^n(L, T) \xrightarrow{\cong} \lim_{i \geq 0} H^n(L, T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z})$$

Finally, we claim that the limit of the $H^n(L, T\otimes^{\mathbb{L}}\mathbb{Z}/\ell^i\mathbb{Z})$ is the same as the limit of the $H^n(L, T/\ell^iT)$. Indeed, we have a canonical exact triangle $T/\ell^iT \longrightarrow T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z} \longrightarrow T[\ell^i]$ which yields an exact sequence

$$\lim_{i\geq 0} H^{n-1}(L, T[\ell^i]) \longrightarrow \lim_{i\geq 0} H^n(L, T \otimes^{\mathbb{L}} \mathbb{Z}/\ell^i\mathbb{Z}) \longrightarrow \lim_{i\geq 0} H^n(L, T/\ell^iT) \longrightarrow \lim_{i\geq 0} H^n(L, T[\ell^i])$$

But now, because the torsion part of T killed by ℓ^i for sufficiently big i, the $T[\ell^i]$ form a null–system, hence the $H^n(L, T[\ell^i])$. □

5.2. Lie groups and Lie algebras associated with a 1–motive

We now come to the Lie group L^M and its subgroups we already encountered in the introduction. We shall define these Lie groups and give some rough structure results. We fix for the whole section a number field k with algebraic closure $\overline{k}$, and write $\Gamma := \mathrm{Gal}(\overline{k}|k)$.

– 5.2.1. Let M be a torsion–free 1–motive over k. The group Γ acts continuously on the finitely generated free $\mathbb{Z}_\ell$–module $\mathrm{T}_\ell M$. We define

$$L^M := \mathrm{im}\left(\Gamma \longrightarrow \mathrm{GL}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell M)\right)$$

Because Γ is compact, this image is closed, hence an ℓ–adic Lie group. In the same fashion, we define the Lie groups $L^{M_A}, L^G, L^Y, \ldots$. Then, we define

$$L^M_G := \ker\left(L^M \longrightarrow L^G\right)$$

In words, L^M_G is the subgroup of L^M consisting of those elements acting trivially on the Tate module of G. Similarly, L^M_{Y,M_A} stands for the subgroup of L^M consisting of those elements which act trivially on the Tate modules of Y and M_A. In the very same fashion, we define $L^{M_A}_A, L^G_Y, L^G_{Y,A}$ and so on. We can associate Lie algebras to these Lie groups, which we shall write as $\mathfrak{l}^M, \mathfrak{l}^M_G, \mathfrak{l}^A$ and so forth.

– 5.2.2. The Lie groups introduced above are quotients of the Galois group Γ, thus correspond to extensions of k. The group L^Y is the Galois group of the smallest Galois extension of k which trivializes Y. In particular, $\mathfrak{l}^Y$ is trivial because L^Y is finite.
All the other Lie groups we are considering are in general infinite. We can describe them as follows: Let H be a commutative geometrically connected algebraic group over k, and let $S \subseteq H(\overline{k})$ be a subset. We write k_S for the subfield of $\overline{k}$ generated by the coordinates of all points $R \in H(\overline{k})$ such that $\ell^n R \in S$ for some $n \geq 0$. If $S = \{P\}$ is a single point, we write k_P instead of k_S. The following relations are clear:

$$k_{S\cup S'} = \langle k_S, k_{S'}\rangle \qquad \text{and} \qquad k_{\langle S\rangle} = k_S$$

Here $\langle S\rangle$ is the subgroup of $H(\overline{k})$ generated by S. In particular, if 1_H denotes the identity of H, then $k_{1_H} \subseteq k_S$, provided S is nonempty. Moreover, if $\varphi : H \longrightarrow H'$ is a surjective morphism of algebraic groups defined over k, then the relation

$$k_{\varphi(S)} \subseteq k_S$$

holds. By definition, an element of the Galois group Γ acts trivially on k_{1_H} if and only if it acts trivially on all ℓ^n–torsion points of $H(\overline{k})$, that is to say if and only it acts trivially on the Tate module $\mathrm{T}_\ell H$. Thus, coming back to our semiabelian variety, if O_G, O_A and 1_T denote the identity element of G, A and T respectively, we have

$$L^G = \mathrm{Gal}(k_{O_G}|k) \qquad \text{and} \qquad L^A = \mathrm{Gal}(k_{O_A}|k) \qquad \text{and} \qquad L^T = \mathrm{Gal}(k_{1_T}|k)$$

An element of Γ acts trivially on the Tate module of M if and only if it acts trivially on Y and on all $R \in G(\overline{k})$ such that $\ell^n R = u(y)$ for some $y \in Y$ and $n \geq 0$. Therefore, if k' denotes the minimal Galois extension of k which trivializes Y, we have

$$L^M = \mathrm{Gal}(k'_{u(Y)}|k) \qquad \text{and} \qquad L^{M_A} = \mathrm{Gal}(k'_{v(Y)}|k)$$

where $M_A = [v : Y \longrightarrow A]$. The relative groups can now be explained by

$$L^M_{G,Y} = \mathrm{Gal}(k'_{u(Y)}|k'_{O_G}) \qquad \text{and} \qquad L^G_A = \mathrm{Gal}(k_{O_G}|k_{O_A}) \qquad \text{and} \qquad L^{M_A}_{A,Y} = \mathrm{Gal}(k'_{v(Y)}|k'_{O_A})$$

and so on.

– 5.2.3. To the 1–motive M over k, we have associated several Lie algebras, which act naturally on the ℓ–adic representation spaces. We would appreciate to have a complete structure result for these algebras. Unfortunately, already the Lie algebra $\mathfrak{l}^A$ associated to the abelian variety A over k is not fully understood. For instance, it seems not to be known whether the dimension of $\mathfrak{l}^A$ is independent of the prime ℓ or not.
For elliptic curves, Serre ([**Ser68**], IV.2) gives a complete structure result: If A is an elliptic curve without complex multiplication, then $\mathfrak{l}^A = \mathfrak{gl}(\mathrm{V}_\ell A) \simeq \mathfrak{gl}_2\mathbb{Q}_\ell$, and if A has complex multiplication, then $\mathfrak{l}^A$ is commutative and two dimensional, thus consists of the diagonal elements of $\mathfrak{gl}(\mathrm{V}_\ell A)$. So far, the only result that applies to general abelian varieties is due to F.A.Bogomolov, who proved in [**Bog81**] (Theorem 3) the following result, originally conjectured by Serre:

THEOREM 5.2.4 (Bogomolov 1981). *The Lie algebra $\mathfrak{l}^A \leq \mathfrak{gl}(\mathrm{V}_\ell A)$ is algebraic and contains the scalars.*

Serre conjectured more precisely ([**Ser71**], §2, remark 3) that $\mathfrak{l}^A$ coincides with the Lie algebra of the Hodge group of A, augmented by the scalars. This is known to be true for products of elliptic curves (see [**Ima76**]).
The analogue for a torus T is banal: The Lie algebra $\mathfrak{l}^T$ is one dimensional except for trivial T, and acts as scalar multiplication on $\mathrm{V}_\ell T$. The Lie algebra $\mathfrak{l}^Y$ is always trivial.

PROPOSITION 5.2.5. *The Lie algebras $\mathfrak{l}^M, \mathfrak{l}^M_G, \mathfrak{l}^A, \ldots$ do not change when k is replaced by a finite extension of k, nor do they change when M is replaced by a 1–motive isogenous to M.*

PROOF. Replacing k by a finite extension replaces Γ and thus L^M by an open subgroup, hence leaves $\mathfrak{l}^M$ invariant. Replacing M by an isogenous 1–motive leaves L^M unchanged. Indeed, if $M \longrightarrow M'$ is an isogeny, then the map $\mathrm{V}_\ell M \longrightarrow \mathrm{V}_\ell M'$ is an isomorphism of Γ–modules, and we can look at L^M also as being the image of Γ in $\mathrm{GL}(\mathrm{V}_\ell M)$. The same goes for all the other Lie algebras. □

PROPOSITION 5.2.6. *Let A be a nonzero abelian variety with dual $A^\vee$, and write O and $O^\vee$ for the origins of A and $A^\vee$ respectively. The fields k_O and $k_{O^\vee}$ are equal, and contain all ℓ–th power roots of unity.*

PROOF. There exist isogenies $A \longrightarrow A^\vee$, and therefore the inclusion $k_{O^\vee} \subseteq k_O$ holds. The situation is symmetric, so we have in fact $k_{O^\vee} = k_O$. The Weil pairing $e_{\ell^n} : A[\ell^n] \times A^\vee[\ell^n] \longrightarrow \mu_{\ell^n}$ is nondegenerate, hence surjective, and Galois invariant. Thus, if an element of Γ acts trivially on k_O, it acts trivially on $A[\ell^n]$ and on $A^\vee[\ell^n]$, hence trivially on μ_{ℓ^n}. □

COROLLARY 5.2.7. *Let A be a nonzero abelian variety and T be a torus over k. The projection $L^{A\times T} \longrightarrow L^A$ has finite kernel, and the induced Lie algebra map $\mathfrak{l}^{A\times T} \longrightarrow \mathfrak{l}^A$ is an isomorphism.*

PROOF. Without loss of generality we may suppose that T is split. But in that case, the proposition even shows that $L^{A\times T} = \mathrm{Gal}(\langle k_{O_A}, k_{1_T}\rangle\,|k) \longrightarrow \mathrm{Gal}(k_{O_A}|k) = L^A$ is an isomorphism. $\square$

– 5.2.8. We will now have a closer look at some of the subgroups of L^M and the corresponding subalgebras of $\mathfrak{l}^M$ introduced above. The overall picture is given by the following diagrams of Lie groups and algebras:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L^M_{G,M_A} \arrow[r] \arrow[d] & L^M_{G,Y} \arrow[r] \arrow[d] & L^{M_A}_{G,Y} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L^M_{T,M_A} \arrow[r] \arrow[d] & L^M_{T,A,Y} \arrow[r] \arrow[d] & L^{M_A}_{A,Y} \arrow[r] & 0 \\
0 \arrow[r] & L^G_{T,M_A} \arrow[r] \arrow[d] & L^G_{T,A} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathfrak{l}^M_{G,M_A} \arrow[r] \arrow[d] & \mathfrak{l}^M_{G} \arrow[r] \arrow[d] & \mathfrak{l}^{M_A}_{G} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{l}^M_{T,M_A} \arrow[r] \arrow[d] & \mathfrak{l}^M_{T,A} \arrow[r] \arrow[d] & \mathfrak{l}^{M_A}_{A} \arrow[r] & 0 \\
0 \arrow[r] & \mathfrak{l}^G_{T,M_A} \arrow[r] \arrow[d] & \mathfrak{l}^G_{T,A} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Much about these Lie groups and algebras is told by the following generality:

PROPOSITION 5.2.9. *Let $0 \longrightarrow V' \longrightarrow V \longrightarrow \overline{V} \longrightarrow 0$ be a short exact sequence of free $\mathbb{Z}_\ell$–modules of finite rank, and let $L \leq \mathrm{GL}(V)$ be a closed subgroup which leaves V' invariant. Let H be the subgroup of L consisting of those elements which act trivially on V' and on $\overline{V}$. Then, as an L–group via the conjugation action, H is naturally isomorphic to a submodule of* $\mathrm{Hom}(\overline{V}, V')$*. In particular, the Lie group H is commutative and torsion free.*

PROOF. Choose a linear section $s : \overline{V} \longrightarrow V$ of the quotient map, and define $\vartheta : H \longrightarrow \mathrm{Hom}(\overline{V}, V)$ by sending $h \in H$ to the linear map $\overline{v} \longmapsto hs(\overline{v}) - s(\overline{v})$. That this map ϑ is an injective L–module homomorphism and independent of the choice of s is straightforward to check. $\square$

COROLLARY 5.2.10. *There are canonical injections of L^M–modules (or Γ–modules)*

$$L^M_{G,Y} \longrightarrow \mathrm{Hom}(Y\otimes\mathbb{Z}_\ell, \mathrm{T}_\ell G) \qquad \textit{and} \qquad L^M_{T,M_A} \longrightarrow \mathrm{Hom}(\mathrm{T}_\ell M_A, \mathrm{T}_\ell T)$$

as well as canonical injections of $\mathfrak{l}^M$–modules

$$\mathfrak{l}^M_G \longrightarrow \mathrm{Hom}(Y\otimes\mathbb{Q}_\ell, \mathrm{V}_\ell G) \qquad \textit{and} \qquad \mathfrak{l}^M_{T,M_A} \longrightarrow \mathrm{Hom}(\mathrm{V}_\ell M_A, \mathrm{V}_\ell T)$$

All Lie groups in 5.2.8 in the left hand side diagram are torsion free, and, with the possible exception of $L^M_{T,A,Y}$, commutative. The corresponding Lie algebras are commutative, except maybe $\mathfrak{l}^M_{T,A}$ which is nilpotent.

– 5.2.11. We call these injections *Kummer injections*. The formula for ϑ in Proposition 5.2.9 reminds us of the formula for a connecting homomorphism in group cohomology. Indeed, because $L^M_{G,Y}$ acts trivially on $\mathrm{T}_\ell G$ the cohomology group $H^1(L^M_{G,Y}, \mathrm{T}_\ell G)$ can be identified with the group of $\mathbb{Z}_\ell$–linear homomorphisms $\mathrm{Hom}(L^M_{G,Y}, \mathrm{T}_\ell G)$. Consider now the short exact sequence of $L^M_{G,Y}$–modules $0 \longrightarrow \mathrm{T}_\ell G \longrightarrow \mathrm{T}_\ell M \longrightarrow Y \otimes \mathbb{Z}_\ell \longrightarrow 0$. Part of the associated long exact sequence reads

$$0 \longrightarrow (\mathrm{T}_\ell M)^\Gamma \longrightarrow Y \otimes \mathbb{Z}_\ell \xrightarrow{\partial} \mathrm{Hom}(L^M_{G,Y}, \mathrm{T}_\ell G) \longrightarrow H^1(L^M_{G,Y}, \mathrm{T}_\ell M) \longrightarrow \cdots$$

From the usual description of the connecting morphism ∂ and from the construction of ϑ it is now immediate that the equality $\partial(y)(g) = \vartheta(g)(y)$ holds for all $y \in Y \otimes \mathbb{Z}_\ell$ and $g \in L^M_{G,Y}$.

5.3. Lie algebra cohomology of the Tate module

In this section we compute some Lie algebra cohomology groups associated with a 1–motive. What makes our computation work is the combination of Bogomolov's theorem 5.2.4 together with the elementary Lemma 5.1.6. The main statement is the following theorem, generalizing Serre's theorem 2 in [**Ser71**].

THEOREM 5.3.1. *Let G be a semiabelian variety over k with abelian part A and toric part T. Then, for all $i \in \mathbb{Z}$, the following holds:*

(1) *The groups $H^i(\mathfrak{l}^A, \mathrm{V}_\ell A)$, $H^i(\mathfrak{l}^T, \mathrm{V}_\ell T)$ and $H^i(\mathfrak{l}^{A\times T}, \mathrm{V}_\ell(A \times T))$ are trivial.*

(2) *There is a canonical, natural isomorphism $H^i(\mathfrak{l}^G, \mathrm{V}_\ell A) \cong H^{i-1}(\mathfrak{l}^{A\times T}, \mathrm{Hom}(\mathfrak{l}^G_{A\times T}, \mathrm{V}_\ell A))$.*

(3) *There is a canonical, natural isomorphism $H^i(\mathfrak{l}^G, \mathrm{V}_\ell T) \cong H^{i-2}(\mathfrak{l}^{A\times T}, \mathrm{Hom}(\bigwedge^2 \mathfrak{l}^G_{A\times T}, \mathrm{V}_\ell T))$.*

with the convention that cohomology groups of negative degree are zero.

PROOF. Before starting the proof, let us point out a few useful facts: If $x \in \mathfrak{l}^A$ acts as scalar multiplication by λ on $\mathrm{V}_\ell A$, then x acts also as λ on $\mathrm{V}_\ell A^\vee$. Indeed, any polarization $A \longrightarrow A^\vee$ yields an isomorphism of Γ–modules $\mathrm{V}_\ell A \cong \mathrm{V}_\ell A^\vee$. On the tensor product $\mathrm{V}_\ell A \otimes \mathrm{V}_\ell A^\vee$, an element $x \in \mathfrak{l}^A$ acts according to the rule $x.(v \otimes w) = x.v \otimes w + v \otimes x.w$. Thus if x acts as multiplication by λ in $\mathrm{V}_\ell A$, then it acts as 2λ on $\mathrm{V}_\ell A \otimes \mathrm{V}_\ell A^\vee$. Because the Weil pairing $\mathrm{V}_\ell A \otimes \mathrm{V}_\ell A^\vee \longrightarrow \mathbb{Q}_\ell(1)$ is a surjective $\mathfrak{l}^A$–module map, x acts also as 2λ on $\mathbb{Q}_\ell(1)$.

(1) By Bogomolov's Theorem 5.2.4, the Lie algebra $\mathfrak{l}^A$ contains an element x which acts like a nonzero scalar on $\mathrm{V}_\ell A$. This x satisfies the hypothesis of Lemma 5.1.6, thus $H^i(\mathfrak{l}^A, \mathrm{V}_\ell A)$ is trivial for $i \geq 0$. Similarly, the Lie algebra $\mathfrak{l}^T \cong \mathbb{Q}_\ell$ is commutative and acts diagonally on $\mathrm{V}_\ell T$. In particular, every nonzero $x \in \mathfrak{l}^G$ is central and acts as an automorphism on $\mathrm{V}_\ell T$. We conclude again by Lemma 5.1.6. For the last statement of (1), we may suppose that A is nontrivial, so that $\mathfrak{l}^{T\times A} \cong \mathfrak{l}^A$ by 5.2.7. We just have to check that $H^i(\mathfrak{l}^A, \mathrm{V}_\ell T)$ is trivial. Indeed, if $x \in \mathfrak{l}^A$ acts as scalar multiplication by $\lambda \in \mathbb{Q}_\ell^*$ on $\mathrm{V}_\ell A$, then, as we have explained at the beginning of the proof, x acts as multiplication by 2λ on $\mathrm{V}_\ell \mathbb{G}_m$, hence on $\mathrm{V}_\ell T$. Again by 5.1.6, we find that $H^i(\mathfrak{l}^A, \mathrm{V}_\ell T) = 0$.

(2) We can suppose that A is nontrivial, and thus $\mathfrak{l}^{T\times A} \cong \mathfrak{l}^A$ and $\mathfrak{l}^G_{T,A} = \mathfrak{l}^G_A$. The Hochschild–Serre spectral sequence associated to the short exact sequence $0 \longrightarrow \mathfrak{l}^G_A \longrightarrow \mathfrak{l}^G \longrightarrow \mathfrak{l}^A \longrightarrow 0$ reads

$$H^i\big(\mathfrak{l}^A, H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell A)\big) \implies H^{i+j}(\mathfrak{l}^G, \mathrm{V}_\ell A)$$

Because $\mathfrak{l}^G_A$ is commutative and acts trivially on $\mathrm{V}_\ell A$, the cohomology group $H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell A)$ is the space of alternating $\mathbb{Q}_\ell$–multilinear maps from $(\mathfrak{l}^G_A)^j$ to $\mathrm{V}_\ell A$, thus

$$H^i\big(\mathfrak{l}^A, \mathrm{Hom}(\textstyle\bigwedge^j \mathfrak{l}^G_A, \mathrm{V}_\ell A)\big) \implies H^{i+j}(\mathfrak{l}^G, \mathrm{V}_\ell A)$$

If $x \in \mathfrak{l}^A$ acts as scalar multiplication by λ in $\mathrm{V}_\ell A$, then x acts also by λ on $\mathfrak{l}^G_A$, because $\mathfrak{l}^G_A$ is as a $\mathfrak{l}^A$–module isomorphic to a submodule of $\mathrm{Hom}(\mathrm{V}_\ell T, \mathrm{V}_\ell A)$. Thus, x acts as multiplication by $j\lambda$ on the j–th exterior product of $\mathfrak{l}^G_A$, hence as multiplication by $(j-1)\lambda$ on $H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell A)$. By 5.1.6, we get $H^i\big(\mathfrak{l}^A, \mathrm{Hom}(\bigwedge^j \mathfrak{l}^G_A, \mathrm{V}_\ell A)\big) = 0$ for $j \neq 1$, and the claim follows.

(3) We can suppose again that A is nontrivial. The Hochschild–Serre spectral sequence for the same short exact sequence is this time

$$H^i\big(\mathfrak{l}^A, H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell T)\big) \implies H^{i+j}(\mathfrak{l}^G, \mathrm{V}_\ell T)$$

Because $\mathfrak{l}^G_A$ is commutative and acts trivially on $\mathrm{V}_\ell T$, the cohomology group $H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell T)$ is the space of alternating $\mathbb{Q}_\ell$–linear maps from $(\mathfrak{l}^G_A)^j$ to $\mathrm{V}_\ell T$, thus

$$H^i\big(\mathfrak{l}^A, \mathrm{Hom}(\textstyle\bigwedge^j \mathfrak{l}^G_A, \mathrm{V}_\ell T)\big) \implies H^{i+j}(\mathfrak{l}^G, \mathrm{V}_\ell T)$$

If $x \in \mathfrak{l}^A$ acts as scalar multiplication by λ in $\mathrm{V}_\ell A$, then x acts as scalar multiplication by $j\lambda$ on the j–th exterior product of $\mathfrak{l}^G_A$, and as scalar multiplication by 2λ on $\mathrm{V}_\ell T$, hence as scalar multiplication by $(j-2)\lambda$ on $H^j(\mathfrak{l}^G_A, \mathrm{V}_\ell T)$. Thus, by 5.1.6, we get $H^i\big(\mathfrak{l}^A, \mathrm{Hom}(\bigwedge^j \mathfrak{l}^G_A, \mathrm{V}_\ell T)\big) = 0$ for $j \neq 2$, and the claim follows. $\square$

COROLLARY 5.3.2. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. The extensions of Lie algebras*

$$0 \longrightarrow \mathfrak{l}^{M_A}_A \longrightarrow \mathfrak{l}^{M_A} \longrightarrow \mathfrak{l}^A \longrightarrow 0 \qquad \textit{and} \qquad 0 \longrightarrow \mathfrak{l}^G_A \longrightarrow \mathfrak{l}^G \longrightarrow \mathfrak{l}^A \longrightarrow 0$$

are split.

PROOF. By 5.2.10, the $\mathfrak{l}^A$–modules $\mathfrak{l}^{M_A}_A$ and $\mathfrak{l}^G_A$ are both isomorphic to a submodule of a power of $\mathrm{V}_\ell A$. Because $\mathrm{V}_\ell A$ is a semisimple $\mathfrak{l}^A$–module and $H^2(\mathfrak{l}^A, \mathrm{V}_\ell A) = 0$, one has $H^2(\mathfrak{l}^A, \mathfrak{l}^{M_A}_A) = 0$ and $H^2(\mathfrak{l}^A, \mathfrak{l}^G_A) = 0$. These cohomology groups classify extensions modulo split extensions by [**Wei94**] theorem 7.6.3, so the claim follows. $\square$

COROLLARY 5.3.3. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. If G is a split semiabelian variety, then there are canonical isomorphisms*

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

PROOF. The Hochschild–Serre spectral sequence for $0 \longrightarrow \mathfrak{l}^M_G \longrightarrow \mathfrak{l}^M \longrightarrow \mathfrak{l}^G \longrightarrow 0$ yields a short exact sequence in low degrees

$$0 \longrightarrow H^1(\mathfrak{l}^G, \mathrm{V}_\ell G) \longrightarrow H^1(\mathfrak{l}^M, \mathrm{V}_\ell G) \xrightarrow{\cong} H^0(\mathfrak{l}^G, H^1(\mathfrak{l}^M_G, \mathrm{V}_\ell G)) \longrightarrow H^2(\mathfrak{l}^G, \mathrm{V}_\ell G)$$

By claim (1) of Theorem 5.3.1, the first and last group in this sequence are zero, the morphism in the middle is thus an isomorphism as indicated. Because $\mathfrak{l}^M_G$ acts trivially on $\mathrm{V}_\ell G$ by definition, we have $H^1(\mathfrak{l}^M_G, \mathrm{V}_\ell G) = \mathrm{Hom}(\mathfrak{l}^M_G, \mathrm{V}_\ell G)$. $\square$

COROLLARY 5.3.4. *Let G be a split (or split up to isogeny) semiabelian variety over k. There is a canonical isomorphism of finite groups $H^1(L^G, \mathrm{T}_\ell G) \cong G(k)[\ell^\infty]$.*

PROOF. The group $H^1(L^G, \mathrm{T}_\ell G)$ is finite, because it is a $\mathbb{Z}_\ell$–module of finite type, and its tensor product with $\mathbb{Q}_\ell$ is $H^1(L^G, \mathrm{V}_\ell G)$ which is zero by 5.3.1. Say then $H^1(L^G, \mathrm{T}_\ell G)$ is killed by ℓ^N. The cohomology sequence associated with the short exact sequence $0 \longrightarrow \mathrm{T}_\ell G \longrightarrow \mathrm{T}_\ell G \longrightarrow G(\bar{k})[\ell^N] \longrightarrow 0$ shows the claim. $\square$

5.4. Relation with Galois cohomology

In this section we show how to pass from Lie group cohomology to Galois cohomology using the functor H^1_* which associates with a topological group G and a continuous G–module T the set of those cohomology classes in $H^1(G,T)$ that become trivial on each monogenous subgroup of G. A topological group is called *monogenous* if it contains a dense subgroup generated by a single element. In [**Ser64**], the idea to consider this object is attributed to J. Tate.

Definition 5.4.1. For a Hausdorff topological group G and a continuous G–module T, we write

$$H^1_*(G,T) := \ker\Big(H^1(G,T) \longrightarrow \prod H^1(C,T)\Big)$$

the product running over the monogenous subgroups C of G. Analogously for a Lie algebra $\mathfrak{l}$ and an $\mathfrak{l}$–module V we define

$$H^1_*(\mathfrak{l},V) := \ker\Big(H^1(\mathfrak{l},V) \longrightarrow \prod H^1(\mathfrak{c},V)\Big)$$

the product running over the one dimensional subalgebras $\mathfrak{c}$ of $\mathfrak{l}$.

– 5.4.2. A 1–cocycle $c : G \longrightarrow T$ represents an element of $H^1_*(G,T)$ if and only if for every element $g \in G$ there exists a an element $t_g \in T$ such that $c(g) = gt_g - t_g$. One of the main features of H^1_* is the following

Proposition 5.4.3 ([**Ser64**] Proposition 6). *Let N be a closed normal subgroup of G which acts trivially on T. Then, the restriction map $H^1(G/N,T) \longrightarrow H^1(G,T)$ induces an isomorphism $H^1_*(G/N,T) \longrightarrow H^1_*(G,T)$.*

The similar statement for Lie algebras holds as well. Mind that for cohomology groups of degree $i \neq 1$ the analogue definition doesn't make much sense. Our motivation to consider these groups is the following. Let S be a set of places of k of density 1, and let T be an ℓ–adic sheaf on k. We shall be concerned following group,

$$H^1_S(k,T) := \ker\left(H^1(k,T) \longrightarrow \prod_{v\in S} H^1(k_v,T)\right)$$

already used by Serre in [**Ser64**]. One of our main goals, as explained in the introduction, is to compute the group $H^1_S(k,\mathrm{T}_\ell M)$ for a torsion free 1–motive M over k. As Proposition 8 in [**Ser64**] (we reproduce it below, see 5.4.4) the group $H^1_S(k,T)$ is contained in $H^1_*(\Gamma,T)$. On the other hand, as O. Gabber hinted to us (see Lemma 5.4.5), if S does not contain a finite list of bad places, then even equality $H^1_S(k,T) = H^1_*(\Gamma,T)$ holds (both groups are subgroups of $H^1(\Gamma,T)$). Proposition 5.4.3 shows that the group $H^1_*(\Gamma,T)$ is the same as $H^1_*(L^T,T)$, where L^T is the image of Γ in $\mathrm{GL}\,T$, and this brings us back to Lie groups.

Proposition 5.4.4 ([**Ser64**], Proposition 8). *Let T be a finitely generated $\mathbb{Z}_\ell$–module with continuous Γ–action and let S be a set of finite places of k of natural density 1. The group $H^1_S(k,T)$ is contained in $H^1_*(\Gamma,T)$.*

Proof. It is enough to show that the proposition holds for finite Galois modules of order a power of ℓ, since T can be written as a limit of such, and the general case follows then by Proposition 5.1.9 and left exactness of limits.
So let F be a finite Galois module of order a power of ℓ. Let $c : \Gamma \longrightarrow F$ be a continuous cocycle representing an element of $H^1_S(\Gamma,T)$. Because F is finite, there exists an open subgroup N of Γ

on which c is zero. We may suppose that N is normal and acts trivially on F. Now let σ be an element of Γ, and let σ_N be its class in Γ/N. By Frobenius's density theorem, there exists a place $v \in S$ and an extension w of v to $\overline{k}$ such that decomposition group of w in Γ/N equals the group generated by σ_N. Since the restriction of c to the decomposition group $D_w \subseteq \Gamma$ is a coboundary, there exists a $x \in F$ such that

$$c(\tau) = \tau x - x \qquad \text{for all } \tau \in D_w$$

As N acts trivially on F, the same holds for all $\tau \in D_w N$, and in particular for $\tau = \sigma$. Since σ was arbitrary, this shows that the cohomology class of c belongs to $H^1_*(\Gamma, F)$. □

Lemma 5.4.5 (Gabber). *Let T be a finitely generated $\mathbb{Z}_\ell$–module with continuous Γ–action and let S be a set of finite places of k of natural density 1. Suppose that S does not contain the places dividing ℓ nor the places where T is ramified. The natural inclusion $H^1_S(k, T) \longrightarrow H^1_*(\Gamma, T)$ is an equality.*

Proof. Without loss of generality we suppose that S contains all but finitely many places of k and corresponds thus to the set of closed points of an open subscheme U of $\operatorname{spec} \mathcal{O}_k$. The Galois module T extends thus to an étale ℓ–adic sheaf on U. Write $\pi_U := \pi_1^{\text{ét}}(U, \overline{k})$ for the étale fundamental group of U with respect to the base point $\operatorname{spec} \overline{k} \longrightarrow \operatorname{spec} U$. The group π_U is a quotient of Γ, which can also be realized as the Galois group $\operatorname{Gal}(k_U|k)$, where k_U is the maximal extension of k in $\overline{k}$ unramified in U. The action of Γ on T factors over π_U, and so it makes sense to define

$$H^1_S(\pi_U, T) := \ker\left(H^1(\pi_U, T) \longrightarrow \prod_{v \in S} H^1(k_v, T)\right)$$

There is a natural injection $H^1_S(\pi_U, T) \longrightarrow H^1_S(\Gamma, T)$ induced by the inflation map. By Proposition 5.4.3 we know that $H^1_*(\pi_U, T)$ is isomorphic to $H^1_*(\Gamma, T)$ via inflation, and it is thus enough to show that the natural inclusion

$$H^1_S(\pi_U, T) \longrightarrow H^1_*(\pi_U, T)$$

is an isomorphism. But this is clear, since every decomposition group in π_U corresponding to a place in S is monogenous. □

– 5.4.6. Let M be a torsion free 1–motive over k. Working with Lie algebras and Lie algebra cohomology we shall be able to compute the group $H^1_*(k, \mathrm{V}_\ell M)$, which is essentially the same as $H^1_S(k, \mathrm{T}_\ell M)$, except that all information about torsion is lost. However, we have also big interest in controlling the torsion part of $H^1_*(L^M, \mathrm{T}_\ell M)$. To anticipate this, we will solve in Chapter 8 the problem of "detecting subgroups by reductions". This is heavily based on the vanishing of the torsion in $H^1_*(L^M, \mathrm{T}_\ell M)$ for certain 1–motives.
We end this section with presenting a handy criterion for $H^1_*(L, T)$ to be torsion free for a general compact ℓ–adic Lie group L acting on a finitely generated free $\mathbb{Z}_\ell$–module T. In [**Ser64**] it is shown that if there exists an element $g \in L^M$ such that the only element of $\mathrm{T}_\ell M$ fixed under g is 0, then $H^1_*(L^M, \mathrm{T}_\ell M)$ is torsion free. Such an element can always be found if $M = [0 \longrightarrow G]$ is a semiabelian variety, but in general it does not exist. We use the following lemma instead.

Lemma 5.4.7. *Let T be a finitely generated free $\mathbb{Z}_\ell$–module, set $V := T \otimes \mathbb{Q}_\ell$, and let $L \subseteq \operatorname{GL} T$ be a Lie group with Lie algebra $\mathfrak{l}$. If the equality $V^L = V^{\mathfrak{l}}$ holds then $H^1_*(L, T)$ is torsion free.*

– 5.4.8. The proof of this lemma needs some preparation. Let us introduce the following ambulant terminology: Given a finitely generated free $\mathbb{Z}_\ell$–module T and a Lie group $L \subseteq \mathrm{GL}\,V$ for $V = T \otimes \mathbb{Q}_\ell$ we say that L is *tight* or that L acts *tightly* if the equality

$$\bigcap_{g\in L} (T + V^g) = T + V^L$$

holds. A bit more generally, if V_2 is another vector space over $\mathbb{Q}_\ell$ we say that a family Φ of linear operators $\varphi : V \longrightarrow V_2$ is *tight* if the equality

$$(*) \qquad \bigcap_{\varphi\in\Phi} \big(T + \ker\varphi\big) = T + \bigcap_{\varphi\in\Phi} \ker\varphi$$

holds. So, L acts tightly on V if and only if the family of operators $\{(g - 1_V) \mid g \in L\}$ is tight. The following lemma shows how this is related with the torsion of $H^1_*(L, T)$.

LEMMA 5.4.9. *If $L \subseteq \mathrm{GL}\,T$ acts tightly on V then the group $H^1_*(L, T)$ is a torsion–free $\mathbb{Z}_\ell$–module.*

PROOF. Let $c : L \longrightarrow T$ be a cocycle representing an element of $H^1_*(L, T)[\ell]$, and let us show that c is a coboundary. As ℓc is a coboundary c is a coboundary in $H^1(L, V)$ and there exists an element $v \in V$ such that $c(g) = gv - v$ for all $g \in L$. To say that the cohomology class of c belongs to $H^1_*(L, T)$ is to say that for all $g \in L$, there exists a $t_g \in T$ such that $c(g) = gt_g - t_g$. We find that

$$(g - 1_V)t_g = (g - 1_V)v \qquad \text{for all } g \in L$$

or in other words $v - t_g \in \ker(g - 1_V)$, that is to say $v \in T + V^g$. Now, since L acts tightly, this implies that $v = t + v_0$ for some $t \in T$ and $v_0 \in V^G$. Hence $c(g) = gt - t$ is a coboundary as needed. □

LEMMA 5.4.10. *Let V_2 be a $\mathbb{Q}_\ell$–vector space and let Φ be a linear subspace of* $\mathrm{Hom}(V, V_2)$. *Then Φ is tight.*

PROOF. In $(*)$, the inclusion $\supseteq$ holds trivially, we have to show that the inclusion $\subseteq$ holds as well. Let V^* and V_2^* be the linear duals of V and V_2, and define $\Psi := \{\pi \circ \varphi \mid \varphi \in \Phi, \pi \in V_2^*\}$. We have then

$$\bigcap_{\varphi\in\Phi} \big(T + \ker\varphi\big) \subseteq \bigcap_{\psi\in\Psi} \big(T + \ker\psi\big) \qquad \text{and} \qquad \bigcap_{\varphi\in\Phi} \ker\varphi = \bigcap_{\psi\in\Psi} \ker\psi$$

Hence, it is enough to show that the lemma holds in the case where $V_2 = \mathbb{Q}_\ell$, and where Φ is a linear subspace of the dual space V^*. Write W for the intersection of the kernels $\ker\psi$, so that

$$W = \{w \in V \mid \varphi(v) = 0 \text{ for all } \varphi \in \Phi\} \qquad \text{and} \qquad \Phi = \{\varphi \in V^* \mid \varphi(w) = 0 \text{ for all } w \in W\}$$

Because $T/(T \cap W)$ is torsion free the submodule $W \cap T$ is a direct factor of T (every finitely generated torsion free $\mathbb{Z}_\ell$–module is free, hence projective), so that we can choose a $\mathbb{Z}_\ell$–basis $e_1, \dots, e_s, \dots, e_r$ of T such that $e_1, \dots, e_s$ make up a $\mathbb{Z}_\ell$–basis of $W \cap T$. Let v be an element of V that is contained in $T + \ker\varphi$ for all $\varphi \in \Phi$. We can write v as

$$v = \underbrace{\lambda_1 v_+ \cdots + \lambda_s e_s}_{\in W} + \lambda_{s+1}e_{s+1} + \cdots + \lambda_r e_r$$

where the λ_i are scalars in $\mathbb{Q}_\ell$. Taking for φ the projection onto the i–th component for $s < i \leq r$ shows that $\lambda_i \in \mathbb{Z}_\ell$ for $s < i \leq r$. Hence $\lambda_{s+1}e_{s+1} + \cdots + \lambda_r e_r \in T$, and we find that $v \in W + T$ as required. □

Proof of Lemma 5.4.7. As we have seen in Lemma 5.4.9, it is enough to show that if the equality $V^L = V^{\mathfrak{l}}$ holds, then L acts tightly on V.
Let H be an open subgroup of L such that the logarithm map is defined on H. Such a subgroup always exists, and the exponential of $\log h$ is then also defined and one has $\exp\log h = h$ for all $h \in H$ ([**Bou72**], Ch.II, §8, no.4, proposition 4). The Lie algebra of H is also $\mathfrak{l}$. Let h be an element of H and set $\varphi := \log h$, so that $h = \exp\varphi$. We claim that equality $V^h = \ker\varphi$ holds. On one hand if $hv = v$, then the series

$$\varphi(v) = \log h(v) = (h-1)(v) - \frac{(h-1)^2(v)}{2} + \cdots + (-1)^{n-1}\frac{(h-1)^n(v)}{n} + \cdots$$

is zero, whence $V^h \subseteq \ker\varphi$. On the other hand, if $\varphi(v) = 0$, then the series

$$h(v) = \exp\varphi(v) = 1_V(v) + \varphi(v) + \frac{\varphi^2(v)}{2} + \cdots + \frac{\varphi^n(v)}{n!} + \cdots$$

is trivial except for its first term which is $1_V(v) = v$, whence the inclusion in the other direction. The Lie algebra $\mathfrak{l}$ has the good taste of being a *linear* subspace of $\operatorname{End} V$, so that we apply Lemma 5.4.10. Using these preliminary considerations, Lemma 5.4.10 and the hypothesis we find

$$\bigcap_{g\in L}(T + V^g) \ \subseteq\ \bigcap_{\varphi\in\mathfrak{l}}(T + \ker\varphi) \ =\ T + V^{\mathfrak{l}} \ =\ T + V^L$$

hence L acts tightly on V as claimed. Mind that in the second intersection it does not matter whether we take the intersection over $\varphi \in \mathfrak{l}$ or $\varphi \in \log(H)$, because every element of $\mathfrak{l}$ is a scalar multiple of an element in $\log(H)$. □

Proposition 5.4.11. *Let $M = [u : Y \longrightarrow G]$ be a 1–motive over the number field k, and set $\Gamma := \mathrm{Gal}(\overline{k}|k)$. Write Z for the kernel of the Γ–module map $Y \longrightarrow G(\overline{k})$. If Z is constant then the $\mathbb{Z}_\ell$–module $\mathrm{T}_\ell M$ and the group L^M acting on it satisfy the hypothesis of Lemma 5.4.7, hence $H^1_*(L^M, \mathrm{T}_\ell M)$ and $H^1_S(k, \mathrm{T}_\ell M)$ are torsion free in that case.*

Proof. Observe that $Z^\Gamma = H^{-1}(k, M)$ and that $(\mathrm{T}_\ell M)^\Gamma = H^0(k, \mathrm{T}_\ell M)$. From Corollary 3.3.15 we get an isomorphism

$$Z^\Gamma \otimes \mathbb{Z}_\ell = H^{-1}(k, M) \otimes \mathbb{Z}_\ell \longrightarrow H^0(k, \mathrm{T}_\ell M) = \mathrm{T}_\ell M^{L_M}$$

Tensoring with $\mathbb{Q}_\ell$ yields the first isomorphism of the proposition. An element of $\mathrm{V}_\ell M$ is fixed under the action of the Lie algebra $\mathfrak{l}^M$ if and only if it is fixed under the action of some open subgroup of L^M (as explained in 5.1.7). Every sufficiently small open subgroup of L^M acts trivially on $Z \otimes \mathbb{Z}_\ell$, hence the second isomorphism. □

We shall also need a relative version of Lemma 5.4.7, dealing with a Lie group L and a subgroup D of L. This is the following Lemma, which in the case where D is the trivial subgroup gives back Lemma 5.4.7. In our application, L will be the image of the absolute Galois group of the number field k in $\mathrm{GL}(\mathrm{T}_\ell M)$, and D will be the image of some decomposition group.

Lemma 5.4.12. *Let T be a finitely generated free $\mathbb{Z}_\ell$–module and let $L \leq \mathrm{GL}\, T$ be a Lie group. Let D be a closed subgroup of L. If for all open subgroups N of L containing D the equality $T^L = T^N$ holds, then the map $H^1_*(L, T) \longrightarrow H^1(D, T)$ is injective on torsion elements.*

Proof. Write $\mathfrak{l}$ and $\mathfrak{d}$ for the Lie algebras of L and D, and let N be a sufficiently small open normal subgroup of L on which the logarithm is defined, so that $V^{\mathfrak{l}} = V^N$ and $V^{\mathfrak{d}} = V^{N\cap D}$. Let $c : L \longrightarrow T$ be a cocycle representing an element of order ℓ in $\ker(H^1_*(L, T) \longrightarrow H^1(D, T))$. As in the proof of Lemma 5.4.7, there exists a $v \in V$ such that $c(g) = gv - v$ for all $g \in L$, and we have $v \in V^{\mathfrak{f}} + T$. Since the restriction of c to D is a cocycle, we also have also $v \in V^D + T$, so that

$$v \in (V^{\mathfrak{f}} + T) \cap (V^D + T)$$

Changing v by an element of T, we may without loss of generality assume that $v \in V^D$, hence in $V^{\mathfrak{d}}$. The finite group $G := D/(N \cap D)$ acts on $V^{\mathfrak{d}}$. By Maschke's theorem, there exists a $\mathbb{Q}_\ell$–linear, G equivariant retraction map $r : V^{\mathfrak{d}} \longrightarrow V^{\mathfrak{f}}$ of the inclusion $V^{\mathfrak{f}} \leq V^{\mathfrak{d}}$. Restricting r to $V^{\mathfrak{f}} + (T \cap V^{\mathfrak{d}})$ we find a decomposition of G–modules

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

Writing $v = v_1 + t_1$ with $v_1 \in V^{\mathfrak{f}}$ 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) are invariant under G, so that in particular $v \in (V^{\mathfrak{f}} \cap V^G) + T$. But the intersection $V^{\mathfrak{f}} \cap V^G$ is just $V^N \cap F^D = V^{DN}$, so that

$$v \in V^{DN} + T$$

Now DN is an open subgroup of L containing D, hence $v \in V^L + T$, and that precisely means that c is a coboundary. □

REMARK 5.4.13. In practice we shall use this lemma in the following form. Let, as in the lemma, T be a finitely generated free $\mathbb{Z}_\ell$–module, $L \leq \mathrm{GL}\, T$ be a Lie group, D be a closed subgroup of L and z be a torsion element of $H^1_*(L, T)$. Our Lemma implies that if z restricts to zero on D, then z restricts already to zero on an open subgroup U of L *containing* D.
Indeed, let U be an open subgroup of L containing D, so small such that for any other open subgroup $V \subseteq U$ containing D the equality $T^V = T^U$ holds. The lemma applied to the Lie group $U \subseteq \mathrm{GL}\, T$ shows that the restriction map $H^1_*(U, T) \longrightarrow H^1(D, T)$ is injective on torsion elements. But this just implies that z restricts to zero in $H^1(U, T)$.

5.5. Controlling the torsion of $Ш^1(k, \mathbb{T}_\ell M)$

We now come to a first application of the techniques developed so far. Our goal is to compute the torsion subgroup of $Ш^1(k, \mathbb{T}_\ell M)$ for a 1–motive with torsion M over a number field k, and in particular to establish the isomorphism

$$Ш^0(k, M)[\ell^\infty] \cong Ш^1(k, \mathbb{T}_\ell M)_{\mathrm{tor}}$$

This is what we needed for the duality theorem 4.2.6. More generally, we shall work with a set of places S of k of density 1 and compute the torsion part of the group $H^1_S(k, \mathbb{T}_\ell M)$. The main result of this section is the following theorem.

THEOREM 5.5.1. *Let M be a 1–motive with torsion over k. The group $H^1_S(k, \mathbb{T}_\ell M)$ is a finitely generated $\mathbb{Z}_\ell$–module, its rank being bounded independently of S and ℓ. There is a canonical isomorphism of finite groups*

$$H^0_S(k, M)[\ell^\infty] \xrightarrow{\cong} H^1_S(k, \mathbb{T}_\ell M)_{\mathrm{tor}}$$

both being killed by the degree of any Galois extension $k'|k$ over which $H^{-1}(M)$ is constant.

The proof of Theorem 5.5.1 proceeds as follows. We begin with showing some permanence properties of $H^1_S(k, \mathbb{T}_\ell M)$ (Proposition 5.5.2) and show the theorem in the elementary case where M is of the form $[Y \longrightarrow 0]$. Then, in order to use what we have worked out in the previous sections of this chapter we concentrate first on torsion free 1–motives in Lemma 5.5.4, then we handle a special case of the theorem in another Lemma 5.5.5 and prove finally the theorem itself.

PROPOSITION 5.5.2. *Let M and M' be 1–motives with torsion over k, let $f : M \longrightarrow M'$ be an isogeny over k (Definition 1.1.5), and let $k'|k$ be a finite field extension. Write S' for the set of places of k' lying over places in S. The following holds*

(1) *The map $H^1_S(k, \mathbb{T}_\ell M) \longrightarrow H^1_S(k, \mathbb{T}_\ell M')$ induced by f has finite kernel. In particular, the $\mathbb{Z}_\ell$–ranks of $H^1_S(k, \mathbb{T}_\ell M)$ and $H^1_S(k, \mathbb{T}_\ell M')$ are equal, and the group $H^1_S(k, \mathbb{T}_\ell M)$ is finite if and only if $H^1_S(k, \mathbb{T}_\ell M')$ is.*
(2) *The map $H^1_S(k, \mathbb{T}_\ell M) \longrightarrow H^1_{S'}(k', \mathbb{T}_\ell M)$ induced by inflation has a finite kernel. In particular the $\mathbb{Z}_\ell$–rank of $H^1_S(k, \mathbb{T}_\ell M)$ is less or equal than the $\mathbb{Z}_\ell$–rank of $H^1_{S'}(k', \mathbb{T}_\ell M)$, and if the group $H^1_{S'}(k', \mathbb{T}_\ell M)$ is finite, so is $H^1_S(k, \mathbb{T}_\ell M)$.*

PROOF. The isogeny f induces an exact triangle $F \longrightarrow \mathbb{T}_\ell M \longrightarrow \mathbb{T}_\ell M'$, where F is a ℓ–adic complex with finite homology groups, concentrated in degrees $0, 1, 2$. The long associated exact sequence shows that the kernel of the map $H^1_S(k, \mathbb{T}_\ell M) \longrightarrow H^1_S(k, \mathbb{T}_\ell M')$ is a subgroup of the finite group $H^0(k, F)$. This shows that the $\mathbb{Z}_\ell$–ranks of $H^1_S(k, \mathbb{T}_\ell M)$ is less than the $\mathbb{Z}_\ell$–rank of $H^1_S(k, \mathbb{T}_\ell M')$. The same argument applied to any isogeny $g : M' \longrightarrow M$ show that equality holds. For the second statement, we may assume that $k'|k$ is Galois, with Galois group G. But then, the kernel of the inflation map $H^1(k, \mathbb{T}_\ell M) \longrightarrow H^1(k', \mathbb{T}_\ell M)$ can be identified with the finite group $H^1(G, \mathbb{T}_\ell M)$ by Hochschild–Serre. □

LEMMA 5.5.3. *Let Z be Γ–module which is finitely generated as a group. There are canonical isomorphisms of finite groups*

$$H^1_S(k, Z)[\ell^\infty] \cong H^1_S(k, Z) \otimes \mathbb{Z}_\ell \cong H^1_S(k, Z \otimes \mathbb{Z}_\ell)$$

both being killed by the degree of any Galois extension $k'|k$ over which Z is constant.

PROOF. The first isomorphism simply holds because $H^1_S(k, Z)$ is finite. For the second one, choose a finite Galois extension $k'|k$ such that Z is constant over k'. We can proceed as in the proof of Proposition 4.2.2 in order to express $H^1_S(k, Z)$ and $H^1_S(k, Z \otimes \mathbb{Z}_\ell)$ in terms of cohomology groups of the finite group $\mathrm{Gal}(k'|k)$ and its subgroups. Thus, what we must show is that if we are given a finite group G acting on Z, then there is an isomorphism $H^1(G, Z) \otimes \mathbb{Z}_\ell \cong H^1(G, Z \otimes \mathbb{Z}_\ell)$. Indeed, this isomorphism can be deduced from the long exact cohomology sequence of the short exact sequence of G–modules

$$0 \longrightarrow Z \longrightarrow Z \otimes \mathbb{Z}_\ell \longrightarrow Z \otimes (\mathbb{Z}_\ell/\mathbb{Z}) \longrightarrow 0$$

Observe that the multiplication by a prime $p \neq \ell$ is an isomorphism on $Z \otimes \mathbb{Z}_\ell$ and multiplication by ℓ is an isomorphism on $Z \otimes (\mathbb{Z}_\ell/\mathbb{Z})$. The same holds then for the respective cohomology groups. The long exact cohomology sequence identifies then $H^i(G, Z \otimes \mathbb{Z}_\ell)$ with the ℓ–part of $H^i(G, Z)$ for all $i > 0$, and $H^{i-1}(G, Z \otimes (\mathbb{Z}_\ell/\mathbb{Z}))$ with the prime–to–ℓ part of $H^i(G, Z)$ for all $i > 1$. □

LEMMA 5.5.4. *Let M be a torsion free 1–motive over k. There is a canonical isomorphism of finite groups $H^1_S(k, H^{-1}(M) \otimes \mathbb{Z}_\ell) \cong H^1_S(k, \mathrm{T}_\ell M)_{\mathrm{tor}}$.*

PROOF. Write $Z := H^{-1}(M) = \ker(u : Y \longrightarrow G)$, and fix a Galois extension $k'|k$ with Galois group G, over which Z is constant. From the Hochschild–Serre spectral sequence we get a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^1(G, Z\otimes\mathbb{Z}_\ell) \arrow[r] \arrow[d] & H^1(k, \mathrm{T}_\ell M) \arrow[r] \arrow[d] & H^1(k', \mathrm{T}_\ell M) \arrow[d] \\
0 \arrow[r] & \prod H^1(G_w, H^0(k'_w, \mathrm{T}_\ell M)) \arrow[r] & \prod H^1(k_w, \mathrm{T}_\ell M) \arrow[r] & \prod H^1(k'_w, \mathrm{T}_\ell M)
\end{tikzcd}$$

The kernel of the right hand vertical map is $H^1_S(k', \mathrm{T}_\ell M)$, which is a torsion free $\mathbb{Z}_\ell$–module by Proposition 5.4.11. This shows that every torsion element of $H^1_S(k, \mathrm{T}_\ell M)$ comes from a unique element of $H^1(G, Z\otimes\mathbb{Z}_\ell)$ or say $H^1(k, Z\otimes\mathbb{Z}_\ell)$, and it remains to show that this element is then in $H^1_S(k, Z\otimes\mathbb{Z}_\ell)$. We consider for this the following diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(k, Z\otimes\mathbb{Z}_\ell) \arrow[r] \arrow[d] \arrow[dr, dashed, "\delta"] & H^1(k, \mathrm{T}_\ell M) \arrow[d] \\
& \prod H^1(k_v, Z\otimes\mathbb{Z}_\ell) \arrow[r] & \prod H^1(k_v, \mathrm{T}_\ell M)
\end{tikzcd}$$

The rows are induced by the triangle of Tate–modules associated with the short exact sequence of 1–motives

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

and in the top row we have used Corollary 3.3.15 which shows $H^0(k, \mathbb{T}_\ell[Y/Z \longrightarrow G]) = 0$. We have thus $(\ker\delta)_{\mathrm{tor}} \cong H^1_S(k, \mathrm{T}_\ell M)_{\mathrm{tor}}$ and we must show that every element of $\ker\delta$ maps already to zero in $H^1(k_v, Z\otimes\mathbb{Z}_\ell)$ for all $v\in S$, that is, $(\ker\delta)_{\mathrm{tor}} = H^1_S(k, Z\otimes\mathbb{Z}_\ell)$.
Fix an element x of $H^1_S(k, \mathrm{T}_\ell M)_{\mathrm{tor}}$, a place $v\in S$ and let D_v be a decomposition group for v. We know that x comes via inflation from an element $z\in H^1_*(L^M, \mathrm{T}_\ell M)_{\mathrm{tor}}$. Write D for the image of D_v in $\mathrm{GL}(\mathrm{T}_\ell M)$. 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 5.4.12 and the remark following it, 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 now the diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(\Gamma, Z\otimes\mathbb{Z}_\ell) \arrow[r] \arrow[d] \arrow[dr, dashed, "\delta'"] & H^1(\Gamma, \mathrm{T}_\ell M) \arrow[d] \\
0 \arrow[r] & H^1(\Gamma', Z\otimes\mathbb{Z}_\ell) \arrow[r] \arrow[d] & H^1(\Gamma', \mathrm{T}_\ell M) \arrow[d] \\
& H^1(D_v, Z\otimes\mathbb{Z}_\ell) \arrow[r] & H^1(D_v, \mathrm{T}_\ell M)
\end{tikzcd}$$

We know that the element $x\in H^1_S(k, \mathrm{T}_\ell M)$ comes from an element of $\ker\delta'$. The middle row is exact (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 $H^1(D_v, Z\otimes\mathbb{Z}_\ell)$. □

Lemma 5.5.5. *Let M be a 1–motive with torsion over k, such that $H^{-1}(M) = 0$. Then $H^1_S(k, \mathbb{T}_\ell M)$ is torsion free.*

Proof. We have shown this for torsion–free 1–motives in the previous lemma. Consider then the case of a 1–motive $M = [u : Y \longrightarrow G]$ where Y is free, but where G is no longer connected. Write G° for the connected component of G and Y° for the pull–back of Y to G°. This yields an exact sequence of 1–motives $0 \longrightarrow M^\circ \longrightarrow M \longrightarrow M' \longrightarrow 0$ given by

$$\begin{tikzcd}
0 \arrow[r] & Y^\circ \arrow[r] \arrow[d, "u^\circ"'] & Y \arrow[r] \arrow[d, "u"'] & Y' \arrow[r] \arrow[d, "u'"'] & 0 \\
0 \arrow[r] & G^\circ \arrow[r] & G \arrow[r] & G' \arrow[r] & 0
\end{tikzcd}$$

The map u is injective by hypothesis, hence u° and u'. The groups Y' and G' are finite, and M' is quasi–isomorphic to $[0 \longrightarrow G'/Y']$. This exact sequence yields then an exact triangle of Tate modules

$$\mathbb{T}_\ell M^\circ \longrightarrow \mathbb{T}_\ell M \longrightarrow \mathbb{T}_\ell M'$$

Observe that $\mathbb{T}_\ell M^\circ$ is concentrated in degree 0 and $\mathbb{T}_\ell M'$ is concentrated in degree 1, and that this triangle is nothing but the truncation triangle for the ℓ–adic complex $\mathbb{T}_\ell M$. The ℓ–adic sheaf $F := H^1(\mathbb{T}_\ell M')$ is just a finite group, equal to the ℓ–part of G'/Y'. Writing out the long exact cohomology sequences one finds a diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^1(k, \mathbb{T}_\ell M^\circ) \arrow[r] \arrow[d] & H^1(k, \mathbb{T}_\ell M) \arrow[r] \arrow[d] & H^0(k, F) \arrow[d] \\
0 \arrow[r] & \prod H^1(k_v, \mathbb{T}_\ell M^\circ) \arrow[r] & \prod H^1(k_v, \mathbb{T}_\ell M) \arrow[r] & \prod H^0(k_v, F)
\end{tikzcd}$$

the products running over $v \in S$. Because the rightmost vertical map is injective this yields an isomorphism $H^1_S(k, \mathbb{T}_\ell M^\circ) \cong H^1_S(k, \mathbb{T}_\ell M)$. Since M° is a torsion free 1–motive and u° injective, we know that $H^1_S(k, \mathbb{T}_\ell M^\circ)$ is torsion free, hence $H^1_S(k, \mathbb{T}_\ell M)$.

Finally, consider an arbitrary 1–motive with torsion $M = [u : Y \longrightarrow G]$ such that u is injective. The torsion part Y_{tor} of Y is finite, and injects to G. The 1–motive M is thus quasi–isomorphic to the 1–motive $M' := [Y/Y_{\mathrm{tor}} \longrightarrow G/Y_{\mathrm{tor}}]$. Hence $\mathbb{T}_\ell M$ is isomorphic to $\mathbb{T}_\ell M'$, and because Y/Y_{tor} is torsion free we already know that $H^1_S(k, \mathbb{T}_\ell M')$ is torsion free. This shows the lemma. □

Proof of Theorem 5.5.1. The $\mathbb{Z}_\ell$–rank of $H^1_S(k, \mathbb{T}_\ell M)$ is less or equal than the dimension of $H^1_*(\mathfrak{l}^{M'}, \mathrm{V}_\ell M')$ where M' is any torsion free 1–motive isogenous to M, which in turn can be bounded uniquely in terms of the dimension of $\mathrm{V}_\ell M'$. It remains to show the statement about the torsion subgroup of $H^1_S(k, \mathbb{T}_\ell M)$.

Write $M = [u : Y \longrightarrow G]$, set $Z := H^{-1}(M) = \ker u$ and $\overline{Y} := Y/Z$, so that we get a short exact sequence of 1–motives $0 \longrightarrow Z[1] \longrightarrow M \longrightarrow \overline{M} \longrightarrow 0$ given by

$$\begin{tikzcd}
0 \arrow[r] & Z \arrow[r] \arrow[d] & Y \arrow[r] \arrow[d, "u"'] & \overline{Y} \arrow[r] \arrow[d, "\overline{u}"'] & 0 \\
0 \arrow[r] & 0 \arrow[r] & G \arrow[r, equal] & G \arrow[r] & 0
\end{tikzcd}$$

The morphism $\overline{u}$ is injective, hence $H^1_S(k, \mathbb{T}_\ell \overline{M})_{\mathrm{tor}} = 0$ by Lemma 5.5.5. The associated long exact cohomology sequences yield the following diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(k, Z \otimes \mathbb{Z}_\ell) \arrow[r] \arrow[d] \arrow[dr, dashed, "\delta"] & H^1(k, \mathbb{T}_\ell M) \arrow[r] \arrow[d] & H^1(k, \mathbb{T}_\ell \overline{M}) \arrow[d] \\
\prod H^0(k_v, \mathbb{T}_\ell \overline{M}) \arrow[r] & \prod H^1(k_v, Z \otimes \mathbb{Z}_\ell) \arrow[r] & \prod H^1(k_v, \mathbb{T}_\ell M) \arrow[r] & \prod H^1(k_v, \mathbb{T}_\ell \overline{M})
\end{tikzcd}$$

the products running over $v \in S$. Because the rightmost vertical map is injective on torsion this yields an isomorphism

$$H^1_S(k, \mathbb{T}_\ell M)_{\mathrm{tor}} \cong (\ker \delta)_{\mathrm{tor}}$$

We must show that every torsion element of $\ker \delta$ maps already to zero in $H^1(k_v, Z \otimes \mathbb{Z}_\ell)$ for all $v \in S$. We have shown this for torsion–free 1–motives, and the general case follows then again considering the exact sequence $0 \longrightarrow M^\circ \longrightarrow M \longrightarrow M' \longrightarrow 0$ as in Lemma 5.5.4. Hence the (finite) kernel of the first vertical map gets identified with the torsion in the kernel of the second vertical map, that is

$$H^1_S(k, Z \otimes \mathbb{Z}_\ell) \xrightarrow{\cong} H^1_S(k, \mathbb{T}_\ell M)_{\mathrm{tor}}$$

Together with Lemma 5.5.3 this yields the claimed isomorphism, as well as the additional statement of the theorem. □

CHAPTER 6

The Tate property for 1–motives

In this chapter, we work over a number field k with a fixed algebraic closure $\overline{k}$. We fix also a prime number ℓ. We establish the Tate property for torsion free 1–motives announced in the introduction:

THEOREM 6.0.1. *The natural map* $\mathrm{Hom}_k(M_1, M_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_\Gamma(\mathrm{T}_\ell M_1, \mathrm{T}_\ell M_2)$ *is an isomorphism for all torsion free 1–motives* M_1 *and* M_2 *over* k. *In other words, the canonical functor*

$$\mathrm{T}_\ell : \quad \mathcal{M}_1^{\mathrm{Del}} \otimes \mathbb{Z}_\ell \quad \longrightarrow \quad \begin{Bmatrix} \mathbb{Z}_\ell\text{–}\textit{modules with} \\ \textit{continuous } \Gamma\text{–}\textit{action} \end{Bmatrix}$$

is fully faithful.

This theorem generalizes Faltings famous result on homomorphisms of abelian varieties over number fields. U.Jannsen informed me that he stated this theorem together with a sketch of a proof of in the 1994 ICM Proceedings ([**Jan94**], Theorem 4.3). As G.Wüstholz pointed out to me, the case of semiabelian varieties figures in the unpublished Ph.D. thesis of Y.Fengsheng [**Fen94**]. However, it seems that the proof given in *loc.cit.* contains a mistake.
We shall also prove a slightly more general version of this theorem that works for 1–motives with torsion, involving ℓ–adic complexes.

Convention: In the sequel we shall often write $\mathrm{T}_\ell Y$ for the Tate module of the 1–motive $[Y \longrightarrow 0]$. So in fact we have $\mathrm{T}_\ell Y = Y \otimes \mathbb{Z}_\ell$ as Γ–modules.

6.1. Deficient points

Before we come to the Tate conjecture, we need an auxiliary result on the so–called *deficient* points on a semiabelian variety. The following definition is due to K.Ribet and O.Jacquinot:

DEFINITION 6.1.1. Let G be a semiabelian variety over k, and denote by k_O the field obtained from the field k by adjoining to it all ℓ^n–torsion points of $G(\overline{k})$. Call a rational point $P \in G(k)$ *deficient* if it is ℓ–divisible in $G(k_O)$.

– 6.1.2. The deficient points form a subgroup of $G(k)$ which we denote by $D_G(k)$. We can see $D_G(k)$ as the kernel of the map $G(k) \longrightarrow G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$. It is a finitely generated subgroup of $G(k)$ which contains all rational torsion points but is in general strictly larger. For *split* semiabelian varieties however, equality $D_G(k) = G(k)_{\mathrm{tor}}$ holds, and this is what we show now.

PROPOSITION 6.1.3. *Let* G *be a split semiabelian variety. The kernel of the map* $G(k) \longrightarrow G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ *consists of the finitely many torsion points of* $G(k)$.

Proof. It is enough to show that the kernel of the map $G(k) \longrightarrow G(k_O) \widehat{\otimes} \mathbb{Z}_\ell$ is finite, because on one hand, this kernel contains obviously all torsion points of $G(k)$. Consider the following commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & K_n \arrow[r] \arrow[d, hook] & G(k)/\ell^n G(k) \arrow[r] \arrow[d, hook] & G(k_O)/\ell^n G(k_O) \arrow[d, hook] \\ 0 \arrow[r] & H^1(L^G, G[\ell^n]) \arrow[r] & H^1(k, G[\ell^n]) \arrow[r] & H^1(k_O, G[\ell^n]) \end{tikzcd}$$

The bottom row comes from the Hochschild–Serre spectral sequence associated to the extension $k_O|k$, and the injective vertical maps come from the Kummer sequence associated to the multiplication–by–ℓ^n map on G. We can take limits over $n \geq 0$. Because H^1 commutes with limits of finite modules ([**Ser64**], Proposition 7), the lower line gives the continuous cohomology of the Tate module of G. We get a commutative diagram of $\mathbb{Z}_\ell$–modules

$$\begin{tikzcd} 0 \arrow[r] & \lim K_n \arrow[r] \arrow[d, hook] & G(k) \widehat{\otimes} \mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & G(k_O) \widehat{\otimes} \mathbb{Z}_\ell \arrow[d, hook] \\ 0 \arrow[r] & H^1(L^G, \mathrm{T}_\ell G) \arrow[r] & H^1(k, \mathrm{T}_\ell G) \arrow[r] & H^1(k_O, \mathrm{T}_\ell G) \end{tikzcd}$$

By Corollary 5.3.4, the group $H^1(L^G, \mathrm{T}_\ell G)$ is finite. This implies that the limit of the K_n, i.e. the kernel of the morphism $G(k) \widehat{\otimes} \mathbb{Z}_\ell \longrightarrow G(k_O) \widehat{\otimes} \mathbb{Z}_\ell$ is a finite ℓ–group. The kernel of $G(k) \longrightarrow G(k) \widehat{\otimes} \mathbb{Z}_\ell$ consists of the torsion elements of $G(k)$ of order prime to ℓ, so that the kernel of the composite $G(k) \longrightarrow G(k_O) \widehat{\otimes} \mathbb{Z}_\ell$ is indeed a finite subgroup of $G(k)$. $\square$

Remark 6.1.4. Considering Corollary 5.3.4, we have shown that for split semiabelian varieties there is a canonical isomorphism $D_G(k) \otimes \mathbb{Z}_\ell \cong H^1(L^G, \mathrm{T}_\ell G)$. This holds in fact for general semiabelian varieties.

6.2. Injectivity of Abel–Jacobi maps

In order to prove theorem 6.0.1, it is enough to prove that for all torsion free 1–motives M over k, the Tate map

$$\tau_\ell : \mathrm{End}_k M \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{End}_\Gamma \mathrm{T}_\ell M$$

is an isomorphism. Like so often, the hard part is surjectivity. When one tries to prove theorem 6.0.1 by naïve dévissage along the weight filtration, one immediately faces the problem that surjectivity of the map τ_ℓ follows from injectivity of maps of the type

$$\alpha_\ell : \mathrm{Ext}^1_k(M_1, M_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell M_1, \mathrm{T}_\ell M_2)$$

where M_1 and M_2 are some graded pieces of M. Following [**Jan94**], we call these maps *Abel–Jacobi maps*, and their injectivity is what we will provide in this section. The most interesting, and also most difficult case is when M_1 is a lattice, say $M_1 = [\mathbb{Z} \longrightarrow 0]$, and when $M_2 = [0 \longrightarrow G]$ is a semiabelian variety. We have then $\mathrm{Ext}^1(M_1, M_2) = G(k)$ and so the map α_ℓ becomes

$$\alpha_\ell : G(k) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$$

As we shall see (Proposition 6.2.1), it is easy to show that the map $\alpha : G(k) \longrightarrow \mathrm{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is injective up to torsion points of order prime to ℓ. The difficulty lies in showing that this map remains injective when we tensor with $\mathbb{Z}_\ell$ on the left.

PROPOSITION 6.2.1. *Let G be a semiabelian variety over k. The kernel of the natural map*

$$\rho : G(k) \longrightarrow \mathrm{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$$

consists of the torsion points of $G(k)$ of order prime to ℓ.

PROOF. Let $P \in \ker\rho \subseteq G(k)$, write $M = [u : \mathbb{Z} \longrightarrow G]$ where $u(1) = P$, and choose a Γ–module splitting $\sigma : \mathbb{Z}_\ell \longrightarrow \mathrm{T}_\ell M$ of the projection $\pi : \mathrm{T}_\ell M \longrightarrow \mathbb{Z}_\ell$. Such a splitting σ is entirely described by $\mathbb{Z}_\ell$–linearity and the point $\sigma(1) \in \mathrm{T}_\ell M^\Gamma$. By Corollary 3.3.15, we know that

$$\sigma(1) \in \ker u \otimes \mathbb{Z}_\ell = \mathrm{T}_\ell M^\Gamma$$

To say that $\pi\sigma = \mathrm{id}$ is to say that the map $\ker u \otimes \mathbb{Z}_\ell \longrightarrow \mathbb{Z} \otimes \mathbb{Z}_\ell$ is an isomorphism. This means that $\ker u$ is of finite index prime to ℓ in $\mathbb{Z}$, hence that P is a torsion point of order prime to ℓ. $\square$

– 6.2.2. Define the field k_O by adjoining to k the coordinates of all ℓ–torsion points of G. For a rational point $Q \in G(k)$, we set

$$h_\ell(Q) := \sup\{n \in \mathbb{N} \mid Q \in \ell^n G(k_O)\} \qquad \in \{0, 1, 2, \dots, \infty\}$$

By definition, $h_\ell(Q)$ is infinite if and only if Q is deficient. Recall that for a 1–motive M over k, the group L^M is the image of Γ in $\mathrm{GL}(\mathrm{T}_\ell M)$, and L^M_G is the subgroup of L^M consisting of those elements which act trivially on the subspace $\mathrm{T}_\ell G$ of $\mathrm{T}_\ell M$.

LEMMA 6.2.3. *Let $P \in G(k)$ be a rational point, and define $M = [u : \mathbb{Z} \longrightarrow G]$ by $u(1) = P$. If the image of the Kummer injection $\vartheta : L^M_G \longrightarrow \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is contained in $\ell^n \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ then $h_\ell(G) \geq n$.*

PROOF. Choose any point $R \in G(\overline{k})$ such that $\ell^n R = P$. The composite map

$$L^M_G \xrightarrow{\vartheta} \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G) \longrightarrow \mathrm{Hom}(\mathbb{Z}_\ell, G[\ell^n]) \cong G[\ell^n]$$

sends the class of $g \in \mathrm{Gal}(\overline{k}|k_O)$ to $gR - R$. But to say that the image of $\vartheta : L^M_G \longrightarrow \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is contained in $\ell^n \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is precisely to say that the above composition is zero. Thus we have $R \in G(k_O)$, and thus indeed $h_\ell(P) \geq n$. $\square$

LEMMA 6.2.4. *Let X be a finitely generated subgroup of $G(k)$. There exists an integer $c \geq 0$ depending on k, G and X, with the following property:*
Let $P \in X$ be a point, and let $M = [u : \mathbb{Z} \longrightarrow G]$ be the 1–motive over k defined by $u(1) = P$. If the image of the Kummer injection $\vartheta : L^M_G \longrightarrow \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is contained in $\ell^{n+c} \mathrm{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ then there exists a deficient point $D \in D_G(k) \cap X$ such that $P + D \in \ell^n X$.

PROOF. Since X is a finitely generated group, we can identify $X \otimes_\mathbb{Z} \mathbb{Z}_\ell = X \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$. We consider the canonical map $\alpha : X \otimes \mathbb{Z}_\ell \longrightarrow G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$, and write

$$\mathrm{im}\,\alpha \;\subseteq\; \overline{\mathrm{im}\,\alpha} := \{x \in G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \mid \ell^n x \in \mathrm{im}\,\alpha \text{ for some } n \geq 0\}$$

We claim that the index of $\mathrm{im}\,\alpha$ in $\overline{\mathrm{im}\,\alpha}$ is finite. Indeed, since the ℓ–torsion subgroup of $G(k_O)$ is divisible, $G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ is a torsion free $\mathbb{Z}_\ell$–module. Hence, if $b_1, \dots, b_r$ is a $\mathbb{Z}_\ell$–basis of $\mathrm{im}\,\alpha$, every element of $\overline{\mathrm{im}\,\alpha}$ can be written in a unique fashion as $\lambda_1 b_1 + \cdots + \lambda_r b_r$ for some $\lambda = (\lambda_1, \dots, \lambda_r) \in \mathbb{Q}_\ell^r$. Let $\Lambda \subseteq \mathbb{Q}_\ell^r$ be the set of all λ's occurring. This Λ is a $\mathbb{Z}_\ell$–submodule of $\mathbb{Q}_\ell^r$, containing $\mathbb{Z}_\ell^r \subseteq \Lambda$ as an open submodule, hence is open. Since $G(k_O) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ contains no divisible elements, Λ contains no nontrivial $\mathbb{Q}_\ell$–linear subspace. An open $\mathbb{Z}_\ell$–submodule of a finite dimensional $\mathbb{Q}_\ell$–vector space is compact if and only if it contains no nontrivial $\mathbb{Q}_\ell$–linear subspace ([**Wei67**], II.2, Corollary 1). Hence Λ is compact, and the quotient $\Lambda/\mathbb{Z}_\ell^r \cong \overline{\mathrm{im}\,\alpha}/\mathrm{im}\,\alpha$ is finite.

Let ℓ^c be this index. Now we check that the constant c has the required property. Consider the following diagram:

$$\begin{tikzcd} X \arrow[r, "\subseteq"] \arrow[d, "\varepsilon"'] & G(k_O) \arrow[d, "\varepsilon_O"] \\ X \otimes \mathbb{Z}_\ell \arrow[r, "\alpha"] & G(k_O) \,\widehat{\otimes}\, \mathbb{Z}_\ell \end{tikzcd}$$

If $P \in X$ satisfies the hypothesis of the lemma, then we have also $h_\ell(P) \geq \ell^{n+c}$ by Lemma 6.2.3. So there exists a $Q \in G(k_O)$ such that $\ell^{n+c}Q = P$. It follows that $\alpha\varepsilon P = \ell^{n+c}\varepsilon_O Q$, whence $Q \in \overline{\operatorname{im}\alpha}$. By definition of c we have $\ell^c Q \in \operatorname{im}\alpha$, i.e. there exists $R \in X \otimes \mathbb{Z}_\ell$ such that $\alpha R = \ell^c \varepsilon_O Q$. In other words, $\alpha(\varepsilon P - \ell^n R) = 0$. The kernel of $\alpha\varepsilon$ consists of the deficient points of G contained in X, so that $\ker\alpha = (D_G(k) \cap X) \otimes \mathbb{Z}_\ell$. Hence there is $D \in (D_G(k) \cap X) \otimes \mathbb{Z}_\ell$ such that

$$\varepsilon(P + D) = \ell^n R \quad \in \ell^n(X \otimes \mathbb{Z}_\ell)$$

Replacing $D \in (D_G(k) \cap X) \otimes \mathbb{Z}_\ell$ by an element of $D_G(k) \cap X$ congruent to D mod ℓ^n yields the lemma. □

Proposition 6.2.5. *Let G be a semiabelian variety over k. The Abel–Jacobi map*

$$\rho_\ell : G(k) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$$

is injective.

Proof. It is enough to prove this in the case where G is either an abelian variety or a torus. Indeed, the following diagram with exact rows shows that injectivity of ρ_ℓ follows from injectivity of the corresponding Abel–Jacobi maps for A and T

$$\begin{tikzcd} 0 \arrow[r] & T(k) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d] & G(k) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\rho_\ell"'] & A(k) \otimes \mathbb{Z}_\ell \arrow[d] \\ (\mathrm{T}_\ell A)^\Gamma = 0 \arrow[r] & \operatorname{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell T) \arrow[r] & \operatorname{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell G) \arrow[r] & \operatorname{Ext}^1_\Gamma(\mathbb{Z}_\ell, \mathrm{T}_\ell A) \end{tikzcd}$$

In particular, regarding Theorem 5.3.1 it is enough to prove the proposition under the additional hypothesis that $H^1(\mathrm{I}^G, \mathrm{V}_\ell G) = 0$, so that by Proposition 6.1.3 all deficient points of G are torsion. We suppose this from now on.

Fix an element $x \in \ker\rho_\ell$ and let us show that $x = 0$. Choose $\mathbb{Z}$–linearly independent rational points $P_1, \ldots, P_N \in G(k)$ and ℓ–adic integers $\lambda_1, \ldots, \lambda_N \in \mathbb{Z}_\ell$ and an ℓ–torsion point $T \in G(k)$ such that

$$x = T \otimes 1 \; + \; \sum_{i=1}^N P_i \otimes \lambda_i$$

Let $X \leq G(k)$ be a finitely generated subgroup containing T and all P_i's. Let $c \geq 0$ be an integer as provided by Lemma 6.2.4, and let $n \geq 1$ be an integer. Choose integers $a_1, \ldots, a_N$ and ℓ–adic integers $\mu_1, \ldots, \mu_N$ such that

$$\lambda_i = a_i - \ell^{n+c}\mu_i \qquad\qquad i = 1, 2, \ldots, N$$

We can write $x = P \otimes 1 \; - \ell^{n+c}y$, where $P := T + a_1P_1 + \cdots + a_NP_N$, and $y = P_1 \otimes \mu_1 + \cdots + P_N \otimes \mu_N$. Because $\rho_\ell(x) = 0$, this yields the equality $\rho(P) = \ell^{n+c}\rho_\ell(y)$ which in terms of extensions corresponds to a diagram of Γ–modules

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{T}_\ell G \arrow[r] \arrow[d, "\cdot\ell^{n+c}"'] & E \arrow[r] \arrow[d] & \mathbb{Z}_\ell \arrow[r] \arrow[d, equal] & 0 & \rho_\ell(y) \\ 0 \arrow[r] & \mathrm{T}_\ell G \arrow[r] & \mathrm{T}_\ell M \arrow[r] & \mathbb{Z}_\ell \arrow[r] & 0 & \rho(P) \end{tikzcd}$$

where $M = [u : \mathbb{Z} \longrightarrow G]$ is given by $u(1) = P$. This diagram shows that the image of the corresponding Kummer injection $\vartheta : L_G^M \longrightarrow \operatorname{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$ is contained in $\ell^{n+c}\operatorname{Hom}(\mathbb{Z}_\ell, \mathrm{T}_\ell G)$. By Lemma 6.2.4, this implies that $P = \ell^n R + D$ for a rational point $R \in G(k)$ and a deficient point $D \in D_G(k)$. By our additional hypothesis, D is torsion. Thus, we find

$$x = P \otimes 1 \, - \ell^{n+c} y = D + \ell^n(R - \ell^c y) \in G(k)_{\mathrm{tor}} + \ell^n(G(U) \otimes \mathbb{Z}_\ell)$$

But n was arbitrary, hence $x \in G(k)_{\mathrm{tor}} \otimes \mathbb{Z}_\ell$. So we can write $x = T \otimes 1$ for an ℓ–torsion point T of $G(k)$, and have $0 = \rho_\ell(x) = \rho_\ell(T \otimes 1) = \rho(T)$. This implies that $T = O$ and hence $x = 0$ because ρ is injective on ℓ–torsion points by Proposition 6.2.1. □

Proposition 6.2.6. *Let Y be a lattice and G be a semiabelian variety over k. Let T be a torus and M_A be a 1–motive without toric part over k. The Abel–Jacobi maps*

$$\operatorname{Hom}_k(Y, G) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Ext}^1_\Gamma(\mathrm{T}_\ell Y, \mathrm{T}_\ell G) \qquad \textit{and} \qquad \operatorname{Ext}^1_k(M_A, T) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Ext}^1_\Gamma(\mathrm{T}_\ell M_A, \mathrm{T}_\ell T)$$

are injective.

Proof. By additivity, Proposition 6.2.1 shows the first injectivity in the case where Y has trivial Galois action. For general Y, choose an extension $k'|k$ that trivializes Y. The diagram

$$\begin{array}{ccc} \operatorname{Hom}_k(Y, G) \otimes \mathbb{Z}_\ell & \longrightarrow & \operatorname{Ext}^1_k(\mathrm{T}_\ell Y, \mathrm{T}_\ell A) \\ \downarrow & & \downarrow \\ \operatorname{Hom}_{k'}(Y, G) \otimes \mathbb{Z}_\ell & \longrightarrow & \operatorname{Ext}^1_{k'}(\mathrm{T}_\ell Y, \mathrm{T}_\ell A) \end{array}$$

commutes, and the lower horizontal map and the left vertical map are injective, and hence also the top horizontal map. In order to show the second injectivity write $Y^\vee$ for the character group of the torus T, and $G^\vee$ for the semiabelian variety dual to M_A. Then we can use the diagram

$$\begin{array}{ccc} \operatorname{Hom}_k(Y^\vee, G^\vee) \otimes \mathbb{Z}_\ell & \longrightarrow & \operatorname{Ext}^1_k(\mathrm{T}_\ell Y^\vee, \mathrm{T}_\ell G^\vee) \\ \cong\downarrow & & \downarrow\cong \\ \operatorname{Ext}^1_k(M_A, T) \otimes \mathbb{Z}_\ell & \longrightarrow & \operatorname{Ext}^1_{k'}(\mathrm{T}_\ell M_A, \mathrm{T}_\ell T) \end{array}$$

The left hand isomorphism is given by the Barsotti–Weil formula 1.2.3, and the right hand isomorphism by the Weil pairing. Commutativity is not hard to check. □

Proposition 6.2.7. *Let A and B be abelian varieties over k. The kernels of the natural maps*

$$Ext^1_k(B, A) \longrightarrow \operatorname{Ext}^1_k(\mathrm{T}_\ell B, \mathrm{T}_\ell A)$$

consist of the torsion elements of order prime to ℓ. The same holds for tori in place of A and B or for lattices.

Proof. By a theorem of Milne and Ramachandran ([**PR05**], Theorem 2), the group of extensions $\operatorname{Ext}^1_k(B, A)$ is finite, and since $\operatorname{Ext}^1_\Gamma(\mathrm{T}_\ell B, \mathrm{T}_\ell A)$ is a $\mathbb{Z}_\ell$–module, it is clear that elements of order prime to ℓ are mapped to zero. What we have to show is that the map is injective on the ℓ–torsion part. Fix an element of order ℓ in $\operatorname{Ext}^1_k(B, A)$. We may represent it by a short exact sequence of group schemes, giving rise to an exact sequence of Tate modules

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} B \longrightarrow 0 \qquad 0 \longrightarrow \mathrm{T}_\ell A \xrightarrow{\iota} \mathrm{T}_\ell E \xrightarrow{\pi} \mathrm{T}_\ell B \longrightarrow 0$$

Suppose that the sequence of Tate modules splits, i.e. there exists a Γ–module morphism $\tau : \mathrm{T}_\ell B \longrightarrow \mathrm{T}_\ell E$ such that $\pi\tau = \mathrm{id}_{\mathrm{T}_\ell B}$. We must show that the sequence of abelian varieties splits as well.
To say that the sequence of abelian varieties represents an element of order ℓ in $\operatorname{Ext}^1_k(B, A)$ is to

say that there exist a morphism $s : B \longrightarrow E$ such that $ps = \ell\,\mathrm{id}_B$. Because $\pi(\mathrm{T}_\ell s - \ell\tau) = 0$, there exists a Γ–module morphism $\alpha : \mathrm{T}_\ell B \longrightarrow \mathrm{T}_\ell A$ such that $\iota\alpha = \mathrm{T}_\ell s - \ell\tau$.
Let $f_1, \ldots, f_N$ be a $\mathbb{Z}$–basis of $\mathrm{Hom}_k(B, A)$. Identifying $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell B, \mathrm{T}_\ell A)$ with $\mathrm{Hom}_k(B, A) \otimes \mathbb{Z}_\ell$ via Faltings theorem, we can represent α as $\alpha = f_1 \otimes \lambda_1 + \cdots + f_N \otimes \lambda_N$, where $\lambda_i \in \mathbb{Z}_\ell$. Writing $\lambda_i = n_i + \ell\mu_i$ where the n_i are integers and $\mu_i \in \mathbb{Z}_\ell$, we get

$$\alpha = \mathrm{T}_\ell f + \ell\alpha' \qquad \text{for} \quad f := \sum n_i f_i \qquad \alpha' := \sum f_i \otimes \mu_i$$

Set $s' := s - if$ and $\tau' := \tau + \iota\alpha'$. Then, $ps' = \ell\,\mathrm{id}_B$ and $\pi\tau' = \mathrm{id}_{\mathrm{T}_\ell B}$ and moreover we have by construction $\ell\tau' = \mathrm{T}_\ell s'$.
Now, let $g_1, \ldots, g_M$ be a $\mathbb{Z}$–basis of $\mathrm{Hom}(B, E)$. Identifying $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell B, \mathrm{T}_\ell A)$ with $\mathrm{Hom}_k(B, A) \otimes \mathbb{Z}_\ell$, there are unique integers m_i and unique $\kappa_i \in \mathbb{Z}_\ell$ such that

$$\tau' = \sum g_i \otimes \kappa_i \qquad \text{and} \qquad \mathrm{T}_\ell s' = \sum g_i \otimes m_i$$

By uniqueness and because $\ell\tau' = \mathrm{T}_\ell s'$, we must have $\ell\kappa_i = m_i$. From this, it follows that the κ_i are in fact integers, and that $\tau' = \mathrm{T}_\ell h$ for $h := \kappa_1 g_1 + \cdots + \kappa_M g_M$. We are done, since $\mathrm{T}_\ell(ph) = \pi\tau' = \mathrm{id}_{\mathrm{T}_\ell B} = \mathrm{T}_\ell(\mathrm{id}_B)$, so that $ph = \mathrm{id}_B$.
The case of tori or lattices is completely analogous, noting that finiteness of $\mathrm{Ext}^1_k(-,-)$ follows from the Hochschild–Serre spectral sequence. □

Corollary 6.2.8. *Let A and B be abelian varieties over k. The Abel–Jacobi map*

$$\mathrm{Ext}^1_k(B, A) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Ext}^1_k(\mathrm{T}_\ell B, \mathrm{T}_\ell A)$$

is injective. The analogous statements for tori or for lattices hold as well.

Proof. Indeed, since $\mathrm{Ext}^1_k(B, A)$ is finite, $\mathrm{Ext}^1_k(B, A) \otimes \mathbb{Z}_\ell$ is canonically isomorphic to the ℓ–torsion part of $\mathrm{Ext}^1_k(B, A)$, so the claim follows from 6.2.7. The same goes for tori and lattices. □

6.3. The Tate property

This will be a dévissage orgy. In order not to loose track of what we are doing, we will in a first step prove the Tate property for semiabelian varieties (Lemma 6.3.2), and then for general torsion free 1–motives. We begin with the trivial cases

Proposition 6.3.1. *Let Y be a lattice, T be a torus and A be an abelian variety over k. The groups*

$$\mathrm{Hom}_k(A, T) \qquad \mathrm{Hom}_k(T, A) \qquad \mathrm{Hom}_k(A, Y) \qquad \mathrm{Ext}^1_k(T, A)$$

are all trivial. Between any two out of the three Tate modules $\mathrm{T}_\ell T$, $\mathrm{T}_\ell A$ and $\mathrm{T}_\ell Y$, there are no nontrivial Γ–module morphisms.

Proof. First, $\mathrm{Hom}_k(A, T)$ is trivial because A is a proper and connected variety, and T is affine, and every morphism from a proper to an affine variety is locally constant. Likewise, also T is connected, and every morphism from an affine group scheme to a proper one is locally constant. That $\mathrm{Hom}_k(A, Y)$ is trivial is clear since $A(\overline{k})$ is divisible. Finally, let $Y^\vee$ be the character group of T, so that $T = \mathcal{H}om(Y, \mathbb{G}_m)$. We find

$$\mathrm{Ext}^1_k(T, A) \cong \mathrm{Ext}^1(\mathcal{H}om_k(Y, \mathbb{G}_m), \mathcal{E}xt^1_k(A^\vee, \mathbb{G}_m)) \cong \mathrm{Hom}_k(A^\vee, Y) = 0$$

That the given homomorphism sets between Tate modules are trivial can be seen in several ways. Suppose without loss of generality that T is split and that Y is constant. Choose a place v of

k with residue field κ_v of characteristic $p \neq \ell$, such that A has good reduction in v, and choose a Frobenius element $F_v \in \Gamma$ for this place. The eigenvalues of F_v on $\mathrm{T}_\ell T$, $\mathrm{T}_\ell A$ and $\mathrm{T}_\ell Y$ are of absolute value $\#\kappa_v, (\#\kappa_v)^{1/2}$ and 1 in any complex embedding. Thus, for example, F_v acting on $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell T, \mathrm{T}_\ell A)$ has eigenvalues of absolute value $(\#\kappa_v)^{-1/2} \neq 1$, and can thus not have any nontrivial fixed point. Alternative: Pass to Lie algebras and use Bogomolov's theorem. $\square$

Lemma 6.3.2. *Let G_1 and G_2 be semiabelian varieties over k, and consider the canonical maps*

$$\mathrm{Hom}_k(G_1, G_2) \otimes \mathbb{Z}_\ell \xrightarrow{\tau_\ell} \mathrm{Hom}_\Gamma(\mathrm{T}_\ell G_1, \mathrm{T}_\ell G_2) \quad \text{and} \quad \mathrm{Ext}^1_k(G_1, G_2) \otimes \mathbb{Z}_\ell \xrightarrow{\alpha_\ell} \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell G_1, \mathrm{T}_\ell G_2)$$

The Tate map τ_ℓ is an isomorphism, and the Abel–Jacobi map α_ℓ is injective.

Proof. Write $G := G_1 \times G_2$, and write T and A for the toric part, respectively the abelian quotient of G. By additivity, it is enough to prove that of the canonical maps

$$\mathrm{End}_k(G) \otimes \mathbb{Z}_\ell \xrightarrow{\tau_\ell} \mathrm{End}_\Gamma(\mathrm{T}_\ell G) \qquad \text{and} \qquad \mathrm{Ext}^1_k(G, G) \otimes \mathbb{Z}_\ell \xrightarrow{\alpha_\ell} \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell G, \mathrm{T}_\ell G)$$

τ_ℓ is an isomorphism, and α_ℓ is injective. This goes by dull dévissage. In order to show that α_ℓ is an isomorphism, consider the diagram with exact rows

$$\begin{tikzcd}
\mathrm{Hom}_k(A,T) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Hom}_k(A,G) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "(1)"'] & \mathrm{End}_k A \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & \mathrm{Ext}^1_k(A,T) \otimes \mathbb{Z}_\ell \arrow[d] \\
\mathrm{Hom}_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell T) \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell G) \arrow[r] & \mathrm{End}_\Gamma \mathrm{T}_\ell A \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell T)
\end{tikzcd}$$

The groups $\mathrm{Hom}_k(A,T)$ and $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell T)$ are both zero. The rightmost vertical map is injective by proposition 6.2.6 and the second one from the right is an isomorphism by the Tate property for abelian varieties proven by Faltings. This shows that the map (1) is an isomorphism. Next, we consider the similar diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{End}_k T \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & \mathrm{Hom}_k(T,G) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "(2)"'] & \mathrm{Hom}_k(T,A) \otimes \mathbb{Z}_\ell \arrow[d] \\
0 \arrow[r] & \mathrm{End}_\Gamma \mathrm{T}_\ell T \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell T, \mathrm{T}_\ell G) \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell T, \mathrm{T}_\ell A)
\end{tikzcd}$$

Because $\mathrm{Hom}_k(T,A)$ and $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell T, \mathrm{T}_\ell A)$ are both zero, the map (2) is an isomorphism. Now we look at the diagram

$$\begin{tikzcd}
\mathrm{End}_k A \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\cong"'] & \mathrm{Ext}^1_k(A,T) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Ext}^1_k(A,G) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "(3)"'] & \mathrm{Ext}^1_k(A,A) \otimes \mathbb{Z}_\ell \arrow[d] \\
\mathrm{Hom}_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell A) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell T) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell A)
\end{tikzcd}$$

The first vertical map from the left is an isomorphism by Faltings, and the second one is injective by 6.2.6. By Corollary 6.2.8, the rightmost vertical map is injective. This shows that the map (3) is injective as well. Finally, we can put together what we have shown so far in one diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_k(A,G) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "(1)"'] & \mathrm{End}_k G \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\tau_\ell"'] & \mathrm{Hom}_k(T,G) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "(2)"'] & \mathrm{Ext}^1_k(A,G) \otimes \mathbb{Z}_\ell \arrow[d, "(3)"'] \\
0 \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell G) \arrow[r] & \mathrm{End}_\Gamma \mathrm{T}_\ell G \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell T, \mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell A, \mathrm{T}_\ell G)
\end{tikzcd}$$

Here, the maps labeled with (1) and (2) are isomorphisms, and (3) is injective. Thus, by the five–lemma, the map τ_ℓ is an isomorphism as well. Now we come to injectivity of α_ℓ. We start with the diagram

$$\begin{tikzcd}
\mathrm{Hom}_k(T,A)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Ext}^1_k(T,T)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Ext}^1_k(T,G)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(4)"'] & \mathrm{Ext}^1_k(T,A)\otimes\mathbb{Z}_\ell \arrow[d] \\
\mathrm{Hom}_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell A) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell T) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell A)
\end{tikzcd}$$

Here, $\mathrm{Hom}_k(T,A)$, $\mathrm{Ext}^1_k(T,A)$ and $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell A)$ are all trivial, and the second vertical map from the left is injective by 6.2.8. Therefore, the map (4) is injective. Now, consider

$$\begin{tikzcd}
\mathrm{Hom}_k(T,G)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(2)"'] & \mathrm{Ext}^1_k(A,G)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(3)"'] & \mathrm{Ext}^1_k(G,G)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "\alpha_\ell"'] & \mathrm{Ext}^1_k(T,G)\otimes\mathbb{Z}_\ell \arrow[d, "(4)"'] \\
\mathrm{Hom}_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell G) \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell A,\mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell G,\mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell T,\mathrm{T}_\ell G)
\end{tikzcd}$$

The map (2) is an isomorphism, and (3) and (4) are injective. This shows injectivity of α_ℓ. □

Proof of Theorem 6.0.1. Again we have just to consider the 1–motive $M := M_1 \times M_2$. We begin with the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_k(Y[1],M)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(5)"'] & \mathrm{End}_k\,Y\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Hom}_k(Y,G)\otimes\mathbb{Z}_\ell \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}_k(\mathrm{T}_\ell Y,\mathrm{T}_\ell M) \arrow[r] & \mathrm{End}_\Gamma\,\mathrm{T}_\ell Y \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell G)
\end{tikzcd}$$

The middle vertical map is an isomorphism, and the vertical map on the right is injective by Proposition 6.2.6. Hence (5) is an isomorphism. We go on with the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{End}_k\,G\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Hom}_k(G,M)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(6)"'] & \mathrm{Ext}^1_k(G,Y)\otimes\mathbb{Z}_\ell \arrow[d] \\
0 \arrow[r] & \mathrm{End}_\Gamma\,\mathrm{T}_\ell G \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell G,\mathrm{T}_\ell M) \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell G,\mathrm{T}_\ell Y)
\end{tikzcd}$$

The groups $\mathrm{Ext}^1_k(G,Y)$ and $\mathrm{Hom}_\Gamma(\mathrm{T}_\ell G,\mathrm{T}_\ell Y)$ are trivial, hence (6) is an isomorphism by Lemma 6.3.2, which established the Tate property for semiabelian varieties. We continue with

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Hom}_k(Y,G)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & \mathrm{Hom}_k(Y,M)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(7)"'] & \mathrm{Ext}^1_k(Y,Y)\otimes\mathbb{Z}_\ell \arrow[d] \\
\cdots \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell G) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell M) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell Y)
\end{tikzcd}$$

The first and third vertical maps are injective by Proposition 6.2.6 and Corollary 6.2.8 respectively. Hence (7) is injective. Now we can put together what we have in a last diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_k(Y[1],M)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(5)"'] & \mathrm{End}_k\,M\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "\tau_\ell"'] & \mathrm{Hom}_k(G,M)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "(6)"'] & \mathrm{Hom}_k(Y,M) \arrow[d, "(7)"'] \\
0 \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell M) \arrow[r] & \mathrm{End}_\Gamma\,\mathrm{T}_\ell M \arrow[r] & \mathrm{Hom}_\Gamma(\mathrm{T}_\ell G,\mathrm{T}_\ell M) \arrow[r] & \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell Y,\mathrm{T}_\ell M)
\end{tikzcd}$$

The morphisms (5) and (6) are isomorphisms, and (7) is injective. Hence, the Tate map τ_ℓ is an isomorphism by the five lemma. □

Proposition 6.3.3. *Let M_1 and M_2 be 1–motives over k. The Abel–Jacobi map*

$$\mathrm{Ext}^1_k(M_1,M_2)\otimes\mathbb{Z}_\ell \longrightarrow \mathrm{Ext}^1_\Gamma(\mathrm{T}_\ell M_1,\mathrm{T}_\ell M_2)$$

is injective

Proof. Two more rows of dévissage. □

6.4. 1–motives with torsion

Let $\mathcal{D}_\ell$ be the *derived category of ℓ–adic sheaves on k* introduced in Section 2.1, Definition 2.1.8. Recall that objects of $\mathcal{D}_\ell$ are ℓ–adic complexes, that is, limit systems $(F_i)_{i=0}^\infty$ in the derived category $\mathcal{DF}_k$ which are uniformly bounded in length and such that for each $r \in \mathbb{Z}$ the limit system $H^r(F_i)_{i=0}^\infty$ is an ℓ–adic sheaf on k.

THEOREM 6.4.1. *The canonical functor $\mathbb{T}_\ell : [\mathcal{M}_1] \otimes \mathbb{Z}_\ell \longrightarrow \mathcal{D}_\ell$ is fully faithful.*

– 6.4.2. By Proposition 1.1.8, the functor $[-] : \mathcal{M}_1^{\mathrm{Del}} \longrightarrow [\mathcal{M}_1]$ is fully faithful, hence the induced functor $\mathcal{M}_1^{\mathrm{Del}} \otimes \mathbb{Z}_\ell \longrightarrow [\mathcal{M}_1] \otimes \mathbb{Z}_\ell$. Theorem 6.0.1 shows thus that the functor

$$\mathbb{T}_\ell : \mathcal{M}_1^{\mathrm{Del}} \otimes \mathbb{Z}_\ell \longrightarrow \mathcal{D}_\ell$$

is fully faithful. Its image consists of ℓ–adic complexes whose homology is torsion free and concentrated in degree 0 only. These are just finitely generated free $\mathbb{Z}_\ell$–modules with continuous Γ–action. Hence, the Tate property for torsion free 1–motives is an immediate consequence of Theorem 6.4.1 and Proposition 1.1.8.

PROOF (SKETCH). The proof of Theorem 6.4.1 proceeds again in two steps. First, one shows that the statement holds for finite group schemes, and that moreover the corresponding Abel–Jacobi maps are injective. Then, the conclusion is made by dévissage, using the already proven case of torsion free 1–motives.
The first step is immediate. Indeed, let F_1 and F_2 be finite group schemes on k (or complexes of such for that matter). The ℓ–adic Tate module of F_i is just the ℓ–torsion part of F_i shifted one degree to the right, so the "Tate property" for finite group schemes means only that the following map is an isomorphism

$$\mathrm{Hom}_k(F_1, F_2) \otimes \mathbb{Z}_\ell \xrightarrow{\cong} \mathrm{Hom}_k(F_1[\ell^\infty], F_2[\ell^\infty])$$

and that is banal. The Abel-Jacobi map is injective, and even an isomorphism for the same reason. The various other cases involving a finite group scheme and some other graded piece for a 1–motive follow from this. For example if F_1 is a finite group scheme of order n and G a semiabelian variety over k, then $\mathrm{Hom}_k(F_1, G) \cong \mathrm{Hom}_k(F_1, G[n])$, where $G[n]$ is the n–torsion of G. One gets

$$\mathrm{Hom}_{\mathcal{D}_\ell}(\mathbb{T}_\ell F, \mathbb{T}_\ell G) = \mathrm{Hom}_k(F[\ell^\infty], \mathrm{T}_\ell G/n\mathrm{T}_\ell G) = \mathrm{Hom}_k\left(F[\ell^\infty], (G[n])[\ell^\infty]\right)$$

because the homology of $\mathbb{T}_\ell F$ is in degree 1, and the homology of $\mathbb{T}_\ell G$ is torsion free and in degree 0. The same works for extensions again. The dévissage step itself is then quite dull. □

CHAPTER 7

Dividing points

The main theme of this chapter is the problem of *dividing points* on semiabelian varieties. It is the following Kummer–theoretic problem: Let G be a geometrically connected algebraic group over a field k, let $X \leq G(k)$ be a subset of the group of k–rational points of G and let ℓ be a prime number. We consider the field k_X obtained from k by adjoining the "coordinates" of all algebraic points $R \in G(\overline{k})$ such that $\ell^n R \in X$ for some $n \geq 0$. The question is: How far does the field k_X characterize the set X? And what are the properties of the group $G(k_X)$?

In the first section, we prove the algebraicity theorem stated in the introduction (Theorem 7.1.3), and apply it in section 7.2 to answer to some extent the above questions (Theorem 7.2.2). In section 7.3 we use our algebraicity theorem to compute $H^1_*(L^M, \mathrm{T}_\ell M)$ under some technical assumptions on M. In a last we present a few reasonable conditions under which the group $H^1_*(L^M, \mathrm{T}_\ell M)$, and hence $\text{Ш}^1(k, \mathrm{T}_\ell M)$ is finite for all ℓ. This leads to the additional statement to our duality theorem stated in the introduction, *via* Corollary 4.2.7.

7.1. Algebraicity of Lie algebras

We work over a fixed number field k, with algebraic closure $\overline{k}$ and absolute Galois group $\Gamma := \mathrm{Gal}(\overline{k}|k)$. The action of Γ on the Lie groups $L^M, L^M_G, \ldots$ and on the Lie algebras $\mathfrak{l}^M, \mathfrak{l}^M_G, \ldots$ is understood to be the conjugation action. All 1–motives are torsion free.

– 7.1.1. Let M be a 1–motive over k. The goal of this section is to show that the Lie algebra $\mathfrak{l}^M_G$ associated with M is *algebraic*, in a sense we make precise now. Recall the following result of Mazur, Rubin and Silverberg ([**MRS08**])

Proposition 7.1.2. *Let G be a semiabelian variety and let Y be a lattice of rank r over k.*

(1) *The fppf sheaf $\mathcal{H}om(Y, G)$ over k is representable by a twist of G^r over k, and there is a canonical isomorphism of Γ–modules $\mathrm{T}_\ell\mathcal{H}om(Y, G) \cong \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G)$.*
(2) *The fppf sheaf $Y \otimes G$ over k is representable by a twist of G^r over k, and there is a canonical isomorphism of Γ–modules $\mathrm{T}_\ell(Y \otimes G) \cong \mathrm{T}_\ell Y \otimes_{\mathbb{Z}_\ell} \mathrm{T}_\ell G$.*

Proof. The fppf sheaf $Y \otimes G$ is representable by a twist of G^r by Theorem 2.1 in [**MRS08**]. There is a canonical isomorphism of sheaves $\mathcal{H}om(Y, G) \cong \mathcal{H}om(Y, \mathbb{Z}) \otimes G$, and the sheaf $\mathcal{H}om(Y, \mathbb{Z})$ is a lattice of rank r. Hence, by the same result $\mathcal{H}om(Y, G)$ is representable by a twist of G^r. The statements about Tate modules follow from Theorem 2.2 of *loc.cit.*, which precisely states that there are isomorphisms as we claim but on finite levels. □

So, if $M = [u : Y \longrightarrow G]$ is a 1–motive over k, then the fppf–sheaf $\mathcal{H}om(Y, G)$ is representable by a twist of G, hence a semiabelian variety itself, and the homomorphism $u : Y \longrightarrow G$ corresponds to a k-rational point on $\mathcal{H}om(Y, G)$. Via the canonical isomorphisms in the proposition, the Kummer injection we constructed in Proposition 5.2.9 becomes

$$\vartheta : \mathfrak{l}^M_G \longrightarrow \mathrm{V}_\ell\mathcal{H}om(Y, G)$$

The question is now the following: Does there exist a subvariety of $\mathcal{H}om(Y,G)$ whose associated ℓ–adic representation space is the image of $\mathfrak{l}^M_G$ via the Kummer injection? This is indeed the case as the following theorem shows:

THEOREM 7.1.3. *Let $M = [u : Y \longrightarrow G]$ be a torsion free 1–motive over k where G is a split semiabelian variety. Let H^M_G be the smallest semiabelian subvariety of $\mathcal{H}om(Y,G)$ containing a nonzero multiple of u. The Kummer injection induces an isomorphism of Galois modules*

$$\mathfrak{l}^M_G \xrightarrow{\cong} \mathrm{V}_\ell H^M_G \quad \subseteq \mathrm{V}_\ell \mathcal{H}om(Y,G)$$

In particular, the Lie algebra $\mathfrak{l}^M_G$ is an algebraic subalgebra of $\mathrm{Hom}(\mathrm{V}_\ell Y, \mathrm{V}_\ell G)$*, defined over k, and its dimension is independent of the prime ℓ.*

The analogous statement for nonsplit semiabelian varieties is wrong. Informally, this theorem states that if we add to k_O the coordinates of the ℓ–division points of all points in the image of $u : Y \longrightarrow G(\overline{k})$, then the Galois group that one obtains is "as large as it can possibly be". In its essential parts, the proof of theorem 7.1.3 is due to Ribet and can be found in [**Rib76**]. That in *loc.cit.* Ribet states his theorem only for abelian varieties of CM-type is solely because Falting's results were not available at the time. (See also [**Hin88**], appendix 2. This reference was pointed out to me by A. Perucca). This section is organized as follows: First establish some elementary properties of the variety H^M_A, and prove then the theorem. Finally we point out some consequences of the theorem which we need later.

As we have seen in Corollary 5.2.10, the Kummer injection $\mathfrak{l}^M_G \longrightarrow \mathrm{V}_\ell \mathcal{H}om(Y,G)$ is an injection of Γ–modules, and in particular of $\mathfrak{l}^G$–modules. In the next lemma we check that the Kummer injection has its image in $\mathrm{V}_\ell H^M_G$. Having this, only the difficult part of Theorem 7.1.3 remains to prove, that is, surjectivity of the Kummer map.

LEMMA 7.1.4. *Let $M = [u : Y \longrightarrow G]$ be a 1–motive over k where G is a semiabelian variety split up to isogeny. Let H^M_G be the smallest semiabelian subvariety of $\mathcal{H}om(Y,G)$ containing a nonzero multiple of u. The image of the Kummer injection $\mathfrak{l}^M_G \longrightarrow \mathrm{V}_\ell \mathcal{H}om(Y,G)$ is contained in $\mathrm{V}_\ell H^M_G$.*

PROOF. Replacing M by an isogenous 1–motive and replacing k by a finite field extension, we may suppose without loss of generality that u is a k–rational point of H^M_G and that Y is constant. We claim that under this hypothesis even the Kummer injection on the Lie group level

$$\vartheta : L^M_G \longrightarrow \mathrm{T}_\ell \mathcal{H}om(Y,G)$$

has its image in $\mathrm{T}_\ell H^M_G$. Observe that given a basis $y_1, \ldots, y_r$ of Y we can canonically identify $\mathcal{H}om(Y,G)$ with G^r, and under this identification the rational point u of $\mathcal{H}om(Y,G)$ corresponds to the r–tuple $P := (u(y_1), \ldots, u(y_r)) \in G(k)^r$. Choose now a sequence of points $(P_i)_{i=0}^\infty$ in $H^M_G(\overline{k})$ such that $P_0 = u$ and $\ell P_i = P_{i-1}$ for all $i > 0$. The Kummer injection ϑ is then given by

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

for all $\sigma \in L^M_G$. The sequence $(\sigma P_i - P_i)_{i=0}^\infty$ clearly represents an element of $\mathrm{T}_\ell H^M_G$. □

PROOF OF THEOREM 7.1.3. We have already checked that $\mathfrak{l}^M_G$ is a $\mathfrak{l}^G$–submodule of $\mathrm{V}_\ell H^M_G$ via the Kummer injection. In order to show that equality holds, it is enough to show that the restriction map

$$\mathrm{Hom}_{\overline{k}}(H^M_G, G) \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}_{\mathfrak{l}^G}(\mathrm{V}_\ell H^M_G, \mathrm{V}_\ell G) \longrightarrow \mathrm{Hom}_{\mathfrak{l}^G}(\mathfrak{l}^M_G, \mathrm{V}_\ell G)$$

is injective. Indeed, if $\mathfrak{l}_G^M$ was not equal to $\mathrm{V}_\ell H_G^M$ then we had an $\mathfrak{l}^G$–module decomposition $\mathrm{V}_\ell H_G^M \cong \mathfrak{l}_G^M \oplus V$ because $\mathrm{V}_\ell H_G^M$ is semisimple. But then, the kernel of the restriction map would be $\mathrm{Hom}_{\mathfrak{l}^G}(V, \mathrm{V}_\ell G)$ which is nontrivial because all simple factors of $\mathrm{V}_\ell H_G^M$, hence of V occur in $\mathrm{V}_\ell G$. Working with Lie groups and $\mathbb{Z}_\ell$–modules rather than with Lie algebras and $\mathbb{Q}_\ell$–vector spaces, it is enough to show that the map

$$\mathrm{Hom}_k(H_G^M, G) \otimes \mathbb{Z}_\ell \cong \mathrm{Hom}_\Gamma(\mathrm{T}_\ell H_G^M, \mathrm{T}_\ell G) \longrightarrow \mathrm{Hom}_\Gamma(L_{G,Y}^M, \mathrm{T}_\ell G)$$

given by composition with the Kummer injection $\vartheta : L_{G,Y}^M \longrightarrow \mathrm{T}_\ell H_G^M$ is injective. We shall work with the following diagram of $\mathbb{Z}_\ell$–modules

$$\begin{tikzcd}
 & & \mathrm{Hom}_k(H_G^M, G) \otimes \mathbb{Z}_\ell \arrow[dll, dashed] \arrow[d, hook] & \\
0 \arrow[r] & K \arrow[r] \arrow[d, hook] & G(k) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & G(k_M) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \arrow[d, hook] \\
0 \arrow[r] & H^1(L^M, \mathrm{T}_\ell G) \arrow[r] \arrow[d] & H^1(k, \mathrm{T}_\ell G) \arrow[r] & H^1(k_M, \mathrm{T}_\ell G) \\
 & \mathrm{Hom}_\Gamma(L_{G,Y}^M, \mathrm{T}_\ell G) & &
\end{tikzcd}$$

where k_M is the fixed field of the kernel $\Gamma \longrightarrow \mathrm{GL}(\mathrm{T}_\ell M)$, so that $L^M = \mathrm{Gal}(k_M|k)$. We now explain the maps in this diagram. The top exact row is given by applying the functor $- \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ to the natural inclusion $G(k) \longrightarrow G(k_M)$. The lower exact row comes from the Hochschild–Serre spectral sequence associated with the field extension $k_M|k$ having Galois group L^M. So the first map is inflation, and the second one restriction. From the long exact Kummer sequence

$$0 \longrightarrow G(k)[\ell^i] \longrightarrow G(k) \xrightarrow{\ell^i} G(k) \longrightarrow H^1(k, G[\ell^i]) \longrightarrow H^1(k, G) \longrightarrow \cdots$$

we cut out injections $G(k)/\ell^i G(k) \longrightarrow H^1(k, G[\ell^i])$. Taking limits over all powers of ℓ we find the injection $G(k) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell \longrightarrow H^1(k, \mathrm{T}_\ell G)$. Via this injection the class of a point $P \in G(k)$ is sent to the class of the cocycle

$$c_P : \Gamma \longrightarrow \mathrm{T}_\ell G \qquad c_P(\sigma) = \big(\sigma P_i - P_i\big)_{i=0}^\infty$$

where $P_0 = P$, and where the P_i's are elements of $G(\overline{k})$ such that $\ell P_i = P_{i-1}$. The right hand vertical injection is defined similarly, and the left hand vertical map is given by restricting the one in the middle. The map $H^1(L^M, \mathrm{T}_\ell G) \longrightarrow \mathrm{Hom}_{L^G}(L_G^M, \mathrm{T}_\ell G)$ is given by restricting cocycles. It has finite kernel and cokernel because of the exact sequence

$$H^1(L^{G,Y}, \mathrm{T}_\ell G) \longrightarrow H^1(L^M, \mathrm{T}_\ell G) \longrightarrow H^1(L_{G,Y}^M, \mathrm{T}_\ell G)^\Gamma \longrightarrow H^2(L^{G,Y}, \mathrm{T}_\ell G)$$

coming from the Hochschild–Serre spectral sequence, and because of theorem 5.3.1. Finally, we have a natural homomorphism

$$\mathrm{Hom}_k(H_G^M, G) \longrightarrow G(k) \qquad \psi \longmapsto \psi(u)$$

Recall that u is a rational point of H_G^M, more precisely, H_G^M is the smallest semiabelian subvariety of $\mathcal{H}om(Y, G)$ containing u as a rational point. For this reason, the above map is injective. Indeed, if $\psi(u) = O$, then $\ker \psi$ is a subvariety of H_G^M containing u, and must thus be equal to H_G^M. Applying $- \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$ to this map and observing that $\mathrm{Hom}_k(H_G^M, G)$ is finitely generated yields the map

$$\mathrm{Hom}_k(H_G^M, G) \otimes \mathbb{Z}_\ell \longrightarrow G(k) \mathbin{\widehat{\otimes}} \mathbb{Z}_\ell$$

That this map is again injective follows also from the fact that $\mathrm{Hom}_k(H_G^M, G)$ is finitely generated and that $G(k)$ is almost free (see 3.3.13).
We claim that the dashed arrow in the above diagram exists. Indeed, this amounts to check that for every $\psi \in \mathrm{Hom}_k(H_G^M, G)$ the rational point $\psi(u) \in G(k)$ is ℓ–divisible in $G(k_M)$. But this is

clear, since already u is ℓ–divisible in $H_G^M(k_M)$.
This provides now an injection $\mathrm{Hom}_k(H_G^M, G)\otimes\mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_\Gamma(L_{G,Y}^M, \mathrm{T}_\ell G)$, and it remains to check that this injection is indeed given by composition with the Kummer map $\vartheta : L_G^M \longrightarrow \mathrm{T}_\ell H_G^M$. Let ψ be a homomorphism $H_G^M \longrightarrow G$ defined over k, and set $P := \psi(u) \in G(k)$. The Kummer injection ϑ, if seen as a homomorphism from $L_{G,Y}^M$ to $\mathrm{T}_\ell H_G^M \subseteq \mathrm{T}_\ell \mathcal{H}om(Y,G)$ is simply given by $\vartheta(\sigma) = (\sigma Q_i - Q_i)_{i=0}^\infty$, where $Q_0 = u$ and $\ell Q_i = Q_{i-1}$ (c.f. proof of Lemma 7.1.4). Hence, the composition $\mathrm{V}_\ell\psi\circ\vartheta : \sigma \longmapsto \mathrm{V}_\ell\psi(\vartheta(\sigma))$ is given by

$$\mathrm{V}_\ell\psi\circ\vartheta : \sigma \longmapsto \mathrm{V}_\ell\psi(\vartheta(\sigma)) = \mathrm{V}_\ell\psi(\sigma Q_i - Q_i)_{i=0}^\infty = \big(\sigma\psi Q_i - \psi Q_i\big)_{i=0}^\infty$$

The points $P_i := \psi Q_i$ of $G(\overline{k})$ satisfy $P_0 = P$ and $\ell P_i = P_{i-1}$. The injection we found above maps $\psi\otimes 1$ to the Γ-module homomorphism $c_P : L_{G,Y}^M \longrightarrow \mathrm{T}_\ell G$ given by the formula

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

This shows the equality $c_P = \mathrm{V}_\ell\psi\circ\vartheta$ as needed. □

7.2. Dividing points on abelian varieties and tori

Let A be an abelian variety over the number field k. The Mordell–Weil theorem tells us that the group of rational points $A(k)$ is of finitely generated. In particular, it contains no divisible elements. In contrast, the group of algebraic points $A(\overline{k})$ is divisible. For each $P \in A(\overline{k})$ and integer n, there exist $n^{2\dim A}$ points $R \in A(\overline{k})$ such that $nR = P$.
Given a point $P \in A(k)$ and a prime number ℓ, we can add to the field k the coordinates of all points $R \in A(\overline{k})$ such that $\ell^n R = P$ for some integer $n \geq 0$. This will eventually result in a big field extension k_P of k. By construction, the point P has all its ℓ^n–th roots in $A(k_P)$ and becomes therefore divisible in $A(k_P)$. So we could think of $A(k_P)$ as being a kind of localization of $A(k)$.
A natural question would now be: Is P essentially the only point that has all its ℓ^n–th roots in $A(k_P)$, or are there others? Of course, there are some points for which that happens for stupid reasons: If $\psi : A \longrightarrow A$ is an endomorphism, and if $R \in A(k_P)$ is such that $\ell^n R = P$, then we have $\ell^n\psi(R) = \psi(P)$. Therefore, any image of P under an endomorphism of A over k has its ℓ^n–th roots in $A(k_P)$. So the real question is: Are there other points having all roots in $A(k_P)$ by some strange accident?
First, we introduce a terminology generalizing what we already have introduced in 6.1.1. Recall that for a 1–motive M over k, we write L^M for the image of the natural map $\Gamma \longrightarrow \mathrm{GL}(\mathrm{T}_\ell M)$, and k_M for the field fixed by the kernel of this map, so that $L^M \cong \mathrm{Gal}(k_M|k)$. In other words, k_M is the smallest field extension of k over which Y is constant and such that all $Q \in G(\overline{k})$ with $\ell^n Q = u(y)$ for some $n \geq 0$ and $y \in Y$ are defined over k_M.

Definition 7.2.1. Let $M = [u : Y \longrightarrow G]$ be a 1–motive number field over k. We write $D_M(k)$ for the kernel of the natural map $G(k) \longrightarrow G(k_M)\,\widehat{\otimes}\,\mathbb{Z}_\ell$. In words, $D_M(k)$ is the subgroup of $G(k)$ consisting of those points which are ℓ–divisible in $G(k_M)$. We call these points the *module of deficient points* of M.

Yet another way to characterize deficient points is to say that $P \in G(k)$ is deficient if and only if the field k_P is contained in the field k_M. It is clear that $D_M(k)$ is not only a subgroup, but rather a $\mathrm{End}_k(G)$–submodule of $G(k)$. With this terminology, the question above is the following. Let $[u : \mathbb{Z} \longrightarrow A]$ be a 1–motive over k given by $u(1) = P$. Is $D_M(k)$ equal to the $\mathrm{End}_k A$–module generated by P? The following theorem precisely answers that question.

THEOREM 7.2.2. *Let A be an abelian variety over k and let $P_1,\dots,P_r\in A(k)$ be rational points, giving rise to a 1–motive $M=[\mathbb{Z}^r\longrightarrow A]$. The following statements are equivalent for a rational point $P\in A(k)$:*

(1) *The point P is deficient, that is, $P\in D_M(k)$*
(2) *A nonzero multiple of P is contained in the* $\mathrm{End}_k A$*–module generated by $P_1,\dots,P_r$*

Let me point out again that this theorem, which is a rather straightforward consequence of Theorem 7.1.3, is essentially due to Ribet ([**Rib76**], see also appendix 2 in [**Hin88**]). In an earlier version of this work, I used a different approach to theorems 7.2.2 and 7.1.3, which consisted in proving 7.2.2 for simple abelian varieties in a first step, to extend this to general abelian varieties essentially by induction using Poincaré's reducibility theorem and then to deduce 7.1.3 from it. The way I am presenting things now owes much to a discussion with A. Perucca.

LEMMA 7.2.3. *Let $\varphi:A\longrightarrow B$ be an isogeny of abelian varieties over k and let P be a rational point of A. The fields k_P and $k_{\varphi(P)}$ are equal.*

PROOF. Let $M_A=[u_A:\mathbb{Z}\longrightarrow A]$ and $M_B=[u_B:\mathbb{Z}\longrightarrow B]$ be the 1–motives given by $u_A(1)=P$ and $u_B(1)=\varphi(P)$ respectively. We get a short exact sequence of Γ–modules

$$0\longrightarrow \mathrm{T}_\ell M_A\longrightarrow \mathrm{T}_\ell M_B\longrightarrow F\longrightarrow 0$$

the first map being induced by the isogeny $(\mathrm{id},\varphi):M_A\longrightarrow M_B$, and where F is a finite Γ–module. Tensoring with $\mathbb{Q}_\ell$, we get an isomorphism of Γ–modules $\mathrm{V}_\ell M_A\cong \mathrm{V}_\ell M_B$. An element $\sigma\in\Gamma$ fixes k_P if and only it acts trivially on $\mathrm{V}_\ell M_A$, and fixes $k_{\varphi(P)}$ if and only it acts trivially on $\mathrm{V}_\ell M_B$. Hence $\mathrm{Gal}(\overline{k}|k_P)=\mathrm{Gal}(\overline{k}|k_{\varphi(P)})$. □

PROOF OF THEOREM 7.2.2. (1) $\Longrightarrow$ (2) Suppose that some nonzero multiple of P is contained in the $\mathrm{End}_k A$–module generated by $P_1,\dots,P_r$, that is, $nP=\psi_1P_1+\cdots+\psi_rP_r$. The points P_i are deficient, since by definition of k_M all their ℓ–th power roots are defined over k_M. Hence nP is deficient. Lemma 7.2.3 shows that P is deficient is and only nP is, hence P is deficient.
(2) $\Longrightarrow$ (1) Suppose P is deficient. In the proof of Theorem 7.1.3 we have seen that the canonical map

$$\mathrm{Hom}_k(H_A^M,A)\otimes\mathbb{Z}_\ell\longrightarrow \ker\big(A(k)\otimes\mathbb{Z}_\ell\longrightarrow A(k_M)\otimes\mathbb{Z}_\ell\big)$$

sending a homomorphism $\psi:H_A^M\longrightarrow A$ to the rational deficient point $\psi(u)$ is injective and has finite cokernel. This implies that the image of the map $\mathrm{Hom}_k(A^r,A)\longrightarrow A(k)$ sending $(\psi_1,\dots,\psi_r)$ to $\psi_1P_1+\cdots+\psi_rP_r$ is of finite index in $D_M(k)$. Thus, a nonzero multiple of P is a $\mathrm{End}_k A$–linear combination of the P_i's as claimed. □

– 7.2.4. Everything we did so far for abelian varieties has an analogue for tori, and holds in fact for semiabelian varieties split up to isogeny. Of this, only the following is interesting for us in the sequel.
Let $M=[Y\longrightarrow G]$ be a 1–motive over k where G is a semiabelian variety split up to isogeny. In the proof of theorem 7.1.3 we have seen that the image of the natural map $\mathrm{Hom}_k(H_G^M,G)\longrightarrow G(k)$ lies in $D_M(k)$ with finite index. Tensoring with $\mathbb{Q}_\ell$ yields an isomorphism of $\mathrm{End}_k G$–modules

$$\begin{array}{ccc}\mathrm{Hom}_k(H_G^M,G)\otimes\mathbb{Q}_\ell & \xrightarrow{\cong} & D_M(k)\otimes\mathbb{Q}_\ell\\ \psi\otimes\lambda & \longmapsto & \psi(u)\otimes\lambda\end{array}$$

Hence, every element of $D_M(k)\otimes\mathbb{Q}_\ell$ can be written as a sum of elements of the form $\psi(u)\otimes\lambda$ for some $\psi\in\mathrm{Hom}_k(H_G^M,G)$ and some $\lambda\in\mathbb{Q}_\ell$. This isomorphism, or rather its inverse, can be interpreted as the adjunction map in a canonical pairing between $D_M(k)\otimes\mathbb{Q}_\ell$ and $\mathrm{V}_\ell H_G^M$ given by the formula

$$\begin{array}{rcl}(D_M(k)\otimes\mathbb{Q}_\ell)\times \mathrm{V}_\ell H_G^M & \longrightarrow & \mathrm{V}_\ell G\\ \psi(u)\otimes\lambda \quad , \quad v & \longmapsto & \lambda \mathrm{V}_\ell\psi(v)\end{array}$$

valid for all $\psi\in\mathrm{Hom}_k(H_G^M,G)$ and all $v\in\mathrm{V}_\ell H_G^M$. This is a pairing of $\mathbb{Q}_\ell$–vector spaces, of course linear and Galois equivariant. The next proposition shows in a certain sense that this pairing is nondegenerate, at least if Y is constant.

Proposition 7.2.5. *Let $M=[Y\longrightarrow G]$ be a torsion free 1–motive over k where G is a split semiabelian variety. Write $E:=\mathrm{End}_k\,G\otimes\mathbb{Q}_\ell\cong\mathrm{End}_\Gamma\,\mathrm{V}_\ell G$, and consider the canonical maps*

$$\begin{array}{rcl}D_M(k)\otimes\mathbb{Q}_\ell & \longrightarrow & \mathrm{Hom}_\Gamma(\mathrm{V}_\ell H_G^M,\mathrm{V}_\ell G)\\ \psi(u)\otimes\lambda & \longmapsto & \lambda\mathrm{V}_\ell\psi\end{array}\qquad\qquad \begin{array}{rcl}\mathrm{V}_\ell H_G^M & \longrightarrow & \mathrm{Hom}_E(D_M(k)\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)\\ v & \longmapsto & [\psi(u)\otimes 1\longmapsto \mathrm{V}_\ell\psi(v)]\end{array}$$

The left hand map is an isomorphism, and the right hand map is an isomorphism provided Y is constant.

Proof. That the left hand map is an isomorphism we have already seen. The second statement is a consequence of the following, slightly more general lemma. □

Lemma 7.2.6. *Let G be a semiabelian variety over k split up to isogeny, and let Y be a lattice over k. Let H be a semiabelian subvariety of $\mathcal{H}om(Y,G)$. Write $E:=\mathrm{End}_k\,G\otimes\mathbb{Q}_\ell$. If Y is constant, then the map*

$$\mathrm{V}_\ell H\longrightarrow \mathrm{Hom}_E(\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H,\mathrm{V}_\ell G),\mathrm{V}_\ell G)$$

sending $v\in\mathrm{V}_\ell H$ to the evaluation map $f\longmapsto f(v)$ is an isomorphism.

Proof. In a first step, we show that without loss of generality we may assume that $H=\mathcal{H}om(Y,G)$. Indeed, because G and hence $\mathcal{H}om(Y,G)$ is split up to isogeny, the Γ–module $\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)$ is semisimple. Any Γ–module decomposition

$$\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)=\mathrm{V}_\ell H\oplus\mathrm{V}_\ell H'$$

yields an E–module decomposition

$$\mathrm{Hom}_\Gamma(\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)\mathrm{V}_\ell G)=\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H,\mathrm{V}_\ell G)\oplus\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H,\mathrm{V}_\ell G)$$

This shows that the if the Lemma holds for $\mathcal{H}om(Y,G)$ in place of H, then it holds for H as well. From now on, we set $H:=\mathcal{H}om(Y,G)$. In a next step, let us prove the lemma in the case where Y is constant. We have in this case a canonical isomorphism of E–modules

$$\iota: E\otimes(Y\otimes\mathbb{Q}_\ell)\xrightarrow{\cong}\mathrm{Hom}_\Gamma(\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G),\mathrm{V}_\ell G)=\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H,\mathrm{V}_\ell G)$$

sending $\psi\otimes y\otimes\lambda$ to the Γ–module map $f\longmapsto\psi f(y\otimes\lambda)$. Under this isomorphism the evaluation map in the statement of the lemma becomes

$$\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)=\mathrm{V}_\ell H\longrightarrow\mathrm{Hom}_E(E\otimes(Y\otimes\mathbb{Q}_\ell),\mathrm{V}_\ell G)$$

sending $f\in\mathrm{Hom}(Y\otimes\mathbb{Q}_\ell,\mathrm{V}_\ell G)$ to the E–module map $\psi\otimes y\otimes\lambda\longmapsto\psi f(y\otimes\lambda)$. This is an isomorphism, hence the lemma. □

7.3. Computing $H^1_*(L^M, \mathrm{V}_\ell M)$

The main objective of this section is to explicitly compute the group $H^1_*(L^M, \mathrm{V}_\ell M)$ for a 1–motive M over a number field k. The main result of this section is Proposition 7.3.1 below, which gives us a way to compute $H^1_*(L^M, \mathrm{V}_\ell M)$ effectively by means of elementary linear algebra. It is from this key result that we will later derive finiteness of $H^1_*(L^M, \mathrm{T}_\ell M)$ in several interesting cases. We make two technical assumptions: First that the lattice of M is constant, and second that the semiabelian variety of M is split up to isogeny. It should not be too difficult to get rid of the first assumption (especially regarding Lemma 7.3.3 below). We need this condition in order to apply Proposition 7.2.5. The second of these assumptions however is crucial. We need it to apply Theorem 7.1.3 and several other results which we only established for split semiabelian varieties.

Proposition 7.3.1. *Let k be a number field, let $M = [u : Y \longrightarrow G]$ be a 1–motive over k. Suppose that Y is constant and that G isogenous to a split semiabelian variety. Define*

$$V := D_M(k) \otimes \mathbb{Q}_\ell \qquad W := u(Y) \otimes \mathbb{Q}_\ell \qquad E := \mathrm{End}_k\, G \otimes \mathbb{Q}_\ell$$

and set

$$\overline{W} := \Big\{ v \in V \;\Big|\; f(v) \in f(W) \text{ for all } f \in \mathrm{Hom}_E(V, \mathrm{V}_\ell G) \Big\}$$

There is a canonical isomorphism $H^1_*(L^M, \mathrm{V}_\ell M) \cong \overline{W}/W$.

– 7.3.2. For the sake of clarity, we split the rather technical proof of this proposition up in a series of lemmas. The idea is as follows: Writing out the long exact sequence associated with the L^M–module sequence $0 \longrightarrow \mathrm{V}_\ell G \longrightarrow \mathrm{V}_\ell M \longrightarrow Y \otimes \mathbb{Q}_\ell \longrightarrow 0$ and the definition of $H^1_*(L^M, \mathrm{V}_\ell M)$ one finds maps

$$H^0(L^M, Y \otimes \mathbb{Q}_\ell) \xrightarrow{\ \partial\ } H^1(L^M, \mathrm{V}_\ell G) \xrightarrow{\ \delta\ } \prod_{x \in L^M} H^0(\langle x \rangle, \mathrm{V}_\ell M)$$

The composition of these maps is zero, and one has $H^1_*(L^M, \mathrm{V}_\ell M) \cong \ker \delta / \operatorname{im} \partial$. It is not hard to identify $\operatorname{im} \partial$ with W and $H^1(L^M, \mathrm{V}_\ell G)$ with V. So far we don't need any hypothesis on M. The hard part is then to show that an element $v \in V$ is in $\overline{W}$ if and only if the corresponding cohomology class in $H^1(L^M, \mathrm{V}_\ell G)$ restricts to zero on each monogenous subgroup of L^M.

Lemma 7.3.3. *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, equality*

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

holds[1]*. Moreover, if N is normal there is a canonical isomorphism $H^1_*(L, V) \cong H^1_*(N, V)^{L/N}$, and 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 $H^1(C, V)$ for each monogenous subgroup C contained in N. We must show that c the same holds for all monogeneous subgroups of L. Let $C \subseteq L$ be monogenous. Because L and hence C is compact, the quotient $C/(N \cap C)$ is finite. Thus, by the usual restriction–corestriction argument and using that V is uniquely divisible we see that the restriction map $H^1(C, V) \longrightarrow H^1(C \cap N, V)$ is injective, hence the claim.
Now suppose that N is open and normal. Since L is compact, the quotient L/N is finite and we

[1] That means, in the definition of $H^1_*(L, V)$ we don't need to involve *all* monogenous subgroups of L, it is enough to consider only monogenous subgroups of some open subgroup N of L.

have again by restriction–corestriction that $H^i(L/N, V) = 0$ for all $i > 0$. The Hochschild–Serre spectral sequence yields a canonical isomorphism $H^1(L, V) \cong H^1(N, V)^{L/N}$. Consider

$$\begin{tikzcd}
0 \arrow[r] & H^1_*(L,V) \arrow[r] \arrow[d] & H^1(L,V) \arrow[r] \arrow[d, "\cong"'] \arrow[dr, dashed, "\delta"] & \prod\limits_{x\in L} H^1(\langle x\rangle, V) \arrow[d] \\
0 \arrow[r] & H^1_*(N,V)^{L/N} \arrow[r] & H^1(N,V)^{L/N} \arrow[r] & \prod\limits_{x\in N} H^1(\langle x\rangle, \mathrm{V}_\ell M)
\end{tikzcd}$$

In order to show that the left hand vertical map is an isomorphism, we must show that the kernel of the diagonal map δ is exactly $H^1_*(L, V)$ – but this is just the first statement of the lemma. Finally, if N is sufficiently small we have an isomorphism $H^1(N, V) \cong H^1(\mathfrak{l}, V)$, from which the last statement follows. □

LEMMA 7.3.4. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. Suppose that G is split up to isogeny. If an element of $H^1(L^M, \mathrm{V}_\ell G)$ restricts to zero in $H^1(\langle x\rangle, \mathrm{V}_\ell M)$ for all $x \in L^M_{G,Y}$, then the same holds for all $x \in L^M$.*

PROOF. By Lemma 7.3.3 it is enough to prove the lemma with L^M replaced by an open normal subgroup, or say with k replaced by a finite Galois extension $k'|k$. We may thus suppose without loss of generality that L^M acts trivially on Y. Moreover, we know by Corollary 5.3.2 that the Lie algebra extension

$$0 \longrightarrow \mathfrak{l}^M_G \longrightarrow \mathfrak{l}^M \longrightarrow \mathfrak{l}^G \longrightarrow 0$$

is split. Any Lie algebra section $\mathfrak{l}^G \longrightarrow \mathfrak{l}^M$ of this sequence comes from a Lie group section defined on an open subgroup of L^G. Choosing L^M even smaller (or k' even larger) we may suppose that the corresponding Lie group extension

$$0 \longrightarrow L^M_G \longrightarrow L^M \longrightarrow L^G \longrightarrow 0$$

is split, i.e. that there is a section $s : L^G \longrightarrow L^M$ of the projection map $L^M \longrightarrow L^G$. Choose a $\mathbb{Q}_\ell$–basis of $\mathrm{V}_\ell M$ containing a basis of $\mathrm{V}_\ell G$, so that every element of L^M can be uniquely represented by a 2×2 upper triangular block matrix

$$\sigma = \left(\begin{array}{c|c} \overline{\sigma} & f \\ \hline 0 & 1 \end{array}\right)$$

where $\overline{\sigma}$ is the restriction of σ to $\mathrm{V}_\ell G$ hence an element of L^G, and where $f : Y \otimes \mathbb{Q}_\ell \longrightarrow \mathrm{V}_\ell G$ is a linear map. The subgroup L^M_G of L^M consists now of precisely those matrices with $\overline{\sigma} = 1$. The section map s is now given by a map $s_1 : L^G \longrightarrow \mathrm{Hom}(Y \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G)$ so that

$$s(\overline{\sigma}) = \left(\begin{array}{c|c} \overline{\sigma} & s_1(\overline{\sigma}) \\ \hline 0 & 1 \end{array}\right)$$

Observe that the map s_1 is a cocycle, and that $\mathrm{Hom}(Y \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G)$ is isomorphic to a power of $\mathrm{V}_\ell G$ as a L^G–module. Hence s_1 is a coboundary by Theorem 5.3.1. So there exists a $f \in \mathrm{Hom}(\mathrm{V}_\ell Y, \mathrm{V}_\ell G)$ such that

$$s(\overline{\sigma}) = \left(\begin{array}{c|c} \overline{\sigma} & \overline{\sigma} f - f \\ \hline 0 & 1 \end{array}\right)$$

We now change the chosen basis using for base change matrix the upper triangular block matrix given by the identity on the diagonal and f in the upper corner. In this new basis $s(\overline{\sigma})$ is simply given by a diagonal block matrix formed by the blocks $\overline{\sigma}$ and 1. This means that with respect to this basis we can write every element σ of L^M uniquely as a matrix

$$\sigma = \left(\begin{array}{c|c} \overline{\sigma} & f \\ \hline 0 & 1 \end{array}\right) \qquad \text{with} \qquad \left(\begin{array}{c|c} 1 & f \\ \hline 0 & 1 \end{array}\right) \in L^M_G \qquad \text{and} \qquad \overline{\sigma} \in L^G$$

Consider now a cocycle $c : L^M \longrightarrow \mathrm{V}_\ell G$. To say that the cohomology class represented by c restricts to zero in $H^1(\langle\sigma\rangle, \mathrm{V}_\ell M)$ is precisely to say that there exists a $v \in \mathrm{V}_\ell M$ such that $c(\sigma) = \sigma v - v$. Let us suppose this happens for all $\sigma \in L^M_G$, and let σ be any element of L^M. Write $\sigma = \sigma_1\sigma_2$ with

$$\sigma_1 = \left(\begin{array}{c|c} 1 & f \\ \hline 0 & 1 \end{array}\right) \qquad \text{and} \qquad \sigma_2 = \left(\begin{array}{c|c} \overline{\sigma} & 0 \\ \hline 0 & 1 \end{array}\right)$$

according to the decomposition introduced above. Changing c by a coboundary, we may suppose that $c(\sigma_2) = 0$. We then find

$$c(\sigma) = c(\sigma_1\sigma_2) = c(\sigma_1) = \sigma_1 v - v$$

for some $v \in \mathrm{V}_\ell M = \mathrm{V}_\ell G \oplus \mathrm{V}_\ell Y$ by hypothesis. Writing $v = v_1 + v_2$ for the given decomposition, we have

$$\sigma_1 v - v = \sigma_1 v_1 + v_2 - v_1 - v_2 = \sigma_1 v_1 - v_1 = \sigma v_1 - v_1$$

because σ_2 acts trivially on v_1, hence $c(\sigma) = \sigma v_1 - v_1$ and we are done. $\square$

Lemma 7.3.5. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. Suppose that G is split up to isogeny. There is a commutative diagram*

$$\begin{array}{ccccc} Y^\Gamma \otimes \mathbb{Q}_\ell & \xrightarrow{u\otimes \mathrm{id}} & D_M(k) \otimes \mathbb{Q}_\ell & \xrightarrow{\cong} & \mathrm{Hom}_\Gamma(\mathrm{V}_\ell H^M_G, \mathrm{V}_\ell G) \\ \downarrow\cong & & \downarrow\cong & & \cong\downarrow\circ\vartheta \\ H^0(L^M, Y \otimes \mathbb{Q}_\ell) & \xrightarrow{\partial} & H^1(L^M, \mathrm{V}_\ell G) & \underset{\cong}{\xrightarrow{\mathrm{res}}} & \mathrm{Hom}_\Gamma(L^M_{G,Y}, \mathrm{V}_\ell G) \end{array}$$

with canonical isomorphisms where indicated.

Proof. We begin with the left hand square. The isomorphism $D_M(k)\otimes\mathbb{Q}_\ell \cong H^1(L^M, \mathrm{V}_\ell G)$ is, recall, given as follows. It is $\mathbb{Q}_\ell$–linear, and if $P \in D_M(k)$ is a deficient point, then this isomorphism sends $P \otimes 1$ to the class of the cocycle

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

where $(P_i)_{i=0}^\infty$ is a sequence of points in $G(\overline{k})$ such that $P_0 = P$ and $\ell P_i = P_{i-1}$ for all $i \geq 1$. Now suppose that $P = u(y)$ for some $y \in Y^\Gamma$. The image of y in $H^1(L^M, \mathrm{V}_\ell G)$ via the (obvious) left hand vertical isomorphism and the connecting morphism ∂ is given by a cocycle $c_v : \sigma \longmapsto \sigma v - v$, where v is any element of $\mathrm{V}_\ell M$ projecting to $y \otimes 1$ in $Y \otimes \mathbb{Q}_\ell$. Using our explicit description of the Tate module of M, the sequence $v = (y, P_i)_{i=0}^\infty$ is such a preimage, and the equality $c_P = c_v$ holds. We now come to the square on the right. By the computations in 7.2.4, we know that elements of $D_M(k) \otimes \mathbb{Q}_\ell$ can be written as $\mathbb{Q}_\ell$–linear combinations of elements $\psi(u) \otimes 1$ for some $\psi \in \mathrm{Hom}_k(H^M_G, G)$. The top vertical isomorphism sends $\psi(u) \otimes 1$ to $\mathrm{V}_\ell\psi$. The bottom horizontal isomorphism is given by restricting cocycles. The rightmost vertical map is given by composition with the Kummer injection

$$\vartheta : L^M_{G,Y} \longrightarrow \mathrm{T}_\ell H^M_G \subseteq \mathrm{V}_\ell H^M_G$$

Because the Kummer injection ϑ has open image, this yields indeed an isomorphism. Let us now check that this square commutes. Let $P = \psi(u) \in D_M(k)$ be a deficient point. One way, as we explained, $P \otimes 1$ maps to the Γ–module homomorphism $\mathrm{V}_\ell\psi$ first, and then to the Γ–module homomorphism $\mathrm{V}_\ell\psi \circ \vartheta$, and the other way around P maps to the Γ–module homomorphism c_P given by the formula above. We have already checked the equality $c_P = \mathrm{V}_\ell\psi \circ \vartheta$ at the end of the proof of Theorem 7.1.3. $\square$

Lemma 7.3.6. *Let $M = [Y \longrightarrow G]$ be a 1–motive over k. Suppose that G is split up to isogeny and that Y is constant. Write W for the image of $Y \otimes \mathbb{Q}_\ell$ in $D_M(k) \otimes \mathbb{Q}_\ell$ and set $E := \mathrm{End}_k\, G \otimes \mathbb{Q}_\ell$. Consider the canonical isomorphism from Lemma 7.3.5*

$$D_M(k) \otimes \mathbb{Q}_\ell \cong H^1(L^M, \mathrm{V}_\ell G) \qquad\qquad \psi(u) \otimes \lambda \longmapsto \lambda \mathrm{V}_\ell \psi$$

An element of $H^1(L^M, \mathrm{V}_\ell G)$ restricts to zero on $H^1(\langle x \rangle, \mathrm{V}_\ell M)$ for all $x \in L^M$ if and only if the corresponding element in $D_M(k) \otimes \mathbb{Q}_\ell$ is contained in $f(W)$ for all $f \in \mathrm{Hom}_E(D_M(k) \otimes \mathbb{Q}_\ell, \mathrm{V}_\ell G)$.

Proof. We are considering the two maps

$$D_M(k) \otimes \mathbb{Q}_\ell \longrightarrow \prod_f \mathrm{V}_\ell G / f(W) \qquad \text{and} \qquad H^1(L^M, \mathrm{V}_\ell G) \longrightarrow \prod_{x \in L^M} H^1(\langle x \rangle, \mathrm{V}_\ell M)$$

the left hand one sending $P \otimes \lambda$ to $f(P \otimes \lambda)$ in the factor corresponding to f, and the right hand one given by restriction. The lemma claims that the kernels of these maps correspond to each other under the canonical isomorphism $D_M(k) \otimes \mathbb{Q}_\ell \cong H^1(L^M, \mathrm{V}_\ell G)$. Lemma 7.3.4 shows that if on the right hand side we let the product run over $x \in L^M_{G,Y}$ we still get the same kernel. For every $\sigma \in L^M_{G,Y}$ we have

$$H^1(\langle \sigma \rangle, \mathrm{V}_\ell M) \;\cong\; \frac{\mathrm{V}_\ell M}{\{\sigma v - v \mid v \in \mathrm{V}_\ell M\}} \;=\; \frac{\mathrm{V}_\ell M}{\mathrm{im}(\vartheta(\sigma))}$$

Moreover, recall that the map $H^1(L^M, \mathrm{V}_\ell G) \longrightarrow \mathrm{Hom}_\Gamma(L^M_{G,Y}, \mathrm{V}_\ell G)$ given by restriction of cocycles is an isomorphism. So, we have to show that the kernels of the maps

$$D_M(k) \otimes \mathbb{Q}_\ell \longrightarrow \prod_f \mathrm{V}_\ell G / f(W) \qquad \text{and} \qquad \mathrm{Hom}_\Gamma(L^M_{G,Y}, \mathrm{V}_\ell G) \longrightarrow \prod_{\sigma \in L^M_{G,Y}} \mathrm{V}_\ell G / \operatorname{im} \vartheta(\sigma)$$

correspond under the isomorphism from Lemma 7.3.5. The right hand map sends a Γ–module homomorphism $c : L^M_{G,Y} \longrightarrow \mathrm{V}_\ell G$ to the class of $c(\sigma)$ in the factor corresponding to σ. By Lemma 7.3.5, we can on the left hand side also take $\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H^M_H, \mathrm{V}_\ell G)$ in place of $D_M(k) \otimes \mathbb{Q}_\ell$. Now we must show that the kernels of the maps

$$\mathrm{Hom}_\Gamma(\mathrm{V}_\ell H^M_H, \mathrm{V}_\ell G) \longrightarrow \prod_f \mathrm{V}_\ell G / f(W) \qquad \text{and} \qquad \mathrm{Hom}_\Gamma(L^M_{G,Y}, \mathrm{V}_\ell G) \longrightarrow \prod_{\sigma \in L^M_{G,Y}} \mathrm{V}_\ell G / \operatorname{im} \vartheta(\sigma)$$

correspond to each other via composition with the Kummer map $\vartheta : L^M_{G,Y} \longrightarrow \mathrm{V}_\ell H^M_G$, the left hand product now running over all E–module morphisms $f : \mathrm{Hom}_\Gamma(\mathrm{V}_\ell H^M_H, \mathrm{V}_\ell G) \longrightarrow \mathrm{V}_\ell G$. We have shown in Proposition 7.2.5 (which we can apply as Y is constant) that all these E–module homomorphisms are given by evaluation in an element $v \in \mathrm{V}_\ell H^M_G$. If f is the evaluation in $v = \vartheta(\sigma)$ for some $\sigma \in L^M_{G,Y}$ (and up to a suitable scalar multiple, every f is), then $f(W) = \operatorname{im} \vartheta(\sigma)$, hence the claim of the lemma. □

Proof of Proposition 7.3.1. We consider the following diagram, where the exact row is given by the usual dévissage of the $\mathfrak{l}^M$–module $\mathrm{V}_\ell M$, and where the column is exact by definition:

$$\begin{tikzcd}
 & & H^1_*(L^M, \mathrm{V}_\ell M) \arrow[d, "\subseteq"] \arrow[dr, "0"] & \\
H^0(L^M, Y \otimes \mathbb{Q}_\ell) \arrow[r, "\partial"] & H^1(L^M, \mathrm{V}_\ell G) \arrow[r] \arrow[dr, "\delta"'] & H^1(L^M, \mathrm{V}_\ell M) \arrow[r] \arrow[d] & H^1(L^M, \mathrm{V}_\ell Y) \\
 & & \prod_{x \in L^M} H^1(\langle x \rangle, \mathrm{V}_\ell M) &
\end{tikzcd}$$

The upper diagonal map is zero, because the image of L^M in $\mathrm{GL}(Y \otimes \mathbb{Q}_\ell)$, which we denote L^Y is finite, and hence $H^1_*(L^M, \mathrm{V}_\ell M) \cong H^1_*(L^Y, Y \otimes \mathbb{Q}_\ell)$ is trivial. This shows that every element of $H^1_*(L^M, \mathrm{V}_\ell M)$ comes from an element in $H^1(L^M, \mathrm{V}_\ell G)$, or more precisely that

$$H^1_*(L^M, Y \otimes \mathbb{Q}_\ell) \cong \ker \delta / \operatorname{im} \partial$$

But the lemmas7.3.5 and 7.3.6 precisely ensure that the canonical isomorphism $V := D_M(k) \otimes \mathbb{Q}_\ell \longrightarrow H^1(L^M, \mathrm{V}_\ell M)$ induces isomorphisms $W \cong \operatorname{im} \partial$ and

$$\overline{W} := \{v \in V \mid f(v) \in f(W) \text{ for all } f \in \operatorname{Hom}_E(V, \mathrm{V}_\ell G)\} \cong \ker \delta$$

as needed. □

7.4. Finiteness criteria for Ш$^1(k, \mathbb{T}_\ell M)$

Is Ш$^1(k, \mathbb{T}_\ell M)$ finite for all 1–motives M? Unfortunately, we do not know. In section 5.5 we have shown that the $\mathbb{Z}_\ell$–rank of Ш$^1(k, \mathbb{T}_\ell M)$ is bounded (independently of ℓ), and we have computed the torsion subgroup of Ш$^1(k, \mathbb{T}_\ell M)$. In this section we present some interesting criteria under which Ш$^1(k, \mathbb{T}_\ell M)$ is finite. Since finiteness of Ш$^1(k, \mathbb{T}_\ell M)$ persists under replacing M by an isogenous 1–motive, we can stick to torsion free 1–motives for most of our arguments. As always, k is a number field with fixed algebraic closure $\overline{k}$, and ℓ is a fixed prime number.

So what is the problem in proving finiteness of Ш$^1(k, \mathrm{T}_\ell M)$ (or disproving it)? The problem is that the "bad" primes do matter. With what we worked out so far (above all Proposition 7.3.1) we can compute $H^1_*(k, \mathrm{T}_\ell M)$ under some technical conditions. This group is canonically isomorphic to

$$H^1_S(k, \mathrm{T}_\ell M) := \ker \left(H^1(k, \mathrm{T}_\ell) \longrightarrow \prod_{v \in S} H^1(k_v, \mathrm{T}_\ell M) \right)$$

where S is a set of places of k of density 1, not containing the places where $\mathrm{T}_\ell M$ ramifies and not containing the places that divide ℓ (by 5.4.4 and 5.4.5). It contains Ш$^1(k, \mathrm{T}_\ell M)$, hence if we can show that $H^1_*(k, \mathrm{T}_\ell M)$ is finite we are done. However, the group $H^1_*(k, \mathrm{T}_\ell M)$, and hence $H^1_S(k, \mathrm{T}_\ell M)$ may be infinite. We shall give later an example of a 1–motive M where this is the case, but for which nevertheless Ш$^1(k, \mathrm{T}_\ell M)$ is finite. We do not have any example of a 1–motive for which Ш$^1(k, \mathrm{T}_\ell M)$ is infinite.
For the time being, our only method of proving finiteness of Ш$^1(k, \mathrm{T}_\ell M)$ goes via proving finiteness of $H^1_*(k, \mathrm{T}_\ell M)$. Our main result is:

THEOREM 7.4.1. *Let $M = [u : Y \longrightarrow G]$ be a 1–motive with torsion over k. Suppose that at least one of the following conditions is met.*

(1) *Either G is a geometrically simple abelian variety, or else, a 1–dimensional torus.*
(2) *The rank of Y is ≤ 1 and G is split up to isogeny*

Then the group Ш$^1(k, \mathrm{T}_\ell M)$ is finite for all ℓ, and even trivial for all but finitely many ℓ. In this case, the canonical pairing

$$Ш^0(k, M) \times Ш^2(k, M^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite groups, trivial whenever $\ker u$ is constant. The same conclusions hold for any 1–motive with torsion isogenous to M.

– 7.4.2. As already mentioned, we shall derive Theorem 7.4.1 from our key proposition 7.3.1. Let us recapitulate the situation. We have there a finite dimensional semisimple $\mathbb{Q}_\ell$–algebra E, two E–modules V and V_0, and a $\mathbb{Q}_\ell$–linear subspace W of V. The E–module V_0 (playing the role of $\mathrm{V}_\ell G$) is faithful. The question is how far W is characterized by its images under E–linear maps $f : V \longrightarrow V_0$, i.e. setting

$$\overline{W} := \left\{ v \in V \;\middle|\; f(v) \in f(W) \text{ for all } f \in \mathrm{Hom}_E(V, V_0) \right\}$$

we want to compute $\overline{W}/W$. Observe for example that if $E = \mathbb{Q}_\ell$ and $V_0 \neq 0$, then equality holds always. Hence, Proposition 7.3.1 tells us that if $\mathrm{End}_k G \otimes \mathbb{Q}_\ell$ is $\mathbb{Q}_\ell$, then $H^1_*(L^M, \mathrm{V}_\ell M)$ is trivial and hence $H^1_*(L^M, \mathrm{T}_\ell M)$ and $\text{Ш}^1(L^M, \mathrm{T}_\ell M)$ finite! Bearing this in mind, the proof of Theorem 7.4.1 just amounts to check some linear algebra generalities, and to conclude using Propositions 7.3.1 and 5.4.4. We begin with some linear algebra.

LEMMA 7.4.3. *Let K be a field of characteristic zero, let E be a finite dimensional division algebra over K, let V and $V_0 \neq 0$ be finite dimensional E–vector spaces, let v be an element of V and let W be a K–linear subspace of V. If $f(v)$ belongs to $f(W)$ for all E–linear maps $f : V \longrightarrow V_0$, then v belongs to W.*

PROOF. Without loss of generality we may suppose that V_0 is E, so we are just considering E–linear forms $f : V \longrightarrow E$. Let $\mathrm{tr}_{E|K} : E \longrightarrow K$ be a trace map, which for us can be just any K–linear map with the property

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

Such a trace map always exists (that is quite standard, see e.g. [**GS06**] section 2.6). Consider then the K–linear map

$$\begin{array}{ccc} \mathrm{Hom}_E(V, E) & \longrightarrow & \mathrm{Hom}_K(V, K) \\ f & \longmapsto & \mathrm{tr}_{E|K} \circ f \end{array}$$

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 of course suppose that $V = E$ is 1–dimensional over 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 $y \longmapsto \mathrm{tr}(yx)$. If this map is zero, then x must be zero by the above property of the trace, hence injectivity. But now, our hypothesis on v implies that

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

for all $f \in \mathrm{Hom}_E(V, E)$, hence $f(v) \in f(W)$ for all $f \in \mathrm{Hom}_K(V, K)$, hence $v \in W$ by "ordinary" linear algebra. □

LEMMA 7.4.4. *Let K be a field of characteristic zero and let E be a finite dimensional semisimple algebra over K. Let V and V_0 be finite dimensional E–modules where V_0 is faithful, let v be an element of V and let W be a K–linear subspace of V of dimension ≤ 1. If $f(v)$ belongs to $f(W)$ for all E–linear maps $f : V \longrightarrow V_0$, then v belongs to W.*

PROOF. Let w be a generator for W. Decompose V as a direct sum of simple E–modules $V = V_1 \oplus \cdots \oplus V_n$, and write $w = w_1 + \cdots + w_n$ and $v = v_1 + \cdots + v_n$ according to this decomposition. Each of the simple E–modules V_i appears as a direct factor of V_0 because V_0 is faithful. We must show that there is a $\lambda \in K$ such that $v = \lambda w$, i.e. $v_i = \lambda w_i$ for all i.
Let $f_i : V \longrightarrow V_0$ be a E–module map which is injective on V_i and zero on V_j for $j \neq i$. By

hypothesis, there exists $\lambda_i \in K$ such that $f_i(v) = f_i(\lambda_i w)$. By our choice of f_i, this means $v_i = \lambda_i w_i$, so that we get

$$v = v_1 + \cdots + v_n = \lambda_1 w_1 + \cdots + \lambda_n w_n$$

we must show that we can chose all the λ_i's equal to one $\lambda \in K$. Observe that if $w_i = 0$, then $v_i = 0$ and we can chose any λ_i we wish. Let us thus suppose that at least one of the w_i's, say w_1 is not zero. Set $\lambda := \lambda_1$, suppose by induction that we have already $\lambda_2 = \cdots = \lambda_{i-1} = \lambda$, and let us show that we can also arrange $\lambda_i = \lambda$. Once we have this, the lemma is proven. Again, if $w_i = 0$, this is trivially possible, so let us suppose that $w_i \neq 0$. We have now two possibilities: Either V_i is isomorphic to V_1, or it is not.

<u>Case 1</u>: V_1 *is isomorphic to* V_i. In this case, choose a simple factor of V_0 isomorphic to V_1 and V_i, and let $f_1 : V \longrightarrow V_0$ be as before. Chose an E–module isomorphism $\varphi : V_i \longrightarrow V_1$, and let $f_i' : V \longrightarrow V_0$ be the E–module map which is $f_1 \circ \varphi$ on V_i and zero on all other factors. As above, we have $v_i = \lambda_i' w_i$ for some $\lambda_i' \in K$. Consider then the E–module map $f := f_1 + f_i'$. There exists by hypothesis a scalar $\mu \in K$ such that $f(v) = f(\mu w)$, and we have $f(v) = f_1(v_1 + \varphi(v_i))$ and $f(\mu w) = f_1(\mu w_1 + \mu\varphi(w_i))$ by definition, hence since f_1 is injective on V_1

$$\lambda w_1 + \lambda_i'\varphi(w_i) = v_1 + \varphi(v_i) = \mu w_1 + \mu\varphi(w_i)$$

If w_1 and $\varphi(w_i)$ are K–linearly independent, this implies that $\mu = \lambda$ and $\mu = \lambda_2$, hence $\lambda_2 = \lambda$. Otherwise, there is a nonzero scalar $\alpha \in K$ such that $\varphi(w_i) + \alpha w_1 = 0$. Considering the E–linear map $g : V \longrightarrow V_0$ given by αf_1 on V_1 and $f_1 \circ \varphi$ on V_i, we see that $g(w) = 0$, hence $g(v) = 0$, that is, $\varphi(v_i) + \alpha v_1 = 0$. Hence

$$\lambda\alpha w_1 = \alpha v_1 = -\varphi(v_1) = -\varphi(\lambda_i' w_i) = \lambda_i \alpha w_1$$

Canceling the nonzero vector αw_1 yields again $\lambda = \lambda_i$, and we are done with this case.

<u>Case 2</u>: V_1 *is not isomorphic to* V_i. Let f_1 and f_i as above, and consider $f := f_1 + f_2$. There exists a $\mu \in K$ such that $f(v) = f(\mu w)$, hence $f(v_1 + v_2) = f(\mu w_1 + \mu w_2)$. Because V_1 and V_i are not isomorphic, the images of the maps f_1 and f_i have trivial intersection, hence f is injective on $V_1 \oplus V_i$. Thus

$$\lambda w_1 + \lambda_i w_i = v_1 + v_2 = \mu w_1 + \mu w_i$$

Since w_1 and w_i are K–linearly independent, this shows that $\mu = \lambda$ and $\mu = \lambda_2$, hence $\lambda_2 = \lambda$. □

Proof of Theorem 7.4.1. Let $M = [Y \longrightarrow G]$ be a 1–motive with torsion over k satisfying one of the conditions in the theorem. Recall from Proposition 5.5.2 that if M' is a 1–motive isogenous to M, then $Ш^1(k, \mathbb{T}_\ell M)$ is finite if and only if $Ш^1(k, \mathbb{T}_\ell M')$. Hence, in order to prove finiteness of $Ш^1(k, \mathbb{T}_\ell M)$ we may without loss of generality replace M by an isogenous torsion free 1–motive which then satisfies the same condition. We can as well, also by Proposition 5.5.2 replace k by a finite extension k' over which Y is constant and prove finiteness of $Ш^1(k', M)$ instead. Let us from now on suppose that M is torsion free and Y constant.

As in Proposition 7.3.1 define the following objects

$$V := D_M(k) \otimes \mathbb{Q}_\ell \qquad\qquad W := u(Y) \otimes \mathbb{Q}_\ell \qquad\qquad E := \operatorname{End}_k G \otimes \mathbb{Q}_\ell$$

and set

$$\overline{W} := \left\{ v \in V \;\middle|\; f(v) \in f(W) \text{ for all } f \in \operatorname{Hom}_E(V, \mathrm{V}_\ell G) \right\}$$

We claim that by our hypothesis on M the equality $W = \overline{W}$ holds. Indeed, if M satisfies condition (1) in the statement of the theorem, then E is a division algebra, hence $W = \overline{W}$ by Lemma 7.4.3. If M satisfies condition (2), then the equality $W = \overline{W}$ holds by Lemma 7.4.4. Now, Proposition 7.3.1 shows that

$$H^1_*(L^M, \mathrm{V}_\ell M) \cong \overline{W}/W = 0$$

To say that $H^1_*(\Gamma, \mathrm{V}_\ell M)$ is trivial is the same as to say that $H^1_*(\Gamma, \mathrm{T}_\ell M)$ is finite, and by Proposition 5.4.4 we have an injection $Ш^1(k, \mathrm{T}_\ell M) \longrightarrow H^1_*(\Gamma, \mathrm{T}_\ell M)$, hence finiteness of $Ш^1(k, \mathrm{T}_\ell M)$.
Coming back to a general 1–motive with torsion over any number field k, the additional statements of the theorem are just a repetition of Corollary 4.2.7. □

Remark 7.4.5. Surely there are interesting conditions on E other than being a division algebra, and also interesting conditions on W, or maybe $\mathrm{V}_\ell G$ which ensure that equality $\overline{W} = W$ holds. For instance, what happens if E is commutative, or say, a product of division algebras? We didn't yet fully explore the consequences of Proposition 7.3.1. Sadly, my time is up.

CHAPTER 8

Congruence problems

In this chapter we investigate the question whether a finitely generated subgroup of the group of rational points of an semiabelian variety is characterized by its reductions modulo sufficiently many prime ideals.
Let G be a semiabelian variety over a number field k, let X be a finitely generated subgroup of $G(k)$ and let $P \in G(k)$ be a point. We want to "decide" whether P belongs to X or not. Choose an open subscheme U of $\operatorname{spec} \mathcal{O}_k$, such that there is a model of G over U and such that P and all points in X extend to U–points (which is possible because X is finitely generated). A necessary condition for P belonging to X is that for all prime ideals $\mathfrak{p} \in U$ the reduction of P modulo $\mathfrak{p}$ belongs to the reduction of X modulo $\mathfrak{p}$. The question whether this condition is also sufficient, formulated by W. Gajda in 2002 for abelian varieties, was named the problem of detecting linear dependence in Mordell–Weil groups. The answer is no in general, as we shall see in the next section.

THEOREM 8.0.1. *Let k be a number field, let $U \subseteq \operatorname{spec} \mathcal{O}_k$ be a nonempty open subscheme and let G be a semiabelian scheme over U. Let $X \subseteq G(U)$ be a subgroup, and let $M = [u : Y \longrightarrow G]$ be a 1–motive with constant lattice Y such that $u(Y) = X$. Let S be a set of closed points of U of density 1. Consider*

$$X \subseteq \overline{X} := \Big\{ P \in G(U) \;\Big|\; \operatorname{red}_\mathfrak{p}(P) \in \operatorname{red}_\mathfrak{p}(X) \qquad \text{for all } \mathfrak{p} \in S \Big\}$$

The quotient $\overline{X}/X$ is a finitely generated free group. For every prime ℓ, its rank is less or equal to the dimension of $H^1_*(L^M, \mathrm{V}_\ell M)$. In particular if $H^1_*(L^M, \mathrm{V}_\ell M) = 0$, then equality $X = \overline{X}$ holds.

The way we formulate the theorem, we don't have to say that X is finitely generated, since the group of U–points $G(U)$ is itself already finitely generated (Proposition 3.3.11). Presumably the dimension of $H^1_*(L^M, \mathrm{V}_\ell M)$ is independent of ℓ, but we don't know this for sure. We also wonder whether the rank of $\overline{X}/X$ may be strictly less than the dimension of $H^1_*(L^M, \mathrm{V}_\ell M)$. Proposition 7.3.1 and Lemma 7.4.3 yield then

COROLLARY 8.0.2. *Let k be a number field and let G be a simple abelian variety or a 1–dimensional torus over k. Let X be a finitely generated subgroup of $G(k)$ and let $P \in G(k)$ be a rational point. If $(P \bmod \mathfrak{p}) \in (X \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of k, then P belongs to X.*

For the multiplicative group $G = \mathbb{G}_m$ this is a theorem of Schinzel, but for abelian varieties this is new, even for elliptic curves. In the last section of this chapter we give an example showing that for nonsimple abelian varieties the statement is wrong in general. Before we prove Theorem 8.0.1, we give a short account on the problem of "detecting linear dependence" in the next section.

8.1. Historical overview

Several special cases of Theorem 8.0.1 already exist in the literature. In this section I give a short and certainly incomplete overview on these. All papers cited there use more or less the same techniques: They deal with Kummer theory on abelian varieties or on the multiplicative group, and make use at least once of a density theorem. Kowalski's paper [**Kow03**] contains a detailed discussion of this technique and relates problems. Our approach is different, insofar as we use Kummer theory and density theorems only *via* our computation of $H^1_*(L^M, \mathrm{T}_\ell M)$.

The first step towards our theorem was probably taken by A. Schinzel in [**Sch60**] by answering affirmatively the following question. Let P and Q be nonzero integers. Suppose that modulo almost all prime numbers p, we have $P \equiv Q^n$ modulo p for some integer n depending on p. Is then P a power of Q? Indeed, this is precisely the setup of our theorem for

$$k = \mathbb{Q}, \qquad U = \operatorname{spec}\mathbb{Z}[P^{-1}, Q^{-1}], \qquad G = \mathbb{G}_m, \qquad P = P, \qquad X = \{Q^n \mid n \in \mathbb{Z}\}$$

In [**Sch75**] the more general case of an arbitrary number field and an arbitrary finitely generated subgroup $X \leq \mathbb{G}_m(k)$ is treated. This is as well shown in [**Kha03**].

The problem of detecting subgroups by reductions is closely related to the so–called *support problem*, suggested by P. Erdős at the 1988 number theory conference in Banff. In our own formulation, Erdős asked the following: Let P and Q be nonzero integers. Suppose that the implication

$$P^n \equiv 1 \mod p \implies Q^n \equiv 1 \mod p$$

holds for almost all prime numbers p not dividing PQ and all integers n. Is then P a power of Q? This hypothesis is of course weaker than the one in Schinzel's problem. In [**CRS97**], C. Corrales-Rodrigáñez and R. Schoof answer affirmatively Erdős's original question, as well as the analogue of it for elliptic curves. This was subsequently generalized by M. Larsen to abelian varieties in [**Lar03**]. It then takes the following form: Let P and Q be rational points of an abelian variety A over k, and suppose that the implication

$$nP \equiv 0 \mod \mathfrak{p} \implies nQ \equiv 0 \mod \mathfrak{p}$$

holds for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$ where A has good reduction and for almost all integers $n \geq 1$. Then, there exists an endomorphism ψ of A and an integer $m \geq 1$ such that $\psi P = mQ$. It is made clear in [**LS06**] that the integer m is really needed, at least for non–simple abelian varieties.

The question whether the statement of Corollary 8.0.2 holds for all abelian varieties was first formulated by W. Gajda in 2002. A first result was obtained by T. Weston shortly after the question was asked in [**Wes03**], where it is shown that if A is an abelian variety over a number field k with *commutative* endomorphism ring, then the relation

$$P \mod \mathfrak{p} \quad \in \quad X \mod \mathfrak{p} \qquad\qquad \text{for almost all } \mathfrak{p}$$

for a subgroup X of $A(k)$ and a point $P \in A(k)$ implies that $P \in X + A(k)_{\mathrm{tor}}$. Our theorem fixes this torsion ambiguity.

In [**KP04**], the authors discuss an analogous problem which deals not with reducing subgroups, but with reducing endomorphisms. Especially noteworthy is Lemma 5 in *loc.cit.*, which can also be used to get rid of the torsion insecurity in Weston's theorem in the case when X is generated by a single element.

In [**BGK05**] and [**GG09**], a statement as in Corollary 8.0.2 is proven for abelian varieties under various technical assumptions. For instance, Theorem B of [**GG09**] states that if A is an abelian variety over k, then the statement of Corollary 8.0.2 holds in the case where X is a free $\mathrm{End}_k A$–module and P generates a free $\mathrm{End}_k A$–module. W. Gajda has informed me that he found independently a proof of Corollary 8.0.2 using different methods. In a recent preprint

([**BK09**]) Banaszak and Krasoń solve this problem for abelian varieties satisfying a certain "growth condition" and modulo some torsion ambiguity. Again, our theorem eliminates all problems with torsion elements.

Our theorem also answers partially Problem 1.1 of [**Kow03**] for semiabelian varieties. It asks whether a local to global principle as in our main theorem holds for a general algebraic group G over k in the case where X is generated by a single element. Kowalski shows that this holds for the multiplicative group for elliptic curves. Proposition 3.2 of *loc.cit.* shows that if an algebraic group G contains the additive group, then the principle fails.

The most precise results so far have been obtained by A. Perucca in [**Per08**], where Gajda's question is answered positively for split semiabelian varieties in three cases: The case when X is cyclic, the case when X is a free left $\mathrm{End}_k G$–submodule of $G(k)$, and the case where X has a set of generators (as a group) which is a basis of a free left $\mathrm{End}_k G$–submodule of $G(k)$. Moreover, it is proven in *loc.cit* that there exists an integer m depending only on G, k and the rank of X such that mP belongs to the left $\mathrm{End}_k G$–submodule of $G(k)$ generated by X.

8.2. Detecting linear dependence

In this section we prove Theorem 8.0.1. We keep fixed a number field k, an open $U \subseteq \operatorname{spec} \mathcal{O}_k$ and a set S of closed points of U of density 1. Let $X \leq G(U)$ and $M = [u : Y \longrightarrow G]$ be as in the theorem. The basic idea is to construct for each prime ℓ an injection

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

Since Y is constant, $H^1_*(L^M, \mathrm{T}_\ell M)$ is torsion free by Proposition 5.4.11. Thus, the existence of an injection as above tells us that $\overline{X}/X$ is of rank less than the $\mathbb{Z}_\ell$–rank of $H^1_*(L^M, \mathrm{T}_\ell M)$ i.e. the dimension of $H^1_*(L^M, \mathrm{V}_\ell M)$, and moreover that $\overline{X}/X$ has no ℓ–torsion. Hence, if for *each* ℓ we find an injection as above, the theorem is proven. At some point it will be more comfortable to work with an invariant

$$Ш^1_S(U, \mathrm{T}_\ell M)$$

in place of $H^1_*(L^M, \mathrm{T}_\ell M)$, which will of course turn out to be isomorphic to $H^1_*(L^M, \mathrm{T}_\ell M)$. We begin with defining this object:

Definition 8.2.1. Let U be an open subscheme of $\operatorname{spec} \mathcal{O}_k$, let ℓ be a prime number invertible on U, and let S be a set of prime ideals of $\mathcal{O}_k$ corresponding to points of U. Let T be an ℓ–adic sheaf on U. We define

$$Ш^1_S(U, T) := \ker\left(H^1(U, T) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(\kappa_\mathfrak{p}, T_\mathfrak{p})\right)$$

where $T_\mathfrak{p}$ denotes the pull–back of T over $\kappa_\mathfrak{p}$, the residue field at $\mathfrak{p}$.

Proposition 8.2.2. *Notation being as in Definition 8.2.1, if S is of density 1, then there is a canonical isomorphism*

$$Ш^1_S(U, T) \xrightarrow{\cong} H^1_*(\Gamma, T)$$

Proof. The arguments are exactly the same as in Proposition 5.4.4 and Lemma 5.4.5, so I re–explain only briefly how this works. Let $\pi_U := \pi_1^{\text{ét}}(U, \overline{k})$ be the étale fundamental group of U. The action of Γ on T factors over π_U, and we can identify the étale cohomology group $H^1(U, T)$ with the continuous Galois cohomology group $H^1(\pi_U, T)$. By Proposition 5.4.3 we have a canonical isomorphism $H^1_*(\Gamma, T) \cong H^1_*(\pi_U, T)$ via inflation. Considering $Ш^1_S(U,T)$ and $H^1_*(\Gamma,T)$ both as subgroups of $H^1(\pi_U,T)$, equality holds. Indeed, the inclusion $\subseteq$ holds by Frobenius's density theorem, and the inclusion $\supseteq$ holds because all decomposition groups in π_U corresponding to places in S (hence corresponding to closed points of U) are monogenous. □

Corollary 8.2.3. *Let $M = [Y \longrightarrow G]$ be a torsion free 1–motive over U, and let S be of density 1. If Y is constant, then $Ш^1_S(U, \mathrm{T}_\ell M)$ is a free $\mathbb{Z}_\ell$–module of rank equal than the dimension of $H^1_*(L^M, \mathrm{V}_\ell M)$.*

Proof. This follows from Proposition 8.2.2 and Proposition 5.4.11 (and 5.1.8). □

Proof of the Theorem. We are given a semiabelian scheme G over U and a subgroup X of $G(U)$. By Proposition 3.3.11, $G(U)$ and hence X are finitely generated. Let us fix a set of primes S of density 1, all corresponding to closed points of U. For $\mathfrak{p} \in S$, we write $\kappa_\mathfrak{p}$ for the residue field $\mathcal{O}_k/\mathfrak{p}$ and $P_\mathfrak{p}$ and $X_\mathfrak{p}$ for the reduction of P and X modulo $\mathfrak{p}$. Since X is a finitely generated group, we can choose a 1–motive $M = [u : Y \longrightarrow G]$ over U, such that Y is torsion free and constant and such that the image of u on U–points is X. The image of $Y \longrightarrow G_\mathfrak{p}(\kappa_\mathfrak{p})$ is then $X_\mathfrak{p}$. Recall that we consider the group

$$\overline{X} := \left\{ P \in G(U) \;\middle|\; P_\mathfrak{p} \in X_\mathfrak{p} \text{ for all } \mathfrak{p} \in S \right\}$$

Of course X is contained in $\overline{X}$. Fix a prime number ℓ. Without loss of generality we can eliminate from S some finitely many places and also restrict G and X to a smaller open contained in U. We may thus suppose that ℓ is invertible on U. In order to prove the theorem, it suffices by Corollary 8.2.3 to produce an injection

$$\overline{X}/X \otimes \mathbb{Z}_\ell \longrightarrow Ш^1_S(U, \mathrm{T}_\ell M)$$

Consider the following diagram with exact rows

$$\begin{tikzcd}
\cdots \arrow[r] & Y \arrow[r, "u_U"] \arrow[d, equal] & G(U) \arrow[r] \arrow[d] & H^0(U,M) \arrow[r] \arrow[d] & 0 = H^1(U,Y) \\
\cdots \arrow[r] & Y \arrow[r, "u_\mathfrak{p}"] & G_\mathfrak{p}(\kappa_\mathfrak{p}) \arrow[r] & H^0(\kappa_\mathfrak{p}, M_\mathfrak{p}) \arrow[r] & 0 = H^1(\kappa_\mathfrak{p}, Y)
\end{tikzcd}$$

From this we see that $\overline{X}$ is the set of points $P \in G(U)$ that map to zero in $H^1(\kappa_\mathfrak{p}, M_\mathfrak{p})$ for all $\mathfrak{p} \in S$. Hence

$$\overline{X}/X \xrightarrow{\cong} \ker\left(H^0(U,M) \xrightarrow{\alpha} \prod_{\mathfrak{p}\in S} H^0(\kappa_\mathfrak{p}, M_\mathfrak{p}) \right)$$

Now, take tensor products with $\mathbb{Z}_\ell$ everywhere. Mind that, since $\mathbb{Z}_\ell$ is flat over $\mathbb{Z}$, the functor $- \otimes_\mathbb{Z} \mathbb{Z}_\ell$ is exact. Permuting $- \otimes \mathbb{Z}_\ell$ with the product may only increase the kernel, hence an injection

$$\overline{X}/X \otimes \mathbb{Z}_\ell \longrightarrow \ker\left(\alpha_\ell : H^0(U,M) \otimes \mathbb{Z}_\ell \longrightarrow \prod_{\mathfrak{p}\in S} \left(H^0(\kappa_\mathfrak{p}, M_\mathfrak{p}) \otimes \mathbb{Z}_\ell \right) \right)$$

We are now left with finding an injection $\ker \alpha_\ell \longrightarrow Ш^1_S(U, \mathrm{T}_\ell M)$ To this end, we consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & H^0(U,M) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\alpha_\ell"'] & H^1(U, \mathrm{T}_\ell M) \arrow[r] \arrow[d] & \mathrm{T}_\ell H^1(U,M) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod H^0(\kappa_\mathfrak{p}, M_\mathfrak{p}) \otimes \mathbb{Z}_\ell \arrow[r] & \prod H^1(\kappa_\mathfrak{p}, \mathrm{T}_\ell M_\mathfrak{p}) \arrow[r] & \prod \mathrm{T}_\ell H^1(\kappa_\mathfrak{p}, M_\mathfrak{p}) \arrow[r] & 0
\end{tikzcd}$$

The rows come from the filtration on the cohomology of the Tate module introduced in 2.2.9. The ℓ–adic completions are here just ordinary tensor products because the involved groups are all finitely generated. The kernel of the second vertical map is $Ⲇ^1_S(U, \mathrm{T}_\ell M)$, hence the desired injection, and the theorem is proven. $\square$

8.3. Examples

In this section we give explicit examples to theorems in this chapter. The first one is an example of an abelian variety and a subgroup of its group of rational points for which the "detecting linear dependence" problem has a negative answer. This example is joint work with Antonella Perucca. The second example provides a 1-motive M and a set of places S such that $H^1_S(k, \mathrm{T}_\ell M)$ is infinite and $Ш^1(k, \mathrm{T}_\ell M)$ finite.

Example 1: Infirming the "detecting linear dependence" problem. Let k be a number field and let E be an elliptic curve without complex multiplication over k such that there are points P_1, P_2, P_3 in $E(k)$ which are $\mathbb{Z}$–linearly independent. Let $P \in E^3(k)$ and $X \subseteq E^3(k)$ be the following:

$$P := \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \qquad \text{and} \qquad X := \Big\{ MP \mid M \in \mathbb{M}_{3\times 3}(\mathbb{Z}) \text{ with } \operatorname{tr} M = 0 \Big\}$$

So the group X consists of the images of the point P under all endomorphisms of E^3 with trace zero. Since the points P_i are $\mathbb{Z}$–linearly independent and since E has no complex multiplications, the point P does not belong to X.

Claim. *Let $\mathfrak{p}$ be a prime of k where E has good reduction. The image of P under the reduction map modulo $\mathfrak{p}$ belongs to the image of X.*

For the rest of this section, we fix a prime $\mathfrak{p}$ of good reduction for E. We write κ for the residue field of k at $\mathfrak{p}$. To ease notation we now write E for the reduction of E modulo $\mathfrak{p}$ (for some fixed model), and let P_i and P denote the given points modulo $\mathfrak{p}$. Our aim is to find an integer matrix M of trace zero such that $P = MP$ in $E^3(\kappa)$.

Let α_1 be the smallest positive integer such that $\alpha_1 P_1$ is a linear combination of P_2 and P_3. Similarly define α_2 and α_3 for P_2 and P_3 respectively. There are integers m_{ij} such that

$$\begin{aligned} \alpha_1 P_1 + m_{12} P_2 + m_{13} P_3 &= O \\ m_{21} P_1 + \alpha_2 P_2 + m_{23} P_3 &= O \\ m_{31} P_1 + m_{32} P_2 + \alpha_3 P_3 &= O \end{aligned}$$

Assume that the greatest common divisor of α_1, α_2 and α_3 is 1 (we prove this assumption later). By Bezout's theorem we can thus find integers a_1, a_2, a_3 such that

$$3 = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3$$

Write then $m_{ii} := 1 - \alpha_i a_i$, so that in particular $m_{11} + m_{22} + m_{33} = 0$. We now find by construction the equality

$$\begin{pmatrix} m_{11} & -a_1 m_{12} & -a_1 m_{13} \\ -a_2 m_{21} & m_{22} & -a_2 m_{13} \\ -a_3 m_{31} & -a_3 m_{32} & m_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$$

Notice that the above matrix has trace zero. Hence we are left to prove that the greatest common divisor of α_1, α_2 and α_3 is indeed 1.

Fix a prime number ℓ and let us show that ℓ does not divide $\gcd(\alpha_1, \alpha_2, \alpha_3)$. Suppose on the contrary that ℓ divides $\gcd(\alpha_1, \alpha_2, \alpha_3)$. This is equivalent with saying that ℓ divides all the coefficients appearing in any linear relation between P_1, P_2 and P_3. In particular, this implies that ℓ divides the order of P_1, P_2 and P_3 in $E(\kappa)$.

Recall (e.g. from [**Sil86**] Corollary III.6.4) that the group $E(\kappa)[\ell]$ is either trivial, isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. In any case, the intersection $X \cap E(\kappa)[\ell]$ is generated by two elements or less. Without loss of generality, let us suppose that P_2 and P_3 generate $X \cap E(\kappa)[\ell]$. We are supposing that ℓ divides all the coefficients appearing in any linear relation of the points. Let $\alpha_1 = x_1\ell$ and write $x_1\ell P_1 + x_2\ell P_2 + x_3\ell P_3 = O$ for some integers x_2 and x_3. It follows that

$$x_1P_1 + x_2P_2 + x_3P_3 = T$$

for some point T in $X \cap E(\kappa)[\ell]$. The point T is a linear combination of P_2 and P_3. This contradicts the minimality of α_1.

Example 2: Schinzel's 1–motive. We consider the 1–motive $M := [u : \mathbb{Z}^3 \longrightarrow \mathbb{G}_m^2]$ over $U = \operatorname{spec} \mathbb{Z}[\frac{1}{6}]$ (or over the field of rational numbers $k = \mathbb{Q}$) given by

$$u(x, y, z) = \begin{pmatrix} 2^x 3^y \\ 2^y 3^z \end{pmatrix}$$

The subgroup $X := u(\mathbb{Z}^3)$ of $\mathbb{G}_m^2(k)$ provides an example of a subgroup which can not be detected my means of reductions modulo primes. Indeed, a calculation analogous to what we did in the first example shows that the point $P := \binom{1}{2}$ belongs to the reduction of X modulo all primes $p \neq 2, 3$, but does not belong to X. This was found by Schinzel in [**Sch75**], so let us call this 1–motive *Schinzel's 1–motive*. The analogue of Theorem 7.2.2 for tori shows that $D_M(k)$ is the $\operatorname{End}_k G = \mathbb{M}_{2\times 2}(\mathbb{Z})$–submodule of $G(U) \subseteq G(k)$ given by

$$D_M(k) = \left\{ \begin{pmatrix} 2^x 3^y \\ 2^z 3^w \end{pmatrix} \;\middle|\; x, y, z, w \in \mathbb{Z} \right\}$$

We now compute $H^1_*(\Gamma, \mathrm{T}_\ell M)$ using Proposition 7.3.1. To this end, fix a prime number ℓ and introduce

$$V := D_M(k) \otimes \mathbb{Q}_\ell \qquad W := u(\mathbb{Z}^3) \otimes \mathbb{Q}_\ell \qquad E := \operatorname{End}_k G \otimes \mathbb{Q}_\ell \cong \mathbb{M}_{2\times 2}(\mathbb{Q}_\ell)$$

As an E–module, V can be identified with $\mathbb{M}_{2\times 2}(\mathbb{Q}_\ell)$ and W with the subspace of V consisting of self adjoint matrices. An elementary matrix calculation shows that

$$\overline{W} := \left\{ v \in V \;\middle|\; f(v) = f(w) \text{ for some } w \text{ with } w = w^t, \text{ for all } f \in \operatorname{Hom}_E(V, \mathbb{Q}_\ell^2) \right\}$$

is equal to V. Hence $\overline{W}/W \cong H^1_*(L^M, \mathrm{V}_\ell M)$ is 1–dimensional. Since $H^1_*(L^M, \mathrm{T}_\ell M)$ is torsion free by 5.4.11 we have $H^1_*(L^M, \mathrm{T}_\ell M) \cong \mathbb{Z}_\ell$, hence Lemma 5.4.5 shows that

$$H^1_S(k, \mathrm{T}_\ell M) \cong \mathbb{Z}_\ell$$

where S is any set of places of k not containing 2 or 3. Hence, Schinzel's 1–motive is an example of a 1–motive with infinite $H^1_S(k, M)$. A little bookkeeping shows that a cocycle $c : \Gamma \longrightarrow \mathrm{T}_\ell M$ representing a generator for $H^1_S(k, \mathrm{T}_\ell M)$ is given by

$$c(\sigma) = \begin{pmatrix} 0 \\ (\sigma\zeta_i - \zeta_i)_{i=0}^\infty \end{pmatrix} \quad \in \mathbb{Z}_\ell(1)^2 \subseteq \mathrm{T}_\ell M$$

where $(\zeta_i)_{i=0}^\infty$ is a sequence of ℓ–th roots of 2 in $\overline{k}^*$, that is $\zeta_0 = 2$ and $\zeta_i^\ell = \zeta_{i-1}$. Let us now check that nevertheless $Ш^1(k, \mathrm{T}_\ell M)$ is finite, and in fact, trivial. To do this we must, as we shall see in a moment, again solve a congruence problem but this time we shall not only consider reductions modulo almost all primes, but reductions modulo all prime powers.

Let Ω be the set of all places of k, and consider once again the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(U,M)\otimes\mathbb{Z}_\ell & \longrightarrow & H^1(U,\mathrm{T}_\ell M) & \longrightarrow & \mathrm{T}_\ell H^1(U,M) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod H^0(k_v,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell & \rightarrow & \prod H^1(k_v,\mathrm{T}_\ell M) & \longrightarrow & \prod \mathrm{T}_\ell H^1(k_v,M) & \longrightarrow & 0 \end{array}$$

the products running over Ω. The right hand map is injective, indeed, the kernel of this map is contained in $\mathrm{T}_\ell D^1(U,M)$, and we know that $D^1(U,M)$ is finite by Proposition 4.3.11 (there is no abelian part here). Thus, the kernels of the left hand and the middle vertical map are isomorphic. But the kernel of the middle vertical map can be identified with those elements of $H^1_S(k,\mathrm{T}_\ell M)$ mapping to zero in $H^1(k_v,\mathrm{T}_\ell M)$ for all $v\notin S$ as well, which is precisely $\text{Ш}^1(k,\mathrm{T}_\ell M)$. Hence an isomorphism

$$\text{Ш}^1(k,\mathrm{T}_\ell M)\cong\ker\left(H^0(U,M)\otimes\mathbb{Z}_\ell\xrightarrow{\alpha_\ell}\prod_{v\in\Omega}H^1(k_v,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell\right)$$

Instead of working with one prime ℓ at a time, let us work with all ℓ simultaneously, by taking in the above expression products over ℓ. We don't do this just because it looks fancier, but for a reason. Working with all ℓ simultaneously brings into play a nontrivial global information, namely that the kernel of each of the α_ℓ is generated by the class of $P:=\binom{1}{2}\in G(U)$ in $H^1(U,M)\otimes\mathbb{Z}_\ell$, *independently* of ℓ. Taking products over all primes ℓ as we said yields an isomoprhism

$$\prod_\ell\text{Ш}^1(k,\mathrm{T}_\ell M)\cong\ker\left(H^0(U,M)\otimes\widehat{\mathbb{Z}}\xrightarrow{\widehat{\alpha}}\prod_{v\in\Omega}\prod_\ell H^1(k_v,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell\right)$$

where $\widehat{\mathbb{Z}}$ denotes the the profinite completion of $\mathbb{Z}$, also known as the Prüfer ring. The kernel of $\widehat{\alpha}$ is generated by the class of P in $H^0(U,M)\otimes\widehat{\mathbb{Z}}$ (this is our global information). Observe now that an element of $H^0(U,M)\cong G(U)/\operatorname{im}u$, say represented by an element $Q\in G(U)$, maps to zero in $H^1(k_v,M)\,\widehat{\otimes}\,\mathbb{Z}_\ell$ if and only if the class of Q is ℓ–divisible in $H^1(k_v,M)$. Thus, in order to establish injectivity of the $\widehat{\alpha}$ and hence triviality of $\text{Ш}^1(k,\mathrm{T}_\ell M)$ for all ℓ we must show that for any integer $n\neq 0$, the class of $P^n=\binom{1}{2^n}\in H^0(k_v,M)\cong G(k_v)/\operatorname{im}u$ is indivisible. Taking Proposition 3.3.7 into account, must show that for any integer $n\neq 0$, the element $\binom{1}{2^n}$ of $G(k_v)=(k_v^*)^2$ is not in the closure of $X=\operatorname{im}u$ in $G(k_v)$. Yet in other words, we must show that if we can solve the equations

$$1\equiv 2^x3^y\mod p^m\qquad\text{and}\qquad 2^n\equiv 2^y3^z\mod p^m$$

modulo all prime powers p^m, (the prime p corresponding to the place v) then $n=0$. Considering only $p=3$ this implication already holds ($p=2$ doesn't do it and of all the other places we have already made use). Indeed, these congruences show that $2^n\equiv 1\bmod 3^m$, so either $n=0$ or n is bigger than the order of 2 in $\mathbb{Z}/3^m\mathbb{Z}$. This being for all $m\geq 0$, we must have $n=0$, and so we are done.

Conclusion: *Let $M=[\mathbb{Z}^3\longrightarrow\mathbb{G}_m^2]$ be Schinzels 1–motive over $k=\mathbb{Q}$, let ℓ be a prime and S be a set of places of k not dividing 6ℓ, of density 1. The group $H^1_S(k,\mathrm{T}_\ell M)$ is a free $\mathbb{Z}_\ell$–module of rank 1, in particular it is infinite. The group $\text{Ш}^1(k,\mathrm{T}_\ell M)$ is trivial for all ℓ, and hence $\text{Ш}^2(k,M^\vee)$ vanishes.*

REMARK 8.3.1. Most of this example is valid for any 1–motive of the form $[\mathbb{Z}^r\longrightarrow\mathbb{G}_m^d]$ over any number field. In particular, finiteness of $\text{Ш}^1(k,\mathrm{T}_\ell M)$ for all ℓ is equivalent with a positive answer to the congruence problem we just saw, involving all prime powers. The problem to make something general out of this is that last checking, which rapidly becomes complicated for more general 1–motives. For 1–motives of the form $[\mathbb{Z}^r\longrightarrow A^d]$ for a simple abelian variety A still much of this works, but one has to suppose finiteness of $\text{Ш}^1(k,A)$ at the moment Proposition 4.3.11 is used.

Ausblick

Instead of an afterword, I shall present here some open problems and questions.

QUESTION A.1. The first serious problem I have encountered in the course of this work, and which is still bogging me is the following: Let S be a reasonable base scheme and let F be a finite flat group scheme on S. We have seen in section 1.2 that $\mathcal{H}om(F, \mathbb{G}_m)$ is representable by the Cartier dual of F, and that the fppf–sheaf $\mathcal{E}xt^1(F, \mathbb{G}_m)$ is trivial. We also know that if the order of F is invertible on S, then the fppf–sheaves $\mathcal{E}xt^r(F, \mathbb{G}_m)$ are trivial for all $r \geq 1$. But if some of the residual characteristics of S divide the order of F, this need not to be true. There is an example by L.Breen, showing that if k is a field of characteristic p, then there is an isomorphism of étale sheaves

$$\mathcal{E}xt^p(\alpha_p, \mathbb{G}_m) \simeq \mathbb{G}_a$$

and it seems to us that Breen's example even shows that for any field k of characteristic p we have $\mathcal{E}xt^p(\alpha_p, \mathbb{G}_m) \simeq \mathbb{G}_a$ on the fppf–site over k. What can we say about the sheaves $\mathcal{E}xt^r(F, \mathbb{G}_m)$ in general? If S is the spectrum of a field, are they representable? And, given an F, is there an integer r_0 such that $\mathcal{E}xt^r(F, \mathbb{G}_m)$ is trivial for all $r > r_0$?

QUESTION A.2. Let S be a scheme, and write $\mathcal{M}_1$ (resp. $[\mathcal{M}_1]$) for the category of 1–motives (up to quasi–isomorphism) on S. What is the cohomological dimension of these categories? N. Mazzari has shown recently (see [**Maz08**]) that the category of Laumon 1–motives up to isogeny over a field of characteristic zero is of dimension 1. Is the same true for 1–motives with torsion? Closely related to this is the question after Hodge realizations of torsion 1–motives. Is there something like "mixed Hodge–structures with torsion" and if yes, is the realization functor (if it exists) from $[\mathcal{M}_1]$ to the category of mixed Hodge–structures with torsion of level ≤ 1 an equivalence of categories?

Thanks a lot again for your work,

QUESTION A.3. As I already mentioned in the introduction, the business of "dividing points on a semiabelian variety" is not entirely finished.

It would be interesting to have

Besides that we don't have a good description of the image of the Kummer injection $L^M_{G,Y} \longrightarrow \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G)$ (see Corollary 5.2.10), the following question remains open. Let $M = [Y \longrightarrow G]$ be a 1–motive over the number field k. On several occasions (proof of 6.1.3, proof of 7.2.2) we saw one or the other special case of the following diagram

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, hook] & G(k) \widehat{\otimes} \mathbb{Z}_\ell \arrow[r] \arrow[d, hook] & G(k_M) \widehat{\otimes} \mathbb{Z}_\ell \arrow[d, hook] \\
0 \arrow[r] & H^1(L^M, \mathrm{T}_\ell G) \arrow[r] & H^1(k, \mathrm{T}_\ell G) \arrow[r] & H^1(k_M, \mathrm{T}_\ell G)
\end{tikzcd}$$

where $k_M|k$ is the field extension with Galois group $\ker(\Gamma \longrightarrow \mathrm{GL}(\mathrm{T}_\ell M))$. Each time we had such a diagram, we have proven that the left hand injective map is an isomorphism, or at least has image of open index. Is this true in general, i.e. in the diagram above?

Question A.4. Many of the duality statements make also sense for other global fields. There seems to be no imminent reason why there should not be analogue theorems over function fields of curves over finite fields. For classical 1–motives, duality theorems have been obtained by C.D. Gonzales-Avilés in [**GA07**] and [**GAT08**]. It should be possible to take over most of our techniques we developed to characteristic p, provided that in the case $\ell = p$ one has to use flat cohomology instead of étale cohomology.

Question A.5. By 4.2.3 we have a pretty good idea how the group $Ш^0(k, M)$ behaves with respect to finite field extensions $k'|k$ and with respect to isogenies $M \longrightarrow M'$. By duality we can also understand how $Ш^2(k, M)$ behaves under these operations. What happens with $Ш^1(k, M)$? Can we describe how this group behaves under field extensions and isogenies, say under the hypothesis that this group is finite?

Bibliography

[And04] Y. Andre, *Une introduction aux motifs*, Panoramas et syntheses, vol. 17, Publications SMF, 2004.

[Beh03] K.A. Behrend, *Derived ℓ–adic categories for algebraic stacks*, no. 774, Memoirs of the AMS, 2003.

[BGK05] G. Banaszak, W. Gajda, and P. Krasoń, *Detecting linear dependence by reduction maps*, Journal of number theory **115** (2005), no. 2, 322–342.

[BK09] G. Banaszak and P. Krasoń, *On arithmetic in Mordell–Weil groups*, (to appear) **0** (2009), no. 0, 0.

[Bog81] F.A. Bogomolov, *Points of finite order on an abelian variety*, Math USSR Izv. **17** (1981), 55–72.

[Bou72] N. Bourbaki, *Groupes et algèbres de Lie*, Diffusion C.C.L.S., 1972.

[Bre69] L. Breen, *Extensions of abelian sheaves and Eilenberg-MacLane algebras*, Inv. Math. **9** (1969), 15–44.

[Bur05] D. Burde, *Lie–algebra kohomologie*, http://homepage.univie.ac.at/Dietrich.Burde/papers/ (2005), 1–1.

[Car85] J.A. Carlson, *The one-motif of an algebraic surface*, Compositio Mathematica **56** (1985), no. 3, 271–314.

[CRS97] C. Corrales-Rodrigánez and R. Schoof, *The support problem and its elliptic analogue*, Journal of Number Theory **64** (1997), no. 2, 276–290.

[Del74] P. Deligne, *Théorie de Hodge III*, Pub. math. IHES **44** (1974), 5–77.

[Eke90] T. Ekedahl, *On the adic formalism*, The Grothendieck Festschrift, vol. II, Birkhäuser, 1990, pp. 197–218.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Math. **73** (1983), 349–366.

[FC90] G. Faltings and C.L. Chai, *Degeneration of abelian varieties*, vol. 22, Ergebnisse der Math., no. 3, Springer Verlag, 1990.

[Fen94] Y. Fengsheng, *Tate property and isogeny estimate for semiabelian varieties*, Ph.D. thesis, Diss. ETH No. 10798, 1994.

[FK87] E. Freitag and R. Kiehl, *Etale cohomology and the Weil conjectures*, Ergebnisse der Math., vol. 13, Springer Verlag, 1987.

[GA07] C. D. Gonzalez-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, ArXiV:0709.4255v4 (2007), 1–33.

[GAT08] C. D. Gonzalez-Avilés and K. S. Tan, *The generalized cassels-tate dual exact sequence for 1-motives*, ArXiV:0806.0658v3 (2008), 1–16.

[GBH$^+$66] A. Grothendieck, I. Bucur, C. Houzel, L. Illusie, J.-P. Jouanolou, and J.-P. Serre, *Cohomologie ℓ–adique et fonctions L*, Lecture notes in Math., vol. 589, Springer Verlag, 1965/66.

[GG09] W. Gajda and K. Górnisiewicz, *Linear dependence in Mordell–Weil groups*, J. reine und angewandte Mathenmatik (2009), 1–15.

[Gre66] M. J. Greenberg, *Rational points in henselian discrete valuation rings*, Publications math. de l'Inst. Hautes Études Scientifiques (1966), no. 31, 59–64.

[Gro66a] A. Grothendieck, *Sga3*, Lecture notes in Math., vol. 589, Springer Verlag, 1965/66.

[Gro66b] ———, *Sga7*, Lecture notes in Math., vol. 589, Springer Verlag, 1965/66.

[GS06] Ph. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge studies in advanced mathematics, vol. 101, Cambridge University Press, 2006.

[Hin88] M. Hindry, *Autour d'une conjecture de Serge Lang*, Inventiones Math. **94** (1988), 575–603.

[Hoo42] R. Hooke, *Linear p–adic groups and their Lie algebras*, Ann. of Math. **43(4)** (1942), 641–655.

[HS05a] D. Harari and T. Szamuely, *Arithmetic duality theorems for 1–motives*, J. reine angew. Math. **578** (2005), 93–128.

[HS05b] ———, *Errata: Arithmetic duality theorems for 1–motives*, www.renyi.hu **1** (2005), 1–4.

[Ima76] H. Imai, *On the hodge groups of some abelian varieties*, Kōdai math. sem. rep. **27** (1976), 367–372.

[Jan88] U. Jannsen, *Continuous étale cohomology*, Math. Annalen **280** (1988), 207–245.

[Jan94] ———, *Mixed motives, Motivic cohomology and Ext–groups*, Proceedings of the ICM, vol. I, Birkhäuser, 1994, pp. 667–679.

[JR87] O. Jacquinot and K. Ribet, *Deficient points on extensions of abelian varieties by $\mathbb{G}_m$*, J. number theory **25** (1987), no. 2, 133–151.

[KBV08] B. Kahn and L. Barbieri-Viale, *On the derived category of 1-motives*, Arxiv.org (2008), 1–999.

[Kha03] C. Khare, *Compatible systems of mod p Galois representations and Hecke characters*, Math. Res. Letters **10** (2003), 71–83.

[Kos50] J.L. Koszul, *Homologie et cohomologie des algèbres de Lie*, Bull. Soc. Math. France **78** (1950), 65–127.

[Kow03] E. Kowalski, *Some local–global applications of Kummer theory*, Manuscripta mathematica **111** (2003), no. 1, 105–139.

[KP04] C. Khare and D. Prasad, *Reduction of homomorphisms mod p and algebraicity*, Journal of number theory **105** (2004), 322–332.

[KS06] M. Kashiwara and P. Schapira, *Categories and sheaves*, Grundlehren der mathematischen Wissenschaften, vol. 332, Springer, 2006.

[Lar03] M. Larsen, *The support problem for abelian varieties*, Journal of Number Theory **101** (2003), no. 2, 398–403.

[Laz65] M. Lazard, *Groupes analytiques p–adiques*, Pub. math. IHES **26** (1965), 5–219.

[LS06] M. Larsen and R. Schoof, *A refined counter–example to the support conjecture for abelian varieties*, Journal of Number Theory **116** (2006), no. 2, 396–398.

[Maz08] N. Mazzari, *Cohomological dimension of Laumon 1–motives up to isogeny*, arXiv:0809.4926v1 (2008), 1–11.

[MG96] Yu.I. Manin and S.I. Gelfand, *Methods of homological algebra*, Springer, 1996.

[Mil80] J.S. Milne, *Etale cohomology*, Princeton University Press, 1980.

[Mil08] ———, *Arithmetic duality theorems*, Academic press, 2008.

[MRS08] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, arXiv:math/0609066v2 (2008), 1–17.

[NSW00] J. Neukirch, A. Schmidt, and K. Wynerg, *Cohomology of number fields*, Grundl. math. Wiss., vol. 323, Springer, 2000.

[Oor66] F. Oort, *Commutative group schemes*, Lecture Notes Math., vol. 15, Springer, 1966.

[Per08] A. Perucca, *On the problem of detecting linear dependence for products of abelian varieties and tori*, preprint, arXiv:math/0811.1495v1 (2008), 1–9.

[PR05] M.A. Papanikolas and N. Ramachandran, *Extensions of abelian varieties defined over a number field*, J. Number Theory **112** (2005), 386–400.

[Ram98] N. Ramachandran, *From Jacobians to one-motives: Exposition of a conjecture of Deligne*, CRM Proceedings and Lecture Notes, vol. 24, AMS, 1998, pp. 1–19.

[Rib76] K. Ribet, *Dividing rational points on abelian varieties of CM–type*, Comp. math. **33(1)** (1976), 69–74.

[Rib87] ———, *Cohomological realization of a family of 1–motives*, J. number theory **25** (1987), no. 2, 152–161.

[Rot95] J. J. Rotman, *An introduction to the theory of groups*, 4 ed., Graduate texts in mathematics, vol. 148, Springer, 1995.

[Rus09] H. Russell, *1–motives with unipotent part*, preprint, arXiv:math/0902.2533v1 (2009), 1–22.

[Sch60] A. Schinzel, *On the congruence* $a^x \equiv b \mod n$, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astron. Phys. **8** (1960), 307–309.

[Sch75] ———, *On power residues and exponential congruences*, Acta Arithmetica **27** (1975), 397–420.

[Ser64] J-P. Serre, *Sur les groupes de congruence des variétés abéliennes*, Izv. Akad. Nauk. SSSR **28** (1964), 3–18.

[Ser68] ———, *Abelian* ℓ*–adic representations and elliptic curves*, Benjamin, New York, 1968.

[Ser71] ———, *Sur les groupes de congruence des variétés abéliennes II*, Izv. Akad. Nauk. SSSR **35** (1971), 731–735.

[Sha72] S.S. Shatz, *Profinite groups, arithmetic and geometry*, Princeton university press, 1972.

[Sil86] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986.

[Wei67] A. Weil, *Basic number theory*, Gr. math. Wiss., vol. 144, Springer, 1967.

[Wei94] C.A. Weibel, *An introduction to homological algebra*, Cambridge university press, 1994.

[Wes03] T. Weston, *Kummer theory of abelian varieties and reduction of mordell-weil groups*, Acta Arith. **110** (2003), 77–88.