Good reduction of 1-motives

Von der Universität Bayreuth
zur Erlangerung des Grades eines
Doktor der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

von

Tzanko Ivanov Matev

aus Pleven

1. Gutachter: Prof. Dr. Michael Stoll

2. Gutachter: Prof. Dr. Michael Dettweiler

3. Gutachter: Prof. Dr. René Schoof

Tag der Einreichung: 25.06.2013

Tag des Kolloquiums: 28.10.2013

Contents

Abstract

In this dissertation we study 1-motives over number fields and their application to questions dealing with reductions of points in semiabelian varieties. We prove a version of the Néron-Ogg-Shafarevich criterion for 1-motives and show how the image of the Frobenius in the ℓ-adic Galois representation associated to a 1-motive determines the ℓ-part of its reduction modulo the corresponding prime. We use this theory to investigate a family of properties for points in tori which we call *algebraic dependences*. In particular, we study the rank of the reduction of a group generated by two rational points in $\mathbb{G}_m^2$, modulo different primes. Finally, we show how our algebraic dependences exhibit an analogy between problems in p-adic transcendence theory and problems concerning reduction of points.

Kurzfassung

In dieser Doktorarbeit werden 1-Motive über Zahlkörpern und ihre Anwendung auf Fragen über die Reduktion von Punkten in semiabelschen Varietäten untersucht. Es wird eine Version des Néron-Ogg-Shafarevich-Kriteriums für 1-Motive bewiesen und es wird beschrieben, wie das Bild des Frobenius-Automorphismus in der dem 1-Motiv zugeordneten ℓ-adischen Galoisdarstellung die Reduktion modulo dem entsprechenden Primideal bestimmt. Wir wenden die von uns entwickelte Theorie an, um eine Familie von Eigenschaften für Punkte auf Tori zu untersuchen, die wir *algebraische Abhängigkeiten* nennen. Ins besondere wird der Rang der Reduktion modulo verschiedenen Primidealen einer von zwei rationalen Punkten in $\mathbb{G}_m^2$ erzeugten Gruppe untersucht. Schließlich wird gezeigt, dass unsere algebraischen Abhängigkeiten eine Analogie zwischen gewissen Probleme der p-adischen Transzendenztheorie und Problemen bezüglich Reduktion von Punkten vermitteln.

Introduction

The main topic of this dissertation is the study of the reduction of points in semiabelian varieties defined over number fields. We develop a formalism which allows us to easily reduce various problems of this type to problems about ℓ-adic Galois representations. We also apply this formalism to study a certain interesting family of properties of points on algebraic tori which we call *algebraic dependences*.

To be more specific let us give some examples of the type of problems to which our results can be applied. Our first example is related to Artin's primitive root conjecture. A weak form of the conjecture is as follows:

A. Conjecture. *Let a be an integer which is different from 0, 1, -1, and which is not a perfect square. There exist infinitely many prime numbers p for which a is a primitive root modulo p.*

Let a and p be as in the conjecture and let $n(a,p)$ denote the order of a modulo p. Then it is trivial to see that a is a primitive root modulo p if and only if the ℓ-adic valuations of $n(a,p)$ and $p-1$ are equal for all prime numbers ℓ. We can therefore fix a and ℓ, and ask for how many primes p the ℓ-adic valuation of $n(a,p)$ is equal to the ℓ-adic valuation of $p-1$. To answer this question one considers the Galois group of the extension $\mathbb{Q}(\sqrt[\ell]{a})/\mathbb{Q}$. This group is isomorphic to a semidirect product $\mathbb{Z}/\ell \rtimes (\mathbb{Z}/\ell)^\times$. One can show that if $p \neq \ell$, then the property stated above holds if and only if the prime p does not split completely in $\mathbb{Q}(\sqrt[\ell]{a})$, or equivalently, it holds if and only if the Frobenius element at p is not trivial. Hence we can apply Chebotarev's density theorem to deduce that the set of primes p, for which the ℓ-adic valuations of $n(a,p)$ and $p-1$ are equal, has density $\left(1 - \frac{1}{\ell(\ell-1)}\right)$. This computation justifies the initial (incorrect) guess by Artin of the density of primes for which a is a primitive root:

$$\prod_{\ell} \left(1 - \frac{1}{\ell(\ell-1)}\right).$$

We refer to [Mur88] for further details.

Let us now consider a different example. The following theorem is a question asked by Erdős and answered by Corrales-Rodrigáñez and Schoof [CRS97].

B. Theorem. *Let x and y be positive integers. Suppose that for all positive integers n the set of prime numbers dividing $x^n - 1$ is equal to the set of prime numbers dividing $y^n - 1$. Then x is equal to y.*

The key observation which leads to the solution of this problem is the following. Let ℓ be a prime number and let q be a power of ℓ. Let a be any

integer and let p be a prime number different from ℓ and coprime to a. Let ζ_q be a primitive q-th root of unity. Suppose that p splits in the field extension $F = \mathbb{Q}(\zeta_q, \sqrt[q]{a})$. Then the ℓ-adic valuation of the order of a modulo p is no greater than the ℓ-adic valuation of $\frac{p-1}{q}$. So we can relate the ℓ-part of the order of the reduction of a number modulo p to the image of the Frobenius element at p in the Galois group of certain Kummer field extensions.

This idea has been very fruitful in studying a number of generalizations of the above theorem which are generally called "the support problem". Most generally one is interested in relations between the orders of reduction of several points $P_1, \ldots, P_n$ lying in a semiabelian variety G defined over a number field K. The number field corresponding to F would in this case be the field of definition of all pre-images of the points P_i under the multiplication-by-q map. Some results in this area are [Kow03], [Lar03], [Wes03], [KP04], [BGK05],[Per09].

Let us finally consider the problem which is the main motivation behind this work. Let P_1 and P_2 be two rational points lying in the 2-dimensional torus $\mathbb{G}_m^2(\mathbb{Q})$ and let Γ be the subgroup spanned by them. For all but finitely many primes p we can reduce P_1 and P_2 modulo p which gives us a group Γ_p lying in $\mathbb{G}_m^2(\mathbb{F}_p) \cong (\mathbb{F}_p^\times)^2$. Then we can ask the following question: When is the reduction Γ_p a cyclic group?

There are a couple of cases for which the reduction is always cyclic. First of all, the reduction will be cyclic if Γ is cyclic. We can take, for example, $P_1 = (2, 3)$ and $P_2 = (4, 9)$. But also Γ_p will be cyclic if Γ is contained in a one-dimensional algebraic subgroup of $\mathbb{G}_m^2$. An example for this case is $P_1 = (2, 4)$ and $P_2 = (3, 9)$. As a result of our work we can prove the following:

C. Theorem. *Assume that the group Γ is a free abelian group of rank 2 and that it is not contained in a proper algebraic subgroup of $\mathbb{G}_m^2$. Then the set of primes p for which Γ_p is cyclic has zero density.*

Since the groups Γ_p are abelian, they decompose as a product $\Gamma_p = \prod_\ell \Gamma_{p,\ell}$, where $\Gamma_{p,\ell}$ is the ℓ-primary part of Γ_p. Then the condition that Γ_p is cyclic is equivalent to saying that the groups $\Gamma_{p,\ell}$ are cyclic for all ℓ. The main ingredient of the proof is then to relate the condition that $\Gamma_{p,\ell}$ is cyclic to the image of the Frobenius at p in the Galois group of the field of definition of all pre-images of P_i under multiplication by ℓ^n, for all n. This field is an infinite extension of $\mathbb{Q}$ whose Galois group is, for all but finitely many ℓ, isomorphic to a semi-direct product $\mathbb{Z}_\ell^u \rtimes \mathbb{Z}_\ell^\times$ for some $0 \leq u \leq 4$. To solve our problem we describe explicitly a subset A of this group with the property that the Frobenius element at p lies in A if and only if $\Gamma_{p,\ell}$ is cyclic. We remark, that although the statement of the theorem seems similar to problems of detecting linear dependence which have been studied in relation to the support problem, this similarity is mostly superficial. The set A turns out to be quite different in nature from the analogous sets studied in relation with the support problem.

The common theme of all of the examples presented above is to take some property of the ℓ-part of the reduction of a finitely-generated group of points in a semiabelian variety and to relate it to the image of the Frobenius automorphism by a certain ℓ-adic Galois representation. In this dissertation we develop a general framework which allows us to easily perform this correspondence. We employ for this purpose the language of 1-motives. Those are objects first discovered by Deligne [Del74] in relation to his study of mixed Hodge structures.

A special case of a 1-motive is any group homomorphism $\mathbb{Z}^n \to G(\mathbb{Q})$, where G is a semiabelian variety defined over the rational numbers. In particular, we see that the data in the three examples above can be given as 1-motives (of types $[\mathbb{Z} \to \mathbb{G}_m]$, $[\mathbb{Z}^2 \to \mathbb{G}_m]$ and $[\mathbb{Z}^2 \to \mathbb{G}_m^2]$ respectively).

To every 1-motive M defined over a field K and every prime number ℓ, one can associate a *Tate module* $\mathrm{T}_\ell M$ of M. This is a finitely-generated free $\mathbb{Z}_\ell$-module which comes equipped with a continuous action of the absolute Galois group Γ_K of K. Thus to every 1-motive M we can attach an ℓ-adic representation $\rho_\ell(M)\colon \Gamma_K \to \mathrm{Aut}(\mathrm{T}_\ell M)$. We show that if K is a number field, then the image of the Frobenius element at primes $\mathfrak{p}$, for which the 1-motive M has good reduction, determines the ℓ-part of the reduction of M modulo $\mathfrak{p}$. Furthermore, we define a map, the *Pink map*, which gives this correspondence explicitly. The precise statement of our result is given in Theorem 4.1.2. This theorem is a generalization of a result of Pink [Pin04] concerning the special case of 1-motives $\mathbb{Z} \to A$, where A is an abelian variety.

We now give a description of the chapters. In Chapter 1 we introduce 1-motives over general schemes S. We also give a characterization of a certain subset of S-1-motives in terms of the action of the fundamental group of S. This characterization (given in Theorem 1.6.2) is the only part of the chapter which is somewhat new.

The main goal of Chapter 2 is to introduce a construction which is very useful for the study of 1-motives. For any sufficiently nice scheme S, a free $\mathbb{Z}$-module Y equipped with the action of the fundamental group $\pi_1(S)$ of S and a commutative S-group scheme G, we construct a *twist* $Y \otimes G$ which satisfies certain nice functoriality properties. This construction is a generalization of the construction for the case when S is the spectrum of a field which was carried out by Mazur, Rubin and Silverberg [MRS07].

In Chapter 3 we introduce the Tate module $\mathrm{T}_\ell M$ of a 1-motive $M = [Y \to G]$ defined over a field and we study those properties which are a consequence of the all-important exact sequence

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

In particular, we define the Pink map $\varepsilon_{\mathrm{T}_\ell M}$ whose domain is a certain subset of the group $\mathrm{Aut}(\mathrm{T}_\ell M)$ and whose image lies in the *Barsotti-Tate group* of $\hat{Y} \otimes G$, that is, $\mathrm{B}_\ell(\hat{Y} \otimes G) = \mathrm{Hom}_{\mathbb{Z}_\ell}(Y \otimes \mathbb{Z}_\ell, \mathrm{T}_\ell G) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$.

Chapter 4 is concerned with studying good reduction of 1-motives defined over local fields or number fields. We prove a generalization of the Néron-Ogg-Shafarevich criterion to 1-motives and we state and prove Theorem 4.1.2 which gives us the promised method to relate reduction to the image of the Frobenius automorphism.

In Chapter 5 we look at Kummer theory. We derive results which allow us to determine the unipotent part of the image of the ℓ-adic Galois representation $\rho_\ell(M)$ whenever $M = [Y \to G]$ is a 1-motive defined over a number field and G is a *split* semiabelian variety. We also determine the image of the Pink map. The method we use goes back to a result of Ribet [Rib79].

In Chapter 6 we give an application of the theory developed so far. We define a certain family of properties of the reduction of 1-motives of the type $[\mathbb{Z}^n \to \mathbb{G}_m]$ which we call *algebraic dependences*. The question that we considered in the third example above is one such algebraic dependence defined for

a motive of the type $[\mathbb{Z}^4 \to \mathbb{G}_m]$. The main result of this section is Theorem 6.1.6 which essentially states that for a generic 1-motive $M = [\mathbb{Z}^r \to \mathbb{G}_m]$ the set of primes, for which the reduction of M satisfies a given algebraic dependence, has zero density. We also show how our main theorem implies Theorem C. stated above. Finally, we consider a certain analogy between our results and questions from p-adic transcendence theory. This peculiar similarity between Kummer theory and transcendence theory was first noticed by Bertrand [Ber88]. The reason behind it seems to be that we can reduce problems from Kummer theory as well as problems from transcendence theory to analogous questions about the image of the decomposition groups under the ℓ-adic representation associated to a 1-motive. In the last section of Chapter 6 we present some partial results in support of this claim.

The appendix contains some standard facts together with relevant references which were used in the main part of the text.

Notation

We will denote the separable closure of a field K by K^s. The absolute Galois group of K will be denoted by Γ_K. If K'/K is a Galois field extension we will denote its Galois group by $\Gamma_{K'/K}$.

There are two different ways to define the group structure on $\Gamma_{K'/K}$. We choose the convention that this set acts on the field K' *on the left*. Since the standard convention for the automorphism group $\mathrm{Aut}_K(\operatorname{Spec} K')$ is again to act on the left this means that $\Gamma_{K'/K}$ is the opposite of the group $\mathrm{Aut}_K(\operatorname{Spec} K')$. Similarly, we choose that Γ_K acts on K^s *on the left* which implies that Γ_K is equal to the opposite group $\mathrm{Aut}_K(\operatorname{Spec} K^s)^{op}$ of the automorphism group of $\operatorname{Spec} K^s$ over $\operatorname{Spec} K$.

If X is any abelian group and n is a positive integer we will write $X[n]$ for the subgroup of those elements whose order divides n. If ℓ is a prime number we will denote by $X[\ell^\infty]$ the subgroup of X consisting of all elements whose order is finite and is a power of ℓ. We will write X/n for the quotient group X/nX.

If S is a scheme we will denote the multiplicative group over S by $\mathbb{G}_{m,S}$ or by $\mathbb{G}_m$ whenever the base scheme is clear from the context.

If X is a scheme over S and $\operatorname{Spec} R' \to S$ is a morphism, we will denote the base change of X to R' by $X \otimes_S R'$. If in addition S is affine, $S = \operatorname{Spec} R$, then we will denote the base change by $X \otimes_R R'$.

If X and Y are two groups we will sometimes denote the set of group-homomorphisms by $\mathrm{Hom}_{gr}(X, Y)$ to differentiate it from the set of all maps from X to Y. Similarly, if X and Y are S-group schemes we will sometimes denote the set of S-group scheme homomorphisms by $\mathrm{Hom}_{S-gr}(X, Y)$ (or $\mathrm{Hom}_{gr}(X, Y)$ if S is clear from the context) to differentiate it from the set $\mathrm{Hom}_S(X, Y)$ of all morphisms of S-schemes. However, we might drop those subscripts whenever they are clear from the context.

Acknowledgements

I would like to thank my advisor, Michael Stoll, for the support and trust that he put in me. The question that he suggested to me became the main

motivation for the results contained in this thesis. He allowed me to pursue my own ideas, and fail – and I did fail quite a lot – instead of leading me by the hand. The experience that I gathered through my failures is probably the most valuable gain that came out from working on this research project.

I would also like to thank Brendan Creutz and Steffen Müller for the many valuable conversations that we had together. It was Brendan who first mentioned the term *1-motive* to me.

My work was to a large extent inspired by the PhD theses of Peter Jossen and Antonella Perucca. I had very fruitful discussions with both of them for which I owe them my gratitude. I would also like to thank Gisbert Wüstholz, Emanuel Kowalski, Tim Dokchitser, Laurent Berger, Romyar Sharifi and Daniel Bertrand for the useful advice that they gave me. I am also indebted to MathOverflow users nosr and S. Carnahan as well as the team which developed and supports the MathOverflow forum.

I have received financial support from Jacobs University Bremen (2008) Universität Bayreuth (2008-2010) and from Deutsche Forschungsgemeinschaft (DFG-Grant STO 299/7-1) 2010-2013)

My parents have always believed in me. Without their love and support none of this would have been possible. There is nothing that I can do which could repay my debt to them.

Chapter 1

The structure of a 1-motive

1-motives were introduced by Deligne [Del74] and were used to give an example of a mixed Hodge structure. Deligne gave two definitions of a 1-motive. A 1-motive M over an algebraically closed field k is a group homomorphism $Y \xrightarrow{u} G(k)$, where Y is a finitely-generated free abelian group and G is a semiabelian variety. On the other hand, a 1-motive M over a general scheme S is a morphism of S-group schemes $Y \xrightarrow{u} G$, where Y is étale locally isomorphic to $\mathbb{Z}^r$ for some r and G is the extension of an abelian scheme by a torus. It is not difficult to see that when S is the spectrum of an algebraically closed field the two definitions coincide. The first definition however is much more explicit and easier to work with.

We will be interested in using the language of 1-motives to study number-theoretic properties of points in semiabelian varieties. To that purpose we would like to study 1-motives over local fields and number fields, as well as 1-motives over Dedekind domains. Consequently it would be of great use to have an explicit definition of a 1-motive in those cases, which is comparable to Deligne's first definition above.

The purpose of this chapter is twofold. We are first going to introduce the building blocks of a 1-motive, that is tori, twisted constant groups, abelian schemes and extensions of abelian schemes by tori. We are going to present all properties of those objects that will be needed later on. We will also define a 1-motive and give its basic properties.

Our second purpose is to isolate a certain family of 1-motives, which we call semi-isotrivial 1-motives, for which we can give a more explicit equivalent description. This is the content of Theorem 1.6.2. As a corollary we can derive the well-known fact that a 1-motive over an arbitrary field k is given by a group homomorphism $Y \xrightarrow{u} G(k^s)$, where G is a semiabelian variety as before, Y is a finitely-generated free $\mathbb{Z}$-module equipped with a continuous action of the absolute Galois group of k, and u is Galois equivariant (see Corollary 1.6.3). We also give a similar explicit description for 1-motives over Dedekind domains (Corollary 1.6.5). The statement (and presumably the proof) of Theorem 1.6.2 must be well-known to the experts, however we are not aware of a written presentation of it.

1.1 Tori

The main reference for this section is [SGA3II, Exp. VIII,IX,X].

We recall that the multiplicative group scheme $\mathbb{G}_{m,\mathbb{Z}}$ over $\operatorname{Spec}\mathbb{Z}$ is the scheme $\mathbb{G}_{m,\mathbb{Z}} := \operatorname{Spec}\mathbb{Z}[x, x^{-1}]$ together with its usual group scheme structure. For any scheme S the multiplicative group over S is the group scheme $\mathbb{G}_{m,S} := \mathbb{G}_{m,\mathbb{Z}} \times_{\operatorname{Spec}\mathbb{Z}} S$.

1.1.1 Definition.

(i) Let S be a scheme and let G be a commutative S-group scheme. G is called a **torus** if for every point $s \in S$ there exists a Zariski open neighborhood U of s and an fpqc-morphism $S' \to U$ such that $G' = G \times_U S'$ is isomorphic to $\mathbb{G}^r_{m,S'}$ for some integer $r \geq 0$. If G is isomorphic over S to $\mathbb{G}^r_{m,S}$ then G is called **trivial**.

(ii) A torus G is called **quasi-isotrivial** if in the above definition one can choose the morphisms $S' \to U$ to be étale and surjective. It is called **isotrivial**, if there exists a surjective finite étale map $S' \to S$ such that $G' = G \times_S S'$ is trivial.

It is clear that torus is a special case of a group of multiplicative type. In the following we shall recall those properties of these groups which will be needed in the sequel.

1.1.2 Lemma. *Let S be a scheme and let T be an S-torus. T is affine, faithfully flat and of finite presentation over S.*

Proof. See [SGA3II, Exp. IX] Proposition 2.1. □

1.1.3 Lemma. *Let n be a positive integer. Let T be an S-torus.*

(i) The multiplication-by-n map $[n]\colon T \to T$ is finite and faithfully flat. Its kernel $T[n]$ is a finite flat group scheme over S.

(ii) If n is coprime to the characteristics of all residue fields of S then $T[n]$ is étale over S.

Proof. The first statement follows from [SGA3II, Exp. IX] 2.1(a,c) and 2.2. The second statement follows from [SGA3II, Exp. IX] 2.1(e) applied to the group scheme $T[n]/S$. □

The next proposition gives a characterization of isotrivial tori.

1.1.4 Proposition. *Let S be a connected locally noetherian scheme, and let $\xi\colon \operatorname{Spec}(\Omega) \to S$ be a geometric point of S, i.e. a homomorphism in S of the spectrum of an algebraically closed field Ω. Let $\pi_1 = \pi_1(S, \xi)$ be the corresponding fundamental group. Then the functor*

$$H \mapsto \operatorname{Hom}_{\Omega-gr}(H_\xi, \mathbb{G}_{m,\Omega})$$

which maps H to the set of Ω-group scheme homomorphisms between $H_\xi = H \times_S \operatorname{Spec}(\Omega)$ and $\mathbb{G}_{m,\Omega}$, is an antiequivalence between the category of isotrivial tori and the category of free $\mathbb{Z}$-modules of finite type equipped with a continuous π_1-action.

Proof. This is a special case of [SGA3II, Exp X] Corollaire 1.2. □

For tori over fields and henselian local rings we have the following characterizations.

1.1.5 Proposition. *Let k be a field, let k^s be its separable closure and let Γ_k be its absolute Galois group.*

(i) Every k-torus is isotrivial;

(ii) The functor

$$T \mapsto \mathrm{Hom}_{k^s}(T, \mathbb{G}_{m,k^s})$$

induces an antiequivalence between the category of k-tori and the category of free finitely-generated $\mathbb{Z}$-modules with continuous Γ_k-action.

Proof. This is a special case of [SGA3II, Exp. X] Proposition 1.4. □

1.1.6 Proposition. *Let R be a henselian local ring, let k be its residue field, and let Γ_k be the absolute Galois group of k.*

(i) Every R-torus is isotrivial;

(ii) The functor

$$T \mapsto T \times_R \operatorname{Spec} k$$

is an equivalence between the categories of R-tori and k-tori. Hence, the category of R-tori is antiequivalent to the category of free finitely-generated $\mathbb{Z}$-modules with continuous Γ_k-action.

Proof. See [SGA3II, Exp. X] Corollaire 4.6. □

1.2 Galois S-modules

The main reference for this section is again [SGA3II, Exp. VIII,IX,X].

Let S be a scheme and Y be a group. We can construct an S-group scheme Y_S associated to S as follows. Set $Y_S := Y \times S$, where $Y \times S$ denotes the disjoint union of copies of S indexed by Y. If Y and Z are two groups, using the universal property of the fibered product, one sees that $(Y \times Z)_S \cong Y_S \times_S Z_S$. Then we define the group operation morphism to be $m\colon Y_S \times_S Y_S \to Y_S$ as follows: if $(y_1, y_2) \in Y \times Y$ then m sends $S_{(y_1,y_2)}$ to $S_{y_1 y_2}$ via the identity morphism. The morphisms for the inversion and identity element, ι and ϵ, are defined analogously. One easily sees that $(Y_S, m, \iota, \epsilon)$ is an S-group scheme. Moreover, if Y is commutative then so is Y_S. This mapping is functorial: group homomorphisms are sent to S-group scheme homomorphisms.

Thus we can consider any group as an S-group scheme over an arbitrary scheme S. In particular, we can consider the group $\mathbb{Z}^r$ as a commutative S-group scheme $\mathbb{Z}^r_S$. Take note that $\mathbb{Z}^r_S$ is not affine, even when S is! Indeed, all affine schemes are quasi-compact, and $\mathbb{Z}^r_S$ isn't.

1.2.1 Definition.

(i) Let S be a scheme. An S-group scheme G is called a **(trivial) constant group scheme** if it is isomorphic to Y_S for some ordinary group Y. It is called a **twisted constant group scheme** if it is locally isomorphic in the fpqc-topology to a constant group scheme.

(ii) A twisted constant S-group scheme G is called **quasi-isotrivial** if it is locally isomorphic for the étale topology to a constant group scheme, i.e. if for every point $s \in S$ there exists a Zariski open neighborhood U of s and an étale surjective morphism $S' \to U$ such that $G' = G \times_S S'$ is constant.

(iii) A twisted constant S-group scheme G is called **isotrivial** if there exists a surjective finite étale morphism $S' \to S$ such that the group $G' = G \times_S S'$ is constant.

In order to simplify notation we are going to introduce the following terminology.

1.2.2 Definition. Let S be a scheme. We will call a commutative S-group scheme Y a **quasi-Galois S-module** if it is a quasi-isotrivial twisted constant S-group scheme which at every point $s \in S$ is étale locally isomorphic to $\mathbb{Z}^r$ for some $r \geq 0$, $r = r(s)$. We will call Y a **Galois S-module** if it is a quasi-Galois S-module which is isotrivial as a twisted constant group. In other words, Y is a Galois S-module if there exists a finite étale surjective map $S' \to S$ such that $Y' = Y \times_S S'$ is isomorphic to $\mathbb{Z}^r_{S'}$ for some $r \geq 0$.

1.2.3 Proposition (Cartier Duality)**.**

(i) Let S be a scheme and let G be either an S-torus or quasi-Galois S-module. Then the functor

$$D_S(G)\colon S' \mapsto \mathrm{Hom}_{S'-gr.}(G, \mathbb{G}_{m,S'})$$

from the category of S-schemes to the category of commutative groups is representable by a quasi-Galois S-module or an S-torus respectively and we have $D_S(D_S(G)) \cong G$.

(ii) The functor

$$G \mapsto D_S(G)$$

induces an antiequivalence between the categories of S-tori and quasi-Galois S-modules. This restricts to an equivalence between the category of isotrivial S-tori and Galois S-modules.

Proof. This is a special case of [SGA3II, Exp. X] Corollaire 5.7. (I owe this reference to Scott Carnahan [Car].) □

Combining Cartier duality with 1.1.4, 1.1.5 and 1.1.6 we arrive at the following corollaries:

1.2.4 Corollary. *Let k be a field, let k^s be its separable closure and let Γ_k be its absolute Galois group.*

(i) Every quasi-Galois k-module is Galois;

(ii) The functor

$$Y \mapsto Y(k^s)$$

induces an equivalence between the category of Galois k-modules and the category of finitely-generated free $\mathbb{Z}$-modules with continuous Γ_k-action. (This justifies the term Galois k-module.*)*

1.2.5 Corollary. *Let R be a henselian local ring, let k be its residue field, and let Γ_k be the absolute Galois group of k.*

(i) Every quasi-Galois R-module is Galois;

(ii) The functor

$$Y \mapsto Y \times_R \operatorname{Spec} k$$

is an equivalence between the categories of Galois R-modules and Galois k-modules. Hence, the category of Galois R-modules is equivalent to the category of finitely-generated free $\mathbb{Z}$-modules with continuous Γ_k-action.

For more general base schemes S we have the following characterization of Galois S-modules.

1.2.6 Proposition. *Let S be a connected locally noetherian scheme and let $x\colon \operatorname{Spec}(\Omega) \to S$ be a fixed geometric point. Let $P = \{P_i\}_i$ be its associated universal covering (see A.2) and let $\pi_1 = \pi_1(S, x)$ be the associated fundamental group.*

(i) Let Y be an isotrivial twisted constant S-group scheme. The natural map

$$Y(P) = \varinjlim_i \operatorname{Hom}_S(P_i, Y) \to \operatorname{Hom}_S(\operatorname{Spec}(\Omega), Y)$$

is an isomorphism.

(ii) The category of Galois S-modules is equivalent to the category of finitely-generated free $\mathbb{Z}$-modules equipped with continuous π_1-action.

Proof. We shall only give a sketch of the proof. For the first statement note that Y is a disjoint union of finite étale S-schemes. Since P pro-represents the functor $X \mapsto \operatorname{Hom}_S(\operatorname{Spec}(\Omega), X)$, where X is finite étale, it follows that the map above is a bijection. One also shows that it is a group homomorphism, whence the claim.

Next we turn to statement (ii). The functor giving the equivalence in question is

$$F_S\colon Y \mapsto Y(P)$$

Since π_1 is the opposite of the automorphism group of P we see that $Y(P)$ is equipped with an action of π_1. Since Y is isotrivial, one shows, using base change to a scheme S'/S which trivializes Y, that $Y(P)$ is a finitely-generated free $\mathbb{Z}$-module, and that the action of π_1 factors through a finite group, which implies its continuity.

To show that F is fully faithful the argument is as follows. Let Y_1 and Y_2 be two Galois S-modules. Pick a Galois covering S' which trivializes both of them and let $Y_j' = Y_j \times_S S'$ for $j = 1, 2$. Then the natural map

$$\operatorname{Hom}(Y_1', Y_2') \to \operatorname{Hom}(F_{S'}(Y_1), F_{S'}(Y_2))$$

is a bijection which is π_1-equivariant. We employ Galois descent A.3.2(i) to show that the natural map

$$\mathrm{Hom}(Y_1, Y_2) \to \mathrm{Hom}(F_S(Y_1), F_S(Y_2))$$

is a bijection which implies that F is fully faithful.

Finally we show that F_S is essentially surjective. Let Z be a finitely-generated free $\mathbb{Z}$-module with continuous π_1-action. We fix a Galois covering S'/S such that the subgroup $\pi_1(S', x)$ acts trivially on Z. We then consider the scheme $Y' = Z \times S'$. One can associate to it a descent datum coming from the action of π_1 on Z. The descent datum is effective since Y' can be represented as a disjoint union of finite étale S-schemes which are closed under the π_1-action. One shows that the S-scheme Y we have produced in this way is a Galois S-module and that $F_S(Y) = Z$. This implies that F_S is essentially surjective and hence an equivalence of categories. □

1.3 Abelian schemes

1.3.1 Definition. Let S be a scheme and let $\pi\colon A \to S$ be an S-group scheme. A is called an **abelian S-scheme** if π is proper and smooth, and has connected fibers. One can show that this implies that A is commutative.

1.3.2 Lemma. *Let n be a positive integer. Let A be an abelian S-scheme.*

(i) The multiplication-by-n map $[n]\colon A \to A$ is finite and faithfully flat. Its kernel $A[n]$ is a finite flat group scheme over S.

(ii) If n is coprime to the characteristics of all residue fields of S then the scheme $A[n]$ is étale over S.

Proof. See [Mil86, §20.7] □

1.4 Semiabelian group schemes

The exposition of the theory of exact sequences of group schemes in this section is based on [SGA3I, Exp. IV].

1.4.1 Definition. Let S be a scheme. Let G, G', G'' be commutative S-group schemes and let $k\colon G' \to G$ and $p\colon G \to G''$ be homomorphisms of S-group schemes. We will say that the sequence

$$0 \to G' \xrightarrow{k} G \xrightarrow{p} G'' \to 0 \tag{1.1}$$

is **exact** if the corresponding sequence of fpqc-sheaves of abelian groups

$$0 \to \widetilde{G'} \xrightarrow{\tilde{k}} \widetilde{G} \xrightarrow{\tilde{p}} \widetilde{G''} \to 0$$

is exact. We recall that the sheaf of groups $\widetilde{G}$ that we associate to an S-group scheme G is given by the presheaf $\widetilde{G}\colon X \mapsto G(X)$ for every morphism $X \to S$. This becomes a sheaf in the fpqc-site associated to S.

1.4.2 Lemma. *Let G, G', G'', k and p be as above. Let (M) be a family of morphisms of schemes which satisfies the following properties:*

(a) *(M) is stable under base extension;*

(b) *The composite of two morphisms in (M) is in (M);*

(c) *Every isomorphism is in (M);*

(d) *Every morphism in (M) is faithfully flat and quasi-compact;*

(e) *Let $f\colon X \to Y$ be a morphism of schemes. If there exists an fpqc-covering $\{Y_i \to Y\}_{i\in I}$ of Y such that for each $i \in I$, $X \times_Y Y_i \to Y_i$ is in (M), then f is in (M).*

Then the following holds:

(i) *Suppose that p is in (M) and that G' is isomorphic to* $\ker p$ *as a G-scheme. Then the sequence* (1.1) *is exact.*

(ii) *Conversely, suppose that the sequence* (1.1) *is exact and that $G' \to S$ is in (M). Then p is in (M).*

Proof. Both statements follow from the theory in [SGA3I, Exp. IV]. To prove statement (i) we use 3.4.7.1 and 4.6.5 applied to the fpqc-topology to show that the quotient sheaf $\widetilde{G}/\widetilde{G'}$ is representable and represented by G''. Hence, by our definition, (1.1) is exact.

Statement (ii) follows from 3.3.4 and 4.6.5. □

1.4.3 Corollary. *Let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of commutative S-group schemes and let (M) be as in Lemma 1.4.2. If the morphisms $G' \to S$ and $G'' \to S$ are in (M) then $G \to S$ is in (M).*

Proof. Indeed, by Lemma 1.4.2(ii) we have that $G \to G''$ is in (M). Since (M) is stable under composition the claim follows. □

We are going to apply the previous lemma for the following two families:

- (M_{fpf}) – the family of finite and faithfully flat morphisms
- $(M_{\acute{e}fg})$ – the family of finite etale surjective morphisms

1.4.4 Lemma. *The families (M_{fpf}) and $(M_{\acute{e}fg})$ satisfy the conditions of Lemma 1.4.2.*

Proof. That finite morphisms satisfy condition (e) follows from fpqc-descent on morphisms (see e.g [EGA4II] Proposition 2.7.1(xv)) The rest of the statement follows from [SGA3I, Exp. IV] Corollaire 6.3.2. □

1.4.5 Definition. Let S be a scheme, let A be an abelian S-scheme and let T be an S-torus. An **extension of A by T** is a commutative S-group scheme G together with homomorphisms $p\colon G \to A$ and $k\colon T \to G$ such that the following sequence is exact:

$$0 \to T \xrightarrow{k} G \xrightarrow{p} A \to 0.$$

When S is the spectrum of a field, G is called a **semiabelian variety**. If X is an S-group scheme such that for every $s \in S$ the fiber $X_s = X \otimes_S k(s)$ is a semiabelian variety, then X is called a **semiabelian scheme**. It is easy to see that every extension of an abelian scheme by a torus is also a semiabelian scheme.

The following lemma gives us the properties of the multiplication-by-n map on extensions of abelian schemes by tori. The proof is based on a MathOverflow post due to user nosr [nos].

1.4.6 Lemma. *Let n be a positive integer. Let G be a commutative S-group scheme which is an extension of an abelian scheme A by a torus T.*

(i) The multiplication-by-n map $[n]\colon G \to G$ is finite and faithfully flat. Its kernel $G[n]$ is a finite flat group scheme over S.

(ii) If n is coprime to the characteristics of all residue fields of S then $G[n]$ is étale over S and the map $[n]\colon G \to G$ is étale.

Proof. By Lemmas 1.1.3, 1.3.2 and 1.4.2(i) it follows that the sequences

$$0 \to \widetilde{T[n]} \to \widetilde{T} \xrightarrow{[n]} \widetilde{T} \to 0$$

and

$$0 \to \widetilde{A[n]} \to \widetilde{A} \xrightarrow{[n]} \widetilde{A} \to 0$$

are exact. Hence applying the Snake Lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widetilde{T} & \longrightarrow & \widetilde{G} & \longrightarrow & \widetilde{A} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \\ 0 & \longrightarrow & \widetilde{T} & \longrightarrow & \widetilde{G} & \longrightarrow & \widetilde{A} & \longrightarrow & 0 \end{array}$$

it follows that the sequences

$$0 \to T[n] \to G[n] \to A[n] \to 0 \tag{1.2}$$

and

$$0 \to G[n] \to G \xrightarrow{[n]} G \to 0 \tag{1.3}$$

are exact. By 1.1.3, 1.3.2 and 1.4.3 applied to (1.2) it follows that $G[n]$ is a finite flat group scheme over S and that it is étale in case (ii) (more precisely it follows that the map $G[n] \to S$ is in (M_{fpf}) or $(M_{\acute{e}fg})$ respectively). Finally, Lemma 1.4.2(ii) applied to (1.3) implies that the map $[n]\colon G \to G$ is finite and faithfully flat and that it is étale if n is coprime to the characteristics of the residue fields of S. □

Let T be an S-torus and let A be an abelian S-scheme. We will use the notation $\mathrm{Ext}_S(A, T)$ to denote the set of all extensions of A by T (up to isomorphism).

The following is a slight generalization, which we have taken from Jossen [Jos09], of a theorem of Oort [Oor66, §III.18.1] which states that $\mathrm{Ext}_S(A, \mathbb{G}_m)$ is parametrized by the S-points of the dual abelian scheme $A^\vee$.

1.4.7 Proposition. *Let S be a noetherian regular scheme. Let T be an S-torus, and let A be an abelian S-scheme. Then there is a canonical isomorphism*

$$\mathrm{Ext}_S(A,T) \to \mathrm{Hom}_S(T^\vee, A^\vee)$$

which is compatible with base change. Here $T^\vee$ is the Cartier dual of T and $A^\vee$ is the dual abelian scheme of A.

Proof. See [Jos09, Proposition 1.2.3]. □

1.5 1-Motives

1.5.1 Definition. Let S be a scheme. A **1-motive** M **over** S consists of the following data:

- A quasi-Galois S-module Y;
- A semiabelian S-group scheme G, which is the extension of an abelian S-scheme A by an S-torus T.
- An S-homomorphism $u\colon Y \to G$.

See [Del74], [Ray94]. We shall use the notation $M = [Y \xrightarrow{u} G]$ to denote a 1-motive.

A morphism between 1-motives $f\colon [Y_1 \xrightarrow{u_1} G_1] \to [Y_2 \xrightarrow{u_2} G_2]$ is a pair of S-homomorphisms $f_{-1}\colon Y_1 \to Y_2$ and $f_0\colon G_1 \to G_2$ which commute with u_1 and u_2.

We shall denote the category of S-1-motives by $\mathbf{Mot}_S$. For fixed Y and G we shall denote the set of S-1-motives $[Y \to G]$ by $\mathrm{Mot}_S(Y,G)$.

Let $M = [Y \xrightarrow{u} G]$ be a 1-motive over a scheme S, where G is an extension of an abelian scheme A by a torus T. There is a standard increasing filtration W, called the **weight filtration**, that we can associate to M. It is defined as follows:

$$W_i(M) = \begin{cases} 0 & \text{for } i < -2, \\ M & \text{for } i \geq 0, \\ G & \text{for } i = -1, \\ T & \text{for } i = -2. \end{cases} \tag{1.4}$$

Here we interpret G and T as the 1-motives $[\{0\} \to G]$ and $[\{0\} \to T]$ respectively, where $\{0\}$ denotes the trivial group scheme over S. We also interpret 0 as the 1-motive $[\{0\} \to \{0\}]$.

For any i we have natural morphisms $W_{i-1}(M) \to W_i(M)$. For example, for $i = 0$ the corresponding morphism is given by the commutative diagram

$$\begin{array}{ccc} \{0\} & \longrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ Y & \longrightarrow & G \end{array}$$

Taking quotients on each component of those morphisms we get the *grading* Gr^W associated to W:

$$Gr_i^W(M) = \begin{cases} 0 & \text{for } i < -2 \text{ or } i \geq 1, \\ Y & \text{for } i = 0, \\ A & \text{for } i = -1, \\ T & \text{for } i = -2. \end{cases} \tag{1.5}$$

Then for each i we have the "exact" sequence:

$$0 \to W_{i-1}(M) \to W_i(M) \to Gr_i^W(M) \to 0$$

This sequence is exact in the sense that it induces exact sequences on the group schemes underlying the given 1-motives. In particular, we have an exact sequence

$$0 \to G \to M \to Y \to 0. \tag{1.6}$$

We remark that we simply take equations (1.4) and (1.5) as the definitions of the objects $W(M)$ and $Gr^W(M)$. In general, for any abelian category $\mathcal{A}$ one can define the notion of a filtered object, which is a pair (A, F), where $A \in \mathcal{A}$, and $F = (F_n(A))_{n\in\mathbb{Z}}$ is a sequence of objects in $\mathcal{A}$ such that for any $n \leq m$ one has $F_n(A) \subseteq F_m(A)$. To any such filtered object one can associate a grading $Gr^F(A)$. The category of S-1-motives is not abelian, however one can regard it as a subcategory of the category of complexes of sheaves of groups for the small fppf-site over S. One can identify an S-1-motive $M = [Y \xrightarrow{u} G]$ with the complex $\widetilde{M} = [\widetilde{Y} \xrightarrow{\widetilde{u}} \widetilde{G}]$, where $\widetilde{Y}$ and $\widetilde{G}$ have degrees -1 and 0 respectively. After this identification the pair (M, W) becomes a filtered object. We refer to [Del71] for more on filtrations. Those considerations are not relevant for our purposes.

1.6 The structure of semi-isotrivial 1-motives

Our next goal is to give a more explicit description of a 1-motive when the group Y is trivial or isotrivial.

1.6.1 Definition. We will say that a motive $M = [Y \xrightarrow{u} G]$ is **semi-trivial** (**semi-isotrivial**), if Y is trivial (isotrivial). We will denote the full subcategory of semi-trivial (semi-isotrivial) 1-motives by $\mathbf{Mot}_S^{st}$ ($\mathbf{Mot}_S^{si}$ respectively).

Let S be a connected locally noetherian scheme and let $x\colon \operatorname{Spec}\Omega \to S$ be a fixed geometric point. Let $P = \{P_i\}_{i\in I}$ be the corresponding universal covering which satisfies the conditions in Lemma A.2.4 and let $\pi_1 = \pi_1(S, x)$ denote the fundamental group. Let $\mathcal{C}(S, x)$ denote the category whose objects are triples (Y^*, u^*, G), where:

- Y^* is a free $\mathbb{Z}$-module of finite type equipped with a continuous left π_1-action;
- G is a commutative S-group scheme, which is an extension of an abelian scheme by a torus;

- u^* is a π_1-equivariant group homomorphism

$$u^*\colon Y^* \to G(P),$$

A morphism $f^*\colon (Y_1^*, u_1^*, G_1) \to (Y_2^*, u_2^*, G_2)$ consists of a pair $f^* = (f_{-1}^*, f_0)$ of homomorphisms $f_{-1}^*\colon Y_1^* \to Y_2^*$ and $f_0\colon G_1 \to G_2$ such that $f_0 u_1^* = u_2^* f_{-1}^*$. We will denote by $\mathcal{C}(S,x)^{st}$ the full subcategory consisting of objects (Y^*, u^*, G) such that the action of π_1 on Y^* is trivial.

1.6.2 Theorem. *Let S be a connected locally noetherian scheme. There is a canonical equivalence of categories $F_S\colon \mathrm{Mot}_S^{si} \to \mathcal{C}(S,x)$.*

Proof. The proof proceeds in the following steps.

a) We define the functor F_S. Let $M = [Y \xrightarrow{u} G]$. Let

$$Y^* := Y(P) = \varinjlim_i Y(P_i)$$

We can take the limit above only over those $i \in I$ for which P_i is Galois. For one such fixed i, the group $\mathrm{Aut}(P_i/P)^{op}$ induces a left action on $Y(P_i)$. Hence the fundamental group $\pi_1 = \varprojlim_i \mathrm{Aut}(P_i/P)^{op}$ (where the limit is taken over the Galois P_i) acts on Y^* on the left.

Since Y is isotrivial, there exists $j \in I$ such that $Y \times P_j$ is trivial. Without loss of generality we can pick j such that P_j is Galois. Then for every $k \geq j$ we have $Y(P_k) = Y(P_j)$, hence

$$Y^* = Y(P_j)$$

and the π_1-action factors through the finite group $\mathrm{Aut}(P_i/P)^{op}$. This implies that Y^* is a free $\mathbb{Z}$-module of finite type on which π_1 acts continuously.

Let $u^*\colon Y^* \to G(P)$ be the unique map which restricts to $u(P_i)$ on $Y(P_i)$ for all $i \in I$. If we pick j such that P_j is Galois and $Y \times P_j$ is trivial we get that for every $k \geq j$ $u(P_k) = u(P_j)$. It follows that $u^* = u(P_j)$. The latter map is π_1-equivariant and its image lies in $G(P_j)$, hence the map u^* satisfies those properties as well.

Finally we define $F_S(M)$ to be

$$F_S(M) := (Y^*, u^*, G)$$

It follows from the arguments above, that $F_S(M)$ is indeed an object in $\mathcal{C}(S,x)$.

Let $M_1 = [Y_1 \xrightarrow{u_1} G_1]$ and $M_2 = [Y_2 \xrightarrow{u_2} G_2]$ be two semi-trivial S-1-motives and let $f = (f_{-1}, f_0) \in \mathrm{Hom}(M_1, M_2)$. Let $f_{-1}^*\colon Y_1^* \to Y_2^*$ be the unique map which restricts to $f_{-1}(P_i)$ for all $i \in I$. There exists $j \in I$ such that P_j is Galois and such that $Y_1 \times P_j$ and $Y_2 \times P_j$ are trivial. Then similarly as above $f_{-1}^* = f_{-1}(P_j)$. It is therefore a π_1-equivariant homomorphism. We set

$$F_S(f) = (f_{-1}^*, f_0),$$

It is trivial to check that F_S is a covariant functor.

Note that if $M = [Y \xrightarrow{u} G]$ is semi-trivial, then $Y^* = Y(S)$ and $u^* = u(S)$.

b) Let Y be a trivial Galois S-module. Then the map

$$\mathrm{Mot}_S(Y,G) \to \mathrm{Hom}_{gr}(Y(S),G(S)),\ [Y \xrightarrow{u} G] \mapsto u(S)$$

is an isomorphism.

Indeed, since Y consists of a set of copies of S indexed by $Y(S)$,

$$Y \cong \{S_y\}_{y\in Y(S)},$$

it follows that $\mathrm{Hom}_S(Y,G)$ consists of sets $\{u_y\}_{y\in Y(S)}$ with $u_y \in G(S)$ for all $y \in Y(S)$. Hence the map

$$f\colon \mathrm{Hom}_S(Y,G) \ni u \mapsto u(S) \in \mathrm{Hom}_{gr}(Y(S),G(S))$$

is an isomorphism. If u is a group-scheme homomorphism, then $u(S) \in \mathrm{Hom}_{gr}(Y(S),G(S))$. Conversely, if $u(S)$ is a group homomorphism, then for any S-scheme S', $u(S')$ is the composition of $u(S)$ with the isomorphism $Y(S') \xrightarrow{\sim} Y(S)$, hence it is a group homomorphism as well. It follows that u is a group-scheme homomorphism.

c) Let M_1 and M_2 be two semi-trivial 1-motives. Then the map

$$\mathrm{Hom}(M_1,M_2) \to \mathrm{Hom}(F_S(M_1),F_S(M_2))$$

is a bijection

Let $M_j = [Y_j \xrightarrow{u_j} G_j]$ for $j = 1,2$. Since the functor $X \mapsto X_S$ which associates an S-group scheme to a group is fully faithful, it follows that the map $\mathrm{Hom}_{gr}(Y_1,Y_2) \to \mathrm{Hom}(Y_1^*,Y_2^*)$ is bijective. Hence we get the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(M_1,M_2) & \xrightarrow{\quad\alpha\quad} & \mathrm{Hom}(F_S(M_1),F_S(M_2)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{gr}(Y_1,Y_2)\times\mathrm{Hom}_{gr}(G_1,G_2) & \xrightarrow{\sim} & \mathrm{Hom}(Y_1^*,Y_2^*)\times\mathrm{Hom}_{gr}(G_1,G_2) \end{array}$$

One easily sees that α is injective.

To show surjectivity, let $(f_{-1}^*, f_0) \in \mathrm{Hom}(F_S(M_1),F_S(M_2))$ and let (f_{-1},f_0) be the corresponding pair in $\mathrm{Hom}_{gr}(Y_1,Y_2)\times\mathrm{Hom}_{gr}(G_1,G_2)$. Recall from *b)* that $u_j \cong \{u_j^*(y)\}_{y\in Y_j^*}$. Similarly we can identify f_{-1} with the indexed set $\{f_{-1}^*(y)\}_{y\in Y_1^*}$. Then

$$u_2 f_{-1} \cong \{u_2^*(f_{-1}^*(y)\}_{y\in Y_1^*} = \{f_0(u_1^*(y))\}_{y\in Y_1^*} \cong f_0 u_1,$$

hence $(f_{-1},f_0) \in \mathrm{Hom}(M_1,M_2)$, which implies the claim.

d) The functor F_S is an equivalence between Mot_S^{st} and $\mathcal{C}(S,x)^{st}$.

That F_S restricted to Mot_S^{st} is fully faithful follows from *c)*. To show that it is essentially surjective, let $M^* = (Y^*,u^*,G) \in \mathcal{C}(S,x)^{st}$. Let $Y = (Y^*)_S$. Then *b)* implies that there exists a 1-motive $M = [Y \xrightarrow{u} G]$ such that $u(S) = u^*$. Clearly we have $F_S(M) = M^*$, which proves the claim.

e) Let M_1 and M_2 be two semi-isotrivial 1-motives. Then the map

$$\mathrm{Hom}(M_1, M_2) \to \mathrm{Hom}(F_S(M_1), F_S(M_2))$$

is a bijection. In other words, the functor F_S is fully faithful.

Let S'/S be a Galois covering such that the base changes $M_1' = M_1 \times S'$ and $M_2' = M_2 \times S'$ are semi-trivial. We have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}(M_1, M_2) & \xrightarrow{\alpha} & \mathrm{Hom}(F_S(M_1), F_S(M_2)) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Hom}(M_1', M_2') & \xrightarrow{\alpha'} & \mathrm{Hom}(F_{S'}(M_1'), F_{S'}(M_2')) \end{array}$$

The map α' is a bijection by c), which implies that α is injective.

Let (f_{-1}^*, f_0) be an element of $\mathrm{Hom}(F_S(M_1), F_S(M_2))$. This pair is an element of the product $\mathrm{Hom}(Y_1^*, Y_2^*) \times \mathrm{Hom}_{gr}(G_1, G_2)$. By 1.2.6(ii) it follows that there is an isomorphism

$$\mathrm{Hom}_{gr}(Y_1, Y_2) \times \mathrm{Hom}_{gr}(G_1, G_2) \xrightarrow{\sim} \mathrm{Hom}(Y_1^*, Y_2^*) \times \mathrm{Hom}_{gr}(G_1, G_2)$$

which restricts to α, and that there is a tuple (f_{-1}, f_0) which is the pre-image of (f_{-1}^*, f_0) under this isomorphism. After changing basis to S' and applying c) we see that $(f_{-1}, f_0) \in \mathrm{Hom}(M_1', M_2')$, i.e., that $u_2' f_{-1} = f_0 u_1'$. Then using Galois descent A.3.2(i) it follows that $u_2 f_{-1} = f_0 u_1$, hence $(f_{-1}, f_0) \in \mathrm{Hom}(M_1, M_2)$. Thus the map α is bijective.

f) The functor F_S is essentially surjective.

Let $M = (Y^*, u^*, G) \in \mathcal{C}(S, x)$. By 1.2.6(ii) there exists a Galois S-module Y corresponding to Y^*. Let S'/S be a Galois covering for which Y splits. By b) the map u^* induces a morphism

$$v \colon Y \times_S S' \to G \times_S S'.$$

One checks that this morphism is compatible with the action of $\Gamma_{S'/S}$ hence it descends to a morphism $u \colon Y \to G$ and we have that $F([Y \xrightarrow{u} G]) = (Y^*, u^*, G)$.

Finally, the statement of the theorem follows from e) and f), and Theorem A.1.1. □

Let K be a field. Since every quasi-Galois K-module is Galois (by 1.2.4(i)) it follows that every K-1-motive is semi-isotrivial. Let $\overline{K}$ be an algebraic closure of K and let K^s be the separable closure of K in $\overline{K}$. We can then replace the universal covering of K induced by the embedding $K \hookrightarrow \overline{K}$ by K^s (as follows from Proposition A.2.5), and the fundamental group in this case is simply the absolute Galois group Γ_K. Hence Theorem 1.6.2 implies the following characterization:

1.6.3 Corollary. *The category* $\mathbf{Mot}_K$ *is isomorphic to the category of Γ_K-equivariant group homomorphisms $u \colon Y \to G(K^s)$, where Y is a free $\mathbb{Z}$-module of finite type equipped with a continuous Γ_K-action and G is a semiabelian variety over K.*

Next, let R be a henselian local ring and let k be its residue field. In this case 1.2.5 implies that every R-1-motive is semi-isotrivial. Fix a geometric point $x \in \operatorname{Spec} \bar{k} \to \operatorname{Spec} k$ and let k^s be the separable closure of k in $\bar{k}$. Then (by Remark A.4.5) the fundamental groups $\pi_1(R, x)$ and $\pi_1(k, x)$ are canonically isomorphic and the universal covering of R at x has a limit which is the strict henselization R^s of R. Hence we get

1.6.4 Corollary. *The category* $\mathbf{Mot}_R$ *is isomorphic to the category of* Γ_k*-equivariant group homomorphisms* $u\colon Y \to G(R^s)$*, where* Y *is a free* $\mathbb{Z}$*-module of finite type equipped with a continuous* Γ_k*-action and* G *is a commutative* R*-group scheme which is an extension of an abelian scheme by a torus.*

Finally, let R be a Dedekind domain and let K be its field of fractions. Fix again a geometric point $x\colon K \to \overline{K}$. By Proposition A.2.6 the embedding $R \hookrightarrow K$ induces a surjective map $\pi_1(K, x) \to \pi_1(R, x)$. We will denote its kernel by I_R, and we will use Γ_R to denote the group $\pi_1(R, x)$. So we have an exact sequence:

$$1 \to I_R \to \Gamma_K \to \Gamma_R \to 1$$

Here the fixed field of I_R is the limit of all finite separable field extensions of K which are unramified at the primes in R. Let L denote this limit and let R^{un} be the integral closure of R in L. Then R^{un} is the limit of the universal covering of R at the point x. Hence, applying Theorem 1.6.2 we arrive at the following characterization of 1-motives over Dedekind rings:

1.6.5 Corollary. *Let* R *be a Dedekind domain. The category of semi-isotrivial* R*-1-motives is equivalent to the category of* Γ_R*-equivariant group homomorphisms* $u\colon Y \to G(R^{un})$*, where* Y *is a free* $\mathbb{Z}$*-module of finite type equipped with a continuous left* Γ_R*-action and* G *is a commutative* R*-group scheme which is an extension of an abelian scheme by a torus.*

Chapter 2

Twisting

Let S be an affine scheme. We want to construct a mapping that associates to every Galois S-module $Y \in \mathbf{Mod}(S)$ and every commutative S-group scheme G which is *quasi-projective* over S, a twist $Y \otimes G$ with certain nice properties. This is a generalization of the twist of a commutative algebraic group which was studied by Mazur, Rubin and Silverberg in [MRS07]. Our construction, as well as the one in [MRS07] is a special case of a tensor product of sheaves for the étale topology, (see [SGA4I, Exp. IV, Proposition 12.7]), however the construction is more explicit and it is clear from it that the twist is representable. We are going to roughly follow the exposition given in [MRS07, Section 1], however we are only going to consider twists over $\mathbb{Z}$. Also we are going to use Galois descent to construct the twist which is slightly different from the method employed in [MRS07].

We will use twists throughout the rest of this work. At the end of this chapter we will present one application of the construction. We show that for certain schemes S the group of 1-motives $\mathrm{Mot}_S(Y, G)$ is isomorphic to the set of S-points in the S-group scheme $\hat{Y} \otimes G$. In other words, every S-1-motive $M = [Y \to G]$ is essentially equivalent to a 1-motive $[\mathbb{Z} \to \hat{Y} \otimes G]$.

2.1 Twisting commutative group schemes

For this whole section S will be an affine, connected, locally noetherian scheme.

Let Y be a Galois S-module and let G be a quasi-projective commutative S-group scheme. Our goal is to construct a certain commutative S-group scheme $Y \otimes G$, and to present some of its properties.

In the following we will need to deal with both left and right group actions. In order to reduce confusion we will fix the convention that the elements in $\mathbb{Z}^r$ will be regarded as column vectors. Then the group $GL_r(\mathbb{Z})$ has a natural *left* action on $\mathbb{Z}^r$. Its opposite group, $GL_r^{op}(\mathbb{Z})$ therefore has a *right* action on $\mathbb{Z}^r$. If $A \in GL_r(\mathbb{Z})$ we will denote its corresponding element in the opposite group $GL_r^{op}(\mathbb{Z})$ by A^{op}. It is easy to see that for any vector $y \in \mathbb{Z}^r$ we have the relation $(yA^{op})^t = y^t A^t$, where we use the superscript t to denote the transpose. Note also that the map $A^{op} \mapsto A^{-1}$ is a group isomorphism between $GL_r^{op}(\mathbb{Z})$ and $GL_r(\mathbb{Z})$. This map induces a *left* action of $GL_r^{op}(\mathbb{Z})$ on $\mathbb{Z}^r$.

Let S'/S be a Galois covering which makes Y trivial. Then $Y(S') \sim \mathbb{Z}^r$ for

some $r \geq 0$. Fix an isomorphism

$$\phi\colon \mathbb{Z}^r \to Y(S').$$

The group $\mathrm{Aut}(S'/S)$ acts on $Y(S')$ *on the right*. It induces a right action A_ϕ^{op} on $\mathbb{Z}^r$ as follows:

$$A_\phi^{op}\colon \mathrm{Aut}(S'/S) \to GL_r^{op}(\mathbb{Z}),\ \sigma \mapsto \left(y \mapsto \phi^{-1}(\phi(y) \circ \sigma)\right).$$

Let $A_\phi(\sigma)$ be the corresponding matrix in $GL_r(\mathbb{Z})$ and let $a_{ij}(\sigma)$ denote the coordinate functions (that is $A_\phi(\sigma) = \{a_{ij}(\sigma)\}$). Then the automorphism $A^{-1}(\sigma) = A(\sigma^{-1})$ acts on $\mathbb{Z}^r$ *on the left*. So if $y = (y_1, \ldots, y_r)^t$ is a column vector in $\mathbb{Z}^r$, then we have the left action

$$A_\phi(\sigma^{-1})y = \left(\sum_j a_{ij}(\sigma^{-1})y_j\right)^t_{1\leq i\leq r}.$$

Let $G' := G \times_S S'$ and let $V' = (G')^r$. Let ρ_G denote the descent datum on G' induced by base change. That is, ρ_G is a group homomorphism: $\rho_G\colon \mathrm{Aut}(S'/S) \to \mathrm{Aut}(G'/S)$ such that for every $\sigma \in \mathrm{Aut}(S'/S)$ the following diagram commutes:

$$\begin{array}{ccc} G' & \xrightarrow{\rho_G(\sigma)} & G' \\ \downarrow & & \downarrow \\ S' & \xrightarrow{\sigma} & S' \end{array}$$

This descent datum induces a descent datum on V', which we will denote by ρ_{G^r}.

We will now give a different descent datum ϕ_* on V'. Note that there is a canonical embedding $GL_r(\mathbb{Z}) \hookrightarrow \mathrm{End}_S(G^r)$, which means that for any σ, $A_\phi(\sigma^{-1})$ acts on G^r, and consequently, on V'. Then we set

$$\phi_*(\sigma) = A_\phi(\sigma^{-1})\rho_{G^r}(\sigma).$$

(Note that $A_\phi(\sigma^{-1})$ and $\rho_{G^r}(\sigma)$ commute, since the first automorphism comes from an automorphism on G^r.) One checks that this indeed is a descent datum on V'. Since G (and hence V') is quasi-projective, we can apply Theorem A.3.3 and Remark (iii) to deduce that the pair (V', ϕ_*) descends to a commutative S-group scheme $V = V(Y, G, S', \phi)$.

2.1.1 Lemma. *The commutative group scheme V constructed above does not depend on the choice of ϕ and S'/S.*

Proof. The proof is relatively straightforward. To see that V does not depend on ϕ pick any other isomorphism $\phi'\colon \mathbb{Z}^r \to Y(S')$. Let $B \in GL_r(\mathbb{Z})$ be the matrix $B = \phi^{-1}\phi'$. B induces an automorphism of G^r, hence it also gives an automorphism of V'. One checks that $A_{\phi'} = B^{-1}A_\phi B$ which implies that $B\phi'_* = \phi_* B$. Hence B induces an isomorphism of descent data

$$(V', \phi'_*) \to (V', \phi_*),$$

which descends to a canonical isomorphism

$$V(Y, G, S'/S, \phi') \cong V(Y, G, S'/S, \phi).$$

To see that V does not depend on S' pick a Galois covering S''/S which extends S'. We can check that the descent datum on $V'' = (G^r) \times_S S''$ induced by ϕ is the lift of the descent datum ϕ_* on V'. Hence $V(G, Y, S'') \cong V(G, Y, S')$. The desired independence follows, since for every two coverings S'_1/S and S'_2/S which trivialize Y one can find a Galois covering S''/S which is both an extension of S'_1 and S'_2. □

2.1.2 Definition. As a result of the previous lemma we are justified to denote the commutative group scheme constructed above by $Y \otimes G$. It will be called the **twist** of G by Y. Notice that for every Galois S' which trivializes Y and for every isomorphism $\phi\colon \mathbb{Z}^r \to Y(S')$ we can associate canonically an S'-isomorphism $\phi_\flat\colon (G \times_S S')^r \to (Y \otimes G) \times_S S'$.

2.1.3 Lemma. *The twist is compatible with base change, that is if $f\colon S_1 \to S$ is a morphism of affine schemes then*

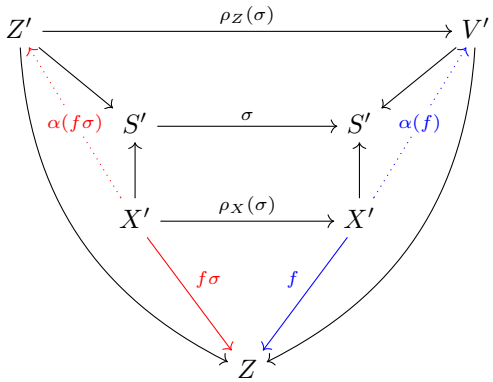
$$(Y \otimes G) \times_S S_1 \cong (Y \times_S S_1) \otimes (G \times_S S_1)$$

Proof. We only give a sketch of the proof, which is fairly standard. We take a Galois covering S'/S which trivializes Y, and let $S'_1 := S_1 \times_S S'$. To prove the lemma one shows that after lifting to S'_1 the two sides of the equation above become canonically isomorphic and that this isomorphism is compatible with the descent data on both sides. □

Let X and Z be S-schemes and let S'/S be a Galois covering. Let $X' = X \times_S S'$ and $Z' = Z \times_S S'$ and let ρ_X and ρ_Z denote the corresponding descent data. The group $\mathrm{Aut}(S'/S)$ acts on X' on the left via ρ_X hence it induces a *right* action on the set $Z(X') = \mathrm{Hom}_S(X', Z)$. It is easy to see that we have a bijection $\alpha\colon \mathrm{Hom}_S(X', Z) \to \mathrm{Hom}_{S'}(X', Z')$. Then one can show that for any $\sigma \in \mathrm{Aut}(S'/S)$ the following relation holds:

$$\alpha(f\sigma) = \rho_Z^{-1}(\sigma)\alpha(f)\rho_X(\sigma)$$

One can see that by studying the following commutative diagram:



We will apply the above considerations to the following situation. Let S'/S be again a Galois covering which trivializes Y and let $\phi\colon \mathbb{Z}^r \to Y(S')$ be any isomorphism. Let X be an S-scheme and let $X' = X \times_S S'$. Let again $V' = (G')^r$. Then we have the bijection

$$\beta\colon \mathbb{Z}^r \otimes_{\mathbb{Z}} \mathrm{Hom}_{S'}(X', G') \xrightarrow{\sim} \mathrm{Hom}_{S'}(X', V')$$

By our considerations above the group $\mathrm{Aut}(S'/S)$ acts on $\mathrm{Hom}_{S'}(X', G')$ by the formula $f \mapsto \rho_G(\sigma^{-1}) f \rho_X(\sigma)$ and on $\mathrm{Hom}_{S'}(X', V')$ by the formula $f \mapsto \phi_*(\sigma^{-1}) f \rho_X(\sigma) = A_\phi(\sigma)\rho_G(\sigma^{-1}) f \rho_X(\sigma)$. Also it acts on $\mathbb{Z}^r$ by the formula $y \mapsto A(\sigma)y$. All actions are *on the right*. One can then check that the bijection above is $\mathrm{Aut}(S'/S)$-equivariant. Hence, composing with the maps ϕ and $\phi_\flat$ we get an $\mathrm{Aut}(S'/S)$-equivariant group isomorphism

$$Y(S') \otimes_{\mathbb{Z}} G(X') \xrightarrow{\sim} (Y \otimes G)(X')$$

We gather our conclusions so far in the statement of the following lemma:

2.1.4 Lemma. *Let S'/S be any Galois covering which trivializes Y. For any S-scheme X there exists a canonical $\mathrm{Aut}(S'/S)$-equivariant isomorphism*

$$\gamma\colon Y(S') \otimes_{\mathbb{Z}} G(X \times_S S') \xrightarrow{\sim} (Y \otimes G)(X \times_S S')$$

which is functorial in S', X, G and Y.

Proof. It remains to show that the bijection we constructed does not depend on the choice of ϕ and that it is functorial. We shall only give a sketch.

To show that this bijection does not depend on the choice of ϕ one computes explicitly how change of basis affects the map β, similarly to the proof of Lemma 2.1.1. To show that the map γ is functorial in S' we fix a further Galois covering S''/S' for which we need to show that the diagram

$$\begin{array}{ccc} Y(S') \otimes \mathrm{Hom}_S(X \times_S S', G) & \longrightarrow & \mathrm{Hom}_S(X \times_S S', Y \otimes G) \\ \downarrow & & \downarrow \\ Y(S'') \otimes \mathrm{Hom}_S(X \times_S S'', G) & \longrightarrow & \mathrm{Hom}_S(X \times_S S'', Y \otimes G) \end{array}$$

commutes. To do that we fix a basis $\phi\colon \mathbb{Z}^r \to Y(S')$. Note that in this case the natural map $Y(S') \to Y(S'')$ is an isomorphism. Then we are reduced to showing that the diagram

$$\begin{array}{ccc} \mathbb{Z}^r \otimes \mathrm{Hom}_{S'}(X \times_S S', G \times_S S') & \longrightarrow & \mathrm{Hom}_{S'}(X \times_S S', (G \times_S S')^r) \\ \downarrow & & \downarrow \\ \mathbb{Z}^r \otimes \mathrm{Hom}_{S'}(X \times_S S'', G \times_S S'') & \longrightarrow & \mathrm{Hom}_{S''}(X \times_S S'', (G \times_S S'')^r) \end{array}$$

commutes, which follows easily from the definitions.

To show that γ is functorial in X, let $f\colon Z \to X$ be a morphism. Also, let $Z' = Z \times_S S'$. Then, after fixing a basis for Y, we a reduced to showing that

the natural diagram

$$\begin{array}{ccc} \mathbb{Z}^r \otimes \mathrm{Hom}_{S'}(X', G') & \longrightarrow & \mathrm{Hom}_{S'}(X', (G')^r) \\ \downarrow & & \downarrow \\ \mathbb{Z}^r \otimes \mathrm{Hom}_{S'}(Y', G') & \longrightarrow & \mathrm{Hom}_{S'}(Z', (G')^r) \end{array}$$

commutes, which is trivial. By an analogous argument it is also easy to show that γ is functorial in G.

Finally, to show that γ is functorial in Y fix a homomorphism of Galois S-modules $f\colon Y \to Z$. Let S'/S be a Galois covering which trivializes both Y and Z. Fix bases $\phi\colon \mathbb{Z}^r \to Y(S')$ and $\psi\colon \mathbb{Z}^s \to Z(S')$. The map f induces morphisms $\mathbb{Z}^r \to \mathbb{Z}^s$ as well as a morphism $(G')^r \to (G')^s$. Then we are reduced to showing that the diagram

$$\begin{array}{ccc} \mathbb{Z}^r \otimes \mathrm{Hom}_{S'}(X', G') & \longrightarrow & \mathrm{Hom}_{S'}(X', (G')^r) \\ \downarrow & & \downarrow \\ \mathbb{Z}^s \otimes \mathrm{Hom}_{S'}(X', G') & \longrightarrow & \mathrm{Hom}_{S'}(X', (G')^s) \end{array}$$

commutes, which is again trivial. □

2.1.5 Theorem. *Let Y be a Galois S-module and let G be a quasi-projective commutative S-group scheme. Let S'/S be any Galois covering, which trivializes Y. Then $Y \otimes G$ represents the functor on S-schemes*

$$X \mapsto (Y \otimes_{\mathbb{Z}} G(X_{S'}))^{\mathrm{Aut}(S'/S)}.$$

More precisely, for every S-scheme X the isomorphism from Lemma 2.1.4 restricts to a functorial group isomorphism

$$(Y \otimes G)(X) \cong (Y \otimes_{\mathbb{Z}} G(X \times_S S'))^{\mathrm{Aut}(S'/S)}$$

Proof. This follows from Lemma 2.1.4, since $(Y \otimes G)(X) \cong ((Y \otimes G)(X \times_S S'))^{\mathrm{Aut}(S'/S)}$. □

2.1.6 Remark. Comparing the theorem above with Theorem 1.4 in [MRS07], and by means of Yoneda's Lemma, we see that when S is the spectrum of a field our definition of the twist is the same as the one given in [MRS07].

We want to show in the following that the association $(Y, G) \mapsto Y \otimes G$ is a covariant functor. Let Y, Z be Galois S-modules and let G and H be two quasi-projective commutative S-group schemes. Fix a Galois covering S'/S which trivializes Y and Z. Write $Y' = Y \times_S S'$, and define similarly Z', G', H',$(Y \otimes G)'$ and $(Z \otimes H)'$. Fix isomorphisms $\phi\colon \mathbb{Z}^r \to Y(S')$ and $\psi\colon \mathbb{Z}^s \to Z(S')$. Consider the natural isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^r, \mathbb{Z}^s) \otimes_{\mathbb{Z}} \mathrm{Hom}_{S'-gr}(G', H') \xrightarrow{\sim} \mathrm{Hom}_{S'-gr}((G')^r, (H')^s). \qquad (2.1)$$

Due to Proposition 1.2.6 the maps ϕ and ψ induce an isomorphism

$$\mathrm{Hom}_{S'-gr}(Y', Z') \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^r, \mathbb{Z}^s),$$

and similarly, we have an isomorphism

$$\mathrm{Hom}_{S'-gr}((G')^r, (H')^s) \to \mathrm{Hom}_{S'-gr}((Y \otimes G)', (Z \otimes H)').$$

Composing all three we get an isomorphism

$$\mathrm{Hom}_{S'-gr}(Y', Z') \otimes_{\mathbb{Z}} \mathrm{Hom}_{S'-gr}(G', H') \xrightarrow{\sim} \mathrm{Hom}_{S'-gr}((Y \otimes G)', (Z \otimes H)') \tag{2.2}$$

and one can check that it does not depend on the choice of ϕ and ψ.

We can equip the groups in (2.1) with a right $\mathrm{Aut}(S'/S)$-action as before. If $\sigma \in \mathrm{Aut}(S'/S)$ and $f \in \mathrm{Hom}(\mathbb{Z}^r, \mathbb{Z}^s)$ set $f\sigma = A_\psi(\sigma^{-1}) f A_\phi(\sigma)$. If $f \in \mathrm{Hom}_{S'-gr}(G', H')$, then set $f\sigma = \rho_H(\sigma^{-1}) f \rho_G(\sigma)$, where ρ_G and ρ_H are the descent data coming from base change as before. And finally, if $f \in \mathrm{Hom}_{S'-gr}((G')^r, (H')^s)$ set $f\sigma = \psi_*(\sigma^{-1}) f \phi_*(\sigma)$. One can check that with this action the isomorphism (2.1) becomes $\mathrm{Aut}(S'/S)$-equivariant and moreover, that the isomorphism (2.2) becomes $\mathrm{Aut}(S'/S)$-equivariant as well.

Since for any two commutative S-group schemes C and D we have the isomorphism $\mathrm{Hom}_{S-gr}(C, D) \cong \mathrm{Hom}_{S'-gr}(C \times_S S', D \times_S S')$, it follows that (2.2) induces an injection

$$\mathrm{Hom}_{S-gr}(Y, Z) \otimes \mathrm{Hom}_{S-gr}(G, H) \hookrightarrow \mathrm{Hom}_{S-gr}(Y \otimes G, Z \otimes H).$$

Therefore to every pair of group homomorphisms $(f, g) \in \mathrm{Hom}_{S-gr}(Y, Z) \times \mathrm{Hom}_{S-gr}(G, H)$ we can associate a homomorphism $f \otimes g \in \mathrm{Hom}_{S-gr}(Y \otimes G, Z \otimes H)$. One can check that this association is indeed functorial, which implies

2.1.7 Proposition. *The association $(Y, G) \mapsto Y \otimes G$ is a covariant functor.*

Finally, we give some properties of twists over fields.

2.1.8 Proposition. *Let K be a field, let Y be a Galois K-module and let G be a commutative algebraic group defined over K. Let $n \in \mathbb{N}$ and let ℓ be a prime number. Let $\mathrm{T}_\ell G$ denote the ℓ-*adic Tate module *of G, that is, the $\mathbb{Z}_\ell$-module $\mathrm{T}_\ell G = \varprojlim_n G(K^s)[\ell^n]$ equipped with its natural action of Γ_K. Then there are Γ_K-equivariant isomorphisms, functorial in Y and G,*

(i) $(Y \otimes G)(K^s) \cong Y(K^s) \otimes_{\mathbb{Z}} G(K^s)$;

(ii) $(Y \otimes G)[n] \cong Y(K^s) \otimes_{\mathbb{Z}} G[n]$;

(iii) $\mathrm{T}_\ell(Y \otimes G) \cong Y(K^s) \otimes_{\mathbb{Z}} \mathrm{T}_\ell G$.

Proof. This is Theorem 2.2 in [MRS07]. We give the proof for the reader's convenience. Note that $\Gamma_K = \mathrm{Aut}(\operatorname{Spec} K^s / \operatorname{Spec} K)^{op}$, so it acts on $Y(K^s)$, $G(K^s)$, etc. *on the left.*

The first statement follows from 2.1.4 taking $X = \operatorname{Spec} K$ and taking the limit over all Galois extensions L/K which trivialize Y. Then (ii) follows from (i), since Y is free, and (iii) follows from taking the inverse limit of (ii) with $n = \ell^m$. □

2.2 The group $\mathrm{Mot}_S(Y,G)$

Let Y be a Galois S-module and let G be a semiabelian S-scheme. Recall that $\mathrm{Mot}_S(Y,G)$ denotes the set of all S-1-motives of the form $[Y \to G]$. (Of course this is just equal to $\mathrm{Hom}_{S-gr}(Y,G)$ but we hope that our notation is better suited to the topics of our study.)

One can make $\mathrm{Mot}_S(Y,G)$ into an abelian group in a natural way: The identity is the 1-motive, whose image in G is trivial, and if $M_1 = [Y \xrightarrow{u_1} G]$ and $M_2 = [Y \xrightarrow{u_2} G]$ are two 1-motives we define their sum to be $M_1 + M_2 := [Y \xrightarrow{u_1+u_2} G]$.

If Y and E are two Galois S-modules we can construct their tensor product $Y \otimes E$. One could do this along the lines of the construction in the previous section, even though E is not quasi-projective, since in this case the descent data that we construct is again effective. Alternatively, we can use Proposition 1.2.6, and say that $Y \otimes E$ is simply the scheme which corresponds to the $\mathbb{Z}$-module $Y(S') \otimes_{\mathbb{Z}} E(S')$, with its associated $\mathrm{Aut}(S'/S)$-action, where S'/S is any Galois covering which trivializes both Y and E. The second construction works only when S is connected and locally noetherian, and for the first construction we also need S to be affine. Those restrictions are unnecessary, but they do not hinder us with respect to our intended applications.

2.2.1 Lemma. *Let S be an affine, connected, locally noetherian scheme. Let Y and E be two Galois S-modules and let G be a quasi-projective semiabelian S-scheme, which is the extension of an abelian scheme by a torus. There is a canonical group isomorphism*

$$\mathcal{S}_E \colon \mathrm{Mot}_S(Y \otimes E, G) \xrightarrow{\sim} \mathrm{Mot}_S(Y, \hat{E} \otimes G)$$

In particular there is a canonical isomorphism

$$\mathcal{S}_Y \colon \mathrm{Mot}_S(Y,G) \xrightarrow{\sim} (\hat{Y} \otimes G)(S).$$

This map is functorial in S.

2.2.2 Remark. If S is the spectrum of a Dedekind domain, Proposition A.5.1 implies that G is automatically quasi-projective.

Proof. Since G is quasi-projective over S, we can construct the twist $\hat{E} \otimes G$ as in the previous section.

Let S'/S be a Galois covering which trivializes Y and E. Then, by Theorem 1.6.2 the groups $\mathrm{Mot}_S(Y \otimes E, G)$ and $\mathrm{Mot}_S(Y, \hat{E} \otimes G)$ are canonically isomorphic to the subsets of $\mathrm{Hom}((Y \otimes E)(S'), G(S'))$ and $\mathrm{Hom}(Y(S'), (\hat{E} \otimes G)(S'))$ which are fixed under the (right) action of the automorphism group $\mathrm{Aut}(S'/S)$. By Lemma 2.1.4 there is a canonical isomorphism

$$(\hat{E} \otimes G)(S') \cong \hat{E} \otimes G(S').$$

Then $\mathcal{S}_E$ is induced by the canonical isomorphism

$$\begin{aligned} \mathrm{Hom}((E \otimes Y)(S'), G(S')) &\to \mathrm{Hom}(Y(S'), \hat{E} \otimes G(S')) \\ u &\mapsto (y \mapsto (e \mapsto u(e \otimes y))) \end{aligned}$$

which is equivariant under the action of $\mathrm{Aut}(S'/S)$, as it is easy to verify.

The proof that the map $\mathcal{S}_E$ is functorial is relatively straightforward, but tedious. We only give a sketch. Let X be an S-scheme which is also affine, connected and locally noetherian. Let Y_X, G_X, ... denote the base change of Y, G, ... to X. For any appropriate S-schemes Z and H there is an injective map $\mathrm{Mot}_S(Z,H) \to \mathrm{Mot}_X(Z_X, H_X)$. So we need to show that the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Mot}_X(Y_X \otimes E_X, G) & \longrightarrow & \mathrm{Mot}_X(Y_X, \hat{E}_X \otimes G) \\ \uparrow & & \uparrow \\ \mathrm{Mot}_S(Y \otimes E, G) & \longrightarrow & \mathrm{Mot}_S(Y, \hat{E} \otimes G) \end{array} \tag{2.3}$$

To do that pick a Galois covering S'/S which trivializes Y and E, and let $X' = X \times_S S'$. Then one shows that the diagram

$$\begin{array}{ccc} \mathrm{Hom}((Y_X \otimes E_X)(X'), G_X(X')) & \longrightarrow & \mathrm{Hom}(Y_X(X'), (E_X \otimes G_X)(X')) \\ \uparrow & & \uparrow \\ \mathrm{Hom}((Y \otimes E)(S'), G(S')) & \longrightarrow & \mathrm{Hom}(Y(S'), (E \otimes G)(S') \end{array}$$

commutes and is equivariant under the natural right $\mathrm{Aut}(S'/S)$-action. Since the groups in (2.3) are precisely the subgroups of the second diagram which are fixed under the action of $\mathrm{Aut}(S'/S)$, the claim follows. □

Chapter 3

The Tate Module

In this chapter we will recall the theory of the Tate module of a K-1-motive for a perfect field K. To any prime number ℓ and any such 1-motive M one can associate a $\mathbb{Z}_\ell$-module $\mathrm{T}_\ell M$ which is called the *Tate module* of M. This module comes with a natural action of the Galois group Γ_K, which induces an ℓ-adic Galois representation. It also comes with additional structure: if $M = [Y \to G]$ then the Tate module $\mathrm{T}_\ell M$ is a part of an exact sequence

$$\alpha_\ell(M)\colon 0 \to \mathrm{T}_\ell G \to \mathrm{T}_\ell M \to Y \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to 0.$$

Our purpose is to construct the Tate module and study some implications for the associated ℓ-adic Galois representation which come from the extension $\alpha_\ell(M)$. We present a relatively standard explicit construction in the first section. Next, in Section 3.2, we define and study the extension $\alpha_\ell(M)$. The mapping $M \mapsto \alpha_\ell(M)$ is called the *Abel-Jacobi map*. We define it and present its basic properties.

In Section 3.3 we define a mapping which we call the *Kummer map*. It is a group homomorphism from a certain subgroup U of Γ_K to the group $\mathrm{Hom}_{\mathbb{Z}_\ell}(Y \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \mathrm{T}_\ell G)$. This map was essentially discovered and studied by Kummer. Actually, studying the Tate modules of 1-motives $[Y \to \mathbb{G}_m]$ over a field K is just another way to look at Kummer extensions.

In the last section we define a certain map $\varepsilon_{\mathrm{T}_\ell M}$ which we have named the *Pink map*. Its domain is a certain open subset $X_{\mathrm{T}_\ell M}$ of the group of $\mathbb{Z}_\ell$-automorphisms of a Tate module $\mathrm{T}_\ell M$. Its image lies in the group $\mathrm{Hom}(Y \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \mathrm{T}_\ell G) \otimes_{\mathbb{Z}_\ell} (\mathbb{Q}_\ell/\mathbb{Z}_\ell)$ which is also isomorphic to the *Barsotti-Tate group* of the twist $\hat{Y} \otimes G$. This map was first studied by Pink (see [Pin04], particularly Section 3) in the case of 1-motives of the type $[\mathbb{Z} \to A]$, where A is an abelian variety. (We owe this reference to Antonella Perucca.) The main application of the Pink map comes when we consider 1-motives M over local fields or number fields. It will be shown in the next chapter that if $\mathfrak{p}$ is a prime ideal for which the ℓ-adic representation associated to M is unramified, then we can use the Pink map to relate the image of the Frobenius automorphism $\phi_\mathfrak{p}$ to the reduction of M modulo $\mathfrak{p}$. In this chapter we will construct the Pink map and present those properties which do not depend on the base field.

Throughout this chapter K will be a fixed perfect field. In view of Theorem 1.6.2 and Corollary 1.6.3, we will identify a Galois K-module Y with its set of

points $Y(K^s)$ equipped with a continuous left Γ_K-action. For any K-1-motive $Y \xrightarrow{u} G$ we will identify u with $u(K^s)$.

3.1 Construction and basic properties

The module M[n]

Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive and let n be a positive integer n. We have a morphism $[n]\colon M \to M$, consisting of the multiplication-by-n maps on Y and G. Its associated commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{u} & G \\ \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle [n]} \\ Y & \xrightarrow{u} & G \end{array}$$

induces a morphism of group schemes $Y \to Y \times_G G$, $y \mapsto (ny, u(y))$. We define

$$M[n] := (Y \times_G G)(\bar{K})/Y(\bar{K}).$$

In other words, $M[n] := K_nM/Q_nM$, where

$$K_nM := \{(y, P) \in Y(\bar{K}) \times G(\bar{K})\colon u(y) = [n]P\},$$

and

$$Q_nM := \{(nz, u(z)) \in K_nM\colon z \in Y\}$$

It is easy to see that $M[n]$ is a $\mathbb{Z}/n$-module. Moreover, the Galois action on $Y(\bar{K})$ and $G(\bar{K})$ induces a Galois action on K_nM, setting $\sigma\colon (y, P) \mapsto (\sigma y, \sigma P)$ for every $\sigma \in \Gamma_K$. This action fixes Q_nM and induces a well-defined Galois action on $M[n]$, which is compatible with the $\mathbb{Z}/n$-module structure.

Let $M = [Y \xrightarrow{u} G]$ and $M' = [Y' \xrightarrow{u'} G']$ be two K-1-motives and let $f\colon M \to M'$ be a morphism, $f = (f_{-1}, f_0)$. We associate to it a morphism $f[n]\colon M[n] \to M'[n]$ of $\mathbb{Z}/n$-modules as follows. The map f induces a morphism

$$K_nf\colon K_nM \to K_nM',\ (y, P) \mapsto (f_{-1}(y), f_0(P)).$$

This is a well-defined map which sends Q_nM in Q_nM', hence it induces a well-defined map $f[n]\colon M[n] \to M'[n]$. One checks that this map is compatible with the action of Γ_K.

Thus the association $M \mapsto M[n]$ becomes a functor of the category of K-1-motives into the category of $(\mathbb{Z}/n)[\Gamma_K]$-modules. We show next that this functor is "exact".

3.1.1 Lemma. *Let M,M' and M'' be K-1-motives and let $f\colon M' \to M$ and $g\colon M \to M''$ be two morphisms. Assume that the sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is exact. Then the following sequence is exact:

$$0 \to M'[n] \xrightarrow{f[n]} M[n] \xrightarrow{g[n]} M''[n] \to 0$$

By an *exact* sequence of 1-motives we mean, as in Section 1.5, that the induced sequences on the underlying schemes are exact.

Proof. Let $M = [Y \xrightarrow{u} G]$, $M' = [Y' \xrightarrow{u'} G']$, $M'' = [Y'' \xrightarrow{u''} G'']$, $f = (f_{-1}, f_0)$, $g = (g_{-1}, g_0)$. The proof of the lemma consists of simple diagram chasing. The following commutative diagram with exact rows can be helpful to follow the argument:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y' & \xrightarrow{f_{-1}} & Y & \xrightarrow{g_{-1}} & Y'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle u'} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u''} & & \\ 0 & \longrightarrow & G' & \xrightarrow{f_0} & G & \xrightarrow{g_0} & G'' & \longrightarrow & 0 \end{array}$$

To show that $f[n]$ is injective suppose that $(y', P') \in K_\ell M'$ is such that $(f_{-1}(y'), f_0(P')) = (nz, u(z))$ for some $z \in Y$. But since f_{-1} is injective and the quotient Y/Y' is torsion-free, it follows that $y' = nz'$ for some $z' \in Y'$, such that $f_{-1}(z') = z$. But then $u'(z') - P' \in \ker f_0$. Since f_0 is injective, it follows that $P' = u(z')$, hence $(y', P') \in Q_\ell M'$. This proves the infectivity of $f[n]$.

Next we show that $g[n]$ is surjective. Let $(y'', P'') \in K_n M''$. By the surjectivity of g_{-1} and g_0 it follows that there exist $y \in Y$ and $P \in G(\bar{K})$ such that $g_{-1}(y) = y''$ and $g_0(P) = P''$. Then $u(y) - nP \in \ker g_0 = \operatorname{Im} f_0$, hence we can pick $Q \in \ker g_0$ such that $nQ = u(y) - nP$. Then $(y, P + Q) \in K_\ell M$ and its image in $K_\ell M''$ is (y'', P''). It follows that $g[n]$ is surjective.

To prove that $\operatorname{Im} f[n] \subseteq \ker g[n]$ is trivial. Let $(y, P) \in K_\ell M$ be such that $(g_{-1}(y), g_0(P)) = (nz'', u''(z))$. Since g_{-1} is surjective, there exists $z \in Y$ such that $g_{-1}(z) = z''$. Then it follows that $y - nz \in \ker g_{-1}$ and that $P - u(Z) \in \ker g_0$. Let $y' \in Y'$ and $P' \in G(\bar{K})$ be such that $f_{-1}(y') = y - nz$ and $f_0(P') = P - u(z)$. Then $u'(y') - nP' \in \ker f_0$, hence $nP' = u(y')$ and $(y', P') \in K_n M$. Since $(f_{-1}(y'), f_0(P')) - (y, P) \in Q_\ell M$ it follows that $\operatorname{Im} f[n] \supseteq \ker g[n]$. This completes the proof. □

Let G be a semiabelian variety and let Y be a Galois K-module. If we interpret them as the 1-motives $[\{0\} \to G]$ and $[Y \to \{0\}]$ respectively, we see that $G[n]$ is the set of n-torsion points in $G(\bar{K})$ and that $Y[n] = Y/n$.

The weight filtration on M[n]

The previous lemma implies that the weight filtration W which we associated to a 1-motive $M = [Y \to G]$ in Section 1.5 induces a corresponding filtration on $M[n]$. Namely, if G is an extension of an abelian variety A by a torus T we have:

$$W_i(M[n]) = \begin{cases} 0 & \text{for } i < -2, \\ M[n] & \text{for } i \geq 0, \\ G[n] & \text{for } i = -1, \\ T[n] & \text{for } i = -2. \end{cases} \tag{3.1}$$

The associated grading Gr^W is

$$Gr_i^W(M[n]) = \begin{cases} 0 & \text{for } i < -2 \text{ or } i \geq 1, \\ Y[n] & \text{for } i = 0, \\ A[n] & \text{for } i = -1, \\ T[n] & \text{for } i = -2, \end{cases} \tag{3.2}$$

and we have exact sequences

$$0 \to T[n] \to G[n] \to A[n] \to 0 \tag{3.3}$$

and

$$0 \to G[n] \to M[n] \to Y[n] \to 0. \tag{3.4}$$

If we set $r := \operatorname{rk} Y$, $a := \dim A$ and $t := \dim T$, it follows from the exact sequences above that $M[n]$ is isomorphic to $(\mathbb{Z}/n)^{r+t+2a}$ as a $\mathbb{Z}/n$-module.

Projection and inclusion maps

Let m and n be two positive integers with m dividing n and let $M = [Y \xrightarrow{u} G]$ be a 1-motive. We have the maps

$$K_nM \to K_mM,\ (y, P) \mapsto (y, \frac{n}{m}P)$$

and

$$K_mM \to K_nM,\ (y, P) \mapsto (\frac{n}{m}y, P),$$

which induce maps

$$\pi_{m|n} \colon M[n] \to M[m]$$

and

$$\iota_{m|n} \colon M[m] \to M[n]$$

respectively. We gather their properties in the following lemma:

3.1.2 Lemma.

(i) The maps $\pi_{m|n}$ and $\iota_{m|n}$ are well-defined, Γ_K-equivariant morphisms of $\mathbb{Z}/n$-modules;

(ii) $\pi_{m|n}$ is surjective; $\iota_{m|n}$ is injective;

(iii) Let $f \colon M \to M'$ be a morphism of 1-motives. Then the following diagrams commute:

$$\begin{array}{ccc} M[n] & \xrightarrow{\pi_{m|n}} & M[m] \\ \downarrow{\scriptstyle f[n]} & & \downarrow{\scriptstyle f[m]} \\ M'[n] & \xrightarrow{\pi_{m|n}} & M'[m] \end{array} \qquad \begin{array}{ccc} M[m] & \xrightarrow{\iota_{m|n}} & M[n] \\ \downarrow{\scriptstyle f[m]} & & \downarrow{\scriptstyle f[n]} \\ M'[m] & \xrightarrow{\iota_{m|n}} & M'[n] \end{array}$$

Proof. Statement (i) follows easily from the definitions. That $\pi_{m|n}$ is surjective follows from the fact that the map $K_nM \to K_mM$, $(y,P) \mapsto (y, \frac{n}{m}P)$ is surjective. To show that $\iota_{m|n}$ is injective note that if $(\frac{n}{m}y, P) \in Q_nM$ then $(y,P) \in Q_mM$. This shows statement (ii). The third statement follows from the commutativity of the diagrams

$$\begin{array}{ccc} K_nM & \longrightarrow & K_mM \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ K_nM' & \longrightarrow & K_mM' \end{array} \qquad \begin{array}{ccc} K_mM & \longrightarrow & K_nM \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ K_mM' & \longrightarrow & K_nM' \end{array}$$

□

It follows from the previous lemma that the maps $\pi_{m|n}$ and $\iota_{m|n}$ are compatible with the weight filtration.

The ℓ-adic Tate module

Let ℓ be a fixed prime number. Let $M = [Y \to G]$ be a K-1-motive. We write $\pi_n := \pi_{\ell^{n-1}|\ell^n}$ and $\iota_n := \iota_{\ell^{n-1}|\ell^n}$. Then the **$\ell$-adic Tate module** of M is the projective limit

$$\mathrm{T}_\ell M := \varprojlim_n M[\ell^n]$$

with respect to the maps $\pi_n \colon M[\ell^n] \to M[\ell^{n-1}]$. The **$\ell$-adic Barsotti-Tate group** of M is the injective limit

$$\mathrm{B}_\ell M := \varinjlim_n M[\ell^n],$$

with respect to the maps $\iota_n \colon M[\ell^{n-1}] \to M[\ell^n]$. We also define the $\mathbb{Q}_\ell$-vector space

$$\mathrm{V}_\ell M := \mathrm{T}_\ell M \otimes \mathbb{Q}_\ell.$$

This space is equipped with a canonical embedding $\mathrm{T}_\ell M \hookrightarrow \mathrm{V}_\ell M$. We can define an ℓ-adic norm $\|\cdot\|_\ell$ on $\mathrm{V}_\ell M$ by declaring the unit ball to be the image of $\mathrm{T}_\ell M$.

The following properties of the ℓ-adic Tate module are a direct consequence of the properties of the modules $M[\ell^n]$ studied above

3.1.3 Lemma. *Let $M = [Y \to G]$ be a K-1-motive, where G is the extension of an abelian variety A by a torus T. Denote $r := \mathrm{rk}\, Y$, $a := \dim A$ and $t := \dim T$.*

(i) The ℓ-adic Tate module $\mathrm{T}_\ell M$ is a free $\mathbb{Z}_\ell$-module of rank $r + t + 2a$.

(ii) The Galois group Γ_K acts continuously on $\mathrm{T}_\ell M$.

(iii) The association $M \mapsto \mathrm{T}_\ell M$ is a covariant functor from Mot_K into the category of finitely-generated free $\mathbb{Z}_\ell$-modules with continuous Γ_K-action.

(iv) The weight filtration W on M induces a weight filtration on $\mathrm{T}_\ell M$:

$$W_i(\mathrm{T}_\ell M) = \begin{cases} 0 & \text{for } i < -2, \\ \mathrm{T}_\ell M & \text{for } i \geq 0, \\ \mathrm{T}_\ell G & \text{for } i = -1, \\ \mathrm{T}_\ell T & \text{for } i = -2. \end{cases} \tag{3.5}$$

The associated grading is

$$Gr_i^W(\mathrm{T}_\ell M) = \begin{cases} 0 & \text{for } i < -2 \text{ or } i \geq 1, \\ \mathrm{T}_\ell Y & \text{for } i = 0, \\ \mathrm{T}_\ell A & \text{for } i = -1, \\ \mathrm{T}_\ell T & \text{for } i = -2, \end{cases} \tag{3.6}$$

and we have exact sequences

$$0 \to \mathrm{T}_\ell T \to \mathrm{T}_\ell G \to \mathrm{T}_\ell A \to 0 \tag{3.7}$$

and

$$0 \to \mathrm{T}_\ell G \to \mathrm{T}_\ell M \to \mathrm{T}_\ell Y \to 0. \tag{3.8}$$

(v) We have canonical isomorphisms

$$\mathrm{B}_\ell M \cong \mathrm{T}_\ell M \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell, \qquad \mathrm{T}_\ell M \cong \mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathrm{B}_\ell M).$$

Proof. The first four statements follow from their respective finite equivalents after taking limits. For the last statement note that $\mathrm{T}_\ell M \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \cong \varinjlim_n (\mathrm{T}_\ell M \otimes \mathbb{Z}/\ell^n) = \varinjlim_n M[\ell^n] = \mathrm{B}_\ell M$, and that $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathrm{B}_\ell M) \cong \varprojlim_n \mathrm{Hom}(\mathbb{Z}/n, M[\ell^n]) = \mathrm{T}_\ell M$. □

We will use the notation $\mathrm{Aut}(\mathrm{T}_\ell M)$ to denote those $\mathbb{Z}_\ell$-automorphisms of the Tate module $\mathrm{T}_\ell M$ which respect the exact sequences (3.7) and (3.8). The action of the Galois group then induces an ℓ-adic Galois representation

$$\rho_\ell(M) \colon \Gamma_K \to \mathrm{Aut}(\mathrm{T}_\ell M).$$

3.2 The Abel-Jacobi map

The Tate module $\mathrm{T}_\ell M$ of a 1-motive $M = [Y \to G]$ is an extension of the $\mathbb{Z}_\ell[\Gamma_K]$-module $\mathrm{T}_\ell Y$ by $\mathrm{T}_\ell G$. Hence to every 1-motive we can associate an element $\alpha_\ell(M)$ in the group of such extensions $\mathrm{Ext}_{\Gamma_K}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G)$. In this section we will study some of the properties of this map, which we call the **Abel-Jacobi map**, following Jannsen [Jan95] and Jossen [Jos09]. This map will be needed to prove the results given in Chapter 5.

First we need to give some generalities about extensions. Let Γ be a profinite group, n be a positive integer and let A and B be $\mathbb{Z}/n$-modules with a continuous Γ-action. We are interested in extensions of $(\mathbb{Z}/n)[\Gamma]$-modules

$$0 \to B \to C \to A \to 0$$

which *split* when considered as $\mathbb{Z}/n$-extensions. We will denote the group of those extensions by $\mathrm{Ext}^s_\Gamma(A, B)$.

3.2.1 Lemma. *Let Γ be a profinite group and let A and B be two $(\mathbb{Z}/n)[\Gamma]$-modules which are free and finitely-generated as $\mathbb{Z}/n$-modules. There is a canonical isomorphism*

$$\beta_n\colon \operatorname{Ext}^s_\Gamma(A,B) \xrightarrow{\sim} H^1(\Gamma, \operatorname{Hom}_{\mathbb{Z}/n}(A,B))$$

Proof. We will describe β_n explicitly. Let

$$\xi\colon 0 \to B \to C \xrightarrow{p} A \to 0$$

be an element in $\operatorname{Ext}_\Gamma(A,B)$. Fix a section $s\colon A \to C$. The group Γ acts on $\operatorname{Hom}_{\mathbb{Z}/n}(A,C)$, by the rule $\sigma f := \sigma \circ f \circ \sigma^{-1}$. One can check that $(\sigma - 1)s$ lies in $\operatorname{Hom}_{\mathbb{Z}/n}(A,B)$, so we can define $\beta_n(\xi)$ to be given by the 1-cocycle

$$\beta_n(\xi) = [\sigma \mapsto (\sigma - 1)s]$$

One checks that this definition does not depend on the choice of s hence $\beta_n(\xi)$ is well-defined.

Next we show that β is a group homomorphism. Let

$$\xi\colon 0 \to B \to C \xrightarrow{p} A \to 0$$

and

$$\xi'\colon 0 \to B \to C' \xrightarrow{p'} A \to 0$$

be two extensions, and let

$$\xi + \xi'\colon 0 \to B \to C'' \xrightarrow{p''} A \to 0$$

C be their Baer sum. This means that C'' is the quotient of $X = \{(c,c')\colon pc = p'c'\}$ by the subgroup $\{(b,-b)\colon b \in B\}$. Let s and s' be sections of p and p' respectively. Then we get a section $t\colon A \to X$, $t\colon a \mapsto (s(a), s'(a))$. Composing with the map $X \to C''$ we get a section $s''\colon A \to C''$. One then checks that for every $\sigma \in \Gamma$ we have $(\sigma - 1)s + (\sigma - 1)s' = (\sigma - 1)s''$, which implies that $\beta_n(\xi) + \beta_n(\xi') = \beta_n(\xi'')$. This shows that β_n is a group homomorphism.

To show that β_n is injective, assume that for some extension $\xi : 0 \to B \to C \xrightarrow{p} A \to 0$, we have that $\beta_n(\xi) = 0$. This means that if $s\colon A \to C$ is a section of p, then there exists a map $f \in \operatorname{Hom}_{\mathbb{Z}/n}(A,B)$ such that for every $\sigma \in \Gamma$ we have $(\sigma - 1)s = (\sigma - 1)f$. But then $s - f$ is a Γ-invariant section of p, which implies that the extension ξ splits. Hence β_n is injective.

Finally we show that $\beta_n(\xi)$ is surjective. Let $f\colon \Gamma \to \operatorname{Hom}_{\mathbb{Z}/n}(A,B)$ be a 1-cycle. Consider the extension

$$\xi\colon 0 \to B \to B \oplus A \to A \to 0,$$

where Γ acts on $B \oplus A$ by the rule $\sigma(b,a) := (\sigma b + f(\sigma)(\sigma a), \sigma a)$. It is easy to check that $\xi \in \operatorname{Ext}^s_\Gamma(A,B)$ and that $\beta_n(\xi) = [f]$. □

Let ℓ be a prime number. If Γ is a profinite group and A and B are finitely-generated free $\mathbb{Z}_\ell$-modules with continuous left Γ-action we will use the notation $\operatorname{Ext}_\Gamma(A,B)$ to denote the group of $\mathbb{Z}_\ell[\Gamma]$-extensions $0 \to B \to C \to A \to 0$. Note that every such extension is split when considered as an extension of $\mathbb{Z}_\ell$-modules.

3.2.2 Lemma. *Let Γ be a profinite group, let ℓ be a prime number and let A and B be two finitely-generated free $\mathbb{Z}_\ell$-modules with continuous left Γ-action. There is a canonical isomorphism*

$$\beta\colon \operatorname{Ext}_\Gamma(A,B) \xrightarrow{\sim} H^1(\Gamma, \operatorname{Hom}_{\mathbb{Z}_\ell}(A,B))$$

Proof. The proof is analogous to the proof of the previous lemma. □

3.2.3 Lemma. *Let A and B be finitely-generated free $\mathbb{Z}_\ell$-modules equipped with a continuous action of a profinite group Γ. Then there is a canonical isomorphism of $\mathbb{Z}_\ell$-modules*

$$\operatorname{Ext}_\Gamma(A,B) \xrightarrow{\sim} \varprojlim_n \operatorname{Ext}^s_\Gamma(A/\ell^n, B/\ell^n)$$

Proof. One could prove this directly, or we can use the isomorphisms we have constructed in the previous two lemmas. It is easy to show that we get a commutative diagram

$$\begin{array}{ccc} \operatorname{Ext}_\Gamma(A,B) & \longrightarrow & \varprojlim_n \operatorname{Ext}^s_\Gamma(A/\ell^n, B/\ell^n) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \varprojlim_n \beta_{\ell^n}} \\ H^1(\Gamma, \operatorname{Hom}_{\mathbb{Z}_\ell}(A,B)) & \longrightarrow & \varprojlim_n H^1(\Gamma, \operatorname{Hom}_{\mathbb{Z}/\ell^n}(A/\ell^n, B/\ell^n)) \end{array}$$

The lower row is an isomorphism due to Lemma A.6.1, which then implies our claim. □

Let us fix a semiabelian variety G and a Galois K-module Y. Then the correspondence $M \mapsto M[n]$ induces a mapping

$$\alpha_{[n]}\colon \operatorname{Mot}_K(Y,G) \to \operatorname{Ext}^s_{\Gamma_K}(Y[n], G[n])$$

which associates to every 1-motive M the extension (3.4). Taking limits over the powers of a prime number ℓ we get the **Abel-Jacobi map**

$$\alpha_\ell\colon \operatorname{Mot}_K(Y,G) \to \operatorname{Ext}_{\Gamma_K}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G).$$

The image of α_ℓ is precisely the extension (3.8)

$$\alpha_\ell(M)\colon 0 \to \mathrm{T}_\ell Y \to \mathrm{T}_\ell M \to \mathrm{T}_\ell G \to 0.$$

3.2.4 Lemma. *The map $\alpha_{[n]}$ is a group homomorphism. In particular, α_ℓ is a group homomorphism.*

Proof. Let $M = [Y \xrightarrow{u} G]$,$M' = [Y \xrightarrow{u'} G]$ be two 1-motives. We need to show that $\alpha_{[n]}(M + M') = \alpha_{[n]}(M) + \alpha_{[n]}(M')$.

Consider the 1-motive $M'' = [Y \xrightarrow{(u,u')} G \times G]$. We have a morphism of 1-motives $f\colon M'' \to M + M'$ given by the commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{(u,u')} & G \times G \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle m} \\ Y & \xrightarrow{u+u'} & G \end{array}$$

where the vertical map on the right is addition. This map induces a morphism $f[n]\colon M''[n] \to (M + M')[n]$. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G[n] \otimes_{\mathbb{Z}/n} G[n] & \longrightarrow & M''[n] & \longrightarrow & Y/n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f[n]} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & G[n] & \longrightarrow & (M+M')[n] & \longrightarrow & Y/n & \longrightarrow & 0 \end{array}$$

By the snake lemma the map in the middle column is surjective, and its kernel is the set $\{(\tau, -\tau)\colon \tau \in G[n]\}$. Hence the extension $(M + M')[n]$ is precisely the Baer sum of $M[n]$ and $M'[n]$. □

Finally, we want to see how the Abel-Jacobi map relates to the map $\mathcal{S}_Y$ defined in Lemma 2.2.1. Consider the semiabelian variety $\hat{Y} \otimes G$. The short exact sequence

$$0 \to (\hat{Y} \otimes G)[n] \to (\hat{Y} \otimes G)(\bar{K}) \xrightarrow{[n]} (\hat{Y} \otimes G)(\bar{K}) \to 0$$

induces an injection

$$(\hat{Y} \otimes G)(K)/n \hookrightarrow H^1(\Gamma_K, (\hat{Y} \otimes G)[n])$$

By 2.1.8 there is a canonical isomorphism $(\hat{Y} \otimes G)[n] \cong \mathrm{Hom}_{\mathbb{Z}}(Y, G[n])$. Composing with the map $(\hat{Y} \otimes G)(K) \to (\hat{Y} \otimes G)(K)/n$ we get a map

$$\gamma_{[n]}\colon (\hat{Y} \otimes G)(K) \to H^1(\Gamma_K, \mathrm{Hom}(Y, G[n]))$$

Taking limits over the ℓ-powers we have the map

$$\gamma_\ell\colon (\hat{Y} \otimes G)(K) \to H^1(\Gamma_K, \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G))$$

3.2.5 Lemma. *The following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Mot}_K(Y, G) & \xrightarrow{\alpha_{[n]}} & \mathrm{Ext}^s_{\Gamma_K}(Y[n], G[n]) \\ \downarrow{\scriptstyle \mathcal{S}_Y} & & \downarrow{\scriptstyle \beta_n} \\ (\hat{Y} \otimes G)(K) & \xrightarrow{\gamma_{[n]}} & H^1(\Gamma_K, \mathrm{Hom}(Y, G[n])) \end{array}$$

In particular, the diagram

$$\begin{array}{ccc} \mathrm{Mot}_K(Y, G) & \xrightarrow{\alpha_\ell} & \mathrm{Ext}_{\Gamma_K}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G) \\ \downarrow{\scriptstyle \mathcal{S}_Y} & & \downarrow{\scriptstyle \beta} \\ (\hat{Y} \otimes G)(K) & \xrightarrow{\gamma_\ell} & H^1(\Gamma_K, \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G)) \end{array}$$

commutes.

Proof. Let $N = [Y \xrightarrow{u_N} G]$ be a $\bar{K}$-1-motive such that $nN = M$. Then $\gamma_{[n]}(\mathcal{S}_Y M)$ is generated by the class of the cocycle $\sigma \mapsto (\sigma - 1)u_N$.

On the other hand, N induces a map

$$Y \xrightarrow{A_N} K_n M,\ y \mapsto (y, u_N(y))$$

which induces a section $s_N \colon Y[n] \to M[n]$. Then $\beta(\alpha_{[n]}(M))$ is the class of the cocycle $\sigma \mapsto (\sigma - 1)s_N$. But $(\sigma - 1)s_N = (\sigma - 1)A_N$, since the image of those maps lies in $G[n]$ which embeds in $K_n M$. Then

$$\begin{aligned}(\sigma - 1)A_N(y) &= \sigma A_N(\sigma^{-1}y) - A_N(y)\\ = (0, \sigma u_N(\sigma^{-1}y) - u_N(y)) &= (0, (\sigma - 1)u_N(y)).\end{aligned}$$

This implies that $\gamma_{[n]}(\mathcal{S}_Y M) = \beta(\alpha_{[n]}(M))$. □

3.3 The Kummer map

Let Γ be a profinite group and let ℓ be a prime number. We fix for the moment a Γ-invariant extension

$$\xi \colon 0 \to B \to C \xrightarrow{p} A \to 0$$

of free $\mathbb{Z}_\ell$-modules with a continuous Γ-action. Let $\mathrm{Aut}(\xi)$ denote all $\mathbb{Z}_\ell$-automorphisms of C (not necessarily Γ-invariant) which induce well-defined automorphisms of B. We define a restriction map

$$p^* \colon \mathrm{Aut}(\xi) \to \mathrm{Aut}(B)$$

and a projection map

$$p_* \colon \mathrm{Aut}(\xi) \to \mathrm{Aut}(A)$$

in the obvious way. We also define the map

$$\begin{aligned}\Delta \colon \mathrm{Hom}(A, B) &\to \mathrm{Aut}(A)\\ f &\mapsto (c \mapsto c + f(pc))\end{aligned}$$

3.3.1 Lemma.

(i) The map Δ is a well-defined group homomorphism.

(ii) The following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(A, B) \xrightarrow{\Delta} \mathrm{Aut}(\xi) \xrightarrow{(p_*, p^*)} \mathrm{Aut}(A) \times \mathrm{Aut}(B) \longrightarrow 1$$

Proof. The first statement is a trivial calculation following from the fact that if $f \in \mathrm{Hom}(A, B)$ then $pf = 0$. It is also trivial to see that the image of Δ lies in $\ker(p_*, p^*)$.

To prove the remainder of the second statement consider the map

$$\delta_\xi \colon \ker(p_*, p^*) \to \mathrm{Hom}(A, B)$$

defined as follows. Let $s \colon A \to C$ be a section of p. Then we set

$$\delta_\xi \colon \sigma \mapsto (a \mapsto (\sigma - 1)s(a))$$

One then checks that this definition of δ_ξ does not depend on the choice of s and that δ_ξ is the inverse map of Δ. We omit those verifications. □

Let ρ_A, ρ_B and ρ_ξ be the representations associated to A, B and C respectively. Let $U_{\hat{A}\otimes B}(\Gamma)$ denote the kernel of the map $(p_*, p^*) \circ \rho_\xi$. It does not depend on ξ since $U_{\hat{A}\otimes B}(\Gamma) = \ker \rho_B \cap \ker \rho_A$.

Composing ρ_ξ with the map δ_ξ defined in the proof of the previous lemma gives us a map

$$\begin{aligned} \boldsymbol{\delta}\colon \operatorname{Ext}_\Gamma(A,B) &\to \operatorname{Hom}(U_{\hat{A}\otimes B}(\Gamma), \operatorname{Hom}(A,B)) \\ \xi &\mapsto \delta_\xi \circ \rho_\xi \end{aligned}$$

3.3.2 Lemma. *Let Q denote the quotient $\Gamma/U_{\hat{A}\otimes B}(\Gamma)$.*

(i) The map $\boldsymbol{\delta}$ is a group homomorphism whose kernel is canonically isomorphic to $H^1(Q, \operatorname{Hom}(A,B))$.

(ii) For any ξ, $\boldsymbol{\delta}(\xi)$ is Q-equivariant.

(iii) If $\varphi \in \operatorname{Hom}_\Gamma(\operatorname{Hom}(A,B), \operatorname{Hom}(A',B'))$ then

$$\boldsymbol{\delta}(\varphi\xi) = \varphi \circ \boldsymbol{\delta}(\xi).$$

Proof. The first two statements follow from noticing that $\boldsymbol{\delta}$ is just the composition of the canonical isomorphism $\beta\colon \operatorname{Ext}_\Gamma(A,B) \to H^1(\Gamma, \operatorname{Hom}(A,B))$ (described in Lemma 3.2.1) with the restriction map

$$H^1(\Gamma, \operatorname{Hom}(A,B)) \to H^1(U_{\hat{A}\otimes B}(\Gamma), \operatorname{Hom}(A,B)).$$

Then they are a corollary of the restriction-inflation sequence

$$0 \to H^1(Q, \operatorname{Hom}(A,B)) \to H^1(\Gamma, \operatorname{Hom}(A,B)) \to H^1(U_{\hat{A}\otimes B}(\Gamma), \operatorname{Hom}(A,B))^Q$$

The third statement follows from the commutative diagram

$$\begin{array}{ccc} H^1(\Gamma, \operatorname{Hom}(A,B)) & \longrightarrow & H^1(U_{\hat{A}\otimes B}(\Gamma), \operatorname{Hom}(A,B)) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ H^1(\Gamma, \operatorname{Hom}(A',B')) & \longrightarrow & H^1(U_{\hat{A}\otimes B}(\Gamma), \operatorname{Hom}(A',B')) \end{array}$$

□

We apply this theory to the case of 1-motives. Let Y be a Galois K-module and let G be a semiabelian variety. Then we construct the map

$$\boldsymbol{\delta}\colon \operatorname{Ext}_{\Gamma_K}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G) \to \operatorname{Hom}(U_{\mathrm{T}_\ell(\hat{Y}\otimes G)}(\Gamma_K), \mathrm{T}_\ell(\hat{Y}\otimes G))$$

To each 1-motive M it associates a map

$$\delta_\ell(M)\colon U_{\mathrm{T}_\ell(\hat{Y}\otimes G)}(\Gamma_K) \to \mathrm{T}_\ell(\hat{Y}\otimes G) \tag{3.9}$$

which we will call the **Kummer map**. This map is a composition of $\boldsymbol{\delta}$ and the Abel-Jacobi map α_ℓ. It has all the properties described in Lemma 3.3.2.

3.4 The Pink map

We retain the notation of the previous section.

The group $\mathrm{Aut}(A) \times \mathrm{Aut}(B)$ acts on $\mathrm{Hom}(A, B)$ as follows: If (σ, τ) is a tuple of automorphisms and $f \in \mathrm{Hom}(A, B)$ then $(\sigma, \tau)f = \tau \circ f \circ \sigma^{-1}$. We consider the following set in $\mathrm{Aut}(\xi)$:

$$X_\xi := \{\sigma \in \mathrm{Aut}(\xi) \colon (p_*\sigma, p^*\sigma) - 1 \text{ is invertible on } \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell\}.$$

Equivalently, X_ξ is the set of all automorphisms $\sigma \in \mathrm{Aut}(\xi)$ that have no non-trivial fixed point on $\mathrm{Hom}(A, B)$. The group $\mathrm{Aut}(\xi)$ acts on X_ξ by conjugation.

3.4.1 Construction. We will next define a map

$$\varepsilon_\xi \colon X_\xi \to \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

(Note that the $\mathbb{Z}_\ell$-module in the codomain of ε_ξ is canonically isomorphic to $(\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell)/\mathrm{Hom}(A, B)$.) Pick a section $s \colon A \to C$ of p. Then the map $(\sigma - 1)s = \sigma \circ s \circ p_*\sigma^{-1} - s$ is an element in $\mathrm{Hom}(A, B) \subset \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell$. We set

$$\varepsilon_\xi \colon \sigma \mapsto (\sigma - 1)^{-1}[(\sigma - 1)s] \mod \mathrm{Hom}(A, B) \tag{3.10}$$

(We use the square brackets for sake of readability. The element inside of them lies in $\mathrm{Hom}(A, B)$.) One checks easily that this definition does not depend on the choice of the section s.

We can equip the set $\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$ with the discrete topology. Then we have

3.4.2 Lemma. *The set X_ξ is an open subset of $\mathrm{Aut}(\xi)$ and the map ε_ξ is continuous.*

Proof. After fixing a basis, X_ξ can be expressed as the complement of the zero set of a non-trivial system of polynomial equations, which implies that X_ξ is open.

To show that ε_ξ is continuous fix a section s. Then ε_ξ is the composition of the map

$$\sigma \mapsto (\sigma - 1)^{-1}[(\sigma - 1)s]$$

with the projection $\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell \to \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$. The latter map is clearly continuous. After fixing a basis, we can express the former map via rational functions with coefficients in $\mathbb{Q}_\ell$, which implies that it is continuous as well. Hence their composition is a continuous map. □

3.4.3 Lemma.

(i) The map ε_ξ is $\mathrm{Aut}(\xi)$-equivariant;

(ii) Let $\sigma, \sigma' \in X_\xi$ and assume that σ' lies in the closure of the subgroup of $\mathrm{Aut}(\xi)$ generated by σ. Then

$$\varepsilon_\xi(\sigma) = \varepsilon_\xi(\sigma');$$

(iii) If $u \in \ker(p_*, p^*)$ *then*

$$\varepsilon_\xi(u\sigma) = \varepsilon_\xi(\sigma) + (\sigma - 1)^{-1}\delta_\xi(u) \mod \mathrm{Hom}(A, B).$$

Proof. Pick a section $s\colon A \to C$. To prove the first statement let $\sigma \in \mathrm{Aut}(\xi)$ and let $\tau \in X_\xi$. Then modulo $\mathrm{Hom}(A, B)$ we have

$$\begin{aligned}
\varepsilon_\xi(\sigma\tau\sigma^{-1}) - \sigma\varepsilon_\xi(\tau) \equiv \\
(\sigma\tau\sigma^{-1} - 1)^{-1}[(\sigma\tau\sigma^{-1} - 1)s] - \sigma(\tau - 1)^{-1}[(\tau - 1)s] \equiv \\
\sigma(\tau - 1)^{-1}[(\tau - 1)\sigma^{-1}s] - \sigma(\tau - 1)^{-1}[(\tau - 1)s] \equiv \\
\sigma(\tau - 1)^{-1}[(\tau - 1)(\sigma^{-1} - 1)s] \equiv 0,
\end{aligned}$$

where the last equality is a consequence of the fact that $(\sigma^{-1} - 1)s$ lies in $\mathrm{Hom}(A, B)$. This proves statement (i).

Next we show statement (ii). Since X_ξ is open, there exists a sequence $\{\sigma^{n_k}\}_{k\in\mathbb{N}} \subset X_\xi$ which converges to σ'. Then modulo $\mathrm{Hom}(A, B)$ we have

$$\begin{aligned}
\varepsilon_\xi(\sigma^{n_k}) \equiv \\
(\sigma^{n_k} - 1)^{-1}[(\sigma^{n_k} - 1)s] \equiv \\
(\sigma^{n_k} - 1)^{-1}(1 + \sigma + \cdots + \sigma^{n_k - 1})[(\sigma - 1)s] \equiv \\
(\sigma - 1)^{-1}[(\sigma - 1)s] \equiv \varepsilon_\xi(\sigma).
\end{aligned}$$

Since the map ε_ξ is continuous, it follows that $\varepsilon_\xi(\sigma') = \varepsilon_\xi(\sigma)$.

To show statement (iii) one checks through analogous computations as above, that

$$(u\sigma - 1)s = (\sigma - 1)s + \delta_\xi(u).$$

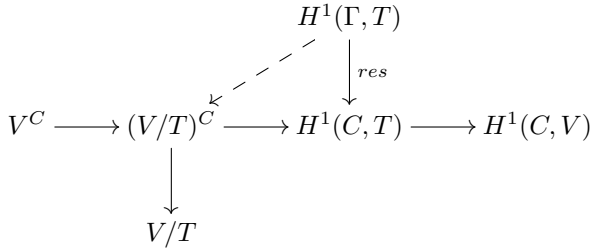
Since $u\sigma - 1$ acts as $\sigma - 1$ on $\mathrm{Hom}(A, B)$, the statement follows immediately. □

The map $\boldsymbol{\varepsilon}$

Let $X_{\hat{A}\otimes B}(\Gamma)$ denote the subset of those elements $\sigma \in \Gamma$ for which $\sigma - 1$ is an automorphism of $\mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell$. We define the map

$$\begin{aligned}
\boldsymbol{\varepsilon}\colon \mathrm{Ext}_\Gamma(A, B) \times X_{\hat{A}\otimes B}(\Gamma) &\to \mathrm{Hom}(A, B) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \\
(\xi, \sigma) &\mapsto \varepsilon_\xi \circ \rho_\xi(\sigma)
\end{aligned}$$

This map has the following cohomological interpretation. Let T be a finitely-generated free $\mathbb{Z}_\ell$-module, and let $V := T \otimes \mathbb{Q}_\ell$. Let Γ be a profinite group acting continuously on T. Let $C \subseteq \Gamma$ be any monogenous subgroup (i.e. C is the closure of a subgroup generated by a single element). Assume that no non-trivial element of V is fixed by C. We have the following commutative diagram whose middle row is exact:



(Here the exact row in the middle comes from applying group cohomology to the short exact sequence $0 \to T \to V \to V/T \to 0$.)

In our case $V^C = \{0\}$. It follows that there exists an element $\sigma \in C$ such that $\sigma - 1$ is an automorphism on V. By Sah's Lemma A.6.3, it follows that $H^1(C, V) = \{0\}$, hence $(V/T)^C \xrightarrow{\sim} H^1(C, T)$. Therefore the restriction map $H^1(\Gamma, T) \to H^1(C, T)$ composed with the embedding $(V/T)^C \subseteq (V/T)$ induces a map

$$\boldsymbol{\varepsilon}_C \colon H^1(\Gamma, T) \to V/T.$$

It is easy to see that after setting $T := \mathrm{Hom}(A, B)$ we arrive at our previous definition. That is, for any $\sigma \in X_{\hat{A}\otimes B}(\Gamma)$ we have

$$\boldsymbol{\varepsilon}(\xi, \sigma) = \boldsymbol{\varepsilon}_{\langle\sigma\rangle}(\beta\xi),$$

where $\langle\sigma\rangle$ denote the closure of the subgroup generated by σ in Γ and β is the canonical isomorphism $\beta \colon \mathrm{Ext}_\Gamma(A, B) \to H^1(\Gamma, \mathrm{Hom}(A, B))$ (see 3.2.1).

The Pink map

Let us apply the constructions given above to the Tate module of a K-1-motive $M = [Y \xrightarrow{u} G]$. We have a map

$$\boldsymbol{\varepsilon} \colon \mathrm{Ext}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G) \times X_{\mathrm{T}_\ell(\hat{Y}\otimes G)}(\Gamma_K) \to \mathrm{B}_\ell(\hat{Y} \otimes G),$$

(see 3.1.3(v)) which to every K-1-motive M associates a map

$$\boldsymbol{\varepsilon}_\ell(M) \colon X_{\mathrm{T}_\ell(\hat{Y}\otimes G)}(\Gamma_K) \to \mathrm{B}_\ell(\hat{Y} \otimes G). \tag{3.11}$$

This map is the composition of the restriction of $\rho_\ell(M)$ on $X_{\mathrm{T}_\ell(\hat{Y}\otimes G)}$ and the map

$$\varepsilon_{\mathrm{T}_\ell M} \colon X_{\mathrm{T}_\ell M} \to \mathrm{B}_\ell(\hat{Y} \otimes G), \tag{3.12}$$

where $X_{\mathrm{T}_\ell M}$ is the set of all automorphisms $\sigma \in \mathrm{Aut}(\mathrm{T}_\ell M)$ which have no non-trivial fixed point in $\mathrm{T}_\ell(\hat{Y} \otimes G)$. We will call latter map the **Pink map**.

Chapter 4

Good reduction of 1-motives

The purpose of this chapter is to study 1-motives over p-adic fields or number fields at places of good reduction. So let us first define what *good reduction* means. This definition is due to Raynaud [Ray94].

4.0.4 Definition.

(i) Let K be a finite extension of $\mathbb{Q}_p$ and let R denote its ring of integers. Let M be a K-1-motive. M has **good reduction** if it can be extended to an R-1-motive, i.e. M has good reduction if there exists an R-1-motive $\mathcal{M}$ whose generic fiber $\mathcal{M} \otimes_R K$ is isomorphic to M. In that case we will call the 1-motive $\overline{M} := \mathcal{M} \otimes_R k$, the **reduction** of M.

(ii) Let K be a number field, R its ring of integers, and let $\mathfrak{p}$ be a prime ideal of R. Let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$. Then a K-1-motive M has **good reduction at $\mathfrak{p}$**, if its lift $M \otimes_K K_\mathfrak{p}$ has good reduction. If this condition holds we will call the 1-motive $M_\mathfrak{p} := \overline{M \otimes_K K_\mathfrak{p}}$, the **reduction of M at $\mathfrak{p}$**.

In the first section we study good reduction over p-adic fields. We prove a version of the Néron-Ogg-Shafarevich criterion for 1-motives (Theorem 4.1.1). We also give the *raison d'être* for the Pink map: It is the means by which the image of the Frobenius automorphism in the ℓ-adic representation associated to a K-1-motive determines the ℓ-part of the reduction of the 1-motive. Thus, the Pink map allows us to translate questions about reduction to questions about Galois representations. This is the meaning of Theorem 4.1.2.

The results about good reduction for 1-motives over p-adic fields have some straightforward corollaries for 1-motives over number fields. We present those corollaries in the second section. In particular, we can combine Theorem 4.1.2 with a version of Chebotarev's density theorem (due to Serre [Ser98]) to compute the densities of prime ideals $\mathfrak{p}$ of good reduction for which the ℓ-part of the reduction of a 1-motive satisfies a given property. The specific statement is given in Theorem 4.2.12. We will present an application of this technique in Chapter 6.

4.1 The local case

In this section we fix a prime number p. We also fix a field K which is a finite extension of $\mathbb{Q}_p$. We will denote its ring of integers by R, the unique maximal ideal by $\mathfrak{p}$ and the residue field by k. We will use Γ_K to denote the absolute Galois group of K and I_K to denote the inertia subgroup. If K'/K is a finite field extension we will use the notation R', $\mathfrak{p}'$, k', $\Gamma_{K'}$ and $I_{K'}$ to denote the corresponding objects associated to K'.

An ℓ-adic representation $\rho\colon \Gamma_K \to \mathrm{Aut}(V)$ is called **unramified** if the inertia subgroup group I_K lies in the kernel of ρ. Then we have the following generalization of of the criterion of Néron-Ogg-Shafarevich to 1-motives:

4.1.1 Theorem. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive. Let ℓ be a prime number, different from p. Then M has good reduction if and only if the ℓ-adic Galois representation $\rho_\ell(M)$ associated to M is unramified.*

Let Y be a Galois k-module and G be a semiabelian variety defined over k. The group $\mathrm{Mot}_k(Y,G)$ is finite and abelian, hence it decomposes as a sum of its ℓ-primary parts over all primes ℓ:

$$\mathrm{Mot}_k(Y,G) = \bigoplus_\ell \mathrm{Mot}_k(Y,G)[\ell^\infty].$$

We will denote the projection of any 1-motive $M \in \mathrm{Mot}_k(Y,G)$ to the ℓ-primary part $\mathrm{Mot}_k(Y,G)[\ell^\infty]$ by $pr_\ell M$ and we will call it the **ℓ-part of** M. Then we have:

4.1.2 Theorem. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive which has good reduction. Let $\phi_\mathfrak{p} \in \mathrm{Aut}(\mathrm{T}_\ell M)$ be the image of the Frobenius automorphism under $\rho_\ell(M)$.*

(i) The element $\phi_\mathfrak{p}$ lies in the domain of the Pink map $\varepsilon_{\mathrm{T}_\ell M}$.

(ii) $\varepsilon_{\mathrm{T}_\ell M}(\phi_\mathfrak{p})$ is an element of $\mathrm{Mot}_K(Y,G)$ which has good reduction.

(iii) The reduction of $\varepsilon_{\mathrm{T}_\ell M}(\phi_\mathfrak{p})$ coincides with the ℓ-part $pr_\ell \overline{M}$ of the reduction of M.

Note that $\varepsilon_{\mathrm{T}_\ell M}(\phi_\mathfrak{p})$ is apriori an element of $\mathrm{B}_\ell(\hat{Y} \otimes G) \cong \mathrm{Hom}_\mathbb{Z}(Y, G[\ell^\infty])$, hence it can be regarded as a K^s-1-motive. Statement (ii) above claims it is actually fixed under the action of Γ_K which makes it into a K-1-motive.

This theorem generalizes Proposition 3.2 in [Pin04]. It can also be rephrased as follows. Let $\mathrm{Mot}_{gr}(Y,G)$ denote the subset of those K-1-motives in $\mathrm{Mot}(Y,G)$ which have good reduction. Then we have a map $\varepsilon_\mathfrak{p}\colon \mathrm{Mot}_{gr}(Y,G) \to \mathrm{B}_\ell(\hat{Y} \otimes G)$ sending M to $\varepsilon_{\mathrm{T}_\ell M}(\phi_\mathfrak{p})$. If $\overline{Y}$ and $\overline{G}$ are the reductions of Y and G over k, then the map pr_ℓ defined above induces a map $\mathrm{Mot}(\overline{Y},\overline{G}) \to \mathrm{B}_\ell(\hat{\overline{Y}} \otimes \overline{G})$, which we will also denote by pr_ℓ. Then the theorem above implies that the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Mot}_{gr}(Y,G) & \xrightarrow{\varepsilon_\mathfrak{p}} & \mathrm{B}_\ell(\hat{Y} \otimes G) \\ \downarrow & & \wr\downarrow \\ \mathrm{Mot}(\overline{Y},\overline{G}) & \xrightarrow{pr_\ell} & \mathrm{B}_\ell(\hat{\overline{Y}} \otimes \overline{G}) \end{array}$$

The rest of this section is devoted to proving the two theorems stated above.

Semiabelian varieties

Let G be a semiabelian variety over K. The following definition is a special case of Definition 4.0.4(i), after we identify G with the 1-motive $[0 \to G]$.

4.1.3 Definition. Let G be a semiabelian variety over K. We say that it has **good reduction** if there exists a semiabelian R-scheme $\mathcal{G}$ which is an extension of an abelian scheme by a torus, such that $G \cong \mathcal{G} \times_R \operatorname{Spec} K$.

Let X be a K-scheme of finite type and let K'/K be a finite field extension. The topology on K' induces a topology on the set $X(K')$ as follows: If X is affine then the topology is the one induced by the standard topology on $\mathbb{A}^n_K(K') \cong K'^n$. If U is a Zariski open subset of X, Y is an affine K-scheme and $f\colon U \to Y$ is any K-morphism, one shows that the induced map $f\colon U(K') \to Y(K')$ is continuous. This implies that one can introduce a topology on an arbitrary K-scheme by taking the topology induced on Zariski open affine subschemes. Any morphism of K-schemes induces thus a continuous morphism on the set of K'-points.

4.1.4 Lemma. *Let X be a separated R-scheme of finite type. Let K'/K be a field extension and let R' be the integral closure of R in K'. Let X_K be the fiber of X at the generic point. Then the map $X(R') \to X_K(K')$ is injective and its image is a compact open subset of $X_K(K')$.*

Proof. Let $P \in X_K(K')$. Consider the diagram

$$\begin{array}{ccccc} \operatorname{Spec} K' & \xrightarrow{P} & X_K & \longrightarrow & X \\ \downarrow & & & \overset{Q}{\nearrow} & \downarrow \\ \operatorname{Spec} R' & & \longrightarrow & & \operatorname{Spec} R \end{array}$$

Since X is separated over R we can apply the Valuative Criterion of Separatedness to conclude that there is at most one point $Q \in X(R')$ which makes the diagram commutative. Hence the map $X(R') \to X_K(K')$ is injective.

For the second part of the statement notice that the image of the map $\mathbb{A}^n_R(R') \to \mathbb{A}^n_K(K')$ is a compact open set. We can therefore show the statement whenever X is affine. The general case follows by gluing. □

4.1.5 Corollary. *Let G be a semiabelian variety that has good reduction $\mathcal{G}$ over R. Let K'/K be a finite field extension and let R' be the integral closure of R in K'. Then the map $\mathcal{G}(R') \to G(K')$ is injective and its image is a compact open subset of $G(K')$.*

Proof. The statement follows from the previous lemma and the fact that $\mathcal{G}$ is separated and of finite type over R. □

4.1.6 Remark. As a result of the previous corollary we can identify the set of integral points $\mathcal{G}(R')$ with its image in $G(K')$.

We have borrowed the following definition from Jossen [Jos09, §3.3.2]

4.1.7 Definition. Let p be a prime number. A commutative topological group T will satisfy property $FG(p)$ if it is topologically finitely generated (that is, it contains a dense finitely-generated subgroup) and contains an open subgroup isomorphic to $\mathbb{Z}_p^r$ for some non-negative integer r.

4.1.8 Lemma. *Let G be a semiabelian variety defined over K. Then the group $G(K)$ satisfies property $FG(p)$.*

Proof. See [Jos09, Proposition 3.3.3]. If G is an abelian variety this is a result of Mattuck [Mat55]. If G is the multiplicative group $\mathbb{G}_m$ over K the result follows from the structure of $K^\times$ and the theory of the p-adic logarithm. This in turn implies the claim for a split torus. For a general torus G which splits over a finite field extension K'/K, we use the fact that $G(K')$ has the required property and that $G(K)$ is a closed subgroup of it. Finally, it is easy to show that if $0 \to A \to B \to C \to 0$ is an exact sequence of commutative topological groups such that A and C satisfy property $FG(p)$ then B satisfies it as well. This proves the general case. □

4.1.9 Lemma. *Let T be a commutative topological group satisfying property $FG(p)$. There exists a unique maximal compact subgroup $T^* \subseteq T$. The points P in T^* are characterized by the property that the identity element is contained in the closure of the set $\{kP \colon k \in \mathbb{Z}_{>0}\}$.*

Proof. Property $FG(p)$ implies that there is an exact sequence of topological groups

$$0 \longrightarrow \mathbb{Z}_p^r \xrightarrow{\ i\ } T \xrightarrow{\ \pi\ } D \longrightarrow 0 \tag{4.1}$$

where D is a finitely-generated abelian group equipped with the discrete topology. Let D^* be its torsion subgroup. Then set $T^* := \pi^{-1}D^*$. The group D^* is finite, hence T^* is compact. Since the image under π of any other compact group must lie in D^* we conclude that T^* is the unique maximal compact subgroup of T.

If $P \in T^*$ then there exists some k such that $kP \in \ker \pi$. Then the sequence $p^n kP$ converges to the identity element e. Conversely, if P is a point such that there exists an increasing sequence a_n with $a_n P \to e$, then $\pi(P)$ must be a torsion point, hence $P \in T^*$. □

4.1.10 Lemma. *Let T be a commutative topological group satisfying property $FG(p)$ and let ℓ be any prime different from p. Then T^* is canonically isomorphic to $T[\ell^\infty] \times T_\ell$, where T_ℓ is the subgroup of infinitely ℓ-divisible points in T.*

Proof. We will again use the exact sequence (4.1). Let D_ℓ denote the infinitely ℓ-divisible subgroup of D. Clearly since D^* is finite we have $D^* = D[\ell^\infty] \times D_\ell$. One also easily sees that

$$\pi(T[\ell^\infty]) \subseteq D[\ell^\infty] \text{ and } \pi(T_\ell) \subseteq D_\ell. \tag{4.2}$$

This implies that $T[\ell^\infty] \cap T_\ell \subseteq \mathbb{Z}_p^r$, hence this intersection is trivial and we have an embedding $T[\ell^\infty] \times T_\ell \subseteq T^*$. To finish the proof of the lemma it is sufficient to show that the embeddings (4.2) are equalities.

We show now that $\pi(T[\ell^\infty]) = D[\ell^\infty]$. Let $x \in D[\ell^\infty]$. Pick a point $y \in T^*$ such that $\pi(y) = x$. Consider the points $y_n = p^n y$. Since $\ell \neq p$ there exists a subsequence $\{n_k\}_{k=1}^\infty$ such that $y - y_{n_k} \in \mathbb{Z}_p^r$. The set $y + \mathbb{Z}_p^r$ is compact, hence the sequence y_{n_k} has a convergent subsequence $y_{n_{k_r}} \longrightarrow x_0$. Let ℓ^s be the order of x. Then $\ell^s y_n = p^n \ell^s y \longrightarrow 0$. We then have that $\pi(x_0) = x$ and $\ell^s x_0 = 0$. This implies that $\pi(T[\ell^\infty]) = D[\ell^\infty]$.

To show that $\pi(T_\ell) = D_\ell$ let $x \in D_\ell$ and let $x_n \in D_\ell$ be a sequence such that $\ell^n x_n = x$. Let $y \in T$ be a pre-image of x and let y_n be arbitrary pre-images of x_n. Then we have $\pi(\ell^n y_n - y) = 0$, hence $\ell^n y_n - y = z_n \in \mathbb{Z}_p^r$. Since ℓ is invertible in $\mathbb{Z}_p$ there exists $z_n' \in \mathbb{Z}_p^r$ such that $\ell^n z_n' = z_n$. Hence $y = \ell^n(y_n - z_n')$ for any n, which implies that $y \in T_\ell$. This concludes the proof of the lemma. □

4.1.11 Proposition. *Let G be a semiabelian variety over K which has good reduction $\mathcal{G}$ over R. Let K'/K be a finite field extension and let R' be the integral closure of R in K'. Then $\mathcal{G}(R') = G(K')^*$.*

Proof. Corollary 4.1.5 implies that $\mathcal{G}(R') \subseteq G(K')^*$. On the other hand, Proposition 4.1.9 implies that for any point $P \in G(K')^*$ there exists n such that $nP \in \mathcal{G}(R')$. By 1.4.6 the multiplication-by-n map $[n]\colon \mathcal{G} \to \mathcal{G}$ is finite, and hence proper. Then the Valuative Criterion of Properness implies that $P \in \mathcal{G}(R')$. □

4.1.12 Proposition. *Let G be a semiabelian variety over K which has good reduction, let $\mathcal{G}$ be the corresponding model for G over R and let $\overline{G}$ denote the reduction of G.*

(i) Let ℓ be a prime number different from p. The reduction map $\mathcal{G}(R) \to \overline{G}(k)$ restricts to a bijection $\mathcal{G}(R)[\ell^\infty] \to \overline{G}(k)[\ell^\infty]$.

(ii) All torsion points of $\mathcal{G}$ whose order is coprime to p are contained in $\mathcal{G}(R^{un})$, where R^{un} is the integral closure of R in the maximal unramified extension K^{un} of K.

Proof. We prove first statement (i). It is sufficient to show that for any $n \in \mathbb{N}$ the map $\mathcal{G}[\ell^n](R) \to \overline{G}[\ell^n](k)$ is a bijection. But if ℓ is coprime to p we know by 1.4.6(ii) that $\mathcal{G}[\ell^n]$ is a finite étale surjective group scheme over R. In particular it is affine over R. Hence by A.4.4 the map

$$\mathrm{Hom}_R(R, \mathcal{G}[\ell^n]) \to \mathrm{Hom}_k(k, \overline{G}[\ell^n] \times_R \mathrm{Spec}\, k)$$

is a bijection. This proves statement (i).

Statement (ii) follows from the following lemma applied to $\mathcal{G}[n]$ for any n which is coprime to p. □

4.1.13 Lemma. *Let X/R be a finite étale scheme. Let K'/K be a finite field extension and let K_0/K be the maximal unramified field extension contained in K'. Then $X(K') \cong X(K_0)$. In particular, if R' and R_0 are the integral closures of R in K' and K_0 respectively, then $X(R') \cong X(R_0)$.*

Proof. Indeed, since X/R is finite, it is proper, hence $X(R') \cong X(K')$ and $X(R_0) \cong X(K_0)$. On the other hand, let k' be the residue field of R'. It is also the residue field of R_0. Then, by A.4.4, it follows that

$$X(R') \cong X(k') \cong X(R_0),$$

which proves the lemma. □

As a result of the previous two propositions it follows that for any n coprime to p we have a group isomorphism

$$G(\bar{K})[n] \to \overline{G}(\bar{k})[n]$$

In particular, if ℓ is a prime number different from p, after taking injective and projective limits over the powers of ℓ we get isomorphisms

$$\mathrm{T}_\ell G \to \mathrm{T}_\ell \overline{G} \text{ and } \mathrm{B}_\ell G \to \mathrm{B}_\ell \overline{G}.$$

4.1.14 Lemma. *Let Y be a Galois R-module and let A be an abelian R-scheme. Then the map*

$$\mathrm{Mot}_R(Y, A) \to \mathrm{Mot}_K(Y_K, A_K)$$

induced by base change $R \to K$ is an isomorphism.

Proof. By 2.2.1, and 2.1.3 we have the isomorphisms

$$\mathrm{Mot}_R(Y, A) \cong (\hat{Y} \otimes A)(R)$$

and

$$\mathrm{Mot}_K(Y_K, A_K) \cong (\hat{Y}_K \otimes A_K)(K) \cong (\hat{Y} \otimes A)_K(K)$$

Since $\hat{Y} \otimes A$ is an abelian scheme, and in particular it is proper, we have that $(\hat{Y} \otimes A)(R) \cong (\hat{Y} \otimes A)_K(K)$. This shows the claim. □

4.1.15 Lemma. *Let G be a semiabelian variety over K which is the extension of an abelian variety A by a torus T. Than G has good reduction if and only if both A and T have good reduction.*

Proof. One direction of the claim is clear. For the other direction, assume that A and T have good reductions $\mathcal{A}$ and $\mathcal{T}$ over R. By the generalized Barsotti-Weil formula 1.4.7 we have the commutative diagram

$$\begin{array}{ccc} \mathrm{Ext}_R(\mathcal{A}, \mathcal{T}) & \longrightarrow & \mathrm{Ext}_K(A, T) \\ \wr\downarrow & & \wr\downarrow \\ \mathrm{Mot}_R(D_S(\mathcal{T}), \widehat{\mathcal{A}}) & \longrightarrow & \mathrm{Mot}_K(D_S(T), \widehat{A}) \end{array}$$

where the vertical arrows are isomorphisms. Our claim is equivalent to stating that the first row of the diagram is an isomorphism. This follows after applying 4.1.14 to the second row. □

1-motives

We have the following necessary and sufficient condition for a K-1-motive to have good reduction:

4.1.16 Proposition. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive, where G is an extension of an abelian variety A by a torus T. M has good reduction over R if and only if it has the following three properties:*

G1. *The group Y considered as a Γ_K-module is unramified (i.e. the inertia subgroup acts trivially on Y);*

G2. *A and T both have good reduction over R;*

G3. *$u(Y)$ is contained in $G(K')^*$ for some finite field extension K' of K.*

4.1.17 Remark. Compare this criterion with the one given in [Ray94] at the beginning of §4.

Proof. Let M_R be an R-1-motive whose generic fiber is M. By 1.6.5 $\mathcal{M}$ is given by a group homomorphism $u_R\colon Y \to G_R(R')$, where Y is a finitely generated free $\mathbb{Z}$-module with a continuous $\Gamma_{K^{un}/K}$-action, G_R is a semiabelian scheme which is the extension of an abelian scheme by a torus, and R' is the integral closure of R in some finite unramified extension K' of K. This, together with 4.1.11 implies conditions **G1.**, **G2.** and **G3.**.

Conversely, assume that M satisfies **G1.**, **G2.** and **G3.**. Lemma 4.1.15 implies that G has a good reduction G_R and conditions **G1.** and **G3.** together with 4.1.11 imply that the map u can be regarded as a group homomorphism $u_R\colon Y \to G_R(R')$. Then, by 1.6.5, the data (Y, u, G_R) defines a R-1-motive M_R whose generic fiber is M. This implies that M has good reduction. □

4.1.18 Lemma. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive which has good reduction. Let ℓ be a prime number different from p. Then the Tate module $\mathrm{T}_\ell M$ is unramified.*

Proof. Since M has good reduction, condition **G3.** implies that there exists a finite unramified field extension K'/K such that $u(Y) \subseteq G(K')^*$. Let $P \in u(Y)$. Lemma 4.1.10 implies that there is a unique representation $P = P_1 + P_2$ where $P_1 \in G(K')[\ell^\infty]$ and $P_2 \in G(K')$ is infinitely ℓ-divisible in $G(K')$. Hence if $Q \in G(\bar{K})$ is any point such that $\ell^n Q = P$ then Q can be represented as $Q = Q_1 + Q_2$, where $\ell^n Q_1 = P_1$, $\ell^n Q_2 = P_2$, $Q_1 \in G(\overline{K})[\ell^\infty]$ and $Q_2 \in G(K')$. Since Proposition 4.1.12 implies that Q_1 lies in an unramified field extension, it follows that the field of definition of Q is unramified as well. This, together with condition **G1.**, imply that the inertia group acts trivially on the groups $M[\ell^n]$, hence the Tate module $\mathrm{T}_\ell M$ is unramified. □

4.1.19 Lemma. *Let $M = [Y \to G]$ be a K-1-motive. Let ℓ be a prime number, different from p. Assume that the Tate module $\mathrm{T}_\ell M$ is unramified. Let $\phi \in \mathrm{Aut}(\mathrm{T}_\ell M)$ be the image of the Frobenius automorphism under $\rho_\ell(M)$. Then*

(i) ϕ lies in the domain $X_{\mathrm{T}_\ell M}$ of the Pink map.

(ii) Let n be any positive integer such that ϕ^n acts trivially on Y. Let K'/K be the unramified field extension of degree n. Then for any $y \in Y$, $\varepsilon_{\mathrm{T}_\ell M}(\phi)(y) \in G(K')[\ell^\infty]$ and $u(y) - \varepsilon_{\mathrm{T}_\ell M}(\phi)(y) \in G(K')_\ell$.

Proof. From the definition of $X_{\mathrm{T}_\ell M}$ in Section 3.4 it follows that $\phi \in X_{\mathrm{T}_\ell M}$ if and only if $\phi - 1$ is an automorphism of $\mathrm{V}_\ell(\hat{Y} \otimes G)$. But if $\phi - 1$ is not an automorphism, then it would follow that ϕ would have a non-trivial fixed vector in $\mathrm{T}_\ell(\hat{Y} \otimes G)$, which is not possible since the set of torsion points in $(\hat{Y} \otimes G)(K)$ is finite. This proves statement (i). Moreover, since $(\hat{Y} \otimes G)(K')$ contains finitely many torsion points for every finite unramified extension K' of K it follows by an analogous argument that $\phi^n \in X_{\mathrm{T}_\ell M}$ for every $n \geq 1$.

Next we show (ii). Let n and K' be as in the statement. By 3.4.3(ii) we have

$$\varepsilon_{\mathrm{T}_\ell M}(\phi) = \varepsilon_{\mathrm{T}_\ell M}(\phi^n)$$

Fix a section $s \in \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell M)$ of the projection map $\pi\colon \mathrm{T}_\ell M \to \mathrm{T}_\ell Y$ and consider the vector $t \in V_\ell G$,

$$t := (\phi^n - 1)^{-1}[(\phi^n - 1)s(y)].$$

Since ϕ^n acts trivially on y we have

$$t = \left((\phi^n - 1)^{-1}[(\phi^n - 1)s]\right)(y) = \varepsilon_{\mathrm{T}_\ell M}(\phi^n)(y) \mod \mathrm{T}_\ell(\hat{Y} \otimes G)$$

There exists $m \in \mathbb{N}$ such that $t = \ell^{-m}t'$ for some $t' \in \mathrm{T}_\ell G$. Then one easily sees that

$$\varepsilon_{\mathrm{T}_\ell M}(\phi)(y) = \varepsilon_{\mathrm{T}_\ell M}(\phi^n)(y) = \pi_m(t'),$$

where $\pi_m\colon \mathrm{T}_\ell G \to G(\bar{K})[\ell^m]$ is the standard projection map. The equation for t implies that

$$(\phi^n - 1)(\ell^m s(y) - t') = 0.$$

Pick a sequence of representatives $s(y) = \{(y_k, P_k)\}_{k=1}^\infty$ and $t' = \{(0, t_k)\}_{k=1}^\infty$. Then a sequence representing the element $0 = (\phi^n - 1)(\ell^m s(y) - t')$ is given by $\{(0, (\phi^n - 1)(P_{k-m} - t_k)\}$ where we assume that $P_k = 0$ for $k \leq 0$. This implies that $P_{k-m} - t_k \in G(K')$. In particular $t_m = \varepsilon_{\mathrm{T}_\ell M}(\phi)(y) \in G(K')$ hence $\varepsilon_{\mathrm{T}_\ell M}(\phi)(y) \in G(K')[\ell^\infty]$.

Let $Q = u(y) - t_m$. Then

$$Q - \ell^k(P_k - t_{k+m}) = u(y) - \ell^k P_k$$

and therefore is an element of $u(\ell^k Y)$ for any $k \in \mathbb{N}$. Since $P_k - t_{k+m}$ lies in $G(K')$ this implies that Q is infinitely ℓ-divisible in $G(K')$, which concludes the proof of the lemma. □

Proof of Theorem 4.1.1. Lemma 4.1.18 implies one direction of the theorem. Assume that the Tate module $\mathrm{T}_\ell M$ is unramified. Let G be the extension of an abelian variety A by a torus T. Since $\mathrm{T}_\ell M$ is unramified it follows that $\mathrm{T}_\ell Y$, $\mathrm{T}_\ell G$, $\mathrm{T}_\ell T$ and $\mathrm{T}_\ell A$ are unramified as well. Then the action of Γ_K on Y is unramified whence condition **G1.** follows. By the Néron-Ogg-Shafarevich criterion (due to Serre and Tate [ST68]) A has good reduction. The action of the Galois group on the character group of T is unramified, hence T has good reduction as well. This shows condition **G2.**.

It remains to show condition **G3.**. Let $n \in \mathbb{N}$ be such that the n-th power Frobenius ϕ^n acts trivially on $\mathrm{T}_\ell Y$ and let K'/K be the unramified field extension of degree n. It suffices to show that $u(Y)$ is contained in $G(K')^*$. But Lemma 4.1.19 (ii) implies that for any y, $u(y) = Q_{tors} + Q_{div}$, where $Q_{tors} \in G(K')[\ell^\infty]$ and $Q_{div} \in G(K')_\ell$. Lemmas 4.1.10 and 4.1.8 then imply that $u(y) \in G(K')^*$. □

Let M be a K-1-motive which has good reduction and let ℓ be a fixed prime different from p. The motive M induces an element $\delta_M \in \mathrm{Hom}(Y, G(K^{un})[\ell^\infty])$ as follows. Fix an unramified field extension K'/K such that the action of the Galois group $\Gamma_{K'}$ on Y is trivial. Let R' be the integral closure of R in K' and let k' be its residue field. Then δ_M is the composition of the maps

$$Y \xrightarrow{u \times k'} \overline{G}(k') \xrightarrow{pr_\ell} \overline{G}(k')[\ell^\infty] \longrightarrow G(K')[\ell^\infty]$$

Note that we can consider δ_M as a K'-1-motive which has good reduction and that its reduction is precisely $pr_\ell \overline{M}$. To finish the proof of Theorem 4.1.2 it is sufficient to show that $\varepsilon_{\mathrm{T}_\ell M}(\phi) = \delta_M$.

4.1.20 Lemma. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive which has good reduction and let ℓ be a fixed prime different from p. Let K'/K be a finite unramified field extension such that the action of $\Gamma_{K'}$ on Y becomes trivial. Then for any $y \in Y$ the point $\delta_M(y) - u(y)$ is infinitely ℓ-divisible in G.*

Proof. Let R' be the integral closure of R in K' and let k' be its residue field. Let $\mathcal{G}$ be an appropriate R-model for G and let $\overline{G}$ be its special fiber. Propositions 4.1.11, 4.1.12, Lemma 4.1.8 and Lemma 4.1.10 imply that the kernel of the map

$$G(K')^* \to \overline{G}(k')[\ell^\infty]$$

which is constructed by composing the reduction map $G(K')^* \cong \mathcal{G}(R') \to \overline{G}(k')$ and the projection map $pr_\ell \colon \overline{G}(k') \to \overline{G}(k')[\ell^\infty]$ is precisely $G(K')_\ell$. The definition of δ_M implies that $u(y) - \delta_M(y)$ lies in this kernel, hence it is infinitely ℓ-divisible in $G(K')$. □

Proof of Theorem 4.1.2. Lemma 4.1.19 (i) implies the first part of the theorem. To finish the proof we need to show that

$$\delta_M = \varepsilon_{\mathrm{T}_\ell M}(\phi).$$

Let $n \in \mathbb{N}$ be such that the n-th power Frobenius ϕ^n acts trivially on $\mathrm{T}_\ell Y$ and let K'/K be the unramified field extension of degree n. Condition **G3.** implies that for any $y \in Y$, $u(y) \in G(K')^*$. By Lemma 4.1.10 there is a unique representation $u(y) = Q_{tors} + Q_{div}$, where $Q_{tors} \in G(K')[\ell^\infty]$ and $Q_{div} \in G(K')_\ell$. But Lemmas 4.1.20 and 4.1.19 (ii) give two such representations: $u(y) = \delta_M(y) + (u(y) - \delta_M(y))$ and $u(y) = \varepsilon_{\mathrm{T}_\ell M}(\phi)(y) + (u(y) - \varepsilon_{\mathrm{T}_\ell M}(\phi)(y))$. It follows that $\delta_M = \varepsilon_{\mathrm{T}_\ell M}(\phi)$. □

4.2 The global case

Theorems 4.1.1 and 4.1.2 have several straightforward consequences regarding 1-motives over number fields which we are going to present here.

Good reduction

A large portion of the text here has been inspired by Perucca's thesis [Per08, Chapter 1]. Let R be a Dedekind domain, whose ideal class group is finite (e.g. the ring of integers of a number field) and let K denote its fraction field. Let $L(R)$ denote the set whose elements are finite sets of prime ideals in R. This set is a partially ordered directed set under the inclusion relation.

To each $\lambda \in L(R)$ we can associate the ring of λ-integers $R_\lambda \subset K$ as follows. Let $\lambda = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$. Since the ideal class group of R is finite, a certain power of the ideals $\mathfrak{p}_i$ is principal. Let $a_1, \dots, a_k \in R$ be generators of some power of $\mathfrak{p}_1, \dots, \mathfrak{p}_k$. Then R_λ is the localization of R by the multiplicative set generated by $a_1 \dots a_k$. It is easy to see that $U_\lambda = \operatorname{Spec} R_\lambda$ is the open subscheme of $\operatorname{Spec} R$ constructed by taking out the points in λ.

If $\lambda, \mu \in L(R)$, $\lambda \geq \mu$, then there is a canonical morphism $U_\lambda \to U_\mu$. Thus, the schemes U_λ form a projective system. This system has a limit in the category of R-schemes, and indeed we have

$$\operatorname{Spec} K = \varprojlim_{\lambda} U_\lambda.$$

4.2.1 Lemma. *Let Y be a Galois K-module. Then Y is a Galois R_λ-module for some $\lambda \in L(R)$.*

Proof. It follows from A.2.6 that for any λ, the fundamental group of U_λ is precisely the Galois group of the maximal extension L/K which is unramified outside the primes in λ. Since the action of Γ_K on Y factors through the Galois group of a finite field extension, it follows it is unramified at all but finitely many primes. Hence, if λ is the set of ramified primes, the action of Γ_K on Y factors through the fundamental group of U_λ. This implies that Y is a Galois R_λ-module. □

4.2.2 Lemma. *Let $\lambda \in L(R)$, let Y_λ be a Galois R_λ-module and let A_λ be an abelian R_λ-scheme. Let $Y = Y_\lambda \otimes_{R_\lambda} K$, $A = A_\lambda \otimes_{R_\lambda} K$. The map*

$$\operatorname{Mot}_{R_\lambda}(Y_\lambda, A_\lambda) \to \operatorname{Mot}_K(Y, A)$$

induced by base change $R_\lambda \hookrightarrow K$ is bijective.

Proof. The proof is the same as the proof of 4.1.14, of which this lemma is a generalization. □

4.2.3 Lemma. *Let G be a semiabelian variety over K. There exists $\lambda \in L(R)$ and a semiabelian R_λ-group scheme G_λ which is an extension of an abelian scheme by a torus and such that $G_\lambda \otimes_{R_\lambda} K \cong G$.*

Proof. This is a standard fact if G is either a torus or an abelian variety. Let G be an extension of A by T. Choose a finite set λ such that both A and T extend to A_λ and T_λ over R_λ. Consider the diagram

$$\begin{array}{ccc} \operatorname{Ext}_{R_\lambda}(A_\lambda, T_\lambda) & \longrightarrow & \operatorname{Ext}_K(A, T) \\ \wr\downarrow & & \wr\downarrow \\ \operatorname{Mot}_{R_\lambda}(D_{R_\lambda}(T_\lambda), \widehat{A_\lambda}) & \longrightarrow & \operatorname{Mot}_K(D_K(T), \widehat{A}), \end{array}$$

The columns are isomorphisms by the generalized Barsotti-Weil formula 1.4.7. The second row is a group isomorphism by the previous lemma. It follows that the first row is a group isomorphism as well, which implies the existence of G_λ with the requested properties. □

In our setting [EGA4III, Th. 8.8.2(i)] implies the following:

4.2.4 Lemma. *Let X_α, G_α be R_α-schemes, such that X_α is quasi-separated and quasi-compact and G_α is locally of finite type. Let $X = X_\alpha \otimes_{R_\alpha} K$, $G = G_\alpha \otimes_{R_\alpha} K$. Let $f \in \mathrm{Hom}_K(X, G)$. Then there exists $\lambda \geq \alpha$ and a morphism $f_\lambda \in \mathrm{Hom}_{R_\lambda}(X_\alpha \otimes R_\lambda, G_\alpha \otimes R_\lambda)$ such that*

$$f = f_\lambda \otimes_{R_\lambda} K.$$

Proof. Let $G_\lambda = G_\alpha \otimes_R R_\lambda$, $G = G_\alpha \otimes_R K$. We have a natural map

$$\varinjlim_\lambda \mathrm{Hom}_{R_\lambda}(U_\lambda, G_\lambda) \to \mathrm{Hom}_K(\mathrm{Spec}\, K, G)$$

By [EGA4III, Th 8.8.2(i)] this map is bijective, whence our claim follows. □

4.2.5 Lemma. *Let G be a semiabelian variety over K and let $P \in G(K)$. There exists $\lambda \in L(R)$ such that G extends to a semiabelian R_λ-scheme G_λ which is an extension of an abelian scheme by a torus and such that there exists a point $P_\lambda \in G(R_\lambda)$ which restricts to P over K.*

Proof. By 4.2.3 there exists $\alpha \in L(R)$ such that G extends to an extension G_α of an abelian scheme by a torus over R_α. Then the claim follows from 4.2.4 applied to $X_\alpha = \mathrm{Spec}\, R_\alpha$, G_α, and the morphism $P \in \mathrm{Hom}(\mathrm{Spec}\, K, G)$. □

4.2.6 Proposition. *Let M be a K-1-motive. There exists $\lambda \in L(R)$ and an R_λ-1-motive M_λ such that $M_\lambda \otimes_{R_\lambda} K \cong M$.*

Proof. Let $M = [Y \xrightarrow{u} G]$. By 4.2.1 and 4.2.3 we can pick $\alpha \in L(R)$ such that Y is a Galois R_α-module, $Y = Y_\alpha \times_{R_\alpha} \mathrm{Spec}\, K$ and such that G can be extended to a commutative R_α-group scheme G_α which is the extension of an abelian scheme by a torus.

For any $\lambda \geq \alpha$ we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Mot}_{R_\lambda}(Y_\lambda, G_\lambda) & \longrightarrow & \mathrm{Mot}_K(Y, G) \\ \wr\downarrow & & \wr\downarrow \\ \hat{Y}_\lambda \otimes G_\lambda(R_\lambda) & \longrightarrow & \hat{Y} \otimes G(K), \end{array}$$

where $G_\lambda = G_\alpha \otimes R_\lambda$, $Y_\lambda = Y_\alpha \otimes R_\lambda$ and where the vertical group isomorphisms are given by the map $\mathcal{S}_Y$ described in 2.2.1. Hence the claim follows trivially from the previous lemma. □

In particular, we have the following straightforward corollary:

4.2.7 Corollary. *Let K be a number field and let M be a K-1-motive. M has good reduction at all but finitely many primes $\mathfrak{p}$.*

If $\rho\colon \Gamma_K \to \mathrm{Aut}(V)$ is a Galois representation, we will say that ρ is **unramified at $\mathfrak{p}$** if $I_\mathfrak{p}$, the inertia subgroup at $\mathfrak{p}$, lies in its kernel. This definition does not depend on the choice of the embedding $K^s \hookrightarrow K^s_\mathfrak{p}$. Then the previous corollary together with Theorem 4.1.1 imply

4.2.8 Theorem. *Let K be a number field and let M be a K-1-motive. Let ℓ be a prime number and let $\rho_\ell(M)$ be the ℓ-adic Galois representation associated to M. Then:*

(i) The representation $\rho_\ell(M)$ is unramified at all but finitely many primes.

(ii) Let $\mathfrak{p}$ be a prime ideal which is coprime to ℓ. The representation $\rho_\ell(M)$ is unramified at $\mathfrak{p}$ if and only if M has good reduction at $\mathfrak{p}$.

Chebotarev's density theorem

In the following K will be a fixed number field. We will denote the set of all finite places of K by Σ_K. Equivalently, Σ_K is the set of all prime ideals in the ring of integers $\mathcal{O}_K$ of K.

4.2.9 Definition. Let P be a subset of Σ_K. For any $x \geq 0$, let $a_x(P)$ denote the number of places $\mathfrak{p} \in P$ whose norm is $\leq x$. Then we say that P **has density** a if

$$\lim_{x\to\infty} \frac{a_x(P)}{a_x(\Sigma_K)} = a.$$

Equivalently, P has density a, if

$$a_x(P) = ax/\log x + o(x/\log x)$$

as x goes to infinity.

The following version of Chebotarev's density theorem is due to Serre [ST68, I, §2.2].

4.2.10 Theorem. *Let L/K be a (possibly infinite) Galois extension which is unramified outside a finite set S. For any place $v \notin S$ let $F_v \subset \Gamma_{L/K}$ denote the conjugacy class of the Frobenius at v. Then*

(i) The Frobenius elements at the unramified places are dense in $\Gamma_{L/K}$.

(ii) Let X be a subset of $\Gamma_{L/K}$ stable under conjugation. Assume that the boundary of X has measure zero with respect to the probability Haar measure μ on $\Gamma_{L/K}$ (i.e. the Haar measure for which $\mu(\Gamma_{L/K}) = 1$). Then the set of places $v \notin S$ such that $F_v \subset X$ has density $\mu(X)$.

Let ℓ be a fixed prime number. Let $\mathfrak{p}$ be a prime ideal, coprime to ℓ, and let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. Let G be a semiabelian variety which has good reduction $G_\mathfrak{p}$ at $\mathfrak{p}$.

We know from 4.1.12 that there is a canonical isomorphism

$$\mathrm{B}_\ell(G \otimes_K K_\mathfrak{p}) \xrightarrow{\sim} \mathrm{B}_\ell G_\mathfrak{p}$$

Fix an embedding $\phi\colon K^s \hookrightarrow K^s_{\mathfrak{p}}$. It induces an injection $G(K^s) \hookrightarrow G(K^s_{\mathfrak{p}})$, which restricts to a group isomorphism on the torsion points. Hence we have an isomorphism

$$\mathrm{B}_\ell G \xrightarrow{\sim} \mathrm{B}_\ell(G \otimes_K K_{\mathfrak{p}}).$$

Composing the two maps we define the reduction map

$$red_{\mathfrak{p}}\colon \mathrm{B}_\ell G \to \mathrm{B}_\ell G_{\mathfrak{p}}. \tag{4.3}$$

This map is a $\mathbb{Z}_\ell$-module isomorphism. It is not canonically defined, it depends on the choice of the embedding ϕ. However, since any two embeddings differ by an element in Γ_K, it follows that the image $red_{\mathfrak{p}}(X)$ of a set X which is invariant under the natural action of Γ_K on $\mathrm{B}_\ell G$, is independent of the choice of embedding.

We recall that if $k_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$, we have a map

$$pr_\ell\colon \mathrm{Mot}_{k_{\mathfrak{p}}}(Y_{\mathfrak{p}}, G_{\mathfrak{p}}) \to \mathrm{B}_\ell(\hat{Y}_{\mathfrak{p}} \otimes G_{\mathfrak{p}})$$

which sends a 1-motive to its ℓ-part. Then Theorem 4.1.2 has the following straightforward corollary:

4.2.11 Corollary. *Let $M = [Y \xrightarrow{u} G]$ be a 1-motive over K. Let ℓ be a prime number and let $\mathfrak{p}$ be a place of good reduction for M which is coprime to ℓ. Fix an embedding $K^s \hookrightarrow K^s_{\mathfrak{p}}$ and let $\phi_{\mathfrak{p}}$ denote the image of the Frobenius element under the ℓ-adic representation $\rho_\ell(M)$. Then*

(i) The element $\phi_{\mathfrak{p}}$ lies in the domain $X_{\mathrm{T}_\ell M}$ of the Pink map $\varepsilon_{\mathrm{T}_\ell M}$;

(ii) $red_{\mathfrak{p}}(\varepsilon_{\mathrm{T}_\ell M}(\phi_{\mathfrak{p}})) = pr_\ell M_{\mathfrak{p}}$.

4.2.12 Theorem. *Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive. Let ℓ be a prime number and let $S \subseteq \mathrm{B}_\ell(\hat{Y} \otimes G)$ be any Galois invariant subset. The set of primes $\mathfrak{p}$ of good reduction of M for which $pr_\ell M_{\mathfrak{p}} \in red_{\mathfrak{p}}(S)$ has density*

$$\mu\left(\varepsilon^{-1}_{\mathrm{T}_\ell M}(S) \cap \operatorname{Im}\rho_\ell(M)\right),$$

where μ is the probability Haar measure on the image of the Galois representation $\rho_\ell(M)$.

Proof. This is an immediate consequence of Chebotarev's theorem 4.2.10(ii) and 4.2.11, as long as we show that the boundary of the set $\varepsilon^{-1}_{\mathrm{T}_\ell M}(S) \cap \operatorname{Im}\rho_\ell(M)$ has measure 0. By 3.4.2 the map $\varepsilon_{\mathrm{T}_\ell M}$ is continuous. Since the topology on $\operatorname{Im}\rho_\ell(M)$ is the one induced by $\mathrm{Aut}(\mathrm{T}_\ell M)$ it follows that the restriction of $\varepsilon_{\mathrm{T}_\ell M}$ on the set $X_{\mathrm{T}_\ell M} \cap \operatorname{Im}\rho_\ell(M)$ is continuous as well. But since S is both open and closed, it follows that the set $\varepsilon^{-1}_{\mathrm{T}_\ell M}(S) \cap \operatorname{Im}\rho_\ell(M)$ is both open and closed as well, whence it has no boundary. This proves the theorem. □

Chapter 5

Kummer theory

In this chapter we study 1-motives over number fields. We are interested in describing the images of the Kummer map $\delta_\ell(M)$ and the Pink map $\varepsilon_\ell(M)$ which we associated to a 1-motive $M = [Y \to G]$ in Chapter 3, whenever G is a *split* semiabelian variety. We show that one can describe those images in terms of the left ideal consisting of those endomorphisms of the variety $\hat{Y} \otimes G$ which kill M.

The description of the image of the Kummer map is not new. The method goes back to Ribet [Rib79], who proves the result after assuming certain conjectures about the ℓ-adic representations of abelian varieties. Those conjectures were later proved by Bogomolov [Bog81] and Faltings [Fal83]. Ribet's result concerns 1-motives of the type $[\mathbb{Z}^r \to G]$ and then only studies the image of the Kummer map modulo ℓ. Later Bertrand [Ber88, Theorem 2] states a description of the image in $\mathrm{T}_\ell G$ for 1-motives $[\mathbb{Z} \to G]$. The proof of Bertrand's theorem was worked out by Hindry [Hin88] in the case when G is an abelian variety. See also [BGK05].

Our result (Theorem 5.2.1) determines the image of the Kummer map for 1-motives $[Y \to G]$ where Y is a general Galois K-module. It is, however, as strong as Bertrand's result. This is due to the twisting trick (Lemma 2.2.1) which allows us to reduce the general case to the special case considered by Bertrand. We do not, rely on Bertrand's theorem in our proof.

Recently Jossen has published a result which is strictly stronger than ours [Jos13, Theorem 6.2]. It can be used to determine the image of the Kummer map even when the semiabelian variety G does not split.

The main idea behind Ribet's method is essentially an abstract statement about profinite group cohomology. It is presented in Section 5.1. One advantage we gain from this abstraction is that in some cases we can also use it to determine the image of the Kummer map for 1-motives over local fields, as is shown in Proposition 6.5.1. In Section 5.2 we state and prove Theorem 5.2.1 which gives the image of the Kummer map. Once we know this image we can easily describe the image of the Pink map. This is done in the final section, specifically in Theorem 5.3.1.

5.1 Ribet's theorem

Let k be a field and let Γ be a group acting on a k-vector space V. Let $\rho\colon \Gamma \to \mathrm{Aut}_k(V)$ be the corresponding representation, let $Q := \operatorname{Im}\rho$ and $U := \ker\rho$. Then we have the restriction-inflation sequence

$$0 \to H^1(Q,V) \to H^1(\Gamma,V) \xrightarrow{\delta} H^1(U,V),$$

Since U acts trivially on V, for every element $M \in H^1(\Gamma,V)$ the element $\delta(M)$ is a homomorphism from U to V. We want to describe the image of this homomorphism in certain cases. More specifically, k will be either $\mathbb{F}_\ell$ or $\mathbb{Q}_\ell$ and Γ will be a profinite group. The vector space V will be finite-dimensional and it will be equipped with the discrete or the ℓ-adic topology respectively. The representation ρ will be continuous and we will use continuous cochain cohomology.

We are going to introduce the following notation. Let R be a (not necessarily commutative) ring and let T be an abelian group equipped with an R-action $R \to \mathrm{End}(T)$. Let $M \in T$ be any element. Then we define the **annihilator** of M to be the left ideal

$$\mathrm{Ann}_R M := \{\phi \in R\colon \phi M = 0\}.$$

For any left ideal $I \subseteq R$ we define the **zero set** of I in T to be the set

$$Z(I,T) := \{x \in T\colon \phi x = 0 \text{ for every } \phi \in I\}.$$

Let $\mathcal{O}$ denote the ring of Γ-equivariant endomorphisms of V. Every endomorphism $\phi \in \mathcal{O}$ induces an endomorphism $\phi_* \in \mathrm{End}(H^1(\Gamma,V))$. Then we have

5.1.1 Lemma. *Let $U \subseteq \ker\rho$ be a normal subgroup and let $Q := \Gamma/U$. Assume that the following conditions hold:*

(i) The representation ρ is semisimple;

(ii) $H^1(Q,V) = 0$.

Then for every $M \in H^1(\Gamma,V)$ the space $Z(\mathrm{Ann}_{\mathcal{O}} M, V)$ is the smallest linear subspace containing the image of $\delta(M)$.

Proof. Let $X := \operatorname{Im}\delta(M)$. For every $\phi \in \mathrm{Ann}_{\mathcal{O}} M$, $\phi \circ \delta(M) = \delta(\phi_* M) = 0$ hence $\phi X = 0$. It follows that $X \subseteq Z(\mathrm{Ann}_{\mathcal{O}} M, V)$.

Assume that there is a vector subspace $Z' \subsetneq Z(\mathrm{Ann}_{\mathcal{O}} M, V)$ such that $X \subseteq Z'$. Since X is Γ-invariant we can assume that Z' is Γ-invariant as well (otherwise take $\bigcap_{\sigma\in\Gamma} \sigma Z'$). Using the semisimplicity of ρ we can construct an endomorphism $\phi \in \mathcal{O}$ such that $\ker\phi = Z'$. Namely, pick any decomposition $V = Z' \oplus W$ where W is a Γ-invariant subspace and take ϕ to be the map which kills Z' and is the identity on W. Then, since $\phi X = 0$, it follows that

$$0 = \phi \circ \delta(M) = \delta(\phi_* M).$$

Condition (ii) implies that $\phi_* M = 0$, hence $\phi \in \mathrm{Ann}_{\mathcal{O}} M$. But since

$$Z(\mathrm{Ann}_{\mathcal{O}} M, V) \not\subseteq \ker\phi$$

we reach a contradiction. □

Now assume that Γ is a profinite group acting continuously on a finitely-generated free $\mathbb{Z}_\ell$-module T via an action $\rho\colon \Gamma_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T)$. Let $\mathcal{O}$ denote the set of Γ-invariant endomorphisms of T. As before let $\delta\colon H^1(\Gamma, T) \to H^1(\ker\rho, T)$ denote the restriction map. Then:

5.1.2 Corollary. *Assume that the following conditions hold*

(i) The representation induced on $T \otimes \mathbb{Q}_\ell$ is semisimple.

(ii) $H^1(\mathrm{Im}\,\rho, T \otimes \mathbb{Q}_\ell) = 0$.

Then for every $M \in H^1(\Gamma, T)$ the image of $\delta(M)$ is a finite-index subgroup of $Z(\mathrm{Ann}_{\mathcal{O}} M, T)$.

Proof. Denote $V = T \otimes \mathbb{Q}_\ell$. Let $\beta\colon H^1(\Gamma, T) \to H^1(\Gamma, V)$ be the map induced by the inclusion $T \subset V$. One easily sees that it induces a map

$$(\mathrm{Ann}_{\mathcal{O}} M) \otimes \mathbb{Q}_\ell \to \mathrm{Ann}_{\mathcal{O}\otimes\mathbb{Q}_\ell} \beta M$$

(Notice that $\mathcal{O} \otimes \mathbb{Q}_\ell$ is precisely the ring of Γ-equivariant endomorphisms of V.) We claim that this map is a bijection. That it is an injection, follows from the injection $\mathcal{O} \subset \mathcal{O} \otimes \mathbb{Q}_\ell$. To show that it is surjective let $\phi \in \mathcal{O} \otimes \mathbb{Q}_\ell$ be any endomorphism that annihilates βM. There is an endomorphism $\psi \in \mathcal{O}$ such that $\phi = \psi \otimes \alpha$ for some $\alpha \in \mathbb{Q}_\ell$. Then by A.6.2 it follows that $\psi_* M$ is torsion. If $n \in \mathbb{N}$ is such that $n\psi_* M = 0$ then we can write ϕ as $\phi = (n\psi) \otimes \alpha/n$. This implies that $\phi \in (\mathrm{Ann}_{\mathcal{O}} M) \otimes \mathbb{Q}_\ell$, which proves our claim.

Let $X = \mathrm{Im}\,\delta(M)$. By Lemma 5.1.1 and the considerations above it follows that $Z(\mathrm{Ann}_{\mathcal{O}\otimes\mathbb{Q}_\ell} \beta M, V) = Z(\mathrm{Ann}_{\mathcal{O}} M, T) \otimes \mathbb{Q}_\ell$ is the smallest vector space containing X. Since, by continuity $X \subset T$ is a $\mathbb{Z}_\ell$-module, the statement follows. □

Let Γ, T and ρ and $\mathcal{O}$ be as before. Let $\mathcal{O}_1$ denote the ring of Γ-equivariant endomorphisms of T/ℓ. We have a map $\mathcal{O}/\ell \to \mathcal{O}_1$ and it is easy to see that it is an injection.

5.1.3 Theorem (Ribet)**.** *Let $M \in H^1(\Gamma, T)$. Assume that the following conditions hold:*

(i) The map $\mathcal{O}/\ell \to \mathcal{O}_1$ is an isomorphism;

(ii) The representations induced on $T \otimes \mathbb{Q}_\ell$ and on T/ℓ are semisimple;

(iii) $H^1(\mathrm{Im}\,\rho, T/\ell) = 0$.

(iv) The natural map

$$\mathrm{Ann}_{\mathcal{O}} M \to \mathrm{Ann}_{\mathcal{O}_1} M_1$$

is surjective, where M_1 is the image of M in $H^1(\Gamma, T/\ell)$.

Then the image of $\delta(M)$ is equal to $Z(\mathrm{Ann}_{\mathcal{O}} M, T)$.

5.1.4 Remark. Conditions (i)-(iv) are analogous to Ribet's axioms B1-B4 in [Rib79]. We will later see that his axiom B4 implies our condition (iv).

Proof. let $X := \operatorname{Im}\delta(M)$, $Q := \operatorname{Im}\rho$ and $U := \ker\rho$. Our first step is to show that X is a finite-index subgroup of $Z(\operatorname{Ann}_{\mathcal{O}} M, T)$.

Condition (iii) implies that the group $H^1(Q,T)$ is trivial. Indeed, Q is a closed subgroup of the ℓ-adic Lie group $\operatorname{Aut}_{\mathbb{Z}_\ell}(T)$, which implies that it is a compact ℓ-adic Lie group. Hence, by A.6.2, $H^1(Q,T)$ is a finitely-generated $\mathbb{Z}_\ell$-module. This implies that $H^1(Q,T)$ is trivial if and only if $H^1(Q,T)/\ell$ is trivial. From the short exact sequence

$$0 \to T \xrightarrow{\ell} T \to T/\ell \to 0$$

we get the exact sequence

$$H^1(Q,T) \xrightarrow{\ell} H^1(Q,T) \to H^1(Q,T/\ell)$$

Therefore $H^1(Q,T)/\ell$ injects in $H^1(Q,T/\ell)$. Since the latter group is trivial, it follows that $H^1(Q,T)$ is trivial as well.

We can therefore apply 5.1.2 to conclude that X is a finite-index subgroup of $Z(\operatorname{Ann}_{\mathcal{O}} M, T)$. To conclude the proof of the theorem it is sufficient to show that the images of the groups X and $Z := Z(\operatorname{Ann}_{\mathcal{O}} M, T)$ in T/ℓ are equal. We will denote those images by $\overline{X}$ and $\overline{Z}$ respectively.

Let $\delta_1 \colon H^1(\Gamma, T/\ell) \to H^1(U, T/\ell)$ be the restriction map. Let $X_1 := \operatorname{Im}\delta_1(M_1)$. We can use Lemma 5.1.1 to conclude that the smallest $\mathbb{F}_\ell$-vector space containing X_1 is $Z_1 := Z(\operatorname{Ann}_{\mathcal{O}_1} M_1, T/\ell)$. Since X_1 is a group, hence an $\mathbb{F}_\ell$-vector space itself, it follows that $X_1 = Z_1$.

Since $\delta_1(M_1)$ is the image of $\delta(M)$ under the map

$$\operatorname{Hom}_c(U,T) \to \operatorname{Hom}_c(U, T/\ell)$$

it follows that $\overline{X} = X_1$. (The subscript "c" above indicates that those are continuous group homomorphisms.) On the other hand, condition (iv) implies that $\overline{Z} \subseteq Z_1$. We get the inclusions

$$X_1 = \overline{X} \subseteq \overline{Z} \subseteq Z_1 = X_1$$

Clearly all inclusions are forced to be equalities. In particular, $\overline{X} = \overline{Z}$ which implies the statement of the theorem. □

5.2 The image of the Kummer map

Let K be a number field, Y be a Γ_K-module and let G be a semiabelian variety over K. Recall that we have an isomorphism $\operatorname{Mot}_K(Y,G) \cong (\hat{Y} \otimes G)(K)$ (Lemma 2.2.1). Hence the ring $\operatorname{End}_K(\hat{Y} \otimes G) \cong (\operatorname{End}_{\bar{K}}(\hat{Y}) \otimes \operatorname{End}_{\bar{K}}(G))^{\Gamma_K}$ acts on $\operatorname{Mot}_K(Y,G)$. We can describe this action explicitly. Let $\theta = \sum_i \phi_i \otimes \psi_i$ be an element in $\operatorname{End}_{K^s}(\widehat{Y}) \otimes \operatorname{End}_{K^s}(G)$. For any ϕ_i, let ϕ_i^t denote the transposed endomorphism of Y. Let $M = [Y \xrightarrow{u} G]$ be a K-1-motive. Then θM is the K^s-1-motive $[Y \xrightarrow{\theta u} G]$, where

$$\theta u \colon y \mapsto \sum_i \psi_i(u(\phi_i^t(y))).$$

One can easily check that if θ is fixed under the Galois action, then θM is a K-1-motive.

In order to simplify notation we shall denote by $\mathcal{O}$ the ring $\mathrm{End}_K(\hat{Y} \otimes G)$. For any prime number ℓ we shall write $\mathcal{O}_\ell$ instead of $\mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell(\hat{Y} \otimes G))$. We have a natural map $\mathcal{O} \otimes \mathbb{Z}_\ell \to \mathcal{O}_\ell$, by which $\mathcal{O}$ acts on $\mathrm{T}_\ell(\hat{Y} \otimes G)$ for any ℓ.

5.2.1 Theorem. *Let G be a* split *semiabelian variety over a number field K and let $M = [Y \to G]$ be a K-1-motive.*

(i) For every prime ℓ the image of the Kummer map $\delta_\ell(M)$ is a finite-index subgroup of $Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell(\hat{Y} \otimes G))$.

(ii) The image of the Kummer map is equal to $Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell(\hat{Y} \otimes G))$ for all but finitely many primes ℓ.

In order to prove Theorem 5.2.1 we are going to apply Ribet's theorem 5.1.3 to Γ_K and the $\mathbb{Z}_\ell$-module $\mathrm{T}_\ell(\hat{Y} \otimes G)$. To do that we will have to verify its four conditions. This is the purpose of the following lemmas.

5.2.2 Lemma. *Let G be a split semiabelian variety defined over a number field K. Then for every finitely-generated subgroup X of $G(K)$ and every prime ℓ, the group*

$$X'_\ell := \{P \in G(K) \colon \ell^n P \in X \text{ for some } n \geq 1\}$$

is such that X'_ℓ/X has finite exponent. Moreover, $X'_\ell = X$ for all but finitely many primes ℓ.

Proof. This is essentially Proposition 2.2 in [Rib79]. We give the proof for the reader's convenience.

Let $G = A \times T$, where A is an abelian variety and T is a torus. For A the statement follows from the Mordell-Weil theorem. To prove it for T we first pass to a finite extension K'/K such that $T \otimes_K K'$ is split. and then we involve Dirichlet's S-unit theorem. It is clear that if the statement holds for $T \otimes_K K'$ then it holds for T as well.

Finally, it is also easy to see that if the statement holds for A and T then it also holds for their product. Indeed, let X_A and X_T be the projections of X to A and T. Then $X \subseteq X_A \times X_T$ and $X'_\ell \subseteq X'_{A,\ell} \times X'_{T,\ell}$. Since all groups involved are finitely-generated, and in particular have finite torsion, the result follows. □

5.2.3 Lemma. *Let G be a split semiabelian variety defined over a number field K and let ℓ be a prime number.*

(i) The ℓ-adic Galois representation associated to $\mathrm{V}_\ell G$ is semisimple. When ℓ is large enough the Galois representation associated to $\mathrm{T}_\ell G/\ell$ is semisimple.

(ii) We have an isomorphism

$$\mathrm{End}_K(G) \otimes \mathbb{Z}_\ell \cong \mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell G).$$

When ℓ is large enough we have an isomorphism

$$\mathrm{End}_K(G)/\ell \cong \mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell G/\ell).$$

In the case of abelian varieties this lemma is a famous result of Faltings [Fal83]. To prove the general case we will first need to show the following claim

5.2.4 Claim. *Let A be an abelian variety defined over a number field K and let ℓ be a prime number. Then the groups*

$$\mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell A, \mathrm{T}_\ell \mathbb{G}_m) \text{ and } \mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell \mathbb{G}_m, \mathrm{T}_\ell A)$$

are trivial. When ℓ is large enough the groups

$$\mathrm{Hom}_{\Gamma_K}(A[\ell], \mathbb{G}_m[\ell]) \text{ and } \mathrm{Hom}_{\Gamma_K}(\mathbb{G}_m[\ell], A[\ell])$$

are trivial.

Proof. Indeed, using the Weil pairing we have an isomorphism

$$\mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell A, \mathrm{T}_\ell \mathbb{G}_m) \cong (\mathrm{T}_\ell A^\vee)^{\Gamma_K},$$

where $A^\vee$ denotes the dual abelian variety. The latter group is trivial, since $A^\vee$ has only finitely many torsion points. By a similar argument, since $A^\vee(K)[\ell]$ is trivial when ℓ is large enough, it follows that for large enough ℓ the group $\mathrm{Hom}_{\Gamma_K}(A[\ell], \mathbb{G}_m[\ell])$ is trivial as well.

To show that $\mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell \mathbb{G}_m, \mathrm{T}_\ell A)$ is trivial note the isomorphism

$$\mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell \mathbb{G}_m, \mathrm{T}_\ell A) \cong \mathrm{Hom}_{\Gamma_K}(\mathrm{T}_\ell A^\vee, \mathbb{Z}_\ell)$$

Since the representation $\mathrm{V}_\ell A^\vee$ is semisimple, in order for the latter group to be non-trivial $\mathrm{T}_\ell A^\vee$ must contain a copy of $\mathbb{Z}_\ell$, which contradicts the fact that $(\mathrm{T}_\ell A^\vee)^{\Gamma_K}$ is trivial. The argument for the finite case is analogous. □

Proof of Lemma 5.2.3. As we said above, when G is an abelian variety this result is due to Faltings. We will show it in the case of a torus and then derive the general case.

So let $G = T$ be a torus. We can write $T \cong E \otimes \mathbb{G}_m$ for some Galois K-module E. Then, by 2.1.8, $\mathrm{T}_\ell G \cong E \otimes_{\mathbb{Z}} \mathrm{T}_\ell \mathbb{G}_m$. The Galois group Γ_K acts on E through a finite quotient, hence, by Maschke's theorem, the Galois representation $E \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is semisimple. Moreover, when ℓ is large enough it does not divide the size of the quotient, hence, again by Maschke's theorem the representation $E \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ is semisimple.

Since $\mathrm{T}_\ell \mathbb{G}_m$ is one-dimensional, every invariant subspace of $E \otimes_{\mathbb{Z}} \mathrm{T}_\ell \mathbb{G}_m \otimes \mathbb{Q}_\ell$ is of the form $V \otimes_{\mathbb{Q}_\ell} \mathrm{V}_\ell \mathbb{G}_m$, where $V \subseteq E \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Since $E \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is semisimple it follows that $E \otimes_{\mathbb{Z}} \mathrm{T}_\ell \mathbb{G}_m \otimes \mathbb{Q}_\ell$ is semisimple. By an analogous argument $E \otimes_{\mathbb{Z}} \mathrm{T}_\ell \mathbb{G}_m \otimes \mathbb{F}_\ell$ is semisimple for large enough ℓ. This proves statement (i) of the lemma.

For statement (ii) we have the isomorphism

$$\mathrm{End}_K(E \otimes \mathbb{G}_m) \cong \mathrm{End}_K(E)$$

Also,

$$\mathrm{End}_{\Gamma_K}(E \otimes_{\mathbb{Z}} \mathrm{T}_\ell \mathbb{G}_m) \cong \mathrm{End}_{\Gamma_K}(E \otimes \mathbb{Z}_\ell).$$

Then the equality of the endomorphism rings is reduced to showing that the map

$$\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{End}_{\Gamma_K}(E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$$

is an isomorphism, which is trivial.

To prove the last part of statement (ii) it is sufficient to show that for large enough ℓ the map

$$\mathrm{End}_{\Gamma_K}(E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)/\ell \to \mathrm{End}_{\Gamma_K}(E/\ell)$$

is surjective. Indeed, let $\phi \in \mathrm{End}_{\Gamma_K}(E/\ell)$ and let $\psi \in \mathrm{End}_{\mathbb{Z}_\ell}(E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$ be any endomorphism that reduces to ϕ. Let Q be the finite quotient group through which Γ_K acts on E. Then when ℓ does not divide the size q of Q, the endomorphism

$$\frac{1}{q}\sum_{\sigma \in Q} \sigma \circ \psi$$

is Γ_K-equivariant and reduces to ϕ. This concludes the proof when G is a torus.

Let $G = A \times T$ be a product of an abelian variety and a torus. Statement (i) follows trivially from the partial cases. As for the second statement, note that $\mathrm{End}_K(G) \cong \mathrm{End}_K(A) \times \mathrm{End}_K(T)$. On the other hand $\mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell G) = \mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell A) \times \mathrm{End}_K(\mathrm{T}_\ell G)$. Indeed, otherwise, we could construct non-trivial elements in the groups $\mathrm{Hom}_{\Gamma_{K'}}(\mathrm{T}_\ell A, \mathrm{T}_\ell \mathbb{G}_m)$ and $\mathrm{Hom}_{\Gamma_{K'}}(\mathrm{T}_\ell \mathbb{G}_m, \mathrm{T}_\ell A)$ for a finite field extension K'/K over which T splits. But due to the claim above there are no such non-trivial homomorphisms. Then the isomorphism

$$\mathrm{End}_K(G) \otimes \mathbb{Z}_\ell \cong \mathrm{End}_{\Gamma_K}(\mathrm{T}_\ell G)$$

follows from the partial cases. When ℓ is large enough the finite analog follows by a similar argument. □

5.2.5 Lemma. *Let $M = [Y \to G]$ be a K-1-motive. Let $\widetilde{M} = \alpha_\ell(M)$ denote its image in $H^1(\Gamma_K, \mathrm{T}_\ell(\hat{Y} \otimes G))$ and let $\widetilde{M}_1$ denote its image in the group $H^1(\Gamma_K, \mathrm{T}_\ell(\hat{Y} \otimes G)/\ell)$. Then the natural map*

$$\mathrm{Ann}_{\mathcal{O}} M \otimes \mathbb{Z}_\ell \to \mathrm{Ann}_{\mathcal{O}_\ell} \widetilde{M}$$

is an isomorphism. For all but finitely many ℓ the natural map

$$(\mathrm{Ann}_{\mathcal{O}} M)/\ell \to \mathrm{Ann}_{\mathcal{O}/\ell} \widetilde{M}_1$$

is an isomorphism.

Proof. We can use Lemma 3.2.5 to reduce this lemma to the case when $Y = \mathbb{Z}$. Then M is essentially a rational point in G. Let ιM denote the image of M in $\varprojlim_n G(K)/\ell^n$. The injectivity of the map

$$\varprojlim_n G(K)/\ell^n \to H^1(\Gamma, \mathrm{T}_\ell G)$$

together with Lemma 5.2.3(ii) imply that there is a canonical isomorphism

$$\mathrm{Ann}_{\mathcal{O}\otimes\mathbb{Z}_\ell} \iota M \xrightarrow{\sim} \mathrm{Ann}_{\mathcal{O}_\ell} \widetilde{M}.$$

It remains to show that the map $\mathrm{Ann}_{\mathcal{O}} M \otimes \mathbb{Z}_\ell \to \mathrm{Ann}_{\mathcal{O}\otimes\mathbb{Z}_\ell} \iota M$ is an isomorphism.

The injectivity of that map is trivial since both sets are subsets of $\mathcal{O} \otimes \mathbb{Z}_\ell$. To show that it is surjective, let $\psi \in \mathrm{Ann}_{\mathcal{O}\otimes\mathbb{Z}_\ell} \iota M$. There is a limit of endomorphisms $\phi_n \in \mathcal{O}$ such that $\phi_n M = \ell^n N_n$ for some $N_n \in G(K)$ and such that ϕ_n converge to ψ in $\mathcal{O} \otimes \mathbb{Z}_\ell$. Consider the group $X = \mathcal{O}M$. Since $\mathcal{O}$ is finitely-generated it follows that X is finitely-generated as well. Then Lemma 5.2.2 implies that there is some k such that if $n \geq k$, then $\ell^k N_n \in X$. Hence

$$\phi_n M = \ell^{n-k} \theta_n M$$

for some $\theta_n \in \mathcal{O}$. The limit $\lim_n(\phi_n - \ell^{n-k}\theta_n)$ converges to ψ and it lies in $\mathrm{Ann}_{\mathcal{O}} M \otimes \mathbb{Z}_\ell$. This proves surjectivity.

The arguments for the second part of the lemma are analogous, however we have to use the injection

$$G(K)/\ell \hookrightarrow H^1(\Gamma, \mathrm{T}_\ell G/\ell)$$

instead. □

5.2.6 Lemma. *Let G be a split semiabelian variety defined over a field K and let ℓ be a prime number. Let Q_K be the image of Γ_K in the group $\mathrm{Aut}(\mathrm{T}_\ell G)$.*

(i) There exists a non-trivial element σ in the center of Q_K such that $\sigma^k - 1$ is an automorphism of $\mathrm{V}_\ell G$ for all $k \geq 1$.

(ii) For all but finitely many primes ℓ one can choose σ so that $\sigma - 1$ is an automorphism of $\mathrm{T}_\ell G$.

Proof. Let $G = A \times T$, where A is an abelian variety and T is a torus. There exists a Galois K-module E such that $T \cong E \otimes \mathbb{G}_m$. Let Q_E denote the quotient of Γ_K by the subgroup of automorphisms which act trivially on E. This is a finite group, we will denote its size by q_E.

For any prime ℓ, let $\rho_\ell(A)\colon \Gamma_K \to \mathrm{Aut}(\mathrm{T}_\ell A)$ denote the ℓ-adic representation associated to A and let $Q_{A,\ell}$ denote the image of $\rho_\ell(A)$. It is a result of Bogomolov [Bog81] that $Q_{A,\ell}$ contains an open subgroup of the homotheties $\mathbb{Z}_\ell^\times$. Moreover, it is a result of Serre [Ser00, Th 2] that the index $c(\ell)$ of $Q_{A,\ell} \cap \mathbb{Z}_\ell^\times$ in $\mathbb{Z}_\ell^\times$ is bounded from above for all ℓ. It follows that we can pick an element $\sigma \in \Gamma_K$ such that $\rho_\ell(A)(\sigma^{q_E})$ is a non-trivial homothety $\lambda \in \mathbb{Z}_\ell^\times$ of $\mathrm{T}_\ell A$, which is not a root of unity, and that for all but finitely many primes ℓ we can pick σ so that $\lambda^2 \not\equiv 1 \mod \ell$. Then $\rho_\ell(A)(\sigma^{q_E k}) - 1$ is an automorphism of $\mathrm{V}_\ell A$ for all $k \geq 1$ and $\rho_\ell(A)(\sigma^{q_E}) - 1$ is an automorphism of $\mathrm{T}_\ell A$ for all but finitely many ℓ.

The element σ^{q_E} acts trivially on E. We will show next that it acts on $\mathrm{T}_\ell \mathbb{G}_m$ via multiplication by λ^2. It then follows that the image of σ^{q_E} in Q_K has the required properties.

Let $A^\vee$ be the dual abelian variety of A. Any isogeny $A \to A^\vee$ induces an isomorphism $\mathrm{V}_\ell A \to \mathrm{V}_\ell A^\vee$. If follows that σ^{q_E} acts via multiplication by λ on $\mathrm{T}_\ell A^\vee$. Since the Weil pairing

$$\mu\colon \mathrm{T}_\ell A \otimes_{\mathbb{Z}_\ell} \mathrm{T}_\ell A^\vee \to \mathrm{T}_\ell \mathbb{G}_m$$

is Galois-equivariant and surjective and since

$$\sigma^{q_E} \mu(a, a') = \mu(\sigma^{q_E} a, \sigma^{q_E} a') = \mu(\lambda a, \lambda a') = \lambda^2 \mu(a, a'),$$

the claim follows. □

5.2.7 Corollary. *Let G be a split semiabelian variety defined over a number field K. Let ℓ be a prime and let $Q_{\ell,G}$ be the image of Γ_K in the group* $\mathrm{Aut}(\mathrm{T}_\ell G)$.

(i) $H^1(Q_{\ell,G}, \mathrm{V}_\ell G) = 0$.

(ii) For all but finitely many primes ℓ, $H^1(Q_{\ell,G}, \mathrm{T}_\ell G/\ell) = \{0\}$.

Proof. Lemma 5.2.6(i) together with Sah's lemma A.6.3 imply the first statement. To prove statement (ii), notice that any automorphism of $\mathrm{T}_\ell G$ induces an automorphism of $\mathrm{T}_\ell G/\ell$. Then the statement follows from 5.2.6(ii), together with Sah's lemma. □

Proof of Theorem 5.2.1. To simplify notation write $T := \mathrm{T}_\ell(\hat{Y} \otimes G)$. Let $\widetilde{M}$ denote the image of M in $H^1(\Gamma_K, T)$ under the Abel-Jacobi map α_ℓ and let $\widetilde{M}_1$ denote its image in $H^1(\Gamma_K, T/\ell)$. Then Lemma 5.2.5 implies that

$$\mathrm{Ann}_{\mathcal{O}} M \otimes \mathbb{Z}_\ell \cong \mathrm{Ann}_{\mathcal{O}_\ell} \widetilde{M}.$$

Hence $Z(\mathrm{Ann}_{\mathcal{O}} M, T) = Z(\mathrm{Ann}_{\mathcal{O}_\ell} \tilde{M}, T)$. Statement (i) of the theorem follows from Corollary 5.1.2. The conditions (i) and (ii) in the corollary follow from 5.2.3(i) and 5.2.7 respectively.

To prove the statement (ii) of the theorem we employ Theorem 5.1.3. Conditions (i)-(iv) follow from 5.2.3, 5.2.7 and 5.2.5. □

5.3 The image of the Pink map

We retain the notation of the previous section. Our goal is to determine the image of the map $\varepsilon_\ell(M)$ for K-1-motives $M \in \mathrm{Mot}_K(Y, G)$.

The ring $\mathrm{End}_{\mathbb{Z}} \hat{Y} \otimes_{\mathbb{Z}} \mathrm{End}_{\bar{K}} G$ acts on the group $\mathrm{B}_\ell(\hat{Y} \otimes G) \cong \mathrm{Hom}(Y, G[\ell^\infty])$. The action is given by the formula

$$(\phi^t \otimes \psi)\colon f \mapsto \psi \circ f \circ \phi.$$

for any $\phi \in \mathrm{End}_{\mathbb{Z}} Y$ and $\psi \in \mathrm{End}_{\bar{K}} G$. In particular, $\mathcal{O}$ acts on $\mathrm{B}_\ell(\hat{Y} \otimes G)$. One can check that this action is compatible with the action of $\mathcal{O}$ on $\mathrm{V}_\ell(\hat{Y} \otimes G)$.

5.3.1 Theorem. *Let G be a split semiabelian variety over K. Let $M \in \mathrm{Mot}_K(Y, G)$ and let ℓ be a prime number. There exist positive integer constants $c = c(\ell, Y, G)$ and $c' = c'(\ell, Y, G)$ such that*

$$\mathrm{Im}\, c\varepsilon_\ell(M) \subseteq Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{B}_\ell(\hat{Y} \otimes G)) \subseteq \mathrm{Im}\, c'\varepsilon_\ell(M) \tag{5.1}$$

For all but finitely many ℓ one can choose $c = c' = 1$.

Proof. To shorten notation we denote $T := \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell G)$, $V := T \otimes \mathbb{Q}_\ell$, $Z_T := Z(\mathrm{Ann}_{\mathcal{O}} M, T)$ and $Z_V := Z(\mathrm{Ann}_{\mathcal{O}} M, V)$. Then (5.1) is equivalent to showing

$$\mathrm{Im}\, c\varepsilon_\ell(M) \subseteq Z_V \bmod T \subseteq \mathrm{Im}\, c'\varepsilon_\ell(M) \tag{5.2}$$

Let $\rho\colon \Gamma_K \to \mathrm{Aut}(T)$ be the ℓ-adic Galois representation associated to $\hat{Y} \otimes G$. We will denote $Q := \mathrm{Im}\, \rho$ and $U := \ker \rho$.

Let c be the size of the group $H^1(Q,T)$. By 5.2.7 and A.6.2 one can show that this group is indeed finite for all ℓ and that it is trivial for all but finitely many ℓ. We will show that this constant satisfies the statement of the theorem.

Since V is semisimple (by 5.2.3), there exists a Γ_K-invariant vector subspace Z'_V of V such that $V = Z_V \oplus Z'_V$. Let $Z'_T := Z'_V \cap T$. One can show that $Z_T = Z_V \cap T$. It follows that $T = Z_T \oplus Z'_T$. We then have the decomposition

$$H^1(\Gamma_K, T) = H^1(\Gamma_K, Z_T) \oplus H^1(\Gamma_K, Z'_T)$$

and we have a similar decomposition of the group $H^1(U,T)$. One can easily see that the restriction map δ sends $H^1(\Gamma_K, Z_T)$ to $H^1(U, Z_T)$ and $H^1(\Gamma_K, Z'_T)$ to $H^1(U, Z'_T)$.

Let $\widetilde{M}$ be the image of M in $H^1(\Gamma_K, T)$ under the Abel-Jacobi map. Theorem 5.2.1 tells us that $\delta(\widetilde{M})$ lies in $H^1(U, Z_T) \cong \mathrm{Hom}_c(U, Z_T)$. This implies that the projection of $\widetilde{M}$ to $H^1(\Gamma_K, Z'_T)$ lies in the kernel $H^1(Q,T)$. Hence $c\widetilde{M}$ is an element of $H^1(\Gamma_K, Z_T)$.

Let $s\colon \mathrm{T}_\ell Y \to \mathrm{T}_\ell M$ be a section for the exact sequence

$$0 \to \mathrm{T}_\ell G \to \mathrm{T}_\ell M \to \mathrm{T}_\ell Y \to 0$$

The class $\widetilde{M}$ is generated by the cocycle $\sigma \mapsto (\sigma - 1)s$. Since $c\widetilde{M} \in H^1(\Gamma_K, Z_T)$, there exists $t \in Z'_T$ such that $(\sigma - 1)(cs - t)$ lies in Z_T for every $\sigma \in \Gamma_K$. Then we have

$$\begin{aligned} c\varepsilon_\ell(M)(\sigma) &\equiv (\sigma - 1)^{-1}(\sigma - 1)cs \mod T \\ &\equiv (\sigma - 1)^{-1}(\sigma - 1)(cs - t) \mod T \end{aligned}$$

Hence the map $c\varepsilon_\ell(M)$ sends every element σ from its domain in the set $Z_V \bmod T$. This proves the first inclusion in (5.2).

To prove the second inclusion let $\sigma \in \Gamma_K$ be any element such that $\sigma^k - 1$ is an automorphism of V for all $k \geq 1$. Such an element exists by Lemma 5.2.6(i). Let c' be any positive integer such that $c'\varepsilon_\ell(M)(\sigma) \equiv 0 \mod T$. Note that due to 5.2.6(ii) one can choose σ such that $c' = 1$ for all but finitely many ℓ. Let Δ be the image of the map $\delta_\ell(M)$ in Z_T. By Lemma 3.4.3 (ii) and (iii) it follows that for every $u \in U$ we have

$$\begin{aligned} c'\varepsilon_\ell(M)(u\sigma^k) &\equiv c'\varepsilon_\ell(M)(\sigma) + (\sigma^k - 1)^{-1}\delta_\ell(M)(u) \mod T \\ &\equiv (\sigma^k - 1)^{-1}\delta_\ell(M)(u) \mod T, \end{aligned}$$

hence the we have the inclusion

$$\left(\bigcup_{k\geq 1} (\sigma^k - 1)^{-1}\Delta\right) \bmod T \subseteq c' \operatorname{Im} \varepsilon_\ell(M)$$

By Theorem 5.2.1, Δ is an open subset of Z_T. Since the group generated by σ is infinite (due to the fact that $\sigma^k - 1$ is an automorphism of V for all $k \geq 1$) it follows that there exist a sequence $\{k_n\}_n$ such that the operator norm of $\sigma^{k_n} - 1$ acting on V converges to zero. Then for any vector v in Z_V there exists n such that $(\sigma^{k_n} - 1)v$ lies in Δ. This implies that

$$Z_V = \bigcup_{k\geq 1} (\sigma^k - 1)^{-1}\Delta,$$

whence the second inclusion in (5.2) follows. □

Chapter 6

Algebraic dependences on $\mathbb{G}_m$

The purpose of this chapter is to define and study a certain family of properties that finitely-generated groups of rational points in tori may have. We give some examples of such properties.

Let $\Gamma \subset \mathbb{G}_m^2(\mathbb{Q})$ be a free abelian group of rational points of rank 2 and let p and ℓ be two different prime numbers. Consider the following properties:

$Cyc\ell_p(\Gamma)$: The group Γ reduces modulo p and its reduction is a cyclic group

$Cyc\ell_p^\ell(\Gamma)$: Γ reduces modulo p and the ℓ-part of its reduction is cyclic

$Cyc\ell_p^p(\Gamma)$: Γ reduces modulo p and its p-adic closure in $\mathbb{G}_m^2(\mathbb{Q}_p)$ is 1-dimensional.

It is easy to see that $Cyc\ell_p(\Gamma)$ is equivalent to $Cyc\ell_p^\ell(\Gamma)$ *for all* $\ell \neq p$. We have the following result:

6.0.2 Theorem. *The set of primes p for which property $Cyc\ell_p(\Gamma)$ holds is either of density 0, or of density 1. In the second case, Γ is contained in a proper algebraic subgroup of $\mathbb{G}_m^2$.*

To see the relationship with the property $Cyc\ell_p^p(\Gamma)$ consider the following conjecture

6.0.3 Conjecture (p-adic Four Exponentials Conjecture)**.** *Assume that property $Cyc\ell_p^p(\Gamma)$ holds for some fixed prime p. Then Γ is contained in a proper algebraic subgroup of $\mathbb{G}_m^2$.*

Let $P_1, P_2 \in \mathbb{G}_m^2(\mathbb{Q})$ be generators of Γ. To say that Γ reduces modulo p is equivalent to saying that the p-adic valuation of the coordinates of P_1 and P_2 is zero, or in other words, it is the same as saying that P_1 and P_2 lie in the subset $(\mathbb{Z}_p^\times)^2$ of $\mathbb{G}_m^2(\mathbb{Q}_p) \cong (\mathbb{Q}_p^\times)^2$. Let $\log_p \colon \mathbb{Z}_p^\times \to \mathbb{Z}_p$ denote the p-adic logarithm, and let $P_1 = (P_{11}, P_{12})$ and $P_2 = (P_{21}, P_{22})$. The p-adic closure of Γ is 1-dimensional if and only if the vectors $(\log_p P_{11}, \log_p P_{12})$ and $(\log_p P_{21}, \log_p P_{22})$ are linearly dependent over $\mathbb{Q}_p$, which is equivalent to saying that $\log_p P_{11} \log_p P_{22} - \log_p P_{12} \log_p P_{21} = 0$. Consider the following matrix:

$$\begin{pmatrix} \log_p P_{11} & \log_p P_{12} \\ \log_p P_{21} & \log_p P_{22} \end{pmatrix}$$

It is not difficult to see that if Γ has rank 1 then the two rows of the matrix above are linearly dependent over $\mathbb{Q}$. On the other hand, if Γ is contained in

a proper algebraic subgroup then the two columns will be linearly dependent over $\mathbb{Q}$. So Conjecture 6.0.3 can be rewritten in the following more familiar form:

6.0.4 Conjecture. *Let P_{11}, P_{12}, P_{21} and P_{22} be rational numbers whose p-adic valuation is 0. Assume that the equation*

$$\log_p P_{11} \log_p P_{22} - \log_p P_{12} \log_p P_{21} = 0$$

holds. Then either the rows or the columns of the matrix

$$\begin{pmatrix} \log_p P_{11} & \log_p P_{12} \\ \log_p P_{21} & \log_p P_{22} \end{pmatrix}$$

are linearly dependent over $\mathbb{Q}$.

The properties described in the examples are related to a certain homogenous polynomial. In this case the polynomial is the determinant of a 2-by-2 matrix (i.e. $y_{11}y_{22} - y_{12}y_{21}$). We will call such polynomials *algebraic dependences*. More generally, if we are interested in a 1-motive $M = [Y \to \mathbb{G}_m]$ defined over a number field, then the associated algebraic dependences are the homogenous ideals in the symmetric algebra of Y. We define those in Section 6.1 and show how to any such 1-motive M and any algebraic dependence one can associate a certain family of properties concerning the ℓ-part of the reduction of M modulo primes of good reduction. The main theorem 6.1.6 gives a characterization of the primes for which those properties hold.

In Section 6.2 we derive Theorem 6.0.2 as a consequence of our main theorem. Then we present the proof of the main theorem in Sections 6.3 and 6.4. The proof is reduced to studying the image of the Frobenius element for primes of good reduction into the ℓ-adic Galois representation associated to M. Finally, in the last section, we introduce several conjectures concerning algebraic dependences, of which Conjecture 6.0.3 is a special case. We also discuss the analogy between our conjectures and the main theorem.

6.1 Algebraic dependences

We fix a number field K and a Galois K-module Y. We will denote by G the Cartier dual of Y. It is equal to $\hat{Y} \otimes \mathbb{G}_m$. Recall that we have isomorphisms $\mathrm{T}_\ell G \cong \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell \mathbb{G}_m)$ and $\mathrm{B}_\ell G \cong \mathrm{Hom}(Y, \mathbb{G}_m[\ell^\infty])$.

We need to introduce the following notation. Let R be a commutative ring and let X be an R-module. We will write $R[X]$ to denote the symmetric algebra generated by X. That is,

$$R[X] := \bigoplus_{n \geq 0} S^n(X),$$

where $S^0(X) = R$ and $S^n(X)$ is the n-th symmetric power of X. If $R \to R'$ is a ring homomorphism, we will write

$$R'[X] := R[X] \otimes_R R'.$$

Since base change commutes with taking symmetric power, we have a canonical isomorphism

$$R'[X] \cong R'[X \otimes_R R'].$$

6.1.1 Definition. The Galois action on Y induces a natural Galois action on $\mathbb{Z}[Y]$. We will call an ideal $I \subset \mathbb{Z}[Y]$ an **algebraic dependence**, if I is a homogenous ideal which is invariant under the action of Γ_K.

We can isolate a special class of algebraic dependences. Let $Z \subseteq Y$ be a Γ_K-invariant submodule. We will denote by $L(Z)$ the ideal in $\mathbb{Z}[Y]$ generated by Z. Every algebraic dependence which is of the form $L(Z)$ for some Z will be called a **linear dependence**.

If $\widehat{\mathrm{T}_\ell G}$ is the $\mathbb{Z}_\ell$-dual of $\mathrm{T}_\ell G$, then $\mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$ is precisely the ring of all polynomial functions on $\mathrm{T}_\ell G$ with coefficients in $\mathbb{Z}_\ell$. One can check that the Γ_K-action is compatible with this interpretation: if $\sigma \in \Gamma_K$ and $f \in \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$ then we have

$$(\sigma f) = f \circ \sigma^{-1}.$$

6.1.2 Lemma. *Let ℓ be a prime number. There is a canonical isomorphism*

$$c_\ell \colon \operatorname{Proj} \mathbb{Z}_\ell[Y] \xrightarrow{\sim} \operatorname{Proj} \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}],$$

This morphism is compatible with the action of Γ_K on both schemes induced by the action on the underlying rings.

Proof. Let τ be any basis element of $\mathrm{T}_\ell \mathbb{G}_m$ (that is, $|\tau|_\ell = 1$). Then τ induces an isomorphism

$$\tau_* \colon \hat{Y} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{T}_\ell G,\ \hat{y} \mapsto \hat{y} \otimes \tau,$$

The $\mathbb{Z}_\ell$-dual of τ_*, after taking symmetric powers, induces an isomorphism

$$\tau^\sharp \colon \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}] \xrightarrow{\sim} \mathbb{Z}_\ell[Y].$$

This isomorphism gives the isomorphism of projective schemes c_ℓ stated in the lemma.

If we pick another basis element $\tau' \in \mathrm{T}_\ell \mathbb{G}_m$, it will follow that

$$(\tau')^\sharp = \alpha \tau^\sharp$$

for some $\alpha \in \mathbb{Z}_\ell^\times$. But then $(\tau')^\sharp$ induces the same isomorphism of projective schemes as $\tau^\sharp$. Hence the isomorphism c_ℓ does not depend on the choice of τ.

Let $\sigma \in \Gamma_K$. An easy computation gives

$$\sigma(\tau^\sharp f) = (\sigma\tau)^\sharp f.$$

Since $\tau^\sharp$ and $(\sigma\tau)^\sharp$ induce the same isomorphism, it follows that c_ℓ is Γ_K-equivariant. □

The lemma above implies that to every homogenous ideal I in $\mathbb{Z}[Y]$ one can associate an ideal $I \otimes \mathbb{Z}_\ell$ in $\mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$.

6.1.3 Construction. Let $J \subseteq \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$ be a set. We will denote by $Z(J, \mathrm{T}_\ell G)$ and $Z(J, \mathrm{V}_\ell G)$ the zero sets of J in $\mathrm{T}_\ell G$ and $\mathrm{V}_\ell G$ respectively. We also want to associate to it a set

$$Z(J, \mathrm{B}_\ell G) \subseteq \mathrm{B}_\ell G.$$

We proceed as follows.

Let $x \in \mathrm{B}_\ell G$. We define $v(x)$ to be the smallest positive integer n such that $\ell^n x = 0$ (in particular $v(0) = 1$). In other words, $v(x) = \min\{n\colon x \in G[\ell^n]\}$.

Every function $f \in \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$ satisfies the inequality

$$|f(x) - f(y)|_\ell \le |x - y|_\ell$$

for every $x, y \in \mathrm{T}_\ell G$. Hence it induces well-defined functions $f_n\colon G[\ell^n] \to \mathbb{Z}/\ell^n$ which are characterized by the following commutative diagram:

$$\begin{array}{ccc} \mathrm{T}_\ell G & \xrightarrow{f} & \mathbb{Z}_\ell \\ \downarrow & & \downarrow \\ G[\ell^n] & \xrightarrow{f_n} & \mathbb{Z}/\ell^n \end{array}$$

Therefore we can define the set

$$Z(J, \mathrm{B}_\ell G) := \{x \in \mathrm{B}_\ell G\colon f_{v(x)}(x) = 0 \text{ for each } f \in J\}. \tag{6.1}$$

Equivalently, $x \in \mathrm{B}_\ell G$ lies in $Z(J, \mathrm{B}_\ell G)$ if and only if for every $f \in J$ we have

$$|f(\tilde{x})|_\ell \le \ell^{-v(x)}$$

where $\tilde{x} \in \mathrm{T}_\ell G$ is an arbitrary pre-image of x under the projection map $\mathrm{T}_\ell G \to G[\ell^{v(x)}]$.

6.1.4 Lemma. *Let $J \subset \mathbb{Z}_\ell[\mathrm{T}_\ell G]$ be a homogenous ideal.*

(i) If $\{f_1, \dots, f_k\}$ is a basis for J then

$$Z(J, \mathrm{B}_\ell G) = Z(\{f_1, \dots, f_k\}, \mathrm{B}_\ell G);$$

(ii) If J is Galois-invariant, then so is $Z(J, \mathrm{B}_\ell G)$;

(iii) The pre-image of $Z(J, \mathrm{B}_\ell G)$ under the quotient map $\mathrm{V}_\ell G \to \mathrm{B}_\ell G$ is the set $Z^*(J, \mathrm{V}_\ell G)$ consisting of those points $x \in \mathrm{V}_\ell G$ for which

$$|f(x)|_\ell \le \|x\|_\ell^{\deg f - 1} \tag{6.2}$$

for every homogenous $f \in J$.

Proof.

(i) Since $\{f_1, \dots, f_k\}$ is a subset of J, it follows trivially that $Z(J, \mathrm{B}_\ell G) \subseteq Z(\{f_1, \dots, f_k\}, \mathrm{B}_\ell G)$. On the other hand every element $f \in J$, can be represented as $f = g_1 f_1 + \dots + g_k f_k$, where $g_1, \dots, g_k \in \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$. Hence if $x \in Z(\{f_1, \dots, f_k\}, \mathrm{B}_\ell G)$ and if $\tilde{x}$ is any pre-image of x in $\mathrm{T}_\ell G$ then

$$|f(\tilde{x})|_\ell \le \max_i \{|g_i(\tilde{x})|_\ell |f_i(\tilde{x})|_\ell\} \le \ell^{-v(x)}$$

It follows that $Z(\{f_1, \dots, f_k\}, \mathrm{B}_\ell G) \subseteq Z(J, \mathrm{B}_\ell G)$ which proves the claim.

(ii) We need to show that if $x \in Z(I, \mathrm{B}_\ell G)$ then $\sigma x \in Z(I, \mathrm{B}_\ell G)$ for all $\sigma \in \Gamma_K$. Indeed, if $f \in J$, then we have

$$f_{v(x)}(\sigma x) = (\sigma^{-1} f_{v(x)})(x) = (\sigma^{-1} f)_{v(x)}(x) = 0,$$

since $\sigma^{-1} f \in J$ for every $f \in J$. (The equality $(\sigma^{-1} f)_{v(x)} = \sigma^{-1} f_{v(x)}$ is an easy corollary of the definitions.) This proves the statement.

(iii) Let $x \in \mathrm{V}_\ell G$ and let $\bar{x}$ denote its image in $\mathrm{B}_\ell G \cong \mathrm{V}_\ell G / \mathrm{T}_\ell G$. If $x \in \mathrm{T}_\ell G$ then $\bar{x} = 0$ and $\bar{x} \in Z(J, \mathrm{B}_\ell G)$. On the other hand $\mathrm{T}_\ell G$ is contained in $Z^*(J, \mathrm{V}_\ell G)$, since for every x in $\mathrm{T}_\ell G$ and every homogenous polynomial f we have the inequality

$$|f(x)|_\ell \leq \|x\|_\ell^{\deg f} \leq \|x\|_\ell^{\deg f - 1},$$

due to the fact that $\|x\|_\ell \leq 1$.

Next let $x \in \mathrm{V}_\ell G \setminus \mathrm{T}_\ell G$. If $\|x\|_\ell = \ell^n$, set $y := \ell^n x$. The element y lies in $\mathrm{T}_\ell G$ and $\bar{x}$ is precisely the image of y under the map $\mathrm{T}_\ell G \to G[\ell^n]$. Let $f \in J$ be a homogenous polynomial. Then $f_n(\bar{x}) = 0$ if and only if $|f(y)| \leq \ell^{-n} = \|x\|_\ell^{-1}$. Since $f(y) = \ell^{n \deg f} f(x)$, it follows that the last inequality is equivalent to (6.2). Hence $\bar{x} \in Z(J, \mathrm{B}_\ell G)$ if and only if $x \in Z^*(J, \mathrm{V}_\ell G)$ for every $x \in \mathrm{V}_\ell G$. □

Let I be an algebraic dependence. We define

$$Z(I, \mathrm{B}_\ell G) := Z(I \otimes \mathbb{Z}_\ell, \mathrm{B}_\ell G)$$

and

$$Z^*(I, \mathrm{V}_\ell G) := Z^*(I \otimes \mathbb{Z}_\ell, \mathrm{V}_\ell G)$$

Let $\mathfrak{p}$ be a prime of good reduction for G, let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K and let $k_\mathfrak{p}$ be the residue field. Let $G_\mathfrak{p}$ denote the reduction of G at $\mathfrak{p}$. Recall that any embedding $K^s \hookrightarrow K_\mathfrak{p}^s$ induces an isomorphism

$$red_\mathfrak{p} \colon \mathrm{B}_\ell G_\mathfrak{p} \cong \mathrm{B}_\ell G.$$

(see (4.3) in Section 4.2). We set

$$Z(I, \mathrm{B}_\ell G_\mathfrak{p})$$

to be the image of $Z(I, \mathrm{B}_\ell G)$ under this isomorphism. As the latter set is Γ_K-invariant, it follows that the image $Z(I, \mathrm{B}_\ell G_\mathfrak{p})$ is independent of the choice of embedding $K^s \hookrightarrow K_\mathfrak{p}^s$.

6.1.5 Definition. Let $M = [Y \xrightarrow{u} \mathbb{G}_m]$ be a 1-motive over K and let I be an algebraic dependence. Let $\mathfrak{p}$ be a prime ideal of good reduction and let p be the characteristic of its residue field $k_\mathfrak{p}$. Let $M_\mathfrak{p}$ denote the reduction of M at $\mathfrak{p}$. We will say that **the ℓ-part of $M_\mathfrak{p}$ satisfies** I if the ℓ-adic projection $pr_\ell(M_\mathfrak{p})$ of $M_\mathfrak{p}$ lies in the set $Z(I, \mathrm{B}_\ell G_\mathfrak{p})$. We say that $M_\mathfrak{p}$ **satisfies** I if the ℓ-part of $M_\mathfrak{p}$ satisfies I for every prime number $\ell \neq p$.

Every algebraic dependence $I \subseteq \mathbb{Z}[Y]$ induces an ideal $I \otimes \mathbb{Q} \subseteq \mathbb{Q}[Y]$. We will say that an algebraic dependence I is **exceptional for** M if $I \otimes \mathbb{Q}$ is contained in $L(\ker u) \otimes \mathbb{Q}$. Otherwise we will call I **generic for** M.

We recall the following notation: if $f(x)$ and $g(x)$ are two real-valued functions whose domain is the set X then we write $f(x) = O(g(x))$ if there exists a non-negative real constant c such that $|f(x)| \leq c|g(x)|$ for all $x \in X$. We write $f(x) = \Theta(g(x))$ if there exist non-negative constants c, c' such that $cg(x) \leq f(x) \leq c'g(x)$ for all $x \in X$. Then we have the following result:

6.1.6 Theorem. *Let Y be a trivial Galois K-module and let $M = [Y \xrightarrow{u} \mathbb{G}_m]$ be a K-1-motive. Let I be an algebraic dependence for Y.*

(i) There exists a finite set of prime numbers S which depends only on M but not on I and such that for every $\ell \notin S$ the following holds: I is exceptional for M if and only if the ℓ-part of $M_{\mathfrak{p}}$ satisfies I for all primes $\mathfrak{p}$ of good reduction;

(ii) If I is exceptional for M, then $M_{\mathfrak{p}}$ satisfies I for all primes $\mathfrak{p}$ of good reduction;

(iii) If I is generic for M, then for every prime number ℓ the set of primes $\mathfrak{p}$ for which the ℓ-part of $M_{\mathfrak{p}}$ satisfies I has density $1 - \Theta(\ell^{-1})$, where the implicit constants depend on M and I.

(iv) If I is generic for M, then the set of primes $\mathfrak{p}$ of good reduction for which $M_{\mathfrak{p}}$ satisfies I has zero density.

6.2 An example: The rank of reduction of $\mathbb{Z}^2 \to \mathbb{G}_m^2$

We will now show how Theorem 6.1.6 implies Theorem 6.0.2 stated in the introduction. We will prove the following slightly more general result:

6.2.1 Theorem. *Let K be a number field and let $\Gamma \subset \mathbb{G}_m^2(K)$ be a torsion-free subgroup of rank 2. Assume that Γ is not contained in any proper algebraic subgroup of $\mathbb{G}_m^2$. Then the set of places $\mathfrak{p}$ for which the reduction of Γ modulo $\mathfrak{p}$ is well-defined and cyclic has zero density.*

We fix points $P_1, P_2 \in \mathbb{G}_m^2(K)$ which generate Γ. Each point P_i can be represented as a tuple $P_i = (P_{i1}, P_{i2})$ where $P_{ij} \in \mathbb{G}_m(K)$ for $i, j \in \{1, 2\}$.

Let Y be a free $\mathbb{Z}$-module of rank 4, on which Γ_K acts trivially. We will fix a basis $\{y_{11}, y_{12}, y_{21}, y_{22}\}$ on Y. Then we will be interested in studying the algebraic dependence induced by the polynomial $f = y_{11}y_{22} - y_{12}y_{21}$ and the 1-motive $M = [Y \xrightarrow{u} \mathbb{G}_m]$ given by $u(y_{ij}) = P_{ij}$. By the general theory (see Corollary 4.2.7) M has good reduction for all but finitely many primes $\mathfrak{p}$, which in turn implies that Γ has well-defined reduction modulo $\mathfrak{p}$ for all but fintely many primes $\mathfrak{p}$. We denote the reduction of M at $\mathfrak{p}$ by $M_{\mathfrak{p}}$.

6.2.2 Proposition. *Let ℓ be a prime number and let $\mathfrak{p}$ be a place of good reduction for M which is coprime to ℓ. Let $\overline{\Gamma}$ denote the reduction of Γ modulo $\mathfrak{p}$. The ℓ-primary part of $\overline{\Gamma}$ is cyclic if and only if the ℓ-part of $M_{\mathfrak{p}}$ satisfies the algebraic dependence f.*

Proof. As before we will denote $G = \hat{Y} \otimes \mathbb{G}_m$. The basis that we have fixed on Y induces a basis $\hat{y}_{11}, \ldots, \hat{y}_{22}$ on $\hat{Y}$. We will fix a basis element τ of $\mathrm{T}_\ell \mathbb{G}_m$ and will denote its projection to $\mathbb{G}_m[\ell^n]$ by τ_n. We will also denote the reduction

of $\mathbb{G}_m$ and G modulo $\mathfrak{p}$ by $\overline{\mathbb{G}}_m$ and $\overline{G}$ respectively. We fix an embedding of K^s into the algebraic closure $K_{\mathfrak{p}}^s$ of the completion of K at $\mathfrak{p}$. It induces compatible isomorphisms $\mathbb{G}_m[\ell^n] \simeq \overline{\mathbb{G}}_m[\ell^n]$ for every n. We will denote by $\bar{\tau}_n$ the images of τ_n under those isomorphisms. Furthermore, we will denote by $\overline{P}_i$ (resp. $\overline{P}_{ij}$) the reduction of P_i (resp. P_{ij}) modulo $\mathfrak{p}$. We have a unique decomposition

$$\overline{P}_i = \sum_{\ell} pr_\ell(\overline{P}_i),$$

where $pr_\ell(\overline{P}_i)$ has order a power of ℓ. We have a similar decomposition of P_{ij}. Then the ℓ-part of $\overline{\Gamma}$ is generated by the points $pr_\ell(\overline{P}_1)$ and $pr_\ell(\overline{P}_2)$.

As in the previous section we have an isomorphism

$$\tau_* \colon \hat{Y} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{T}_\ell G,\ \sum_{ij} \alpha_{ij}\hat{y}_{ij} \mapsto \sum_{ij} \alpha_{ij}\hat{y}_{ij} \otimes \tau,$$

which induces an isomorphism

$$\tau_\flat = (\tau^\sharp)^{-1} \colon \mathbb{Z}_\ell[Y] \to \mathbb{Z}_\ell[\widehat{\mathrm{T}_\ell G}]$$

In particular, we have

$$(\tau_\flat f)\left(\sum_{ij} \alpha_{ij}\hat{y}_{ij} \otimes \tau\right) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}.$$

Let m be the exponent of ℓ in the order of $pr_\ell(M_{\mathfrak{p}})$. Then $pr_\ell(M_{\mathfrak{p}}) \in \overline{G}[\ell^m]$ and there exist $\beta_{ij} \in \mathbb{Z}/\ell^m$ such that

$$pr_\ell(M_{\mathfrak{p}}) = \sum_{ij} \beta_{ij}\hat{y}_{ij} \otimes \bar{\tau}_m.$$

Equivalently, we have $\beta_{ij}\bar{\tau}_m = pr_\ell(\overline{P}_{ij})$. Then by the definitions in the previous section it follows that the ℓ-part of $M_{\mathfrak{p}}$ satisfies f if and only if

$$\beta_{11}\beta_{22} - \beta_{12}\beta_{21} = 0$$

in $\mathbb{Z}/\ell^m$. Equivalently this holds if and only if

$$|\beta'_{11}\beta'_{22} - \beta'_{12}\beta'_{21}|_\ell \leq \ell^{-m}$$

for some arbitrary pre-images $\beta'_{ij} \in \mathbb{Z}_\ell$ of $\beta_{ij} \in \mathbb{Z}/\ell^m$.

6.2.3 Lemma. *Let $\beta_{11}, \ldots, \beta_{22} \in \mathbb{Z}/\ell^m$ be such that at least one β_{ij} is of maximal order. Then the following are equivalent*

(i) $\beta_{11}\beta_{22} - \beta_{12}\beta_{21} = 0$;

(ii) The linear system

$$\left|\begin{array}{ll} \lambda_1\beta_{11} + \lambda_2\beta_{21} & = 0 \\ \lambda_1\beta_{12} + \lambda_2\beta_{22} & = 0 \end{array}\right.$$

has a solution $\lambda = (\lambda_1, \lambda_2) \in (\mathbb{Z}/\ell^m)^2$ whose order is ℓ^m.

Proof. To show that (i) implies (ii) assume, without loss of generality, that the tuple (β_{11}, β_{21}) has maximal order. Then the pair $(\lambda_1, \lambda_2) = (\beta_{11}, -\beta_{21})$ is a solution of maximal order to the linear system in (ii).

Conversely to show that (ii) implies (i) one simply performs Gauss elimination on the linear system (i.e. if e.g. λ_1 is of maximal order multiply the first equation by $\lambda_1^{-1}\beta_{22}$ and the second by $-\lambda_1^{-1}\beta_{21}$ and add the two equations). □

By the previous lemma it follows that the ℓ-part of $M_{\mathfrak{p}}$ satisfies f if and only if the system

$$\left|\begin{array}{ll} \lambda_1\beta_{11}\bar{\tau}_m + \lambda_2\beta_{21}\bar{\tau}_m & = 0 \\ \lambda_1\beta_{12}\bar{\tau}_m + \lambda_2\beta_{22}\bar{\tau}_m & = 0 \end{array}\right.$$

has a solution $(\lambda_1, \lambda_2) \in (\mathbb{Z}/\ell^m)^2 \backslash (\ell\mathbb{Z}/\ell^m)^2$. (Here 0 denotes the trivial element in $\overline{\mathbb{G}}_m$.) But since $\beta_{ij}\bar{\tau}_m = pr_\ell(\overline{P}_{ij})$ this is the same as saying that the ℓ-part of $M_{\mathfrak{p}}$ satisfies f if and only if the equation

$$\lambda_1 pr_\ell(\overline{P}_1) + \lambda_2 pr_\ell(\overline{P}_2) = 0$$

has a solution $(\lambda_1, \lambda_2) \in (\mathbb{Z}/\ell^m)^2 \setminus (\ell\mathbb{Z}/\ell^m)^2$. The last condition is clearly equivalent to saying that the ℓ-part of the reduction of Γ modulo $\mathfrak{p}$ is cyclic. This proves the proposition. □

Let $(\lambda, \mu) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Consider the following submodules of Y:

$$R_{\lambda,\mu} = \mathrm{span}_{\mathbb{Z}}\{\lambda y_{11} + \mu y_{21}, \lambda y_{12} + \mu y_{22}\}$$
$$S_{\lambda,\mu} = \mathrm{span}_{\mathbb{Z}}\{\lambda y_{11} + \mu y_{12}, \lambda y_{21} + \mu y_{22}\}.$$

6.2.4 Lemma. *We have $R_{\lambda,\mu} \not\subseteq \ker u$ and $S_{\lambda,\mu} \not\subseteq \ker u$ for all pairs $(\lambda, \mu) \neq (0,0)$.*

Proof. Recall that we assume that Γ is a free abelian group of rank 2 which is not contained in any proper algebraic subgroup of $\mathbb{G}_m^2$.

If $R_{\lambda,\mu} \subseteq \ker u$ then it follows that $\lambda P_{11} + \mu P_{21} = 0$ and $\lambda P_{12} + \mu P_{22} = 0$ It would follow that $\lambda P_1 + \mu P_2 = 0$. Since P_1 and P_2 are generators of Γ this would contradict the assumption that Γ is a free abelian group of rank 2.

On the other hand, if $S_{\lambda,\mu} \subseteq \ker u$ a similar argument would imply that Γ is contained in the algebraic subgroup $H \subseteq \mathbb{G}_m^2$ described by the relation: $(Q_1, Q_2) \in H$ if and only if $\lambda Q_1 + \mu Q_2 = 0$. This again contradicts our assumptions for Γ. □

Let $L \subseteq \hat{Y} \otimes \mathbb{Q}$ denote the dual vector space of $(\ker u) \otimes \mathbb{Q}$. Let $\hat{R}_{\lambda,\mu}$ and $\hat{S}_{\lambda,\mu}$ denote the dual vector spaces to $R_{\lambda,\mu} \otimes \mathbb{Q}$ and $S_{\lambda,\mu} \otimes \mathbb{Q}$ respectively. Then the previous lemma implies the following

6.2.5 Corollary. *For all $(\lambda, \mu) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ we have $L \not\subseteq \hat{R}_{\lambda,\mu}$ and $L \not\subseteq \hat{S}_{\lambda,\mu}$*

Proof. Indeed, if $L \subseteq \hat{R}_{\lambda,\mu}$ then we will have that $R_{\lambda,\mu} \subseteq \ker u \otimes \mathbb{Q}$. It is then easy to see that there exists $n \in \mathbb{N}$ such that $R_{n\lambda,n\mu} \subseteq \ker u$, which contradicts Lemma 6.2.4. The argument for $\hat{S}_{\lambda,\mu}$ is analogous. □

6.2.6 Proposition. *Assume that f is an exceptional algebraic dependence for M. Then there exists $(\lambda, \mu) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that either $L \subseteq \hat{R}_{\lambda,\mu}$ or $L \subseteq \hat{S}_{\lambda,\mu}$.*

Proof. The set $\hat{Y} \otimes_{\mathbb{Q}} \mathbb{Q}$ can be considered as the set of rational points of the affine scheme $\mathbb{A}^4_{\mathbb{Q}} = \operatorname{Spec} \mathbb{Q}[y_{11}, y_{12}, y_{21}, y_{22}]$. The ideal generated by $\ker u$ then induces an affine subscheme $V_u \subset \mathbb{A}^4_{\mathbb{Q}}$ such that $V_u(\mathbb{Q}) = L$. Similarly f induces the affine subscheme $V_f \subseteq \mathbb{A}^4_{\mathbb{Q}}$:

$$V_f \colon y_{11}y_{22} - y_{12}y_{21} = 0$$

By our definitions, if f is exceptional for M, then $(f) \subseteq (\ker u) \otimes \mathbb{Q}$ which implies that $L \subseteq V_f(\mathbb{Q})$. To prove the proposition we therefore need to understand the linear spaces of 2-by-2 matrices with zero determinant.

The space $\hat{R}_{\lambda,\mu}$ has a basis $\{-\mu\hat{y}_{11} + \lambda\hat{y}_{21}, -\mu\hat{y}_{12} + \lambda\hat{y}_{22}\}$, or in matrix notation $\{\left(\begin{smallmatrix} -\mu & 0 \\ \lambda & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -\mu \\ 0 & \lambda \end{smallmatrix}\right)\}$. It is trivial to see that the column vectors of every matrix in $\hat{R}_{\lambda,\mu}$ are linearly dependent, which implies that $\hat{R}_{\lambda,\mu} \subseteq V_f(\mathbb{Q})$. Similarly $\hat{S}_{\lambda,\mu}$ is spanned by the matrices $\{\left(\begin{smallmatrix} -\mu & \lambda \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ -\mu & \lambda \end{smallmatrix}\right)\}$ and it is easy to see that $\hat{S}_{\lambda,\mu} \subseteq V_f(\mathbb{Q})$. We will show that any linear space contained in $V_f(\mathbb{Q})$ must lie in one of the spaces $\hat{R}_{\lambda,\mu}$ and $\hat{S}_{\lambda,\mu}$

Let $F \subseteq V_f(\mathbb{Q})$ be a linear space. Since V_f is 3-dimensional, non-linear and irreducible, it contains no 3-dimensional linear subspaces. Hence we can assume that we have 4 column vectors $v_1, \ldots, v_4 \in \mathbb{Z}^2$ such that F is spanned by the matrices (v_1, v_2) and (v_3, v_4). We will use the following lemma:

6.2.7 Lemma. *Let K be a field and let $v_1, \ldots, v_4 \in K^2$. Assume that the pairs $\{v_1, v_2\}$, $\{v_3, v_4\}$ and $\{v_1 + v_3, v_2 + v_4\}$ are all linearly dependent. Then one of the following holds:*

(i) $\dim \operatorname{span}_K\{v_1, v_2, v_3, v_4\} \leq 1$*;*

(ii) There exist $\alpha, \beta \in K$, $(\alpha, \beta) \neq (0,0)$ such that

$$\begin{cases} \alpha v_1 + \beta v_2 = 0 \\ \alpha v_3 + \beta v_4 = 0 \end{cases}$$

Proof. Assume that (i) doesn't hold. Then at least one of the vectors $v_1 + v_3$ and $v_2 + v_4$ is non-zero. Assume without loss of generality that $v_1 + v_3 \neq 0$. Again, since the vectors $v_1, \ldots, v_4$ span the whole space K^2 it follows that $v_1 \neq 0$ and $v_3 \neq 0$. Then there exist $a, b, c \in K$ such that

$$\begin{cases} av_1 - v_2 = 0 \\ bv_3 - v_4 = 0 \\ v_2 + v_4 = c(v_1 + v_3) \end{cases}$$

Solving the system and using the fact that v_1 and v_3 are linearly independent we get $a = b = c$ which implies (ii). □

In our situation the matrices (v_1, v_2), (v_3, v_4) and $(v_1 + v_2, v_3 + v_4)$ must lie in $V_f(\mathbb{Q})$ which implies that their rank must be at most 1. Hence the conditions of the lemma are satisfied. To conclude the proof notice that if (i) is satisfied

then F lies in $\hat{R}_{\lambda,\mu}$ for some (λ, μ), and if (ii) is satisfied then F lies in $\hat{S}_{\lambda,\mu}$ for some (λ, μ). We leave this last claim as an exercise for the reader. This proves the proposition. □

We can now finish the proof of Theorem 6.2.1. The algebraic dependence f can either be generic or exceptional for M. But if f is exceptional, then the conclusion of Proposition 6.2.6 would contradict Corollary 6.2.5. This implies that f is generic. Let $\mathfrak{p}$ be a prime of good reduction for M. Then $M_\mathfrak{p}$ satisfies f if and only if the ℓ-part of $M_\mathfrak{p}$ satisfies f for all prime numbers ℓ coprime to $\mathfrak{p}$. By Proposition 6.2.2 this is equivalent to saying that the ℓ-primary part of the reduction of Γ modulo $\mathfrak{p}$ is cyclic for all ℓ coprime to $\mathfrak{p}$. In other words, $M_\mathfrak{p}$ satisfies f if and only if the reduction of Γ modulo $\mathfrak{p}$ is cyclic. We can now apply Theorem 6.1.6(iv) to reach the desired conclusion. □

6.3 The image of the Galois representation

The goal of this section is to describe the image of the Galois representations associated to the 1-motive $M = [Y \xrightarrow{u} \mathbb{G}_m]$ given in the statement of theorem 6.1.6.

Cyclotomic fields

Let K be a number field. We will denote by K_n the smallest field containing K and a primitive n-th root of unity. In particular $\mathbb{Q}_n$ will denote the n-th cyclotomic field.

Let $\Gamma_{K_n/K}$ be the Galois group of the field extension K_n/K. The action of this group on the n-th roots of unity (equivalently on the group $\mathbb{G}_m[n]$, where $\mathbb{G}_m$ is defined over K) induces an injection

$$\rho_n \colon \Gamma_{K_n/K} \hookrightarrow (\mathbb{Z}/n)^\times$$

Let $\varphi(n)$ denote the Euler function. Then we have the following standard result:

6.3.1 Lemma. *For any n, the degree $[\mathbb{Q}_n : \mathbb{Q}]$ of the extension $\mathbb{Q}_n/\mathbb{Q}$ is equal to $\varphi(n)$. Equivalently, for every n the natural map $\Gamma_{\mathbb{Q}_n/\mathbb{Q}} \to (\mathbb{Z}/n)^\times$ is an isomorphism.*

Proof. See [Lan02, VI, Thm. 3.1]. □

6.3.2 Corollary. *Let $m, n \in \mathbb{N}$. Let $d = (m, n)$ be the greatest common divisor of m and n. Then $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_d$.*

Proof. Let $k = [m, n]$ denote the least common multiple. It is easy to see that the compositum $\mathbb{Q}_n\mathbb{Q}_m$ contains a primitive k-th root of unity, which implies that $\mathbb{Q}_k = \mathbb{Q}_n\mathbb{Q}_m$. It is also clear that $\mathbb{Q}_d \subseteq \mathbb{Q}_n \cap \mathbb{Q}_m$. On the other hand we get

$$[\mathbb{Q}_n \cap \mathbb{Q}_m : \mathbb{Q}] = \frac{[\mathbb{Q}_n : \mathbb{Q}][\mathbb{Q}_m : \mathbb{Q}]}{[\mathbb{Q}_m\mathbb{Q}_n : \mathbb{Q}]} = \frac{\varphi(n)\varphi(m)}{\varphi(k)} = \varphi(d) = [\mathbb{Q}_d : \mathbb{Q}].$$

This implies our claim. □

6.3.3 Proposition. *Let K be a number field. There exists a finite set of prime numbers S such that if n is coprime to all elements in S then $[K_n : K] = \varphi(n)$ and the map $\rho_n \colon \Gamma_{K_n/K} \to (\mathbb{Z}/n)^\times$ is an isomorphism.*

Proof. For any abelian $\mathbb{Q}$-extension A contained in K let $Cyc\ell(A)$ denote the smallest cyclotomic extension containing A (due to the Kronecker-Weber theorem and 6.3.2 such an extension exists). We define $c(A)$ to be the smallest number such that $Cyc\ell(A) = \mathbb{Q}_{c(A)}$. If $\mathbb{Q}_n$ contains A, then, since $\mathbb{Q}_n \cap Cyc\ell(A) = Cyc\ell(A)$, it follows that $c(A)$ divides n. Let S denote the set of prime numbers ℓ which divide $c(A)$ for some A. Since there are only finitely many such A, the set S is finite.

Let n be any natural number, coprime to all primes in S. It follows that $K \cap \mathbb{Q}_n = \mathbb{Q}$, hence

$$[K_n : K] = [K\mathbb{Q}_n : K] = [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n),$$

which is what we wanted to prove. □

Applying the proposition above to the prime powers of a fixed prime ℓ and taking limits we get:

6.3.4 Corollary. *Let K be a number field and let $\mathbb{G}_m$ denote the multiplicative group defined over K. For all but finitely many primes ℓ the image of the associated ℓ-adic Galois representation $\rho_\ell(\mathbb{G}_m)$ is equal to $\mathrm{Aut}(\mathrm{T}_\ell\mathbb{G}_m) \cong \mathbb{Z}_\ell^\times$.*

Next, let S be a set of primes. To any 1-motive M over K we can associate the Galois representation:

$$\rho_{\bar{S}}(M) \colon \Gamma_K \to \prod_{\ell \notin S} \mathrm{Aut}_\ell(\mathrm{T}_\ell M).$$

This is the product of the representations $\rho_\ell(M)$ for all primes ℓ not lying in S. Then, after taking limits, Proposition 6.3.3 implies

6.3.5 Corollary. *There exists a finite set of prime numbers S such that the map*

$$\rho_{\bar{S}}(\mathbb{G}_m) \colon \Gamma_K \to \prod_{\ell \notin S} \mathrm{Aut}_\ell(\mathrm{T}_\ell\mathbb{G}_m) \cong \varprojlim_n (\mathbb{Z}/n)^\times$$

is surjective. The limit above is taken over all natural numbers n which are coprime to the primes in S.

The image of $\rho_\ell(M)$

Next, we want to describe the image of the ℓ-adic Galois representation $\rho_\ell(M)$ associated to the 1-motive $M = [Y \xrightarrow{u} \mathbb{G}_m]$. We will need the following notation: We will denote the kernel of u in Y by N, and we will let Q denote the quotient module Y/N. We will write $q = \dim Q \otimes_{\mathbb{Z}} \mathbb{Q}$, that is, q is the rank of the torsion-free part of Q.

We have isomorphisms $\mathrm{T}_\ell G \cong \mathrm{Hom}_{\mathbb{Z}}(Y, \mathrm{T}_\ell\mathbb{G}_m)$ and $\mathrm{B}_\ell G \cong \mathrm{Hom}_{\mathbb{Z}}(Y, \mathrm{B}_\ell\mathbb{G}_m)$. Hence we can consider the groups $\mathrm{Hom}_{\mathbb{Z}}(Q, \mathrm{T}_\ell\mathbb{G}_m)$ and $\mathrm{Hom}_{\mathbb{Z}}(Q, \mathrm{B}_\ell\mathbb{G}_m)$ as subgroups of $\mathrm{T}_\ell G$ and $\mathrm{B}_\ell G$ respectively. Then we have the lemma:

6.3.6 Lemma. *Let $\mathcal{O}$ denote the ring $\mathrm{End}_K(G) = \mathrm{End}_K(\hat{Y} \otimes \mathbb{G}_m)$. Then*

$$Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell G) = \mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m)$$

and

$$Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{B}_\ell G) = \mathrm{Hom}(Q, \mathrm{B}_\ell \mathbb{G}_m).$$

Proof. Let d denote the rank of Y. We have the canonical isomorphism

$$\mathcal{O} \cong \mathrm{End}_K(\hat{Y}).$$

Since Y is assumed to be a trivial Γ_K-module, the latter ring is (non-canonically) isomorphic to the ring of d-by-d integer matrices. For any $\phi \in \mathrm{End}_K(\hat{Y})$ we will denote the dual endomorphism by ϕ^t. Then, by the definition of $\mathrm{Ann}_{\mathcal{O}} M$ in Section 5.1, it follows that

$$\mathrm{Ann}_{\mathcal{O}} M = \{\phi \in \mathrm{End}_K(\hat{Y}) \colon \mathrm{Im}\, \phi^t \subseteq N\}.$$

Similarly, we have

$$Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell G) = \{f \in \mathrm{T}_\ell G \colon \mathrm{Im}\, \phi^t \subseteq \ker f \text{ for every } \phi \in \mathrm{Ann}_{\mathcal{O}} M\}$$

and

$$Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{B}_\ell G) = \{f \in \mathrm{B}_\ell G \colon \mathrm{Im}\, \phi^t \subseteq \ker f \text{ for every } \phi \in \mathrm{Ann}_{\mathcal{O}} M\}.$$

For any element $f \in \mathrm{T}_\ell G$ which lies in $\mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m)$ we have that $N \subseteq \ker f$. This implies that f is an element of $Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell G)$. Conversely, let $f \in Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell G)$. Let $y \in N$. We can construct an endomorphism ϕ such that

$$y \in \mathrm{Im}\, \phi^t \subseteq N.$$

Since such an automorphism is an element of $\mathrm{Ann}_{\mathcal{O}} M$ it follows that y lies in the kernel of f. Hence $N \subseteq \ker f$ which implies that f lies in $\mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m)$. This gives us the desired equality

$$Z(\mathrm{Ann}_{\mathcal{O}} M, \mathrm{T}_\ell G) = \mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m).$$

The argument for the second equality is analogous. □

6.3.7 Corollary.

(i) For all but finitely many primes ℓ the image of the Kummer map $\delta_\ell(M)$ is equal to $\mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m)$.

(ii) For all but finitely many primes ℓ the image of the Pink map $\varepsilon_\ell(M)$ is equal to $\mathrm{Hom}(Q, \mathrm{B}_\ell \mathbb{G}_m)$.

Proof. This follows directly from Theorems 5.2.1, 5.3.1 and the previous lemma. □

We will let $U_\ell \subseteq \mathrm{T}_\ell G$ denote the group $\mathrm{Hom}(Q, \mathrm{T}_\ell \mathbb{G}_m)$. Also, let $\mathrm{T}_\ell N$ denote the $\mathbb{Z}_\ell$-module induced by the image of N in $\mathrm{T}_\ell Y$ and let $\mathrm{T}_\ell Q$ denote their quotient. There is a canonical isomorphism

$$\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{T}_\ell Q, \mathrm{T}_\ell \mathbb{G}_m) \cong \mathrm{Hom}_{\mathbb{Z}}(Q, \mathrm{T}_\ell \mathbb{G}_m) = U_\ell.$$

If we consider N and Y as 1-motives, we have a commutative diagram

$$\begin{array}{ccc} N & \longrightarrow & M \\ & \searrow \quad \swarrow & \\ & Y & \end{array}$$

which induces a diagram of Tate modules

$$\begin{array}{ccc} \mathrm{T}_\ell N & \xrightarrow{\kappa} & \mathrm{T}_\ell M \\ & \searrow \quad \swarrow_{\pi} & \\ & \mathrm{T}_\ell Y & \end{array} \tag{6.3}$$

Since $\mathrm{T}_\ell N$ embeds in $\mathrm{T}_\ell Y$ it follows that the map κ is an injection.

We will denote by H_ℓ the group

$$H_\ell := \{\sigma \in \mathrm{Aut}(\mathrm{T}_\ell M) \colon (\sigma - 1) \circ \kappa = 0\}$$

If we write $C_\ell := \mathrm{Aut}(\mathrm{T}_\ell \mathbb{G}_m)$, then H_ℓ is a part of an exact sequence:

$$0 \to U_\ell \to H_\ell \to C_\ell \to 1 \tag{6.4}$$

6.3.8 Proposition. *The image of the Galois representation $\rho_\ell(M)$ is contained in H_ℓ. It is equal to H_ℓ for all but finitely many primes ℓ.*

Proof. We will write ρ instead of $\rho_\ell(M)$. Also we will write χ for the cyclotomic character $\rho_\ell(\mathbb{G}_m)$. Let Γ_K^U denote the kernel of χ.

Requiring that $\rho(\Gamma_K)$ lies in H_ℓ is equivalent to saying that the commutative diagram (6.3) is equivariant under the Γ_K-action. This holds, due to the properties of the functor T_ℓ, whence the first claim of the proposition follows.

As for the second claim, note that from the exact sequence (6.4) we get the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma_K^U & \longrightarrow & \Gamma_K & \xrightarrow{\chi} & \chi(\Gamma_K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \rho} & & \downarrow & & \\ 0 & \longrightarrow & U_\ell & \longrightarrow & H_\ell & \longrightarrow & C_\ell & \longrightarrow & 1 \end{array}$$

where δ denotes the Kummer map $\delta_\ell(M)$. By 6.3.4 and 6.3.7(i) it follows that for all but finitely many primes ℓ the maps in the left and right column are surjective. It follows then by diagram chasing that the map ρ is also surjective. □

The global image

6.3.9 Lemma. *The group H_ℓ is isomorphic to $\mathbb{Z}_\ell^\times \ltimes \mathbb{Z}_\ell^q$.*

Proof. Fix a section $s\colon \mathrm{T}_\ell Y \to \mathrm{T}_\ell M$ of the projection map π which extends the canonical embedding $\kappa\colon \mathrm{T}_\ell N \to \mathrm{T}_\ell M$. Then the map

$$\mathrm{Aut}(\mathrm{T}_\ell M) \to C_\ell \ltimes \mathrm{Hom}(\mathrm{T}_\ell Y, \mathrm{T}_\ell \mathbb{G}_m), \sigma \mapsto (\pi^*\sigma, (\sigma - 1)s)$$

is a group isomorphism. An element (α, a) lies in the image of H_ℓ if and only if $N \subseteq \ker a$, or in other words, if and only if $a \in U_\ell$. Hence $H_\ell \simeq C_\ell \ltimes U_\ell \simeq \mathbb{Z}_\ell^\times \ltimes \mathbb{Z}_\ell^q$. □

Let n be a positive integer. Let $E_n = K(M[n])$ denote the smallest field extension of K over which all points in $M[n]$ are defined. We will write G_n for the Galois group of the extension E_n/K. Then the previous lemma implies the following corollary:

6.3.10 Corollary. *For all but finitely many primes ℓ and for all positive integers n we have*

$$G_{\ell^n} \simeq (\mathbb{Z}/\ell^n)^\times \ltimes (\mathbb{Z}/\ell^n)^q.$$

Proof. Since G_{ℓ^n} is precisely the image of Γ_K under the composition

$$\Gamma_K \xrightarrow{\rho_\ell} \mathrm{Aut}(\mathrm{T}_\ell M) \to \mathrm{Aut}(M[\ell^n])$$

it follows that G_{ℓ^n} is isomorphic to the quotient of $\rho_\ell(\Gamma_K)$ by the subgroup of elements which leave the submodule $\ell^n \mathrm{T}_\ell M$ invariant.

Let s be as in Lemma 6.3.9 and consider again the isomorphism $\mathrm{Aut}(\mathrm{T}_\ell M) \simeq C_\ell \ltimes \mathrm{T}_\ell G$ induced by it. An element (α, a) acts on $\mathrm{T}_\ell M \simeq \mathrm{T}_\ell \mathbb{G}_m \oplus \mathrm{T}_\ell Y$ by the formula

$$(\alpha, a)\begin{pmatrix} g \\ y \end{pmatrix} = \begin{pmatrix} \alpha g + ay \\ y \end{pmatrix}.$$

Hence the subgroup that leaves $\ell^n \mathrm{T}_\ell M \simeq \ell^n \mathrm{T}_\ell \mathbb{G}_m \oplus \ell^n \mathrm{T}_\ell Y$ invariant is the subgroup of elements $\{(\alpha, a)\colon \alpha \in 1 + \ell^n \mathbb{Z}_\ell,\ a \in \ell^n \mathrm{T}_\ell G\}$. On the other hand, by Proposition 6.3.8, for all but finitely many ℓ, $\rho_\ell(\Gamma_K) = H_\ell$. Hence $G_\ell \cong H_\ell/Q_{\ell^n}$, where Q_{ℓ^n} is the subgroup

$$Q_{\ell^n} = (1 + \ell^n \mathbb{Z}_\ell) \ltimes \ell^n U_\ell,$$

which implies the claim. □

Let S be a fixed finite set of prime numbers satisfying the following conditions:

S1. $2 \in S$;

S2. the map $\rho_{\bar{S}}(\mathbb{G}_m)\colon \Gamma_K \to \prod_{\ell \notin S} C_\ell$ is surjective;

S3. For any $\ell \notin S$ the image of $\rho_\ell(M)$ is equal to H_ℓ.

Due to 6.3.5 and 6.3.8 such a set S exists. We will say that an integer m is *good* if it is coprime to all primes in S.

6.3.11 Lemma. *Let m be a good positive integer. The maximal abelian quotient of the group $(\mathbb{Z}/m)^\times \ltimes (\mathbb{Z}/m)^q$ is $(\mathbb{Z}/m)^\times$.*

Proof. Let G denote the group $(\mathbb{Z}/m)^\times \ltimes (\mathbb{Z}/m)^q$ and let U denote the subgroup $\{(1,a) \in G \colon a \in (\mathbb{Z}/m)^q\}$. We need to show that the U is equal to the commutator $[G,G]$ of G.

The group operation in G is given by the formula

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + \alpha b)$$

and the inverse is

$$(\alpha, a)^{-1} = (\alpha^{-1}, -\alpha^{-1}a).$$

Hence if $x = (\alpha, a)$ and $y = (\beta, b)$ are two elements of G, we have

$$[x, y] = xyx^{-1}y^{-1} = (1, (\alpha - 1)b - (\beta - 1)a)$$

which is an element of U. Conversely if $(1, b) \in U$ then we have

$$(1, b) = [(2, 0), (1, b)],$$

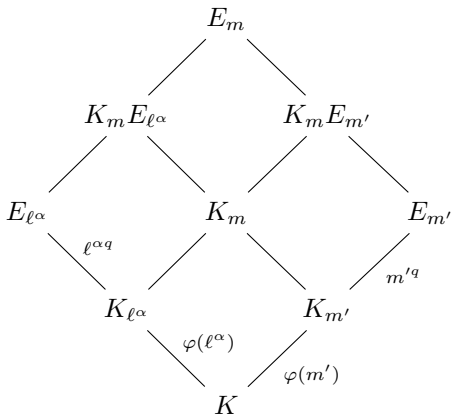
hence $(1, b) \in [G, G]$. (Note that 2 is invertible in $\mathbb{Z}/m$ since by **S1** m is odd.) It follows that $U = [G, G]$ which implies the claim. □

6.3.12 Proposition. *Let m be a good integer, $m = \ell_1^{\alpha_1} \dots \ell_s^{\alpha_s}$. Then*

$$G_m \simeq \prod_{i=1}^{s} G_{\ell_i^{\alpha_i}} \simeq (\mathbb{Z}/m)^\times \ltimes (\mathbb{Z}/m)^q$$

Proof. We are going to prove this statement by induction on the number of distinct prime factors of m. If m is a prime power $m = \ell^\alpha$, then the proposition was proved in 6.3.10, since by condition **S3** the image of $\rho_\ell(M)$ is the whole group H_ℓ.

Let now $m = \ell^\alpha m'$, for some good prime ℓ and some good integer m' which is coprime to ℓ. Assume that $G_{m'} \cong (\mathbb{Z}/m')^\times \ltimes (\mathbb{Z}/m')^q$. It is sufficient to show that $|G_m| = [E_m : K] = \varphi(m)m^q$, where φ denotes the Euler function. We have the following diagram of field extensions:



We have $K_m \cap E_{m'} = K_{m'}$. Indeed, let $X = K_m \cap E_{m'}$ Since X is a subfield of K_m it is an abelian extension of K. But by 6.3.11 and our inductive assumption it follows that the maximal abelian sub-extension of $E_{m'}$ is $K_{m'}$. Hence $X = K_{m'}$. It follows that $[K_m E_{m'} : K_m] = [E_{m'} : K_{m'}] = m'^q$. By an analogous argument we also have $[K_m E_{\ell^\alpha} : K_m] = [E_{\ell^\alpha} : K_{\ell^\alpha}] = \ell^{\alpha q}$.

By **S2** we have that $[K_m : K] = [K_{\ell^\alpha} : K][K_{m'} : K] = \varphi(m)$. Also, since the degrees of the extensions $K_m E_{\ell^\alpha}/K_m$ and $K_m E_{m'}/K_m$ are coprime, and since E_m is the compositum of $K_m E_{\ell^\alpha}$ and $K_m E_{m'}$, it follows that $[E_m : K_m] = [K_m E_{\ell^\alpha} : K_m][K_m E_{m'} : K_m] = m^q$. Hence $[E_m : K] = [E_m : K_m][K_m : K] = \varphi(m)m^q$, which concludes the proof. □

Taking limits we arrive at the following corollary:

6.3.13 Corollary. *There exists a finite set of primes S such that the image of the Galois representation $\rho_{\bar{S}}(M)$ is the product $\prod_{\ell \notin S} H_\ell$. In particular for any finite set of primes P which does not contain any primes in S, the image of the Galois group Γ_K in $\prod_{\ell \in P} \mathrm{Aut}(T_\ell M)$ is the group $\prod_{\ell \in P} H_\ell$.*

6.4 Proof of the main theorem

As a first step we will do the following simplification

6.4.1 Lemma. *In order to prove Theorem 6.1.6 it is sufficient to prove it when the algebraic dependence I is principal, i.e. $I = (f)$ for some homogenous polynomial f.*

Proof. Let $I = (f_1, \ldots, f_k)$. It is a simple corollary of the definitions that I is exceptional if and only if f_i are exceptional for all $i = 1 \ldots k$. Similarly, (the ℓ-part of) $M_{\mathfrak{p}}$ satisfies I if and only if it satisfies f_i for $i = 1 \ldots k$. It follows that the general cases of 6.1.6(i) and 6.1.6(ii) follow from the special case where I is principal.

Next we show 6.1.6(iv). Indeed, if I is generic then there must exist i such that f_i is generic. But the set of primes $\mathfrak{p}$ for which $M_{\mathfrak{p}}$ satisfies I is a subset of the set of primes $\mathfrak{p}$ for which $M_{\mathfrak{p}}$ satisfies (f_i). It follows that if the latter set has zero density, then the former must have zero density as well.

Finally we show 6.1.6(iii). Let D_ℓ^I denote the density of primes of good reduction $\mathfrak{p}$ for which the ℓ-part of $M_{\mathfrak{p}}$ satisfies I (it follows from 4.2.12 that this density exists). We are going to prove the statement by induction on the number of generators of I. If I has one generator then it is principal and the claim is trivial. Let $I = I' + (f)$. If I is generic then either I' of (f) must also be generic. Hence we have

$$D_\ell^I \leq \min\{D_\ell^{I'}, D_\ell^f\} = 1 - \Theta(\ell^{-1})$$

by the inductive hypothesis. On the other hand we have the inequality

$$D_\ell^I + 1 \geq D_\ell^{I'} + D_\ell^f = 2 - \Theta(\ell^{-1})$$

The two inequalities imply the desired asymptotic $D_\ell^I = 1 - \Theta(\ell^{-1})$. □

As a consequence of the previous lemma we will assume from now on that I is principal and we will fix a generator $f \in I$. We set d to denote the degree of f. We also fix a basis $\{y_1, \ldots, y_n\}$ of Y, which allows us to identify f with a homogenous polynomial in $\mathbb{Z}[y_1, \ldots, y_n]$.

Let ℓ be a prime number. We want to associate to the polynomial f a set $A_\ell^f \subseteq \mathrm{Aut}(\mathrm{T}_\ell M)$. We proceed as follows. Let $s\colon \mathrm{T}_\ell Y \to \mathrm{T}_\ell M$ be a section of the standard projection map $\pi\colon \mathrm{T}_\ell M \to \mathrm{T}_\ell Y$. Let $\tau \in \mathrm{T}_\ell \mathbb{G}_m$ be a fixed basis element. The section s, together with the bases τ and $y_1, \ldots, y_n$, allow us to identify $\mathrm{Aut}(\mathrm{T}_\ell M)$ with the set of matrices

$$\mathrm{Aut}(T_\ell M) = \left\{ \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} : \alpha \in \mathbb{Z}_\ell^\times,\ b \in \mathbb{Z}_\ell^n \right\},$$

where I_n is the identity matrix. Then we let A_ℓ^f denote the set

$$A_\ell^f := \left\{ \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} : |f(b)|_\ell \leq |\alpha - 1|_\ell \|b\|_\ell^{\deg f - 1} \right\},$$

where $\|b\|_\ell$ denotes the maximum norm of the vector b, i.e. if $b = (b_1, \ldots, b_n)$, then $\|b\|_\ell := \max\{|b_1|_\ell, \ldots, |b_n|_\ell\}$.

6.4.2 Lemma. *The set A_ℓ^f is the closure of the pre-image of $Z(I, \mathrm{B}_\ell G)$ under the Pink map $\varepsilon_{\mathrm{T}_\ell M}$.*

Proof. After fixing the bases τ and $\{y_1, \ldots, y_n\}$ the vector space $\mathrm{V}_\ell G$ is canonically identified with $\mathbb{Q}_\ell^n$. Then it is easy to see from the construction in Section 3.4 that the Pink map is the composition of the map

$$\varepsilon'\colon \mathrm{Aut}(\mathrm{T}_\ell M) \to \mathrm{V}_\ell G, \quad \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} \mapsto (\alpha - 1)^{-1} b$$

with the canonical projection $\mathrm{V}_\ell G \to \mathrm{B}_\ell G$. The pre-image of the set $Z(I, \mathrm{B}_\ell G)$ under the latter is the set

$$Z^*(I, \mathrm{V}_\ell G) = \{x\colon |f(x)|_\ell \leq \|x\|_\ell^{d-1}\}$$

(as follows from Lemma 6.1.4(iii)). Substituting $(\alpha - 1)^{-1} b$ for x and using the fact that f is homogenous of degree d, it follows that the pre-image of $Z(I, \mathrm{B}_\ell G)$ under the Pink map is precisely the set

$$\left\{ \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} : \alpha \neq 1 \text{ and } |f(b)|_\ell \leq |\alpha - 1|_\ell \|b\|_\ell^{d-1} \right\}.$$

Clearly, A_ℓ^f is the closure of this set. □

Notice that this lemma implies that the set A_ℓ^f does not depend on the choice of basis.

6.4.3 Lemma. *Let ℓ be a fixed prime number. The following properties are equivalent:*

(i) $H_\ell \subseteq A_\ell^f$;

(ii) The restriction of f on U_ℓ is zero;

(iii) The algebraic dependence f is exceptional for M.

Proof. As in Lemma 6.3.9 we can choose a section $s : \mathrm{T}_\ell Y \to \mathrm{T}_\ell M$ such that the subgroup H_ℓ becomes isomorphic to the group of matrices

$$\left\{ \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} : b \in U_\ell \right\}.$$

Then clearly if $f(b) = 0$ for all $b \in U_\ell$ we have that $0 = |f(b)|_\ell \leq |\alpha - 1|_\ell \|b\|_\ell^{d-1}$ for any $\alpha \in C_\ell$, hence (ii) implies (i). Conversely, when we consider U_ℓ as a subgroup of H_ℓ the condition $H_\ell \subseteq A_\ell^f$ implies that for any $b \in U_\ell$ we have $|f(b)|_\ell \leq |1 - 1|_\ell \|b\|_\ell^{d-1} = 0$. Hence (i) implies (ii).

To show that (ii) and (iii) are equivalent notice that U_ℓ is precisely the set of common zeros for the linear dependence $L(\ker u)$ in $\mathrm{T}_\ell G$, or in other words, that $U_\ell = Z(L(\ker u), \mathrm{T}_\ell G)$. Hence the restriction of f on U_ℓ is zero if and only if $Z(f, \mathrm{T}_\ell G) \supseteq Z(L(\ker u), \mathrm{T}_\ell G)$. Then we are reduced to the following problem:

6.4.4 Claim. *Let $f \in \mathbb{Q}_\ell[x_1, \ldots x_n]$ be a homogenous polynomial and let $L \subseteq \mathbb{Q}_\ell[x_1, \ldots x_n]$ be an ideal generated by linear polynomials. Let V_f and V_L be the affine $\mathbb{Q}_\ell$-schemes induced by f and L. Then $f \in L$ if and only if $V_f(\mathbb{Z}_\ell) \supseteq V_L(\mathbb{Z}_\ell)$.*

Proof. One direction of the claim is clear. To prove the other direction, we proceed by induction on n. If $n = 1$ then L is one of the ideals (0) or (x_1). In both cases the claim follows easily.

Next we prove the statement for n, having assumed that it holds for $n - 1$. Note that $V_L(\mathbb{Z}_\ell) \subseteq V_f(\mathbb{Z}_\ell)$ if and only if $V_L(\mathbb{Q}_\ell) \subseteq V_f(\mathbb{Q}_\ell)$. If $L = (0)$ then f vanishes on every point in $\mathbb{Q}_\ell^n$, which implies $f = 0$. Otherwise, let $L = (g_1, \ldots, g_k)$. Without loss of generality we can assume that $g_1 = x_n - g'(x_1, \ldots, x_{n-1})$ for some linear form g', and that $g_2, \ldots, g_k \in \mathbb{Q}_\ell[x_1, \ldots, x_{n-1}]$. (One can always find such generators of L using Gauss elimination, and possibly relabeling of the variables.) Let $L' = (g_2, \ldots, g_k)$ and let $f'(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, g'(x_1, \ldots, x_{n-1}))$. Notice that every point in $V_{L'}(\mathbb{Q}_\ell)$ lies also in $V_{f'}(\mathbb{Q}_\ell)$. Hence by the inductive hypothesis it follows that $f' \in L' \subseteq L$. But if we write

$$f = \sum_i f_i x_n^i$$

for some polynomials $f_i \in \mathbb{Q}_\ell[x_1, \ldots x_{n-1}]$ we see that

$$f - f' = \sum_i f_i (x_n^i - g'^i)$$

is divisible by g_1. Hence $f \in L$. □

In our case our claim implies that the restriction of f on U_ℓ is zero if and only if $f \in L(\ker u) \otimes \mathbb{Q}_\ell$. Since f has integer coefficients the last condition is equivalent to saying that f is exceptional for M. □

Proof of Theorem 6.1.6(i,ii). Let f be an exceptional algebraic dependence for M. Fix an arbitrary prime number ℓ. Lemma 6.4.3 then implies that $H_\ell \subseteq A_\ell^f$. By Proposition 6.3.8 we have that the image of the Galois representation $\rho_\ell(M)$

is contained in H_ℓ and by Lemma 6.4.2 it follows that after applying the Pink map, the image of every Frobenius element corresponding to an unramified prime will lie in $Z(f, \mathrm{B}_\ell G)$. This implies that for every prime of good reduction $\mathfrak{p}$, the ℓ-part of $M_\mathfrak{p}$ satisfies f. Since this claim holds for all prime numbers ℓ, it follows that $M_\mathfrak{p}$ satisfies f for every prime ideal $\mathfrak{p}$ of good reduction. This proves Theorem 6.1.6(ii) and one implication of Theorem 6.1.6(i).

Let S be a finite set of prime numbers such that for every prime ℓ outside of S the image of $\rho_\ell(M)$ is equal to H_ℓ. By Proposition 6.3.8 such a set exists. Let ℓ be a fixed prime lying outside of S. If the ℓ-part of $M_\mathfrak{p}$ satisfies f for every prime of good reduction, then every Frobenius element in the image of $\rho_\ell(M)$ must lie in A_ℓ^f. By the Chebotarev density theorem (or more precisely by the Frobenius density theorem) and by our assumption it follows that $H_\ell \subseteq A_\ell^f$. Then Lemma 6.4.3 implies that the algebraic dependence f is exceptional for M. This proves the second part of Theorem 6.1.6(i). □

Let μ_ℓ denote the probability Haar measure on H_ℓ and let $D_\ell^f := \mu(A_\ell^f \cap H_\ell)$. For all but finitely many prime numbers ℓ, D_ℓ^f is precisely the density of the primes $\mathfrak{p}$ for which the ℓ-part of $M_\mathfrak{p}$ satisfies f. The proof of rest of the theorem is based on the following key estimate:

6.4.5 Proposition. *If $H_\ell \subseteq A_\ell^f$ then $D_f = 1$. Otherwise,*

$$D_f = 1 - \frac{1}{\ell - 1}\left(1 + O(\ell^{-1})\right).$$

(Here the constant in the O-term does not depend on ℓ.)

The first claim of the proposition is trivial. So from now on we will assume that $H_\ell \not\subseteq A_\ell^f$.

Let χ_f denote the characteristic function of A_ℓ^f. Then

$$D_f = \int_{H_\ell} \chi_f(h)\, dh$$

We will fix an isomorphism $H_\ell \simeq C_\ell \ltimes U_\ell$ and will simply identify H_ℓ with the corresponding semidirect product. Consider the map

$$\psi\colon C_\ell \times U_\ell \to C_\ell \ltimes U_\ell,\ (\alpha, a) \mapsto (\alpha, a)$$

This map is not a group homomorphism. However, if we introduce the probability Haar measures on U_ℓ, C_ℓ and their product $U_\ell \times C_\ell$ it turns out that ψ is an isometry. More precisely:

6.4.6 Lemma. *Let $f \in C_c(H_\ell)$. Then if μ' denotes the probability Haar measure on $C_\ell \times U_\ell$, we have*

$$\int_{H_\ell} f\, d\mu = \int_{H_\ell} \psi^*(f)\, d\mu'.$$

Proof. To avoid confusion we will denote the group operation in H_ℓ by "$\star$" and the one in $C_\ell \times U_\ell$ by "$*$". Let $g \in C_c(C_\ell)$ be the function

$$g(\alpha) = \int_{U_\ell} f((1, u) \star (\alpha, 0))\, du$$

Since $(1,u)\star(\alpha,0)=(1,u)*(\alpha,0)$ we also have

$$g(\alpha)=\int_{U_\ell}\psi^*(f)((1,u)*(\alpha,0))\,du.$$

Then

$$\int_{H_\ell} f\,d\mu=\int_{C_\ell} g(\alpha)\,d\alpha=\int_{C_\ell\times U_\ell}\psi^*(f)\,d\mu',$$

where we have used [Fol95, Theorem 2.49] to relate an integral over a locally compact group to an integral over a quotient group. □

It follows from the previous lemma that

$$\int_{H_\ell}\chi\,d\mu=\int_{U_\ell\times C_\ell}\psi^*(\chi)\,d\mu'=\int_{U_\ell} g\,du, \tag{6.5}$$

where

$$g(u)=\int_{C_\ell}\chi((\alpha,u))\,d\alpha=\mu_{C_\ell}\left(\{\alpha\in C_\ell\colon |f(u)|_\ell\le|\alpha-1|_\ell\|u\|^{d-1}\}\right). \tag{6.6}$$

Recall that $C_\ell=\mathbb{Z}_\ell^\times$.

6.4.7 Lemma. *We have*

$$\mu\left(\{\alpha\in\mathbb{Z}_\ell^\times\colon|\alpha-1|_\ell\ge\ell^{-n}\}\right)=1-\frac{1}{\ell-1}\ell^{-n}.$$

Proof. Let $F_n:=\{\alpha\in\mathbb{Z}_\ell^\times\colon|\alpha-1|_\ell\le\ell^{-1}\}$. One easily sees that $\mu(F_0)=1$ and $\mu(F_n)=\frac{1}{\ell-1}\ell^{1-n}$ for $n\ge1$. Then

$$\mu\left(\{\alpha\in\mathbb{Z}_\ell^\times\colon|\alpha-1|_\ell\ge\ell^{-n}\}\right)=1-\mu(F_{n+1})=1-\frac{1}{\ell-1}\ell^{-n}.$$

□

Applying this lemma to (6.6) we get

$$D_f=\int_{U_\ell} g(u)\,du=1-\frac{1}{\ell-1}\int_{U_\ell}\frac{|f(u)|_\ell}{\|u\|_\ell^{d-1}}\,du \tag{6.7}$$

6.4.8 Lemma. *We have*

$$\int_{U_\ell}\frac{|f(u)|}{\|u\|_\ell^{d-1}}\,du=\left(1+O(\ell^{-q-1})\right)\int_{U_\ell}|f(u)|_\ell\,du.$$

Proof. Denote by I the integral on the left-hand side in the expression above. We have

$$I=\int_{\ell U_\ell}\frac{|f(u)|}{\|u\|_\ell^{d-1}}\,du+\int_{U_\ell\setminus\ell U_\ell}\frac{|f(u)|}{\|u\|_\ell^{d-1}}\,du. \tag{6.8}$$

After changing variables $u\mapsto\ell u$ and using the fact that f is homogenous of degree d we get for the first integral the relation

$$\int_{\ell U_\ell}\frac{|f(u)|}{\|u\|_\ell^{d-1}}\,du=\ell^{q+1}I \tag{6.9}$$

For the second integral we have

$$\int_{U_\ell \setminus \ell U_\ell} \frac{|f(u)|}{\|u\|_\ell^{d-1}}\, du = \int_{U_\ell \setminus \ell U_\ell} |f(u)|_\ell \, du.$$

Again, using the fact that f is homogenous, we get

$$\int_{\ell U_\ell} |f(u)|_\ell \, du = \ell^{-q-d} \int_{U_\ell} |f(u)|_\ell \, du$$

which allows us to conclude that

$$\int_{U_\ell \setminus \ell U_\ell} \frac{|f(u)|}{\|u\|_\ell^{d-1}}\, du = (1 - \ell^{-q-d}) \int_{U_\ell} |f(u)|_\ell \, du. \tag{6.10}$$

Combining (6.8), (6.9) and (6.10) and solving for I we get

$$I = \frac{1 - \ell^{-q-d}}{1 - \ell^{-q-1}} \int_{U_\ell} |f(u)|_\ell \, du.$$

Since $\frac{1-\ell^{-q-d}}{1-\ell^{-q-1}} = 1 + O(\ell^{-q-1})$ the claim follows. □

Applying this lemma to (6.7) we get the estimate

$$D_f = 1 - \frac{1}{\ell - 1} \left(1 + O(\ell^{-q-d})\right) \int_{U_\ell} |f(u)|_\ell \, du \tag{6.11}$$

6.4.9 Lemma. *Let $f \in \mathbb{F}_\ell[x_1, \ldots, x_n]$ be a non-zero polynomial of total degree d. Then f has at most $nd\ell^{n-1}$ zeros in $\mathbb{F}_\ell^n$.*

Proof. We will prove this statement by induction on n. If $n = 1$ the statement is standard. Assume that the statement is true for n. Let $f \in \mathbb{F}_\ell[x_1, \ldots, x_{n+1}]$ be a non-zero polynomial. Write

$$f = \sum_{i=0}^{d_{n+1}} g_i x_{n+1}^i$$

for some polynomials $g_i \in \mathbb{Z}[x_1, \ldots, x_n]$. Since at least one of the polynomials g_i is non-zero we can conclude by the inductive hypothesis that the set of common zeros of $g_0, \ldots, g_{d_{n+1}}$ has size at most $nd\ell^{n-1}$. Each of those zeros induces ℓ zeros of f. On the other hand, each element of $\mathbb{F}_\ell^n$ which is not a common zero of the polynomials g_i induces at most $d_{n+1} \leq d$ zeros of f. Hence the total number of zeros is bounded from above by

$$(nd\ell^{n-1})\ell + \ell^n d = (n+1)d\ell^n.$$ □

Notice that for all but finitely many primes ℓ the restriction of f to U_ℓ has non-zero reduction modulo ℓ. Indeed we can assume, without loss of generality that $N = \ker u$ is contained in the submodule generated by the basis elements $\{y_{q+1}, \ldots, y_n\}$ (otherwise just change the basis). This implies that for all but finitely many ℓ the images of $\{y_1, \ldots, y_q\}$ in Q form a basis of $\mathrm{T}_\ell Q$. Then the restriction of f to U_ℓ is given by the polynomial $f(y_1, \ldots, y_q, 0, \ldots, 0)$. Since

this is a non-zero polynomial with integer coefficients it follows that for all but finitely many ℓ its reduction modulo ℓ is not zero.

Therefore, if N_ℓ denotes the number of zeros of the restriction of f to U_ℓ reduced modulo ℓ, we can apply Lemma 6.4.9 to conclude that

$$N_\ell = O(\ell^{q-1}) \tag{6.12}$$

(Since there are only finitely many primes for which Lemma 6.4.9 does not apply we can we can include them in the above estimate by increasing the implicit constant. This constant still depends only on M and f.)

Let $S_\ell \subseteq U_\ell$ denote the set $S_\ell = \{u \in U_\ell \colon |f(u)|_\ell < 1\}$. Clearly $\mu(S_\ell) = \ell^{-q} N_\ell = O(\ell^{-1})$. Then equation (6.11) gives us

$$\begin{aligned} D_f &= 1 - \frac{1}{\ell - 1}\left(1 + O(\ell^{-\ell-d})\right)\left(\mu(U_\ell \setminus S_\ell) + \int_{S_\ell} |f(u)|_\ell \, du\right) \\ &= 1 - \frac{1}{\ell - 1}\left(1 + O(\ell^{-\ell-d})\right)\left(1 + O(\ell^{-1}) + O(\ell^{-1})\right) \\ &= 1 - \frac{1}{\ell - 1}\left(1 + O(\ell^{-1})\right). \end{aligned}$$

This completes the proof of Proposition 6.4.5. □

Proof of Theorem 6.1.6(iii). If f is generic then by Lemma 6.4.3 it follows that for every ℓ we have $H_\ell \not\subseteq A_\ell^f$. Hence by Proposition 6.4.5 we have

$$D_\ell^f = 1 - \frac{1}{\ell - 1}\left(1 + O(\ell^{-1})\right) = 1 - \Theta(\ell^{-1})$$

For all but finitely many primes ℓ the image of the Galois representation $\rho_\ell(M)$ is equal to H_ℓ. Hence for all but finitely many primes ℓ the density of prime ideals $\mathfrak{p}$ of good reduction for which the ℓ-part of $M_\mathfrak{p}$ satisfies f is equal to $D_\ell^f = 1 - \Theta(\ell^{-1})$. To include all primes ℓ one just needs to modify the implicit constants. □

Proof of Theorem 6.1.6(iv). By Corollary 6.3.13 there exists a finite set of prime numbers S such that for any finite set of primes P outside of S the image of the Galois group Γ_K in $\prod_{\ell \in P} \mathrm{Aut}(\mathrm{T}_\ell M)$ is the group $H_P := \prod_{\ell \in P} H_\ell$.

Let P be such a finite set of primes and let ρ_P denote the representation $\rho_P \colon \Gamma_K \to H_P$ induced by M.

Let $\mathfrak{p}$ be a prime ideal of good reduction for M and assume furthermore that it is coprime to all elements in P. If $M_\mathfrak{p}$ satisfies f then, by definition, the ℓ-part of $M_\mathfrak{p}$ satisfies f for all prime numbers $\ell \in P$. Equivalently, for every $\ell \in P$ the image of the Frobenius $\phi_\mathfrak{p}$ at $\mathfrak{p}$ under the Pink map $\varepsilon_{\mathrm{T}_\ell M}$ is contained in $Z(f, \mathrm{B}_\ell G)$. By Lemma 6.4.2 it follows that the Frobenius lies in $\prod_{\ell \in P} A_\ell^f \cap \rho_P(\Gamma_K) = \prod_{\ell \in P}(A_\ell^f \cap H_\ell)$. We can therefore apply Chebotarev's density theorem 4.2.10 to conclude that the density of all prime ideals $\mathfrak{p}$ such that $M_\mathfrak{p}$ satisfies f, if it exists, is bounded from above by

$$\mu\Big(\prod_{\ell \in P} A_\ell^f \cap H_\ell\Big) = \prod_{\ell \in P} D_\ell^f.$$

Since f is generic, Theorem 6.1.6(iii) implies that

$$\prod_{\ell \in P} D_\ell^f \leq \prod_{\ell \in P} \left(1 - \frac{c}{\ell}\right)$$

for some positive constant c which depends on M and f. But since

$$\prod_{\ell \text{ prime}} \left(1 - \frac{c}{\ell}\right) = 0$$

(which one can show by taking logarithms for example) it follows that as we vary P we can get an arbitrarily small upper bound for the density of primes $\mathfrak{p}$ for which $M_\mathfrak{p}$ satisfies f. It therefore follows that this density exists and is equal to 0. □

6.5 Relations to transcendence theory

The local image of the Kummer map

Let K be a finite $\mathbb{Q}_p$-extension and let $M = [Y \xrightarrow{u} \mathbb{G}_m]$ be a trivial K-1-motive of good reduction. We would like to determine the image of the Kummer map $\delta_p(M)$. Denote the ring of integers of K by R, the maximal ideal by $\mathfrak{m}$ and the residue field by k. Furthermore, we fix a uniformizing element $\pi \in R$.

Since M is of good reduction it follows that $u(Y) \subseteq R^\times$. The map u induces maps

$$u_n \colon Y/p^n \to R^\times/p^n$$

for every $n \geq 1$. The group $R^\times$ has a canonical decomposition as a product $R^\times \cong U \times k^\times$, where U is the subgroup of all points which reduce to the identity modulo $\mathfrak{m}$. Since the order of $k^\times$ is coprime to p it follows that $R/p^n \cong U/p^n$ for all $n \geq 1$. U is a pro-p group hence

$$\varprojlim_n U/p^n \cong U$$

Therefore after taking projective limits we get a map

$$u' \colon \mathrm{T}_p Y \to U$$

This map is a continuous homomorphism of $\mathbb{Z}_\ell$-modules.

Let $t_{\mathbb{G}_m}$ denote the tangent space of $\mathbb{G}_m$. One has a well-defined logarithm map

$$\log \colon \mathbb{G}_m(R) \to t_{\mathbb{G}_m}(K)$$

which we can extend to the whole group $\mathbb{G}_m(K)$ by fixing $\log \pi = 0$. This map is defined via the usual analytic series

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^n}{n}$$

whenever the p-adic absolute value of x is sufficiently small, and is extended to all points in $R^\times$ by homomorphism. Its kernel in $R^\times$ is precisely the torsion subgroup.

Let us then define the map $L \colon T_p Y \to t_{\mathbb{G}_m}(K)$, $L = \log \circ u'$. Then we have

6.5.1 Proposition. *The image of the Kummer map $\delta_p(M)$ in the Tate module $\mathrm{T}_pG = \mathrm{Hom}(\mathrm{T}_pY, \mathrm{T}_p\mathbb{G}_m)$ is a finite index subgroup of the submodule*

$$\mathrm{Hom}(\mathrm{T}_pY/\ker L, \mathrm{T}_p\mathbb{G}_m).$$

Proof. Let T denote the module $\mathrm{Hom}(\mathrm{T}_pY, \mathrm{T}_p\mathbb{G}_m)$, and let $\widetilde{M}$ be the image of M in $H^1(\Gamma_K, T)$ under the Abel-Jacobi map α_p. Recall that the Abel-Jacobi map is a limit of maps

$$\alpha_{[n]}\colon \mathrm{Mot}_K(Y, \mathbb{G}_m) \to H^1(\Gamma_K, T/p^n)$$

It follows from the definitions that a 1-motive $X = [Y \xrightarrow{v} \mathbb{G}_m]$ lies in the kernel of $\alpha_{[n]}$ if and only if the induced map $u_n\colon Y/p^n \to K^\times/p^n$ is trivial.

Let $\mathcal{O}$ denote the ring of Γ_K-equivariant endomorphisms of T. Since Y is a trivial Γ_K-module, $T \otimes \mathbb{Q}_\ell$ can be represented as a sum of 1-dimensional Γ_K-representations, which implies that it is semi-simple. Let Q be the image of the representation

$$\rho_p(\hat{Y} \otimes \mathbb{G}_m)\colon \Gamma_K \to \mathrm{End}(T).$$

Since the image of the cyclotomic character $\Gamma_K \to \mathbb{Z}_p^\times$ is an open subgroup of $\mathbb{Z}_p^\times$ one can show, using arguments similar to those in Lemma 5.2.6, that $H^1(Q, T\otimes\mathbb{Q}_\ell) = 0$. It follows that the conditions of Corollary 5.1.2 are satisfied, hence we can conclude that the image of $\delta_\ell(M)$ is a finite index subgroup of the $\mathbb{Z}_p$-submodule $Z(\mathrm{Ann}_{\mathcal{O}}\widetilde{M}, T)$. To conclude the proof we have to show the equality

$$Z(\mathrm{Ann}_{\mathcal{O}}\widetilde{M}, T) = \mathrm{Hom}(\mathrm{T}_pY/\ker L, \mathrm{T}_p\mathbb{G}_m). \tag{6.13}$$

Let N_n denote the kernel of the map u_n, and let N be the inverse limit of N_n. This is also the kernel of the map u', and since the kernel of log is finite, it follows that N is a finite index subgroup of $\ker L$. This implies

$$\mathrm{Hom}(\mathrm{T}_pY/N, \mathrm{T}_p\mathbb{G}_m) = \mathrm{Hom}(\mathrm{T}_pY/\ker L, \mathrm{T}_p\mathbb{G}_m) \tag{6.14}$$

Since Γ_K acts trivially on Y it is easy to show that $\mathcal{O} \cong \mathrm{End}_K(\hat{Y} \otimes \mathbb{G}_m) \otimes \mathbb{Z}_p \cong \mathrm{End}_K(\hat{Y}) \otimes \mathbb{Z}_p$. The latter ring is non-canonically isomorphic to the ring of $m \times m$-matrices with coefficients in $\mathbb{Z}_p$, where m is the rank of Y.

Let $\phi \in \mathrm{Ann}_{\mathcal{O}}\widetilde{M}$. Let $\phi_n \in \mathrm{End}_K(\hat{Y})$ be a sequence of homomorphisms such that $\phi \equiv \phi_n \bmod p^n$. $\phi\widetilde{M} = 0$ if and only if $\alpha_{[n]}(\phi_n M) = 0$ for all n. This holds if and only if $u \circ \phi_n^t$ is trivial, where ϕ^t denotes the homomorphism dual to ϕ. The last statement is equivalent to saying that the image of ϕ_n^t lies in N_n.

Let $A_n = \{\phi \in \mathrm{End}(\hat{Y})\colon \mathrm{Im}\,\phi \subseteq N_n\}/p^n$. The arguments above imply that $\mathrm{Ann}_{\mathcal{O}}\widetilde{M} = \varprojlim_n A_n$. The sets A_n are left ideals of the rings $\mathcal{O}/p^n$, which act on T/p^n. One can show that

$$Z(\mathrm{Ann}_{\mathcal{O}}\widetilde{M}, T) = \varprojlim_n Z(A_n, T/p^n)$$

Using arguments similar to the ones in Lemma 6.3.6 it is easy to show that $Z(A_n, T/p^n) = \mathrm{Hom}_{\mathbb{Z}/p^n}(Y/N_n, \mathrm{T}_p\mathbb{G}_m/p^n)$. Taking limits on both sides of this equation and using (6.14), one derives the equality in (6.13). □

Conjectures

We restrict ourselves to the case of trivial 1-motives over $\mathbb{Q}$. Let $M = [Y \xrightarrow{u} \mathbb{G}_m]$ be such a trivial $\mathbb{Q}$-1-motive and let p be a fixed prime of good reduction. Further, we fix a basis $y_1, \dots, y_n$ of Y. Let $P_i := u(y_i)$ for $i = 1, \dots, n$. Let $f \in \mathbb{Z}[y_1, \dots, y_n]$ be a fixed homogenous polynomial. Let $\log_p \colon \mathbb{Z}_p^\times \to \mathbb{Z}_p$ denote the p-adic logarithm map. Note that since p is a prime of good reduction for M, it follows that $u(Y)$ is contained in $\mathbb{Z}_p^\times$. Then we have the following conjecture:

6.5.2 Conjecture. *Suppose that $f(\log_p P_1, \dots, \log_p P_n) = 0$. Then the p-adic numbers $\log_p P_i, \dots \log_p P_i$ are linearly dependent over $\mathbb{Q}$.*

This is a standard conjecture from p-adic transcendence theory. It is a special case of the p-adic version of Schanuel's conjecture. We will show that this conjecture can be reinterpreted as a conjecture about the p-adic Galois representation associated to the 1-motive M. A related result due to Bertolin [Ber02] (see also [And04, §23]) shows that in the complex case Schanuel's conjecture is equivalent to a generalization of Grothendieck's period conjecture applied to 1-motives of the type $[\mathbb{Z}^r \to \mathbb{G}_m^s]$.

We can state Conjecture 6.5.2 in a slightly stronger form by describing what the conjectural linear relation between the p-adic logarithms looks like. Using the language we have introduced above we have

6.5.3 Conjecture. *The following statements are equivalent:*

(i) $f(\log_p P_1, \dots, \log_p P_n) = 0$.

(ii) The algebraic dependence (f) is exceptional for M.

It is easy to see that Conjecture 6.5.3 implies Conjecture 6.5.2.

We would like next to state a conjecture, which is equivalent to Conjecture 6.5.3. To do so we fix an embedding of $\mathbb{Q}^s$ into $\mathbb{Q}_p^s$ which allows us to regard the absolute Galois group $\Gamma_{\mathbb{Q}_p}$ as a subgroup of $\Gamma_{\mathbb{Q}}$. Let again $G = \hat{Y} \otimes \mathbb{G}_m$ be the Cartier dual of Y. Recall that we have a well-defined zero-set $Z(f, \mathrm{T}_p G) \subseteq \mathrm{T}_p G$ due to the fact that f is homogenous. Recall also that there is an exact sequence

$$0 \to \mathrm{T}_p G \to \mathrm{Aut}(\mathrm{T}_p M) \to \mathrm{Aut}(\mathrm{T}_p \mathbb{G}_m) \to 1$$

6.5.4 Conjecture. *The following two statements are equivalent:*

(i) The intersection of $\rho_p(M)(\Gamma_{\mathbb{Q}_p})$ with $\mathrm{T}_p G$ is contained in $Z(f, \mathrm{T}_p G)$;

(ii) The algebraic dependence (f) is exceptional for M.

One easily sees that (ii) implies (i). The conjectural part is that the converse implication also holds.

6.5.5 Proposition. *Conjectures 6.5.3 and 6.5.4 are equivalent.*

Proof. Let $M_p = M \otimes_{\mathbb{Q}} \mathbb{Q}_p$ denote the base change of M to $\mathbb{Q}_p$. Then the intersection of $\rho_p(M)(\Gamma_{\mathbb{Q}_p})$ with $\mathrm{T}_p G$ is precisely the image of the Kummer

map $\delta_p(M_p)$. Let $\tau \in \mathrm{T}_p\mathbb{G}_m$ be a fixed basis element. Let $v \in \mathrm{V}_p\mathbb{G}$ be the vector

$$v = \sum_{i=1}^{n} (\log_p P_i)\hat{y}_i \otimes \tau$$

Proposition 6.5.1 in this case implies that the image of the Kummer map $\delta_p(M_p)$ is a finite-index subgroup of the intersection of the vector space $\mathbb{Q}_p v$ with $\mathrm{T}_p G$. Since a vector $w = \sum_{i=1}^{n} \alpha_i \hat{y}_i \otimes \tau$ lies in $Z(f, \mathrm{T}_p G)$ if and only if $f(\alpha_1, \ldots, \alpha_n) = 0$, it is clear that $f(\log_p P_1, \ldots, \log_p P_n) = 0$ if and only if the image of $\delta_p(M_p)$ is contained in $Z(f, \mathrm{T}_p G)$. Hence statement (i) of Conjecture 6.5.3 is equivalent to statement (i) of Conjecture 6.5.4, which proves the proposition. □

Finally, we would like to show that there exists a certain analogy between our conjectures and Theorem 6.1.6. Recall the set A_p^f of automorphisms of $\mathrm{Aut}(\mathrm{T}_p M)$, which, after picking a section $\mathrm{T}_p Y \to \mathrm{T}_p M$, can be identified with the set of matrices

$$A_p^f := \left\{ \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} : |f(b)|_p \leq |\alpha - 1|_p \|b\|_p^{\deg f - 1} \right\},$$

In the proof of Theorem 6.1.6 we showed that the ℓ-part of the reduction of a 1-motive M modulo p satisfies the algebraic relation (f) if and only if the decomposition group at p is contained in A_ℓ^f. For the case $\ell = p$ we have the following analogous situation:

6.5.6 Proposition. *Suppose that $p \geq 3$. Statement (i) of Conjectures 6.5.3 and 6.5.4 holds if and only if the image of $\Gamma_{\mathbb{Q}_p}$ under the p-adic Galois representation $\rho_p(M)$ is contained in A_p^f.*

Proof. Compare with the proof of Lemma 6.4.3. Let W_p denote the image of the decomposition subgroup $\Gamma_{\mathbb{Q}_p}$ under the Galois representation $\rho_p(M)$, let X_p denote the image of the cyclotomic character and let Y_p denote the kernel of the map $W_p \to X_p$, or in other words, the image of the Kummer map $\delta_p(M \otimes_{\mathbb{Q}} \mathbb{Q}_p)$. After we identify $\mathrm{Aut}(\mathrm{T}_p M)$ with a group of matrices as in the previous section, the map $W_p \to X_p$ is given by

$$W_p \ni \begin{pmatrix} \alpha & b \\ 0 & I_n \end{pmatrix} \mapsto \alpha \in X_p,$$

and the map $Y_p \to W_p$ is given by

$$Y_p \ni b \mapsto \begin{pmatrix} 1 & b \\ 0 & I_n \end{pmatrix} \in W_p.$$

It is then clear that if W_p is contained in A_p^f, then $f(b) = 0$ for all $b \in Y_p$ which implies that Y_p lies in $Z(f, \mathrm{T}_p G)$.

Next assume that Y_p lies in $Z(f, \mathrm{T}_p G)$. By the theory of cyclotomic extensions, X_p is equal to $\mathbb{Z}_p^\times$. Let $\alpha \in X_p$ be any topological generator of X_p and let $w \in W_p$ be a pre-image. Then w can be represented by a matrix

$$w = \begin{pmatrix} \alpha & a \\ 0 & I_n \end{pmatrix}$$

One can show that any element of the form

$$\begin{pmatrix} \beta & \frac{\beta-1}{\alpha-1}a \\ 0 & I_n \end{pmatrix}$$

is contained in the closure of the group generated by w. Indeed, if $\beta = \alpha^m$ for some integer m then the element above is simply w^m. The general case follows by continuity.

Let

$$\sigma = \begin{pmatrix} \beta & b \\ 0 & I_n \end{pmatrix}$$

be an arbitrary element in W_p. We can represent σ as the following product of elements in W_p:

$$\sigma = \begin{pmatrix} 1 & \frac{1-\beta}{\alpha-1}a + b \\ 0 & I_n \end{pmatrix} \begin{pmatrix} \beta & \frac{\beta-1}{\alpha-1}a \\ 0 & I_n \end{pmatrix}$$

By our assumption it follows that $f(b + \frac{1-\beta}{\alpha-1}a) = 0$. Let d denote the degree of f. Since f is homogenous with integer coefficients and since $\|a\|_p \leq 1$, we have

$$f(b + \frac{1-\beta}{\alpha-1}a) = f(b) + C,$$

where

$$|C|_p \leq \max_{0 \leq j \leq d-1} \left\{ \|b\|_p^j \left| \frac{\beta-1}{\alpha-1} \right|_p^{d-j} \right\}$$

Note that $|\alpha - 1|_p = 1$ due to the fact that α generates $\mathbb{Z}_p^\times$ and $p \geq 3$. There are two cases. If $\|b\|_p \leq |\beta - 1|_p$ then

$$|f(b)|_p \leq \|b\|_p^d \leq |\beta - 1|_p \|b\|_p^{d-1}$$

implying that σ lies in A_p^f. On the other hand, if $|\beta - 1|_p < \|b\|_p$ then

$$|f(b)|_p = |C|_p \leq |\beta - 1|_p \|b\|_p^{d-1}$$

which brings us to the same conclusion.

We have thus proved that Y_p lies in $Z(f, \mathrm{T}_p G)$ if and only if W_p lies in A_p^f. This proves the proposition. □

As a consequence of the considerations above we see that there exists a certain correspondence between the question of whether the reduction of a 1-motive satisfies a given algebraic dependence and certain problems of p-adic transcendence theory. In particular the problem corresponding to the example given in Section 6.2 is the p-adic four exponentials conjecture stated in the introduction of this chapter.

Appendix A

Appendix

A.1 Equivalence of categories

The main reference for this section is MacLane [ML98] (or any other book on category theory).

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A (covariant) functor $F\colon \mathcal{C} \to \mathcal{D}$ is called **full** if for every pair of objects $a, b \in \mathcal{C}$ the map $\mathrm{Hom}(a,b) \to \mathrm{Hom}(Fa, Fb)$ sending every arrow $a \xrightarrow{f} b$ to its corresponding arrow $Fa \xrightarrow{Ff} Fb$ is surjective. The functor F is **faithful** if for every pair of objects $a, b \in \mathcal{C}$ the map described above is injective. It is **fully faithful** if it is both full and faithful. If $F\colon \mathcal{C} \to \mathcal{D}$ is a contravariant functor we say that it is full, faithful or fully faithful if the corresponding functor $F^{op}\colon \mathcal{C} \to \mathcal{D}^{op}$ from $\mathcal{C}$ to the opposite category $\mathcal{D}^{op}$ of $\mathcal{D}$ has any of the stated properties above.

A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called **essentially surjective** if for every object $d \in \mathcal{D}$ there exists an object $c \in \mathcal{C}$ such that Fc is isomorphic to d.

The functor $F\colon \mathcal{C} \to \mathcal{D}$ is called an **equivalence of categories** if there exists a functor $G\colon \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $G \circ F \cong Id_{\mathcal{C}}$ and $F \circ G \cong Id_{\mathcal{D}}$, where $Id_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$ and $Id_{\mathcal{D}}\colon \mathcal{D} \to \mathcal{D}$ are the identity functors of $\mathcal{C}$ and $\mathcal{D}$ respectively. In this case we will also say that the categories $\mathcal{C}$ and $\mathcal{D}$ are **equivalent**.

We have the following criterion (see [ML98, IV, Theorem 4.1]):

A.1.1 Theorem. *The following properties of a functor $F\colon \mathcal{C} \to \mathcal{D}$ are logically equivalent:*

(i) F is an equivalence of categories;

(ii) F is fully faithful and essentially surjective.

A.2 Galois theory

We recall the main results of Galois theory as presented by Grothendieck. This section is based on the exposition in [SGA1, Exp V], we have simply translated all facts which are relevant to us. We refer to the original source for proofs.

A.2.1 Definition. A category $\mathcal{C}$ is called a **Galois category** if it is equivalent to the category $\mathcal{C}(\pi)$ of finite sets with continuous π-action, where π is some

profinite topological group. The group π is called the **fundamental group** of $\mathcal{C}$.

A.2.2 Theorem. *Let S be a connected, locally noetherian scheme. The category* $\mathbf{FET}(S)$*, consisting of finite étale surjective morphisms $X \to S$ (also called* ***étale coverings****), is a Galois category.*

Proof. See [SGA1, Exp V, 7]. □

We can give a more explicit description of the equivalence $\mathcal{C} \to \mathcal{C}(\pi)$ in the definition above. A **pro-object** in $\mathcal{C}$ is any covariant functor $P\colon I \to \mathcal{C}$, where I is a small cofiltered category. The pro-objects of a category $\mathcal{C}$ form a category $Pro - \mathcal{C}$.

A.2.3 Theorem. *Let $\mathcal{C}$ be a Galois category with fundamental group π. There exists a pro-object P of $\mathcal{C}$ such that π is isomorphic to the opposite group of* $\mathrm{Aut}(P)$*. In this case the functor*

$$F_P\colon X \mapsto \mathrm{Hom}(P, X) = \varinjlim_{i \in I} \mathrm{Hom}(P_i, X)$$

is an equivalence between $\mathcal{C}$ and $\mathcal{C}(\pi)$. Moreover, every equivalence $F\colon \mathcal{C} \to \mathcal{C}(\pi)$ is isomorphic to F_P for some pro-object P.

The pro-objects P having the property described in the previous theorem are called **fundamental pro-objects**, and their associated functors F_P are called **fundamental functors**. One can show that every two fundamental pro-objects are isomorphic. Note that if a pro-object P has a limit in some category $\mathcal{C}'$ of which $\mathcal{C}$ is a subcategory, then one can replace P by its limit in the definition of the functor F_P above.

For any fundamental functor F there is a certain maximal fundamental pro-object P for which $F = F_P$. More precisely we have

A.2.4 Lemma. *Let $\mathcal{C}$ be a Galois category with fundamental group π and let F be a fundamental functor. There exists a fundamental pro-object $P = \{P_i\}_{i \in I}$ such that $F = F_P$ and such that the following two conditions are satisfied:*

(i) Every morphism $P_i \to P_j$, for $j \leq i$ is an epimorphism;

(ii) Every epimorphism $P_i \to P'$ is equivalent to some morphism $P_i \to P_j$ for some $j \leq i$.

Furthermore, this fundamental pro-object P is uniquely determined.

Let $\mathcal{C}$ be a Galois category, let $P = \{P_i\}_{i \in I}$ be a fundamental pro-object and F_P be its associated fundamental functor. We say that P_i is **Galois** if the group $\mathrm{Aut}(P_i)$ acts transitively on the set $F_P(P_i)$. One can then show that if the conditions in the lemma above are satisfied then $\mathrm{Aut}(P)$ is the limit of the groups $\mathrm{Aut}(P_i)$ for all Galois P_i. For every $j \in I$ there exists $i \geq j$ such that P_i is Galois.

Let S be a connected locally noetherian scheme. We can associate a fundamental functor and a fundamental pro-object to the category $\mathbf{FET}(S)$ as follows: Pick an algebraically closed field Ω and a geometric point $x\colon \mathrm{Spec}(\Omega) \to S$ and let F_x be the functor from the category $\mathbf{FET}(S)$ to the category of finite

sets which associates to every object $X \in \mathbf{FET}(S)$ the set $F_x(X)$ of all geometric points lying above x. The proof of Theorem A.2.2 consists essentially in showing that there exists a group $\pi = \pi_1(S, x)$ such that F_x induces an equivalence of categories $\mathbf{FET}(S) \to \mathcal{C}(\pi)$. The group $\pi_1(S, x)$ is called the **fundamental group of** S **at** x and the pro-object associated to F_x is called the **universal covering of** S **at** x. Picking a different point x' induces a group $\pi_1(S, x')$ which is non-canonically isomorphic to $\pi_1(S, x)$.

If $f\colon S' \to S$ is a morphism of connected locally noetherian schemes, x' is a geometric point in S' and $x = f(x')$, we get a functor $f^\bullet\colon \mathbf{FET}(S) \to \mathbf{FET}(S')$ and one has an isomorphism of fundamental functors $F_x \cong F_{x'} \circ f^\bullet$. Moreover we have a canonical group homomoprhism

$$\pi_1(f, x')\colon \pi_1(S', x') \to \pi_1(S, x).$$

The following proposition relates Grothendieck's Galois theory to its traditional form

A.2.5 Proposition. *Let S be the spectrum of a field k and let Ω be an algebraic closure of k which defines a geometric point $x\colon \operatorname{Spec}\Omega \to S$. Let k^s be the separable closure of k in Ω. Then the spectrum of k^s is the limit (in the category of S-schemes) of the universal covering for S at x. The group $\pi_1(S, x)$ is canonically isomorphic to the topological Galois group of the extension k^s/k.*

Proof. See [SGA1, Exp. V,8.1] □

A.2.6 Proposition. *Let S be the spectrum of a Dedekind domain R, and let S be the spectrum of its fraction field K. Let Ω be an algebraic closure of K, defining corresponding geometric points $x' \in S'(\Omega)$ and $x \in S(\Omega)$. Then the homomorphism*

$$\pi_1(S', x') \to \pi_1(S, x)$$

is surjective. If we identify the first group with the Galois group of K^s/K, then the kernel of the homomorphism above is the absolute Galois group of the maximal field extension of K which is unramified over R.

Proof. This is a special case of [SGA1, Exp. V,8.2] □

A.3 Galois descent

In the following we are going to recall the basic theory of Galois descent which we need in the first two chapters. The main reference we use is Bosch-Lütkebohmert-Raynaud [BLR90], Sections 6.1 and 6.2.

A morphism $p\colon S' \to S$ of schemes is called **faithfully flat** if it is flat and surjective.

A scheme X is called **quasi-affine** if it is isomorphic to a quasi-compact open subscheme of an affine scheme (see [EGA2, §5.1.1]).

A morphism $f\colon X \to Y$ of schemes is **quasi-separated** if the diagonal morphism $\Delta\colon X \to X \times_Y X$ is quasi-compact (see [EGA4I, §1.2.1]).

Let $p\colon S' \to S$ be a finite and faithfully flat morphism of schemes. We say that p is a **Galois covering** if there exists a finite group Γ of S-automorphisms of S' such that the morphism

$$\Gamma \times S' \to S' \times_S S',\ (\sigma, x) \mapsto (\sigma x, x),$$

is an isomorphism. Here, $\Gamma \times S'$ is the disjoint union of copies of S' indexed by Γ.

We give the standard instance of a Galois covering. Let S be a connected, locally noetherian scheme, let $x\colon \operatorname{Spec}\Omega \to S$ be a geometric point and let $P = \{P_i\}_{i\in I}$ be its associated universal covering. Then an element P_i is Galois in the sense of the previous section if and only if the morphism $P_i \to S$ is a Galois covering. The group Γ in this case is simply the automorphism group $\operatorname{Aut}_S(P_i)$. It is a quotient of the automorphism group of the universal covering $\operatorname{Aut}_S(P)$, which is the opposite of the fundamental group $\pi_1(S, x)$.

We will fix in the following a Galois covering $p\colon S' \to S$ with Galois group Γ. Let X' be an S'-scheme. A **descent datum** ϕ on X' is an action $\phi\colon \Gamma \times X' \to X'$ compatible with the action of Γ on S'. In other words, we require that for every $\sigma \in \Gamma$ the following diagram is commutative:

$$\begin{array}{ccc} X' & \xrightarrow{\sigma} & X' \\ \downarrow & & \downarrow \\ S' & \xrightarrow{\sigma} & S' \end{array}$$

Let X' and Y' be two S'-schemes with descent data. An S'-scheme morphism $f\colon X' \to Y'$ is **compatible with the descent data** if for every $\sigma \in \Gamma$ we have $f \circ \sigma = \sigma \circ f$. Thus, the S'-schemes with associated descent data form a category.

A.3.1 Remark. The definition of descent data given above is equivalent to the standard definition of descent data associated to S'-schemes X' where $p\colon S' \to S$ is a faithfully flat and quasi-compact morphism (see [BLR90], 6.2/Example B).

To every S-scheme X we can associate an S'-scheme with descent datum. Namely, take $X' = p^*X = X \times_S S'$. Then every automorphism $\sigma\colon S' \to S'$ lifts to an automorphism $\sigma\colon X' \to X'$ and thus, we have an action of Γ on the S'-scheme X' which is compatible with the action on S'. Moreover, every morphism $f\colon X \to Y$ of S-schemes lifts to a morphism $p^*f\colon X' \to Y'$ which is compatible with the descent data. Thus we have a functor p^* from the category of S-schemes to the category of S'-schemes with descent datum.

We say that the descent datum of an S'-scheme X' is **effective** if there exists an S-scheme X such that $X' \cong p^*X$ and such that the descent datum on X' is isomorphic to the one induced by p^*.

A.3.2 Theorem. *Let $p\colon S' \to S$ be a Galois covering.*

(i) The functor $X \mapsto p^*X$ from S-schemes to S'-schemes with descent data is fully faithful

(ii) Assume that S and S' are affine and let X' be a quasi-separated S'-scheme. Then a descent datum ϕ on X' is effective if and only if the Galois orbit of every $x \in X'$ is contained in a quasi-affine open subscheme of X'.

See [BLR90], Theorem 6.1/6 and Example 6.2/B.

A.3.3 Remark.

(i) The first statement of the theorem implies that if the descent datum on X' is effective then the S-scheme X to which it "descends" is uniquely determined up to isomorphism.

(ii) A second corollary of the first statement is that commutative diagrams of morphisms of S'-schemes with effective descent data "descend" canonically to commutative diagrams of morphisms of S-schemes. In particular, this means that an S'-group scheme with effective descent datum, which is compatible with the group structure, descends to an S-group scheme.

(iii) The second condition is satisfied if $X' \to S'$ is quasi-projective (see [BLR90, Example 6.2/B]).

A.4 Henselian rings

We give here a quick review of those properties of henselian rings which we have used. For further reference see [EGA4IV, §18], [Ray70a] [Mil80, I.§4] or [BLR90, §2.3].

A.4.1 Definition. Let R be a local ring. It is called **henselian** if every finite R-algebra decomposes into a product of local rings. It is called **strictly henselian** if it is henselian and its residue field is separably closed.

This is one of several equivalent definitions for henselian local rings. An alternative definition is: R is henselian if Hensel's lemma holds for the ring $R[T]$. See any of the references given above for further details.

A.4.2 Proposition. *Any complete local ring is henselian. In particular, any field is henselian.*

Proof. See [Mil80, Proposition I.4.5] or [EGA4IV, §18.5.14]. □

A.4.3 Definition. Let R be a ring and let A be an R-algebra. A is called an **étale R-algebra** if the corresponding map $\operatorname{Spec} A \to \operatorname{Spec} R$ is étale.

A.4.4 Proposition. *Let R be a henselian local ring and let k be its residue field. The functor $A \mapsto A \otimes_R k$ induces an equivalence between the category of finite étale R-algebras and the category of finite étale k-algebras.*

Proof. See [Mil80, Proposition I.4.4], [EGA4IV, §18.5.15]. [Ray70a, p. 84, Corollaire]. □

A.4.5 Remark. The proposition above induces an equivalence of categories $F\colon \mathbf{FET}(R) \to \mathbf{FET}(k)$. Hence if $x'\colon \operatorname{Spec}\Omega \to \operatorname{Spec} k$ is a geometric point and $x\colon \operatorname{Spec}\Omega \to \operatorname{Spec} R$ is the corresponding image of x, then we have an isomorphism

$$\pi_1(\operatorname{Spec} K, x') \xrightarrow{\sim} \pi_1(\operatorname{Spec} R, x).$$

If $(P_i)_{i\in I}$ is the universal covering of $\operatorname{Spec} k$ over x', then $(F^{-1}(P_i))_{i\in I}$ is the universal covering of $\operatorname{Spec} R$ over x. This covering has a limit R^s which is called a **strict henselisation** of R. R^s is a strictly henselian local ring and its residue field is k^s, the separable closure of k in Ω. See any of the references above for further details.

A.5 Group schemes

We recall briefly the definition of a group scheme. Let S be a scheme. A **group scheme over** S (or an *S-group scheme*) consists of the data (X, m, ι, ϵ), where $p\colon X \to S$ is an S-scheme, and $m\colon X \times_S X \to X$, $\iota\colon X \to X$ and $\epsilon\colon S \to X$ are S-morphisms for which the following diagrams are commutative:

GS1. associativity

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{m \times \mathrm{id}_X} & X \times X \\ \downarrow{\scriptstyle \mathrm{id}_X \times m} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array}$$

GS2. existence of left-identity

$$\begin{array}{ccccc} X & \xrightarrow{(p, \mathrm{id}_X)} & S \times X & \xrightarrow{\epsilon \times \mathrm{id}_X} & X \times x \\ & \searrow^{\mathrm{id}_X} & & & \downarrow{\scriptstyle m} \\ & & & & X \end{array}$$

GS3. existence of a left-inverse

$$\begin{array}{ccc} X & \xrightarrow{(\iota, id_X)} & X \times X \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{\epsilon} & X \end{array}$$

Moreover, the S-group scheme is **commutative** if the structure morphisms satisfy the following commutative diagram:

GS4. commutativity

$$\begin{array}{ccc} X \times X & \xrightarrow{\tau} & X \times X \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & X \end{array}$$

where τ commutes the factors.

(All products above are fibered products in the category of S-schemes.)

Furthermore, we define morphisms of S-group schemes to be morphisms of schemes which are compatible with the group structures (see e.g. [BLR90, §4.1] for details).

We need the following result

A.5.1 Proposition. *Let S be a noetherian integral regular scheme whose irreducible components all have dimension 1. Every smooth S-group scheme which is quasi-compact and separated over S is quasi-projective.*

Proof. This is a special case of a result of Raynaud [Ray70b, Théorème VIII.2] □

A.6 Homological algebra

Profinite group cohomology

We will give a quick review of those results on profinite group cohomology, which we have used in Chapters 3 and 5. Our main reference is [Ser64].

A topological group is called **profinite** if it is a projective limit of finite groups, or equivalently, if it is compact and totally disconnected. Let Γ be such a group and let A be a topological left Γ-module, which is separated as a topological space. An *n-cochain* of Γ with values in A is a *continuous* function f from the product $\Gamma \times \cdots \times \Gamma$, where Γ is taken n times, to A. The *coboundary* df of f is defined by the formula

$$df(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1 f(\sigma_2, \ldots, \sigma_{n+1}) +$$
$$\sum_{i=1}^{n} (-1)^i f(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n).$$

This gives us a complex $C^\bullet(\Gamma, A)$, whose cohomology groups we denote by $H^n(\Gamma, A)$.

The set $H^0(\Gamma, A)$ is identified with the subset A^Γ of elements fixed under the action of Γ. As for the first cohomology $H^1(\Gamma, A)$, it is the quotient of 1-cocycles by 1-coboundaries $Z^1(\Gamma, A)/B^1(\Gamma, A)$. Here $Z^1(\Gamma, B)$ consists of all function s f from Γ to A, which satisfy the 1-cocycle condition

$$f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$$

The set of 1-coboundaries consists of all functions f such that $f(\sigma) = (\sigma - 1)a$ for some a in A.

If $0 \to A \to B \to C \to 0$ is an exact sequence of topological Γ-modules we get the usual long exact sequence

$$\cdots \to H^n(\Gamma, A) \to H^n(\Gamma, B) \to H^n(\Gamma, C) \xrightarrow{d} H^{n+1}(\Gamma, A) \to \cdots$$

A.6.1 Lemma. *Let Γ be a profinite group and let $M = \varprojlim_n M_n$ be a projective limit of compact Γ-modules . We have*

$$H^1(\Gamma, M) = \varinjlim_n H^1(\Gamma, M_n).$$

Proof. See Proposition 7 in [Ser64]. □

A.6.2 Lemma. *Let Γ be a compact ℓ-adic Lie group acting continuously on a finitely-generated free $\mathbb{Z}_\ell$-module T. Then $H^1(\Gamma, T)$ is a fintely-generated $\mathbb{Z}_\ell$-module and we have that*

$$H^1(\Gamma, T) \otimes \mathbb{Q}_\ell \cong H^1(\Gamma, T \otimes \mathbb{Q}_\ell)$$

Proof. See Proposition 9 in [Ser64]. □

A.6.3 Lemma (Sah)**.** *Let Γ be a profinite group and let A be a topological Γ-module. Let σ be an element in the center of Γ. Then $\sigma - 1$ kills $H^1(\Gamma, A)$. In particular, if $\sigma - 1$ is an automorphism of A then $H^1(\Gamma, A) = 0$.*

Proof. This is proved in the case of standard group cohomology in [Lan02, VI, Lemma 10.2]. For profinite group cohomology the proof is the same. □

Bibliography

[And04] Yves André. *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*. Vol. 17. Panoramas et Synthèses [Panoramas and Syntheses]. Paris: Société Mathématique de France, 2004, pp. xii+261. ISBN: 2-85629-164-3.

[Ber02] Cristiana Bertolin. "Périodes de 1-motifs et transcendance". In: *J. Number Theory* 97.2 (2002), pp. 204–221. ISSN: 0022-314X. DOI: 10.1016/S0022-314X(02)00002-1. URL: http://dx.doi.org/10.1016/S0022-314X(02)00002-1.

[Ber88] D. Bertrand. "Galois representations and transcendental numbers". In: *New advances in transcendence theory (Durham, 1986)*. Cambridge: Cambridge Univ. Press, 1988, pp. 37–55.

[BGK05] G. Banaszak, W. Gajda, and P. Krasoń. "Detecting linear dependence by reduction maps". In: *J. Number Theory* 115.2 (2005), pp. 322–342. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2005.01.008. URL: http://dx.doi.org/10.1016/j.jnt.2005.01.008.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Berlin: Springer-Verlag, 1990, pp. x+325. ISBN: 3-540-50587-3.

[Bog81] F.A. Bogomolov. "Points of finite order on an Abelian variety." English. In: *Math. USSR, Izv.* 17 (1981), pp. 55–72. DOI: 10.1070/IM1981v017n01ABEH001329.

[Car] S. Carnahan (mathoverflow.net/users/121). *Reference request for Cartier Duality of algebraic tori*. MathOverflow. http://mathoverflow.net/questions/98462 (version: 2012-05-31).

[CRS97] Capi Corrales-Rodrigáñez and René Schoof. "The support problem and its elliptic analogue". In: *J. Number Theory* 64.2 (1997), pp. 276–290. ISSN: 0022-314X. DOI: 10.1006/jnth.1997.2114. URL: http://dx.doi.org/10.1006/jnth.1997.2114.

[Del71] Pierre Deligne. "Théorie de Hodge. II". In: *Inst. Hautes Études Sci. Publ. Math.* 40 (1971), pp. 5–57. ISSN: 0073-8301.

[Del74] Pierre Deligne. "Théorie de Hodge. III". In: *Inst. Hautes Études Sci. Publ. Math.* 44 (1974), pp. 5–77. ISSN: 0073-8301.

[EGA2] A. Grothendieck. "Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes". In: *Inst. Hautes Études Sci. Publ. Math.* 8 (1961), p. 222. ISSN: 0073-8301.

[EGA4I] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I". In: *Inst. Hautes Études Sci. Publ. Math.* 20 (1964), p. 259. ISSN: 0073-8301.

[EGA4II] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II". In: *Inst. Hautes Études Sci. Publ. Math.* 24 (1965), p. 231. ISSN: 0073-8301.

[EGA4III] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III". In: *Inst. Hautes Études Sci. Publ. Math.* 28 (1966), p. 255. ISSN: 0073-8301.

[EGA4IV] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV". In: *Inst. Hautes Études Sci. Publ. Math.* 32 (1967), p. 361. ISSN: 0073-8301.

[Fal83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Invent. Math.* 73.3 (1983), pp. 349–366. ISSN: 0020-9910. DOI: 10.1007/BF01388432. URL: http://dx.doi.org/10.1007/BF01388432.

[Fol95] Gerald B. Folland. *A course in abstract harmonic analysis*. Studies in Advanced Mathematics. Boca Raton, FL: CRC Press, 1995, pp. x+276. ISBN: 0-8493-8490-7.

[Hin88] Marc Hindry. "Autour d'une conjecture de Serge Lang". In: *Invent. Math.* 94.3 (1988), pp. 575–603. ISSN: 0020-9910. DOI: 10.1007/BF01394276. URL: http://dx.doi.org/10.1007/BF01394276.

[Jan95] Uwe Jannsen. "Mixed motives, motivic cohomology, and Ext-groups". In: *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*. Basel: Birkhäuser, 1995, pp. 667–679.

[Jos09] Peter Jossen. "On the arithmetic of 1-motives". PhD thesis. Central Europen University, 2009.

[Jos13] Peter Jossen. "On the Mumford-Tate conjecture for 1-motives". In: *Invent. Math.* (to appear).

[Kow03] E. Kowalski. "Some local-global applications of Kummer theory". In: *Manuscripta Math.* 111.1 (2003), pp. 105–139. ISSN: 0025-2611. DOI: 10.1007/s00229-003-0356-6. URL: http://dx.doi.org/10.1007/s00229-003-0356-6.

[KP04] Chandrashekhar Khare and Dipendra Prasad. "Reduction of homomorphisms mod p and algebraicity". In: *J. Number Theory* 105.2 (2004), pp. 322–332. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2003.10.006. URL: http://dx.doi.org/10.1016/j.jnt.2003.10.006.

[Lan02] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. New York: Springer-Verlag, 2002, pp. xvi+914. ISBN: 0-387-95385-X.

[Lar03] Michael Larsen. "The support problem for abelian varieties". In: *J. Number Theory* 101.2 (2003), pp. 398–403. ISSN: 0022-314X. DOI: 10.1016/S0022-314X(03)00040-4. URL: http://dx.doi.org/10.1016/S0022-314X(03)00040-4.

[Mat55] Arthur Mattuck. "Abelian varieties over p-adic ground fields". In: *Ann. of Math. (2)* 62 (1955), pp. 92–119. ISSN: 0003-486X.

[Mil80] James S. Milne. *Étale cohomology*. Vol. 33. Princeton Mathematical Series. Princeton, N.J.: Princeton University Press, 1980. ISBN: 0-691-08238-3.

[Mil86] James S. Milne. "Abelian varieties". In: *Arithmetic geometry (Storrs, Conn., 1984)*. New York: Springer, 1986, pp. 103–150.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*. Second. Vol. 5. Graduate Texts in Mathematics. New York: Springer-Verlag, 1998, pp. xii+314. ISBN: 0-387-98403-8.

[MRS07] B. Mazur, K. Rubin, and A. Silverberg. "Twisting commutative algebraic groups". In: *J. Algebra* 314.1 (2007), pp. 419–438. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2007.02.052. URL: http://dx.doi.org/10.1016/j.jalgebra.2007.02.052.

[Mur88] M. Ram Murty. "Artin's conjecture for primitive roots". In: *Math. Intelligencer* 10.4 (1988), pp. 59–67. ISSN: 0343-6993. DOI: 10.1007/BF03023749. URL: http://dx.doi.org/10.1007/BF03023749.

[nos] nosr (mathoverflow.net/users/28172). *Is the n-torsion of an extension of an abelian variety by a torus, finite and flat?* MathOverflow. http://mathoverflow.net/questions/112718 (version: 2012-11-17).

[Oor66] F. Oort. *Commutative group schemes*. Vol. 15. Lecture Notes in Mathematics. Berlin: Springer-Verlag, 1966, vi+133 pp. (not consecutively paged).

[Per08] Antonella Perucca. "On the order of the reductions of points on abelian varieties and tori". PhD thesis. Universita di Roma La Sapienza, 2008.

[Per09] Antonella Perucca. "Prescribing valuations of the order of a point in the reductions of abelian varieties and tori". In: *J. Number Theory* 129.2 (2009), pp. 469–476. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2008.07.004. URL: http://dx.doi.org/10.1016/j.jnt.2008.07.004.

[Pin04] Richard Pink. "On the order of the reduction of a point on an abelian variety". In: *Math. Ann.* 330.2 (2004), pp. 275–291. ISSN: 0025-5831. DOI: 10.1007/s00208-004-0548-8. URL: http://dx.doi.org/10.1007/s00208-004-0548-8.

[Ray70a] Michel Raynaud. *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Berlin: Springer-Verlag, 1970, pp. v+129.

[Ray70b] Michel Raynaud. *Faisceaux amples sur les schémas en groupes et les espaces homogènes*. Lecture Notes in Mathematics, Vol. 119. Berlin: Springer-Verlag, 1970, pp. ii+218.

[Ray94] Michel Raynaud. "1-motifs et monodromie géométrique". In: *Astérisque* 223.223 (1994). Périodes p-adiques (Bures-sur-Yvette, 1988), pp. 295–319. ISSN: 0303-1179.

[Rib79] Kenneth A. Ribet. "Kummer theory on extensions of abelian varieties by tori". In: *Duke Math. J.* 46.4 (1979), pp. 745–761. ISSN: 0012-7094. URL: http://projecteuclid.org/getRecord?id=euclid.dmj/1077313720.

[Ser00] Jean-Pierre Serre. "Résumé des cours de 1985-1986". In: *Œuvres. Collected papers.* Vol. 4. Springer-Verlag, 2000, pp. 33–37.

[Ser64] Jean-Pierre Serre. "Sur les groupes de congruence des variétés abéliennes". In: *Izv. Akad. Nauk SSSR Ser. Mat.* 28 (1964), pp. 3–20. ISSN: 0373-2436.

[Ser98] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves.* Vol. 7. Research Notes in Mathematics. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. Wellesley, MA: A K Peters Ltd., 1998, p. 199. ISBN: 1-56881-077-6.

[SGA1] *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)]. Paris: Société Mathématique de France, 2003, pp. xviii+327. ISBN: 2-85629-141-4.

[SGA3I] Philippe Gille and Patrick Polo, eds. *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes.* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 7. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64], A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre, Revised and annotated edition of the 1970 French original. Paris: Société Mathématique de France, 2011, pp. xxviii+610. ISBN: 978-2-85629-323-2.

[SGA3II] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux.* Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152. Berlin: Springer-Verlag, 1970, pp. ix+654.

[SGA4I] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos.* Lecture Notes in Mathematics, Vol. 269. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat. Berlin: Springer-Verlag, 1972, pp. xix+525.

[ST68] Jean-Pierre Serre and John Tate. "Good reduction of abelian varieties". In: *Ann. of Math. (2)* 88 (1968), pp. 492–517. ISSN: 0003-486X.

[Wes03] Tom Weston. "Kummer theory of abelian varieties and reductions of Mordell-Weil groups". In: *Acta Arith.* 110.1 (2003), pp. 77–88. ISSN: 0065-1036. DOI: 10.4064/aa110-1-6. URL: http://dx.doi.org/10.4064/aa110-1-6.

Index