Compositio Mathematica **138:** 1–54, 2003. 1

On the Iwasawa Theory of p-Adic Lie Extensions

OTMAR VENJAKOB
Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany. e-mail: otmar@mathi.uni-heidelberg.de

(Received: 8 May 2001; accepted in final form: 16 October 2002)

Abstract. In this paper, the new techniques and results concerning the structure theory of modules over noncommutative Iwasawa algebras are applied to arithmetic: we study Iwasawa modules over p-adic Lie extensions k_∞ of number fields k 'up to pseudo-isomorphism'. In particular, a close relationship is revealed between the Selmer group of Abelian varieties, the Galois group of the maximal Abelian unramified p-extension of k_∞ as well as the Galois group of the maximal Abelian p-extension unramified outside S where S is a certain finite set of places of k. Moreover, we determine the Galois module structure of local units and other modules arising from Galois cohomology.

Mathematics Subject Classifications (2000). 11R23, 11R34, 11G10, 14K15.

Key words. Abelian varieties, Iwasawa theory, p-adic analytic groups, pseudo-isomorphism.

1. Introduction

The starting point of the *Iwasawa theory of* (*noncommutative*) *p-adic Lie groups* was M. Harris' thesis [15] in 1979. For an elliptic curve E over a number field k without complex multiplication, he studied the Selmer group $\mathrm{Sel}(E, k_\infty)$ over the extension $k_\infty = k(E(p))$ which arises by adjoining the p-division points of E to k. Then, the Galois group $G = G(k_\infty/k)$ is an open subgroup of $\mathrm{Gl}_2(\mathbb{Z}_p)$ – due to a celebrated theorem of Serre [38] – and so a (compact) p-adic Lie group. Following Iwasawa's general idea, he studied the Pontryagin dual $\mathrm{Sel}(E, k_\infty)^\vee$ of the Selmer group as module over the Iwasawa algebra $\Lambda(G) = \mathbb{Z}_p[\![G]\!]$, i.e. the completed group algebra of G with coefficients in $\mathbb{Z}_p$.

In the late 90s J. Coates and S. Howson [4, 6, 7, 17] as well as Y. Ochi [33] revived this Iwasawa-theoretic approach. Among other things, they proved a remarkable Euler characteristic formula for the Selmer group, studied ranks, torsion-properties and projective dimensions of standard local and global Iwasawa modules.

The contributions of this work to the Iwasawa theory of p-adic Lie groups are obtained by applying some new techniques we have developed in [40]. There we introduced the concept of pseudo-null modules over $\Lambda = \Lambda(G)$, which is based on a general dimension theory for Auslander regular rings (for the definition, see Subsection 2.2 and note that Λ is a noncommutative ring in general). Therefore it is fundamental for our applications that $\Lambda(G)$ is an Auslander regular ring if G is a compact p-adic Lie group without p-torsion (cf. [40, Thm. 3.26]). As a first example in which this approach proves effective, we consider the following generalization of a theorem of R. Greenberg [13] and T. Nguyen-Quang-Do [31] (who considered the case $G \cong \mathbb{Z}_p^d$): For a finite set S of places of a number field k let $k_\infty \mid k$ be a Galois extension unramified outside S such that the Galois group $G = G(k_\infty/k)$ is a torsion-free p-adic Lie-group and let k_S be the maximal outside S unramified extension of k. Then there is a basic result on the structure of the Galois group $X_S = G(k_S/k_\infty)^{\mathrm{ab}}(p)$ of the maximal Abelian p-extension of k_∞ unramified outside S considered as $\Lambda(G)$-module, which is by definition the maximal Abelian pro-p quotient of the Galois group $G_S(k_\infty) := G(k_S/k_\infty)$.

THEOREM (Theorem 4.5). *If* $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, *then the* $\Lambda(G)$*-module* X_S *does not contain any nontrivial pseudo-null submodule.*

Once having available the concept of pseudo-null modules one is tempted to study Iwasawa modules 'up to pseudo-isomorphism'. We will write $M \sim N$ if there exists a Λ-homomorphism $M \to N$ whose kernel and cokernel is pseudo-null. Since in general $\sim$ is not a symmetric relation we consider also the quotient category $\Lambda\text{-mod}/\mathcal{PN}$ with respect to subcategory $\mathcal{PN}$ of pseudo-null Λ-modules, which is a Serre subcategory, i.e. closed under subobjects, quotients and extensions.

Now it turns out that – as in the classical $\mathbb{Z}_p$-extension case – the $\Lambda(G)$-module X_S is closely related to the modules X_{nr} and X_{cs}^S which denote the Galois groups of the maximal Abelian unramified pro-p-extension of k_∞ and the maximal Abelian unramified pro-p-extension of k_∞ in which every prime above S is completely decomposed, respectively. In the next theorem, G_v denotes the decomposition group of G at a place v, S_f is the set of finite places in S, $\mathrm{E}^1(M)$ the Iwasawa adjoint $\mathrm{Ext}^1_\Lambda(M, \Lambda)$ of a Λ-module M and $M(-1)$ means the twist of M with the Galois module $\mathbb{Z}_p(-1) := \mathrm{Hom}(\mu, \mathbb{Q}_p/\mathbb{Z}_p)$.

THEOREM (Theorem 4.9). *If* $\mu_{p^\infty} \subseteq k_\infty$, *and* $\dim(G_v) \geqslant 2$ *for all* $v \in S_f$, *then*

$$X_{nr}(-1) \sim X_{cs}^S(-1) \sim \mathrm{E}^1(\mathrm{tor}_\Lambda X_S).$$

If, in addition, $G \cong \mathbb{Z}_p^r$, $r \geqslant 2$, *then even the following holds:*

$$X_{nr}(-1) \sim X_{cs}^S(-1) \sim (\mathrm{tor}_\Lambda X_S)^\circ,$$

where $^\circ$ *means that* G *operates via the involution* $g \mapsto g^{-1}$.

In this context we should mention that it is still an open question – even for $G \cong \mathbb{Z}_p^r$, $r \geqslant 2$ – whether in general X_{nr} is pseudo-isomorphic to the dual $(\mathrm{Cl}(k_\infty)(p)^\vee)^\circ$ of the direct limit of the p-primary ideal class groups in a p-adic tower of number fields with involution $-^\circ$ (which can also be defined for noncommutative p-adic Lie groups under additional assumptions, see Proposition 2.4) $X_{nr} \sim (\mathrm{Cl}(k_\infty)(p)^\vee)^\circ$?

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

In the $\mathbb{Z}_p$-case this is a well-known theorem due to Iwasawa, see 4.17 for further discussion.

Drawing our attention to cohomology groups associated with an Abelian varieties $\mathcal{A}$ defined over k, we set $k_\infty = k(\mathcal{A}(p))$ and mention that $\mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p))^\vee$ has no nonzero pseudo-null submodule (Theorem 4.39). With respect to the (p)-Selmer group $\mathrm{Sel}(\mathcal{A}, k_\infty)$ of $\mathcal{A}$ over $k_\infty = k(\mathcal{A}(p))$ we generalize a result of P. Billot in the case of good, *supersingular* reduction, i.e. $\widetilde{\mathcal{A}_{k_v}}(p) = 0$, at any place dividing p. Over a $\mathbb{Z}_p$-extension an analogous statement was proved by K. Wingberg [41, Cor. 2.5]. We shall write $\mathcal{A}^d$ for the dual Abelian variety of $\mathcal{A}$. Assume that $G(k_\infty/k)$ is a pro-p-group without any p-torsion. Then the following holds (Corollary 4.38):

$$X_{cs} \otimes_{\mathbb{Z}_p} (\mathcal{A}^d(p))^\vee \sim \mathrm{E}^1(\mathrm{tor}_\Lambda(\mathrm{Sel}(\mathcal{A}, k_\infty)^\vee)).$$

We also refer the reader to our joint work with Y. Ochi [35] where we prove under certain conditions that the Pontryagin dual of the Selmer group of an elliptic curve without CM and good *ordinary* reduction at any place dividing p does not contain any nonzero pseudo-null Λ-submodule.

Furthermore, we proved a structure theory for the $\mathbb{Z}_p$-torsion part of a Λ-module M in [40]. Up to pseudo-isomorphism any $\mathbb{Z}_p$-torsion Λ-module is of the form $\bigoplus_i \Lambda/p^{n_i}$.

In particular, we obtained a natural definition of the μ-invariant $\mu(M) := \sum_i n_i$ of M. Defining $\mu(M) := \mu(\mathrm{tor}_{\mathbb{Z}_p} M)$ for an arbitrary Λ-module M, this invariant is additive on short exact sequences of Λ-torsion modules. Hence, we can formulate and prove a generalization of Theorem 11.3.7 of [29]:

THEOREM (Theorem 4.18). *Let $k_\infty \mid k$ be a p-adic pro-p Lie extension such that G is without p-torsion and $\mathbb{F}_p[\![G]\!]$ is an integral ring (e.g. if G is uniform). Then $\mathcal{G} = G(k_S(p)/k_\infty)$ is a free pro-p-group if and only if $\mu(X_S) = 0$ and the weak Leopoldt conjecture holds, i.e.* $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

In Theorem 4.19 we describe how the weak Leopoldt conjecture and the vanishing of $\mu(X_S)$ – if considered simultaneously – behave under change of the base field. Furthermore, we get a formula for the μ-invariants for different S.

We briefly outline further results. In Section 3 we generalize Wintenberger's result on the Galois module structure of local units. Let k be a finite extension of $\mathbb{Q}_p$ and assume that $k_\infty \mid k$ is a Galois extension with Galois group $G \cong \Gamma \rtimes_\rho \Delta$, where Γ is a pro-p Lie group of dimension 2 (e.g. $\Gamma = \mathbb{Z}_p \rtimes \mathbb{Z}_p$) and Δ is a profinite group of *possibly infinite* order prime to p, which acts on Γ via $\rho\colon \Delta \to \mathrm{Aut}(\Gamma)$. Then we characterize the $\Lambda(G)$-module structure of the Galois group $G^{\mathrm{ab}}_{k_\infty}(p) = G(k_\infty(p)/k_\infty)$, where $k_\infty(p)$ is the maximal Abelian p-extension of k_∞, see Theorem 3.10.

Then we apply these results to the local study of elliptic curves E *with CM*, i.e. we determine the structure of local cohomology groups with certain division points of E as coefficients.

Section 4 is devoted to the study of ‘global’ Iwasawa modules. Besides the themes already mentioned above, we study the norm-coherent S-units of k_∞ $\mathbb{E}_S := \varprojlim_{k'}(\mathcal{O}^\times_{k',S} \otimes \mathbb{Z}_p)$ by means of Jannsen's spectral sequence for Iwasawa adjoints. Using Kummer theory, we compare $\mathbb{E}_S$ to

$$\mathcal{E}_S(k_\infty) := (E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\vee,$$

where $E_S(k_\infty) = \varinjlim_{k'} E_S(k')$ denotes the (discrete module of) S-units of k_∞. In particular, we show that $\mathrm{E}^0(\mathbb{E}_S) \cong \mathrm{E}^0\mathrm{E}^0(\mathcal{E}_S(k_\infty))$, where $\mathrm{E}^0(M)$ denotes $\mathrm{Hom}_\Lambda(M, \Lambda)$ for any Λ-module M, and thus $\mathrm{rk}_\Lambda \mathbb{E}_S = \mathrm{rk}_\Lambda \mathcal{E}_S = r_2(k)$ under some assumptions, see Corollary 4.27. If $\mathrm{E}^0(\mathbb{E}_S)$ is projective, its structure can be described more precisely. A criterion which tells us when this is the case is given in Proposition 4.28.

GENERAL NOTATION AND CONVENTIONS

We follow the notation in the paper [40], which is similar to that used in [29]. In particular, this means:

(i) For a discrete (resp. compact) $\mathbb{Z}_p$-module N with continuous action by some profinite group G, $N^\vee = \mathrm{Hom}_{\mathbb{Z}_p,\mathrm{cont}}(N, \mathbb{Q}_p/\mathbb{Z}_p)$ is the compact (resp. discrete) Pontryagin dual of N with its natural G-action. If N is p-divisible,

$$T_p(N) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, N) = \varprojlim_i {}_{p^i}N$$

denotes the Tate module of N, where ${}_{p^i}N$ denotes the kernel of the multiplication by p^i. For $G = G_k$ the absolute Galois group of number or local field k, we define the rth Tate twist of N by $N(r) := N \otimes_{\mathbb{Z}_p} T_p(\mu)^{\otimes r}$ for $r \in \mathbb{N}$ and $N(r) := N \otimes_{\mathbb{Z}_p} \mathrm{Hom}(T_p(\mu)^{\otimes r}, \mathbb{Z}_p)$ for $-r \in \mathbb{N}$, where μ denotes the G_k-module of all roots of unity and by convention $T_p(\mu)^{\otimes 0} = \mathbb{Z}_p$ with trivial G-action. Finally, we set

$$N^* := \varinjlim_i \mathrm{Hom}({}_{p^i}N, \mu_{p^\infty}) (= T_p(N)^\vee(1)).$$

(ii) For a finitely generated Abelian p-primary group A we denote by A_{div} the quotient of A by its maximal p-divisible subgroup.

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

(iv) If G is any profinite group, by $G(p)$ and G^{ab} we denote the maximal pro-p squotient and the maximal Abelian quotient $G/[G, G]$ of G, respectively. For an Abelian group A we also denote by $A(p)$ its p-primary component.

(v) Let k be a field. For a G_k-module A, we write $A(k) := H^0(G_k, A)$.

(vi) By a Noetherian ring, we mean a left and right Noetherian ring (with a multiplicative unit). By $\mathrm{pd}_\Lambda(M)$ we denote the projective dimension of M while $\mathrm{pd}(\Lambda)$ denotes the global dimension of Λ.

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(vii) The dual of an Abelian variety $\mathcal{A}$ is denoted by $\mathcal{A}^d$.
(viii) We refer the reader to Subsection 2.4 for the definitions of $R^{\text{ab}}(p)$, $N^{\text{ab}}(p)$, X, Y, J and Z.

2. Algebraic Properties of Λ-Modules

2.1. NOTATION AND PRELIMINARIES

We recall some basic facts on p-adic Lie groups and their Iwasawa algebras which are thoroughly discussed in [40]; the reader who is not familiar with them is recommended to read first or parallel Sections 1–3 of [40]. For any compact p-adic Lie group G the completed group algebra $\Lambda = \Lambda(G)$ is Noetherian (see [24]V 2.2.4). If, in addition, G is pro-p and has no element of finite order, e.g. if G is uniform, then $\Lambda(G)$ is an integral domain, i.e. the only zero-divisor in $\Lambda(G)$ is 0 (see [30]); for uniform G the corresponding statement holds also for the completed group algebra $\mathbb{F}_p[\![G]\!]$ with coefficients in the finite field $\mathbb{F}_p$ with p elements. For instance, for $p \geqslant n+2$, the group $\mathrm{Gl}_n(\mathbb{Z}_p)$ has no elements of order p, in particular, $\mathrm{GL}_2(\mathbb{Z}_p)$ contains no elements of finite p-power order if $p \geqslant 5$ (see [17] 4.7). In any case, the normal subgroup $\Gamma_i := \ker(\mathrm{Gl}_n(\mathbb{Z}_p) \to \mathrm{Gl}_n(\mathbb{Z}/p^i))$ of $\mathrm{Gl}_n(\mathbb{Z}_p)$ is a uniform pro-p group for $i \geqslant 1$ if $p \neq 2$ or $i \geqslant 2$ if $p = 2$ by [10, Thm. 5.2]. We should also mention that G has finite cohomological dimension $\mathrm{cd}_p G = m$ if and only if G has no element of finite p-power order and its dimension as p-adic analytic manifold equals m.

If Λ is Noetherian and without zero-divisors we can form a skew field $Q(G)$ of fractions of Λ (see [11]). This allows us to define the rank of a Λ-module:

DEFINITION 2.1. The rank $\mathrm{rk}_\Lambda M$ is defined to be the dimension of $M \otimes_\Lambda Q(G)$ as a left vector space over $Q(G)$. Obviously, the rank is finite for any M in the category Λ-mod of finitely generated Λ-modules. For the rest of this section, we assume that *all* Λ*-modules considered are finitely generated.*

By $\mathrm{Ho}(\Lambda)$ we denote the category of 'Λ-modules up to homotopy' and we write $M \simeq N$, if M and N are homotopy equivalent, i.e. isomorphic in $\mathrm{Ho}(\Lambda)$, which holds if and only if $M \oplus P \cong N \oplus Q$ with projective Λ-modules P and Q. In particular, $M \simeq 0$ if and only if M is projective.

For $M \in \Lambda$-mod we define the Iwasawa adjoints of M to be

$$\mathrm{E}^i(M) := \mathrm{Ext}^i_\Lambda(M, \Lambda), \quad i \geqslant 0,$$

which are a-priori right Λ-modules by functoriality and the right Λ-structure of the bi-module Λ but will be considered as left modules via the involution of Λ. By convention we set $\mathrm{E}^i(M) = 0$ for $i < 0$. The Λ-dual $\mathrm{E}^0(M)$ will also be denoted by M^+.

It can be shown that for $i \geqslant 1$ the functor E^i factors through $\mathrm{Ho}(\Lambda)$ defining a functor $\mathrm{E}^i\colon \mathrm{Ho}(\Lambda) \to \Lambda$-mod. By D we denote the transpose $\mathrm{D}\colon \mathrm{Ho}(\Lambda) \to \mathrm{Ho}(\Lambda)$, which is a contravariant duality functor, i.e. it satisfies $\mathrm{D}^2 = \mathrm{Id}$. Furthermore, if $\mathrm{pd}_\Lambda M \leqslant 1$, then $\mathrm{D}M \simeq \mathrm{E}^1(M)$. The next property will be of particular importance:

PROPOSITION 2.2 (cf. [29, Prop. 5.4.9]). *For* $M \in \Lambda$-mod *there is a canonical exact sequence*

$$0 \longrightarrow \mathrm{E}^1\mathrm{D}M \longrightarrow M \xrightarrow{\phi_M} M^{++} \longrightarrow \mathrm{E}^2\mathrm{D}M \longrightarrow 0,$$

where ϕ_M *is the canonical map from* M *to its bi-dual. In the following we will refer to the sequence as 'the' canonical sequence* (*of homotopy theory*).

A Λ-module M is called *reflexive* if ϕ_M is an isomorphism from M to its bi-dual $M \cong M^{++}$.

As Auslander and Bridger [1] suggest, the module $\mathrm{E}^1\mathrm{D}M$ should be considered as torsion submodule of M. Indeed, if Λ is a Noetherian integral domain this submodule is a torsion module while M^{++} is torsion-free and thus $\mathrm{E}^1\mathrm{D}M$ coincides exactly with the set* of torsion elements $\mathrm{tor}_\Lambda M$. Hence, a Λ-module M is called Λ-*torsion module* if $\phi_M \equiv 0$, i.e. if $\mathrm{tor}_\Lambda M := \mathrm{E}^1\mathrm{D}M = M$. We say that M is Λ-*torsion-free* if $\mathrm{E}^1\mathrm{D}M = 0$. It turns out that 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 integral. Since M^{++} embeds into a free Λ-module the torsion-free Λ-modules are exactly the submodules of free modules (see [40, before Prop. 2.7] for details).

Sometimes it is also convenient to have the notation of the *first syzygy* or *loop space* functor $\Omega\colon \Lambda\text{-mod} \to \mathrm{Ho}(\Lambda)$ which is defined as follows (see [20, 1.5]): Choose a surjection $P \to M$ with P projective. Then ΩM is defined by the exact sequence

$$0 \longrightarrow \Omega M \longrightarrow P \longrightarrow M \longrightarrow 0.$$

2.2. DIMENSION THEORY FOR THE AUSLANDER REGULAR RING $\Lambda(G)$

Let G be any compact p-adic group without p-torsion. In [40] we proved that $\Lambda = \Lambda(G)$ is an *Auslander regular ring*, i.e. Λ has finite projective dimension $d := \mathrm{pd}\,\Lambda = \mathrm{cd}_p\, G + 1$ (by a result of Brumer) and satisfies the Auslander condition: For any Λ-module M, any integer m and any submodule N of $\mathrm{E}^m(M)$, the grade of N satisfies $j(N) \geqslant m$. Recall that the *grade* $j(N)$ is the smallest number i such that $\mathrm{E}^i(N) \neq 0$ holds.

Therefore, there is a nice dimension theory for Λ-modules which we will recall briefly (for proofs and further references see [40]). A priori, any $M \in \Lambda$-mod comes equipped with a finite filtration

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

If we call the number $\delta := \min\{i \mid \mathrm{T}_i(M) = M\}$ the *dimension* $\delta(M)$ then $\mathrm{T}_i(M)$ is just the maximal submodule of M with δ-dimension less or equal to i. We should

*A-priori, it is not clear whether this sets forms a submodule if Λ is not commutative.

mention that for Abelian G the dimension $\delta(M)$ coincides with the Krull dimension of $\mathrm{supp}_\Lambda(\mathrm{M})$.

The filtration is related to the Iwasawa adjoints via a spectral sequence, in particular we have

$$\mathrm{T}_i(M)/\mathrm{T}_{i-1}(M) \subseteq \mathrm{E}^{d-i}\mathrm{E}^{d-i}(M)$$

and either of these two terms is zero if and only the other is. Furthermore, the equality $\delta(M) + j(M) = d$ holds for any $M \neq 0$.

Note that M is a Λ-torsion module if and only if its codimension $\mathrm{codim}(M) := d - \delta(M)$ is greater or equal to 1.

A Λ-module M is called *pseudo-null* if its codimension $\mathrm{codim}(M)$ is greater or equal to 2. As in the commutative case we say that a homomorphism $\varphi: M \to N$ of Λ-modules is a *pseudo-isomorphism* if its kernel and cokernel are pseudo-null. A module M is by definition pseudo-isomorphic to a module N, denoted $M \sim N$, if and only if there exists a pseudo-isomorphism from M to N. In general, $\sim$ is not symmetric even in the $\mathbb{Z}_p$-case. While in the commutative case $\sim$ is symmetric at least for torsion modules, we do not know whether this property still holds in the general case.

If we want to reverse pseudo-isomorphisms, we have to consider the quotient category $\Lambda\text{-mod}/\mathcal{PN}$ with respect to subcategory $\mathcal{PN}$ of pseudo-null Λ-modules, which is a Serre subcategory, i.e. closed under subobjects, quotients and extensions. By definition, this quotient category is the localization $(\mathcal{PI})^{-1}\Lambda\text{-mod}$ of Λ-mod with respect to the multiplicative system $\mathcal{PI}$ consisting of all pseudo-isomorphisms. Since Λ-mod is well-powered, i.e. the family of submodules of any module $M \in \Lambda\text{-mod}$ forms a set, these localization exists, is an Abelian category and the universal functor $q: \Lambda\text{-mod} \to \Lambda\text{-mod}/\mathcal{PN}$ is exact. Furthermore, $q(M) = 0$ in $\Lambda\text{-mod}/\mathcal{PN}$ if and only if $M \in \mathcal{PN}$. Recall that a morphism $h: q(M) \to q(N)$ in the quotient category can be represented, for instance, by two Λ-homomorphisms $f: M' \to M$ and $g: M' \to N$ where f is a pseudo-isomorphism and such that $h \circ q(f) = q(g)$; it is an isomorphism if and only if g is a pseudo-isomorphism. If there exists an isomorphism between $q(M)$ and $q(N)$ in the quotient category we also write $M \equiv N \bmod \mathcal{PN}$.

Note that for any pseudo-isomorphism $f: M \to N$ the induced homomorphism $\mathrm{E}^1(f)$ is a pseudo-isomorphism, too. If M, N are Λ-torsion modules, also the converse statement holds. By the universal property of the localization, we obtain a functor

$$\mathrm{E}^1: \Lambda\text{-mod}/\mathcal{PN} \to \Lambda\text{-mod}/\mathcal{PN},$$

which is exact if it is restricted to the full subcategory $\Lambda\text{-mod}^{\geqslant 1}/\mathcal{PN}$ of $\Lambda\text{-mod}/\mathcal{PN}$ consisting of all Λ-modules of codimension greater or equal to 1, i.e. Λ-torsion modules. More precisely, there is a natural isomorphism of functors:

$$\mathrm{E}^1 \circ \mathrm{E}^1 \cong \mathrm{Id} : \Lambda\text{-mod}^{\geqslant 1}/\mathcal{PN} \to \Lambda\text{-mod}^{\geqslant 1}/\mathcal{PN}.$$

It is known that any torsion-free module M embeds into a reflexive module with pseudo-null cokernel while any torsion module M is pseudo-isomorphic to

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

$\mathrm{E}^1\mathrm{E}^1(M)$ (cf. [40, Prop. 3.13]). Moreover, there is a canonical pseudo-isomorphism $\mathrm{E}^1(M) \sim \mathrm{E}^1(\mathrm{tor}_\Lambda M)$ for any Λ-module M.

By Λ-mod(p) we shall write the plain subcategory of Λ-mod consisting of $\mathbb{Z}_p$-torsion modules while by $\mathcal{PN}(p)$ ' $= \mathcal{PN} \cap \Lambda$-mod$(p)$' we denote the Serre subcategory of Λ-mod(p) the objects of which are pseudo-null Λ-modules. In other words M belongs to $\mathcal{PN}(p)$ if and only if it is a Λ/p^n-module for an appropriate n such that $\mathrm{E}^0_{\Lambda/p^n}(M) = 0$. Recall that there is a canonical exact functor $q\colon \Lambda\text{-mod}(p) \to \Lambda\text{-mod}(p)/\mathcal{PN}(p)$. Then, there is the following structure theorem on the $\mathbb{Z}_p$-torsion part of a finitely generated Λ-module:

THEOREM 2.3 (cf. [40, Thm. 3.40]). *Assume that G is a p-adic analytic pro-p group without p-torsion and such that Λ/p is integral (e.g. if G is uniform). Let M be in Λ-mod(p). Then there exist uniquely determined natural numbers $n_1, \dots, n_r$ and an isomorphism $M \equiv \bigoplus_{1\leqslant i\leqslant r} \Lambda/p^{n_i}$ mod $\mathcal{PN}(p)$ in Λ-mod$(p)/\mathcal{PN}(p)$.*

We define the μ-invariant of a Λ-module M as $\mu(M) = \sum_i n_i(\mathrm{tor}_{\mathbb{Z}_p} M)$, where the $n_i = n_i(\mathrm{tor}_{\mathbb{Z}_p} M)$ are determined uniquely by the structure theorem applied to $\mathrm{tor}_{\mathbb{Z}_p} M$. This invariant is additive on short exact sequences of Λ-torsion modules and stable under pseudo-isomorphisms. Alternatively, it can be described as

$$\mu(M) = \mathrm{rk}_{\mathbb{F}_p[\![G]\!]} \bigoplus_{i\geqslant 0} {}_{p^{i+1}}M/{}_{p^i}M = \mathrm{rk}_{\mathbb{F}_p[\![G]\!]} \bigoplus_{i\geqslant 0} p^i\, \mathrm{tor}_{\mathbb{Z}_p} M/p^{i+1}\, \mathrm{tor}_{\mathbb{Z}_p} M.$$

Very recently, J. Coates, R. Sujatha and P. Schneider [8] found a general structure theorem for Λ-torsion modules. They proved that any finitely generated $\Lambda(G)$-torsion module decomposes into the direct sum of cyclic modules up to pseudo-isomorphism, i.e. in the quotient category Λ-mod$^{\geqslant 1}/\mathcal{PN}$.

THEOREM (Coates–Schneider–Sujatha). *Let G be a p-valued compact p-adic analytic group. Then, for any finitely generated $\Lambda(G)$-torsion module M there exist finitely many reflexive left ideals $J_1, \dots, J_r$ and an injective $\Lambda(G)$-homomorphism $\bigoplus_{1\leqslant i\leqslant r} \Lambda/J_i \hookrightarrow M/M_{\mathrm{ps}}$ with pseudo-null cokernel, where $M_{\mathrm{ps}} = T_{\dim(G)-2}(M)$ denotes the maximal pseudo-null submodule of M. In particular, it holds $M \equiv \bigoplus_{1\leqslant i\leqslant r} \Lambda/J_i \bmod \mathcal{PN}$.*

For the precise definition of a p-valued compact Lie group see [8] or directly in Lazard's article [24]; we just want to mention that any uniform pro-p-group belongs to this class of pro-p Lie groups, which is stable under taking closed subgroups.

It is still not known whether the ideals J_i can be chosen as principal ideals as in the commutative case. Anyway, if we restrict to this kind of modules, we can define a second involution

$$\circ\colon \Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN} \to \Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN}$$

on the full subcategory $\Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN}$ of $\Lambda\text{-mod}^{\geqslant 1}/\mathcal{PN}$ consisting of those objects which are isomorphic (in the quotient category) to a direct sum of cyclic modules of the form $\Lambda/\Lambda f$, $f \in \Lambda$. For any such f we set $(\Lambda/\Lambda f)^{\circ} := \Lambda/\Lambda f^{\circ}$, where $^{\circ}\colon \Lambda \to \Lambda$ also denotes the involution of the group algebra (induced by $g \mapsto g^{-1}$). The following proposition implies among other things that this definition is invariant under pseudo-isomorphism and therefore it extends to the whole category $\Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN}$.

PROPOSITION 2.4. *Let G be a profinite group such that $\Lambda = \Lambda(G)$ is a Noetherian integral ring. Then the following holds:*

(i) *For any $f \in \Lambda$ there is an isomorphism $\mathrm{E}^1(\Lambda/\Lambda f) \cong \Lambda/\Lambda f^{\circ}$.*
(ii) *Assuming that G is a p-adic analytic group without p-torsion the above two involutions coincide:*

$$-^{\circ} \cong \mathrm{E}^1(-)\colon \Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN} \to \Lambda\text{-mod}^{\geqslant 1}_{\mathrm{pr}}/\mathcal{PN}$$

The proof is standard, see for example the proof of Proposition 2.12, where we denote the involution on Λ by ι.

We conclude this section with a technical result which will be needed in the arithmetic applications.

PROPOSITION 2.5. *Let Λ be an Auslander regular ring. For any Λ-module M such that $\mathrm{pd}_{\Lambda}\mathrm{E}^0(M) \leqslant 1$ (e.g. if $\mathrm{pd}\,\Lambda = 3$ or if $\mathrm{pd}\,\Lambda = 4$ and $\mathrm{E}^4\mathrm{E}^1(M) = 0$) its double dual $\mathrm{E}^0\mathrm{E}^0(M)$ is a 2-syzygy of $\mathrm{E}^1\mathrm{E}^0(M)$, i.e. there is an exact sequence*

$$0 \longrightarrow \mathrm{E}^0\mathrm{E}^0(M) \longrightarrow P_0 \longrightarrow P_1 \longrightarrow \mathrm{E}^1\mathrm{E}^0(M) \longrightarrow 0$$

with projective modules P_0 and P_1. Furthermore, in the case of $\mathrm{pd}\,\Lambda = 3$ or 4, it holds that $\mathrm{E}^1\mathrm{E}^0(M) \cong \mathrm{E}^3\mathrm{E}^1(M)$. If, in addition, M itself is reflexive and $\mathrm{pd}\,\Lambda = 3$, then $\mathrm{E}^3\mathrm{E}^1 M \cong \mathrm{E}^1(M)^{\vee}$.

Proof. First observe that $\mathrm{E}^0(M)$ is a 2-syzygy of $\mathrm{D}(M)$ due to the definition of the latter module, i.e. $\mathrm{pd}_{\Lambda}\mathrm{E}^0(M) \leqslant \mathrm{pd}\,\Lambda - 2 = 1$, if $\mathrm{pd}\,\Lambda = 3$. In the case of $\mathrm{pd}\,\Lambda = 4$ it holds $\mathrm{E}^3\mathrm{E}^0(M) = \mathrm{E}^4\mathrm{E}^0(M) = 0$ and $\mathrm{E}^2\mathrm{E}^0(M) \cong \mathrm{E}^4\mathrm{E}^1(M)$ due to Björk's spectral sequence (see [40, 3.1]). Hence, if $\mathrm{E}^4\mathrm{E}^0(M)$ vanishes, it follows that $\mathrm{pd}_{\Lambda}\mathrm{E}^0(M) \leqslant 1$. Now, choosing a projective resolution of $E^0(M)$

$$0 \longrightarrow \mathrm{E}^0(P_1) \longrightarrow \mathrm{E}^0(P_0) \longrightarrow \mathrm{E}^0(M) \longrightarrow 0,$$

we derive the exact sequence

$$0 \longrightarrow \mathrm{E}^0\mathrm{E}^0(M) \longrightarrow P_0 \longrightarrow P_1 \longrightarrow \mathrm{E}^1\mathrm{E}^0(M) \longrightarrow 0.$$

But $\mathrm{E}^1\mathrm{E}^0(M) \cong \mathrm{E}^3\mathrm{E}^1(M)$ due to Björk's spectral sequence for $\mathrm{pd}\,\Lambda \leqslant 4$. If M itself is reflexive and $\mathrm{pd}\,\Lambda = 3$, then $\mathrm{E}^1\mathrm{E}^1(M) = \mathrm{E}^2\mathrm{E}^1(M) = 0$, i.e. $\mathrm{E}^1(M)$ is finite, respectively $\mathrm{E}^3\mathrm{E}^1(M) \cong \mathrm{E}^1(M)^{\vee}$. □

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

2.3. SOME REPRESENTATION THEORY

In the following lemma we shall write $I(\Gamma)$ for the kernel of the canonical map $\mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p[\![G/\Gamma]\!]$, where Γ is any closed normal subgroup of the profinite group G. By Rad_G we denote the radical of $\mathbb{Z}_p[\![G]\!]$, i.e. the intersection of all open maximal left (right) ideals of $\mathbb{Z}_p[\![G]\!]$. Finally, we write $M_G = M/I_G M$ for the module of coinvariants of M and $\mathrm{H}_*(G, M)$ for the G-homology of a compact Λ-module M, which can be defined as left derived functor of $-_G$ or alternatively as $\mathrm{Tor}_*^{\Lambda}(\mathbb{Z}_p, M)$, where Tor denotes the left derived functor of the complete tensor product $-\widehat{\otimes}_{\Lambda} -$.

LEMMA 2.6. *Let $G = \Gamma \rtimes \Delta$ be the semi-direct product of a uniform pro-p-group Γ of dimension t and a finite group Δ of order k prime to p. If we write $U_n = \Gamma^{p^n} \trianglelefteq G$, then for any compact $\Lambda = \Lambda(G)$-module M, the following statements are equivalent:*

(i) $M \cong \Lambda^d$,

(ii) $M_\Gamma \cong \mathbb{Z}_p[\Delta]^d$ *as $\mathbb{Z}_p[\Delta]$-module and for all n*

$$\mathrm{rk}_{\mathbb{Z}_p} M_{U_n} = \mathrm{rk}_{\mathbb{Z}_p} \mathbb{Z}_p[G/U_n]^d = dkp^{tn},$$

(iii) $M_\Gamma/p \cong \mathbb{F}_p[\Delta]^d$ *as $\mathbb{F}_p[\Delta]$-module and for all n*

$$\log_p \#(M_{U_n}/p^n) = \log_p \#(\mathbb{Z}/p^n[G/U_n]^d) = ndkp^{tn}.$$

Proof. Obviously, (i) implies (ii) and (iii). For the converse let us first assume that (ii) holds and let $m_1, \ldots, m_d \in M$ be lifts of a $\mathbb{Z}_p[\Delta]$-basis of M_Γ. Then the map $\phi\colon \bigoplus_{i=1}^d \Lambda e_i \to M$, which sends e_i to m_i, is surjective, because $I(\Gamma) \subseteq \mathrm{Rad}_G$ (compare to the proof of [29]. 5.2.14 (i), $d \Rightarrow b$) and therefore we can apply Nakayama's lemma [29], 5.2.16 (ii), (with Rad_G instead of $\mathfrak{M}$). Hence, the induced maps $\phi_{U_n}\colon \bigoplus_{i=1}^d \Lambda(G/U_n)e_i \to M_{U_n}$, are surjective, too. But since both modules have the same $\mathbb{Z}_p$-rank by assumption, these maps are isomorphisms and (i) follows. The implication (iii) $\Rightarrow$ (i) is proved analogously noting that $p\Lambda + I(\Gamma) \subseteq \mathrm{Rad}_G$. □

For a finite group G we denote by $K_0(\mathbb{Q}_p[G]) = K_0'(\mathbb{Q}_p[G])$ the Grothendieck group of finitely generated $\mathbb{Q}_p[G]$-modules (which are projective by Maschke's theorem). If G is a profinite group and $U \trianglelefteq G$ an open normal subgroup we define the Euler characteristic $h_U(M)$ of a finitely generated $\Lambda = \Lambda(G)$-module M to be the class

$$h_U(M) := \sum (-1)^i [\mathrm{H}_i(U, M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p] \in K_0(\mathbb{Q}_p[G/U]).$$

Before stating the next result we recall some facts about the representation theory of finite groups. So let Δ be a finite group of order n prime to p. Then, there is a decomposition

$$\mathbb{Z}_p[\Delta] \cong \prod \mathbb{Z}_p[\Delta]e_i, \quad e_i = \frac{n_i}{n}\sum_{g\in\Delta}\chi_i(g^{-1})g$$

of $\mathbb{Z}_p[\Delta]$ in 'simple' components (in the sense that they are simple algebras after tensoring with $\mathbb{Q}_p$). If $G = \Gamma \times \Delta$, this induces a decomposition of $\Lambda = \prod \Lambda^{e_i}$, $\Lambda^{e_i} = \mathbb{Z}_p[\![\Gamma]\!][\Delta]e_i$ into a product of rings. Here $\{\chi_i\}$ is the set of irreducible $\mathbb{Q}_p$ characters ($\triangleq \mathbb{F}_p$-characters because n is prime to p) of Δ and n_i are certain natural numbers associated with χ_i (see below). The simple algebras $\mathbb{Q}_p[\Delta]e_i$ decompose into the direct sum of their simple left ideals which all belong to the same isomorphism class, say N_i, i.e. there is a isomorphism of $\mathbb{Q}_p[\Delta]$-modules $\mathbb{Q}_p[\Delta]e_i \cong N_i^{n_i}$. In particular, n_i is the length of $\mathbb{Q}_p[\Delta]e_i$ and can be expressed as

$$n_i = \chi(e_i)(\dim_{\mathbb{Q}_p} N_i)^{-1},$$

where χ is the character of the left regular representation of $\mathbb{Q}_p[\Delta]$.

Now let G be again a p-adic Lie group and set $\Lambda := \Lambda(G)$. Recall that a finitely generated Λ-module M is a Λ-torsion module if and only if M is a $\Lambda(G')$-torsion module for some open pro-p subgroup $G' \subseteq G$ such that $\Lambda(G')$ is integral.

PROPOSITION 2.7. *Let $G = \Gamma \times \Delta$ be the product of a pro-p Lie group Γ of finite cohomological dimension* $\mathrm{cd}_p(\Gamma) = m$ *and a finite group Δ of order n prime to p and let $U \trianglelefteq \Gamma$ be an open normal subgroup. Then, for any finitely generated Λ-torsion module M, it holds $h_U(M) = 0$.*

Remark 2.8. For semi-direct products this statement is false in general. For example, it is easy to see that for $G = \mathbb{Z}_p \rtimes_\omega \Delta$ with nontrivial ω the Euler characteristic of $\mathbb{Z}_p$ is not zero: $h_U(\mathbb{Z}_p) = [\mathbb{Q}_p] - [\mathbb{Q}_p(\omega)] \neq 0$.

Proof (of Proposition 2.7). We claim that under the assumptions of the theorem M possesses a finite free resolution. Indeed, since the Noetherian ring Λ has finite global dimension $\mathrm{pd}\,\Lambda = m + 1$, there is always a resolution of the form

$$0 \longrightarrow P \longrightarrow \Lambda^{d_m} \longrightarrow \cdots \longrightarrow \Lambda^{d_0} \longrightarrow 0,$$

with a projective module P. Since M^{e_i} is a $\Lambda(\Gamma)$-torsion module (it is even $\Lambda(\Gamma')$-torsion!) and since P^{e_i} is a free $\Lambda(\Gamma)$-module, it must hold that $P^{e_i} \cong (\Lambda(\Gamma))^{k_i d_{m+1}}$ as $\Lambda(\Gamma)$-modules, where $k_i = \chi(e_i)$ denotes the $\mathbb{Z}_p$-rank of $\mathbb{Z}_p[\Delta]e_i$ and $d_{m+1} = \sum_{i=0}^m (-1)^i d_{m-i}$. Consequently, $P_\Gamma^{e_i} \cong \mathbb{Z}_p^{k_i d_{m+1}}$ as $\mathbb{Z}_p$-modules, respectively $P_\Gamma^{e_i} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p^{k_i d_{m+1}}$ as $\mathbb{Q}_p$-modules holds. But $P_\Gamma^{e_i} \otimes \mathbb{Q}_p$ must be isomorphic to the direct sum of m copies of N_i for some m due to the semi-simplicity of $\mathbb{Q}_p[\Delta]$. Counting $\mathbb{Q}_p$-dimensions, we obtain $m = n_i d_{m+1}$ and hence $P_\Gamma^{e_i} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[\Delta]e_i^{d_{m+1}}$. Since $P_\Gamma^{e_i}$ is a projective $\mathbb{Z}_p[\Delta]$-module, this implies $P_\Gamma^{e_i} \cong \mathbb{Z}_p[\Delta]e_i^{d_{m+1}}$, respectively $P^{e_i} \cong \Lambda(G)e_i^{d_{m+1}}$ (compare to the proof of Lemma 2.6) and $P \cong \Lambda(G)^{d_{m+1}}$. This proves the claim.

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Furthermore, we observe that $\sum(-1)^i d_i = 0$ and denote the resolution by $F^* \to M$. Using the fact that the Euler characteristic of a bounded complex equals the Euler characteristic of its homology, we calculate

$$\begin{aligned}\sum(-1)^i[\mathrm{H}_i(U, M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p] &= \sum(-1)^i[\mathrm{H}_i(F^* \otimes_\Lambda \mathbb{Q}_p[G/U])] \\ &= \sum(-1)^i[F^* \otimes_\Lambda \mathbb{Q}_p[G/U]] \\ &= \sum(-1)^i[\mathbb{Q}_p[G/U]^{d_i}] \\ &= \Big(\sum(-1)^i d_i\Big)[\mathbb{Q}_p[G/U]] = 0. \qquad \square\end{aligned}$$

LEMMA 2.9. *Let G be a profinite group, $H \subseteq G$ a closed subgroup and $U \trianglelefteq G$ an open normal subgroup. Then for any compact $\mathbb{Z}_p[\![H]\!]$-module M the following is true:*

(i) $(\mathrm{Ind}_G^H(M))_U \cong \mathrm{Ind}_{G/U}^{HU/U}(M_{U\cap H})$ *and*
(ii) $\mathrm{H}_i(U, (\mathrm{Ind}_G^H(M))) \cong \mathrm{Ind}_{G/U}^{HU/U}\mathrm{H}_i(U \cap H, M)$ *for all $i \geqslant 0$.*

Proof. The dual statement of (i) is proved in [23] while (ii) follows from (i) by homological algebra. $\square$

LEMMA 2.10. *Let $G = \Gamma \times \Delta$ be the product of a pro-p-group Γ and a finite group Δ of order prime to p. Then, for any $\Lambda = \mathbb{Z}_p[\![\Gamma]\!][\Delta]$-module M and for any irreducible character χ of Δ with values in $\mathbb{Q}_p$, the following is true:*

(i) $\mathrm{Hom}_\Lambda(M^{e_\chi}, \Lambda) \cong \mathrm{Hom}_\Lambda(M, \Lambda)^{e_{\chi^{-1}}}$,
(ii) $\mathrm{E}^i_\Lambda(M^{e_\chi}) \cong \mathrm{E}^i_\Lambda(M)^{e_{\chi^{-1}}}$ *for any $i \geqslant 0$.*

Proof. While (ii) is a consequence of (i) by homological algebra the first statement can be verified at once using the decompositions $M \cong \bigoplus M^{e_\chi}$ and $\Lambda \cong \bigoplus \Lambda^{e_\chi}$:

$$\begin{aligned}\mathrm{Hom}_\Lambda(M, \Lambda)^{e_{\chi^{-1}}} &\cong \mathrm{Hom}_\Lambda(M, \Lambda^{e_\chi}) \\ &\cong \mathrm{Hom}_\Lambda(M^{e_\chi}, \Lambda^{e_\chi}) \\ &\cong \mathrm{Hom}_\Lambda(M^{e_\chi}, \Lambda). \qquad \square\end{aligned}$$

2.4. MODULES ASSOCIATED WITH GROUP PRESENTATIONS

Let $\mathcal{C}$ be a class of finite groups closed under taking subgroups, homomorphic images and group extensions. Given an exact sequence of pro-$\mathcal{C}$-groups $1 \to \mathcal{H} \to \mathcal{G} \to G \to 1$, where $\mathcal{G}$ is assumed to be finitely generated, we choose a presentation $\mathcal{F} \twoheadrightarrow \mathcal{G}$ of $\mathcal{G}$ by a free pro-$\mathcal{C}$-group $\mathcal{F}_d$ of rank d and we associate the following

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

commutative diagram to it:

$$\begin{array}{ccccccccc} & & 1 & & 1 & & & & \\ & & \uparrow & & \uparrow & & & & \\ 1 & \longrightarrow & \mathcal{H} & \longrightarrow & \mathcal{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & R & \longrightarrow & \mathcal{F}_d & \longrightarrow & G & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & & & \\ & & N & = & N & & & & \\ & & \uparrow & & \uparrow & & & & \\ & & 1 & & 1 & & & & \end{array} \tag{2.1}$$

Here, R and N are defined by the exactness of the corresponding sequences. In general, the *p-relation module* $N^{\mathrm{ab}}(p)$ *of* $\mathcal{G}$ *with respect to the chosen free presentation* (and similarly $R^{\mathrm{ab}}(p)$ with respect to G instead of $\mathcal{G}$) fits into the following exact sequence, which is called Fox–Lyndon resolution associated with the above free representation of $\mathcal{G}$:

$$0 \longrightarrow N^{\mathrm{ab}}(p) \longrightarrow \Lambda(\mathcal{G})^d \longrightarrow \Lambda(\mathcal{G}) \longrightarrow \mathbb{Z}_p \longrightarrow 0. \tag{2.2}$$

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

Furthermore, the augmentation ideal $I_{\mathcal{F}_d}$, i.e. the kernel of $\Lambda(\mathcal{F}_d) \to \mathbb{Z}_p$, is a free $\Lambda(\mathcal{F}_d)$-modules of rank d: $I_{\mathcal{F}_d} \cong \Lambda(\mathcal{F}_d)^d$ (for a proof of these facts, see [29], Chap. V.6).

Let A be a p-divisible p-torsion Abelian group of finite $\mathbb{Z}_p$-corank r with a continuous action of $\mathcal{G}$.

DEFINITION 2.11. For a finitely generated $\Lambda = \Lambda(\mathcal{G})$-module M we define the finitely generated Λ-module $M[A] := M \otimes_{\mathbb{Z}_p} A^{\vee} = \mathrm{Hom}_{\mathrm{cont.},\mathbb{Z}_p}(M, A)^{\vee}$ with diagonal $\mathcal{G}$-action. We shall also write $M(\rho)$ for this r-dimensional twist where $\rho\colon G \to \mathrm{Gl}_r(\mathbb{Z}_p)$ denotes the operation of G on $A^{\vee}$.

Note that the functor $-[A]$ is exact and that $\Lambda[A]$ is a free Λ-module of rank r (cf. [35, Lem. 4.2]).

PROPOSITION 2.12. *For every* $i \geqslant 0$, $\mathrm{E}^i(M(\rho)) \cong \mathrm{E}^i(M)(\rho^d)$, *where* ρ^d *is the contragredient representation, i.e.* $\rho^d(g) = \rho(g^{-1})^t$ *is the transpose matrix of* $\rho(g^{-1})$.

Proof. By homological algebra (and using a free presentation of M) it suffices to prove the case $i = 0$ for free modules. Finally, we only have to check the commutativity of the following diagram which is associated to an arbitrary

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

homomorphism $\phi\colon \Lambda \to \Lambda$

$$\begin{array}{ccc}
\mathrm{Hom}_{\Lambda}(\Lambda(\rho), \Lambda) & \xrightarrow{\phi(\rho)^*} & \mathrm{Hom}_{\Lambda}(\Lambda(\rho), \Lambda) \\
\downarrow & & \downarrow \\
\Lambda^r & & \Lambda^r \\
\downarrow & & \downarrow \\
\mathrm{Hom}_{\Lambda}(\Lambda, \Lambda)\,(\rho) & \xrightarrow{\phi^*(\rho^d)} & \mathrm{Hom}_{\Lambda}(\Lambda, \Lambda)\,(\rho).
\end{array}$$

First note that via the identification $\Lambda^r \overset{\psi_\rho}{=} \Lambda(\rho)$ the matrix representing $\phi(\rho)$ is $A := \sum a_g g \rho(g^{-1})$, where we assume for simplicity that $\phi(1) =: a = \sum a_g g \in \mathbb{Z}_p[G]$. We denote by $\imath$ both the involution $\Lambda \to \Lambda, g \mapsto g^{-1}$ (also extended to matrices with coefficients in Λ) and the isomorphism of left Λ-modules $\Lambda \to \mathrm{Hom}_{\Lambda}(\Lambda, \Lambda), g \mapsto (1 \mapsto g^{-1})$. Then its easy to see that the following two diagrams commute

$$\begin{array}{ccc}
\mathrm{Hom}_{\Lambda}(\Lambda(\rho), \Lambda) & \xrightarrow{\phi(\rho)^*} & \mathrm{Hom}_{\Lambda}(\Lambda(\rho), \Lambda) \\
\downarrow{\scriptstyle (\psi_\rho)^*} & & \downarrow{\scriptstyle (\psi_\rho)^*} \\
\mathrm{Hom}_{\Lambda}(\Lambda^r, \Lambda) & & \mathrm{Hom}_{\Lambda}(\Lambda^r, \Lambda) \\
\downarrow{\scriptstyle i^r} & & \downarrow{\scriptstyle i^r} \\
\Lambda^r & \xrightarrow{\quad \imath(A^t) \quad} & \Lambda^r,
\end{array}$$

$$\begin{array}{ccc}
\Lambda^r & \xrightarrow{\quad B \quad} & \Lambda^r \\
\downarrow{\scriptstyle \psi_{\rho^d}} & & \downarrow{\scriptstyle \psi_{\rho^d}} \\
\Lambda(\rho) & \xrightarrow{\quad \imath(a)(\rho^d) \quad} & \Lambda(\rho) \\
\downarrow{\scriptstyle i(\rho^d)} & & \downarrow{\scriptstyle i(\rho^d)} \\
\mathrm{Hom}_{\Lambda}(\Lambda, \Lambda)\,(\rho) & \xrightarrow{\phi^*(\rho)} & \mathrm{Hom}_{\Lambda}(\Lambda, \Lambda)\,(\rho),
\end{array}$$

where $B = \sum a_g g^{-1} \rho^d(g)$, because $\imath(a) = \sum a_g g^{-1}$. We are done if we can verify $B = \imath(A^t)$. But

$$\imath(A^t) = \sum a_g g^{-1} \rho(g^{-1})^t = \sum a_g g^{-1} \rho^d(g) = B. \qquad \square$$

With the notation

$$X := X_{\mathcal{H},A} := \mathrm{H}^1(\mathcal{H}, A)^\vee, \tag{2.3}$$

$$Y := Y_{\mathcal{H},A} := (I_{\mathcal{G}}[A])_{\mathcal{H}}, \tag{2.4}$$

$$J := J_{\mathcal{H},A} := \ker(\Lambda(\mathcal{G})[A]_{\mathcal{H}} \to (A^\vee)_{\mathcal{H}}), \tag{2.5}$$

we get the following proposition:

PROPOSITION 2.13 ([35, Lem. 4.5]). *We have a commutative and exact diagram*

$$
\begin{array}{ccccccccccc}
 & & & & & & 0 & & 0 & & \\
 & & & & & & \uparrow & & \uparrow & & \\
 & & & & & & J & & J & & \\
 & & & & & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{H}^2(\mathcal{H},A)^\vee & \longrightarrow & (N^{\mathrm{ab}}(p)[A])_{\mathcal{H}} & \longrightarrow & \Lambda(G)^{dr} & \longrightarrow & Y & \longrightarrow & 0 \\
 & & \| & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathrm{H}^2(\mathcal{H},A)^\vee & \longrightarrow & (\mathrm{H}^1(N,A)^{\mathcal{H}})^\vee & \longrightarrow & \mathrm{H}^1(R,A)^\vee & \longrightarrow & X & \longrightarrow & 0 \\
 & & & & & & \uparrow & & \uparrow & & \\
 & & & & & & 0 & & 0 & &
\end{array}
$$

Furthermore, if $\mathrm{cd}_p(\mathcal{G}) \leqslant 2$, *then* $N^{\mathrm{ab}}(p)[A]$ *is a projective* $\Lambda(\mathcal{G})$*-module and* $(N^{\mathrm{ab}}(p)[A])_{\mathcal{H}}$ *a projective* $\Lambda(G)$*-module.*

Remark 2.14. Assume A is trivial as $\mathcal{H}$-module. Then the above diagram can be easily obtained by twisting Jannsen's original diagram (i.e. with coefficients $\mathbb{Q}_p/\mathbb{Z}_p$): diagram$(A) =$ diagram$(\mathbb{Q}_p/\mathbb{Z}_p)[A]$. Also the higher Iwasawa adjoints of the occurring modules can be calculated via Proposition 2.12:

$$
\begin{aligned}
&\mathrm{E}^i(X_{\mathcal{H},A}) \cong \mathrm{E}^i(X_{\mathcal{H},\mathbb{Q}_p/\mathbb{Z}_p})(\rho^d),\\
&\mathrm{E}^i(Y_{\mathcal{H},A}) \cong \mathrm{E}^i(Y_{\mathcal{H},\mathbb{Q}_p/\mathbb{Z}_p})(\rho^d),\\
&\quad \ldots
\end{aligned}
$$

The following theorem is a consequence of the diagram. The restriction to p-adic Lie groups without p-torsion is necessary in order to apply the dimension theory developed in [40].

THEOREM 2.15. *Let* $\mathrm{cd}_p(\mathcal{G}) \leqslant 2$ *and* G *a* p*-adic Lie group of dimension* h *without* p*-torsion. If the 'weak Leopoldt conjecture holds for* A *and* $\mathcal{H}$*', i.e. if* $\mathrm{H}^2(\mathcal{H}, A) = 0$, *then neither* Y *nor* X *have nonzero pseudo-null submodules:* $\mathrm{T}_{h-1}(X) = \mathrm{T}_{h-1}(Y) = 0$.

Proof. Apply Proposition 3.10 of [40] to Y, which has $\mathrm{pd}(Y) \leqslant 1$ according to the above diagram, and note that $\mathrm{T}_{h-1}(X) \subseteq \mathrm{T}_{h-1}(Y)$ by Proposition 3.2 of [40]. □

Let

$$Z = Z_{\mathcal{H},A} := (D_2^{(p)}(\mathcal{G}, A)^{\mathcal{H}})^\vee, \tag{2.6}$$

where

$$D_2^{(p)}(\mathcal{G}, A) = \varinjlim_{U \subseteq_o \mathcal{G}, n} (H^2(U, {}_{p^n}A))^\vee$$

and the direct limit is taken with respect to the p-power map and the dual of the corestriction. Then there is a description of the $\Lambda(G)$-module Y as follows:

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

PROPOSITION 2.16. *Assume that* $\mathrm{cd}_p(\mathcal{G}) = 2$ *and that* $N^{\mathrm{ab}}(p)$ *is a finitely generated* $\Lambda(\mathcal{G})$*-module. Then* $Y \simeq DZ$ *and* $\mathrm{E}^0(Z) \cong \mathrm{H}^2(\mathcal{H}, A)^\vee$*, thus* Y *is determined by* Z *up to projective summands. Suppose, in addition, that* $\mathrm{H}^2(\mathcal{H}, A) = 0$*. Then* $\mathrm{E}^1(Y) \cong Z$.

For a proof of the Proposition, see [29], 5.6.8 and [33], Thm. 3.13.

3. Local Iwasawa Modules

3.1. THE GENERAL CASE

In this section we study the structure of Iwasawa modules arising from 'p-adic representations' $\mathcal{G} \to \mathrm{Aut}(A)$, where $\mathcal{G} = G_k$ is the absolute Galois group of a finite extension k of $\mathbb{Q}_\ell$ and A is a p-divisible p-torsion Abelian group of finite $\mathbb{Z}_p$-corank r. Having fixed a p-adic Lie extension k_∞ of k with Galois group G, we write $\mathcal{H} = G(\bar{k}/k_\infty) \subseteq \mathcal{G}$ where $\bar{k}$ denotes the algebraic closure of k. We are going to apply the general results of Section 2.4 to the module

$$X_A := X_{\mathcal{H},A} = \mathrm{H}^1(\mathcal{H}, A)^\vee = \mathrm{H}^1(k_\infty, A)^\vee,$$

i.e. we will determine the $\Lambda(G)$-modules occurring in the canonical exact sequence

$$0 \longrightarrow \mathrm{E}^1\mathrm{D}(X_A) \longrightarrow X_A \longrightarrow \mathrm{E}^0\mathrm{E}^0(X_A) \longrightarrow \mathrm{E}^2\mathrm{D}(X_A) \longrightarrow 0.$$

The statements in this section often say that the module X_A (or another one) fits into an exact sequence of $\Lambda(G)$-modules. In general, this will not determine its Galois-module structure uniquely. But if it happens that such a sequence describes X_A as 1st or 2nd syzygy of some $\Lambda(G)$-module with well-known structure, then the Galois-module structure of X_A is uniquely determined *up to homotopy*, i.e. up to projective summands (see Subsection 2.1).

For the sake of completeness and for the convenience of the reader we restate some general results from [34], but see also [33]. Since we have fixed $\mathcal{H}$, we shall omit it in the notation and write Y_A, Z_A, etc. Recall that G has finite cohomological dimension $\mathrm{cd}_p\, G = m$ if and only if G has no element of finite p-power order and its dimension as p-adic analytic manifold equals m.

LEMMA 3.1 (cf. [33]).

(i) *If* k *is a finite extension of* $\mathbb{Q}_\ell$ *and* k_∞ *is a Galois extension of* k*, then* $Z = A^*(k_\infty)^\vee$*, where* $A^* = (T_pA)^\vee(1)$ *by definition,*
(ii) $\mathrm{E}^1\mathrm{D}(X_A) \cong \mathrm{E}^1(A^*(k_\infty)^\vee)$,
(iii) $\mathrm{E}^2\mathrm{D}(X_A) \subseteq \mathrm{E}^2\mathrm{D}(Y_A) \cong \mathrm{E}^2(A^*(k_\infty)^\vee)$,
(iv) *If* $\mathrm{cd}_p(G) \leqslant 2$ *or* $\mathrm{cd}_p(G) = 3$ *and* $A(k_\infty)^\vee$ *is* $\mathbb{Z}_p$*-torsion-free, then* $\mathrm{D}X_A \simeq \mathrm{E}^1(X_A)$.

Proof. (i) is just local Tate duality while (ii) is a consequence of (i):

$$\mathrm{E}^1\mathrm{D}(X_A) \cong \mathrm{E}^1\mathrm{D}(Y_A) \cong \mathrm{E}^1(Z_A) \cong \mathrm{E}^1(A^*(k_\infty)^\vee)$$

(Note that the first isomorphism holds because J_A is torsion-free as $\Lambda(U)$-module for a suitable open pro-p-subgroup $U \subseteq G$, such that $\Lambda(U)$ is integral.) By the same reason and using the snake lemma, one sees that $\mathrm{E}^2\mathrm{D}(X_A) \subseteq \mathrm{E}^2\mathrm{D}(Y_A)$. To prove (iv) just note that in these cases $\mathrm{pd}\, X_A \leqslant 1$ by the Diagram 2.13, the defining sequence (2.5) of J_A, corollary [40, Cor. 6.3] and [40, Cor. 4.8]. □

Recall that for a finitely generated Abelian p-primary group A we denote by A_{div} the quotient of A by its maximal p-divisible subgroup. The next result generalizes a result of Greenberg [14]:

PROPOSITION 3.2 (cf. [34, Section 2]). *Let $n = [k : \mathbb{Q}_\ell]$, $\ell = p$, be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a Galois extension of k with Galois group $G \cong \Gamma \rtimes_\omega \Delta$, where $\Gamma \cong \mathbb{Z}_p$ and Δ is a finite group of order t prime to p, which acts on Γ via the character $\omega: \Delta \to \mathbb{Z}_p^*$. If $\chi = \omega^{-1}$ denotes the inverse of the character which determines the action on the p-dualizing module of G, the canonical sequence becomes*

$$0 \longrightarrow T_pA^*(k_\infty)(\chi) \longrightarrow X_A \longrightarrow P \longrightarrow M \longrightarrow 0,$$

where P is a projective $\Lambda(G)$-module of $\mathrm{rk}_{\Lambda(\Gamma)}P = rnt$ and M fits into the exact sequence

$$0 \longrightarrow M \longrightarrow A^*(k_\infty)_{\mathrm{div}}(\chi) \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(A(k_\infty)^\vee).$$

Furthermore,

(i) *if $A^*(k_\infty)$ is finite, then $T_pA^*(k_\infty)(\chi) = 0$. If, in addition, $A(k_\infty)^\vee$ is $\mathbb{Z}_p$-free, then $M \cong A^*(k_\infty)$.*
(ii) *if $A^*(k_\infty)^\vee$ is $\mathbb{Z}_p$-free, then $X_A \cong P \oplus T_pA^*(k_\infty)(\chi)$. In particular, X_A is projective, if $A^*(k_\infty) = 0$.*

Proof. First note that according to Lemma 3.1 and [40, Cor. 4.8]

$$\begin{aligned}\mathrm{E}^1\mathrm{D}(X_A) &\cong \mathrm{E}^1(A^*(k_\infty)^\vee)\\ &\cong \mathrm{E}^1(A^*(k_\infty)^\vee/\mathrm{tor}_{\mathbb{Z}_p})\\ &\cong (A^*(k_\infty)^\vee \otimes \mathbb{Q}_p/\mathbb{Z}_p(\chi^{-1}))^\vee\\ &\cong T_pA^*(k_\infty)(\chi).\end{aligned}$$

To determine $E^2\mathrm{D}(X_A) \cong \mathrm{E}^2\mathrm{E}^1(X_A)$ we use the short exact sequences ((2.5) and Proposition 2.13)

$$0 \longrightarrow X_A \longrightarrow Y_A \longrightarrow J_A \longrightarrow 0,$$
$$0 \longrightarrow J_A \longrightarrow \Lambda(G)^d \longrightarrow A(k_\infty)^\vee \longrightarrow 0,$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

i.e. $E^1(J_A) \cong E^2(A(k_\infty)^\vee) \cong A(k_\infty)_{\mathrm{div}}(\chi)$ by [40, Cor. 4.8] and

$$A(k_\infty)_{\mathrm{div}}(\chi) \longrightarrow E^1(Y_A) \longrightarrow E^1(X_A) \longrightarrow 0$$

is exact. Forming the long exact Ext-sequence and applying Lemma 3.1 and [40, Cor. 4.8] again, gives the desired result. □

Let us now consider the case $\ell \neq p$:

PROPOSITION 3.3 (cf. [34, Section 2]). *In the situation of the last theorem but with $\ell \neq p$ there is an isomorphism $X_A \cong T_pA^*(k_\infty)(\chi)$.*

Proof. In [33], Prop. 3.12, it was calculated that the $\Lambda(\Gamma)$-rank of X_A equals the $\Lambda(\Gamma)$-corank of $H^2(k_\infty, A)$, but the latter module vanishes because the order of G is divisible by p^∞ (cf. [29], 7.1.8). □

PROPOSITION 3.4 (cf. [34, Section 2]). *Let $n = [k : \mathbb{Q}_p]$ be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a p-adic Lie extension of k such that its Galois group G has cohomological dimension $\mathrm{cd}_p(G) = 2$. Let $\Gamma \subseteq G$ be an arbitrary open uniform pro-p-subgroup, i.e. $\Lambda(\Gamma)$ is integral, and let t be the index $(G : \Gamma)$. If χ denotes the inverse of the character which determines the action of G on the p-dualizing module, then the canonical sequence becomes*

$$0 \longrightarrow X_A \longrightarrow R \longrightarrow E^2D(X_A) \longrightarrow 0,$$

where R is a reflexive $\Lambda(G)$-module with $\mathrm{rk}_{\Lambda(\Gamma)} R = rnt$. If, in addition, $A(k_\infty)^\vee$ is $\mathbb{Z}_p$-free, then $E^2D(X_A)$ fits into the exact sequence

$$0 \longrightarrow E^2D(X_A) \longrightarrow T_pA^*(k_\infty)(\chi) \longrightarrow \mathrm{Hom}(T_pA(k_\infty), \mathbb{Z}_p).$$

Proof. Using again Lemma 3.1 and [40, Cor. 4.8], the proof is completely analogous to that in the one-dimensional case of Proposition 3.2. □

Note that in the case $p \neq l$ and $\mathrm{cd}_p(G) \geqslant 2$ we have $\mathcal{H} = 0$, i.e. $X_A = 0$, because the Galois group $G_k(p)$ of the maximal p-extension of any local field k over $\mathbb{Q}_\ell$ is isomorphic to $\mathbb{Z}_p(1) \rtimes \mathbb{Z}_p$ (resp. $\mathbb{Z}_p$) if $\mu_p \subseteq k$ (otherwise). Thus it does not have any nontrivial quotient G which satisfies these conditions.

PROPOSITION 3.5 (cf. [34, Section 2]). *Let $n = [k : \mathbb{Q}_p]$ be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a p-adic Lie extension of k such that its Galois group G has cohomological dimension $\mathrm{cd}_p(G) \geqslant 3$. Let $\Gamma \subseteq G$ be an arbitrary open uniform pro-p-subgroup, i.e. $\Lambda(\Gamma)$ is integral, and let t be the index $(G : U)$. Then $X_A \cong E^0E^0X_A$ is a reflexive $\Lambda(G)$-module with $\mathrm{rk}_{\Lambda(\Gamma)} X_A = rnt$.*

Proof. This follows from Lemma 3.1 and [40, Cor. 4.8] as above. □

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

At the end of this part we want to restate the results concerning the ranks of the considered modules. The result was obtained independently by S. Howson [17, 6.1] and Y. Ochi [33, Thm. 3.3], see also [34, Thm. 2].

PROPOSITION 3.6 (Howson, Ochi). *Let k be a finite extension of $\mathbb{Q}_\ell$ and k_∞ be a pro-p Lie extension of k with Galois group $G = G(k_\infty/k)$. As before r denotes the $\mathbb{Z}_p$-rank of* $\operatorname{rank}(A^\vee)$. *Assume that $\Lambda = \Lambda(G)$ is integral, then*

$$\operatorname{rk}_\Lambda \mathrm{H}^1(k_\infty, A)^\vee = \begin{cases} r[k:\mathbb{Q}_p] & \text{if } \ell = p, \\ 0 & \text{otherwise.} \end{cases}$$

Proof (cf. Ochi). Noting the vanishing of $\mathrm{H}^2(k_\infty, A)$ and that $N^{\mathrm{ab}}(p) \cong \Lambda(\mathcal{G})$ for $d = [k : \mathbb{Q}_p] + 2$ (conferring [20], Thm. 5.1c)), the result follows from the diagram in Proposition 2.13 and the above remarks with respect to the case $\ell \neq p$. □

3.2. THE CASE $A = \mathbb{Q}_p/\mathbb{Z}_p$

3.2.1. *Local Units*

If we specialize to the important case $A = \mathbb{Q}_p/\mathbb{Z}_p$ with trivial Galois action, we are able to determine the module structure more exactly using local class field theory: $X := X_{\mathbb{Q}_p/\mathbb{Z}_p} \cong \mathcal{H}^{\mathrm{ab}}(p)^\star$ is the Galois group of the maximal Abelian p-extension of k_∞, which is canonically isomorphic to the inverse limit $X \cong \mathbb{A}(k_\infty) := \varprojlim_{k'} \mathbb{A}(k')$ of the p-completions $\mathbb{A}(k')$ of the multiplicative groups of finite subextensions k' of k in $k_\infty : \mathbb{A}(k') = \varprojlim_m (k')^*/(k')^{*p^m}$, where the limit is taken via the norm maps. Since the Galois module structure of $\mathbb{A}(k')$ is well known if tensored with $\mathbb{Q}_p$, we get

THEOREM 3.7. *Let $n = [k : \mathbb{Q}_\ell]$, $\ell = p$, be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a Galois extension of k with Galois group $G \cong \Gamma \rtimes_\omega \Delta$, where $\Gamma \cong \mathbb{Z}_p$ and Δ is a finitely generated profinite group of order prime to p, which acts on Γ via the character $\omega: \Delta \to \mathbb{Z}_p^*$. We write k_0 for the fixed field of Γ and denote by $\chi = \omega^{-1}$ the inverse of the character which determines the action on the p-dualizing module of G.*

(i) *If $\mu_{p^\infty} \subseteq k_\infty$, i.e. k_∞ is the cyclotomic $\mathbb{Z}_p$-extension of k_0 and $G = \Gamma \times \Delta$, then it holds $\mathbb{A}(k_\infty) \cong \Lambda^n \oplus \mathbb{Z}_p(1)$.*

(ii) *Let $\mu(k_\infty)(p)$ be finite. Then there is an exact sequence of Λ-modules*

$$0 \longrightarrow \mathbb{A}(k_\infty) \oplus I_G \longrightarrow \Lambda^{n+1} \longrightarrow \mu(k_\infty)(p)(\chi) \longrightarrow 0.$$

For any presentation

$$1 \longrightarrow K \longrightarrow \mathcal{F}_{d'} \longrightarrow G \longrightarrow 1$$

by a free profinite group $\mathcal{F}_{d'}$ on $d' \leqslant n+1$ generators, there exists an exact sequence

$$0 \longrightarrow \mathbb{A}(k_\infty) \longrightarrow \Lambda^{n-d'+1} \oplus K^{\mathrm{ab}}(p) \longrightarrow \mu(k_\infty)(p)(\chi) \longrightarrow 0.$$

*This notation refers to diagram (2.1) of Section 2.4 where we represent the absolute local Galois group $\mathcal{G}$ of k by a free profinite group of rank $d = [k : \mathbb{Q}_\ell] + 2$ according to [29], Theorem 7.4.1.

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Remark 3.8. (i) The existence of a presentations in (ii) is always guaranteed by [19] Theorem 4.3. Indeed, one can choose $d' = 2$.

(ii) Using the Krull–Schmidt and Maschke's theorem, it is easily proved (see the proof below) that

$$\mathrm{E}^0(I_G)(\omega) \oplus I_G \cong \mathbb{Z}_p[\![G]\!]^2,$$
$$\bigoplus_{i=1}^{m-1} I_G(\omega^i) \oplus I_G \cong \mathbb{Z}_p[\![G]\!]^m,$$

where m denotes the order of ω. Hence, from the isomorphism $K^{\mathrm{ab}}(p) \oplus I_G \cong \mathbb{Z}_p[\![G]\!]^d$ according to the Lyndon sequence (2.2), we get isomorphisms (for $m \leqslant d$)

$$K^{\mathrm{ab}}(p) \cong \mathbb{Z}_p[\![G]\!]^{d-2} \oplus \mathrm{E}^0(I_G)(\omega)$$
$$\cong \mathbb{Z}_p[\![G]\!]^{d-m} \oplus \bigoplus_{i=1}^{m-1} I_G(\omega^i).$$

In particular, if ω is an involution and $d = 2$, then $K^{\mathrm{ab}}(p) \cong \mathrm{E}^0(I_G)(\omega) \cong I_G(\omega)$ holds.

Proof. Let us first consider the case that Δ is a finite group, which grants that $\Lambda(G)$ is Noetherian. Then the statements are consequences of Theorem 3.2 once having determined the structure of $P = \mathrm{E}^0\mathrm{E}^0 X$. We will apply the Krull–Schmidt theorem and we first observe that for any open normal subgroup $U \trianglelefteq \Gamma$ and $\bar{G} := G/U$ it holds: $X_U \otimes \mathbb{Q}_p \cong P_U \otimes \mathbb{Q}_p$ and, if k' denotes the fixed field of U, there are exact sequences of $\bar{G}$-modules

$$0 \longrightarrow U^{\mathrm{ab}}(p) \longrightarrow (I_G)_U \longrightarrow \mathbb{Z}_p[\bar{G}] \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$
$$0 \longrightarrow X_U \longrightarrow \bar{G}^{\mathrm{ab}}_{k'}(p) \longrightarrow U^{\mathrm{ab}}(p) \longrightarrow 0.$$

Hence, by Maschke's theorem and using $\bar{G}^{\mathrm{ab}}_{k'}(p) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[\bar{G}]^n \oplus \mathbb{Q}_p$ (cf. [29], 7.4.3), we get

$$P_U \otimes \mathbb{Q}_p \oplus (I_G)_U \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[\bar{G}]^{n+1},$$

i.e. $P \oplus I_G \cong \Lambda^{n+1}$.

Now, taking U-coinvariants of the augmentation sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}_p[\![G]\!] \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

and tensoring with $\mathbb{Q}_p(\omega^i)$ gives

$$\mathbb{Q}_p[\bar{G}] \oplus \mathbb{Q}_p(\omega^{i+1}) \cong (I_G(\omega^i))_U \otimes \mathbb{Q}_p \oplus \mathbb{Q}_p(\omega^i).$$

For (i) just note that I_G is projective and ω trivial because Δ acts trivially on Γ, hence: $I_G \cong \mathbb{Z}_p[\![G]\!]$. The first sequence in (ii) is immediate while the second one results from the isomorphism $K^{\mathrm{ab}}(p) \oplus I_G \cong \mathbb{Z}_p[\![G]\!]^d$ according to the Lyndon sequence (2.2).

Now let us assume that Δ is infinite. If $\Delta' \subseteq \Delta$ is an open subgroup then the functor obtained by taking Δ'-coinvariants is exact because $\mathrm{H}_1(\Delta', M) = 0$ for any Λ-module M. Since the automorphism group is virtually pro-p, there is an open normal subgroup Δ_0 of Δ which acts trivially on Γ, in particular any open normal subgroup Δ' of Δ which is contained in Δ_0 is normal in G. Now a free presentation of G

$$1 \longrightarrow K \longrightarrow \mathcal{F}_{d'} \longrightarrow G \longrightarrow 1$$

induces a free presentation of $G' := G/\Delta'$

$$1 \longrightarrow K_{\Delta'} \longrightarrow \mathcal{F}_{d'} \longrightarrow G/\Delta' \longrightarrow 1.$$

Using the Lyndon sequence, it is easy to verify that $(I_G)_{\Delta'} \cong I_{G/\Delta'}$ and $K^{\mathrm{ab}}(p)_{\Delta'} \cong K^{\mathrm{ab}}_{\Delta'}(p)$. Now the strategy is as follows. Take a $\Lambda(G)$-module M and show that for any Δ' as above its Δ'-coinvariants are isomorphic to certain finitely generated $\Lambda(G')$-modules of the same type, e.g. $\mathbb{A}(k') \oplus I_{G'}$, where k' is the fixed field of k_∞ by Δ'. Then it follows easily (using a compactness argument to grant the existence of a compatible system of isomorphisms) that $M \cong \mathbb{A}(k_\infty) \oplus I_G$. As an example we prove the first statement in (ii): choose a surjection $\Lambda(G)^{n+1} \twoheadrightarrow \mu(k_\infty)(p)(\chi)$ and define M to be the kernel of it. Taking Δ'-coinvariants and comparing it with the result for k', i.e. for (finite) Δ/Δ', we obtain an isomorphism $M_{\Delta'} \cong \mathbb{A}(k') \oplus I_{G'}$ by Schanuel's lemma (see [20, 1.3] for a generalized version). The other statements follow by similar arguments.

The second isomorphism of the remark can be deduced by summing up $(I_G(\omega^i))_U \otimes \mathbb{Q}_p$ for $0 \leqslant i \leqslant m$. For the first one, use that due to the projectivity of I_G

$$\begin{aligned} \mathrm{E}^0(I_G)_U \otimes \mathbb{Q}_p &\cong \mathrm{Hom}_{\mathbb{Z}_p[\![G]\!]}(I_G, \mathbb{Z}_p[\![G]\!])_U \otimes \mathbb{Q}_p \\ &\cong \mathrm{Hom}_{\mathbb{Z}_p[\bar{G}]}((I_G)_U, \mathbb{Z}_p[\bar{G}]) \otimes \mathbb{Q}_p \\ &\cong \mathrm{Hom}_{\mathbb{Q}_p}((I_G)_U, \mathbb{Q}_p) \otimes \mathbb{Q}_p \end{aligned}$$

holds. □

THEOREM 3.9. *In the situation of the last theorem but with $\ell \neq p$ there is an isomorphism*

$$X \cong \begin{cases} \mathbb{Z}_p(1)(\chi) & \text{if } \mu_p \subseteq k_0, \\ 0 & \text{otherwise.} \end{cases}$$

The next theorem generalizes results of Wintenberger [42] who restricts himself to the case in which G is Abelian. It applies for example to $\Gamma \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Recall that R, respectively $R^{\mathrm{ab}}(p)$, were defined via diagram (2.1).

THEOREM 3.10. *Let $n = [k : \mathbb{Q}_p]$ be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a Galois extension of k with Galois group $G \cong \Gamma \times_\rho \Delta$, where Γ is a pro-p Lie group of dimension 2 and Δ is a profinite group of order prime to p, which acts on Γ via $\rho\colon \Delta \to \mathrm{Aut}(\Gamma)$. Let k_0 be the fixed field of Γ and let $\chi = \det \rho^{-1}$ denote the inverse of the character which determines the action on the p-dualizing module of G.*

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(i) *If* $\mu(k_0)(p) = 1$*, then* $X \oplus \Lambda \cong R^{\mathrm{ab}}(p)$*. If* ρ *is trivial, then* $X \cong \Lambda^n$*.*

(ii) *If* $\mu_{p^\infty} \subseteq k_\infty$ *and* G *is without p-torsion and such that its dualizing module is not isomorphic to* μ_{p^∞}*, then there is an exact sequence of* Λ*-modules*

$$0 \longrightarrow X \oplus \Lambda \longrightarrow R^{\mathrm{ab}}(p) \longrightarrow \mathbb{Z}_p(1)(\chi) \longrightarrow 0.$$

If ρ *is trivial, then*

$$0 \longrightarrow X \longrightarrow \Lambda^n \longrightarrow \mathbb{Z}_p(1) \longrightarrow 0$$

is exact.

(iii) *If* $\mu(k_\infty)(p)$ *and* Δ *are finite, then* $X \cong \mathrm{E}^0\mathrm{E}^0(X)$ *is reflexive, i.e. there is an exact sequence*

$$0 \longrightarrow X \longrightarrow R^{\mathrm{ab}}(p) \longrightarrow \Lambda \longrightarrow \mu(k_\infty)(p).$$

If, in addition, $\mu(k)(p) = 1$*, but* $\mu(k_\infty)(p) \neq 1$ *and* $\chi^{-1} \neq \chi_{\mathrm{cycl}}$*, then the right map is also surjective (in particular* X *is not free in this case).*

Remark 3.11. For extensions $k_\infty \mid k$ of the type $G \cong \Gamma \times \Delta$ with $\Gamma \cong \mathbb{Z}_p^s$, $s \geqslant 3$ and finite Δ, we can consider the relative situation

$$0 \longrightarrow X(k_\infty)_{\Gamma'} \longrightarrow X(K_\infty) \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

where Γ' is direct factor of Γ isomorphic to $\mathbb{Z}_p$, i.e. $\Gamma \cong \Gamma' \times \mathbb{Z}_p^{s-1}$, and K_∞ is the fixed field of k_∞ with respect to Γ'. By induction and applying Diekert's theorem ([29]) one reobtains at once Wintenberger's results (but now more generally with not necessarily Abelian Δ): For any irreducible character $\chi \neq 1, \chi_{\mathrm{cycl}}$ the component $X(k_\infty)^{e_\chi}$ is a free $\Lambda(G)^{e_\chi}$-module of rank n $X(k_\infty)^{e_\chi} \cong (\Lambda(G)^{e_\chi})^n$. But since we already know that $\mathrm{pd}_\Lambda X = s - 2$ for $s \geqslant 3$, X can not be projective in this case, i.e. $X(k_\infty)^{e_1}$ or $X(k_\infty)^{e_{\chi_{\mathrm{cycl}}}}$ is definitely not of this type.

We will prove the theorem only for finite Δ because the general case follows similarly as in Theorem 3.7. Just note that also in this case the automorphism group of Γ is virtually pro-p (see [10, 5.6]). But before giving the proof we need some preparation:

LEMMA 3.12. *Let* $G = \Gamma \times \Delta$ *be the product of a pro-p Lie group* Γ *with* $\mathrm{cd}_p(\Gamma) = 2$ *and a finite group* Δ *of order prime to p. Then* $R^{\mathrm{ab}}(p) \cong \Lambda^{n+1}$*.*

Proof. Let $U_n := p^n\Gamma \trianglelefteq G$. By the Lyndon sequence (2.2) and using Proposition 2.7, we calculate the Euler characteristic $h_{U_n}(R^{\mathrm{ab}}(p)) = h_{U_n}(\mathbb{Z}_p) + h_{U_n}(\Lambda^{n+1}) = h_{U_n}(\Lambda^{n+1})$. The result follows. □

LEMMA 3.13. *If in the situation of the theorem* $\mu(k_\infty)(p)$ *is infinite, then both* $\mathrm{E}^0(X)$ *and* $\mathrm{E}^0\mathrm{E}^0(X)$ *are projective.*

Proof. Since $\mathrm{E}^0(-)$ preserves projectives and $\mathrm{E}^0\mathrm{E}^0\mathrm{E}^0(X) \cong \mathrm{E}^0(X)$ by [40, Prop. 3.11], it is sufficient to prove the statement for $\mathrm{E}^0\mathrm{E}^0(X)$. But according to Proposition 2.5, the latter module is the 2-syzygy of $\mathrm{E}^3\mathrm{E}^1(X)$. We claim that $Y \simeq X \oplus \Lambda$,

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

i.e. that $\mathrm{E}^3\mathrm{E}^1(X) \cong \mathrm{E}^3\mathrm{E}^1(Y) \cong \mathrm{E}^3(\mu(k_\infty)(p)^\vee) = 0$, which implies the lemma. Indeed, due to Poincaré-duality

$$\mathrm{H}^2(G, \mu(k_\infty)(p))^\vee \cong \mathrm{Hom}_G(\mu(k_\infty)(p), D_2^{(p)}) = 0,$$

if $D_2^{(p)} \neq \mu_{p^\infty}$. Hence, $Y \simeq X \oplus \Lambda$ by the second description of 4.5(b) in [20]*. □

Proof of the Theorem. Let $U_m = p^m\Gamma \trianglelefteq G$ and denote the fixed field of U_m by k_m. From the exact sequence

$$1 \longrightarrow G_{k_\infty} \longrightarrow G_{k_m} \longrightarrow U_m \longrightarrow 1$$

we obtain the associated homological Hochschild–Serre sequence

$$0 = \mathrm{H}_2(k_m, \mathbb{Z}_p) \longrightarrow \mathrm{H}_2(U_m, \mathbb{Z}_p) \longrightarrow X_{U_m} \longrightarrow G_{k_m}^{\mathrm{ab}}(p) \longrightarrow \mathrm{H}_1(U_m, \mathbb{Z}_p) \longrightarrow 0.$$

After tensoring with $\mathbb{Q}_p$, it follows that

$$X_{U_m} \otimes \mathbb{Q}_p \oplus \mathrm{H}_1(U_m, \mathbb{Z}_p) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[\bar{G}]^n \oplus \mathbb{Q}_p \oplus \mathrm{H}_2(U_m, \mathbb{Z}_p) \otimes \mathbb{Q}_p,$$

where we used Maschke's theorem and $\bar{G}_{k_m}^{\mathrm{ab}}(p) \otimes \mathbb{Q}_p \cong \mathbb{Q}_p[\bar{G}]^n \oplus \mathbb{Q}_p$ (cf. [29], 7.4.3). On the other hand, the Euler characteristic of the projective module $R^{\mathrm{ab}}(p)$ can be calculated by means of the Lyndon sequence:

$$\begin{aligned}[R^{\mathrm{ab}}(p)_{U_m} \otimes \mathbb{Q}_p] &= h_{U_m}(R^{\mathrm{ab}}(p)) \\ &= h_{U_m}(\mathbb{Z}_p) + h_{U_m}(\Lambda^{n+1}) \\ &= [\mathbb{Q}_p] - [\mathrm{H}_1(U_m, \mathbb{Z}_p) \otimes \mathbb{Q}_p] + [\mathrm{H}_2(U_m, \mathbb{Z}_p) \otimes \mathbb{Q}_p] + \\ &\quad + [\mathbb{Q}_p[\bar{G}]^{n+1}]\end{aligned}$$

and, hence, $X_{U_m} \otimes \mathbb{Q}_p \oplus \mathbb{Q}_p[\bar{G}] \cong R^{\mathrm{ab}}(p)_{U_m} \otimes \mathbb{Q}_p$.

Assume that $\mu(k_0)(p) = 1$, i.e. $\mathrm{tor}_{\mathbb{Z}_p}\mathbb{A}(k_0) = 1$ and X_{U_0} is $\mathbb{Z}_p$-free. Therefore, since t is prime to p, it follows that X_{U_0} is $\mathbb{Z}_p[\Delta]$-projective. If ρ is trivial, we conclude, by the calculation above under consideration of $h_{U_m}(\mathbb{Z}_p) = 0$ (by Lemma 2.7) and using the Krull–Schmidt theorem, that $X_{U_0} \cong \mathbb{Z}_p[\Delta]^n$. Applying Lemma 2.6, gives the desired result in this case. Anyway, these arguments show that X is projective also in the case with non-trivial ρ, i.e. we obtain $X \oplus \Lambda \cong R^{\mathrm{ab}}(p)$ in the general case.

In order to prove (ii), we apply Theorem 3.4: Since $X \oplus \Lambda \simeq Y$ in this case (see the proof of Lemma 3.13), we obtain

$$\begin{aligned}\mathrm{E}^2 D(X) &\cong \mathrm{E}^2 D(Y) \\ &\cong \mathrm{E}^2(\mathbb{Z}_p(-1)) \\ &\cong \mathbb{Z}_p(1)(\chi),\end{aligned}$$

*For $\Gamma = \mathbb{Z}_p^2$ this statement was proved by Jannsen ([20], 5.2(c)): Though there the claimed isomorphism $R^{\mathrm{ab}}(p) \cong \Lambda^{d-1}$ is only correct if ρ is trivial, the arguments (which we restated above) still prove $X \oplus \Lambda \simeq Y$.

where we applied Lemma 3.1 and [20, 2.6]. Note that

$$\chi^{-1}(x) = \det(Adx) = \det\rho(x)\colon G \to \Delta \overset{\det\rho}{\to} \mathbb{Z}_p^*$$

(cf. [24] V 2.5.8.1). We still have to determine the module $P = \mathrm{E}^0\mathrm{E}^0(X)$, which is projective according to Lemma 3.3: it is easily seen that $P_{U_m} \otimes \mathbb{Q}_p \cong X_{U_m} \otimes \mathbb{Q}_p$, i.e. $P \oplus \Lambda \cong R^{\mathrm{ab}}(p)$, by the above calculations. If ρ is trivial, Lemma 3.2 gives the desired result.

The first statement of (iii) is just Theorem 3.4 and Lemma 3.1. By Proposition 2.5, we obtain an exact sequence

$$0 \longrightarrow X \longrightarrow P \longrightarrow \Lambda^s \longrightarrow \mu(k_\infty)(p)$$

for some s. Splitting up the sequence, taking the long exact $\mathrm{H}_i(U_m, -)$-sequences and using the above calculations, one immediately sees that $P_{U_m} \otimes \mathbb{Q}_p \cong R^{\mathrm{ab}}(p)_{U_m} \otimes \mathbb{Q}_p \oplus \mathbb{Q}_p[\bar{G}]^{s-1}$, i.e. $P \cong R^{\mathrm{ab}}(p) \oplus \Lambda^{s-1}$. After possibly changing the basis of Λ^d and using the Krull–Schmidt theorem, one easily sees that we can get rid off the summand Λ^{s-1}.

In order to prove the last statement, we assume that $\chi^{-1} \neq \chi_{\mathrm{cycl}}$ and consider the exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{E}^1(X)^\vee & \longrightarrow & \mathrm{E}^1(Y)^\vee & \longrightarrow & \mathrm{E}^1(I)^\vee \\ & & & & \| & & \| \\ & & & & \mu(k_\infty)(p) & & \mathbb{Q}_p/\mathbb{Z}_p(\chi^{-1}). \end{array}$$

The decomposition of the sequence with respect to the irreducible $\mathbb{Q}_p$-characters of Δ gives $(\mathrm{E}^1(X)^\vee)^{\chi_{\mathrm{cycl}}} = \mu(k_\infty)(p)^{\chi_{\mathrm{cycl}}} = \mu(k_\infty)(p)$. □

3.2.2. *Principal Units*

When $l = p$, we are also interested in the Λ-structure of the inverse limit of the principal units $\mathbb{U}^1(k_\infty) := \varprojlim_{k'} \mathbb{U}^1(k')$, where k' runs through all finite subextensions of $k_\infty \mid k$ and the limit is taken with respect to the norm maps.

PROPOSITION 3.14. *Let k be a finite extension of $\mathbb{Q}_p$ and k_∞ a Galois extension of k.*

(i) *If k_∞ contains the maximal unramified p-extension of k, i.e. if p^∞ divides the degree of the residue field extension associated with $k_\infty \mid k$, then $\mathbb{U}^1(k_\infty) \cong \mathbb{A}(k_\infty)$.*
(ii) *In the other case there is the following exact sequence*

$$0 \longrightarrow \mathbb{U}^1(k_\infty) \longrightarrow \mathbb{A}(k_\infty) \longrightarrow \mathbb{Z}_p \longrightarrow 0.$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Proof. For finite extensions $K' \,|\, K \,|\, k$ of k with associated residue field extensions $\lambda' \,|\, \lambda \,|\, \kappa$ consider the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{U}^1(K')/p^m & \longrightarrow & \mathbb{A}(K') & \longrightarrow & \mathbb{Z}_p/p^m & \longrightarrow & 0 \\ & & \Big\downarrow N_{K'/K} & & \Big\downarrow N_{K'/K} & & \Big\downarrow [\lambda' : \lambda] & & \\ 0 & \longrightarrow & \mathbb{U}^1(K)/p^m & \longrightarrow & \mathbb{A}(K) & \longrightarrow & \mathbb{Z}_p/p^m & \longrightarrow & 0. \end{array}$$

While in case (i) the inverse limit $\lim_{\longleftarrow_{K,m}} \mathbb{Z}_p/p^m$ vanishes, because for any m and any K there is an extension K' such that $p^m \,|\, [\lambda' : \lambda]$, in the second case it is isomorphic to $\mathbb{Z}_p$. □

THEOREM 3.15. *Assume in the situation of Theorem* 3.10 *that k_∞ contains μ_{p^∞} but not the maximal unramified p-extension of k. Then there exists an exact sequence*

$$0 \longrightarrow \mathbb{U}^1(k_\infty) \oplus \Lambda \longrightarrow R^{\mathrm{ab}}(p) \longrightarrow M \longrightarrow 0,$$

where M fits into the exact sequence

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow M \longrightarrow \mathbb{Z}_p(1)(\chi) \longrightarrow 0.$$

In particular, if ρ is trivial, there exists an exact sequence

$$0 \longrightarrow \mathbb{U}^1(k_\infty) \longrightarrow \Lambda^n \longrightarrow M \longrightarrow 0.$$

Proof. Evaluating the long exact E^i-sequence associated with the exact sequence from the proposition above and noting that $\mathrm{pd}_\Lambda \mathbb{U}^1(k_\infty) \leqslant 1$ due to $\mathrm{pd}_\Lambda \mathbb{A}(k_\infty) \leqslant 1$ and $\mathrm{pd}_\Lambda \mathbb{Z}_p = 2$, one obtains that

(i) $\mathrm{E}^0(\mathbb{U}^1(k_\infty)) \cong \mathrm{E}^0(X)$,
(ii) $\mathrm{E}^1\mathrm{D}(\mathbb{U}^1(k_\infty)) = 0$ and an exact sequence,
(iii) $0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathrm{E}^2\mathrm{D}(\mathbb{U}^1(k_\infty)) \longrightarrow \mathbb{Z}_p(1)(\chi) \longrightarrow 0$.

Here we used that $\mathrm{E}^2\mathrm{E}^2(\mathbb{Z}_p) \cong \mathbb{Z}_p$, because $\mathbb{Z}_p$ is a Cohen–Macaulay module of dimension 2. The result follows from the canonical sequence. □

Remark 3.16. In the situation of Theorem 3.7 with trivial action of Δ the structure of the principal units is described in [29] as follows:

(i) If $\mu_{p^\infty} \subseteq k_\infty$, then

$$\mathbb{U}^1(k_\infty) \cong \Lambda^n \oplus \mathbb{Z}_p(1).$$

(ii) If $\mu(k_\infty)(p)$ is finite, then there is an exact sequence

$$0 \longrightarrow \mathbb{U}^1(k_\infty) \longrightarrow \Lambda^n \longrightarrow \mu(k_\infty)(p).$$

(iii) If $k_\infty \,|\, k$ is unramified, then $\mathbb{U}^1(k_\infty) \cong \mathbb{A}(k_\infty)$.

But the proof of [29] works also if ω is not trivial.

3.3. THE LOCAL CM-CASE

As a consequence of Theorem 3.10 we can also determine up to homotopy the structure of $X_A = \mathrm{H}^1(k_\infty, A)^\vee$ in the trivializing case, i.e. $k(A) \subseteq k_\infty$:

THEOREM 3.17. *Let $n = [k:\mathbb{Q}_p]$ be the finite degree of k over $\mathbb{Q}_p$ and k_∞ a Galois extension of k with Galois group $G \cong \Gamma \rtimes_\rho \Delta$, where Γ is a pro-p Lie group of dimension 2 and Δ is a finite group of order t prime to p, which acts on Γ via $\rho\colon \Delta \to \mathrm{Aut}(\Gamma)$. Let k_0 be the fixed field of Γ and let $\chi = \det \rho^{-1}$ denote the inverse of the character which determines the action on the p-dualizing module of G. For any A with $\mathrm{rk}_{\mathbb{Z}_p} A^\vee = r$ such that $k(A) \subseteq k_\infty$ the following is true.*

(i) *If $\mu(k_0)(p) = 1$, then $X_A \oplus \Lambda^r \cong R^{\mathrm{ab}}(p)[A]$, in particular, if ρ is trivial: $X_A \cong \Lambda^{nr}$.*

(ii) *If $\mu_{p^\infty} \subseteq k_\infty$ and G is p-torsion-free and its dualizing module is not isomorphic to μ_{p^∞}, then there is an exact sequence of Λ-modules*

$$0 \longrightarrow X_A \oplus \Lambda^r \longrightarrow R^{\mathrm{ab}}(p)[A] \longrightarrow A^\vee(1)(\chi) \longrightarrow 0.$$

In particular, if ρ is trivial, then

$$0 \longrightarrow X_A \longrightarrow \Lambda^{nr} \longrightarrow A^\vee(1) \longrightarrow 0$$

is exact.

(iii) *If $\mu(k_\infty)(p)$ is finite, then $X_A \cong \mathrm{E}^0\mathrm{E}^0(X_A)$ is reflexive, i.e. there is an exact sequence*

$$0 \longrightarrow X_A \longrightarrow R^{\mathrm{ab}}(p)[A] \longrightarrow \Lambda^r \longrightarrow \mu(k_\infty)(p)[A].$$

If, in addition, $\mu(k)(p) = 1$, but $\mu(k_\infty)(p) \neq 1$ and $\chi^{-1} \neq \chi_{\mathrm{cycl}}$, then the right map is also surjective (in particular, X_A is not free in this case).

Proof. In this case the subgroups $\mathcal{H}$, R and N act trivially on $A = A(k_\infty)$, i.e. $X_A \cong X[A]$. □

This result applies to the following situation: Let K be a imaginary quadratic number field, F a finite, Abelian extension of K and E an elliptic curve defined over F with complex multiplication (CM) by the ring of integers $\mathcal{O}_K$ of K such that $F(E_{\mathrm{tor}})$ is an Abelian extension of K. Assume that the rational prime p splits in K, i.e. $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, and that E has good reduction at all places lying over p. Set $G = G(F(E(p))/F)_{\mathfrak{P}}$ the decomposition group at some $\mathfrak{P} \mid \mathfrak{p}$. According to [9, 1.9], the prime $\mathfrak{P}$ ramifies totally in $F(E(\mathfrak{p})) \mid F$ and decomposes only finitely (and is unramified) in $F(E(\bar{\mathfrak{p}})) \mid F$. Therefore the decomposition group G is an open subgroup of $G(F(E(p))/F)$, i.e. of type $\mathbb{Z}_p^2 \times \Delta$ where Δ is a finite Abelian group. Thus we obtain an exact sequence

$$0 \longrightarrow \mathrm{H}^1(F(E(p))_{\mathfrak{P}}, E(p))^\vee \longrightarrow \Lambda(G)^{2n} \longrightarrow T_pE \longrightarrow 0,$$

where $n = [F_{\mathfrak{p}}:\mathbb{Q}_p]$. By the same argument, but now using Theorem 3.7(ii), there

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

exists an exact sequence

$$0 \longrightarrow \mathrm{H}^1(F(E(\mathfrak{p})_{\mathfrak{P}}, E(\mathfrak{p}))^{\vee} \longrightarrow \Lambda(G')^n \longrightarrow \mu(F(E(\mathfrak{p})_{\mathfrak{P}})[E(\mathfrak{p})] \longrightarrow 0,$$

where $G' = G(F(E(\mathfrak{p}))/F)_{\mathfrak{P}}$, and a similar one for $\bar{\mathfrak{p}}$.

4. Global Iwasawa Modules

Let k_∞ be a p-adic Lie extension of the number field k contained in k_S with Galois group G and let A be a p-divisible p-torsion Abelian group with $\mathbb{Z}_p$-corank r and on which $G_S(k) = G(k_S/k)$ acts continuously where S is a finite set of places of k containing all places S_p over p and all infinite places S_∞ (and by definition all places at which A is ramified). Here k_S denotes the maximal S-ramified extension of k, i.e. the maximal extension of k which is unramified outside S. In order to derive information about the $\Lambda = \Lambda(G)$-modules $\mathrm{H}^i(G(k_S/k_\infty), A)$ we would like to apply the diagram (2.1) to the group $\mathcal{G} = \mathcal{G}_S := G(k_S/k)$. On the other hand we have to guarantee that $\mathcal{G}$ is finitely generated as a profinite group which, unfortunately, is not known for the group $\mathcal{G}_S$. But using a theorem of Neumann, i.e. the inflation maps are isomorphisms

$$\mathrm{H}^i(G(\Omega/k_\infty), A) \cong \mathrm{H}^i(G_S(k_\infty), A), \quad i \geqslant 0,$$

for any (p, S)-closed extension Ω of k (i.e. Ω is a S-ramified extension of k which does not possess any nontrivial S-ramified p-extension) and for any p-torsion $G(\Omega/k_\infty)$-module A, we are free to replace $G_S(k)$ for example by the Galois group $\mathcal{G} := G(\Omega/k)$ where Ω is the maximal S-ramified p-extension of $k'(A)$ and k' is a Galois subextension of k_∞/k such that $G(k_\infty/k')$ is an open (normal) pro-p-group. Regarding this technical detail, we assume in what follows that k_∞ is contained in such a (p, S)-closed field Ω. Then, since $\mathcal{G}$ has an open pro-p Sylow group, it is finitely generated and has $\mathrm{cd}_p(\mathcal{G}) \leqslant 2$ for odd p. Note that $Y_{S,A} := Y_{G(\Omega/k_\infty),A}$ (2.4) and $X_{S,A} := X_{G(\Omega/k_\infty),A}$ (2.3) do not depend on the choice of Ω. The next lemma shows among other things that the corresponding module Z (2.6) only depends on k_∞, A and S. Recall that $T_pA = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A)$ denotes the 'Tate module' of A. We shall write $\mathrm{H}^*_{cts}(G_S(k), T_pA) \cong \lim_{\leftarrow_n} \mathrm{H}^*(G_S(k), {}_{p^n}A)$ for the continuous cochain cohomology groups (see [29, II. Section 3.]).

LEMMA 4.1. *Let k, k_∞ and A be as above. Then*

$$Z_{S,A} := Z_{G(\Omega/k_\infty),A} \cong \varprojlim_{k \subseteq k' \subseteq k_\infty} H^2_{cts}(G_S(k'), T_pA).$$

A basic structure result is the following theorem:

THEOREM 4.2. *Let G a p-adic Lie group without p-torsion. If the 'weak Leopoldt conjecture holds for A and k_∞', i.e. $\mathrm{H}^2(G_S(k_\infty), A) = 0$, then neither $Y_{S,A}$ nor $X_{S,A} \cong \mathrm{H}^1(G_S(k_\infty), A)^{\vee}$ have nonzero pseudo-null submodules.*

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Proof. The conditions of Theorem 2.15 are fulfilled. □

Furthermore, the Λ-rank of $X_{S,A}$ can be determined, using diagram (2.4):

THEOREM 4.3 (Ochi [34]). *Let $k_\infty \mid k$ be a p-adic pro-p extension. Assume that $k(A) \mid k$ is a pro-p-extension and that Λ is an integral domain. Then*

$$\mathrm{rk}_\Lambda \mathrm{H}^1(G_S(k_\infty), A)^\vee - \mathrm{rk}_\Lambda \mathrm{H}^2(G_S(k_\infty), A)^\vee = r_2(k)r$$

Here $r_2(k)$ denotes as usual the number of complex places of k.

Thus, if the weak Leopoldt conjecture holds for A and k_∞, one obtains a simple formula for the Λ-rank of $\mathrm{H}^1(G_S(k_\infty), A)^\vee$. So, we conclude with a brief discussion and motivation concerning this conjecture:

In [21] Jannsen extended the *strong* Leopoldt conjecture, which is equivalent to the vanishing of $\mathrm{H}^2(G_S(k), \mathbb{Q}_p/\mathbb{Z}_p)$, to the following setting: Let X be a smooth projective variety of pure dimension over k and assume that S contains S_p, S_∞ and all places S_{bad} where X has bad reduction. Then the étale cohomology $T^i(n) := \mathrm{H}^i_{\text{ét}}(X \times_k \bar{k}, \mathbb{Z}_p(n))$ is a compact $G_S(k)$-module which is finitely generated over $\mathbb{Z}_p$; here $\bar{k}$ denotes as usual an algebraic closure of k. Hence $A^i(n) := T^i(n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is a p-divisible discrete $G_S(k)$-module, for $X = \mathrm{Spec}(k)$ and $i = 0$ isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)(n)$. Assuming $p \neq 2$ or that k is totally imaginary his conjecture (cf. [21, Conjecture 1, Lem. 1]) predicts

$$\mathrm{H}^2(G_S(k), A^i(n)) = 0 \quad \text{if} \begin{cases} \text{(i)} & i+1<n, \quad \text{or} \\ \text{(ii)} & i+1 > 2n. \end{cases}$$

Thus, if this conjecture true for fixed X, i as well as n for *all* number fields contained in k_∞, it implies obviously the weak Leopoldt conjecture for $A^i(n)$ over k_∞. While in the 'unstable' range $n \leqslant i+1 \leqslant 2n$ the cohomology group $\mathrm{H}^2(G_S(k), A^i(n))$ is nontrivial in general, it is supposed to vanish after going up a 'nice' p-adic Lie-extension (cf. Corollary 4.8 for an example of this phenomena).

It is a result of Iwasawa that over the cyclotomic $\mathbb{Z}_p$-extension of *any* number field the *original* weak Leopoldt (i.e. for $A = \mathbb{Q}_p/\mathbb{Z}_p$) holds and consequently for $(\mathbb{Q}_p/\mathbb{Z}_p)(n)$ for all $n \in \mathbb{Z}$ (see [29, 10.3.25] for a cohomological proof). This leads to

Remark 4.4. The weak Leopoldt conjecture for A and k_∞ holds for example if $k(A)$ and the cyclotomic $\mathbb{Z}_p$-extension of k are contained in k_∞. The claim follows by expressing $\mathrm{H}^2(G_S(k_\infty), A)$ (considered as Abelian group) as direct limit $\lim_{\longleftarrow_{k'}} \mathrm{H}^2(G_S(k'_{\mathrm{cyc}}), \mathbb{Q}_p/\mathbb{Z}_p)^r$, where k' runs through the finite extensions of k in k_∞.

For a discussion about the weak Leopoldt conjecture over the cyclotomic $\mathbb{Z}_p$-extension of a number field for other p-adic representations than above we refer the reader to Section 1.3 and Appendix B of [36].

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

4.1. THE MULTIPLICATIVE GROUP $\mathbb{G}_m$

4.1.1. *The Maximal Abelian p-Extension of k_∞ Unramified Outside S*

We still consider p-adic Lie extensions $k_\infty \mid k$ with Galois group $G = G(k_\infty/k)$ such that k_∞ is contained in the maximal S-ramified extension k_S of k. Here, as before, S denotes a finite set of places of k containing all places S_p over p and all infinite places S_∞. For $K\mid k$ finite let $S_f(K)$ be the set of finite primes in K lying above S. In this paragraph we specialize to the case $A = \mathbb{Q}_p/\mathbb{Z}_p$ and we shall write X_S for the $\Lambda = \Lambda(G)$-module $X_{S,\mathbb{Q}_p/\mathbb{Z}_p}$ (2.3)

$$X_S := X_{S,\mathbb{Q}_p/\mathbb{Z}_p} = \mathrm{H}^1(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong G(k_S/k_\infty)^{\mathrm{ab}}(p),$$

and respectively for Y_S (2.4) and Z_S (2.6).

In this case, Theorem 4.2 is a generalization of the theorems of Greenberg [13] and Nguyen-Quang-Do [31], who considered the case $G \cong \mathbb{Z}_p^d$. Indeed, it confirms Greenberg's suggestion that an analogous statement also should hold for p-adic Lie extensions.

THEOREM 4.5. *Let G be a p-adic Lie group without p-torsion. If the 'weak Leopoldt conjecture holds for k_∞', i.e. $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, then $X_S \cong G_S(k_\infty)^{\mathrm{ab}}(p)$ has no nonzero pseudo-null Λ-submodule.*

Remark 4.6. Recall that the weak Leopoldt conjecture for k_∞ holds if the cyclotomic $\mathbb{Z}_p$-extension of k is contained in k_∞.

We will also consider the Λ-modules

$$X_{nr} = G(L/k_\infty), \qquad X_{cs}^S = G(L'/k_\infty),$$

where L is the maximal Abelian unramified pro-p-extension of k_∞ and L' is the maximal subextension in which every prime above S is completely decomposed.

For an arbitrary number field K, we denote the ring of integers (resp. S-integers) by $\mathcal{O}_K$ (resp. $\mathcal{O}_{K,S}$) and its units by $E(K) := \mathcal{O}_K^\times$ (resp. $E_S(K) := \mathcal{O}_{K,S}^\times$). Then we define

$$\mathbb{E} := \varprojlim_{k'} (\mathcal{O}_{k'}^\times \otimes \mathbb{Z}_p), \qquad \mathbb{E}_S := \varprojlim_{k'} (\mathcal{O}_{k',S}^\times \otimes \mathbb{Z}_p),$$

where the limit is taken with respect to the norm maps. This should not be confused with the discrete module of units (resp. S-units) $E(k_\infty) = \varinjlim_{k'} E(k')$ (resp. $E_S(k_\infty) = \varinjlim_{k'} E_S(k')$).

Finally, we write for the local-global modules

$$\mathbb{A}_S = \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} \mathbb{A}_v, \qquad \mathbb{U}_S = \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} \mathbb{U}_v,$$

where $\mathbb{A}_v = \mathbb{A}(k_{\infty,v})$ (resp. $\mathbb{U}_v = \mathbb{U}^1(k_{\infty,v})$) are the local modules introduced in Section 3.2. The above modules are connected via global class field theory and the Poitou–Tate sequence as follows

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

PROPOSITION 4.7 (Jannsen). *There are the following exact and commutative diagrams of Λ-modules:*

(i)

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{H}^2(G_S(k_\infty),\mathbb{Q}_p/\mathbb{Z}_p)^\vee & \longrightarrow & \mathbb{E} & \longrightarrow & \mathbb{U}_S & \longrightarrow & X_S & \longrightarrow & X_{nr} & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^2(G_S(k_\infty),\mathbb{Q}_p/\mathbb{Z}_p)^\vee & \longrightarrow & \mathbb{E}_S & \longrightarrow & \mathbb{A}_S & \longrightarrow & X_S & \longrightarrow & X^S_{cs} & \longrightarrow & 0 \end{array}$$

(ii)

$$0 \longrightarrow \mathbb{E} \longrightarrow \mathbb{E}_S \longrightarrow \bigoplus_{S_{un}(k)} \mathrm{Ind}_G^{G_v}\mathbb{Z}_p \longrightarrow X_{nr} \longrightarrow X^S_{cs} \longrightarrow 0,$$

where $S_{un} := \{v \in S(k) \mid p^\infty \nmid f_v\}$ *and* $f_v = f(k_{\infty,v}/k_v)$ *denotes the degree of the extension of the corresponding residue class fields.*

(iii)

$$0 \longrightarrow X^S_{cs} \longrightarrow Z_{S,\mathbb{Q}_p/\mathbb{Z}_p(1)} \longrightarrow \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v}\mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

and, if $\mu_{p^\infty} \subseteq k_\infty$,

$$0 \longrightarrow X_{cs}(-1) \longrightarrow Z_S \longrightarrow \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v}\mathbb{Z}_p(-1) \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0.$$

In particular, $X^S_{cs} = X_{cs} := X^{S_p}_{cs}$ *is independent of* S *in this case.*

(iv) $N^{\mathrm{ab}}(p)$ *(see* (2.1)–(2.2)) *is a finitely generated, projective* $\Lambda(G(k_{\infty S}(p)/k))$*-module and, if the free presentation of* $\mathcal{G} = G(k_{\infty S}(p)/k)$ (*cf.* Section 2.4) *is chosen such that* $d \geqslant r_1' + r_2 + 1$, *then*

$$N^{\mathrm{ab}}(p)_{G_S(k_\infty)(p)} \cong \bigoplus_{S'_\infty} \mathrm{Ind}_G^{G_v}\mathbb{Z}_p \oplus \Lambda(G)^{d-r_2-r_1'-1},$$

where S'_∞ *is the set of real places of* k *which ramify* (*i.e. become complex*) *in* k_∞, r_1' *is the cardinality of* S'_∞, *and* r_2 *is the number of complex places of* k.

Proof. The assertions (i) and (iii) are obtained by taking inverse limits of the Tate–Poitou sequence (see [20, Thm. 5.4]) and recalling Lemma 4.1 while (ii) follows from (i) by the snake lemma and Proposition 3.14. □

From these diagrams and the fact that Λ is Noetherian it follows that the modules X_{nr}, X^S_{cs} are finitely generated. Furthermore, S. Howson [17, 7.14–7.16] and Y. Ochi [33, 4.10] independently proved that X_{nr} and X^S_{cs} are Λ-torsion. Actually, this result was first proved by M. Harris [15, Thm. 3.3] but, as S. Howson remarked, his proof is incomplete because it relies on the false 'strong Nakayama' lemma ([15, Lemma 1.9]), see the discussion in [2]. However, in a recent correction Harris [16] has given a new proof of the result. In the case $G \cong \mathbb{Z}_p^d$, this result is originally proved by Greenberg [12].

COROLLARY 4.8. (i) *If* $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p(1)) = 0$ (*e.g. if* $\dim(G_v) \geqslant 1$ *for all* $v \in S_f$), *then* X^S_{cs} *is a* Λ*-torsion module.*

(ii) *If* $\dim(G_v) \geqslant 1$ *for all* $v \in S_f$, *then* X_{nr} *is a* Λ*-torsion module.*

For example, the conditions of the corollary are satisfied if k_∞ contains the cyclotomic $\mathbb{Z}_p$-extension.

Proof (cf. [34]). The first statement follows from 2.16 while the second one is a consequence of the first one and the above proposition (To calculate the (co)dimension of $\mathrm{Ind}^{G_v}_G \mathbb{Z}_p$ use [40, 4.8, 4.9]. Note that the condition '$\dim(G_v) \geqslant 1$ for all $v \in S_f$' implies, using Tate–Poitou duality,

$$\begin{aligned}\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p(1)) &= \text{Ш}^2(G_S(k_\infty), \mu_{p^\infty})\\ &= \varinjlim_{k',n} \text{Ш}^1(G_S(k'), \mathbb{Z}/p^n)^\vee\\ &= \varinjlim_{k'} \mathrm{Cl}_S(k') \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\\ &= 0\end{aligned}$$

because $\mathrm{Cl}_S(k')$ is finite. □

THEOREM 4.9. *If* $\mu_{p^\infty} \subseteq k_\infty$, *and* $\dim(G_v) \geqslant 2$ *for all* $v \in S_f$, *then*

$$X_{nr}(-1) \sim X^S_{cs}(-1) \sim \mathrm{E}^1(Y_S) \sim \mathrm{E}^1(\mathrm{tor}_\Lambda Y_S) \cong \mathrm{E}^1(\mathrm{tor}_\Lambda X_S).$$

If, in addition, $G \cong \mathbb{Z}^r_p$, $r \geqslant 2$, *then even the following holds:*

$$X_{nr}(-1) \sim X^S_{cs}(-1) \sim (\mathrm{tor}_\Lambda X_S)^\circ,$$

where $^\circ$ *means that* G *operates via the involution* $g \mapsto g^{-1}$.

Remark 4.10. In case $\mathrm{tor}_\Lambda X_S$ is isomorphic in Λ-mod$/\mathcal{PN}$ to a direct sum of cyclic modules of the form Λ modulo a (left) principal ideal the Proposition 2.4 implies that

$$E^1(\mathrm{tor}_\Lambda X_S) \equiv (\mathrm{tor}_\Lambda X_S)^\circ \bmod \mathcal{PN}$$

holds under the conditions of the theorem.

Proof. Note that $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, since Remark 4.4 applies. The first two pseudo-isomorphisms follow again from Proposition 4.7 using [40, 4.8,4.9] and 2.16. The third one is just [40, Prop. 3.13]. Note that there is even an isomorphism $\mathrm{tor}_\Lambda Y_S \cong \mathrm{tor}_\Lambda X_S$ because the augmentation ideal I_G is torsion-free. □

The following consequence generalizes a result of McCallum [25, Thm. 8] who considered the $\mathbb{Z}^r_p$-case:

COROLLARY 4.11. *With the assumptions of the theorem the following holds.*

(i) *There is a pseudo-isomorphism* $\mathrm{tor}_\Lambda X_S \sim \mathrm{E}^1(X_{cs}^S(-1))$.
(ii) *If* $\dim(G) \geqslant 3$, *then there is an isomorphism* $\mathrm{tor}_\Lambda X_S \cong \mathrm{E}^1(X_{cs}^S(-1))$.

Proof. The cokernel $K := \mathrm{coker}(X_{cs}^S(-1) \hookrightarrow Z_S \cong \mathrm{E}^1(Y_S))$ is pseudo-null, i.e. $\mathrm{E}^1(K) = 0$. If $\dim(G) \geqslant 3$, then $\mathrm{E}^2(K) = 0$, too, as can be calculated using [40, Prop. 2.7]. Now, the long exact E-sequence gives the result observing $\mathrm{E}^1\mathrm{E}^1(Y_S) \cong \mathrm{E}^1\mathrm{D}\,Y_S \cong \mathrm{tor}_\Lambda Y_S \cong \mathrm{tor}_\Lambda X_S$. □

Remark 4.12. The condition '$\dim(G_v) \geqslant 2$ for all $v \in S_f$', is known to hold in 'most' extensions arising from geometry, e.g. for the set $S_f = S_{\mathrm{bad}} \cup S_p$, if $k_\infty = k(\mathcal{A}(p))$ arises by adjoining the p-division points of an abelian variety $\mathcal{A}$ over k with good reduction at all places dividing p and such that $G(k_\infty/k)$ is a pro-p-group without p-torsion, see (the proof of) Corollary 4.38 below. The latter condition is satisfied if, for instance, k contains, $k({}_p\mathcal{A})$ for $p \neq 2$ or $k({}_{p^2}\mathcal{A})$ for $p = 2$, see at the beginning of Section 2.1.

Other important cases are the following ones:

(a) Let k_∞ be the maximal multiple $\mathbb{Z}_p$-extension $\tilde{k}$ of k, i.e. the composite of all $\mathbb{Z}_p$-extensions of k, and assume that $\mu_{2p} \subseteq k$ or
(b) let k_∞ be a multiple $\mathbb{Z}_p$-extension with $G \cong \mathbb{Z}_p^r$, $r \geqslant 2$, and assume that there is only one prime of k lying over p.

Then, as has been observed independently by T. Nguyen-Quang-Do [32, Thm. 3.2] and McCallum [25, Proof of Thm. 7], the condition holds for $S = S_p \cup S_\infty$. Indeed, since $\mathbb{Q}(\mu_{2p})$ has only one prime dividing p, it suffices to consider the second case. But then all inertia groups T_v, $v \in S_p$, are conjugate, thus they are all equal and hence an open subgroup of G due to the finiteness of the ideal class group.

With respect to the composite $\tilde{k}$ of all $\mathbb{Z}_p$-extensions of k there is the following outstanding conjecture:

CONJECTURE (R. Greenberg). For any number field k, the $\Lambda(G(\tilde{k}/k))$-module X_{nr} is pseudo-null.

Recently, W. McCallum [25] proved this conjecture for the base field $k = \mathbb{Q}(\mu_p)$ under some mild assumptions. For a list of other cases in which this conjecture is known to hold, see [32, Rem. 4.6]. Assume that $\mu_p \subseteq k$ and that the condition '$\dim(G_v) \geqslant 2$, for all $v \in S_f$', holds. Then, by the above theorem and Theorem 4.5, Greenberg's conjecture is equivalent to the statement that X_S is Λ-torsion-free, compare with [32, 4.4] and [25, Cor. 13].

The observation of the previous proof leads also to:

PROPOSITION 4.13. *If* $\dim(G_v) \geqslant 2$ *for all* $v \in S_f$, *then* $\mathbb{E} \sim \mathbb{E}_S$.

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

We are also interested in the (Pontryagin duals of the) direct limits

$$\mathrm{Cl}_S(k_\infty)(p) = \varinjlim_{k'} \mathrm{Cl}_S(k')(p),$$
$$\mathcal{E}_S(k_\infty) := (E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\vee,$$

of the p-part of the ideal class group, resp. of the global (S-)units of finite extensions k' of k inside k_∞.

PROPOSITION 4.14. *Let T be a set of places of k such that $S_\infty \subseteq T \subseteq S$. Assume that* $\dim(T_v) \geqslant 1$ *for all $v \in S\backslash T$, where $T_v \subseteq G_v$ denotes the inertia group of v.*

(i) *There is an exact sequence of Λ-modules*

$$0 \longrightarrow \mathrm{Cl}_S(k_\infty)(p)^\vee \xrightarrow{\psi} \mathrm{Cl}_T(k_\infty)(p)^\vee \longrightarrow \mathcal{E}_S(k_\infty) \xrightarrow{\varphi} \mathcal{E}_T(k_\infty) \longrightarrow 0.$$

(ii) *Assume that $S\backslash T = \{v\}$. Then, if* $\dim(G_v) \geqslant 1$ (*resp.* $\dim(G_v) \geqslant 2$), *then* $\mathrm{coker}(\psi) \cong \ker(\varphi)$ *is Λ-torsion* (*resp. pseudo-null*).

(iii) *If* $\dim(G_v) \geqslant 2$ *for every $v \in S\backslash T$, then there are canonical pseudo-isomorphisms*

$$\mathrm{Cl}_S(k_\infty)(p)^\vee \sim \mathrm{Cl}_T(k_\infty)(p)^\vee, \quad \mathcal{E}_S(k_\infty) \sim \mathcal{E}_T(k_\infty).$$

Proof. Consider the canonical exact diagram for a finite extension k' of k in k_∞

$$E_T(k') \otimes_{\mathbb{Z}} \mathbb{Z}_p \overset{i_{k'}}{\hookrightarrow} E_S(k') \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \bigoplus\nolimits_{(S\backslash T)(k')} \mathbb{Z}_p \longrightarrow \mathrm{Cl}_T(k')(p) \overset{\pi_{k'}}{\twoheadrightarrow} \mathrm{Cl}_S(k')(p).$$

Setting

$$C(k') := \mathrm{coker}(i_{k'}) \quad (\text{resp. } D(k') := \ker(\pi_{k'})),$$
$$C_\infty = \varinjlim C(k') \quad (\text{resp. } D_\infty = \varinjlim D(k'))$$

and tensoring with $\mathbb{Q}_p/\mathbb{Z}_p$, we get the following exact sequences

$$0 \to E_T(k') \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to E_S(k') \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to C(k') \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to 0,$$
$$0 \longrightarrow D(k') \longrightarrow C(k') \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \bigoplus\nolimits_{(S\backslash T)(k')} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$
$$0 \longrightarrow D(k') \longrightarrow \mathrm{Cl}_T(k')(p) \longrightarrow \mathrm{Cl}_S(k')(p) \longrightarrow 0.$$

Taking the direct limit over all finite subextensions k', we get an isomorphism $D_\infty \cong C_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p$ because the transition maps for the sum of the $\mathbb{Q}_p/\mathbb{Z}_p$'s is just the multiplication with the ramification index. The first result follows after taking the Pontryagin dual. Now assume that $S\backslash T$ consists of a single prime and set $\bar{G} := G(k'/k)$. Since then $\bar{G}_v = G_v G(k_\infty/k')/G(k_\infty/k')$ acts trivial on $\bigoplus_{(S\backslash T)(k')} \mathbb{Z}_p \cong \mathrm{Ind}_{\bar{G}}^{\bar{G}_v} \mathbb{Z}_p$ and therefore also on $C(k') \otimes \mathbb{Q}_p/\mathbb{Z}_p$, it follows that G_v acts trivial on $(C_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$. But then any surjection $\Lambda^n \twoheadrightarrow (C_\infty \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ factors through $(\mathrm{Ind}_G^{G_v} \mathbb{Z}_p)^n$ which is torsion (resp. pseudo-null) if $\dim(G_v) \geqslant 1$ (resp. $\dim(G_v) \geqslant 2$). The last statement is a consequence of the second one. □

The Λ-modules $\mathrm{Cl}_S(k_\infty)(p)^\vee$ and $\mathcal{E}_S(k_\infty)$ are related to each other and to X_S via Kummer theory:

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

PROPOSITION 4.15. *Assume that* $\mu_{p^\infty} \subseteq k_\infty$, *then the following holds:*

(i) *There are exact sequences of* Λ*-modules*

$$0 \longrightarrow \mathrm{Cl}_S(k_\infty)(p)^\vee \longrightarrow X_S(-1) \longrightarrow \mathcal{E}_S(k_\infty) \longrightarrow 0$$

and, if k_∞ *is contained in* k_Σ, *where* $\Sigma = S_p \cup S_\infty$,

$$0 \longrightarrow \mathrm{Cl}(k_\infty)(p)^\vee \longrightarrow X_\Sigma(-1) \longrightarrow \mathcal{E}(k_\infty) \longrightarrow 0.$$

In particular, $\mathrm{Cl}_S(k_\infty)(p)^\vee$ *and* $\mathrm{Cl}(k_\infty)(p)^\vee$ *do not contain any pseudo-null submodule in these cases.*

(ii) $\mathrm{Cl}_S(k_\infty)(p)^\vee$ *is* Λ*-torsion. If* $\dim(G_v) \geqslant 1$ *for every* $v \in S_p$, *then* $\mathrm{Cl}(k_\infty)(p)^\vee$ *is* Λ*-torsion, too. In particular, there are exact sequences*

$$0 \longrightarrow \mathrm{Cl}_S(k_\infty)(p)^\vee \longrightarrow \mathrm{tor}_\Lambda X_S(-1) \longrightarrow \mathrm{tor}_\Lambda \mathcal{E}_S(k_\infty) \longrightarrow 0,$$
$$0 \longrightarrow \mathrm{Cl}(k_\infty)(p)^\vee \longrightarrow \mathrm{tor}_\Lambda X_\Sigma(-1) \longrightarrow \mathrm{tor}_\Lambda \mathcal{E}(k_\infty) \longrightarrow 0.$$

Proof. The long exact $\mathrm{H}^i(G(k_S/k_\infty), -)$-sequence of

$$0 \to \mu_{p^n} \to E_S(k_S) \xrightarrow{p^n} E_S(k_S) \to 0$$

induces the short exact sequence

$$0 \longrightarrow E_S(k_\infty)/p^n \to \mathrm{H}^1(G(k_S/k_\infty), \mu_{p^\infty}) \to_{p^n} \mathrm{H}^1(G(k_S/k_\infty), E_S(k_s)) \to 0,$$

i.e. after taking the direct limit with respect to n

$$0 \to E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{H}^1(G(k_S/k_\infty), \mathbb{Q}_p/\mathbb{Z}_p)(1) \to \mathrm{Cl}_S(k_\infty)(p) \to 0.$$

Taking the dual, we obtain the first statement. A canonical map $\mathrm{Cl}(k_\infty(p)^\vee) \to X_S(-1)$ which is compatible with the inclusion $\mathrm{Cl}_S(k_\infty)(p)^\vee \to X_S(-1)$ from the first sequence can be defined exactly as in the $\mathbb{Z}_p$-case, see [29, 11.4.2 and errata]. Then the exactness of the second sequence at the first term is obtained from the first one and Proposition 4.15:

$$\mathrm{Cl}(k_\infty)(p)^\vee/\mathrm{Cl}_\Sigma(k_\infty)(p)^\vee \subseteq \mathcal{E}_\Sigma \cong X_\Sigma(-1)/\mathrm{Cl}_\Sigma(k_\infty)(p)^\vee,$$

i.e. $\mathrm{Cl}(k_\infty)(p)^\vee$ can be considered as submodule of $X_\Sigma(1)$ and then its quotient is $\mathcal{E}$.

Comparing the ranks of X_S and $\mathcal{E}_S$ (see 4.27) (with respect to an arbitrary open subgroup $H \subseteq G$ such that $\Lambda(H)$ is integral), we conclude that $\mathrm{Cl}_S(k_\infty)(p)^\vee$ is Λ-torsion while the analogous result for $\mathrm{Cl}(k_\infty)(p)^\vee$ follows from Proposition 4.15. Now, the last sequences can be derived from the prior ones by rank considerations or by applying the snake lemma to the canonical sequence of homotopy theory (2.2). □

QUESTION 4.16. Is it true for any p-adic Lie extension k_∞ (of dimension at least one) that $\mathrm{Cl}(k_\infty)(p)^\vee$ and $\mathrm{Cl}_S(k_\infty)(p)^\vee$ don't have no nonzero pseudo-null Λ-submodules?

In the $\mathbb{Z}_p$-case there exists a remarkable duality between the inverse and direct limit of the (S-) ideal class groups in the $\mathbb{Z}_p$-tower, viz the pseudo-isomorphisms

$$X_{nr} \sim \mathrm{E}^1(\mathrm{Cl}(k_\infty)(p)^\vee) \sim (\mathrm{Cl}(k_\infty)(p)^\vee)^\circ,$$
$$X_{cs}^S \sim \mathrm{E}^1(\mathrm{Cl}_S(k_\infty)(p)^\vee) \sim (\mathrm{Cl}_S(k_\infty)(p)^\vee)^\circ.$$

Therefore it seems natural (though maybe very optimistic) to pose the following

QUESTION 4.17. Is it true that for any p-adic Lie extension (at least under the assumption '$\dim(G_v) \geqslant 2$, for all $v \in S_f$,') there exist pseudo-isomorphisms

$$X_{nr} \sim \mathrm{E}^1(\mathrm{Cl}(k_\infty)(p)^\vee) \equiv (\mathrm{Cl}(k_\infty)(p)^\vee)^\circ \bmod \mathcal{PN},$$
$$X_{cs}^S \sim \mathrm{E}^1(\mathrm{Cl}_S(k_\infty)(p)^\vee) \equiv (\mathrm{Cl}_S(k_\infty)(p)^\vee)^\circ \bmod \mathcal{PN}?$$

Observe, that $X_{nr} \sim X_{cs}^S$ and $\mathrm{Cl}_S(k_\infty)(p)^\vee \sim \mathrm{Cl}(k_\infty)(p)^\vee$ by Propositions 4.7 and 4.14. Hence, it would suffice to prove the existence of one of the pseudo-isomorphisms. By Proposition 4.15(ii) and Theorem 4.9 the question would be true if one could show that the Λ-torsion of $\mathcal{E}_S(k_\infty)$ is pseudo-null. But it seems difficult to prove the latter statement directly. In fact, in the case of a multiple $\mathbb{Z}_p$-extension $k_\infty \mid k$ where $\mu_{p^\infty} \subseteq k_\infty$ and k has only one prime above p, W. McCallum [25, Thm. 7] answers the above question positively and then derives $\mathrm{tor}_\Lambda \mathcal{E}_S(k_\infty) = 0$ just from the desired pseudo-isomorphism. This is the only case to the knowledge of the author where a positive answer to this question is known. Also J. Nekovar [28, 0.14.2] proved partial results in the direction of the question. In a forthcoming paper [39], we will present the first non-Abelian example (for $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ the semidirect product of two copies of $\mathbb{Z}_p$), in which such a duality holds.

The next result generalizes theorem 11.3.7 of [29].

THEOREM 4.18. *Let $k_\infty \mid k$ be a p-adic pro-p Lie extension such that G is without p-torsion and $\mathbb{F}_\varphi[[G]]$ is an integral domain. Then $\mathcal{G} = G(k_S(p)/k_\infty)$ is a free pro-p-group if and only if $\mu(X_S) = 0$ and the weak Leopoldt conjecture holds:* $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Proof. Since $\mathcal{G}$ is pro-p it is free if and only if $\mathrm{H}^2(\mathcal{G}, \mathbb{Z}/p) = 0$, i.e. if and only if ${}_p(X_S)$ and $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ vanish. But, by Remark 3.33 of [40] and since X_S does not contain any pseudo-null submodule, these two conditions are equivalent to the vanishing of $\mu(X_S)$ and the validity of the weak Leopoldt conjecture. □

The next theorem, which generalizes theorem 11.3.8 in [29], shows that the validity of the weak Leopoldt conjecture and the vanishing of the μ-invariant are properties which should be considered simultaneously if one studies the behavior of X_S under change of the base field.

THEOREM 4.19. *Let $K \mid k$ be a finite Galois p-extension inside k_S, $k_\infty \mid k$ a p-adic pro-p Lie extension such that*

$$G = G(k_\infty/k) \text{ is without } p\text{-torsion and } \mathbb{F}_\varphi[[G]] \text{ is an integral.} \qquad (*)$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Set $K_\infty = Kk_\infty$ and $G' = G(K_\infty/K)$. Then G' satisfies the condition ($*$), *too, and the following holds*

$$\left\{\begin{matrix}\mu(X_S(k_\infty/k)) = 0 \text{ and} \\ \mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}\mu(X_S(K_\infty/K)) = 0 \text{ and} \\ \mathrm{H}^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0\end{matrix}\right\}.$$

In particular, if k_∞ contains the cyclotomic $\mathbb{Z}_p$-extension, then

$$\mu(X_S(k_\infty/k)) = 0 \Leftrightarrow \mu(X_S(K_\infty/K)) = 0.$$

Proof. Let $\mathcal{H}' := \mathcal{H} \cap G(k_S(p)/K)$. Then, by Theorem 4.18, the statements to be compared are equivalent to the freeness of $\mathcal{H}$, resp. $\mathcal{H}'$, thus equivalent to $\mathrm{cd}_p(\mathcal{H}) = 1$, resp. $\mathrm{cd}_p(\mathcal{H}') = 1$. But, since $\mathcal{H}'$ is open in $\mathcal{H}$ and $\mathrm{cd}_p(\mathcal{H}) < \infty$, we have $\mathrm{cd}_p(\mathcal{H}') = \mathrm{cd}_p(\mathcal{H})$ by [29] 3.3.5(ii). □

The same arguments prove the following theorem:

THEOREM 4.20. *Let $K_\infty \,|\, k_\infty \,|\, k$ be p-adic pro-p Lie extensions (inside k_S) such that for both $G(K_\infty/K)$ and $G(k_\infty/k)$ the condition* ($*$) *of the previous theorem holds. Then*

$$\left\{\begin{matrix}\mu(X_S(k_\infty/k)) = 0 \text{ and} \\ \mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0\end{matrix}\right\} \Leftrightarrow \left\{\begin{matrix}\mu(X_S(K_\infty/K)) = 0 \text{ and} \\ \mathrm{H}^2(G_S(K_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0\end{matrix}\right\}.$$

The next theorem, which generalizes Theorem 11.3.5 in [29], describes the 'difference' if we vary the finite set of places S defining the module X_S. By $T(K/k) \subseteq G(K/k)$ we shall denote the inertia subgroup for a Galois extension $K\,|\,k$ of local fields and, for an arbitrary set of places S of k and a p-adic analytic extension $k_\infty\,|\,k$, we write $S^{cd}(k)$ for the subset of finite places which decompose completely in $k_\infty\,|\,k$.

THEOREM 4.21. *Let $S \supseteq T \supseteq S_p \cup S_\infty$ be finite sets of places of k and let $k_\infty\,|\,k$ be a p-adic pro-p Lie extension inside k_T with Galois group G. Assume that G does not contain any p-torsion element and that the weak Leopoldt conjecture holds for $k_\infty\,|\,k$. Then there exists a canonical exact sequence of Λ-modules*

$$0 \longrightarrow \oplus_{(S\backslash T)(k)} \mathrm{Ind}_G^{G_v} T(k_v(p)/k_v)_{G_{k_{\infty,v}}} \longrightarrow X_S \longrightarrow X_T \longrightarrow 0$$

and the direct sum on the left is isomorphic to

$$\bigoplus_{\substack{(S\backslash T)(k) \\ p^\infty \,|\, f_v,\ \mu_p \subseteq k_v}} \mathrm{Ind}_G^{G_v} \mathbb{Z}_p(1) \oplus \bigoplus_{(S\backslash T)^{cd}(k)} \Lambda/p^{t_v},$$

where $p^{t_v} = \#\mu(k_v)(p)$ and, as before, $f_v = f(k_{\infty,v}/k_v)$ denotes the degree of the extension of the corresponding residue class fields. In particular, there is an exact sequence of Λ-torsion modules

$$0 \longrightarrow \oplus_{(S\backslash T)(k)} \mathrm{Ind}_G^{G_v} T(k_v(p)/k_v)_{G_{k_{\infty,v}}} \longrightarrow \mathrm{tor}_\Lambda X_S \longrightarrow \mathrm{tor}_\Lambda X_T \longrightarrow 0.$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

Proof. Since $\mathrm{H}^2(G_T(k_\infty)(p), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, we have an exact sequence

$$0 \longrightarrow G(k_S(p)/k_T(p))^{\mathrm{ab}}_{G_T(k_\infty)} \longrightarrow X_S \longrightarrow X_T \longrightarrow 0.$$

Setting $\mathcal{G} = G_T(k)(p)$ and using [29, 10.5.4, 10.6.1] as well as Lemma 2.9, we obtain

$$\begin{aligned} G(k_S(p)/k_T(p))^{\mathrm{ab}}_{G_T(k_\infty)} &\cong \Bigg(\bigoplus_{(S\backslash T)(k)} \mathrm{Ind}_{\mathcal{G}}^{\mathcal{G}_v} T(k_T(p)_v(p)/k_T(p)_v)\Bigg)_{G_T(k_\infty)} \\ &\cong \bigoplus_{(S\backslash T)(k)} \mathrm{Ind}_G^{G_v} T(k_v(p)/k_v)_{G_{k_{\infty,v}}}. \end{aligned}$$

Observe that, for $v \in S\backslash T$,

$$T(k_v(p)/k_v) \cong \begin{cases} \mathbb{Z}_p(1), & \text{if } \mu_p \subseteq k_v, \\ 0, & \text{otherwise.} \end{cases}$$

Since G is without p-torsion and $v \in S\backslash T$ is unramified in $k_\infty \,|\, k$, there are only two possibilities for G_v:

$$G_v = \begin{cases} 0, & \text{if } v \text{ is completely decomposed in } k_\infty \,|\, k, \\ \mathbb{Z}_p, & \text{if } p^\infty \,|\, f_v, \end{cases}$$

respectively,

$$G_{k_\infty,v}(p) \cong \begin{cases} \mathbb{Z}_p(1) \rtimes \mathbb{Z}_p, & \text{if } v \text{ is completely decomposed in } k_\infty \,|\, k, \\ \mathbb{Z}_p(1), & \text{if } p^\infty \,|\, f_v. \end{cases}$$

It follows that

$$G(k_S(p)/k_T(p))^{\mathrm{ab}}_{G_T(k_\infty)} \cong \bigoplus_{\substack{(S\backslash T)(k) \\ p^\infty \,|\, f_v,\ \mu_p \subseteq k_v}} \mathrm{Ind}_G^{G_v} \mathbb{Z}_p(1) \oplus \bigoplus_{(S\backslash T)^{cd}(k)} \Lambda/p^{t_v}.$$

In particular, this module is Λ-torsion and therefore the second statement follows from the first. □

Recalling that μ is additive on short exact sequences of Λ-torsion modules we obtain the following

COROLLARY 4.22. *Under the assumptions of the theorem,*

$$\mu(X_S) = \mu(X_T) + \sum_{(S\backslash T)^{cd}(k)} t_v,$$

where $p^{t_v} = \#\mu(k_v)(p)$.

4.1.2. *Global Units*

We still consider p-adic Lie extensions $k_\infty \,|\, k$ with Galois group $G = G(k_\infty/k)$.

Recall that we denote the norm compatible S-units of k_∞ by $\mathbb{E}_S := \varprojlim_{k'} (\mathcal{O}^\times_{k',S} \otimes \mathbb{Z}_p)$. Noting that $\mathbb{E}_S \cong \varprojlim_{k'} \mathrm{H}^1(G_S(k'), \mathbb{Z}_p(1))$ by Kummer theory and

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

the finiteness of the S-ideal class group, we are going to derive some relations between $\mathbb{E}_S$ and $\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee$ by interpreting Jannsen's spectral sequence ([22], see also [40, Thm. 4.5]) or for Iwasawa adjoints with respect to $A = \mathbb{Q}_p/\mathbb{Z}_p(1) = \mu_{p^\infty}(k_S)$. We assume that G does not have any p-torsion, i.e. G is a Poincaré group at p, and we denote the character which gives the operation of G on the dualizing module by χ^{-1}.

PROPOSITION 4.23. (i) *If* $\mu_{p^\infty} \subseteq k_\infty$, *then*

(a) *if* $\mathrm{cd}_p(G) = 1$:

$$\mathbb{E}_S \cong \mathbb{Z}_p(1)(\chi) \oplus \mathrm{E}^0(X_S(-1))$$

$$\varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \cong \mathrm{E}^1(X_S(-1)),$$

$$\mathrm{E}^i(X_S(-1)) = 0 \quad \textit{for} \quad i \geqslant 2.$$

(b) *if* $\mathrm{cd}_p(G) = 2$: *there is an exact sequence*

$$0 \longrightarrow \mathbb{E}_S \longrightarrow \mathrm{E}^0(X_S(-1)) \longrightarrow \mathbb{Z}_p(1)(\chi) \longrightarrow \varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \longrightarrow \mathrm{E}^1(X_S(-1)) \longrightarrow 0,$$

and

$$\mathrm{E}^i(X_S(-1)) = 0 \textit{ for } i \geqslant 2.$$

(c) *if* $\mathrm{cd}_p(G) = 3$: *there is an exact sequence*

$$0 \longrightarrow \varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \longrightarrow \mathrm{E}^1(X_S(-1)) \longrightarrow \mathbb{Z}_p(1)(\chi) \longrightarrow 0,$$

and

$$\mathbb{E}_S \cong \mathrm{E}^0(X_S(-1)),$$
$$\mathrm{E}^i(X_S(-1)) = 0 \textit{ for } i \geqslant 2.$$

(d) *if* $\mathrm{cd}_p(G) \geqslant 4$:

$$\mathbb{E}_S \cong \mathrm{E}^0(X_S(-1)),$$

$$\varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \cong \mathrm{E}^1(X_S(-1)),$$

$$\mathrm{E}^i(X_S(-1)) = \begin{cases} \mathbb{Z}_p(1)(\chi) & \textit{if } i = \mathrm{cd}_p(G) - 2, \\ 0 & \textit{otherwise}, \end{cases} \quad \textit{for} \quad i \geqslant 2.$$

Similar results hold for arbitrary A *with* $k(A) \subseteq k_\infty$ *if* $\mathbb{E}_S$ *is replaced by* $\varprojlim_{k'} \mathrm{H}^1(G_S(k'), T_pA)$, $X_S(-1)$ *by* $X_S[A]$, ...

(ii) *If* $\mu(k_\infty)(p)$ *is finite, then*

(a) *if* $\mathrm{cd}_p(G) = 1$: *then there is an exact sequence*

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

$$0 \longrightarrow \mathbb{E}_S \longrightarrow \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) \longrightarrow \mu(k_\infty)(p)^\vee(\chi) \longrightarrow \varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)).$$

(a$_1$) *If in addition* $\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty}) = 0$, *then the cokernel of the sequence is* $\mathrm{E}^1(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee)$ *and*

$\mathrm{E}^i(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) = 0$ *for* $i \geqslant 2$.

(a$_2$) *If in addition* $\mathrm{H}^2(G_S(k_\infty), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, *then there is a short exact sequence*

$$0 \longrightarrow \mathbb{E}_S \longrightarrow \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) \longrightarrow \mu(k_\infty)(p)^\vee(\chi) \longrightarrow 0.$$

(b) *if* $\mathrm{cd}_p(G) = 2$, *then* $\mathbb{E}_S \cong \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee)$.
If in addition $\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty}) = 0$, *then there is an exact sequence*

$$0 \longrightarrow \varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \longrightarrow \mathrm{E}^1(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee)$$
$$\longrightarrow \mu(k_\infty)(p)^\vee(\chi) \longrightarrow 0$$

and

$$\mathrm{E}^i(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) = 0 \quad \textit{for} \quad i \geqslant 2.$$

(c) *if* $\mathrm{cd}_p(G) \geqslant 3$, *then* $\mathbb{E}_S \cong \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee)$.
If in addition $\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty}) = 0$, *then*

$$\mathbb{E}_S \cong \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee),$$
$$\varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \cong \mathrm{E}^1(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee),$$
$$\mathrm{E}^i(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) = \begin{cases} \mu(k_\infty)(p)(\chi), & \textit{if } i = \mathrm{cd}_p(G) - 1, \\ 0 & \textit{otherwise}, \end{cases} \textit{for } i \geqslant 2.$$

(iii) *If* $\mu(k_\infty)(p) = 0$, *then there is in addition to the results for finite* $\mu(k_\infty)(p)$ *the following exact sequence:*

$$0 \longrightarrow \mathrm{E}^1(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) \longrightarrow \varprojlim_{k'} H^2(G_S(k'), \mathbb{Z}_p(1)) \longrightarrow$$
$$\longrightarrow \mathrm{E}^0(\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty})^\vee) \longrightarrow \mathrm{E}^2(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) \longrightarrow 0,$$

and

$$\mathrm{E}^i(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee) \cong \mathrm{E}^{i-2}(\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty})^\vee)).$$

For the proof apply Jannsen's theorem (see [40, Thm. 4.5, Cor. 4.6]) and note the following facts: $\mathrm{H}^1(G_S(k_\infty), A)^\vee \cong X_S[A]$ if $k(A) \subseteq k_\infty$, $\mathrm{H}^2(G_S(k_\infty), A) = 0$ if $\mu_{p^\infty} \subseteq k_\infty$ because the weak Leopoldt conjecture is true for the cyclotomic extension of any number field. Furthermore, we applied several times [20, 2.6]. Also observe, that the reflexive module $\mathrm{E}^0(X_S(-1))$ is projective in the case $\mathrm{cd}_p(G) = 1$ regarding the defining sequence of the transpose functor D and using that $\mathrm{pd}(\Lambda) = \mathrm{cd}_p(G) + 1 = 2$. The last statement of (ii)(a) is proved in [29], 11.3.9.

These results bear a lot of information about the structure of $\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee$ and $\mathbb{E}_S$, e.g. one can derive the projective dimension of the latter module (using Corollary [40, Cor. 6.3]) and some information about the dimensions of the modules occurring above, in particular whether a module is torsion(free). Furthermore, we see that $\mathbb{E}_S$ is reflexive for almost all cases with $\mathrm{cd}_p(G) \geqslant 2$ by Proposition 3.11 of [40].

In order to relate $\mathbb{E}_S$ to the finitely generated Λ-module

$$\mathcal{E}_S(k_\infty) = (E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\vee$$

we need some technical lemmas.

LEMMA 4.24. (i) *Let* $G = G(k_\infty/k) \cong \mathbb{Z}_p^d$, $d \geqslant 1$, *and* $G_n := p^n G$.

(a) *If* $\mu_{p^\infty} \subseteq k_\infty$, *then with* $\Gamma = G(k(\mu_{p^\infty})$ *and* $\Gamma_n = p^n\Gamma$ *the following holds*

$$\mathrm{H}^i(G_n, \mu_{p^\infty}) = \mu(k_n)(p)^{\binom{d-1}{i}},$$

where $k_n = k(\mu_{p^\infty})^{\Gamma_n}$.

(b) *If* $\mu(k_\infty)(p)$ *is finite, then for any n such that* $\mu(k_\infty)(p)^{G_n} = \mu(k_\infty)(p)$ *it holds*

$$\mathrm{H}^i(G_n, \mu_{p^\infty}) = \mu(k_\infty)(p)^{\binom{d}{i}}.$$

(ii) *Let G be a finitely generated pro-p Lie group without p-torsion which fits into a exact sequence*

$$1 \longrightarrow U \longrightarrow G \xrightarrow{\pi} \Gamma \longrightarrow 1,$$

with $\Gamma \cong \mathbb{Z}_p$ *and let* G_n *be an open subgroup. Assume that* $\Gamma_n := \pi(G_n)$ *acts via a splitting trivially on* $U_n = G_n \cap U$. *Then* $\mathrm{H}^2(G_n, \mu(k_\infty)(p))$ *is finite and the following holds*

(a) *If* $\mu_{p^\infty} \subseteq k_\infty$ *and* $\Gamma = G(k(\mu_{p^\infty})$, *then*

$$\mathrm{H}^1(G_n, \mu(k_\infty)(p)) \cong \mu(k_n)(p)^s \oplus \bigoplus_i \mu_{p^{v_i}}(k_n),$$

where $U_n^{\mathrm{ab}} \cong \mathbb{Z}_p^s \oplus \bigoplus_i \mathbb{Z}_p/p^{v_i}$ *with* $U_n = U \cap G_n$.

(b) *If* $\mu(k_\infty)(p)$ *is finite, then for any n such that* $\mu(k_\infty)(p)^{G_n} = \mu(k_\infty)(p)$ *there is an exact sequence*

$$0 \longrightarrow \mu(k_\infty)(p) \longrightarrow \mathrm{H}^1(G_n, \mu(k_\infty)(p)) \longrightarrow \mu(k_\infty)(p)^s \oplus \bigoplus_i \mu_{p^{v_i}}(k_\infty) \longrightarrow 0.$$

(c) *If* $\mathrm{cd}_p(G) = 2$, *then*

$$\mathrm{H}^2(G_n, \mu(k_\infty)(p)) \cong \begin{cases} 0, & \textit{if } \mu_{p^\infty} \subseteq k_\infty, \\ \mu(k_\infty)(p), & \textit{otherwise.} \end{cases}$$

Proof. Consider the exact sequence

$$1 \longrightarrow U \longrightarrow G \xrightarrow{\pi} \Gamma \longrightarrow 1,$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

and let $U_n = G_n \cap U$ and $\Gamma_n = \pi(G_n)$. The Hochschild–Serre spectral sequence gives

$$\mathrm{H}^1(\Gamma_n, \mathrm{H}^i(U_n, \mu(k_\infty)(p))) \hookrightarrow \mathrm{H}^{i+1}(G_n, \mu(k_\infty)(p)) \twoheadrightarrow \mathrm{H}^{i+1}(U_n, \mu(k_\infty)(p))^{\Gamma_n}$$

for $i \geqslant 0$.

Let us first assume that $\mu_{p^\infty} \subseteq k_\infty$: Since U_n acts trivially on μ_{p^∞}, we get

$$\mathrm{H}^i(U_n, \mathbb{Q}_p/\mathbb{Z}_p(1)) = \mathrm{H}^i(U_n, \mathbb{Q}_p/\mathbb{Z}_p)(1) = (\mathbb{Q}_p/\mathbb{Z}_p)^{\binom{d-1}{i}}.$$

in the Abelian case by the Künneth formula. As $\mathbb{Q}_p/\mathbb{Z}_p(1)_{\Gamma_n} = 0$ it follows that $\mathrm{H}^i(G_n, \mu_{p^\infty}) = \mathrm{H}^i(U_n, \mu_{p^\infty})^{\Gamma_n} = \mu(k_n)^{\binom{d-1}{i}}$. In the non-Abelian case we calculate

$$\begin{aligned}\mathrm{H}^1(G_n, \mu_{p^\infty}) &= \mathrm{H}^1(U_n, \mathbb{Q}_p/\mathbb{Z}_p)(1)^{\Gamma_n}\\ &= (U_n^{\mathrm{ab}})^\vee(1)^{\Gamma_n}\\ &= \mu(k_n)(p)^s \oplus \bigoplus \mu_{p^{\nu_i}}(k_n).\end{aligned}$$

Hence $\mathrm{H}^1(\Gamma_n, \mathrm{H}^1(U_n, \mu(k_\infty)(p)))$ is finite and the finiteness of $\mathrm{H}^2(G_n, \mu_{p^\infty})$ follows because $\mathrm{H}^2(U_n, \mu_{p^\infty})^{\Gamma_n} \cong \mathrm{H}^2(U_n, \mathbb{Q}_p/\mathbb{Z}_p)(1)^{\Gamma_n}$ is also finite ($H^2(U_n, \mathbb{Q}_p/\mathbb{Z}_p)$ is a cofinitely generated Abelian group).

Now we consider the case of finite $\mu(k_\infty)(p)$: Here $\mathrm{H}^1(\Gamma_n, \mu(k_\infty)(p)) = \mu(k_\infty)(p)$ and the Abelian case follows again using the Künneth formula. In the non-abelian case the finiteness of $\mathrm{H}^2(G_n, \mu_{p^\infty})$ is trivial while $\mathrm{H}^1(U_n, \mu(k_\infty)(p))^{\Gamma_n}$ can be calculated similarly as above. For the last assertion just note that $U_n \cong \mathbb{Z}_p$. □

LEMMA 4.25. (i) *In the situation Lemma* 4.24 (ii) *it holds*

(a) $\varprojlim_{m,n} {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty)) \cong \varprojlim_{m,n} {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)) = 0$,
(b) $\varprojlim_n \mathrm{H}^1(G_n, E_S(k_\infty)) \subseteq X_{cs}^S$,
(c) $$\begin{aligned}\mathrm{E}^0(\mathcal{E}_S(k_\infty)) &\cong \varprojlim_{m,n} {}_{p^m}(E_S(k_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{G_n}\\ &\cong \varprojlim_{m,n} (E_S(k_\infty)/\mu(k_\infty))^{G_n}/p^m,\end{aligned}$$
(d) $\mathrm{T}_0(\varprojlim_n \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty))) = \mathrm{T}_0(\mathrm{E}^1((E_S(k_\infty) \bigotimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^\vee))$,
(e) *that the following sequence is exact:*

$$\begin{aligned}0 \longrightarrow \varprojlim_n \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow \mathrm{E}^1(\mathcal{E}_S(k_\infty)) \longrightarrow\\ \varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow 0.\end{aligned}$$

(ii) *If, in addition,* $\mathrm{cd}_p(G) \leqslant 2$, *then with* $\kappa = 1$ *if* $\mu(k_\infty)(p)$ *is finite,* 0 *otherwise, there are the following exact sequences*

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(*a*) *if* $\mathrm{cd}_p(G) = 2$:

$$0 \longrightarrow \varprojlim_n \mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow \varprojlim_{m,n} \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty))/p^m \longrightarrow \mu(k_\infty)(p)^\kappa \longrightarrow D \longrightarrow 0,$$

$$0 \longrightarrow \varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)) \longrightarrow \varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow D \longrightarrow \varprojlim_{m,n} \mathrm{H}^2(G_n, E_S(k_\infty))/p^m \longrightarrow \varprojlim_{m,n} \mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty))/p^m \longrightarrow 0,$$

where D is some finite module.

(b) *if* $\mathrm{cd}_p(G) = 1$:

$$0 \longrightarrow \mathrm{E}^2\mathrm{E}^1(\mathbb{E}_S) \longrightarrow \mu(k_\infty)(p)^\kappa \longrightarrow \varprojlim_n \mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow \varprojlim_{m,n} \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty))/p^m \longrightarrow 0$$

and

$$\varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)) \cong \varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty)).$$

Proof. If we split the long exact cohomology sequence induced by

$$0 \longrightarrow \mu(k_\infty) \longrightarrow E_S(k_\infty) \longrightarrow E_S(k_\infty)/\mu(k_\infty) \longrightarrow 0,$$

we get the following short exact sequences

$$0 \longrightarrow F_n \longrightarrow \mathrm{H}^1(G_n, \mu(k_\infty)) \longrightarrow A_n \longrightarrow 0,$$
$$0 \longrightarrow A_n \longrightarrow \mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow B_n \longrightarrow 0,$$
$$0 \longrightarrow B_n \longrightarrow \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow C_n \longrightarrow 0$$

and, furthermore, a map $C_n \hookrightarrow \mathrm{H}^2(G_n, \mu(k_\infty)(p))$. Evaluating the associated long exact sequences of p^m-torsion (snake lemma) and noting the finiteness of A_n and C_n according to the previous lemma, we get

$$\varprojlim_m {}_{p^m}B_n \cong \varprojlim_m {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty)),$$

$$0 \longrightarrow \varprojlim_m {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow \varprojlim_m {}_{p^m}B_n \longrightarrow A_n,$$

and therefore

$$0 \longrightarrow \varprojlim_{m,n} {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow \varprojlim_{m,n} {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow \varprojlim_n A_n$$

is exact. But $\varprojlim_n A_n$ is a quotient of

$$\varprojlim_n \mathrm{H}^1(G_n, \mu(k_\infty)(p)) = \begin{cases} \mu(k_\infty)(p) & \text{if } d = 1 \text{ and } \mu(k_\infty)(p) \text{ is finite,} \\ 0 & \text{otherwise.} \end{cases}$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(See the previous lemma and note that the transition maps are partially norm maps besides the nontrivial case where they are the natural projections, i.e. identities for n sufficiently big.) Since the middle term is $\mathbb{Z}_p$-torsion free, we get the desired isomorphism, because, by the Hochschild–Serre spectral sequence, it can be seen in any case that the first group is contained in $\varprojlim_{m,n} {}_{p^m}\mathrm{Cl}_S(k_n) = 0$. This proves (i)(a) while (b) is again the cited spectral sequence.

The first equality of (i)(c) is just Theorem 4.7(iii) of [40] because $\mathcal{E}_S(k_\infty)$ has no $\mathbb{Z}_p$-torsion while the second one follows by the exact sequence

$$(E_S(k_\infty)/\mu(k_\infty))^{G_n}/p^m \hookrightarrow {}_{p^m}(E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{G_n} \twoheadrightarrow {}_{p^m}\mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty))$$

and (a). Similar arguments apply for (i)(e), i.e.

$$\mathrm{E}^1(\mathcal{E}_S(k_\infty)) \cong \varprojlim_{m,n} \mathrm{H}^1(G_n, {}_{p^m}(E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)).$$

The assertion (d) is a direct consequence of (e), because $\varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty))$ is $\mathbb{Z}_p$-torsion-free.

Now let us assume that $\mathrm{cd}_p(G) \leqslant 2$. With the notation as above and recalling that A_n, B_n and C_n are finite, we get exact sequences

$$0 \longrightarrow A_n \longrightarrow \mathrm{H}^1(G_n, E_S(k_\infty)) \longrightarrow B_n \longrightarrow 0,$$

$$0 \longrightarrow B_n \longrightarrow \varprojlim_m \mathrm{H}^1(G_n, E_S(k_\infty)/\mu(k_\infty))/p^m \longrightarrow C_n \longrightarrow 0$$

and

$$0 \longrightarrow C_n \longrightarrow \mathrm{H}^2(G_n, \mu(k_\infty)) \longrightarrow D_n \longrightarrow 0.$$

Passing to the limit gives the first exact sequence in (ii)(a) (Note that the transition maps of the system $\{C_n\}$ are the canonical projections, i.e. identities for n sufficiently large). The second one is proved similarly using

$$D_n \hookrightarrow \mathrm{H}^2(G_n, E_S(k_\infty)) \longrightarrow \mathrm{H}^2(G_n, E_S(k_\infty)/\mu(k_\infty)) \longrightarrow \mathrm{H}^3(G_n, \mu(k_\infty)(p)) = 0$$

and $\mathrm{H}^2(G_n, \mu(k_\infty)(p)) \twoheadrightarrow D_n$. The proof of (ii)(b) is completely analogous, just note that $\varprojlim_n F_n \cong \mathrm{E}^2\mathrm{E}^1(\mathbb{E}_S)$ because the latter module is the cokernel of $\mathbb{E}_S \to \mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S) \cong \mathrm{E}^0(\mathcal{E}_S(k_\infty))$. □

PROPOSITION 4.26. *There is an exact sequence*

$$0 \longrightarrow \mathbb{Z}_p(1)^\delta \longrightarrow \mathbb{E}_S \longrightarrow \mathrm{E}^0(\mathcal{E}_S(k_\infty)) \longrightarrow C$$

with

$$C = \begin{cases} \mu(k_\infty)(p), & \text{if } d = 1 \text{ and } \mu(k_\infty)(p) \text{ finite}, \\ \mathbb{Z}_p(1), & \text{if } d = 2 \text{ and } \mu_{p^\infty} \subseteq k_\infty, \\ \text{f.g. } \mathbb{Z}_p\text{-module}, & d \geqslant 3 \text{ and } G \text{ non-Abelian}, \\ 0, & \text{otherwise} \end{cases}$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

and

$$\delta = \begin{cases} 1, & \text{if } d = 1, \mu_{p^\infty} \subseteq k_\infty, \\ 0, & \text{otherwise}. \end{cases}$$

If in addition the weak Leopoldt conjecture holds, the right map is onto in the case $d = 1$ and $\mu(k_\infty)(p)$ finite.

Proof. Taking G_n-invariants of the exact sequence

$$0 \longrightarrow \mu(k_\infty)(p) \longrightarrow E_S(k_\infty) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow (E_S(k_\infty)/\mu(k_\infty)) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow 0$$

and passing to the inverse limit, we get

$$0 \longrightarrow \varprojlim_n \mu(k_n)(p) \longrightarrow \mathbb{E}_S \longrightarrow \varprojlim_{m,n} (E_S(k_\infty)/\mu(k_\infty))^{G_n}/p^m \longrightarrow \varprojlim_n \mathrm{H}^1(G_n, \mu(k_\infty)(p))$$

The result follows except the fact that E^0 maps onto the finite group of roots of unity in the case when $d = 1$. But this is proved in [29], 11.3.9, under the assumption that the weak Leopoldt conjecture holds. □

COROLLARY 4.27. *Let $k_\infty \mid k$ be a p-adic Lie extension such that G does not have any p-torsion. Then*

$$\mathrm{E}^0(\mathbb{E}_S) \cong \mathrm{E}^0\mathrm{E}^0(\mathcal{E}_S(k_\infty)) \cong \mathrm{E}^0(\mathrm{H}^1(G_S(k_\infty), \mu_{p^\infty})^\vee).$$

In particular, if G is in addition pro-p and $\mathrm{H}^2(G_S(k_\infty), \mu_{p^\infty}) = 0$ (e.g. if $\mu_{p^\infty} \subseteq k_\infty$), then $\mathrm{rk}_\Lambda \mathbb{E}_S = \mathrm{rk}_\Lambda \mathcal{E}_S = r_2(k)$.

Now the question arises whether the module $\mathrm{E}^0(\mathbb{E}_S)$ is not only reflexive but also projective. While in the case $\mathrm{cd}_p(G) = 1$ this is always true, in higher dimensions one needs additional conditions. We will only get a satisfying answer in the two-dimensional case:

PROPOSITION 4.28. *Let $k_\infty \mid k$ be a p-adic Lie extension such that $\mathrm{cd}_p(G) = 2$ and assume that the weak Leopoldt conjecture holds for k_∞. Then the following is equivalent:*

(i) $\mathrm{E}^0(\mathbb{E}_S)$ *is projective,*
(ii) $\mathrm{T}_0\mathrm{E}^1(\mathcal{E}_S(k_\infty)) = 0$.

Remark 4.29. These equivalent statements hold for example, if either $\mu_{p^\infty} \subseteq k_\infty$ or $\mu(k_\infty)(p) = 0$, and $\mathrm{T}_0(X_{cs}^S) = 0$, i.e. if X_{cs}^S does not have any nonzero finite submodule, because then $\mathrm{T}_0\mathrm{E}^1(\mathcal{E}_S(k_\infty)) = 0$ by Lemma 4.25.

Proof. Since we already know that $\mathrm{pd}(\mathrm{E}^0(\mathbb{E}_S)) \leqslant 1$, because $\mathrm{E}^0(\mathbb{E}_S)$ is the second syzygy of $\mathrm{D}\mathbb{E}_S$, the projectivity is equivalent to the vanishing of $\mathrm{E}^1\mathrm{E}^0(\mathbb{E}_S)$. Now the equivalence stated above follows from the next lemma. □

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

LEMMA 4.30. *In the situation of the proposition it holds*

$$\mathrm{T}_0\mathrm{E}^1(\mathcal{E}_S(k_\infty)) \cong \mathrm{E}^1\mathrm{E}^0(\mathbb{E}_S) \cong \mathrm{E}^3\mathrm{E}^1(\mathbb{E}_S)$$

Proof. Set $M := \mathcal{E}_S(k_\infty)$ and consider the exact sequence

$$0 \longrightarrow M/\mathrm{T}_1(M) \longrightarrow \mathrm{E}^0(\mathbb{E}_S) \longrightarrow \mathrm{E}^2 D(M) \longrightarrow 0.$$

The long exact sequence for E^i gives

$$0 = \mathrm{E}^1\mathrm{E}^2 D(M) \longrightarrow \mathrm{E}^1\mathrm{E}^0(M) \longrightarrow \mathrm{E}^1(M/\mathrm{T}_1(M)) \longrightarrow \mathrm{E}^2\mathrm{E}^2 D(M).$$

On the other hand there is the exact sequence

$$0 = \mathrm{E}^0(\mathrm{T}_1(M)) \longrightarrow \mathrm{E}^1(M/\mathrm{T}_1(M)) \longrightarrow \mathrm{E}^1(M) \longrightarrow \mathrm{E}^1\mathrm{E}^1 D(M).$$

Since $\mathrm{E}^i\mathrm{E}^i D(M)$ is pure of codimension i, the isomorphism follows. But $\mathrm{E}^1\mathrm{E}^0(\mathbb{E}_S) \cong \mathrm{E}^3\mathrm{E}^1(\mathbb{E}_S)$ by the spectral sequence due to Björk, see Proposition 2.5. □

The proposition above should be compared with the following result which has already been observed by Kay Wingberg (unpublished):

PROPOSITION 4.31. *If* $\mathrm{cd}_p(G) = 1$, *then for sufficiently large n there is a canonical exact sequence*

$$0 \longrightarrow \mathcal{E}_S(k_\infty)^{G_n} \longrightarrow \mathcal{E}_S(k_\infty) \longrightarrow \mathrm{E}^0(\mathbb{E}_S) \longrightarrow C \longrightarrow 0$$

where $C = \mathrm{E}^2\mathrm{D}(\mathcal{E}_S(k_\infty))$ *is connected with* $\mathrm{E}^2\mathrm{D}(\mathbb{E}_S)$ *by the exact sequence*

$$0 \longrightarrow \mathrm{E}^2\mathrm{D}(\mathbb{E}_S) \longrightarrow \mu(k_\infty)(p)^\kappa \longrightarrow \mathrm{T}_0 X_{cs}^S \longrightarrow C^\vee \longrightarrow 0.$$

Proof. The first sequence is just the canonical sequence 2.2 for the module $\mathcal{E}_S(k_\infty)$ while the second one already occurred in Lemma 4.25(ii)(b) as we show now: The fact that $\mathrm{T}_0(X_{cs}^S) \cong \varprojlim \mathrm{H}^1(G_n, E_S(k_\infty))$ is well known (see for example [29, XI. Section 3.]). Recall ^{n}that $\mathrm{E}^2\mathrm{E}^1(\mathcal{E}_S(k_\infty)) \cong \mathrm{T}_0(\mathrm{E}^1(\mathcal{E}_S(k_\infty)))^\vee$ and apply Lemma 4.25(i)(d) to recover C. Using 4.25(i)(e) and (ii)(b), we see that $\mathrm{E}^1\mathrm{E}^1(\mathcal{E}_S(k_\infty)) \cong \mathrm{E}^1(\varprojlim_{m,n}{}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty)))$, which we will determine by means of [40, Thm. 4.7(iii)]:

$$M := \varprojlim_{m,n} {}_{p^m}\mathrm{H}^2(G_n, E_S(k_\infty))^\vee \cong \varinjlim_{m,n} \mathcal{E}_S(k_\infty)^{G_n}/p^m = \varinjlim_{m} \mathcal{E}_S(k_\infty)^{G_n}/p^m$$

for n sufficiently large, because $\mathcal{E}_S(k_\infty)$ is a finitely generated Λ-module. Hence

$$\mathrm{E}^1(M) \cong \varprojlim_{m,n}({}_{p^m}M)_{G_n} = \mathcal{E}_S(k_\infty)^{G_n}.$$

for n large enough. □

PROPOSITION 4.32. *Let k_∞/k be a p-adic Lie extension such that $G \cong \Gamma \times \Delta$, where Γ is a pro-p-Lie group of* $\mathrm{cd}_p(\Gamma) = 2$, *$\Delta$ is a finite group of order prime to p. Assume that the weak Leopoldt conjecture holds for k_∞. Then the following is true:*

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(i) *There is an exact sequence*

$$0 \longrightarrow \mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S) \longrightarrow \Lambda^{r_2+r_1-r_1'-s} \oplus \bigoplus_{S^{cd}\cup S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p) \longrightarrow$$

$$\Lambda^s \longrightarrow \mathrm{T}_0\mathrm{E}^1(\mathcal{E}_S(k_\infty)) \longrightarrow 0.$$

(ii) *If* $\mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S)$ *is projective, then*

$$\mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S) \cong \Lambda^{r_2+r_1-r_1'} \oplus \bigoplus_{S^{cd}\cup S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p).$$

Proof. We calculate the Euler characteristic with respect to an arbitrary open normal subgroup $U \trianglelefteq \Gamma$ using Lemma 2.7, Proposition 2.13, [20] 5.4b),

$$\begin{aligned} h_U(\mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S)) &= h_U(\mathbb{E}_S) \\ &= h_U(\mathbb{A}_S) - h_U(X_S) + h_U(X_{cs}^S) \\ &= h_U(\mathbb{A}_S) - h_U(Y_S) + h_U(I_G) \\ &= h_U(\mathbb{A}_S) - h_U(\Lambda^d) + h_U(N_{\mathcal{H}}^{\mathrm{ab}}(p)) + h_U(\Lambda) - h_U(\mathbb{Z}_p) \\ &= h_U(\mathbb{A}_S) - h_U(\Lambda^{r_2+r_1'}) + h_U\left(\bigoplus_{S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p)\right) \\ &= \sum_S \mathrm{Ind}_G^{G_v} h_{U\cap G_v}(\mathbb{A}_v) - h_U(\Lambda^{r_2+r_1'}) + h_U\left(\bigoplus_{S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p)\right) \\ &= \sum_{S^{cd}} \mathrm{Ind}_G^{G_v} h_U(\mathbb{Z}_p) + h_U(\Lambda^{r_2+r_1-r_1'}) + h_U\left(\bigoplus_{S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p)\right). \end{aligned}$$

Therefore, if $\mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S)$ is projective, it follows that

$$\mathrm{E}^0\mathrm{E}^0(\mathbb{E}_S) \cong \Lambda^{r_2+r_1-r_1'} \oplus \bigoplus_{S^{cd}\cup S'_\infty} \mathrm{Ind}_G^{G_v}(\mathbb{Z}_p).$$

This proves (ii) while (i) follows easily by applying Proposition 2.5. □

4.2. SELMER GROUPS OF ABELIAN VARIETIES

In this section let k be a number field, $\mathcal{A}$ a g-dimensional Abelian variety defined over k and p a fixed rational *odd* prime number. For a nonempty, finite set S of places of k containing the places S_{bad} of bad reduction of $\mathcal{A}$, the places S_p lying over p and the places S_∞ at infinity we write $\mathrm{H}^i(G_S(k), \mathcal{A})$, respectively $\mathrm{H}^i(k_v, \mathcal{A})$, for the cohomology groups $\mathrm{H}^i(G_S(k), \mathcal{A}(k_S))$, respectively $\mathrm{H}^i(G_v, \mathcal{A}(\bar{k}_v))$, where $G_S(k)$ denotes the Galois group of the maximal outside S unramified extension of k, $\bar{k}_v$ the algebraic closure of the completion of k at v and G_v the corresponding decomposition group. The (p^m)-)Selmer group $\mathrm{Sel}(\mathcal{A}, k, p^m)$ and the Tate–Shafarevich group $\text{Ш}(\mathcal{A}, k, p^m)$ fit by definition into the following commutative exact diagram

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

$$\begin{CD}
@. @. 0 @. 0 @. \\
@. @. @VVV @VVV @. \\
0 @>>> \mathcal{A}(k)/p^m @>>> \mathrm{Sel}(\mathcal{A},k,p^m) @>>> \text{Ш}(\mathcal{A},k,p^m) @>>> 0\\
@. @| @VVV @VVV @. \\
0 @>>> \mathcal{A}(k)/p^m @>>> \mathrm{H}^1(G_S(k),{}_{p^m}\mathcal{A}) @>>> {}_{p^m}\mathrm{H}^1(G_S(k),\mathcal{A}) @>>> 0\\
@. @. @VVV @VVV @. \\
@. @. \bigoplus_{S(k)}\mathrm{H}^1(k_v,\mathcal{A})(p) @= \bigoplus_{S(k)}\mathrm{H}^1(k_v,\mathcal{A})(p). @.
\end{CD}$$

If k_∞ is an infinite Galois extension of k with Galois group $G = G(k_\infty/k)$, we get the following commutative exact diagram by passing to the direct limit with respect to m and finite subextensions k' of k_∞/k:

$$\begin{CD}
@. @. 0 @. 0 @. \\
@. @. @VVV @VVV @. \\
0 @>>> \mathcal{A}(k_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p @>>> \mathrm{Sel}(\mathcal{A},k_\infty,p^\infty) @>>> \text{Ш}(\mathcal{A},k_\infty,p^\infty) @>>> 0\\
@. @| @VVV @VVV @. \\
0 @>>> \mathcal{A}(k_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p @>>> \mathrm{H}^1(G_S(k_\infty),\mathcal{A}(p)) @>>> \mathrm{H}^1(G_S(k_\infty),\mathcal{A})(p) @>>> 0\\
@. @. @VVV @VVV @. \\
@. @. \bigoplus_{S(k)}\mathrm{Coind}_G^{G_v}\mathrm{H}^1(k_{\infty,v},\mathcal{A})(p) @= \bigoplus_{S(k)}\mathrm{Coind}_G^{G_v}\mathrm{H}^1(k_{\infty,v},\mathcal{A})(p). @.
\end{CD}$$

Note that

$$\varinjlim_{k'}\bigoplus_{S(k')}\mathrm{H}^1(k'_v,\mathcal{A})(p) \cong \bigoplus_{S(k)}\mathrm{Coind}_G^{G_v}\mathrm{H}^1(k_{\infty,v},\mathcal{A})(p).$$

Alternatively, we can pass to the inverse limits and we will get the following commutative exact diagram

$$\begin{CD}
@. @. 0 @. 0 @. \\
@. @. @VVV @VVV @. \\
0 @>>> \hat{\mathcal{A}}_{k_\infty} @>>> \widehat{\mathrm{Sel}}(k_\infty,\mathcal{A}) @>>> \varprojlim_{k',m}\text{Ш}(\mathcal{A},k',p^m) @>>> 0\\
@. @| @VVV @VVV @. \\
0 @>>> \hat{\mathcal{A}}_{k_\infty} @>>> \varprojlim_{k'}\mathrm{H}^1(G_S(k'),T_p\mathcal{A}) @>>> \varprojlim_{k'}T_p\mathrm{H}^1(G_S(k'),\mathcal{A}) @>>> 0\\
@. @. @VVV @VVV @. \\
@. @. \varprojlim_{k'}\bigoplus_{S(k')}T_p\mathrm{H}^1(k'_v,\mathcal{A}) @= \varprojlim_{k'}\bigoplus_{S(k')}T_p\mathrm{H}^1(k'_v,\mathcal{A}). @.
\end{CD}$$

where

$$\hat{\mathcal{A}}_{k_\infty} := \varprojlim_{k',m}\mathcal{A}(k')/p^m \quad\text{and}\quad \widehat{\mathrm{Sel}}(k_\infty,\mathcal{A}) := \varprojlim_{k',m}\mathrm{Sel}(k',\mathcal{A},p^m)$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(The limits are taken with respect to corestriction maps and multiplication by p).

Henceforth we will drop the p from the notation of the Selmer group:

$$\mathrm{Sel}(\mathcal{A}, k_\infty) := \mathrm{Sel}(\mathcal{A}, k_\infty, p^\infty).$$

Furthermore, we shall use the following notation for the local-global modules

$$\mathbb{U}_{S,\mathcal{A}} := \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} \mathrm{H}^1(k_{\infty,v}, \mathcal{A})(p)^\vee,$$
$$\mathbb{A}_{S,\mathcal{A}} := \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} \mathrm{H}^1(k_{\infty,v}, \mathcal{A}(p))^\vee,$$
$$\mathbb{T}_{S,\mathcal{A}} := \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} (\mathcal{A}(k_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

As a consequence of the long exact sequence of the Poitou–Tate duality theorem we have the following (compact) analogue of Proposition 4.7, where we shall write $\mathcal{A}^d$ for the dual Abelian variety of $\mathcal{A}$ and $\text{Ш}^1_S(k_\infty, \mathcal{A}(p))$ for the kernel of the localization map

$$\mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p)) \to \bigoplus_{S(k)} \mathrm{Coind}_G^{G_v} \mathrm{H}^1(k_{\infty,v}, \mathcal{A}(p)).$$

PROPOSITION 4.33. *Let $k_\infty \mid k$ be a p-adic Lie extension with Galois group G. Then, there are the following exact commutative diagrams of $\Lambda = \Lambda(G)$-modules*

(i)

$$\begin{array}{ccccc}
0 & & 0 & & \\
\uparrow & & \uparrow & & \\
\mathrm{Sel}(\mathcal{A}, k_\infty)^\vee & \twoheadrightarrow & \text{Ш}^1_S(k_\infty, \mathcal{A}(p))^\vee & & \\
\uparrow & & \uparrow & & \\
\mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p))^\vee & = & \mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p))^\vee & & \\
\uparrow & & \uparrow & & \\
\mathbb{U}_{S,\mathcal{A}} & \hookrightarrow & \mathbb{A}_{S,\mathcal{A}} & \twoheadrightarrow & \mathbb{T}_{S,\mathcal{A}} \\
\uparrow & & \uparrow & & \| \\
\widehat{\mathrm{Sel}}(k_\infty, \mathcal{A}^d) & \hookrightarrow & \varprojlim_{k'} \mathrm{H}^1(G_S(k'), T_p(\mathcal{A}^d)) & \longrightarrow & \mathbb{T}_{S,\mathcal{A}}, \\
\uparrow & & \uparrow & & \\
\mathrm{H}^2(G_S(k_\infty), \mathcal{A}(p))^\vee & = & \mathrm{H}^2(G_S(k_\infty), \mathcal{A}(p))^\vee & & \\
\uparrow & & \uparrow & & \\
0 & & 0 & &
\end{array}$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

(ii)

$$0 \longrightarrow \widehat{\mathrm{Sel}}(k_\infty, \mathcal{A}^d) \longrightarrow \varprojlim_{k'} \mathrm{H}^1(G_S(k'), T_p\mathcal{A}^d) \longrightarrow \mathbb{T}_{S,\mathcal{A}} \longrightarrow \mathrm{Sel}(\mathcal{A}, k_\infty)^\vee \longrightarrow \text{Ш}^1_S(k_\infty, \mathcal{A}(p))^\vee \longrightarrow 0,$$

(iii)

$$0 \longrightarrow \text{Ш}^1_S(k_\infty, \mathcal{A}(p))^\vee \longrightarrow Z_{S,\mathcal{A}^d(p)} \longrightarrow \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v}(\mathcal{A}(k_{\infty,v})(p))^\vee \longrightarrow \mathcal{A}(k_\infty)(p)^\vee \longrightarrow 0.$$

For the proof, just note that by virtue of local Tate duality ([27, Cor.3.4]), the Weil pairing and 4.1,

(i) $\mathrm{H}^1(k_{\infty,v}, \mathcal{A})(p)^\vee \cong \widehat{(\mathcal{A}^d)}_{\infty,v} := \varprojlim_{k',m} \mathcal{A}^d(k'_v)/p^m$,

(ii) $Z_{S,\mathcal{A}^d(p)} \cong \varprojlim_{k'} \mathrm{H}^2(G_S(k'), T_p(\mathcal{A}^d))$,

(iii) $(\mathcal{A}(k_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \varprojlim_{k'} T_p\mathrm{H}^1(k'_v, \mathcal{A}^d)$ and

(iv) $\mathrm{H}^1(k_{\infty,v}, \mathcal{A}(p))^\vee \cong \varprojlim_{k'} \mathrm{H}^1(k'_v, T_p(\mathcal{A}^d))$

hold.

By a well-known theorem of Mattuck, we have an isomorphism $\mathcal{A}(k'_v) \cong \mathbb{Z}_l^{g[k'_v:\mathbb{Q}_l]} \times$ (a finite group), for any finite extension k'_v of $\mathbb{Q}_l$. Recall that g denotes the dimension of the Abelian variety $\mathcal{A}$. Clearly $\mathcal{A}(k'_v) \bigotimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = 0$ for all $l \neq p$ and $v \mid l$, i.e. $\mathrm{H}^1(k'_v, \mathcal{A})(p) \cong \mathrm{H}^1(k'_v, \mathcal{A}(p))$, respectively $\mathrm{H}^1(k'_{\infty,v}, \mathcal{A})(p) \cong \mathrm{H}^1(k'_{\infty,v}, \mathcal{A}(p))$, in this case. On the other hand, Coates and Greenberg proved that for primes $v \mid p$ with good reduction

$$\mathrm{H}^1(k_{\infty,v}, \mathcal{A})(p) \cong \mathrm{H}^1(k_{\infty,v}, \tilde{\mathcal{A}}(p))$$

holds, if k_∞ is a deeply ramified, where $\tilde{\mathcal{A}}$ denotes the reduction of $\mathcal{A}$ (see [5, Prop. 4.8]). We recall that an algebraic extension k of $\mathbb{Q}_p$ is called *deeply ramified* if $\mathrm{H}^1(k, \bar{\mathfrak{m}})$ vanishes, where $\bar{\mathfrak{m}}$ is the maximal ideal of the ring of integers of an algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$; see [5, p. 143] for equivalent conditions and for the following statement (loc. cit. Thm. 2.13): A field k_∞ which is a p-adic Lie extension of a finite extension k of $\mathbb{Q}_p$ is deeply ramified if the inertial subgroup of $G(k_\infty/k)$ is infinite.

For arbitrary reduction at $v \mid p$, the same result as above holds, if one replaces $\tilde{\mathcal{A}}_{p^\infty}$ by the quotient $\mathcal{A}(p)/\mathcal{F}_{\mathcal{A}}(\bar{\mathfrak{m}})(p)$, where $\mathcal{F}_{\mathcal{A}}$ denotes the formal group associated with the Neron model of $\mathcal{A}$ over a possibly finite extension of k_v, such that the Neron model has semi-stable reduction. Taking these facts into account, we get the following description for $\mathbb{U}_{S,\mathcal{A}}$, where $T(k_{\infty,v}/k_v)$ denotes the inertia subgroup of G_v.

PROPOSITION 4.34 (cf. [35, Lemma 5.4]). *Assume that* $\dim(T(k_{\infty,v}/k_v)) \geqslant 1$ *for all* $v \in S_p$. *Then there is an isomorphism of* Λ*-modules*

$$\mathbb{U}_{S,\mathcal{A}} \cong \bigoplus_{S_p(k)} \mathrm{Ind}_G^{G_v}\mathrm{H}^1(k_{\infty,v}, \tilde{\mathcal{A}}(p))^\vee \oplus \bigoplus_{S\setminus S_p(k)} \mathrm{Ind}_G^{G_v}\mathrm{H}^1(k_{\infty,v}, \mathcal{A}(p))^\vee.$$

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

In particular, if $\dim(G_v) \geqslant 2$ *for all* $v \in S_f$, *then*

$$\mathbb{U}_{S,\mathcal{A}} \cong \bigoplus_{S_p(k)} \mathrm{Ind}_G^{G_v} \mathrm{H}^1(k_{\infty,v}, \tilde{\mathcal{A}}(p))^\vee$$

and $\mathbb{U}_{S,\mathcal{A}}$ *is* Λ*-torsion-free.*

Proof. The first assertion has been explained above while the second statement follows from the local calculations in Propositions 3.4 and 3.5 with respect to the p-adic representations $A = \tilde{\mathcal{A}}(p)$, respectively $A = \mathcal{A}(p)$, and the comment before Proposition 3.5. □

Before going on we would like to recall some well-known facts about Abelian varieties:

Remark 4.35. (i) $\mathrm{rk}_{\mathbb{Z}_p}(\mathcal{A}(p)^\vee) = 2\mathrm{g}$, where g denotes the dimension of $\mathcal{A}$.

(ii) There exists always an isogeny from $\mathcal{A}$ to its dual $\mathcal{A}^d$, by which the Weil-pairing induces a nondegenerate skew-symmetric pairing on the Tate-module $T_p\mathcal{A}$ of $\mathcal{A}$, (combine [26, Cor. 7.2, Lem. 16.2(e), Prop. 16.6]). If $\mathcal{A} = E$ is an elliptic curve this isogeny can be chosen as a canonical isomorphism between E and E^d. Again for an arbitrary Abelian variety it follows that $k(\mu_{p^\infty}) \subseteq k(\mathcal{A}(p)) = k(\mathcal{A}^d(p))$ (see [37, Section 0 Lem. 7]).

THEOREM 4.36. *Assume that* $\mathrm{H}^2(G_S(k_\infty), (\mathcal{A}^d)(p)) = 0$. *If* $\dim(G_v) \geqslant 2$ *for all* $v \in S_f$, *then*

$$\text{III}^1_S(k_\infty, \mathcal{A}(p))^\vee \sim \mathrm{E}^1(Y_{S,\mathcal{A}^d(p)}) \sim \mathrm{E}^1(\mathrm{tor}_\Lambda Y_{S,\mathcal{A}^d(p)}) \cong \mathrm{E}^1(\mathrm{tor}_\Lambda X_{S,\mathcal{A}^d(p)}).$$

If, in addition, $G \cong \mathbb{Z}_p^r$, $r \geqslant 2$, *then the following holds:*

$$\text{III}^1_S(k_\infty, \mathcal{A}(p))^\vee \sim (\mathrm{tor}_\Lambda X_{S,\mathcal{A}^d(p)})^\circ,$$

where $^\circ$ *means that the G acts via the involution* $g \mapsto g^{-1}$.

Remark 4.37. In case $\mathrm{tor}_\Lambda X_{S,\mathcal{A}^d(p)}$ is isomorphic in $\Lambda\text{-mod}/\mathcal{PN}$ to a direct sum of cyclic modules of the form Λ modulo a (left) principal ideal Proposition 2.4 implies that

$$\text{III}^1_S(k_\infty, \mathcal{A}(p))^\vee \equiv (\mathrm{tor}_\Lambda X_{S,\mathcal{A}^d(p)})^\circ \bmod \mathcal{PN}$$

holds under the conditions of the theorem.

Proof. The first condition implies $Z_{S,\mathcal{A}^d(p)} \cong \mathrm{E}^1(Y_{S,\mathcal{A}^d(p)})$ while the other condition grants that $\bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v}(\mathcal{A}(k_{\infty,v})(p))^\vee$ is pseudo-null because $\mathcal{A}(k_{\infty,v})(p)^\vee$ is a finitely generated (free) $\mathbb{Z}_p$-module. Now everything follows as in 4.9 using here Proposition 4.33. □

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press

COROLLARY 4.38. *Let $\mathcal{A}$ be an Abelian variety over k with good supersingular reduction, i.e. $\mathcal{A}_{k_v}(p) = 0$, at all places v dividing p. Set $k_\infty = k(\mathcal{A}(p))$ and assume that $G(k_\infty/k)$ is a pro-p-group without any p-torsion. Then, for $\Sigma_{\mathrm{bad}} := S_{\mathrm{bad}} \cup S_p \cup S_\infty$ the following holds:*

$$X_{cs}[\mathcal{A}^d(p)] \cong \text{Ш}^1_{\Sigma_{\mathrm{bad}}}(k_\infty, \mathcal{A}^d(p))^\vee \sim \mathrm{E}^1(\mathrm{tor}_\Lambda(\mathrm{Sel}(\mathcal{A}, k_\infty)^\vee)).$$

In particular, if $\mathcal{A}$ has CM, then there is even a pseudo-isomorphism

$$X_{cs}[\mathcal{A}^d(p)] \sim (\mathrm{tor}_\Lambda(\mathrm{Sel}(\mathcal{A}, k_\infty)^\vee))^\circ.$$

Therewith, in the case of an elliptic curve with CM, we reobtain a theorem of P. Billot [3, 3.23]. Over a $\mathbb{Z}_p$-extension an analogous statement was proved by K. Wingberg [41, cor. 2.5]. Of course, remark 4.37 applies literally to $\mathrm{tor}_\Lambda \mathrm{Sel}(\mathcal{A}, k_\infty)^\vee$, i.e. under the conditions mentioned there it holds

$$X_{cs}[\mathcal{A}^d(p)] \equiv (\mathrm{tor}_\Lambda \mathrm{Sel}(\mathcal{A}, k_\infty)^\vee)^\circ \bmod \mathcal{PN}.$$

Proof. First note that by the Néron–Ogg–Shafarevich criterion the sets of bad reduction of $\mathcal{A}$ and its dual $\mathcal{A}^d$ coincide. Therefore, it suffices to prove that $\dim(G_v) \geqslant 2$ for all $v \in S_{\mathrm{bad}} \cup S_p$ because then the theorem applies to $\mathcal{A}^d$ and Proposition 4.34 shows that $\mathbb{U}_{S,\mathcal{A}} = 0$, i.e. $X_{S,\mathcal{A}(p)} \cong \mathrm{Sel}(\mathcal{A}, k_\infty)^\vee$.

So, let v be either in S_p or in S_{bad}. Since $k_v(\mathcal{A}(p))$ contains $k_v(\mu_{p^\infty})$, we only have to show that $G(k_v(\mathcal{A}(p))/k_v(\mu_{p^\infty}))$ is not trivial because then it automatically has to be infinite as $G_v \subseteq G$ has no finite subgroup by assumption.

If $v \mid p$, by a theorem of Imai★ [18] $\mathcal{A}(k_v(\mu_{p^\infty}))(p)$ is finite and thus $k_v(\mathcal{A}(p)) \neq k_v(\mu_{p^\infty})$.

If $v \in S_{\mathrm{bad}}$, then the Néron–Ogg–Shafarevich criterion implies that $G(k_v(\mathcal{A}(p))/k_v(\mu_{p^\infty})) = T(k_v(\mathcal{A}(p))/k_v)$ is nontrivial. □

By Remarks 4.4 and 4.35 the conditions of Theorem 4.2 are fulfilled for the p-torsion points $\mathcal{A}(p)$ and its trivializing extension of k, i.e. the extension which is obtained by adjoining the p-torsion points of $\mathcal{A}$:

THEOREM 4.39. *Let $k_\infty = k(\mathcal{A}(p))$ and assume that G does not have any p-torsion. Then $\mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p))^\vee$ has no nonzero pseudo-null submodule.*

Recall that G does not have any p-torsion if $p \geqslant 2\dim(\mathcal{A}) + 2$. Otherwise one only has to replace k by a finite extension inside k_∞.

We should mention that the rank of the global module $\mathrm{H}^1(G_S(k_\infty), \mathcal{A}(p))^\vee$ is $g[k:\mathbb{Q}]$, which was determined by Y. Ochi who also calculated the ranks and torsion-submodules of the local, respectively local-global modules (i.e. those global modules which are induced from local ones) that occur in Proposition 4.33

★I owe to John Coates the idea to use Imai's theorem here.

(cf. [33, 5.7, 5.11, 5.12]). See also the results in S. Howson's PhD thesis [17, 5.30, 6.1, 6.5–6.9, 6.13–6.14, 7.3].

Furthermore, in the case of elliptic curves S. Howson proved the following result.

PROPOSITION 4.40 (Howson [17, 6.14–15]). *Let E be an elliptic curve over k without complex multiplication and with good* ordinary *reduction at all places over p. Assume that $G = G(k(E(p)/k)$ is pro-p without any p-torsion. Then*

$$\mathbb{T}_{S,E} \cong \mathbb{A}_{S,\tilde{E}} \cong \bigoplus_{S_f(k)} \mathrm{Ind}_G^{G_v} \varprojlim_{k'} \mathrm{H}^1(k'_v, T_p(\tilde{E}))$$

and these modules are $\Lambda(G)$-torsion-free. Furthermore, there is an isomorphism

$$\mathbb{U}_{S,E} \cong \mathrm{E}^0(\mathbb{T}_{S,E}).$$

Acknowledgements

This article is based on a part of my Dissertation, Heidelberg 2000, and I would like to thank my supervisor Kay Wingberg most warmly for leading me to the field of 'higher dimensional' Iwasawa theory. John Coates receives my special gratitude for his great interest and valuable suggestions. I also wish to express my warm thanks to Yoshi Ochi for our fruitful interchange of ideas when he stayed in Heidelberg in 1999/2000. Susan Howson is heartily acknowledged for providing me with a copy of her PhD thesis and for the discussions in Heidelberg as well as in Cambridge. Finally, I thank the referee for pointing out some inaccuracies and for his or her comments which helped to improve the exposition.

Note added in proof. With the publication of [8], it has come into vogue to use again Lazard's original terminology in the context of p-adic Lie groups instead of that in [10], just because it is slightly more general. For example, the fact that the completed group algebra $\mathbb{F}_p[\![G]\!]$ is an integral ring holds for the whole class of *p-valuable* groups, see [24, Thm. III.3.1.7] for the definition. This follows immediately from [24, III.2.3.3/4]. In particular, this is useful for the application of Theorems 2.3, 4.18, 4.19 and 4.20.

References

1. Auslander, M. and Bridger, M.: Stable module theory, *Mem. Amer. Math. Soc.* **94** (1969).
2. Balister, P. N. and Howson, S.: Note on Nakayama's lemma for compact Λ-modules, *Asian J. Math.* **1**(2) (1997), 224–229.
3. Billot, P.: Quelques aspects de la descente sur une courbe elliptique dans le cas de reduction supersinguliere, *Compositio Math.* **58** (1986), 341–369.

4. Coates, J.: Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication, In: *Arithmetic Theory of Elliptic Curves*, Lectures given at the 3rd session of the Centro Internazionale Matematico Estivo (CIME), Centraro, Italy, 12–19 July 1997, Lecture Notes in Math. 1716, Springer, New York, 1999, pp. 1–50.
5. Coates, J. and Greenberg, R.: Kummer theory for abelian varieties over local fields, *Invent. Math.* **124** (1996), 129–174.
6. Coates, J. and Howson, S.: Euler characteristics and elliptic curves, *Proc. Natl. Acad. Sci. USA* **94**(21) (1997), 11115–11117.
7. Coates, J. and Howson, S.: Euler characteristics and elliptic curves II, *J. Math. Soc. Japan* **53**(1) (2001), 175–235.
8. Coates, J., Sujatha, R. and Schneider, P.: Modules over Iwasawa algebras, *J. Inst. Math. Jussieu* **2**(1) (2003) 73–108.
9. de Shalit, E.: *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Perspect. Math. 3, Academic Press, New York, 1987.
10. Dixon, J. D., du Sautoy, M. P. F., Mann, A. and Segal, D.: *Analytic Pro-p Groups*, 1st edn, London Math. Soc. Lecture Note Ser. 157, Cambridge Univ. Press, 1991.
11. Goodearl, K. R. and Warfield, R. B.: *An Introduction to Noncommutative Noetherian Rings*, London Math. Soc. Student Texts 16, Cambridge Univ. Press, 1989.
12. Greenberg, R.: The Iwasawa invariants of Γ-extensions of a fixed number field, *Amer. J. Math.* **95** (1973), 204–214.
13. Greenberg, R.: On the structure of certain Galois groups, *Invent. Math.* **47** (1978), 85–99.
14. Greenberg, R.: *Iwasawa Theory for p-adic Representations*, Adv. Stud. Pure Math. 17, Kinokuniya, Tokyo, 1989, pp. 97–137.
15. Harris, M.: p-adic representations arising from descent on Abelian varieties, *Compositio Math.* **39** (1979), 177–245.
16. Harris, M.: Correction to p-adic representations arising from descent on Abelian varieties., *Compositio Math.* **121** (1) (2000), 105–108.
17. Howson, S.: *Iwasawa theory of Elliptic Curves for p-adic Lie extensions*, PhD thesis, University of Cambridge, July 1998.
18. Imai, H.: A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions, *Proc. Japan Acad.* **51** (1975), 12–16.
19. Jannsen, U.: On the structure of Galois groups as Galois modules, In: *Number Theory, Proc. J. Arith., Noordwijkerhout/Neth. 1983*, Lecture Notes in Math. 1068, Springer, New York, 1984, pp. 109–126.
20. Jannsen, U.: *Iwasawa Modules up to Isomorphism*, Adv. Stud. Pure Math. 17, Kinokuniya, Tokyo, 1989, pp. 171–207.
21. Jannsen, U.: On the l-adic cohomology of varieties over number fields and its Galois cohomology, In: *Galois Groups over* **Q** (*Berkeley, CA, 1987*), Springer, New York, 1989, 315–360.
22. Jannsen, U.: A spectral sequence for Iwasawa adjoints, Unpublished, 1994.
23. Kuz'min, L. V.: Local extensions associated with l-extensions with given ramification, *Math. USSR Izv.* **9**(4) (1975) (1976), 693–726.
24. Lazard, M.: Groupes analytiques p-adiques, *Publ. Math. IHES* **26** (1965), 389–603.
25. McCallum, W. G.: Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions, *Amer. J. Math.* **123**(5) (2001), 909–930.
26. Milne, J. S.: Abelian varieties, In: *Arithmetic Geometry* (*Storrs, Conn., 1984*), Springer, New York, 1986, pp. 103–150.
27. Milne, J. S.: *Arithmetic duality theorems*, Perspect. Math. 1, Academic Press, New York, 1986.
28. Nekovár, J.: *Selmer complexes*, to appear in *Astérisque*.

29. Neukirch, J., Schmidt, A. and Wingberg, K.: *Cohomology of Number Fields*, Grundlehren Math. Wiss. 323, Springer, Berlin, 2000.
30. Neumann, A.: Completed group algebras without zero divisors, *Arch. Math.* **51** (1988), 496–499.
31. Nguyen-Quang-Do, T.: Formations de classes et modules d'Iwasawa, In: *Number Theory, Proc. J. Arith., Noordwijkerhout/Neth. 1983*, Lecture Notes in Math. 1068, Springer, New York, 1984.
32. Nguyen-Quang-Do, T. and Lannuzel, A.: Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombre, *Prépublications de l'équipe de mathématique de Besancon*, **99** (13) (1999).
33. Ochi, Y.: Iwasawa modules via homotopy theory, PhD thesis, University of Cambridge, 1999.
34. Ochi, Y. and Venjakob, O.: On ranks of Iwasawa modules over p-adic Lie extensions, *Math. Proc. Cambridge Philos. Soc.* **135** (2003) 25–43.
35. Ochi, Y. and Venjakob, O. On the structure of Selmer groups over p-adic Lie extensions, *J. Algebraic Geom.* **11** (2002) 547–580.
36. Perrin-Riou, B.: *p-adic L-Functions and p-adic Representations*, Amer. Math. Soc., Providence, RI, 2000.
37. Schneider, P.: Die Galoiscohomology p-adischer Darstellungen über Zahlkörpern, Dissertation, Universität Regensburg, 1980.
38. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques (Galois properties of points of finite order of elliptic curves), *Invent. Math.* **15** (1972) 259–331.
39. Venjakob, O.: A noncommutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. Reine Angew. Math.* **559** (2003) 153–191.
40. Venjakob, O.: On the structure theory of the Iwasawa algebra of a p-adic Lie group, *J. Eur. Math. Soc.* **4** (2002), 271–311.
41. Wingberg, K.: Duality theorems for abelian varieties over $\mathbb{Z}_p$-extensions, *Adv. Stud. Pure Math.* **17** (1989), 471–492.
42. Wintenberger, J.-P.: Structure galoisienne de limites projectives d'unites locales, *Compositio Math.* **42**(1) (1981), 89–103.

https://doi.org/10.1023/A:1025413030203 Published online by Cambridge University Press