On the structure of Selmer groups over p-adic Lie extensions

Yoshihiro Ochi[1] and Otmar Venjakob

Abstract. The goal of this paper is to prove that the Pontryagin dual of the Selmer group over the trivializing extension of an elliptic curve without complex multiplication does not have any nonzero pseudo-null submodule. The main point is to extend the definition of pseudo-null to modules over the completed group ring $\mathbb{Z}_p[[G]]$ of an arbitrary p-adic Lie group G without p-torsion. For this purpose we prove that $\mathbb{Z}_p[[G]]$ is an Auslander regular ring. For the proof we also extend some results of Jannsen's homotopy theory of modules and study intensively higher Iwasawa adjoints.

1 Introduction

Let K be a finite extension of $\mathbb{Q}$, and let E be an elliptic curve over K with $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$. Let p be a rational prime ≥ 5, and let E_{p^∞} be the group of all p-th power division points on E, and put $K_\infty = K(E_{p^\infty})$. From the point of view of arithmetic geometry, there is great interest in studying the (p-primary) Selmer group of E over K_∞, which we denote by $\mathrm{Sel}_p(K_\infty, E)$ (see § 5 for the definition). We write $\mathrm{Sel}_p(K_\infty, E)^\vee$ for the compact Pontryagin dual of $\mathrm{Sel}_p(K_\infty, E)$. R. Greenberg has remarked that $\mathrm{Sel}_p(K_\infty, E)^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has infinite dimension over $\mathbb{Q}_p$ for all $p \geq 5$ (see the appendix of [CH]), and earlier M. Harris ([Ha2]) had given examples where $E(K_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ has infinite dimension over $\mathbb{Q}_p$. Let G denote the Galois group of K_∞ over K, and write $\Lambda(G) = \mathbb{Z}_p[[G]]$ for the completed group algebra, or Iwasawa algebra, of G. Then $\mathrm{Sel}_p(K_\infty, E)^\vee$ has a natural structure as a module over $\Lambda(G)$, and it seems to be a fundamental question to study its structure as a $\Lambda(G)$-module. M. Harris conjectured in [Ha1] that $\mathrm{Sel}_p(K_\infty, E)^\vee$ is torsion over $\Lambda(G)$ when E has good ordinary reduction at all primes of K above p. Recently, the first examples of elliptic curves E and primes p where this conjecture can be proved were given in [CH]. We shall assume throughout this paper that E has good reduction at all primes of K above p. The aim of the present paper is to prove the following basic result.

Theorem (Theorem 5.1). *Assume that E has good ordinary reduction at all primes above p and that $\mathrm{Sel}_p(K_\infty, E)^\vee$ is a Λ-torsion module. Then $\mathrm{Sel}_p(K_\infty, E)^\vee$ has no non-zero pseudo-null Λ-submodule.*

We shall actually prove the theorem under a weaker condition which is a generalized

[1]During this research, Y. Ochi has been supported by the Deutsche Forschungsgemeinschaft(DFG) "Forschergruppe Arithmetik" at the Mathematical Institute, Heidelberg.

conjecture on the rank of $\mathrm{Sel}_p(K_\infty, E)^\vee$. There is a similar theorem due to B. Perrin-Riou on non-existence of pseudo-null submodule in the CM case ([Pe], Theorem 2.4). Also there is a theorem of Greenberg ([Gr3]) and the work of Hachimori-Matsuno on finite submodules of the Selmer group over the cyclotomic $\mathbb{Z}_p$-extension ([HM]). In this case, it is known that non-zero finite submodules can occur in the dual of Selmer over the cyclotomic $\mathbb{Z}_p$-extension.

Let K_{cycl} denote the field $K(\mu_{p^\infty})$. Then by the Weil paring K_∞ contains K_{cycl}. Putting $H = G(K_\infty/K_{cycl})$ and $\Gamma = G(K_{cycl}/K)$, $\mathrm{Sel}_p(K_\infty, E)^\vee$ has a structure of $\Lambda(H)$-module by restriction. An observation of Coates and Howson ([CH]) is that if $\mathrm{Sel}_p(K_{cycl}, E)^\vee$ is $\Lambda(\Gamma)$-torsion and its Iwasawa μ-invariant is zero, then $\mathrm{Sel}_p(K_\infty, E)^\vee$ is finitely generated over $\Lambda(H)$. It is easily checked that the set of all the $\Lambda(H)$-torsion elements of it forms a G-stable $\Lambda(H)$-module. Hence it is a $\Lambda(G)$-submodule of $\mathrm{Sel}_p(K_\infty, E)^\vee$, which will turn out to be pseudo-null. Therefore the theorem answers a question of John Coates positively as follows:

Theorem (Theorem 6.1). *Assume that G is pro-p and that $Sel_p(K_{cycl}, E)^\vee$ is a finitely generated $\mathbb{Z}_p$-module. Then* $\mathrm{Sel}_p(K_\infty, E)^\vee$ *is a finitely generated $\Lambda(H)$-module, whose $\Lambda(H)$-torsion submodule is zero.*

As a numerical example of this theorem, take E to be the modular elliptic curve $X_1(11)$, with equation

$$y^2 + y = x^3 - x^2 \ ,$$

take $p = 5$, and $K = \mathbb{Q}(\mu_5)$. Then $G = G(K_\infty/K)$ is a pro-5 group. Moreover, $K_{cycl} = \mathbb{Q}(\mu_{5^\infty})$. Then Coates and Howson ([CH]) show that $\mathrm{Sel}_5(K_\infty, E)^\vee$ is a finitely generated $\Lambda(H)$-module of rank 4, where $H = G(K_\infty/\mathbb{Q}(\mu_{5^\infty}))$. The above theorem shows that the $\Lambda(H)$-torsion submodule of $\mathrm{Sel}_5(K_\infty, E)^\vee$ is zero. It does not seem possible to prove this latter statement other than by using the techniques of our paper.

The reader may have realized that the most important point in the above statement of our main theorem is yet to be explained: What is the adequate definition of *pseudo-null* in the noncommutative case ? For a commutative Noetherian ring R and a finitely generated R-module M the definition is standard: The dimension of M is defined to be the Krull dimension of the support of M in $\mathrm{Spec}(R)$ and M is said to be pseudo-null, if its codimension is greater than 1. However, we have to work with a noncommutative ring since by a well-known theorem of J.-P. Serre, G is identified with an open subgroup of $GL_2(\mathbb{Z}_p)$, which is not an abelian group and consequently Λ is not commutative either. In this noncommutative case a vague definition of pseudo-null ("trivial mod $\mathcal{C}$" in his terminology) was given by Harris ([Ha1]). But besides some more or less trivial cases it turned out very difficult to verify whether a module is pseudo-null, because the definition relies heavily on a certain filtration of Λ, which in general differs from the $\mathfrak{M}$-adic one and cannot be described easily. Moreover, with his definition, one has to calculate the dimension of the associated graded module, which in general is almost impossible. Hence we follow a different philosophy, which we will explain now.

In [Ja1] U. Jannsen proposed to use the homotopy theory for Λ-modules in order to study modules over the completed group algebra $\Lambda = \mathbb{Z}_p[[G]]$ for compact p-adic Lie groups G. In this theory the "higher" Iwasawa adjoints $\mathrm{E}^r(M) := \mathrm{Ext}^r_\Lambda(M, \Lambda)$ play a crucial role and can be considered as a certain analogue of homotopy groups. In an absolutely different context and for an arbitrary (left and right Noetherian) associative ring Λ, J.-E. Björk ([Bj1]) analyzed a spectral sequence for such Ext-groups associated with the bidualizing complex and gave a definition of the dimension of a finitely generated Λ-module M in the case that Λ is an Auslander regular ring. Now it is a result of the second author's thesis that the completed group algebra for a compact p-adic Lie group without p-torsion is indeed an Auslander regular ring. This allows us to apply Björk's results ([Bj1]) to Iwasawa theory and in particular to give a good definition of pseudo-null modules. Since in the case of $G = \mathbb{Z}_p^d$, Björk's dimension turns out equal to the Krull dimension of the support of M with respect to Λ we are convinced that our definition is the right generalization to the noncommutative case.

Using these new methods we are going to examine the following general situation: For a number field K, let V be a p-adic representation of G_K of finite $\mathbb{Q}_p$-dimension,where G_K denotes the Galois group of $\bar{\mathbb{Q}}$ over K, T a G_K-stable lattice of V and $A = V/T$ the quotient. Assuming that V is a G_K-module unramified outside finitely many places, we denote by S a finite set of places which contains each prime above p, all archimedian places and all places at which V ramifies. Let K_∞ be a p-adic Lie extension inside the maximal S-ramified extension K_S of K and denote its Galois group by $G = G(K_\infty/K)$. In the following we study the $\Lambda = \Lambda(G)$-modules $H^r(\mathrm{G}_{\mathrm{S},\infty}, A)$, where $\mathrm{G}_{\mathrm{S},\infty}$ denotes the Galois group $G(K_S/K_\infty)$. Along the way to the proof of the theorem, we shall actually prove a few more things. The first one, where we use the notation $A^* := T_p(A)^\vee(1)$ with the Tate module $T_p(A) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A)$, is:

Theorem (Theorem 4.11). *Let K be either a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}$, K_∞/K a p-adic Lie extension such that $K(A) \subset K_\infty$, and A as above. Put $G = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \Lambda(G)$.*

(i) *Let K be a finite extension of $\mathbb{Q}_p$. Then the Λ-module $H^1(K_\infty, A)^\vee$ is homotopically determined by the Λ-module $A^*(K_\infty)$ and a class $\xi \in \mathrm{Ext}^2_\Lambda(A^\vee, A^*)^\vee$.*

(ii) *Let K be a finite extension of $\mathbb{Q}$. Then the Λ-module $H^1(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$ is homotopically determined by the Λ-module $Z_A \cong \varprojlim_{K \subset F \subset K_\infty} H^2(G_S(F), T_p A)$ and and a class $\xi \in \mathrm{Ext}^2_\Lambda(A^\vee, Z_A^\vee)^\vee$.*

This theorem generalizes a main result of Jannsen's article [Ja1], while the next one extends results of Greenberg ([Gr1]) and Nguyen-Quang-Do ([Ng]):

Theorem (Theorem 4.6). *If $H^2(G_{S,\infty}, A) = 0$, then $H^1(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$ has no nontrivial pseudo-null $\Lambda(G')$-submodule for any open subgroup G' of G without p-torsion.*

Note that the cohomology group $H^2(G_{S,\infty}, A)$ vanishes if K_∞ contains the trivializing extension $K(A)$ and the cyclotomic $\mathbb{Z}_p$-extension, for the weak Leopoldt conjecture is known to hold for the cyclotomic extension K_{cycl} of any number field K (This result can be deduced from Iwasawa's rank calculation of some Γ-module but see [Sc1] Lemma 7 or [NSW] Theorem (10.3.25) for a proof).

Now we specialize to the case $A = E_{p^\infty}$ where E_{p^∞} are the p-torsion points of an elliptic curve defined over K without complex multiplication. Then the trivializing extension $K_\infty = K(E_{p^\infty})$ is a p-adic Lie extension over K and the above theorems apply to this situation. The corresponding (global and local) results allow us to derive consequences for one of the most important invariants in the study of K_n-rational points of elliptic curves, the Selmer group $\mathrm{Sel}_p(K_n, E)$, respectively, taking the limit, $\mathrm{Sel}_p(K_\infty, E)$. Utilizing Coates and Greenberg's Kummer theory of abelian varieties over local fields ([CG]) as well as results of Serre ([Se1]), we are able to prove our main theorem.

ACKNOWLEDGEMENTS. We would like to thank Uwe Jannsen not only for inspiring us by his work but also for some helpful suggestions. We are very thankful to John Coates for his interest, valuable comments and important questions related to this work. We are also grateful to Kay Wingberg for his advice and encouragement. Yoshihiro Ochi thanks him in particular for inviting him to the Mathematical Institute, University of Heidelberg. He also thanks the DFG for its support. We thank R. Sujatha for some helpful comments. Finally Susan Howson is warmly acknowledged for discussions during her staying in Heidelberg in the winter of 1999.

A part of the material, especially the section about filtrations, is taken from the second author's thesis.

Notations and Conventions

(1) Throughout this paper we always assume that p is an odd rational prime number.

(2) For a $\mathbb{Z}_p$-module N, $N^\vee = \mathrm{Hom}_{\mathbb{Z}_p,cont}(N, \mathbb{Q}_p/\mathbb{Z}_p)$, is the Pontryagin dual of N, and for a p-divisible $\mathbb{Z}_p$-module, $N^* = \varinjlim_i \mathrm{Hom}(N_{p^i}, \mu_{p^\infty}) = T(N)^\vee(1)$, where N_{p^i} denotes the kernel of the multiplication by p^i and $T(N) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, N) = \varprojlim_i N_{p^i}$.

(3) By a Noetherian ring, we mean a left and right Noetherian ring (with a multiplicative unit). By $pd_\Lambda(M)$ we denote projective dimension of M. But the global dimension of Λ is denoted $pd(\Lambda)$.

(4) Let G be a profinite group and H a closed subgroup of G. For a $\Lambda(H)$-module M, we define $\mathrm{Ind}_H^G M := M\widehat{\otimes}_{\Lambda(H)}\Lambda(G)$ (compact or completed induction), where $\widehat{\otimes}$ denotes completed tensor product. Also $\mathrm{Coind}_H^G M := \mathrm{Hom}_{\Lambda(H)}(M, \Lambda(G))$.

(5) Whenever we deal with an elliptic curve over a number field K and a fixed rational prime number p, we always assume that E has good reduction at all places dividing p.

(6) If H is any profinite group, by $H(p)$, resp. H^{ab}, we denote the maximal pro-p quotient, resp. the maximal abelian quotient $H/[H,H]$, of H.

(7) Let K be a field. For a $G(\bar{K}/K)$-module A, we write $A(K) := H^0(G(\bar{K}/K), A)$.

2 A Canonical Filtration of Λ-Modules and the Definition of Pseudo-Null

Let G be a compact p-adic Lie group without p-torsion and $\Lambda := \Lambda(G) := \mathbb{Z}_p[[G]]$ its completed group ring, which is Noetherian (cf. [La] V 2.2.4) and of finite global dimension $d = \mathrm{cd}_p(G) + 1$. In this section we discuss a canonical filtration on finitely generated Λ-modules, a more general and detailed treatment of which can be found in [Ve]. From now on, all Λ-modules are assumed to be finitely generated and we use the following

Notation. For a Λ-module M,

$$\mathrm{E}^i(M) := \mathrm{Ext}^i_\Lambda(M, \Lambda)$$

for any integer i and $\mathrm{E}^i(M) = 0$ for $i < 0$ by convention. We also write $M^+ = E^0(M) = \mathrm{Hom}_\Lambda(M, \Lambda)$.

We recall the following

Definition 2.1 *1. If $M \neq 0$ is a Λ-module, then $j(M) := min\{i \mid E^i(M) \neq 0\}$ is called the grade of M.*

2. A Noetherian ring Λ is called Auslander regular ring if it has finite global homological dimension and the following Auslander-condition holds: For any Λ-module M, any integer m and any submodule N of $E^m(M)$, the grade of N satisfies $j(N) \geq m$.

Remark. Let Λ be a commutative ring. Then, Λ is Auslander regular if and only if it is regular (in the usual sense) and of finite Krull dimension. (The implications concerning the global homological dimensions are well known. For the Auslander-condition see [Au, Cor. 4.6,Prop. 4.21])

Suppose for the moment that Λ is any Auslander regular ring. It was Björk [Bj1] who studied in detail the bidualizing complex in order to evaluate the equality $M = \mathbf{R}\mathrm{Hom}(\mathbf{R}\mathrm{Hom}(M, \Lambda), \Lambda)$ in the derived category of complexes of Λ-modules: the associated filtrations of this double complex give rise to two convergent spectral sequences, the first of which degenerates. On the other hand, the second one becomes

$$E_2^{p,q} = \mathrm{E}^p(\mathrm{E}^{-q}(M)) \Rightarrow \mathrm{H}^{p+q}(\Delta^\bullet(M)),$$

where $\Delta^\bullet(M)$ is a filtered complex, which is exact in all degrees except zero: $\mathrm{H}^0(\Delta^\bullet) = M$, i.e. there is a canonical filtration

$$\mathrm{T}_0(M) \subseteq \mathrm{T}_1(M) \subseteq \cdots \subseteq \mathrm{T}_{d-1}(M) \subseteq \mathrm{T}_d(M) = M$$

on every module M. The convergence of the spectral sequence implies

$$E_\infty^{p,q} = \begin{cases} \mathrm{T}_{d-p}(M)/\mathrm{T}_{d-p-1}(M) & if \quad p+q=0 \\ 0 & otherwise \end{cases}$$

(By convention, $\mathrm{T}_i(M) = 0$ *for* $i < 0$).

Definition 2.2 *1. The number* $\delta := min\{i \mid \mathrm{T}_i(M) = M\}$ *is called the dimension* $\delta(M)$ *of a* Λ*-module* M*.*

2. If M *is a* Λ*-module we say that it has pure* δ*-dimension if* $\mathrm{T}_{\delta-1}(M) = 0$*, i.e. the filtration degenerates to a single term* M*.*

3. We call a Λ*-module* M *pseudo-null, if* $M = \mathrm{T}_{d-2}(M)$*, i.e. if* $\delta(M) \leq d-2$ *holds (recall* $d = pd(\Lambda)$*).*

By Grothendieck's local duality, this definition coincides with the Krull dimension of $\mathrm{Supp}_\Lambda(M)$ if Λ is a commutative local Noetherian regular ring, see for example [Brun, Cor. 3.5.11].

First we want to state some basic facts of the δ-dimension. The functoriality of the spectral sequence implies

Proposition 2.3 *1. If* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *is an exact sequence of* Λ*-modules then* $\mathrm{T}_i(M') \subseteq \mathrm{T}_i(M)$ *for all* i *and both* $\delta(M')$ *and* $\delta(M'')$ *are* $\leq \delta(M)$*.*

2. $\mathrm{T}_i(\bigoplus_k(M_k)) = \bigoplus_k \mathrm{T}_i(M_k)$ *and* $\delta(\bigoplus_k M_k) = \max_k \delta(M_k)$*.*

In order to get further nice properties the Auslander-condition is essential:

Proposition 2.4 *Assume that* Λ *is Auslander regular of global dimension* d *and let* M *be a* Λ*-module. Then*

1. *(a) For all* i*, there is an exact sequence of* Λ*-modules*
   $$0 \longrightarrow \mathrm{T}_i(M)/\mathrm{T}_{i-1}(M) \longrightarrow E^{d-i}E^{d-i}(M) \longrightarrow Q_i \longrightarrow 0,$$
   where Q_i *is a subquotient of* $\bigoplus_{j\geq 1} E^{d-i+j+1}E^{d-i+j}(M)$*.*
   (b) $\mathrm{T}_i(M)/\mathrm{T}_{i-1}(M) = 0$ *if and only if* $E^{d-i}E^{d-i}(M) = 0$*.*
2. $\delta(M) + j(M) = d$*.*
3. *(a)* $j(E^i(M)) \geq i$*, i.e.* $E^jE^i(M) = 0$ *for all* $j < i$*.*
   (b) $\delta(E^i(M)) \leq d - i$*.*
   (c) $E^{j(M)}(M)$ *has pure* δ*-dimension* $\delta(M)$*.*
4. *(a)* $\delta(\mathrm{T}_i(M)) \leq i$*.*
   (b) $\mathrm{T}_i(M)$ *is the maximal submodule of* M *with* δ*-dimension less or equal to* i*.*
5. *If* $\delta(M) = 0$ *then* M *is finite.*
6. $E^{k+j(M)+1}E^{k+j(M)}E^{j(M)}(M) = 0$ *for all* $k \geq 1$*.*

Proof: Except for 1 (a), and 4, these properties are all proved in [Bj1] or they are trivial(3 (a) is just the Auslander condition and 3 (b) is a consequence of it by 2.): Prop. 1.21 (for 1 (b)), 1.16 (for 2), Prop. 1.18 (for 3 (c)), Remark before 1.19 (for 6), and 1.27 (for 5), while 1 (a) is proved in [Le, Cor. 4.3]

So let us prove 4: By 2, (a) is equivalent to $j(\mathrm{T}_i(M)) \geq d - i$ and this is true because of the Auslander-condition plus induction (compare the proof of 2, [Bj1] p.65). Now let M be a Λ-module with $\delta(M) = \delta$ and assume that there is a submodule N of M with $\delta(N) \leq \delta - 1$ but $N \not\subseteq \mathrm{T}_{\delta-1}(M)$. Then the submodule $N + \mathrm{T}_{\delta-1}(M)$ of M has dimension $\leq \delta - 1$ and therefore also the quotient $(N + \mathrm{T}_{\delta-1}(M))/\mathrm{T}_{\delta-1}(M)$ by 2.3. Hence,

$$\begin{aligned} 0 \neq (N + \mathrm{T}_{\delta-1}(M))/\mathrm{T}_{\delta-1}(M) &= \mathrm{T}_{\delta-1}((N + \mathrm{T}_{\delta-1}(M))/\mathrm{T}_{\delta-1}(M)) \\ &\subseteq \mathrm{T}_{\delta-1}(\mathrm{E}^{d-\delta}\mathrm{E}^{d-\delta}(M)) = 0 \end{aligned}$$

by 3 (c), which is a contradiction. So $\mathrm{T}_{\delta-1}(M)$ contains all submodules of dimension less or equal to $\delta - 1$ and (b) follows by induction. □

Proposition 2.5 *A Λ-module M with projective dimension $pd_\Lambda(M) = k$ has no non-trivial submodule of dimension less or equal to $d - k - 1$, i.e. $\mathrm{T}_{d-k-1}(M) = 0$. In particular, if $pd_\Lambda(M) \leq 1$, then M has no non-trivial pseudo-null submodule.*

Proof: See prop. 2.4, 1 (b).

□

The following theorem which has been proved in [Ve] allows us to apply Björk's theory in our context.

Theorem 2.6 *Let G be a compact p-adic analytic group without p-torsion. Then the completed group ring $\Lambda(G)$ is an Auslander regular ring.*

For the convenience of the reader we recall the main ingredients of the proof here. The idea of it consists of endowing Λ with a suitable filtration Σ and studying the associated graded ring $gr(\Lambda) = \bigoplus \Sigma_i/\Sigma_{i-1}$. Then we wish to apply the following criterion due to Björk:

Theorem 2.7 (Björk) *Assume that $gr(\Lambda)$ is an Auslander regular ring and that Σ satisfies the closure condition. Then Λ is an Auslander regular ring.*

By a filtration (in the sense of Björk) on a ring Λ we mean an increasing (!) sequence of additive subgroups $\Sigma_{i-1} \subseteq \Sigma_i \subseteq \Sigma_{i+1}$ satisfying $\bigcup \Sigma_i = \Lambda$ and $\bigcap \Sigma_i = 0$ and the inclusions $\Sigma_i\Sigma_k \subseteq \Sigma_{i+k}$ hold for all pairs of integers i and k. The main example on a local ring is the $\mathfrak{M}$ -adic filtration with $\Sigma_{-i} = \mathfrak{M}^i$ for all $i \geq 0$ (by convention, $\mathfrak{M}^0 = \Lambda$), where $\mathfrak{M}$ denotes the maximal ideal.

Then the closure condition just means that the additive subgroups $\Sigma_{i-m_1}u_1 + \cdots + \Sigma_{i-m_s}u_s$ and $u_1\Sigma_{i-m_1} + \cdots + u_s\Sigma_{i-m_s}$ are closed with respect to the topology induced by Σ for any finite subset $u_1, \ldots, u_s$ in Λ and all integers $i, m_1, \ldots, m_s$.

It is easily verified that the $\mathfrak{M}$-adic filtration on $\Lambda(G)$ satisfies this condition (cf. [Ve]). If we restrict ourselves to extra-powerful pro-p-groups (i.e. the relation $[G, G] \subseteq G^{p^2}$ holds) we are able to prove

Theorem 2.8 *Let G be a uniform and extra-powerful pro-p-group of dimension $dim(G) = r$. Then there is a $gr(\mathbb{Z}_p)$-algebra-isomorphism*

$$gr(\Lambda(G)) \cong \mathbb{F}_p[X_0, \ldots, X_r].$$

In particular, $gr(\Lambda(G))$ is a commutative regular Noetherian ring.

For the proof of the theorem we need some more terminology. Let G be a uniform pro-p-group with a minimal system of (topological) generators $\{x_1, \ldots, x_r\}$, i.e. $dim(G) = r$. Then the lower p-series is given by $P_1(G) = G,\ P_{i+1}(G) = (P_i(G))^p,\ i \geq 1$, in this case. This filtration defines a p-valuation $\omega : G \longrightarrow \mathbb{N}_{>0} \cup \{\infty\} \subseteq \mathbb{R}_{>0} \cup \{\infty\}$ of G in the sense of Lazard via $\omega(g) := \sup\{i \mid g \in P_i(G)\}$, which induces a filtration on $\mathbb{Z}_p[G]$, too (cf. [La, Chap. III, 2.3.1.2]).

Lemma 2.9 *The filtration on $\mathbb{Z}_p[G]$, induced by ω, is the $\mathfrak{M}_d$-adic one, where $\mathfrak{M}_d = \mathfrak{m} + I_d(G)$ with the augmentation ideal $I_d(G)$ of $\mathbb{Z}_p[G]$.*

Proof: Conferring the proof of Lemma III, (2.3.6) in [La] the induced filtration is given by the following ideals in $\mathbb{Z}_p[G]$, $n \in \mathbb{N} : A_n$ is generated as $\mathbb{Z}_p$-module by the elements $p^l(g_1 - 1) \cdots (g_m - 1)$ where $l, m \in \mathbb{N},\ g_i \in G$ and $l + \omega(g_1) + \ldots + \omega(g_m) \geq n$, whereas the $\mathfrak{M}_d$-adic filtration is defined by the ideals $\mathfrak{M}_d^n$, which are generated (over $\mathbb{Z}_p[G]$) by the elements $p^l(g_1 - 1) \cdots (g_m - 1)$, where $l, m \in \mathbb{N},\ g_i \in G$ and $l + m = n$. Since $\omega(g) \geq 1$ for all $g \in G$ the ideal $\mathfrak{M}_d^n$ is obviously contained in A_n. The converse is a consequence of the following

Claim: Let $g \in G$ with $\omega(g) = t \geq 1$, then $g - 1 \in \mathfrak{M}_d^t$.

Since G is uniform the map $G \longrightarrow P_t(G)$ which assigns $g^{p^{t-1}}$ to g is surjective (cf. [DSMS, lemma 4.10]), i.e. there is an element $h \in G$ with $g = h^{p^{t-1}}$. Writing

$$g - 1 = (1 + (h-1))^{p^{t-1}} - 1 = \sum_{k \geq 1} \left(\begin{array}{c} p^{t-1} \\ k \end{array} \right) (h-1)^k$$

one verifies that $g - 1 \in \mathfrak{M}_d^t$, because $v_p(\left(\begin{array}{c} p^{t-1} \\ k \end{array} \right)) = t - 1 - v_p(k) \geq t - k$, i.e. $\left(\begin{array}{c} p^{t-1} \\ k \end{array} \right) (h-1)^k \in \mathfrak{M}_d^t$. □

Lemma 2.10 *The $\mathfrak{M}_d$-adic filtration on $\mathbb{Z}_p[G]$ induces the $\mathfrak{M}$-adic filtration on $\mathbb{Z}_p[[G]]$.*

Proof: See [Ve]. □

Now we can prove theorem 2.8.

Proof: Since $gr(G) = \bigoplus P_i(G)/P_{i+1}(G)$ is a Lie algebra, which is free of rank r as $gr(\mathbb{Z}_p)$-module, we get the following inclusion:

$$\begin{aligned} gr(G) \subseteq Ugr(G) &\cong gr(\mathbb{Z}_p[G]) \\ &\cong gr(\mathbb{Z}_p[[G]]), \end{aligned}$$

where the first equation holds cf. [La, Chap. III, 2.3.3] and $Ugr(G)$ is the enveloping algebra of the Lie algebra $gr(G)$, whereas the second one is a consequence of lemma 2.10. But according to [Wil, Theorem 8.7.7] the graded ring $gr(\mathbb{Z}_p[[G]])$ is commutative (G is assumed to be extra-powerful), i.e.

$$Ugr(G) \cong gr(\mathbb{Z}_p)[X_1, \dots, X_r] \cong \mathbb{F}_p[X_0, \dots, X_r]$$

□

As p-adic analytic group G posses an open characteristic subgroup N which is an uniform, extra-powerful pro-p-group (cf. [DSMS, Cor. 9.36] and [Wil, Prop. 8.5.3]), by the theorem of Björk and Theorem 2.8, $\Lambda(N)$ is an Auslander regular ring, because $gr(\mathbb{Z}_p[[N]])$ has this property as a regular commutative Noetherian ring (cf. [Bj2, pp. 65-69]). But $\mathrm{E}^i_{\Lambda(G)}(M) \cong \mathrm{E}^i_{\Lambda(N)}(M)$ as $\Lambda(N)$-modules for any $\Lambda(G)$-module M, by which the Auslander-condition is easily verified. This proves theorem 2.6.

3 Jannsen's Homotopy Theory

In this section we briefly recall Jannsen's homotopy theory for the convenience of the reader. We will not give a full account of it but only what we shall need later on. We refer to the original paper [Ja1] or Chapter V of [NSW] for complete exposition. Let Λ be a Noetherian ring. Denote by $\Lambda - mod$ the category of finitely generated Λ-modules with usual Λ-linear homomorphisms as morphisms. From this category is made another category called homotopy category or stable category of $\Lambda - mod$, denoted $Ho(\Lambda)$. The objects are the same as in $\Lambda - mod$ but for objects M and N the set of morphisms is given by

$$[M, N] = \mathrm{Hom}_{Ho(\Lambda)}(M, N) := \mathrm{Hom}_{\Lambda - mod}(M, N)/\{f : f \simeq 0\}.$$

Here a Λ-homomorphism $f : M \to N$ is defined to be homotopic to zero, written $f \simeq 0$, if f factors through a projective Λ-module, that is there exists a projective Λ-module P and homomorphisms $g : M \to P$ and $h : P \to N$ such that $f = hg$. If M is isomorphic to N in the category $Ho(\Lambda)$, we say M is homotopically equivalent to N and write $M \simeq N$. There is the following fact:

$M \simeq N$ if and only if $M \oplus P \cong N \oplus Q$ in $\Lambda - mod$ for some finitely generated projective Λ-modules P and Q.

Therefore, for instance, projective dimension makes sense in the category $Ho(\Lambda)$. However, it is not an abelian category in general. To see this, suppose Λ is an integral domain. Consider the obvious exact sequence $0 \to \Lambda \xrightarrow{\times p} \Lambda \to \Lambda/p \to 0$. If the category $Ho(\Lambda)$ was abelian, we would have the following commutative diagram and the snake lemma:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \xrightarrow{\times p} & \Lambda & \longrightarrow & \Lambda/p & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \simeq} & & \uparrow{\scriptstyle \simeq} & & \uparrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & 0 & \xrightarrow{\times p} & 0 & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

Note $\Lambda \simeq 0$ since Λ itself is of course projective. This would imply that ϕ was also homotopical equivalence and hence $\Lambda/p \simeq 0$, which is absurd since Λ/p is neither 0 nor projective.

Jannsen defines three functors on the category $Ho(\Lambda)$. The first one is called the "loop space functor" Ω: For a finitely generated Λ-module M, we take a surjective homomorphism from a projective module P. Write the map $f : P \to M$. Then define $\Omega M := \mathrm{Ker}(f)$. This is easily checked to be determined uniquely in $Ho(\Lambda)$ up to isomorphism.

Next we recall the definition of the "transpose functor" D. For a finitely generated Λ-module M, take any projective resolution $P_1 \to P_0 \to M \to 0$ (exact). Then we define DM as the cokernel of the induced map $(P_0)^+ \to (P_1)^+$. This is well defined, i.e., it determines the unique object in $Ho(\Lambda)$ (up to isomorphism). Finally, he defines the "suspension functor" Σ, but we can define it via the earlier functors by $\Sigma := D\Omega D$.

It is easily verified that $D^2 = 1$. Also,if M has projective dimension less than 2, then $DM \simeq \mathrm{E}^1(M)$. These properties will be found useful as well as the following exact sequence([Ja1]):

$$0 \to \mathrm{E}^1(DM) \to M \stackrel{\phi_M}{\to} M^{++} \to \mathrm{E}^2(DM) \to 0. \tag{1}$$

Recall that a finitely generated Λ-module M is called reflexive if the map ϕ_M in the sequence (1) is an isomorphism.

Lemma 3.1 *Assume Λ has no zero divisors. Let M be any finitely generated Λ-module. Then the set of all torsion elements in M forms a Λ-submodule of M, and it is isomorphic to $E^1(DM)$.*

Proof: From the conditions on Λ follows that it has a unique quotient field (see, e.g., [Bj1] Ch 1, 8.2). This makes it possible to define Λ-rank. Then it is checked that M and M^{++} have the same Λ-rank. Hence $\mathrm{E}^1(DM)$ is exactly the set of all torsion elements in M. □

This observation caused Auslander and Bridger to suggest that the module $\mathrm{E}^1(DM)$ should be considered as torsion submodule of M in general, even if Λ has zero divisors:

Definition 3.2 *A Λ-module M is called* Λ-torsion module *if $\phi_M \equiv 0$, i.e. if* $\mathrm{tor}_\Lambda M := \mathrm{E}^1(DM) = M$. *We say that M is* Λ-torsion-free *if* $\mathrm{E}^1(DM) = 0$.

For $\Lambda = \Lambda(G)$ where G is a p-adic Lie group this definition means the following: First let us recall the fact that if G is any pro-p group and has no element of order p, then $\Lambda(G)$ has no divisors of zero(see [DSMS]). Then a finitely generated Λ-module M is a Λ-torsion module if and only if M is a $\Lambda(G')$-torsion module (in the strict sense) for some open pro-p subgroup $G' \subseteq G$ such that $\Lambda(G')$ is without zero divisors. Indeed, we have an isomorphism $\mathrm{E}^1_{\Lambda(G)}(D_{\Lambda(G)}M) \cong \mathrm{E}^1_{\Lambda(G')}(D_{\Lambda(G')}M)$ of $\Lambda(G')$-modules by [Ja1] Lemma 2.3 (and the analoguous statement for DM).

From now on we assume that Λ is an Auslander regular ring. The following proposition generalizes Proposition (5.1.8) in [NSW].

Proposition 3.3 *Assume Λ has no zero divisors. Let M be a finitely generated torsion-free Λ-module. Then there exists an injective homomorphism of M into a reflexive Λ-module with a pseudo-null cokernel.*

Proof: Since M is a finitely generated torsion-free Λ-module, by Lemma 3.1 we have $\mathrm{E}^1(DM) = 0$ and hence the following exact sequence

$$0 \to M \to M^{++} \to \mathrm{E}^2(DM) \to 0.$$

But $\mathrm{E}^2(DM)$ is pseudo-null by Proposition 2.4, 3 (b). To complete, we have to show M^{++} is reflexive. Actually we will show that M^+ is reflexive (this itself is a generalization of Corollary (5.1.3) in [NSW]). Let $N := \mathrm{E}^0(M)$ and and apply Proposition 2.4.6 to conclude that $\bigoplus_{k\geq 1} \mathrm{E}^{k+1}\mathrm{E}^k(N) = \bigoplus_{k\geq 1} \mathrm{E}^{k+1}\mathrm{E}^k\mathrm{E}^0(M) = 0$, i.e. $Q_d(N) = 0$. Since we already know by 2.4.3(c) that N is of pure dimension d (if $N \neq 0$) the statement follows considering 2.4.1(a). □

Proposition 3.4 *Let M be a finitely generated Λ-module such that $E^0(M) = 0$. Then M is pseudo-null if and only if $E^1(M) = 0$.*

Proof: Since $\mathrm{E}^0(M) = 0$, $\mathrm{E}^1(M) = 0$ is equivalent to $j(M) \geq 2$, and this is equivalent to M being pseudo-null by Proposition 2.4, 2. □

Remark. Let G be a p-adic analytic group, G' a uniform open subgroup of G and $\Lambda = \mathbb{Z}_p[[G']]$. Let M be a pseudo-null Λ-module. Then there exists a torsion-free Λ-module L of projective dimension ≤ 1 such that $M \simeq DL \simeq \mathrm{E}^1(L)$. By the above proposition, $\mathrm{E}^1(M) = 0$. Hence $\mathrm{E}^1\mathrm{E}^1(L) = 0$, which means L is torsion-free. The proposition also immediately implies an isomorphism $\mathrm{E}^1(M) = \mathrm{E}^1(M/T_{pn}(M))$, where $T_{pn}(M)$ denotes the maximal pseudo-null submodule of a finitely generated Λ-module M.

We end this section with the following observation, which was independently noticed and proved by R. Sujatha([Su]).

Proposition 3.5 *Let $\Lambda = \Lambda(G)$ be a completed group algebra of a p-adic analytic group G of dimension r without elements of order p. Let M be a $\Lambda(G)$-module, which is a finitely generated as a $\mathbb{Z}_p$-module. Then $\delta(M) \leq 1$. In particular, if $r > 1$, M is pseudo-null.*

Proof: It is enough to show $j(M) \geq r$ by Proposition 2.4 (note that the dimension of Λ is $d = r + 1$). For this we need to see $\mathrm{E}^i(M) = 0$ for all $i \leq r - 1$. But this follows from 2.6 of [Ja1] or (5.4.15) of [NSW]. □

A very interesting case of such an M that Sujatha considers is the Tate module of an abelian variety A with Tate twist: $M = T_p(A)(n)$, with G the image of Galois in the automorphism group of $T_p(A)$ (see [Su] for an important conclusion of this).

4 The Powerful Diagram

In this section we shall generalize some of Jannsen's work in [Ja1].

4.1 Fox-Lyndon Resolution and Twists

Let $\mathcal{G}$ be a pro-$\mathcal{C}$ group topologically of finite type, where $\mathcal{C}$ is a class of finite groups closed under taking subgroups, homomorphic images and group extensions, i.e. $\mathcal{G}$ is the projective limit of an appropriate inverse system in $\mathcal{C}$. Suppose that $\{x_1, \cdots, x_d\}$ is a set of generators of $\mathcal{G}$. Then there is a surjective homomorphism from a free pro-$\mathcal{C}$ group $\mathcal{F}(d)$ of rank d to $\mathcal{G}$ and we get an exact sequence

$$0 \to \mathcal{N} \to \mathcal{F}(d) \to \mathcal{G} \to 0$$

where $\mathcal{N}$ is defined as the kernel. This is called a free presentation of $\mathcal{G}$ and $\mathcal{N}^{ab}(p)$ is called the *p-relation module of G*.

In general, $\mathcal{N}^{ab}(p)$ fits into the following exact sequence, which is called Fox-Lyndon resolution associated with the above free representation of $\mathcal{G}$:

$$0 \to \mathcal{N}^{ab}(p) \to \Lambda(\mathcal{G})^d \to \Lambda(\mathcal{G}) \to \mathbb{Z}_p \to 0. \tag{2}$$

Hence, if $cd_p(\mathcal{G}) \leq 2$, then $\mathcal{N}^{ab}(p)$ is a projective $\Lambda(\mathcal{G})$-module.

Furthermore, the augmentation ideal $I(\mathcal{F})$, i.e. the kernel of $\Lambda(\mathcal{F}) \to \mathbb{Z}_p$, is a free $\Lambda(\mathcal{F})$-modules of rank d:

$$I(\mathcal{F}) \cong \Lambda(\mathcal{F})^d \tag{3}$$

(for a proof of these facts, see [NSW] Chap V.6).

Now we are going to study certain "twists" of $\Lambda(\mathcal{G})$-modules. So let A be a p-divisible p-primary abelian group of finite $\mathbb{Z}_p$-corank r with a continuous action of $\mathcal{G}$.

Definition 4.1 *For a finitely generated $\Lambda(\mathcal{G})$-module M, we define*

$$M[A] := \mathrm{Hom}_{\mathbb{Z}_p, cont}(M, A)^\vee = M \otimes_{\mathbb{Z}_p} A^\vee,$$

where we recall that $A^\vee = \mathrm{Hom}_{\mathbb{Z}_p, cont}(A, \mathbb{Q}_p / \mathbb{Z}_p)$.

$M[A]$ has the usual Λ-action, i.e. $\mathcal{G}$ acts diagonally on the tensor product. Note that this twist defines an exact functor.

Lemma 4.2 [2] *The module $\Lambda[A]$ is a free Λ-module of rank r.*

Proof: Fix an isomorphism of abelian groups $\phi : A^\vee \cong {\mathbb{Z}_p}^r$ and, for pairs (U, m) consisting of an $m \in \mathbb{N}$ and an open normal subgroup $U \trianglelefteq \mathcal{G}$ such that U acts trivially on $A^\vee / p^m$, consider the well-known isomorphism of Λ-modules

$$\mathbb{Z}_p[\mathcal{G}/U] \otimes_{\mathbb{Z}_p} (A^\vee)/p^m \cong \mathbb{Z}_p[\mathcal{G}/U] \otimes_{\mathbb{Z}_p} {\mathbb{Z}_p}^r/p^m,$$

[2] We thank Alexander Schmidt for drawing our attention to the fact that $\Lambda[A]$ should not only be projective but even free.

which sends $gU \otimes (a + p^m A^\vee)$ to $gU \otimes (\phi(g^{-1}a) + p^m {\mathbb{Z}_p}^r)$. It is easily seen that these isomorphisms form an compatible system, i.e.

$$\begin{aligned}
\Lambda \otimes_{\mathbb{Z}_p} A^\vee &= \Lambda \widehat{\otimes}_{\mathbb{Z}_p} A^\vee \\
&= \varprojlim_{(U,m)} \mathbb{Z}_p[\mathcal{G}/U] \otimes_{\mathbb{Z}_p} (A^\vee)/p^m \\
&= \varprojlim_{(U,m)} \mathbb{Z}_p[\mathcal{G}/U] \otimes_{\mathbb{Z}_p} {\mathbb{Z}_p}^r/p^m \\
&= \varprojlim_{U,m} \mathbb{Z}_p/p^m[\mathcal{G}/U]^r \\
&= \Lambda^r.
\end{aligned}$$

□

From this lemma, it follows that if P is a projective Λ-module, then so is $P[A]$.

4.2 The Diagram

Let K be a number field. Let V be a finite dimensional vector space over $\mathbb{Q}_p$, which is endowed with a continuous action of $G_K = G(\bar{\mathbb{Q}}/K)$, and let T be a $\mathbb{Z}_p$-lattice in V stable under the action of G_K. By A we denote the quotient $A = V/T$ unless otherwise stated. Define dual of these as follows:

$$T^* = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1)), V^* = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1)), A^* = V^*/T^* = \varinjlim \mathrm{Hom}(A_{p^j}, \mu_{p^\infty}).$$

A typical example we have in mind is

$$T = T_n^i := H_{et}^i(X \times \bar{K}, \mathbb{Z}_p(n))/torsion$$

where X is a proper smooth scheme over K. Then

$$V = H_{et}^i(X \times \bar{K}, \mathbb{Q}_p(n)) := T \otimes \mathbb{Q}_p;$$

$$A = V/T = \text{maximal } p\text{-divisible subgroup of } H_{et}^i(X \times \bar{K}, \mathbb{Q}_p / \mathbb{Z}_p(n)).$$

In particular, and this is our most concerning case, $H_{et}^1(X \times \bar{K}, \mathbb{Z}_p(1)) \cong T_p(\mathrm{Pic}^0(X_{/K}))$, where $\mathrm{Pic}^0(X_{/K}))$ denotes the Picard variety of X and T_p denotes the (p-adic) Tate module. Of course, $H_{et}^1(X \times \bar{K}, \mathbb{Z}_p(1)) \cong T_p(X')$ if X is an abelian variety over K (X' is the dual abelian variety of X).

Let A be as above. The extension $K(A)/K$ is defined by the kernel of $\rho : G_K \to \mathrm{Aut}(V) = GL_d(\mathbb{Q}_p)$, where $d = \dim_{\mathbb{Q}_p}(V)$. Therefore $K(A)/K$ is a Galois extension with $G(K(A)/K) \cong G_K/\mathrm{Ker}(\rho)$. Since $GL_d(\mathbb{Z}_p)$ is a compact p-adic Lie group and any closed subgroup of it is again a compact p-adic Lie group, $G(K(A)/K)$ is also a compact p-adic Lie group. Hence $K(A)/K$ is a p-adic Lie extension. The finite Galois extensions $K(A_{p^n})$, $n = 1, 2, \ldots$, of K are defined similarly, where $A_{p^n} = A[p^n]$ denotes the kernel of $A \xrightarrow{p^n} A$. We put $K_0 = K(A_p)$ and $K_n = K(A_{p^{n+1}})$. Clearly $K(A) = \cup_n K_n$.

By $S(K)$ we denote a set of places of K containing each prime above p and every archimedian place and every place whose inertia group acts nontrivially on V. *We*

always assume that $S(K)$ is finite. In another words, only a finite number of places of K ramify in $K(A)$ (see below for the definition of $K(A)$). $S_f(K)$ is the set of all finite places in $S(K)$ and $S_p(K)$ is $\{v \in S_f(K) : v \mid p\}$. By K_S we denote the maximal S-ramified extension of K.

Definition 4.3 *We say that an extension K_∞/K is a* p-adic Lie extension *if it is a Galois extension and the Galois group* $\mathrm{Gal}(K_\infty/K)$ *is a compact p-adic Lie group. If it is a pro-p Lie group, we say K_∞/K is a pro-p Lie extension. Throughout this chapter, whenever we consider a p-adic Lie extension K_∞ of a number field K, we always assume that K_∞ is contained in K_S.*

From now on we are in the following situation. We fix V and A once and for all. Let K be a finite extension of $\mathbb{Q}$ (or of $\mathbb{Q}_\ell$ including the case $\ell = p$) and by K' we denote an intermediate field of K_0/K determined by a p-Sylow subgroup of $G(K(A)/K)$. Let Ω be the maximal S-ramified p-extension of $K(A)$ (respectively K_0). Let us denote $G(\Omega/K)$ by $\mathcal{G}$ and $G(\Omega/K')$ by $\mathcal{G}'$.

Lemma 4.4 (i) *The extension Ω/K is Galois.*

(ii) *The profinite group $\mathcal{G}$ is topologically finitely generated.*

(iii) $K(A) \subset \Omega$.

(iv) $cd_p(\mathcal{G}) \leq 2$.

Proof: (i) This follows from the maximality of Ω and $K(A)/K$ being Galois.

(ii) Because we have an exact sequence $1 \to G(\Omega/K_0) \to \mathcal{G} \to G(K_0/K) \to 1$ with both $G(\Omega/K_0)$ and $G(K_0/K)$ finitely generated by a theorem of Shafarevich.

(iii) Obvious.

(iv) Since $cd_p(G_S(K)) \leq 2$ (recall we always assume that p is odd), $H^3(G_S(K), \mathbb{Z}/p\mathbb{Z}) = 0$. Since $H^3(G_S(K), \mathbb{Z}/p\mathbb{Z}) = H^3(\mathcal{G}', \mathbb{Z}/p\mathbb{Z})$, $cd_p(\mathcal{G}') \leq 2$. For any p-primary $\mathcal{G}$-module B, the corestriction map $H^n(\mathcal{G}', B) \to H^n(\mathcal{G}, B)$ is surjective for all n. Hence $cd_p(\mathcal{G}) \leq 2$.

□

Let K_∞ be a p-adic Lie extension of K contained in Ω with Galois group $G = G(K_\infty/K)$. Put $\mathcal{H} = G(\Omega/K_\infty)$. We have the following commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{H} & \longrightarrow & \mathcal{G} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \| & & \\
1 & \longrightarrow & \mathcal{R} & \longrightarrow & \mathcal{F}(d) & \longrightarrow & G & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & & & \\
 & & \mathcal{N} & = & \mathcal{N} & & & &
\end{array}$$

Here, as before $\mathcal{N}$ denotes the kernel of $\mathcal{F}(d) \to \mathcal{G}$, and we define $\mathcal{R}$ to be the kernel of the natural map $\mathcal{F}(d) \to G$ obtained by composing the previous map with $\mathcal{G} \to G$.

Letting A as before, we recall $M[A]$ is defined to be $M \otimes A^\vee$ for any finitely generated $\Lambda(\mathcal{G})$-module M. As A is now fixed, we shall write $M^\#$ for $M[A]$. We have an exact sequence

$$0 \to I(\mathcal{G})^\# \to \Lambda(\mathcal{G})^\# \to A^\vee \to 0. \tag{4}$$

By Lemma 4.2, $\Lambda(\mathcal{G})^\#$ is a projective $\Lambda(\mathcal{G})$-module. Hence we have the following exact sequence.

$$0 \to H_1(\mathcal{H}, A^\vee) \to (I(\mathcal{G})^\#)_\mathcal{H} \to (\Lambda(\mathcal{G})^\#)_\mathcal{H} \to (A^\vee)_\mathcal{H} \to 0. \tag{5}$$

We introduce the following notation:

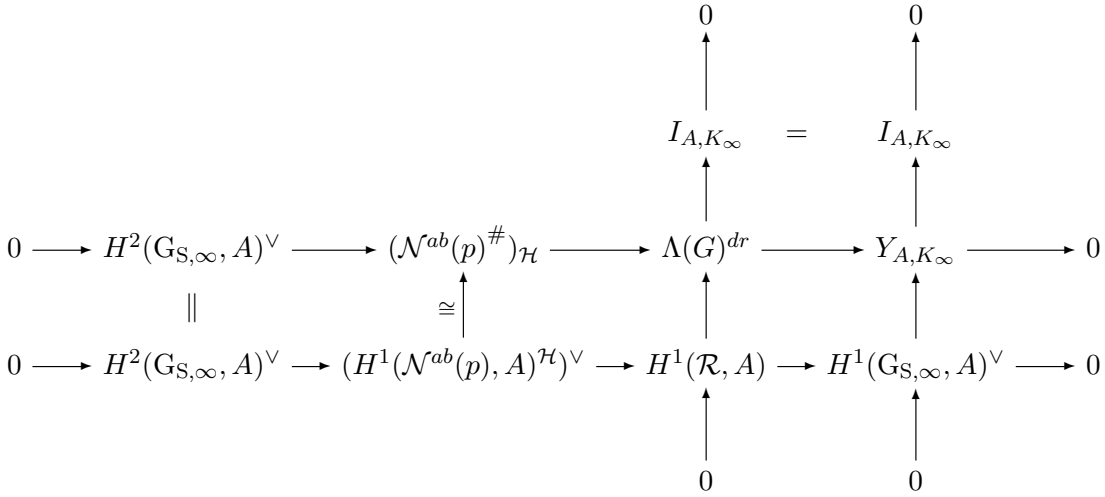
- $X = X_{A,K_\infty} = H_1(\mathcal{H}, A^\vee)$.
- $Y = Y_{A,K_\infty} = (I(\mathcal{G})^\#)_\mathcal{H}$.
- $I = I_{A,K_\infty} = \mathrm{Ker}((\Lambda(\mathcal{G})^\#)_\mathcal{H} \to (A^\vee)_\mathcal{H})$.

Thus the exact sequence (5) gives the exact sequence

$$0 \to X \to Y \to I \to 0. \tag{6}$$

The next lemma is very powerful in applications, and generalizes Lemma 4.3 of [Ja1].

Lemma 4.5 *Under the above situation, there is the following commutative exact diagram of $\Lambda(G)$-modules (recall $r = \mathbb{Z}_p$-rank of $A^\vee$).*



Furthermore, $(\mathcal{N}^{ab}(p)^\#)_\mathcal{H}$ is a projective $\Lambda(G)$-module, and it is isomorphic to $(\mathcal{N}^{ab}(p)_\mathcal{H})^\#$ if the action of $\mathcal{H}$ on A is trivial.

Proof: 1. THE VERTICAL SEQUENCES.- The right one has already been obtained above after noting the isomorphisms (for all i):

$$H_i(\mathcal{H}, A^\vee) \cong H^i(G_S(K_\infty), A)^\vee.$$

From the exact sequence $0 \to I(\mathcal{F}(d))^{\#} \to \Lambda(\mathcal{F}(d))^{\#} \to A^{\vee} \to 0$, we obtain the following long exact sequence

$$0 = H_1(\mathcal{R}, \Lambda(\mathcal{F}(d))^{\#}) \to H_1(\mathcal{R}, A^{\vee}) \to I(\mathcal{F}(d))^{\#}{}_{\mathcal{R}} \to$$

$$\Lambda(\mathcal{F}(d))^{\#}{}_{\mathcal{R}} \to (A^{\vee})_{\mathcal{R}} \to 0.$$

But by Fox - Lyndon, $I(\mathcal{F}(d))^{\#}{}_{\mathcal{R}} \cong \Lambda(G)^{dr}$. So we have an exact sequence

$$0 \to H_1(\mathcal{R}, A^{\vee}) \to \Lambda(G)^{dr} \to \Lambda(G)^{r} \to (A^{\vee})_{\mathcal{R}} \to 0.$$

Now $(A^{\vee})_{\mathcal{R}} = (A^{\vee})_{\mathcal{H}}$ as N acts trivially on A, so the sequence

$$0 \to H_1(\mathcal{R}, A^{\vee}) \to \Lambda(G)^{dr} \to I \to 0. \tag{7}$$

is exact.

2. THE HORIZONTAL SEQUENCES. -(2.1) The upper one:

The Fox - Lyndon resolution for $1 \to \mathcal{N} \to \mathcal{F}(d) \to \mathcal{G} \to 1$ yields an exact sequence

$$0 \to \mathcal{N}^{ab}(p)^{\#} \to \Lambda(\mathcal{G})^{d\#} \to I(\mathcal{G})^{\#} \to 0. \tag{8}$$

Take $\mathcal{H}$ - homology and we have the following exact sequence

$$0 \to H_1(\mathcal{H}, I(\mathcal{G})^{\#}) \to \mathcal{N}^{ab}(p)^{\#}{}_{\mathcal{H}} \to (\Lambda(\mathcal{G})^{\#^d})_{\mathcal{H}} \to I(\mathcal{G})^{\#}{}_{\mathcal{H}} \to 0.$$

Since $H_1(\mathcal{H}, I(\mathcal{G})^{\#}) \cong H_2(\mathcal{H}, A^{\vee}) \cong H^2(\mathcal{H}, A)^{\vee}$, $\Lambda(\mathcal{G})^{\#^d}_{\mathcal{H}} \cong \Lambda(G)^{dr}$, hence the following is an exact sequence:

$$0 \to H^2(\mathcal{H}, A)^{\vee} \to \mathcal{N}^{ab}(p)^{\#}{}_{\mathcal{H}} \to \Lambda(G)^{dr} \to Y \to 0. \tag{9}$$

(2.2) The lower horizontal sequence:

The Hochschild-Serre spectral sequence for $1 \to \mathcal{N} \to \mathcal{R} \to \mathcal{H} \to 1$ gives

$$H_2(\mathcal{R}, A^{\vee}) \to H_2(\mathcal{H}, A^{\vee}) \to H_1(\mathcal{N}, A^{\vee})_{\mathcal{H}} \to H_1(\mathcal{R}, A^{\vee}) \to H_1(\mathcal{H}, A^{\vee}) \to 0.$$

As $\mathcal{R}$ is a closed subgroup of $\mathcal{F}$, $cd_p(\mathcal{R}) \leq cd_p(\mathcal{F}) = 1$, $H_2(\mathcal{R}, A^{\vee}) = 0$ while $H_1(\mathcal{N}, A^{\vee}) \cong \mathrm{Hom}(\mathcal{N}^{ab}(p), A)^{\vee} = \mathcal{N}^{ab}(p)^{\#}$, because $\mathcal{N}$ acts on A trivially. Since $cd_p(\mathcal{G}) \leq 2$ by lemma 4.4, $\mathcal{N}^{ab}(p)$ is a projective $\Lambda(\mathcal{G})$-module, i.e. $(\mathcal{N}^{ab}(p)^{\#})_{\mathcal{H}}$,too.

3. The commutativity of the diagram is clear. □

Remarks. 1. If $cd_p(G) = 1$ or if $cd_p(G) = 2$ and $(A^{\vee})_{\mathcal{H}}$ has no p-torsion, then it is seen from the above argument in the proof that $H_1(\mathcal{R}, A^{\vee})$ is a free $\Lambda(G)$-module: $H_1(\mathcal{R}, A^{\vee}) \cong \Lambda(G)^{(d-1)r}$.

2. In [Ja1] 5.4, the structure of $(\mathcal{N}^{ab}(p))_{\mathcal{H}}$ has been determined as follows:

$$(\mathcal{N}^{ab}(p))_{\mathcal{H}} \cong \bigoplus_{v \in S'_{\infty}(K)} \mathrm{Ind}_{G_v}^{G} \mathbb{Z}_p \bigoplus \Lambda(G)^{d-r_1(K)'-r_2(K)-1}$$

where $S'_\infty(K)$ is the set of real places of K which ramify in K_∞, and $r_1(K)'$ is the cardinality of $S'_\infty(K)$ and $r_2(K)$ is the number of complex places of K.

3. Lemma 4.5 also holds for local fields. In the local case we have $H^2(K_\infty, A) = 0$ and hence the projective dimension of Y is less than 2.

The following theorem generalizes the theorems of Nguyen-Quang-Do ([Ng]) and Greenberg ([Gr2]), who considered the case $G \cong \mathbb{Z}_p^k$, $A = \mathbb{Q}_p/\mathbb{Z}_p$, i.e. $X \cong G_S(K_\infty)^{ab}(p)$.

Theorem 4.6 *If $H^2(G_{S,\infty}, A) = 0$, then $H^1(G_{S,\infty}, A)^\vee$ has no nontrivial pseudo-null submodule.*

Proof: By the diagram, it is enough to show that Y has no nontrivial pesudo-null submodule. By the assumption $H^2(G_{S,\infty}, A) = 0$, we have $pd_\Lambda(Y) \leq 1$. Hence from Proposition 2.5 follows the theorem. □

Recall that there is the "weak Leopoldt conjecture" stating that if K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of K, then $H^2(G_{S,\infty}, A) = 0$ (e.g., [Gr3] or [Ja2]). As an important case of the theorem, we have the following

Corollary 4.7 *Let $\mathcal{A}$ be an abelian variety defined over a number field K. Let S be a finite set of places of K containing all primes above p and ∞ and all primes at which $\mathcal{A}$ has bad reduction. Put $K_\infty = K(\mathcal{A}[p^\infty])$. Then we have $H^1(G_S(K_\infty), \mathcal{A}[p^\infty])^\vee$ has no nonzero pseudo-null submodule.*

Proof: We need to show $H^2(G_S(K_\infty), \mathcal{A}[p^\infty]) = 0$. Since $H^2(G_S(K_\infty), \mathcal{A}[p^\infty]) = H^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^{dim\mathcal{A}}$ as abelian groups, we only need to show $H^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. First we check that K_∞ contains $K(\mu_{p^\infty})$. Let $\mathcal{A}'$ be its dual abelian variety. From the Galois equivariant Weil pairing $V_p(\mathcal{A}) \times V_p(\mathcal{A}') \to V_p(\mu_{p^\infty})$ we know that $K(\mathcal{A}[p^\infty], \mathcal{A}'[p^\infty])$ contains $K(\mu_{p^\infty})$. But $V_p(\mathcal{A})$ and $V_p(\mathcal{A}')$ are isomorphic as a Galois module since $\mathcal{A}$ is isogenious to $\mathcal{A}'$ over K. Hence $K(\mathcal{A}[p^\infty], \mathcal{A}'[p^\infty]) = K(\mathcal{A}[p^\infty])$. It is known that the weak Leopoldt conjecture holds ([NSW] Theorem (10.3.25)): $H^2(\mathrm{Gal}(F_S/F(\mu_{p^\infty})), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Hence we have $H^2(\mathrm{Gal}(F_S/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim_n H^2(\mathrm{Gal}(F_S/F_n(\mu_{p^\infty})), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. □

Definition 4.8 *Let K be either a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}$. Put $G_S(K) = G(K_S/K)$ (if K is a finite extension of $\mathbb{Q}_p$, then by K_S we mean an algebraic closure $\bar{K}$). Let F be an extension of K contained in K_S. Then we define*

$$Z = Z_A(F/K) := H^0(G_S(F), \varinjlim_n D_2(A_{p^n}))^\vee$$

where

$$D_2(A_{p^n}) = \varinjlim_{K \subset L \subset K_S} (H^2(L, A_{p^n}))^\vee$$

and the direct limit in $\varinjlim_n D_2(A_{p^n})$ is taken with respect to the p-th power map $A_{p^{n+1}} \xrightarrow{\mathrm{p}} A_{p^n}$.

The following is immediate from Tate local duality and Poitou-Tate global duality.

Lemma 4.9 (i) *If K is a finite extension of $\mathbb{Q}_p$ and F is an extension of K, then $Z_A(F/K) = A^*(F)^\vee$.*

(ii) *If K is a finite extension of $\mathbb{Q}$ and F is an extension of K contained in K_S, then*

$$Z \cong \varprojlim_{K \subset L \subset F} H^2(G_S(L), T_p A).$$

Proposition 4.10 *Let K be a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}$ and let K_∞ be a p-adic Lie extension of K. We keep the assumption above.*

(i) $Y_A \simeq DZ_A$.

(ii) $Z_A^+ = H^2(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$ *where* $\mathrm{G}_{\mathrm{S},\infty}$ *should be replaced by* K_∞ *if* K *is local.*

Proof: These are proved for $A = \mathbb{Q}_p / \mathbb{Z}_p$ (with trivial Galois action) in [Ja1]. The same proof works for a general A. However, let us use this place to correct the following misprint on p. 190 in [Ja1], which was pointed out to us by Jannsen himself. It should read as follows: For profinite groups H, G and Γ such that there is an exact sequence $1 \to H \to G \to \Gamma \to 1$, the following isomorphism holds for every finitely generated projective $\Lambda(G)$-module P;

$$(\mathrm{Hom}_{\Lambda(G)}(P, \Lambda(G)))_H \cong \mathrm{Hom}_{\Lambda(\Gamma)}(P_H, \Lambda(\Gamma)). \tag{10}$$

□

4.3 The Case $K(A) \subset K_\infty$

In the paper [Ja1], U. Jannsen has proved the following as a main theorem via homotopy theory of modules.

Theorem. *Let k be a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}$ and K/k a Galois extension with $G = \mathrm{Gal}(K/k)$. Put $\Lambda = \Lambda(G)$*[3].

(i) *Let k be a local field and let M be the maximal abelian p-extension of K. Then the Λ-module $X = \mathrm{Gal}(M/K)$ is homotopically determined by the Λ-module $\mu_K(p)$ and a canonical class $\chi \in H^2(G, \mu_K(p))^\vee$, where $\mu_K(p)$ is the group of p-power roots of unity in K.*

(ii) *Let k be a global field. Let $S \supseteq \{v|p\}$ be a finite set of places of k. Assume that K/k is unramified outside S, and let k_S (resp. M_S) be the maximal (resp. maximal abelian) S-ramified p-extension of k (resp.K). Then the Λ-module $X_S = \mathrm{Gal}(M_S/K)$ is homotopically determined by the Λ-module $W_S = H^0(\mathrm{Gal}(k_S/K), \mathrm{E}_2^{(p)})$ $-$where $E_2^{(p)}$ is the dualizing module of $\mathrm{Gal}(k_S/K)-$ and a canonical class $\chi \in H^2(G, W_S)^\vee$.*

In this section we assume $K(A) \subset K_\infty$. Then we can give a generalization of the above theorem of Jannsen as follows.

[3] In order for the Λ to be Noetherian, it may be necessary to restrict the extension K/k such as a p-adic Lie extension.

Theorem 4.11 *Let K be either a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{Q}$, K_∞/K a p-adic Lie extension such that $K(A) \subset K_\infty$, and A as before. Put $G = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \Lambda(G)$.*

(i) *Let K be a a finite extension of $\mathbb{Q}_p$ and put $X = H^1(K_\infty, A)^\vee$. Then the Λ-module X is homotopically determined by the Λ-module $A^*(K_\infty)$ and a class $\xi \in \mathrm{Ext}^2_\Lambda(A^\vee, A^*)^\vee$.*

(ii) *Let K be a finite extension of $\mathbb{Q}$. Let S be a finite set of places of K as explained above. Assume that K_∞/K is unramified outside S. Then the Λ-module $X_S = H^1(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$ is homotopically determined by the Λ-module Z_A and and a class $\xi \in \mathrm{Ext}^2_\Lambda(A^\vee, Z_A^\vee)^\vee$.*

Recall the notation $[M, N] = \mathrm{Hom}_{Ho(\Lambda)}(M, N) = \mathrm{Hom}_\Lambda(M, N)/\{f : f \simeq 0\}$ for finitely generated Λ-modules M, N. First we show the following

Lemma 4.12 *Let G and Λ be the same as in Theorem 4.11, and let M be a finitely generated Λ-module. Write $I = I(G)$. Then we have the following isomorphisms:*

$$[DM, I[A]] = \mathrm{Tor}_2^\Lambda(A^\vee, M) = \mathrm{Ext}^2_\Lambda(A^\vee, M^\vee)^\vee$$

where DM is transpose of M.

Proof: Take a projective presentation of $M : P_1 \to P_0 \to M \to 0$ and let N be the kernel of the map so that we have the following exact sequence: $0 \to N \to P_1 \to P_0 \to M \to 0$. We now show that $\mathrm{Tor}_2^\Lambda(A^\vee, M) = \mathrm{Ker}(N \otimes_\Lambda A^\vee \to P_1 \otimes_\Lambda A^\vee)$. In [Ja1], it is shown that $\mathrm{Tor}_2^{\Lambda(\mathcal{G})}(\mathbb{Z}_p, M) = \mathrm{Ker}(N \otimes_\Lambda \mathbb{Z}_p \to P_1 \otimes_\Lambda \mathbb{Z}_p)$. Hence the following is exact:

$$0 \to \mathrm{Tor}_2^{\Lambda(\mathcal{G})}(\mathbb{Z}_p, M) \to N \otimes_\Lambda \mathbb{Z}_p \to P_1 \otimes_\Lambda \mathbb{Z}_p.$$

As $(N \otimes_\Lambda \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} A^\vee \cong N \otimes_\Lambda A^\vee$ and $(P_1 \otimes_\Lambda \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} A^\vee \cong P_1 \otimes_\Lambda A^\vee$, noting also that $A^\vee$ is a free $\mathbb{Z}_p$-module (hence flat as a $\mathbb{Z}_p$-module), we see that the following is exact:

$$0 \to \mathrm{Tor}_2^{\Lambda(\mathcal{G})}(\mathbb{Z}_p, M) \otimes_{\mathbb{Z}_p} A^\vee \to N \otimes_\Lambda A^\vee \to P_1 \otimes_\Lambda A^\vee.$$

In [Ja1], it is also shown that $\mathrm{Tor}_2^{\Lambda(\mathcal{G})}(\mathbb{Z}_p, M) = [DM, I]$. Therefore we have to show $[DM, I] \otimes_{\mathbb{Z}_p} A^\vee = [DM, I[A]]$.

Firstly one checks $\mathrm{Hom}_\Lambda(DM, I) \otimes_{\mathbb{Z}_p} A^\vee = \mathrm{Hom}_\Lambda(DM, I \otimes_{\mathbb{Z}_p} A^\vee)$. Write $\mathrm{Hom}_0(M, N)$ for $\{f \in \mathrm{Hom}_\Lambda(M, N) : f \simeq 0\}$. Now the lemma is proved by looking at the following exact sequences:

$$0 \to \mathrm{Hom}_0(DM, I) \to \mathrm{Hom}(DM, I) \to [DM, I] \to 0$$

and

$$\mathrm{Hom}_0(DM, I) \otimes_{\mathbb{Z}_p} A^\vee = \mathrm{Hom}_0(DM, I \otimes_{\mathbb{Z}_p} A^\vee),$$

□

Now we prove Theorem 4.11. By Proposition 4.10 and Lemma 4.12 , in the local case we have $DY \simeq A^*(K_\infty)^\vee$; in the global case we have $DY \simeq \varprojlim H^2(G_S(K_n), T_pA)$. Recall we have the exact sequence

$$0 \to X \to Y \xrightarrow{\phi} I[A] \to 0.$$

This map ϕ from Y to $I[A]$ determines an element in

$$[Y, I[A]] = [DZ, I[A]] = \mathrm{Ext}^2_\Lambda(A^\vee, Z^\vee)^\vee$$

by Lemma 4.12. This finishes the proof.

Remark. To calculate $\mathrm{Ext}^2_\Lambda(A^\vee, Z^\vee)$, the following spectral sequence (base change of rings) may be useful sometimes:

$$E_2^{i,j} = \mathrm{Ext}^i_{\mathbb{Z}_p}(B, \mathrm{Ext}^j_\Lambda(\mathbb{Z}_p, N)) \Longrightarrow \mathrm{Ext}^{i+j}_\Lambda(B, N)$$

where B is a $\mathbb{Z}_p$-module and N a Λ-module. For instance, let N be a p- primary discrete G-module (eg. $N = A^*$). Then $\mathrm{Ext}^j_\Lambda(A^\vee, N)$ are p-torsion modules. We have an exact sequence:

$$\mathrm{Ext}^2_\Lambda((A[p])^\vee, N) \to \mathrm{Ext}^2_\Lambda(A^\vee, N) \xrightarrow{\mathrm{p}} \mathrm{Ext}^2_\Lambda(A^\vee, N).$$

Therefore if $\mathrm{Ext}^2_\Lambda((A[p])^\vee, N) = 0$, then $\mathrm{Ext}^2_\Lambda(A^\vee, N) = 0$. Assume $K_0 = K$. Then as Λ-modules, $A[p] \cong (\mathbb{Z}/p\,\mathbb{Z})^r$. From the spectral sequence $\mathrm{Ext}^i_{\mathbb{Z}_p}(\mathbb{Z}/p\,\mathbb{Z}, \mathrm{Ext}^j_\Lambda(\mathbb{Z}_p, N)) \Rightarrow \mathrm{Ext}^{i+j}_\Lambda(\mathbb{Z}/p\,\mathbb{Z}, N)$, we have

$$\mathrm{Ext}^2_\Lambda(\mathbb{Z}/p\,\mathbb{Z}, N) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}/p\,\mathbb{Z}, \mathrm{Ext}^2_\Lambda(\mathbb{Z}_p, N)) \tag{11}$$

Hence if $H^2(G, N) = 0$, then $\mathrm{Ext}^2_\Lambda(A^\vee, N) = 0$.

Examples. 1. Of course, if $A = \mathbb{Q}_p/\mathbb{Z}_p$ (with trivial Galois action), then $K(A) = K$ and Theorem 4.11 is the theorem of Jannsen at the beginning of this section.

2. Suppose $\mu_p \subset K$, $A = \mu_{p^\infty} (= \mathbb{G}_m(p))$ and $K_\infty = K(\mu_{p^\infty})$. Then $\mathrm{Ext}^2_\Lambda(\mu^\vee_{p^\infty}, Z^\vee) = \mathrm{Ext}^1_\Lambda(I^\#, Z^\vee) = 0$ since $I^\#$ is projective in this case (as is easily seen or see [Ja1]). Hence, in particular, if K is a finite extension of $\mathbb{Q}_p$, then X is determined only by $\mathbb{Z}_p$ in the stable category; one can show actually that $X \cong \Lambda^r \oplus \mathbb{Z}_p$ where r is free rank of X^{++} which is a free Λ-module.

3. Assume K is a finite extension of $\mathbb{Q}_p$. Let E be an elliptic curve over K. Let $A = E_{p^\infty}$. Put $X = H^1(K_\infty, E_{p^\infty})$. Assume $K(E[p]) = K$ and $K_\infty = K(E_{p^\infty})$ with $G = G(K_\infty/K)$ and $\Lambda = \Lambda(G)$. Suppose $dim(G) = 2$. Then $\mathrm{Ext}^2_\Lambda(E^\vee_{p^\infty}, E_{p^\infty}) = 0$. To show this, by the remark above, it is enough to show $H^2(G, E_{p^\infty}) = 0$. But by using Poincare duality, $H^2(G, E_{p^\infty}) = (\varprojlim_{i,n} H^0(G_i, E_{p^\infty}/p^n))^\vee = 0$. Hence in this case, X is homotopically determined by E_{p^∞}. In relation to this there is an exact sequence:

$$0 \to X \to X^{++} \to T_pE \to 0.$$

Note that $(\mathrm{E}^2(DX) =) \mathrm{Hom}_{\mathbb{Z}_p}({E_{p^\infty}}^\vee \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) = T_pE$.

Let us end this section by noting the following remark: In the proof of Lemma 4.5 is given a projective resolution of $A^\vee$ and from it we have a chain complex whose homology groups are $H^i(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$.

Corollary 4.13 *We keep the notation as before and assume $K(A) \subset K_\infty$. Then in the category of $\Lambda(\mathcal{G})$-modules (with usual Λ-linear homomorphisms as morphisms), there is a projective resolution of $A^\vee$:*

$$0 \to \mathcal{N}^{ab}(p)[A] \to \Lambda(\mathcal{G})[A]^d \to \Lambda(\mathcal{G})[A] \to A^\vee \to 0.$$

The following is a chain complex whose homology groups are $H^i(\mathrm{G}_{\mathrm{S},\infty}, A)^\vee$:

$$0 \to \mathcal{N}^{ab}(p)[A]_{\mathcal{H}} \to \Lambda(G)[A]^d \to \Lambda(G)[A] \to 0.$$

5 Nonexistence of Pseudo-Null Submodules

Let E be an elliptic curve over a number field F without complex multiplication (over $\bar{\mathbb{Q}}$). Let $E_{p^\infty} = \cup_{n\geq 1} E_{p^n}$ and $F_\infty = F(E_{p^\infty})$. Denote by G any open subgroup having no p-torsion of the Galois group $G(F_\infty/F)$. Recall the definition of the Selmer group:

$$\mathrm{Sel}_p(F_\infty, E) := \mathrm{Ker}(H^1(F_\infty, E_{p^\infty}) \to \prod_w H^1(F_{\infty,w}, E)) \tag{12}$$

where w runs over all places of F_∞ and $F_{\infty,w}$ means the union of the completions at F_∞ of all finite extensions of $\mathbb{Q}$ contained in F_∞. The Selmer group has a G-module structure through the usual G-action on $H^1(F_\infty, E_{p^\infty})$ (see below). In this section we shall prove that the Pontryagin dual of the Selmer group has no nonzero pseudo-null $\Lambda(G)$-submodule. However, if we have shown that it has no pseudo-null $\Lambda(U)$-module for some open subgroup U of G, then it will imply that it has no nonzero pseudo-null $\Lambda(G)$-submodule because, as was pointed out in the proof of Theorem 2.6, there is the following isomorphism of $\Lambda(U)$-modules:

$$\mathrm{Ext}^i_{\Lambda(G)}(M, \Lambda(G)) \cong \mathrm{Ext}^i_{\Lambda(U)}(M, \Lambda(U))$$

for any $\Lambda(G)$-module M and all $i \geq 0$ ([Ja1], Lemma 2.3). Recall that M does not contain any pseudo-null submodules if $\mathrm{E}^i\mathrm{E}^i(M) = 0$ for all $i \geq 2$. Therefore we may take $F_0 = F(E_p)$ as our base field instead of F and write $K = F_0$, $K_\infty = F_\infty$ and $G_0 = \mathrm{Gal}(K_\infty/K)$. We then regard E_{p^∞} as a G_K-module so that $H^1(K_\infty, E_{p^\infty})$ has the usual G_0-action: for $g \in G_0$, $\phi \in H^1(K_\infty, E_{p^\infty})$, any cocycle, and $\sigma \in G_{K_\infty}$, $(g\phi)(\sigma) := g\phi(\tilde{g}^{-1}\sigma\tilde{g})$, where $\tilde{g}$ is any lift of g to G_K. Denote by S the following set of places of K:

$$S = \{v : v|p\} \cup \{v : v|\infty\} \cup \{v : E \text{ has bad reduction at } v\}.$$

By K_S we denote the maximal S-ramified extension of K. Then we have the following exact sequence:

$$0 \to \mathrm{Sel}_p(K_\infty, E) \to H^1(G_{S,\infty}, E_{p^\infty}) \to \bigoplus_{v\in S} \mathrm{Coind}^G_{G_v} H^1(K_{v,\infty}, E)(p)$$

where $G_{S,\infty} = G(K_S/K_\infty)$ and $G_v = G(K_{v,\infty}/K_v)$, $K_{v,\infty} = K_v(E_{p^\infty})$.

Now assume that E has good reduction at all $v|p$. Then Coates and Greenberg ([CG]) showed the following isomorphism for $v|p$:

$$H^1(K_{v,\infty}, E)(p) \cong H^1(K_{v,\infty}, \widetilde{E}_{p^\infty})$$

where $\widetilde{E}_{p^\infty}$ is the G_v-module which sits in the following exact sequence:

$$0 \to \widehat{E}_{p^\infty} \to E_{p^\infty} \xrightarrow{g} \widetilde{E}_{p^\infty} \to 0$$

where g is the reduction map. If v does not divide p, then since $E(K_{v,\infty}) \otimes \mathbb{Q}_p \,/\, \mathbb{Z}_p = 0$ bu virtue of Mattuck's theorem, we have

$$H^1(K_{v,\infty}, E)(p) \cong H^1(K_{v,\infty}, E_{p^\infty})$$

by Kummer sequence. Hence the above exact sequence is written as follows:

$$0 \to \mathrm{Sel}_p(K_\infty, E) \to H^1(G_{S,\infty}, E_{p^\infty}) \xrightarrow{\phi} \bigoplus_{v \in S'} \mathrm{Coind}_{G_v}^G H^1(K_{v,\infty}, E_{p^\infty}) \oplus \bigoplus_{v|p} \mathrm{Coind}_{G_v}^G H^1(K_{v,\infty}, \widetilde{E}_{p^\infty}) \tag{13}$$

where S' denotes the subset of S which consists of all the primes that do not divide p. It is conjectured that the map ϕ above is surjective. Indeed, at least if $p \geq 5$, then it is equivalent to a generalized conjecture of Harris (See Conjecture 2.4 and Proposition 3.4 in [CH]).

Theorem 5.1 *Let E/F, K, and K_∞ be as above. Put $G_0 = G(K_\infty/K)$.*

Assume:

(i) *E has good reduction at all $v|p$, $v \in S$.*

(ii) *The map ϕ in the above exact sequence (13) is surjective.*

Then $\mathrm{Sel}_p(K_\infty, E)^\vee$ has no nonzero pseudo-null $\Lambda(G_0)$-submodule. Therefore it has no nonzero pseudo-null $\Lambda(G)$-submodule for any open p-adic Lie subgroup G without p-torsion of $\mathrm{Gal}(K_\infty/F)$.

In particular, the theorem holds, if E has good supersingular reduction at any $v|p$, because then $\mathrm{Sel}_p(K_\infty, E) \cong H^1(G_{S,\infty}, E_{p^\infty})$, see below.

We would like to prove the theorem in a slightly more general setting. First we recall Greenberg's Selmer group ([Gr2]). Let A be as before. Let K_∞/K be a pro-p Lie extension such that $G = G(K_\infty/K)$ has no elements of order p. Greenberg's Selmer group for this A over K_∞ is defined as follows:

$$\mathrm{Sel}(K_\infty, A) := \ker(H^1(K_\infty, A) \to \prod_{w \nmid p} H^1(K_{\infty,w}^{nr}, A) \bigoplus \prod_{w|p} H^1(K_{\infty,w}^{nr}, A/A_v)) \tag{14}$$

Here $K_{\infty,w}^{nr}$ is the maximal unramified extension of $K_{\infty,w}$ and A_v is a p-divisible G_v-submodule of A. The choice of A_v is rather subtle (see [Gr2] and [Sc2]). But we will not make this explicit here, since it does not matter for our purposes. *However, in the case $A = E_{p^\infty}$, we always take $A_v = \widehat{E}_{p^\infty}$ if E has ordinary reduction at v, and $A_v = E_{p^\infty}$ if E has supersingular reduction at v.* We write $\widetilde{A}_v$ for A/A_v. Denote by S

$$S = \{v : v|p\} \cup \{v : v|\infty\} \cup \{v : \text{the inertia group } I_w \text{ acts on } A \text{ nontrivially } (w|v)\}.$$

Then again we have the following exact sequence.

$$0 \to \mathrm{Sel}(K_\infty, A) \to H^1(G_{S,\infty}, A) \xrightarrow{\phi} \bigoplus_{v \in S'} \mathrm{Coind}_{G_v}^G H^1(K_{v,\infty}^{nr}, A) \oplus \bigoplus_{v|p} \mathrm{Coind}_{G_v}^G H^1(K_{v,\infty}^{nr}, \widetilde{A}_v). \tag{15}$$

We always assume that K_∞ is contained in K_S. We shall prove the following

Theorem 5.2 *Let K, A, S and K_∞/K be as above. Write $G = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \Lambda(G)$. Assume:*

(i) $H^2(G_{S,\infty}, A) = 0$;

(ii) *ϕ in the sequence (15) is surjective;*

(iii) $K_{v,\infty}^{nr} = K_{v,\infty}$ *(for simplicity) if $v \nmid p$ or if $v|p$ and $H^1(K_{v,\infty}, \widetilde{A}_v) \neq 0$;*

(iv) $\dim(G) > \dim(G_v) \geq 2$ *if $v \nmid p$;*

(v) *For any $v|p$ such that $H^1(K_{v,\infty}^{nr}, \widetilde{A}) \neq 0$, we assume* $\dim(G) > \dim(G_v) \geq 3$.

Then $\mathrm{Sel}(K_\infty, A)^\vee$ *has no nonzero pseudo-null $\Lambda(G)$-submodule.*

This will imply Theorem 5.1. For first it is easy to see $K_{v,\infty}^{nr} = K_{v,\infty}$. If E has supersingular good reduction at some $v|p$, then by Coates-Greenberg, we have $H^1(K_{v,\infty}, \widetilde{E}_{p^\infty}) = 0$. In the case of supersingular reduction at *any* $v|p$, we have actually $\mathrm{Sel}_p(K_\infty, E) = \mathrm{Sel}(K_\infty, E_{p^\infty}) = H^1(G_{S,\infty}, E_{p^\infty})$. So already by Theorem 4.6, $\mathrm{Sel}_p(K_\infty, E)^\vee$ has no nonzero pseudo-null submodule. If E has ordinary reduction at $v|p$, then by a result of Serre (see [Se2] IV-43), we have $\dim(G_v) = 3$ (see [CH] Lemma 5.1). Also if $v \nmid p$ and E has potentially multiplicative reduction at v, then $\dim(G_v) = 2$ and by a result of Serre-Tate ([ST] 2 Corollary 2) it does not occur that E has bad but potential good reduction at v. Finally we know $\dim(G) = 4$ and $H^2(G_{S,\infty}, E_{p^\infty}) = 0$ (Corollary 4.7).

Before beginning to prove Theorem 5.2, we would like to make sure that $\mathrm{Sel}(K_\infty, A)^\vee$ is not trivial. This follows, for instance, from

Proposition 5.3 *Under the same assumptions as in Theorem 5.2, the projective dimensions of $Sel(K_\infty, A)^\vee$ and $H^1(G_{S,\infty}, A)^\vee$ are the same and it is $dim(G) - 2$ if $A(K_\infty)^\vee$ has no finite submodule and $dim(G) - 1$ if $A(K_\infty)^\vee$ has a nonzero finite submodule.*

Proof: See [HO]. □

Put $U = \bigoplus_{v \in S'} \mathrm{Ind}_{G_v}^G H^1(K_{v,\infty}, A)^\vee \oplus \bigoplus_{v|p} \mathrm{Ind}_{G_v}^G H^1(K_{v,\infty}, \widetilde{A}_v)^\vee$, $X_S = H^1(G_{S,\infty}, A)^\vee$ and $X_f = \mathrm{Sel}(K_\infty, A)^\vee$. By the assumption (ii), we have the following exact sequence:

$$0 \to U \to X_S \to X_f \to 0. \tag{16}$$

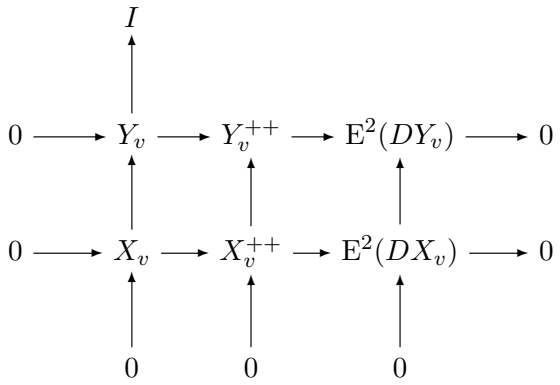
From now on, for simplicity of the argument, we assume that $A(K_\infty)$ has no nontrivial finite submodule.

Put $X_v = H^1(K_{v,\infty}, \widetilde{A_v})^\vee$ or $H^1(K_{v,\infty}, A)^\vee$, according to v being over p or not. Also with X_v we write Y_v for the $\Lambda(G_v)$-module Y in the diagram in Lemma 4.5.

Lemma 5.4 (i) *If $dim(G_v) \geq 2$, then X_v and Y_v are torsion-free. If $dim(G_v) > 2$, then X_v and Y_v are reflexive.*

(ii) *Suppose v does not divide p. If $dim(G_v) \geq 2$, then $X_v = 0$.*

Proof: (i) For the first statement, see [HO]. For the second statement of (i), consider the following commutative diagram:



Now if $\dim(G) > 2$, then $\mathrm{E}^2(DY_v) = \mathrm{E}^2((\widetilde{A}(K_{v,\infty})^*)^\vee) = 0$ by [Ja1] 2.6.

(ii) See [HO]. □

Lemma 5.5 *For a finitely generated $\Lambda(G_v)$-module M and any $i \geq 0$, we have an isomorphism:*

$$\mathrm{Ext}^i_{\Lambda(G)}(\mathrm{Ind}_{G_v}^G M, \Lambda(G)) = \mathrm{Ind}_{G_v}^G \mathrm{Ext}^i_{\Lambda(G_v)}(M, \Lambda(G_v)). \tag{17}$$

Proof: First we check that $\Lambda(G)$ is a flat $\Lambda(G_v)$-module. For it we just need to check that for any ideal $\mathfrak{a}$ of $\Lambda(G_v)$, the natural map $\mathfrak{a} \otimes_{\Lambda(G_v)} \Lambda(G) \to \Lambda(G)$ is injective. Write $G_n = G/U_n$, where U_n is a open normal subgroup, and $G_{n,v}$ for $G_v/(G_v \cap U_n)$. Then $\Lambda(G) = \varprojlim_n \mathbb{Z}_p[G_n]$ and $\Lambda(G_v) = \varprojlim_n \mathbb{Z}_p[G_{n,v}]$. Let f_n be the natural surjective map $\Lambda(G_v) \to \mathbb{Z}_p[G_{n,v}]$. Let $\mathfrak{a}$ be any (left, say) ideal of $\Lambda(G_v)$. Then $\mathfrak{a} = \varprojlim_n \mathfrak{a}_n$, where $\mathfrak{a}_n$ is the ideal of $\mathbb{Z}_p[G_{n,v}]$ generated by $f_n(\mathfrak{a})$. Then the following is exact since $\mathbb{Z}_p[G_n]$ is a projective $\mathbb{Z}_p[G_{n,v}]$-module:

$$0 \to \mathfrak{a}_n \otimes_{\mathbb{Z}_p[G_{n,v}]} \mathbb{Z}_p[G_n] \to \mathbb{Z}_p[G_n].$$

Take projective limit and we have

$$0 \to \varprojlim_n (\mathfrak{a}_n \otimes_{\mathbb{Z}_p[G_{n,v}]} \mathbb{Z}_p[G_n]) \to \varprojlim_n \mathbb{Z}_p[G_n].$$

But $\varprojlim_n (\mathfrak{a}_n \otimes_{\mathbb{Z}_p[G_{n,v}]} \mathbb{Z}_p[G_n]) \cong \mathfrak{a} \otimes_{\mathbb{Z}_p[[G_v]]} \mathbb{Z}_p[[G]]$ ([Br] Lemma A.4 and Lemma 2.1 (ii)). Hence the claim at the beginning. Now since $\Lambda(G)$ is flat over $\Lambda(G_v)$, we have the following isomorphism:

$$\mathrm{Hom}_{\Lambda(G_v)}(M, \Lambda(G_v)) \otimes_{\Lambda(G_v)} \Lambda(G) \cong \mathrm{Hom}_{\Lambda(G)}(M \otimes_{\Lambda(G_v)} \Lambda(G), \Lambda(G)).$$

Because completed tensor product $\widehat{\otimes}$ is right exact, $\mathrm{Ind}_{G_v}^G$ is an exact functor from the category of $\Lambda(G_v)$-modules to the category of $\Lambda(G)$-modules. Finally, to show the isomorphisms (17), use the definition of $\mathrm{Ext}^i_{\Lambda(G_v)}(M, \Lambda(G_v))$ by taking a free resolution of the finitely generated $\Lambda(G_v)$-module M.

$$0 \to \Lambda(G_v)^{r_n} \to \cdots \to \Lambda(G_v)^{r_1} \to \Lambda(G_v)^{r_0} \to M \to 0. \tag{18}$$

This yields a free resolution of $\mathrm{Ind}_{G_v}^{G} M$:

$$0 \to \Lambda(G_v)^{r_n} \otimes_{\Lambda(G_v)} \Lambda(G) \to \cdots \to \Lambda(G_v)^{r_1} \otimes_{\Lambda(G_v)} \Lambda(G) \to \Lambda(G_v)^{r_0} \otimes_{\Lambda(G_v)} \Lambda(G) \to \mathrm{Ind}_{G_v}^{G} M \to 0.$$

On the other hand, the resolution (18) gives rise to a chain complex:

$$0 \overset{\phi_{-1}}{\to} \mathrm{Hom}(\Lambda(G_v)^{r_0}, \Lambda(G_v)) \overset{\phi_0}{\to} \cdots \overset{\phi_{n-1}}{\to} \mathrm{Hom}(\Lambda(G_v)^{r_{n-1}}, \Lambda(G_v)) \overset{\phi_n}{\to} \mathrm{Hom}(\Lambda(G_v)^{r_n}, \Lambda(G_v)) \overset{\phi_{n+1}}{\to} 0$$

such that $\mathrm{Ext}^i(M, \Lambda(G_v)) := \mathrm{Ker}(\phi_i)/\mathrm{Im}(\phi_{i-1})$ for $i \geq 0$. As $\mathrm{Ind}_{G_v}^{G}$ is an exact functor, we have

$$\mathrm{Ext}^i(M, \Lambda(G_v)) \otimes_{\Lambda(G_v)} \Lambda(G) = (\mathrm{Ker}(\phi_i)/\mathrm{Im}(\phi_{i-1})) \otimes_{\Lambda(G_v)} \Lambda(G)$$

$$= (\mathrm{Ker}(\phi_i) \otimes_{\Lambda(G_v)} \Lambda(G))/(\mathrm{Im}(\phi_{i-1}) \otimes_{\Lambda(G_v)} \Lambda(G)) = \mathrm{Ext}^i(\mathrm{Ind}_{G_v}^{G} M, \Lambda(G)).$$

□

Lemma 5.6 (i) $E^i(X_S) = 0$ *for all* $i \neq 0, 1, dim(G) - 2$.
(ii) $E^{i+1}E^i(U) = 0$ *for any* $i \geq 1$.

Proof: (i) This follows from $pd(Y) \leq 1$ and so $\mathrm{E}^i(X_S) = \mathrm{E}^{i+2}(A(K_\infty)^\vee)$ for $i \geq 2$.
(ii) By Lemma 5.5 we have

$$\mathrm{Ext}^i_{\Lambda(G)}(U) = \bigoplus \mathrm{Ind}_{G_v}^{G} \mathrm{Ext}^i_{\Lambda(G_v)}(X_v).$$

hence for any $i \geq 2$, we have

$$\mathrm{E}^i_{\Lambda(G)}\mathrm{E}^i_{\Lambda(G)}(U) = \bigoplus \mathrm{Ind}_{G_v}^{G} \mathrm{E}^i_{\Lambda(G_v)}\mathrm{E}^{i+2}_{\Lambda(G_v)}(\widetilde{A}_v) = 0.$$

Now we show $\mathrm{E}^2\mathrm{E}^1(U) = 0$. We need to show $\mathrm{E}^2_{\Lambda(G_v)}\mathrm{E}^1_{\Lambda(G_v)}(X_v) = 0$. Write $\mathrm{E}^i = \mathrm{E}^i_{\Lambda(G_v)}$. We have an exact sequence $0 \to X_v \to Y_v \to I_v \to 0$. This gives $\mathrm{E}^1(I_v) \to \mathrm{E}^1(Y_v) \to \mathrm{E}^1(X_v) \to \mathrm{E}^2(I_v)$. But $\mathrm{E}^i(I_v) = 0$ for $i = 1, 2$ since $\dim(G_v) \geq 3$. Therefore $\mathrm{E}^2\mathrm{E}^1(Y_v) = \mathrm{E}^2\mathrm{E}^1(X_v)$. Since $pd(Y_v) \leq 1$, $\mathrm{E}^2\mathrm{E}^1(Y_v) = \mathrm{E}^2(DY_v)$. But this is zero since Y_v is reflexive. Therefore $\mathrm{E}^2\mathrm{E}^1(X_v) = 0$. □

We are going to show $\mathrm{E}^i\mathrm{E}^i(X_f) = 0$ for all $i \geq 2$. We will repeatedly use the fact that $\mathrm{E}^i\mathrm{E}^i(X_S) = 0$ for all $i > 1$, which is because X_S does not have nonzero pseudo-null submodules (Corollary 4.7 and Proposition 2.4, 1, (b)). Now suppose $i > 2$. We have an exact sequence

$$\mathrm{E}^{i-1}(X_S) \to \mathrm{E}^{i-1}(U) \to \mathrm{E}^i(X_f) \to \mathrm{E}^i(X_S) \to \mathrm{E}^i(U).$$

Assume $i = pd_\Lambda(X_S)(= \dim(G) - 2)$. Then we know by Lemma 5.6 and the last hypothesis in Theorem 5.2 that $\mathrm{E}^{i-1}(X_S) = \mathrm{E}^i(U) = 0$. Hence we get a short exact sequence $0 \to \mathrm{E}^{i-1}(U) \to \mathrm{E}^i(X_f) \to \mathrm{E}^i(X_S) \to 0$. This gives

$$\mathrm{E}^i\mathrm{E}^i(X_S) \to \mathrm{E}^i\mathrm{E}^i(X_f) \to \mathrm{E}^i\mathrm{E}^{i-1}(U).$$

We have $\mathrm{E}^i\mathrm{E}^i(X_S) = 0$ as noted above and $\mathrm{E}^i\mathrm{E}^{i-1}(U) = 0$ by Lemma 5.6. Hence $\mathrm{E}^i\mathrm{E}^i(X_f) = 0$. Since $i = pd_\Lambda(X_f)$ as well (Proposition 5.3), We also have $\mathrm{E}^n\mathrm{E}^n(X_f) = 0$ for all $n \geq pd_\Lambda(X_S)$.

If $2 < i < pd_\Lambda(X_S)$, then we have $\mathrm{E}^{i-1}(U) = \mathrm{E}^i(X_f)$. Hence $\mathrm{E}^i\mathrm{E}^i(X_f) = \mathrm{E}^i\mathrm{E}^{i-1}(U) = 0$.

Finally we have to show $\mathrm{E}^2\mathrm{E}^2(X_f) = 0$. Assume $\dim(G) = 4$. Consider the following long exact sequence

$$\mathrm{E}^1(X_f) \to \mathrm{E}^1(X_S) \to \mathrm{E}^1(U) \to \mathrm{E}^2(X_f) \to \mathrm{E}^2(X_S) \to \mathrm{E}^2(U).$$

We have $\mathrm{E}^2(U) = 0$ since $pd_\Lambda(U) \leq 1$. From this we make the following three short exact sequences:

$$0 \to B \to \mathrm{E}^2(X_f) \to \mathrm{E}^2(X_S) \to 0;$$
$$0 \to C \to \mathrm{E}^1(U) \to B \to 0;$$
$$0 \to D \to \mathrm{E}^1(X_S) \to C \to 0.$$

From the first sequence, we have an exact sequence

$$\mathrm{E}^2\mathrm{E}^2(X_S) \to \mathrm{E}^2\mathrm{E}^2(X_f) \to \mathrm{E}^2(B).$$

But $\mathrm{E}^2\mathrm{E}^2(X_S) = 0$. Hence $\mathrm{E}^2\mathrm{E}^2(X_f) = \mathrm{E}^2(B)$ since $\mathrm{E}^3\mathrm{E}^2(X_S) = \mathrm{E}^3\mathrm{E}^4(A^\vee(K_\infty)) = 0$. From the second sequence, we have an exact sequence

$$\mathrm{E}^1\mathrm{E}^1(U) \to \mathrm{E}^1(C) \to \mathrm{E}^2(B) \to \mathrm{E}^2\mathrm{E}^1(U).$$

But $\mathrm{E}^2\mathrm{E}^1(U) = 0$ by Lemma 5.6 and $\mathrm{E}^1\mathrm{E}^1(U) = 0$ as U is torsion free.

Therefore we get $\mathrm{E}^1(C) = \mathrm{E}^2(B)$. From the third sequence, we have an immersion:

$$0 \to \mathrm{E}^1(C) \hookrightarrow \mathrm{E}^1\mathrm{E}^1(X_S).$$

Claim: $\mathrm{tor}_\Lambda(X_S) = \mathrm{E}^1\mathrm{E}^1(X_S)$.

To show this, first we get $\mathrm{E}^1(Y) = \mathrm{E}^1(X_S)$ from the exact sequence $0 \to X_S \to Y \to I \to 0$ in the (powerful) diagram because $\mathrm{E}^{i-1}(I) = \mathrm{E}^i(A(K_\infty)^\vee) = 0$ for $i = 2, 3$ by the assumption $\dim(G) = 4$ and 2.6 of [Ja1] or (5.4.15) of [NSW] (recall we assume that $A(K_\infty)$ has no nontrivial finite submodule). But $pd_\Lambda(Y) \leq 1$, hence, as we noted in the section 3, we have $DY \simeq \mathrm{E}^1(Y)$. Therefore $\mathrm{tor}_\Lambda(X_S) = \mathrm{tor}_\Lambda(Y) = \mathrm{E}^1(DY) = \mathrm{E}^1(\mathrm{E}^1(Y)) = \mathrm{E}^1(\mathrm{E}^1(X_S))$.

We now have that $\mathrm{E}^1(C) = \mathrm{E}^2(B)$ and $\mathrm{E}^2(B)$ is a pseudo-null module by Proposition 2.4, 3, (b). But X_S has no pseudo-null submodule. Therefore $\mathrm{E}^2(B) = 0$, i.e., $\mathrm{E}^2\mathrm{E}^2(X_f) = 0$.

If $\dim(G) > 4$, the argument is similar. In this case $\mathrm{E}^2(X_S) = 0$, hence we have an exact sequence $0 \to V \to \mathrm{E}^1(X_f) \to \mathrm{E}^1(X_S) \to \mathrm{E}^1(U) \to \mathrm{E}^2(X_f) \to 0$ with some V. Split this into two exact sequences:

$$0 \to W \to \mathrm{E}^1(U) \to \mathrm{E}^2(X_f) \to 0;$$
$$0 \to V \to \mathrm{E}^1(X_S) \to W \to 0.$$

Then from the first sequence we have $\mathrm{E}^1\mathrm{E}^1(U) = 0 \to \mathrm{E}^1(W) \to \mathrm{E}^2\mathrm{E}^2(X_f) \to \mathrm{E}^2\mathrm{E}^1(U) = 0$. Hence $\mathrm{E}^1(W)$ is pseudo-null. From the second sequence we know that $\mathrm{E}^1(W)$ is a submodule of $\mathrm{tor}_\Lambda(X_S)$. Hence $\mathrm{E}^1(W) = 0$, and in consequence $\mathrm{E}^2\mathrm{E}^2(X_f) = 0$.

6 Structure as $\Lambda(H)$- and $\Lambda(C)$-Module

Let E, F, F_∞, G and $\mathrm{Sel}_p(F_\infty, E)$ be the same as at the beginning of the last section. By F_{cycl} we denote the cyclotomic $\mathbb{Z}_p$-extension $F(\mu_{p^\infty})$ of F, which is contained in F_∞ as we have seen. Putting $H = \mathrm{Gal}(F_\infty/F_{cycl})$ Coates and Howson have shown that under some conditions (see the assumptions in the theorem below), $\mathrm{Sel}_p(F_\infty, E)^\vee$ is finitely generated over $\Lambda(H)$ ([CH], Theorem 6.4). The question of John Coates was whether in this case the previous Theorem 5.1 could tell if the Iwasawa module $\mathrm{Sel}_p(F_\infty, E)^\vee$ has no $\Lambda(H)$-torsion. We answer this question with the following

Theorem 6.1 *Let E, F, F_∞, G, H and $\mathrm{Sel}_p(F_\infty, E)$ be as above. Assume the following:*

(i) $G = \mathrm{Gal}(F_\infty/F)$ is pro-p.

(ii) $Sel_p(F_{cycl}, E)^\vee$ is a finitely generated $\mathbb{Z}_p$-module.

Then $\mathrm{Sel}_p(F_\infty, E)^\vee$ is a torsion-free finitely generated $\Lambda(H)$-module.

Remark. Note that condition (ii) of the theorem is equivalent to
(ii)' $\mathrm{Sel}_p(F_{cycl}, E)^\vee$ is $\Lambda(\Gamma)$-torsion, where $\Gamma = G(F_{cycl}/F)$, and the μ-invariant of $\mathrm{Sel}_p(F_{cycl}, E)^\vee$ is zero.

The point is to show that the set of all the $\Lambda(H)$-torsion elements, say N, forms a pseudo-null $\Lambda(G)$-module. It is easy to see that N becomes a $\Lambda(G)$-module. To show that it is pseudo-null is equivalent to showing $\mathrm{E}^1(N) = 0$ by Proposition 3.4. In [Ve] the vanishing has been proved by using a certain spectral sequence in a more general setting. For completeness, however, we would like to give another proof here using the graduation which has been shown to exist in Theorem 2.8.

We first prove a few lemmas. First let us recall Theorem 2.8: there exists an open subgroup G' of G called "extra powerful" pro-p group such that $gr(\Lambda(G')) \cong \mathbb{F}_p[X_0, \cdots, X_r]$ with $r = \mathrm{pd}(\Lambda(G'))$ through $\mathfrak{M}$-adic filtration, where $\mathfrak{M}$ is the maximal ideal of $\Lambda(G')$. Assume now $G = G'$. Then any $\Lambda(G)$-module M has a good filtration and we can associate a graded module $gr_{\mathfrak{M}}(M) = \bigoplus_{i=0}^{\infty} \mathfrak{M}^i M/\mathfrak{M}^{i+1}M$, which is a finitely generated $gr(\Lambda(G))$-module. Now $gr_{\mathfrak{M}}(M)$ is a finitely generated module over a commutative Noetherian ring, so the dimension is defined in the usual way.

Lemma 6.2 *The dimension of M, $\delta(M)$, is equal to the dimension of $gr_{\mathfrak{M}}(M)$.*

Proof: Recall $\delta(M) + j(M) = \mathrm{pd}(\Lambda(G))$ (Proposition 2.4). But $j(M) = j(gr_{\mathfrak{M}}(M))$ according to [Bj1]. On the other hand, from commutative algebra, we know $\dim(gr_{\mathfrak{M}}(M)) + j(gr_{\mathfrak{M}}(M)) = \dim(gr(\Lambda(G)))$. But $\dim(gr(\Lambda(G))) = \mathrm{pd}(\Lambda(G))$, hence the equality. □

Put $S = gr(\Lambda(G))$. Now let us consider $\Lambda(H)$ too. Denote the maximal ideal by $\mathfrak{N}$. Put $R = gr_{\mathfrak{N}}(\Lambda(H))$. Suppose M is a finitely generated S-module. Of course M is also a R-module by restriction. If M is also finitely generated over R, then what is the relation between $\dim_S(M)$ and $\dim_R(M)$? The following lemma gives a partial answer.

Lemma 6.3 *Let R, S and M be as above. Then we have always*

$$dim_S(M) \leq dim_R(M).$$

This is also deduced from the spectral sequence in [Ve]. The following proof is provided us by J. Manoharmayum[4].

Proof: Put $d_R = \dim_R(M)$ and $d_S = \dim_S(M)$. Also put $a_j = \dim_k(\mathfrak{N}^j M/\mathfrak{N}^{j+1}M)$ and $b_j = \dim_k(\mathfrak{M}^j M/\mathfrak{M}^{j+1}M)$. Then there exist polynomials $H_R(t), H_S(t) \in \mathbb{Q}[t]$ such that $H_R(j) = a_j$ and $H_S(j) = b_j$ for all $j \gg 0$ and $\deg(H_R) = d_R - 1$ and $\deg(H_S) = d_S - 1$. Hence there exist polynomials $L_R(t), L_S(t) \in \mathbb{Q}[t]$ of degree d_R, d_S respectively such that $L_R(j) = \ell_R(M/\mathfrak{N}^{j+1}M)$ and $L_S(j) = \ell_S(M/\mathfrak{M}^{j+1}M)$ for all $j \gg 0$ (here ℓ denotes length). Now there is the natural surjective map of R-modules: $f_{j+1} : M/\mathfrak{N}^{j+1}M \to M/\mathfrak{M}^{j+1}M$. Hence if any chain of S-modules is given:$0 \subsetneqq N_1 \subsetneqq N_2 \cdots \subsetneqq N_r \subsetneqq M/\mathfrak{M}^{j+1}M$, we will have a chain of R-modules: $0 \subsetneqq f_{j+1}^{-1}(N_1) \subsetneqq f_{j+1}^{-1}(N_2) \cdots \subsetneqq f_{j+1}^{-1}(N_r) \subsetneqq M/\mathfrak{N}^{j+1}M$. Hence $\ell_S(M/\mathfrak{M}^{j+1}M) \leq \ell_R(M/\mathfrak{N}^{j+1}M)$. Therefore $L_S(j) \leq L_R(j)$ for all $j \gg 0$. This implies $d_S \leq d_R$. □

Proof: (of Theorem 6.1) First note that Theorem 5.1 holds in the category of $\Lambda(G(F_\infty/F_n))$-modules for any $n \geq 0$. Let N be set of all $\Lambda(H)$-torsion elements in $\mathrm{Sel}_p(F_\infty, E)^\vee$. Then N is a $\Lambda(H)$-module since it is isomorphic to $\mathrm{E}^1_{\Lambda(H)}(D(\mathrm{Sel}_p(F_\infty, E)^\vee))$ as $\Lambda(H)$ is a Noetherian ring without zero divisors. We are going to show $N = 0$. For the purpose, we may take $F(E_{p^n})$ as a base field for some sufficiently large n so that we have $G \cong \{A \in GL_2(\mathbb{Z}_p) : A \equiv 1(\mathrm{mod}\ p^n)\}$. Then we have $G = CH$ where $H \cong \{A \in GL_2(\mathbb{Z}_p) : det(A) = 1\}$ and $C \cong \{a \in \mathbb{Z}_p^\times : a \equiv 1(\mathrm{mod}\ p^n)\}$. Let us check that N is G-stable for this G. Take any $g \in G$ and write $g = ch$. Take any $x \in N$. Since N is a $\Lambda(H)$-module, $hx \in N$ and $z(hx) = 0$ for some $z \in \Lambda(H)$. Then since c is in the centre of G, we have $z(gx) = z(chx) = cz(hx) = 0$. Therefore N is a $\Lambda(G)$-submodule of $\mathrm{Sel}_p(F_\infty, E)^\vee$. But now N is finitely generated $\Lambda(G)$-torsion module and also finitely generated and torsion over $\Lambda(H)$ by Coates-Howson. From the two lemmas above, we have $\dim_{\Lambda(G)}(N) \leq \dim_{\Lambda(H)}(N) \leq 3$. Therefore $\mathrm{codim}_{\Lambda(G)}(N) \geq 2$, which means N is a pseudo-null $\Lambda(G)$-submodules of $\mathrm{Sel}_p(F_\infty, E)^\vee$. By Theorem 5.1, we conclude $N = 0$. □

Another important question is how the centre C of G acts on the Selmer group. The only implication we get about it is the following corollary to our main theorem, which follows by the same argument as above:

Theorem 6.4 *Assume that G is a pro-p-group or that G is a profinite group with its centre C isomorphic to $\mathbb{Z}_p$. Then the $\Lambda(C)$-torsion submodule* $\mathrm{tor}_{\Lambda(C)}(\mathrm{Sel}_p(F_\infty, E)^\vee)$ *is either zero or* not *finitely generated as $\Lambda(C)$-module.*

References

[Au] M. Auslander, M. Bridger. *Stable Module Theory*, volume 94 of *Memoirs of the AMS*. AMS, 1969.

[4]We thank Jayanta Manoharmayum for the proof.

[Bj1] J.-E. Björk *Filtered noetherian rings,* In *Noetherian rings and their applications, Conf. Oberwolfach/FRG 1983*, Math. Surv. Monogr., 24, 59-97, 1987.

[Bj2] J.-E. Björk. *Rings of Differential Operators,* North-Holland Math. Library, 21, 1979.

[Br] A. Brumer *Pseudocompact algebras, profinite groups and class formations*, J. Algebra, 4, 442-470, 1966.

[Brun] W. Bruns, J. Herzog. Cohen-Macauly Rings, Cambridge studies in advance mathematics 39, Cambridge University Press, 1993.

[Co] J. Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curve without complex multiplication*, in Arithmetic of Elliptic Curves, LNM 1716, Springer 1999.

[CG] J. Coates and R. Greenberg, *Kummer theory of abelian varieties over local fields*, Invent. Math., 124 (1996), 129-174.

[CH] J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, to appear.

[DSMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal. Analytic Pro-p Groups, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, 2nd edition, 1999.

[Gr1] R. Greenberg *On the structure of certain Galois groups* Invent. Math. 47, 85-99, 1978.

[Gr2] R. Greenberg, *Iwasawa theory for p-adic representations* Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 97-137, 1989.

[Gr3] R. Greenberg, *Iwasawa theory for elliptic curves*, in Arithmetic of Elliptic Curves, LNM 1716, Springer, 1999.

[Ha1] M. Harris, *p-adic Representations arising from descent on abelian varieties*, Compositio Math., 39(1979), 177-245.

[Ha2] M. Harris, *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Invent Math., 51(1979), 123-141.

[HM] Y. Hachimori and K. Matsuno, *On finite Λ-submodules of Selmer groups of elliptic curves*, Proc. Amer. Math. Soc. 128 (2000), 2539-2541.

[HO] S. Howson and Y. Ochi, *Structure of Iwasawa modules arising from Galois cohomology*, preprint.

[Iw] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*,

Ann of Math., 98, 246-326, 1973.

[Ja1] U. Jannsen, *Iwasawa modules up to isomorphism*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 171-207, 1989.

[Ja2] U. Jannsen, *On the ℓ-adic cohomology of varieties over number fields and its Galois cohomology*, Galois Groups over $\mathbb{Q}$, 315-360, Springer, 1989.

[Ja3] U. Jannsen, *Continuous etale cohomology*, Mathematische Annalen 280 (1988), 207-245.

[Ja4] U. Jannsen, *A spectral sequence for Iwasawa adjoints*, unpublished notes 1994.

[La] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I. H. E. S., 26, 1965.

[Le] Thierry Levasseur. *Grade des modules sur certains anneaux filtres.* Commun. Algebra, 9(15),1519–1532, 1981.

[Ma] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. math., 18 (1972), 183-226.

[Ng] T. Nguyen-Quang-Do *Formations de classes et modules d'Iwasawa,in:* Number Theory Noordwigerhout 1983, LNM 1068, Spinger 1984.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer 2000.

[Oc] Y. Ochi, *Iwasawa modules via homotopy theory*, PhD thesis, University of Cambridge, 1999.

[Pe] B. Perrin-Riou, *Groupe de Selmer d'une courbe elliptique a multiplication complexe*, Compo. Math., vol. 43 (1981), 387-417.

[Sc1] P. Schneider, *Über gewisse Galoiscohomologiegruppen*, Math. Z. 168 (1979), 181-205.

[Sc2] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields, a first approach*, Invent. Math. 71 (1983), 251-293.

[Sc3] P. Schneider, *Motivic Iwasawa theory*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa pp.421-456, 1989.

[Se1] J-P. Serre, Cohomologie Galoisienne, Lecture Notes in Math., 5, Springer 1965.

[Se2] J-P. Serre, Abelian ℓ-adic representations and Elliptic Curves, W. A. Benjamin. INC, 1968.

[ST] J-P. Serre and J. Tate, *Good reduction of abelain varieties*, Ann. of Math., 88 pp. 492-517, (1968).

[Si] J. Silverman, The Arithmetic of Ellpitic Curves, Springer 1986.

[Su] R. Sujatha, *Euler-Poincare characteristics of p-adic Lie groups and arithmetic*, preprint, 2000.

[Ve] O. Venjakob, *New methods in the Iwasawa Theory of p-adic Lie extensions*, Dissertation, University of Heidelberg, 2000.

[We] C. Weibel, Introduction to Homological Algebra, Cambridge U.P., 1994.

[Wil] J.S. Wilson *Profinite Groups*, volume 19 of *London Mathematical Society Monographs New Series*. Oxford University Press, 1st edition, 1998.

[Wi1] K. Wingberg, *Duality theorems for* Γ*-extensions of algebraic number fields*, Compositio Math., 55 (1985), 333-381.

[Wi2] K. Wingberg, *On the rational points of abelian varieties over* $\mathbb{Z}_p$*-extensions of number fields*, Math. Ann. 279, (1987) 279-324.

[Wi3] K. Wingberg, *Duality theorems for abelian varieties over* $\mathbb{Z}_p$*-extensions*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa pp.471-492, 1989.

Yoshihiro Ochi
Mathematisches Institut
Im Neuenheimer Feld 288
69120 Heidelberg, Germany.

ochi@mathi.uni-heidelberg.de

Otmar Venjakob
Mathematisches Institut
Im Neuenheimer Feld 288
69120 Heidelberg, Germany.

otmar@mathi.uni-heidelberg.de
http://www.mathi.uni-heidelberg.de/∼otmar/