Iwasawa modules up to isomorphism

by Uwe Jannsen

dedicated to Kenkichi Iwasawa

Universität Regensburg
NWF I - Mathematik
Universitätsstraße 31
D-8400 Regensburg

West Germany

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

West Germany

MPI/88-15

In classical Iwasawa theory one considers modules over the completed group ring $\Lambda = \mathbb{Z}_p[[G]]$ for $G \cong \mathbb{Z}_p$, and one often studies these up to quasi-isomorphism, i.e., by neglecting finite G-modules. In this paper we propose some methods for the study of Λ-modules up to isomorphism, which at the same time work for more general groups G (where a good structure theory in terms of quasi-isomorphisms is missing anyway). A future application we have in mind is the investigation of Galois extensions defined by torsion points of abelian varieties. Such extensions have compact p-adic Lie groups as Galois groups, and we show at several places that the theory works very nicely for these.

A basic tool is the homotopy theory for Λ-modules, recalled in § 1. It amounts to considering Λ-modules up to projective factors (which is no serious restriction in view of the Krull-Schmidt theorem), and has a formalism quite analogous to the one in topology: one has a loop space functor Ω, a suspension Σ, fibrations, cofibrations etc., and a certain analogue of homotopy groups in form of the Λ-modules $E^r(M) := \mathrm{Ext}^r_\Lambda(M,\Lambda)$.

There is also an analogue of the Postnikov tower describing how a module M is "glued together" from the modules $E^r(M)$. Instead of describing this in general, we have described the first step in 1.9, and the result for $G \cong \mathbb{Z}_p$ in § 3: in this case a Λ-module M is determined up to isomorphism by $E^0(M) \cong \Lambda^{\mathrm{rank}_\Lambda M}$, $E^1(M)$, $E^2(M)$, and a class in $\mathrm{Ext}^2_\Lambda(E^2(M),E^1(M))$. We then discuss the modules $E^r(M)$ in some detail. For example, we express various properties of M - like the existence of finite submodules or the freeness of $M/\mathrm{Tor}_\Lambda M$ - in terms of the $E^r(M)$. We also give some formulae for the E^r , in terms of inverse limits often encountered in the applications.

These formulae are derived from a discussion for general G in § 2, where we relate the E^r to the "dualizing modules" $D_r(A) = \varinjlim H^r(U,A)^*$ (the limits running over the open subgroups U of G) introduced by Tate for the study of duality theorems for profinite groups.

In the last three sections we give some applications to Galois theoretic Iwasawa modules. We start in § 4 with a general result on profinite groups $\mathcal{G}$ of p-cohomological dimension two. If $\mathcal{H} \leq \mathcal{G}$ is a closed normal subgroup and $G = \mathcal{G}/\mathcal{H}$, we show how to describe the Λ-module $\mathcal{H}/[\mathcal{H},\mathcal{H}](p)$ in terms of the dualizing module $E_2^{(p)}(\mathcal{G}) = \varinjlim_m D_2(\mathbb{Z}/p^m)$ of $\mathcal{G}$.

In § 5 this is applied to study the Λ-module structure of certain abelian Galois groups over K , for a Galois extension K/k of number fields with Galois group G . The main results are:

<u>Theorem</u>. If k is local, then the Λ-module $X = \mathrm{Gal}(M/K)$, M the maximal abelian pro-p-extension of K , is determined by $\mu_K(p)$ - the group of p-power roots of unity in K - and a canonical class $\chi \in H^2(G,\mu_K(p))^\vee$ (where $^\vee$ denotes the Pontrjagin dual).

<u>Theorem</u>. If k is global, let $S \supseteq \{\mathfrak{p}|p\}$ be a finite set of primes in k , let K/k be S-ramified, and let K^S (resp. M^S) be the maximal (resp. maximal abelian) S-ramified pro-p-extension of K . Then the Λ-module $X_S = \mathrm{Gal}(M^S/K)$ is determined by

$W_S = E_2^{(p)\,\mathrm{Gal}(K^S/K)}$ - where $E_2^{(p)}$ is the dualizing module of $\mathrm{Gal}(K^S/k)$ - and a canonical class $\chi \in H^2(G,W_S)^{\vee}$.

The local theorem in particular gives a complete description of the Galois module structure of $\varprojlim_m K^\times/K^{\times p^m}$ for a finite Galois extension K/k and contains all previous results on this subject due to Iwasawa, Borevič,... (see [J1] for references).

In the global case we show that W_S is closely related to $X' = \mathrm{Gal}(L'/K)$, where L'/K is the maximal unramified abelian pro-p-extension in which every prime above p is completely decomposed. For example, if $k(\mu_{p^\infty}) \subseteq K$, then we get an exact sequence

$$0 \longrightarrow X'(-1) \longrightarrow W_S^{\vee} \longrightarrow \bigoplus_{\mathfrak{p}\in S} \overline{\mathrm{Ind}}_{G_{\mathfrak{p}}}^{G}(\mathbb{Z}_p(-1)) \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0 ,$$

where $G_{\mathfrak{p}} \leq G$ is a decomposition group at $\mathfrak{p}$ and $\overline{\mathrm{Ind}}_{G_{\mathfrak{p}}}^{G}$ is the compact induction. If $K = k(\mu_{p^\infty})$, then $W_S^{\vee} \cong E^1(X_S)$, and by the quasi-isomorphism $\mathrm{Tor}_\Lambda(X_S) \sim E^1(X_S)^{\circ}$ (where M° is M with the new action $\gamma\cdot m = \gamma^{-1}m$ for $\gamma \in G$ and $m \in M$) we reobtain the known relations between the characteristic invariants of X_S and X' (see [W1] 7.10). The above result makes this precise up to isomorphism and shows how to extend it to arbitrary G .

In § 6 we derive some exact sequences for $K = k(\mu_{p^\infty})$, which were obtained by K. Wingberg [W1] up to quasi-isomorphism. As corollaries we get results on the Λ-torsion of X_S for varying S and on the Galois structure of the S-units.

I thank Kay Wingberg for several interesting discussions and the MPI at Bonn for hospitality and financial support during the preparation of the final version of this paper. My investigations on the homotopy theory and first versions of the theorems cited above already go back to 1984, when I stayed at the Harvard University, supported by a grant from the DFG. It is perhaps not too late to thank both institutions warmly. Also, it is a pleasure to thank Ted Chinburg for stimulating discussions during that time.

§ 1 Homotopy of modules

A homotopy theory for modules over a ring was introduced by Eckmann and Hilton [Hi], and it was further used and developed by Auslander and Bridger [AB], and by the author [J2]. We recall the basic definitions and results.

Let Λ be a noetherian ring with unit - not necessarily commutative. An example we have in mind is the completed group ring $\mathbb{Z}_p[[G]]$ of a p-adic Lie group G [La] 2.2.4. All Λ-modules considered are assumed to be finitely generated.

1.1. Definition A morphism $f : M \longrightarrow N$ of Λ-modules is homotopic to zero, if it factorizes

$$f : M \longrightarrow P \longrightarrow N$$

through a projective module P. Two morphisms f, g are homotopic $(f \simeq g)$, if $f - g$ is homotopic to zero. Let $[M , N] = \mathrm{Hom}_\Lambda(M , N)/\{f \simeq 0\}$ be the group of homotopy classes of morphisms from M to N, and let $Ho(\Lambda)$ be the category, whose objects are (finitely generated) Λ-modules and whose morphism sets are given by $\mathrm{Hom}_{Ho(\Lambda)}(M , N) = [M , N]$, that is, the category of "Λ-modules up to homotopy".

1.2. Proposition Let M, N be Λ-modules and let $f : M \longrightarrow N$ be a Λ-morphism.

a) $f \simeq 0$ if and only if $f^* : \operatorname{Ext}^i_\Lambda(N, R) \longrightarrow \operatorname{Ext}^i_\Lambda(M, R)$ is zero for all Λ-modules R and all $i \geq 1$ (it suffices to consider $i = 1$) .

b) f is a homotopy equivalence if and only if $f^* : \operatorname{Ext}^i_\Lambda(N, R) \longrightarrow \operatorname{Ext}^i_\Lambda(M, R)$ is an isomorphism for all Λ-modules R and all $i \geq 1$ (it suffices to consider $i = 1$) .

c) $M \simeq N$ (i.e., M and N are homotopy equivalent, i.e., isomorphic in $H_0(\Lambda)$) 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.

As a first application of the concept of homotopy, we get the following generalization of Schanuel's lemma.

<u>1.3. Lemma</u> Let $f, g : M \longrightarrow N$ be surjective Λ-morphisms. If $f \simeq g$, then $\ker f \simeq \ker g$.

<u>Proof</u> Let $f - g = \pi \circ \varphi : M \xrightarrow{\varphi} P \xrightarrow{\pi} N$ with P projective, then we get a commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "\wr"'] & M \oplus P \arrow[r, "f+\pi"] \arrow[d, "\wr"', "\Phi"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r] & N \oplus P \arrow[r, "g+\pi"] & N \arrow[r] & 0
\end{tikzcd} ,$$

where $\phi : (m, p) \longmapsto (m, p + \varphi(m))$ is the mapping cylinder of φ. But $K \cong \ker f \oplus P$ by the commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker f \arrow[r] \arrow[d, hook] & M \arrow[r, "f"] \arrow[d, hook] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & k \arrow[r] \arrow[d] & M \oplus P \arrow[r, "f+\pi"] \arrow[d] & N \arrow[r] & 0 \\
& P \arrow[r, equal] & P & &
\end{tikzcd},$$

and similarly $L \cong P \oplus \ker g$.

The following groups will become important in the sequel. Their role is similar to that of the homotopy groups in topology.

<u>1.4. Definition</u> Let $E^{o}(M) = M^{+} = \mathrm{Hom}_{\Lambda}(M, \Lambda)$ be the Λ-dual, and more generally, let $E^{i}(M) = \mathrm{Ext}^{i}_{\Lambda}(M, \Lambda)$ for $i \geq 0$. If M is a left Λ-module, say, these are right Λ-modules by functoriality and the right Λ-structure of the bi-module Λ.

The following functors are well-defined (only) up to homotopy, i.e., as functors from $\mathrm{Ho}(\Lambda)$ to $\mathrm{Ho}(\Lambda)$.

<u>1.5. Definition and theorem</u>

a) The <u>loop space</u> functor $M \leadsto \Omega M$ is defined as follows:

i) Choose a surjection $P \xrightarrow{\pi} M$ with P projective.

ii) Let $\Omega = \ker \pi$.

Thus, ΩM is characterized by an exact sequence

$$(1.5.1) \qquad 0 \longrightarrow \Omega M \longrightarrow P \longrightarrow M \longrightarrow 0$$

with P projective (i.e., ΩM is "the" first syzygy-module).

b) Ω has a left adjoint Σ (i.e., $[\Sigma M , N] \cong [M , \Omega N]$ functorially in M and N) , the suspension functor $M \leadsto \Sigma M$ which is defined as follows:

i) Choose a surjection $P \xrightarrow{\pi} M^+$ with P projective

ii) Let $\Sigma M = \operatorname{Coker}(M \xrightarrow{\varphi_M} M^{++} \xrightarrow{\pi^+} P^+)$, where $\varphi_M : M \longrightarrow M^{++}$ is the canonical map into the bi-dual.

One has $N \cong \Sigma M$ if and only if $E^1(N) = 0$ and there is an exact sequence

$$(1.5.2) \qquad M \xrightarrow{\varphi} Q \longrightarrow \Sigma M \longrightarrow 0$$

with $\ker \varphi = T_1(M) := \ker \varphi_M$.

c) The transpose DM is defined as follows

i) Choose $P_1 \xrightarrow{\pi_1} P_o \longrightarrow M \longrightarrow 0$ exact with projectives P_1

and P_o .

ii) Let $DM = \mathrm{Coker}(P_o^+ \xrightarrow{\pi_1^+} P_1^+)$.

In other words, DM is defined by the exact sequence

(1.5.3) $$0 \longrightarrow M^+ \longrightarrow P_o^{\ +} \longrightarrow P_1^{\ +} \longrightarrow DM \longrightarrow 0 .$$

Then one has $D^2 = \mathrm{Id}$ and $D\Omega = \Sigma D$ (hence also $D\Sigma = \Omega D$) .

For the proofs one uses the defining properties of projectives and the facts that for a projective P the module P^+ is also projective and $\varphi_P : P \longrightarrow P^{++}$ is an isomorphism. For example, the last facts immediately imply $D^2 = \mathrm{Id}$, and the functoriality of Ω is obtained by a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \Omega M \arrow[r] \arrow[d, dashed, "\Omega f"'] & P \arrow[r] \arrow[d, dashed] & M \arrow[r] \arrow[d, "f"] & 0 \\ 0 \arrow[r] & \Omega N \arrow[r] & Q \arrow[r] & N \arrow[r] & 0 \end{tikzcd} ,$$

where the dotted lifting of f exists by the projectivity of P , and Ωf is the induced map.

The reader should be aware of the fact that D and the E^i

interchange left and right Λ-action . In the case of a group ring there is a natural equivalence between left and right modules, induced by the involution of the group ring given by passing to the inverses of the group elements. Equivalently, we may in this case use the two left Λ-module structures of Λ to give the $E^i(M)$ and hence DM left Λ-module structures again, if M is a left Λ-module , say. In general this is not possible, but for the theory it is not necessary either, and in the following we shall not specify, if we are talking of left or right Λ-modules or if a functor interchanges left and right Λ-action . This would only cause notational complications, and it will always be clear where one had to insert "left" or "right".

Recall that the projective dimension $pd_\Lambda(M)$ of a Λ-module M is the infimum over the numbers $n \geq 0$ such that there exists a resolution of length n

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_o \longrightarrow M \longrightarrow 0$$

with projectives P_i (with the usual convention that $\inf \emptyset = \infty$) .

<u>1.6. Theorem</u> The functor $M \mapsto E^1(M)$ induces an equivalence of categories

$$\left\{\begin{matrix}\Lambda\text{-modules } M \text{ with} \\ pd_\Lambda(M) \leq 1 \text{ up to homotopy}\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}\Lambda\text{-modules } N \\ \text{with } N^+ = 0\end{matrix}\right\} .$$

Proof One simply observes that D gives an essential inverse: Namely, for a module M with $pd_\Lambda(M) \leq 1$ one obviously has $DM \simeq E^1(M)$ and hence $DE^1(M) \simeq DDM \simeq M$. Moreover, one has $E^1(M)^+ = 0$ in view of 1.5.3. On the other hand, if $N^+ = 0$, then $pd_\Lambda(DN) \leq 1$ by 1.5.3 and hence $E^1(DN) \simeq DDN \simeq N$ by the above. It remains to remark that for Λ-modules N , N' with $N^+ = 0$ one obviously has $Hom_\Lambda(N, N') \cong [N, N']$.

1.7. Remark This theorem generalizes and sharpens theorem 2.1 in [J1] (cf. 2.5 below) and should be compared with section VII § 3 in [Kun].

1.8. Lemma and Definition Let $T_1(M) = \ker \varphi_M$ as above and $T_2(M) = \mathrm{Coker}\, \varphi_M$, so that

$$(1.8.1) \qquad 0 \longrightarrow T_1(M) \longrightarrow M \xrightarrow{\varphi_M} M^{++} \longrightarrow T_2(M) \longrightarrow 0$$

is exact. Then canonically $T_1(M) \cong E^1(DM)$ and $T_2(M) \cong E^2(DM)$. In view of this let

$$(1.8.2) \qquad T_i(M) = E^i(DM) \qquad , \quad i \geq 1 .$$

(It is clear that $E^i(N)$ only depends on N up to homotopy for $i \geq 1$) .

The proof is straightforward, compare [HS] IV ex. 7.3. We are now ready to answer the following question. Suppose we know ΩM

or ΣM for a Λ-module M. Obviously some information on M is lost (e.g., $\Omega M \simeq 0$ if $pd_\Lambda(M) \leq 1$) ; how can we recover M itself? Theorem 1.6 tells us that at least we have to invoke $E^1(M)$ (or, dually, $T_1(M)$) ; the general answer is:

<u>1.9. Theorem</u> A Λ-module M is determined up to homotopy by

a) ΣM , $T_1(M)$, and a class $\chi_M \in \mathrm{Ext}^1_\Lambda(\Omega\Sigma M , T_1(M))$, or by

b) ΩM , $E^1(M)$, and a class $\psi_M \in \mathrm{Ext}^1_\Lambda(D\Sigma\Omega M , E^1(M))$.

(Note that these Ext-groups in the first variable only depend on modules up to homotopy).

<u>Proof</u>

a) Let χ_M be the class of the extension

(1.9.1) $0 \longrightarrow T_1(M) \longrightarrow M \longrightarrow \mathrm{Im}\ \varphi_M \longrightarrow 0$,

via the canonical identification

(1.9.2) $\mathrm{Im}\ \varphi_M \simeq \Omega\Sigma M$,

which is obvious from the definitions of Σ and Ω (let us remark at this place that under this identification, the map $M \longrightarrow \mathrm{Im}\ \varphi_M$ is the adjunction map $M \longrightarrow \Omega\Sigma M$) . Since M is determined by $T_1(M)$, $\operatorname{Im} \varphi_M$ and the extension class of 1.9.1, the result follows.

b) is obtained by dualizing, i.e., by applying the above to DM . Note that M is determined by DM up to homotopy (this is not true for M^+ !) and that we have $T_1(DM) = E^1(M)$ and $\Omega\Sigma DM = D\Sigma\Omega M$, so that we define $\psi_M = \chi_{DM}$.

For the understanding of this theorem it should be added that no information is lost in passing from ΩM (respectively, ΣM) to $\Sigma\Omega M$ (respectively, $\Omega\Sigma M$) , by the following result.

<u>1.10. Theorem</u> The functors Σ and Ω induce quasiinverse equivalences of categories

$$\left\{\begin{matrix}\Lambda\text{-modules } M \text{ with } T_1(M) = 0\\ \text{up to homotopy}\end{matrix}\right\} \underset{\underset{\Omega}{\sim}}{\overset{\Sigma}{\underset{\sim}{\rightleftarrows}}} \left\{\begin{matrix}\Lambda\text{-modules } N \text{ with } E^1(N) = 0\\ \text{up to homotopy}\end{matrix}\right\}$$

<u>Proof</u> Note that for any Λ-module M we have $E^1(\Sigma M) = 0$ by 1.5 b), and hence $T_1(\Omega M) = E^1(D\Omega M) = E^1(\Sigma DM) = 0$. The result now easily follows from the characterization of ΣM in 1.5 b).

<u>1.11. Corollary</u>

a) The following statements are equivalent:

i) $T_1(M) = 0$.

ii) M is submodule of a free module.

iii) $M \simeq \Omega N$ for some Λ-module N .

iv) The adjunction map $M \longrightarrow \Omega\Sigma M$ is a homotopy equivalence.

b) The following statements are equivalent:

i) $E^1(N) = 0$.

ii) $N \simeq \Sigma M$ for some Λ-module N .

iii) The adjunction map $\Sigma\Omega N \longrightarrow N$ is a homotopy equivalence.

<u>1.12. Remark</u> We have worked with finitely generated modules to ensure that P^+ is again projective and that φ_P is an isomorphism for projective P . We have assumed Λ to be noetherian to make sure that M^+ , ΩM etc. are finitely generated again. For non-noetherian Λ one formally obtains the same results, if one ensures that all considered modules are finitely generated. For example, D is defined for finitely presented Λ-modules.

§ 2. Group rings of profinite groups

For a profinite group G define the completed group ring over $\mathbb{Z}_p$ by

$$\Lambda = \Lambda(G) = \mathbb{Z}_p[[G]] = \varprojlim_{U \trianglelefteq G} \mathbb{Z}_p[G/U] ,$$

where U runs over all open normal subgroups of G.

For a closed subgroup $S \leq G$ and a discrete G-module A Tate has defined the groups

$$D_r(S,A) = \varinjlim_{U \geq S} H^r(U,A)^* \qquad (r \geq 0)$$

where $B^* = \mathrm{Hom}(B,\mathbb{Q}/\mathbb{Z})$ for an abelian group B, and where the limit runs over all open subgroups U of G containing S, with transition maps the transposes of the corestriction map ([S1] I-79 ff.). This is contravariant in A, and if S is a normal subgroup, then $D_r(S,A)$ is a discrete G/S-module in a natural way. In particular, one has the discrete G-module

$$D_r(A) = D_r(\{1\},A) \qquad (r \geq 0) .$$

In the following assume that Λ is noetherian. For example, G can be a profinite (= compact) Lie group over $\mathbb{Q}_p$ ([La] V 2.2.4). Then a finitely generated Λ-module M has a natural compact topology as a pseudo-compact module over the pseudo-compact algebra Λ (cf. [Br]), and its Pontrjagin dual $M^\vee = \mathrm{Hom}_{cont}(M,\mathbb{Q}_p/\mathbb{Z}_p)$ $= \varinjlim_{U} M_U{}^*$ (where U runs over the open subgroups of G and M_U

is the module of coinvariants) is a discrete G-module. The functors $M \mapsto M^\vee$ and $A \mapsto A^\vee$ are quasi-inverse equivalences between the category of pseudo-compact Λ-modules and the category of discrete, $\mathbb{Z}_p$-torsion G-modules ([Br]). Here $A^\vee$ is the Pontrjagin dual of A, i.e. $A^\vee = A^*$, with the topology of pointwise convergence. For an abelian group B and $n \in \mathbb{N}$ let $B/n = B/nB$ and ${}_nB = \{b \in B \mid nb = 0\}$.

<u>2.1 Theorem</u>. Let M be a finitely generated Λ-module.

a) There are functorial exact sequences

$$0 \to D_r(M^\vee) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to E^r(M)^\vee \to \mathrm{Tor}\, D_{r-1}(M^\vee) \to 0$$

for all $r \geq 0$, where by definition $D_{-1} = 0$.

b) There is a long exact sequence

$$\dots \to E^r(M)^\vee \to \varinjlim_m D_r({}_{p^m}(M^\vee)) \to \varinjlim_m D_{r-2}(M^\vee/p^m) \to E^{r-1}(M)^\vee \to \dots ,$$

functorial in M and in G.

<u>Proof</u>. We start by observing that $M \mapsto M^\vee$ maps projectives to injectives and that $A \mapsto A^*$ carries injectives to projectives, since $\Lambda^\vee \cong \mathrm{Ind}_G(\mathbb{Q}_p/\mathbb{Z}_p)$ (the induced module). Furthermore we have canonically

$$M^+ = \mathrm{Hom}_\Lambda(M,\Lambda) \cong \varprojlim_{U \trianglelefteq G} \mathrm{Hom}_\Lambda(M,\mathbb{Z}_p[G/U])$$

$$\cong \varprojlim_{U \trianglelefteq G} \mathrm{Hom}_{\mathbb{Z}_p[G/U]}(M_U,\mathbb{Z}_p[G/U])$$

$$\cong \varprojlim_{U \trianglelefteq G} \mathrm{Hom}_{\mathbf{Z}_p}(M_U, \mathbf{Z}_p) ,$$

where the limit is taken via the norms. Hence

$$(M^+)^\vee \cong \varinjlim_{U \trianglelefteq G} \mathrm{Hom}_{\mathbf{Z}_p}(M_U, \mathbf{Z}_p)^\vee$$

$$\cong \varinjlim_{U \trianglelefteq G} M_U \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p ,$$

where we have used the relation

$$\left(\varprojlim_m \mathrm{Hom}_{\mathbf{Z}_p}(N/p^m, \mathbf{Z}/p^m)\right)^\vee \cong \varinjlim_m N/p^m$$

for a finitely generated $\mathbf{Z}_p$-module N. We may rewrite this as

$$(2.1.1) \qquad (M^+)^\vee = \left(\varinjlim_{U \trianglelefteq G} ((M^\vee)^U)^*\right) \otimes \mathbf{Q}_p/\mathbf{Z}_p$$

or as

$$(2.1.2) \qquad (M^+)^\vee = \varinjlim_m \left(\varinjlim_{U \trianglelefteq G} (((M/p^m)^\vee)^U)^*\right) .$$

In other words, 2.1.1 describes $M \leadsto (M^+)^\vee$ as the composition of the right exact functors $M \leadsto D_0(M^\vee)$ and $N \leadsto N \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$, while 2.1.2 describes it as the composition of the right exact functors $M \leadsto \underline{C}_p(M)$ and $(M_m) \leadsto \varinjlim_m D_0(M_m{}^\vee)$, where $\underline{C}_p$ sends M to the inductive system (M/p^m), with transition maps $M/p^m \longrightarrow M/p^{m+1}$ induced by the p-multiplication. Now the r-th left derivative of $M \leadsto D_0(M^\vee)$ is $M \leadsto D_r(M^\vee)$, and the first functors in the compositions map projectives to acyclics for the second functors. Since $M \mapsto M^\vee$ and filtering direct limits are exact, we get two Grothendieck spectral sequences of homological type

$$E^2_{r,s} = \mathrm{Tor}_r^{\mathbb{Z}_p}(D_s(M^\vee), \mathbb{Q}_p/\mathbb{Z}_p) \Rightarrow E_{r+s} = E^{r+s}(M)^\vee$$

$$E^2_{r,s} = \varinjlim_n D_r(L^s \underline{C}_p(M)^\vee) \Rightarrow E_{r+s} = E^{r+s}(M)^\vee .$$

The exact sequences in a) and b) follow from this, since

$$\mathrm{Tor}_r^{\mathbb{Z}_p}(N, \mathbb{Q}_p/\mathbb{Z}_p) = \begin{cases} N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p & r = 0 , \\ \mathrm{Tor}_{\mathbb{Z}_p}(N) & r = 1 , \\ 0 & r \geq 2 , \end{cases}$$

and the left derivatives of $\underline{C}_p$ are

$$L^s \underline{C}_p(M) = \begin{cases} (M/p^m) & s = 0 , \\ ({}_{p^m}M) & s = 2 , \\ 0 & s \geq 2 , \end{cases}$$

since projective modules are torsion-free. In b) we also use the fact that $(M/p^m)^\vee = {}_{p^m}(M^\vee)$ and $({}_{p^m}M)^\vee = M^\vee/p^m$.

2.2 Remarks. a) The above can be extended to the case of an arbitrary profinite group G , i.e., to non-noetherian Λ , as follows. Call a Λ-module noetherian, if it has a resolution by finitely projective Λ-modules. By looking at such a resolution it easily follows that 2.1 a) remains true for noetherian modules M

and that 2.1 b) still holds, if $\operatorname{Tor}_{\mathbb{Z}_p}$ and $M/\operatorname{Tor}_{\mathbb{Z}_p}(M)$ (and hence M) are noetherian. The other results of this section extend similarly.

b) It is easy to see that the sequence in 2.1 b) can be identified with the long exact sequence

$$\ldots \to E^r(M)^\vee \to E^r(M/\operatorname{Tor}_{\mathbb{Z}_p}(M))^\vee \to E^{r-1}(\operatorname{Tor}_{\mathbb{Z}_p}(M))^\vee \to E^{r-1}(M)^\vee \to \ldots .$$

<u>2.3 Lemma</u>. If $U \leq G$ is an open subgroup of G , then the restriction induces a functorial isomorphism of Λ_U-modules

$$E^r_G(M) := \operatorname{Ext}^r_{\Lambda(G)}(M,\Lambda(G)) \xrightarrow{\sim} \operatorname{Ext}^r_{\Lambda(U)}(M,\Lambda(U)) =: E^r_U(M)$$

for every $\Lambda(G)$-module M .

<u>Proof</u>. Since $\Lambda(G)$ is projective as a $\Lambda(U)$-module, this follows from the obvious case $r = 0$ by looking at a free resolution of M .

<u>2.4 Corollary</u>. Let $n = \operatorname{vcd}_p(G)$ be the virtual p-cohomological dimension of G , then $E^r(M) = 0$ for $r > n+1$.

<u>Proof</u>. Recall that $\operatorname{vcd}_p(G) \leq n$ means that there is an open subgroup U of G with p-cohomological dimension $\operatorname{cd}_p(U) \leq n$. This obviously implies $D_r(A) = 0$ for $r > n$, hence the result by 2.1 a). One may also use 2.3 and [Br] 4.1.

<u>2.5 Corollary</u>. Let G be a finite group, then $E^0(M) = \operatorname{Hom}_{\mathbb{Z}_p}(M,\mathbb{Z}_p)$, $E^1(M) = \operatorname{Tor}_{\mathbb{Z}_p}(M)^\vee$, and $E^r(M) = 0$ for $r \geq 2$.

Proof. One has $vcd_p(G) = 0$, so the result follows with 2.4 and 2.1 a). One may also use 2.3 and the isomorphisms $\mathrm{Ext}^r_{\mathbb{Z}_p}(M,\mathbb{Z}_p) \cong \mathrm{Tor}_r^{\mathbb{Z}_p}(M,\mathbb{Q}_p/\mathbb{Z}_p)^\vee$.

2.6 Corollary. Assume that G is virtually strict Cohen-Macaulay at p (i.e., that an open subgroup has this property, see [S1] V 4,1), with $vcd_p(G) = n$. (Examples of such groups are p-Poincaré groups of dimension n, in particular, by a result of Lazard [La] V 2.5.8, compact Lie groups of dimension n over $\mathbb{Q}_p$, e.g., $G = \mathbb{Z}_p^n$). Then

a) $E^r(\mathbb{Z}_p) = 0$ for $r \neq n$, and $E^n(\mathbb{Z}_p)^\vee \cong E_n^{(p)}(G)$, the p-torsion dualizing module.

b) If N is a finite G-module, then $E^r(N) = 0$ for $r \neq n+1$, and $E^{n+1}(N)^\vee \cong \mathrm{Hom}_{\mathbb{Z}_p}(N^\vee, E_n^{(p)}(G))$.

c) If M is a finitely generated, torsion-free $\mathbb{Z}_p$-module with continuous action of G, then $E^r(M) = 0$ for $r \neq n$ and $E^n(M)^\vee \cong \varinjlim_m D_n((M/p^m)^\vee) \cong M \otimes_{\mathbb{Z}_p} E_n^{(p)}(G)$.

Proof c): By 2.1 b) we get

$$E^r(M)^\vee \cong \varinjlim_m D_r((M/p^m)^\vee) .$$

This is zero for $r \neq n$ by the assumptions (cf. [S1] V 3.1, 5) c) and I annexe, théorème 3), while for any finite G-module A we have

7

$$D_n(A) = \varinjlim_{U\leq G,\mathrm{cor}^*} H^n(U,A)^*$$

(2.6.1)

$$\cong \varinjlim_{U\leq G,\mathrm{res}} H^0(U,\mathrm{Hom}_{\mathbb{Z}_p}(A,E_n^{(p)}(G))) = \mathrm{Hom}_{\mathbb{Z}_p}(A,E_n^{(p)}(G))$$

by duality (see loc.cit). For M as in c) this implies

$$\varinjlim_m D_n((M/p^m)^\vee) = \varinjlim_m \mathrm{Hom}_{\mathbb{Z}_p}((M/p^m)^\vee,\ E_n^{(p)}(G)) \cong M \otimes_{\mathbb{Z}_p} E_n^{(p)}(G) \quad ,$$

hence the result. Part a) is a special case of c), while for N as in b) we may use 2.1 a) to obtain

$$E^r(N) \cong D_{r-1}(N^\vee) \quad ,$$

hence the claim by the previous considerations.

<u>2.7 Remarks</u>. a) In the cited notes by Tate and Verdier the groups are assumed to have finite p-cohomological dimension, but for our applications we only had to assume $\mathrm{vcd}_p(G) < \infty$, since we could always pass to some open subgroup.

b) Usually one considers left discrete G-modules A and gives A^* a left G-module structure by $(\sigma f)(a) = f(\sigma^{-1}a)$ for $f : A \to \mathbb{Q}/\mathbb{Z}$, $\sigma \in G$ and $a \in A$, similarly for compact G-modules M and $M^\vee$. If we do so, we have to give $E^r(M)$ the left G-module structure in the statements above, cf. the discussion in § 1. Otherwise we have to endow A^* and $M^\vee$ with the canonical right G-structure ($(\sigma f)(a) = f(\sigma a)$ etc.).

§ 3. The case $G = \mathbb{Z}_p$

In this section let $G = \mathbb{Z}_p$, so that $\Lambda = \Lambda(\mathbb{Z}_p)$ is the classical Iwasawa algebra. Then G is a p-Poincaré group of cohomological dimension 1 with dualizing module $E_1^{(p)}(G) \cong \mathbb{Q}_p/\mathbb{Z}_p$ (compare [S1] I 3.5 Exemples), and we can deduce several of the following results from this and the results in the previous section. Instead we have preferred to argue more directly, by using well-known facts on Λ, e.g., that it is a noetherian local ring with projective dimension $pd(\Lambda) = 2$ (recall that $pd(\Lambda) = \sup pd_\Lambda(M)$, where M runs over all finitely generated Λ-modules). This implies that $E^i(M) = 0 = T_i(M)$ for $i \geq 3$. We now investigate these groups for $i \leq 2$; for this let $T_0(M)$ be the maximal finite submodule of M.

3.1 Lemma. Let M be a noetherian Λ-module (as always).

a) $T_1(M)$ is the Λ-torsion submodule of M.

b) $E^1(M)$ is a Λ-torsion module. If M is Λ-torsion, then $E^1(M)$ is the Iwasawa adjoint $\alpha(M)$ of M ([Iw] 1.3) and has no non-zero finite submodule. Finally, $E^1(N) = 0$ for a finite module N.

c) $T_2(M)$ is finite. One has $T_2(M) = 0$ if and only if $M/T_1(M)$ is free, i.e., if and only if $M \cong T_1(M) \oplus \Lambda^r$ for some $r \geq 0$. In particular, $T_2(M) = 0$ for Λ-torsion modules.

d) $E^2(M)$ is finite, one has $E^2(M) \cong E^2(T_0(M)) \cong T_0(M)^\vee$, and the following properties are equivalent:

i) $E^2(M) = 0$,

ii) $pd_\Lambda(M) \leq 1$,

iii) $T_0(M) = 0$,

iv) M is a submodule of an elementary Λ-module.

Proof. a) is clear by tensoring with the field of fractions of Λ. The first statement in b) follows from a) since $E^1(M) = T_1(DM)$. For the second statement see [P-R] I.2.2 and [Bi] 1.2 and remarque, and $T_0(\alpha(M)) = 0$ follows from Iwasawa's first description of $\alpha(M)$ in [Iw] 1.3.

By the exact sequence $0 \to \Lambda \xrightarrow{\gamma-1} \Lambda \to \mathbb{Z}_p \to 0$, where γ is a topological generator of G, we immediately deduce $E^1(\mathbb{Z}_p) \cong \mathbb{Z}_p$ (this always denotes the module $\mathbb{Z}_p$ with trivial action of G). The exact sequence

$$0 \to E^1(\mathbb{Z}/p) \to E^1(\mathbb{Z}_p) \xrightarrow{p} E^1(\mathbb{Z}_p) \to E^2(\mathbb{Z}/p) \to 0$$

now shows $E^1(\mathbb{Z}/p) = 0$ and hence $E^1(N) = 0$ for every finite module N, since such N possesses a composition series with quotients isomorphic to $\mathbb{Z}/p$.

d): By the structure theory for Iwasawa modules there exists an exact sequence

$$0 \to A \to M \xrightarrow{f} E \to C \to 0 ,$$

where E is elementary and A and C are finite. One has $pd_\Lambda(E) \leq 1$ and $T_0(E) = 0$. The last property implies $A = T_0(M)$, the first one implies $E^2(\mathrm{Im}\, f) = 0$, since this is a quotient of $E^2(E) = 0$, hence we get $E^2(M) \xrightarrow{\sim} E^2(A)$. The isomorphism

$$E^2(A) \cong \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$$

now follows from the local duality for the regular local ring Λ of dimension 2 with residue field $\mathbb{Z}/p$ (cf. [Bi] 1.2). The rest is

/10

clear: f is injective if and only if $T_0(M) = 0$, i.e., if and only if $T_0(M)^\vee = E^2(T_0(M)) \cong E^2(M)$ is zero, i.e., if and only if $pd_\Lambda(M) \leq 1$: look at a resolution

$$0 \to P_2 \xrightarrow{\pi_2} P_1 \to P_0 \to M \to 0 ;$$

if $E^2(M) = 0$, then π_2 has a left inverse.

c) now easily follows from the relation $T_2(M) = E^2(DM)$, the exact sequence 1.8.1 and the well-known fact that M^{++} is projective for $cd(\Lambda) \leq 2$ (which can be deduced from the exact sequence 1.5.3), and that projective modules are free for local rings.

We now use theorem 1.9 to describe, how a Λ-module M is determined by the above invariants. This result is valid more generally for rings Λ with $pd(\Lambda) \leq 2$.

3.2 Theorem. A Λ-module M is determined up to homotopy by
a) $T_1(M)$, $T_2(M)$ and a class $\chi_M \in Ext^2_\Lambda(T_2(M), T_1(M))$, or by
b) $E^1(M)$, $E^2(M)$ and a class $\psi_M \in Ext^2_\Lambda(E^2(M), E^1(M))$.

Proof. In our case M^{++} is projective, so from the exact Ext-sequence associated to the exact sequence

$$(3.2.1) \quad 0 \to Im\, \phi_M \to M^{++} \to T_2(M) \to 0$$

we obtain an isomorphism

$$\mathrm{Ext}^1_\Lambda(\mathrm{Im}\ \phi_M, T_1(M)) \xrightarrow{\sim} \mathrm{Ext}^2_\Lambda(T_2(M), T_1(M)) \ .$$

If by abuse of notation we denote the image of χ_M under this isomorphism (which is the class of the 2-extension 1.8.1) again by χ_M , a) immediately follows from 1.9 a). Note that 3.2.1 implies $\mathrm{Im}\ \phi_M \simeq \Omega\ T_2(M)$ so that $\mathrm{Im}\ \phi_M$ is determined by $T_2(M)$ up to homotopy, and in fact, 1.10 implies $T_2(M) \simeq \Sigma\ \mathrm{Im}\ \phi_M \simeq \Sigma\ \Omega\ \Sigma\ M \simeq \Sigma\ M$, since $E^1(T_2(M)) = 0$ by 3.1 b).

Part b) follows by dualizing, i.e., applying everything to DM , letting $\psi_M = \chi_{DM}$ under the identifications $T_1(DM) = E^1(M)$ and $T_2(DM) = E^2(M)$.

We now further investigate E^1 and T_1 .

<u>3.3 Lemma</u>. a) One has $E^1(M) \xleftarrow{\sim} E^1(M/T_0(M))$, and equivalence of the following statements:

i) $E^1(M) = 0$.

ii) $M/T_0(M)$ is free, i.e., $M \cong T_0(M) \oplus \Lambda^r$ for some $r \geq 0$.

b) the following statements are equivalent:

i) $T_1(M) = 0$.

ii) There is an exact sequence $0 \to M \to P \to C \to 0$ with P projective (= free) and C finite.

<u>Proof</u>. a) The first claim follows from the exact sequence

$$0 = E^0(T_0(M)) \to E^1(M/T_0(M)) \to E^1(M) \to E^1(T_0(M)) = 0 \ .$$

But by 3.1 d) we have $\mathrm{pd}_\Lambda(M/T_0(M)) \leq 1$, hence $M/T_0(M) \simeq 0$ if and only if $E^1(M/T_0(M)) = 0$ by 1.6.

b) The implication ii) $\Rightarrow$ i) is clear (cf. also 1.11). For the converse we may take the sequence 3.2.1.

3.4 Lemma. If $0 \to M \to P \to C \to 0$ is exact with P projective and C finite, then there is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d, equal] & P \arrow[r] \arrow[d, "\alpha", "\wr"'] & C \arrow[r] \arrow[d, "\beta", "\wr"'] & 0 \\ 0 \arrow[r] & M \arrow[r] & M^{++} \arrow[r] & T_2(M) \arrow[r] & 0 \end{tikzcd}$$

with canonical isomorphisms α and β .

Proof. The map $i : M \longrightarrow P$ induces an isomorphism $i^+ : P^+ \xrightarrow{\sim} M^+$, since $C^+ = 0 = E^1(C)$. The commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "\phi_M"'] & P \arrow[r] \arrow[d, "\phi_P", "\wr"'] & C \arrow[r] & 0 \\ 0 \arrow[r] & M^{++} \arrow[r, "i^{++}", "\sim"'] & P^{++} & & \end{tikzcd}$$

shows that we may take $\alpha = (i^{++})^{-1} \circ \phi_P$, and for β the induced map.

3.5 By 1.2 c) and the Krull-Schmidt theorem for Λ , a Λ-module is determined by its homotopy type and its rank. Hence by the above discussion the investigation of Λ-modules up to isomorphism can be reduced to the following three types of Λ-modules

13

A) free modules,

(3.5.1) B) Λ-torsion modules with $\mathrm{pd}_\Lambda(M) \leq 1$,

C) finite modules,

and two extension classes. For a Λ-module M the modules in question are

(3.5.2) A) M^{++} B) $T_1(M)/T_0(M)$ C) $T_0(M)$, $T_2(M)$

with the extension classes χ_M and the one describing the extension $0 \to T_0(M) \to T_1(M) \to T_1(M)/T_0(M) \to 0$. In the "dual picture" we have

(3.5.3) A) $E^0(E^0(M))$ B) $E^1(E^1(M))$ C) $E^2(E^1(M))$, $E^2(E^2(M))$,

ψ_M and another class described below. The three types of Λ-modules are characterized by the properties

A) $E^1(M) = 0 = E^2(M)$,

B) $E^0(M) = 0 = E^2(M)$,

C) $E^0(M) = 0 = E^1(M)$,

i.e., they have only one non-vanishing E^i .

For the categories of Λ-modules given by A), B) and C) one has self-dualities given by

A) E^0 ,

B) E^1 ,

C) E^2 .

This is clear for A), while for a finite module N we have $E^2(E^2(N)) \cong E^2(N^\vee) \cong N^{\vee\vee} \cong N$ by 3.1 d). The duality for modules of type B) has been treated in [P-R] I 2.4, it also follows from 1.6 by restricting to modules of type B) on both sides. Of course, all three cases follow from the general duality theory for

Cohen-Macaulay modules (cf. [Gr]) or from the simple remark that canonically $P. \xrightarrow{\sim} P.^{++}$ for a complex $P.$ of projective Λ-modules.

3.6 Remarks. a) The modules in 3.5.2 and 3.5.3 are related to the spherical filtration and approximation theorems of [AB] 2 § 6, cf. also the "Postnikov tower" of M in [J2].
b) In [Jak] Jakovlev has initiated an interesting classification theory for modules of type B) in terms of cohomology. This has been continued and extended in [Ko] and [Še].

We now show that the sets of invariants in 3.5.2 and 3.5.3 are in fact the same.

3.7 Lemma. a) There is an exact sequence

$$0 \to E^2(T_2(M)) \to E^1(M) \to E^1(T_1(M)) \to 0$$

inducing isomorphisms

i) $E^2(T_2(M)) \cong E^1(M/T_1(M)) \cong T_0(E^1(M))$,

ii) $E^1(T_1(M)) \cong E^1(M)/T_0(E^1(M))$.

b) There are canonical isomorphisms

i) $E^1(E^1(M)) \cong T_1(M)/T_0(M)$,

ii) $E^2(E^1(M)) \cong T_2(M)$,

iii) $E^2(E^2(M)) \cong T_0(M)$.

Proof. a): By splitting the sequence

$$0 \to T_1(M) \to M \xrightarrow{\phi_M} M^{++} \to T_2(M) \to 0$$

into two short exact sequences containing $B = \operatorname{Im} \phi_M = M/T_1(M)$ we obtain exact sequences

$$0 = E^1(M^{++}) \to E^1(B) \to E^2(T_2(M)) \to E^2(M^{++}) = 0$$

$$0 = E^0(T_1(M)) \to E^1(B) \to E^1(M) \to E^1(T_1(M)) \to E^2(B) = 0$$

and hence the result - note that $T_0(E^1(T_1(M))) = 0$ by 3.1 b) and that $E^2(T_2(M))$ is finite by 3.1 d).

b): From 3.3 a) we have $E^1(E^1(M)) \cong E^1(E^1(M)/T_0E^1(M)) \cong E^1(E^1(T_1(M))) \cong E^1(E^1(T_1(M)/T_0(M))) \cong T_1(M)/T_0(M)$, since $T_1(M)/T_0(M)$ is of type B). With a) we conclude

$$E^2(E^1(M)) \cong E^2(T_0E^1(M)) \cong E^2(E^2(T_2(M))) \cong T_2(M) ,$$

since $T_2(M)$ is of type c). The third isomorphism is clear from 3.1 d).

<u>3.8 Corollary</u>. $E^1(M)$ is finite $\Leftrightarrow T_1(M)$ is finite $\Leftrightarrow E^1(E^1(M)) = 0$.

From § 2 we deduce the following formulae for the E^r-groups, which should be compared with [W3] 1.1.

<u>3.9 Lemma</u>. Let M be a finitely generated Λ-module, let G_n be the subgroup of index p^n in G, and let $M^\delta = \bigcup_n M^{G_n}$ be the maximal submodule of M on which G acts discretely. Then

a) $E^0(M) = \varprojlim_{n,m} {}_{p^m}(M^\vee)^{G_n}$ is free of the same rank as M ,

b) $E^1(\mathrm{Tor}_{\mathbb{Z}_p}(M)) \cong \varprojlim_{n,m} (M^\vee/p^m)^{G_n}$,

c) $E^1(M/\mathrm{Tor}_{\mathbb{Z}_p}(M)) \cong \varprojlim_{n,m} ({}_{p^m}(M^\vee))_{G_n}$,

d) $E^1(M^\delta) \cong \varprojlim_{n,m} {}_{p^m}((M^\vee)_{G_n}) \cong \mathrm{Hom}_{\mathbb{Z}_p}(M^\delta,\mathbb{Z}_p)$,

e) $E^1(M/M^\delta) \cong \varprojlim_{n,m} ((M^\vee)^{G_n})/p^m$,

f) $E^2(M) \cong \varprojlim_{n,m} (M^\vee/p^m)_{G_n} \cong \varprojlim_{n,m} (M^\vee)_{G_n}/p^m$,

where the transition maps are the obvious ones.

<u>Proof</u>. Since $H^0(G_n,A) = A^{G_n}$ and $H^1(G_n,A) \cong A_{G_n}$ for a discrete G-module A , a),b),c) and f) immediately follow with 2.1 b) and remark 2.2 b). From 2.1 a) we get an exact sequence

$$0 \longrightarrow \varprojlim_{n,m} (M^\vee)^{G_n}/p^m \longrightarrow E^1(M) \longrightarrow \varprojlim_{n,m} {}_{p^m}((M^\vee)_{G_n}) \longrightarrow 0 .$$

The cokernel obviously is isomorphic to $\mathrm{Hom}_{\mathbb{Z}_p}(M^\delta,\mathbb{Z}_p)$, while the kernel vanishes for $M = M^\delta$. On the other hand one has an exact sequence

$$0 \longrightarrow E^1(M/M^\delta) \longrightarrow E^1(M) \longrightarrow E^1(M^\delta) \longrightarrow 0 ,$$

because $(M^\delta)^+ = 0 = E^2(M/M^\delta)$ (cf. 3.1 d)). Since the first exact sequence is functorial in M , we conclude together that it must be isomorphic to the second one.

§ 4. Profinite groups of cohomological dimension two

4.1 We shall encounter the following situation for global as well as for local fields. Let $\mathcal{G}$ be a finitely generated profinite group with p-cohomological dimension $cd_p(\mathcal{G}) \leq 2$ for a fixed prime p. Let $\mathcal{H}$ be a closed normal subgroup and let $G = \mathcal{G}/\mathcal{H}$. We are interested in the structure of $X = \mathcal{H}(p)^{ab} = \mathcal{H}^{ab}(p)$ as a module over the completed group algebra $\Lambda = \mathbb{Z}_p[[G]]$, where $\mathcal{H}^{ab} = \mathcal{H}/[\mathcal{H},\mathcal{H}]$ is the maximal abelian and $\mathcal{H}(p)$ is the maximal pro-p quotient of a profinite group $\mathcal{H}$.

Let $\pi : \mathcal{F} \to \mathcal{G}$ be a surjection, where $\mathcal{F}$ is a free profinite group on finitely many generators $x_1,\dots,x_d$. We obtain a commutative exact diagram

(4.1.1)
$$\begin{tikzcd}
1 \arrow[r] & \mathcal{H} \arrow[r] & \mathcal{G} \arrow[r] & G \arrow[r] & 1 \\
1 \arrow[r] & \mathcal{R} \arrow[r] \arrow[u, two heads] & \mathcal{F} \arrow[r] \arrow[u, two heads, "\pi"'] & G \arrow[r] \arrow[u, equal] & 1 \\
 & \mathcal{N} \arrow[u, hook] \arrow[r, equal] & \mathcal{N} \arrow[u, hook] & &
\end{tikzcd}$$
,

and it follows easily with the methods of Fox and Lyndon that one has an exact sequence of Λ-modules

(4.1.2)
$$0 \longrightarrow \mathcal{R}(p)^{ab} \longrightarrow \Lambda^d \longrightarrow \Lambda \xrightarrow{aug} \mathbb{Z}_p \longrightarrow 0$$
$$e_i \longmapsto \bar{x}_i - 1$$

where aug is the usual augmentation, $\{e_i\}_{i=1}^{d}$ is a basis of Λ^d, and $\bar{x}_i$ is the image of x_i in $G \subset \Lambda$ (cf. [W1] for the case of a finite p-group).

In [NQD] Nguyen-Quang-Do has (for pro-p-groups) defined a canonical Λ-module Y which is very useful for our purposes:

4.2 Definition. Let $Y = I(G)_H$, where $I(G)$ is the augmentation ideal of $\mathbb{Z}_p[[G]] = \Lambda(G)$.

4.3 Lemma (cf. [NQD] 1.7) a) There is a commutative exact diagram of Λ-modules

$$\begin{tikzcd}
 & & & 0 & 0 & \\
 & & & I \arrow[u] \arrow[r, equal] & I \arrow[u] & \\
0 \arrow[r] & H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)^\vee \arrow[r] & N/[N,R](p) \arrow[r] & \Lambda^d \arrow[u] \arrow[r] & Y \arrow[u] \arrow[r] & 0 \\
0 \arrow[r] & H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)^\vee \arrow[r] \arrow[u, equal] & N/[N,R](p) \arrow[r] \arrow[u, equal] & R^{ab}(p) \arrow[u] \arrow[r] & X \arrow[u] \arrow[r] & 0 \\
 & & & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

where I is the augmentation ideal of Λ.

b) $N/[N/R](p)$ is a projective Λ-module.

Proof. a) follows as in [NQD] 1.7, by taking the H-homology of the two exact sequences

(4.3.1) $0 \longrightarrow I(G) \longrightarrow \mathbb{Z}_p[[G]] \longrightarrow \mathbb{Z}_p \longrightarrow 0$

(4.3.2) $0 \longrightarrow N^{ab}(p) \longrightarrow \mathbb{Z}_p[[G]]^d \longrightarrow I(G) \longrightarrow 0$

coming from the Lyndon resolution for $\mathcal{G}$ (cf. 4.1.2 for $G = \mathcal{G}$), noting that

$$H_1(H,\mathbb{Z}_p) = H^1(H,\mathbb{Q}_p/\mathbb{Z}_p)^\vee = H^{ab} ,$$

$$H_0(H,I(\mathcal{G})) = I(\mathcal{G})_H = Y ,$$

$$H_1(H,I(\mathcal{G})) = H_2(H,\mathbb{Z}_p) = H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)^\vee .$$

b): $N^{ab}(p)$ is a projective $\Lambda(\mathcal{G})$-module, since $cd_p(\mathcal{G}) \leq 2$, see [Br] 5.2. Hence $N^{ab}(p)_H = N/[N,R](p)$ is a projective Λ-module.

We now show how to determine X and Y in terms of the dualizing module of $\mathcal{G}$ (Strictly speaking, $E_2^{(p)}$ is only the dualizing module in the (most interesting) case $cd_p(\mathcal{G}) = 2$; for $cd_p(\mathcal{G}) = 1$ we have $E_2^{(p)} = 0$).

<u>4.5 Theorem</u>. Let $E_2^{(p)} = E_2^{(p)}(\mathcal{G}) = \varinjlim_{m,U} H^2(U,\mathbb{Z}/p^m)^*$ be defined as as in § 2, let $W = (E_2^{(p)})^H$ and $Z = W^\vee$, and assume that $N^{ab}(p)$ is a finitely generated $\Lambda(\mathcal{G})$-module.

a) One has $Y \simeq DZ$, in particular, Y is determined by Z up to projective summands.

b) Up to projective summands, X is determined by W and a class $\chi \in H^2(G,W)^* = H_2(G,Z) \cong [Y,I]$, via lemma 1.3 and the exact sequence

$$0 \longrightarrow X \longrightarrow Y \xrightarrow{f} I \longrightarrow 0$$

(χ corresponds to the homotopy class of f). As an alternative description, there is an exact sequence

$$0 \longrightarrow R(p)^{ab} \longrightarrow X \oplus \Lambda^d \longrightarrow Y \longrightarrow 0 ,$$

whose extension is the image of χ under the injection $[Y,I] \hookrightarrow \mathrm{Ext}^1_\Lambda(Y,R(p)^{ab})$.

c) Let $\chi_0 \in H^2(G,E_2^{(p)})^*$ be the canonical class: this is the class corresponding to the identity map under the canonical isomorphism (cf. [S1] I-8.1)

$$H^2(G,E_2^{(p)})^* \cong \mathrm{Hom}_G(E_2^{(p)},E_2^{(p)}) .$$

Then χ is the image of χ_0 under the map

$$H^2(G,E_2^{(p)})^* \longrightarrow H^2(G,W)^* ,$$

which is the transpose of the inflation.

d) The modules X and Y are determined up to isomorphism by the above invariants and the isomorphism class of $N/[N,R](p)$.

Proof. a) By the projectivity of $N^{ab}(p)$, 4.3.2 induces an exact sequence

$$(4.5.1) \quad (\Lambda(G)^d)^+ \longrightarrow (N^{ab}(p))^+ \longrightarrow E^1_G(I(G)) \longrightarrow 0 .$$

By assumption, $\mathbb{Z}_p$ is a noetherian $\Lambda(G)$-module (2.2), so by 4.3.1 and 2.1 b) we get

$$E^1_G(I(G)) \cong E^2_G(\mathbb{Z}_p) \cong (\varinjlim_m D_2(\mathbb{Z}/p^m))^\vee = (E_2^{(p)})^\vee ,$$

hence, by taking H-coinvariants, an exact sequence

$$(4.5.2) \quad (\Lambda^d)^+ \longrightarrow (N/[N,R](p))^+ \longrightarrow Z \longrightarrow 0 ,$$

where we have used the canonical isomorphisms

$$N^{ab}(p)_H \cong N/[N,R](p) \quad ,$$

$$(4.5.3) \qquad \mathrm{Hom}_{\Lambda(G)}(M,\Lambda(G))_H \cong \mathrm{Hom}_\Lambda(M_H,\Lambda) \quad ,$$

for every finitely generated $\Lambda(G)$-module M . The result now follows by comparing 4.5.2 with the exact sequence from 4.3 a)

$$N/[N/R](p) \longrightarrow \Lambda^d \longrightarrow Y \longrightarrow 0 \ .$$

b) The first isomorphism is clear since $Z = W^\vee$, and the second one is proved in lemma 4.6 b) below. Then the first claim immediately follows from 1.3. For the second claim note that the exact sequence

$$0 \longrightarrow R^{ab}(p) \longrightarrow \Lambda^d \longrightarrow I \longrightarrow 0$$

by 4.6 a) below induces an exact sequence

$$0 \longrightarrow [Y,I] \xrightarrow{\delta} \mathrm{Ext}^1_\Lambda(Y,R^{ab}(p)) \longrightarrow E^1(Y)^d \ .$$

Now by definition δ maps the class of f to the class of the pull-back extension

$$\begin{tikzcd}
0 \arrow[r] & R^{ab}(p) \arrow[r] & \Lambda^d \arrow[r] & I \arrow[r] & 0 \\
0 \arrow[r] & R^{ab}(p) \arrow[r] \arrow[u, equal] & X' \arrow[r] \arrow[u] & Y \arrow[r] \arrow[u] & 0 \\
& & X \arrow[u, hook] \arrow[r, phantom, "="] & X \arrow[u, hook] &
\end{tikzcd} \quad ,$$

22

and obviously $X' \cong X \oplus \Lambda^d$.

c) This follows from the functionality in 4.6 c) below: the above discussion is also valid for $G = G$, and the class of $f : Y \longrightarrow I$ is the image of the identity map under

$$[I(G),I(G)] \longrightarrow [I(G)_H,I(G)_H] \xrightarrow{f_*} [Y,I] .$$

It remains to show that the identity map corresponds to χ_0 via the isomorphism 4.6 b) for G and $M = E_G^2(\mathbb{Z}_p)$, via the identification $DM = DE_G^2(\mathbb{Z}_p) = DE_G^1(I(G)) = I(G)$. Looking at the diagram

$$\begin{array}{ccccccccccc} & & \Lambda(G)^+ & \longrightarrow & (\Lambda(G)^d)^+ & \longrightarrow & (N^{ab}(p))^+ & \longrightarrow & E_G^2(\mathbb{Z}_p) & \longrightarrow & 0 \\ & & \downarrow & & \| & & \| & & \| & & \\ 0 & \to & I(G)^+ & \longrightarrow & (\Lambda(G)^d)^+ & \longrightarrow & (N^{ab}(p))^+ & \longrightarrow & E_G^2(\mathbb{Z}_p) & \longrightarrow & 0 , \end{array}$$

with exact bottom row, one easily checks that both classes correspond to the class of the natural inclusion $I(G) \hookrightarrow \Lambda(G)$ in $H_2(G,E_G^2(\mathbb{Z}_p)) = \mathrm{Ker}((I(G)^+)_G \longrightarrow ((\Lambda(G)^d)^+)_G)$.

d) has only to be shown for Y , by (the proof of) 1.3 and the Krull-Schmidt theorem for Λ . For Y it suffices to show the following: if

$$\Lambda^d \xrightarrow{g} P \longrightarrow Z \longrightarrow 0$$

$$\Lambda^d \xrightarrow{h} Q \longrightarrow Z \longrightarrow 0$$

are two exact sequences of Λ-modules. with finitely generated projectives P and Q , then $P \cong Q$ implies

$$\mathrm{Coker}(P^+ \xrightarrow{g^+} (\Lambda^d)^+) \cong \mathrm{Coker}(Q^+ \xrightarrow{h^+} (\Lambda^d)^+) .$$

This easily follows with the same techniques as in the proof of 1.3, together with the Krull-Schmidt theorem.

4.6 Lemma. a) Let $0 \longrightarrow R \xrightarrow{\alpha} P \xrightarrow{\beta} N \longrightarrow 0$ be an exact sequence of Λ-modules, with P finitely generated projective, and let M be another finitely generated Λ-module. In the long exact Ext-sequence

$$\mathrm{Hom}_\Lambda(M,P) \xrightarrow{\beta_*} \mathrm{Hom}_\Lambda(M,N) \longrightarrow \mathrm{Ext}^1_\Lambda(M,R) \xrightarrow{\alpha_*} \mathrm{Ext}^1_\Lambda(M,P)$$

one has $\mathrm{Ker}\ \alpha_* \cong \mathrm{Coker}\ \beta_* \cong [M,N]$.

b) Let M be a finitely presented $\Lambda = \Lambda(G)$ - module, then there is a canonical, functorial isomorphism

$$H_2(G,M) \cong [DM,I] .$$

c) This isomorphism is functorial in G , in the following sense: if H is a closed normal subgroup of G , then the diagram

$$\begin{array}{ccc} H_2(G,M) & \xrightarrow{\sim} & [DM,I(G)] \\ \Big\downarrow & & \Big\downarrow \\ & & [(DM)_H, I(G)_H] \\ \Big\downarrow & & \Big\downarrow \\ H_2(G/H,M_H) & \xrightarrow{\sim} & [D(M_H),I(G/H)] \end{array}$$

is commutative, where the left arrow is the deflation and the right arrows are obtained by the obvious functoriality of [,], the canonical identification $(DM)_H \simeq D(M_H)$, and the map $I(G)_H \longrightarrow I(G/H)$.

Proof. a) Obviously for $f : M \longrightarrow N$ one has $f \in \operatorname{Im} \beta_* \Rightarrow f \sim 0$. For the converse implication note that every map $Q \longrightarrow N$, with Q projective, factorizes through β .

b) Choose an exact sequence (of right Λ-modules, say)

$$0 \longrightarrow N \xrightarrow{\iota} F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0 ,$$

with finitely generated free modules F_0, F_1 , so that DM is defined by exactness of

$$F_0^+ \longrightarrow F_1^+ \longrightarrow DM \longrightarrow 0 .$$

Then we have a canonical isomorphism $N \cong (DM)^+$, by the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d] & F_1 \arrow[r] \arrow[d, "\phi_{F_1}"] & F_0 \arrow[d, "\phi_{F_0}"] \\ 0 \arrow[r] & DM^+ \arrow[r] & F_1^{++} \arrow[r] & F_0^{++} \end{tikzcd} .$$

On the other hand we have

$$H_2(G,M) \cong \operatorname{Ker}(N_G \longrightarrow (F_1)_G) \cong \iota^{-1}(F_1 I)/NI .$$

Now it is readily checked that

$$F_1 I \cong F_1^{++} I = \operatorname{Hom}_\Lambda(F_1^+,\Lambda) I \cong \operatorname{Hom}_\Lambda(F_1^+, I) ,$$

and so we may identify

$$\iota^{-1}(F_1 I) \cong \operatorname{Hom}_\Lambda(DM, I) \subseteq \operatorname{Hom}_\Lambda(DM,\Lambda) .$$

On the other hand the exact sequence

$$\begin{array}{ccccccc}
\mathrm{Hom}_\Lambda(DM,\Lambda^d) & \longrightarrow & \mathrm{Hom}_\Lambda(DM,I) & \longrightarrow & [DM,I] & \longrightarrow & 0 \\
\| & & \cap| & & & & \\
\mathrm{Hom}_\Lambda(DM,\Lambda)^d & \longrightarrow & \mathrm{Hom}_\Lambda(DM,\Lambda) & & & & \\
(h_1,\ldots,h_d) & \longmapsto & \sum_{i=1}^{d} h_i(\bar{x}_i-1) & & & &
\end{array}$$

coming from a) and 4.1.2 shows

$$NI = \mathrm{Hom}_\Lambda(DM,\Lambda)I = \{f \in \mathrm{Hom}_\Lambda(DM,I)\,|\,f \sim 0\} .$$

Together we obtain the result, the functoriality in M being clear by the existence of compatible resolutions.

c) The deflation being the canonical extension of the isomorphism

$$H_0(G,M) = M_G \cong (M_H)_{G/H} = H_0(G/H,M_H)$$

to the higher homology groups, this follows immediately by going through the steps of the above construction. The identification $(DM)_H \simeq D(M_H)$ is deduced from formula 4.5.3.

<u>4.7 Remarks</u>. a) Obviously, 4.6 a) holds for any ring Λ , while 4.6 b) and c) remain true for any profinite group G with finitely many topological generators. More generally, one can show isomorphisms

$$[D\mathbb{Z}_p,\Omega^i M] \cong H_{i+1}(G,M),\ i \geq 0 ,$$

under the assumption that $\Omega^i M$ is finitely generated. This implies 4.6 b) by an isomorphism $[D\mathbb{Z}_p,\Omega M] \cong [DM,I]$, which for finitely

26

generated $R^{ab}(p)$ coincides with

$$[D\mathbb{Z}_p,\Omega M] \cong [\Sigma D\mathbb{Z}_p,M] \cong [D\Omega\mathbb{Z}_p,M] \cong [DM,\Omega\mathbb{Z}_p] \ .$$

b) From 4.5.2 and 4.3 we obtain an isomorphism

$$Z^+ \cong H^2(H,\mathbb{Q}_p/\mathbb{Z}_p)^\vee \ .$$

c) Assume that $H^2(H,\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Then $\mathrm{pd}_\Lambda(Y) \leq 1$, and we can compare 4.5 with the general method 1.9 b) as follows: Choosing a surjection $P \twoheadrightarrow R^{ab}(p)$ with P projective we get a commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & N/[N,R](p) \arrow[r] & R^{ab}(p) \arrow[r] & X \arrow[r] & 0 & \\
 & & P \arrow[u, two heads] \arrow[r, phantom, "="] & P \arrow[u, two heads] & & \\
 & 0 \arrow[r] & \Omega R^{ab}(p) \arrow[r] \arrow[u, hook] & \Omega X \arrow[r] \arrow[u, hook] & N/[N,R](p) \arrow[r] & 0 \ ,
\end{tikzcd}$$

i.e., $\Omega X \simeq \Omega R^{ab}(p) \simeq \Omega^2 I$. Furthermore we have morphisms

$$\mathrm{Ext}^1_\Lambda(D\Sigma\Omega X,E^1(X)) \cong \mathrm{Ext}^1_\Lambda(D\Sigma\Omega^2 I,\ E^1(X))$$

$$\xrightarrow{\alpha}\!\!> [\Omega D\Sigma\Omega^2 I,E^1(X)] \cong [\Omega^2\Sigma^2 DI,E^1(X)] \xrightarrow{\beta} [DI,E^1(X)] \ ,$$

with α induced by the Ext-sequence for

$$0 \longrightarrow \Omega D\Sigma\Omega^2 I \longrightarrow Q \longrightarrow D\Sigma\Omega^2 I \longrightarrow 0$$

(Q projective), and β by the adjunction of Ω and Σ . One easily checks that under the composition ψ_X (from 1.9 b)) is mapped to the same class as $\chi = \chi(X)$ (from 4.5 b)) under

$$[Y,I] \cong [DI,DY] = [DI,E^1(Y)] \xrightarrow{\gamma} [DI,E^1(X)] \ .$$

If $E^1(R^{ab}(p)) \cong E^2(I) \cong E^3(\mathbb{Z}_p)$ vanishes, then $\Sigma\Omega R^{ab}(p) \simeq R^{ab}(p)$ by 1.10 and thus α is an isomorphism. If both $E^3(\mathbb{Z}_p)$ and $E^1(I) \cong E^2(\mathbb{Z}_p)$ vanish (e.g., if G is virtually strict p-Cohen-Macaulay with $vcd_p(G) = n \neq 2,3$) , then $\Sigma^2\Omega^2 I \simeq I$ and so β is an isomorphism, and γ is an isomorphism by the exact sequence from 4.3

$$E^1(I) \longrightarrow E^1(Y) \longrightarrow E^1(X) \longrightarrow E^2(I) \ .$$

§ 5 Applications to number theory

We apply the results of the previous section to the following number theoretic situation. Fix a prime p and let k be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. In the case of a p-adic field let Ω/k be a p-closed Galois extension, i.e., an extension which has no non-trivial p-extension. For a global field k let S be a finite set of places containing those obove $p \cdot \infty$, and let Ω/k be a (p, S) - closed Galois extension, i.e., Ω/k is unramified outside S (S - ramified) and Ω has no non-trivial S - ramified p-extension. Let K/k be a Galois subextension and set $\mathcal{G} = \mathrm{Gal}(\Omega/k)$, $\mathcal{H} = \mathrm{Gal}(\Omega/K)$, and $G = \mathrm{Gal}(K/k)$. For any field L denote by $\mu_L(p)$ the group of p-power roots of unity.

As in § 4, we want to study the $\Lambda = \Lambda(G)$ - module $X = \mathcal{H}^{ab}(p)$.

<u>5.1. Theorem</u> Let k be a finite extension of $\mathbb{Q}_p$, $n = [k : \mathbb{Q}_p]$.

a) There is an isomorphism of Λ-modules

$$X = \varprojlim_{L} A(L) ,$$

where L runs over all finite extensions L/k, $L \subseteq \Omega$, and $A(L) = \varprojlim_{m} L^{\times}/(L^{\times})^{p^m}$ is the p-completion of $L^{\times}$.

b) One has $cd_p(G) \leq 2$, $H^2(H, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, and an isomorphism of G-modules

$$E_2^{(p)}(G) \cong \mu_\Omega(p) .$$

c) G is generated by $d = n+2$ elements as a profinite group. Let $F \xrightarrow{\pi} G$, N , R , Y etc. be as in § 4, then

$$N^{ab}(p) \cong \mathbb{Z}_p[[G]] .$$

d) Let $\sigma_1, \dots, \sigma_{n+2}$ be topological generators of G , and let $a_i \in \mathbb{Z}_p$ with $\sigma_i(\zeta) = \zeta^{a_i}$ for all $\zeta \in \mu_K(p)$, $i = 1, \dots, n+2$. Then there is an exact sequence

$$\text{(5.1.1)} \qquad \begin{array}{c} 0 \longrightarrow \Lambda \longrightarrow \Lambda^{n+2} \longrightarrow Y \longrightarrow 0 \\ 1 \longmapsto (\sigma_1 - a_1, \dots, \sigma_{n+2} - a_n) . \end{array}$$

e) X is determined up to isomorphism by $\mu_K(p)$ and the image of $H^2(G, \mu_\Omega(p))^* \xrightarrow{\inf^*} H^2(G, \mu_K(p))^*$.

Proof

a) is clear from class field theory.

b) If A is a p-torsion G-module , then the inflation

(5.1.2) $$H(G\,,A) \xrightarrow[\sim]{\inf} H(k\,,A)$$

is an isomorphism for all $r \geq 0$, since $cd_p(\mathrm{Gal}(\bar{k}/\Omega)) \leq 1$ for an algebraic closure $\bar{k}$ of k (same argument as in [S1] II 5.6). The first two claims thus follow from the fact that $scd_p(\mathrm{Gal}(\bar{k}/k)) = 2$ (loc. cit. 5.3). Applying 5.1.2 to a finite extension L/k , $L \subseteq \Omega$, we get an isomorphism

$$H^2(\mathrm{Gal}(\Omega/L)\,,\mathbb{Z}/p^m)^* \cong H^2(L\,,\mathbb{Z}/p^m) \cong \mu_{L,p^m} \quad ,$$

with the group of p^m-th roots of unity in L , by Tate's local duality theorem (loc. cit. 5.2). By passing to the limit over m and L we obtain the last claim.

c) This follows from [J1] 3.1 and 3.2. Note that it suffices to prove $N/[N\,,R](p) \cong \mathbb{Z}_p[G]$ in the case of finite G , since two pseudocompact $\mathbb{Z}_p[[G]]$ - modules M and M' , with M finitely generated, are isomorphic if $M_H \cong M'_H$ for every open normal subgroup H of G (use that an inverse limit of non-emty compact sets is non-empty). By Swan's theorem (see [S3] 16.1 Cor. 2) and the projectivity of $N^{ab}(p)$ it suffices to show the above isomorphism after tensoring with $\mathbb{Q}_p$,which follows from [J1] 3.1 and 4.3 above, together with the vanishing of $H^2(H\,,\mathbb{Q}_p/\mathbb{Z}_p)$.

d) With the notations of § 4 we have $W = \mu_K(p)$ and $Z = \mu_K(p)^\vee$. Since $Y \simeq DZ$ and $H^2(H\,,\mathbb{Q}_p/\mathbb{Z}_p) = 0$, we immediately get 5.1.1 from transposing the exact sequence

$$\Lambda^{n+2} \longrightarrow \Lambda \xrightarrow{\rho} \mu_K(p)^\vee \longrightarrow 0$$

(5.1.3)

$$e_i \longmapsto \sigma_i - a_i^{-1}$$

where $\{e_i\}_{i=1}^{n+2}$ is a basis of Λ^{n+2} and ρ sends 1 to a generator of $\mu_K(p)^\vee$ (given the <u>left</u> action of G), once we have shown that $(\mu_K(p)^\vee)^+ = 0$. This is clear, because $(\mu_K(p)^\vee)_U$ is finite for every open normal subgroup U of G.

e) This is clear from 4.5 b) and d), since χ_o generates the pro-cyclic group $H^2(G, \mu_\Omega(p))^* \cong \mathrm{End}(\mu_\Omega(p))$ and any two generators differ by multiplication with an element $a \in \mathbb{Z}_p^\times$.

5.2. Examples

a) If G is finite cyclic, then there is a commutative diagram

$$\begin{array}{ccccc} H^2(G, \mu_K(p)) & \xrightarrow{\mathrm{inf}} & H^2(G, \mu_\Omega(p)) & \subseteq & H^2(G, \Omega^\times) \\ \| \wr & & & & \cup\mid \mathrm{inf} \\ \hat{H}^o(G, \mu_K(p)) & \longrightarrow & \hat{H}^o(G, K^\times) & \cong & H^2(G, K^\times) \end{array},$$

so the Galois module $A(K)$ is determined by the order of the group $\mu_K(p) \cap N_{K/k}(K^\times)$, and one easily reobtains the results in [Ger].

b) If $cd_p(G) \leq 1$, then I is projective (cf. [Br] 5.1), hence $Y \cong X \oplus I$, and in particular, $X \simeq D(\mu_K(p)^\vee)$ has projective dimension ≤ 1 and is determined by $E^1(X) \cong \mu_K(p)^\vee$. For example, assume that $G \cong \mathbb{Z}_p \times \Delta$ with a finite group Δ, $p \nmid (\Delta : 1)$, then with 2.6 we obtain the following. If $\mu_K(p)$ is infinite, then

$$X \cong \Lambda^n \oplus \mathbb{Z}_p(1) ,$$

and if $\mu_K(p)$ is finite, then X is determined by an exact sequence

$$0 \longrightarrow X \longrightarrow \Lambda^n \longrightarrow \mu_K(p) \longrightarrow 0 .$$

(Note that $E^2(X) = 0$ and $E^1(X) \cong E^2(\mu_K(p)) \cong \mu_K(p)^\vee$ in the last case). This regives results of Iwasawa [Iw] theorem 21 and Dummit [Du], cf. also [J1] 4.3.

c) If G has an open subgroup $U \cong \mathbb{Z}_p^2$, with $p \nmid (G : U)$, and if $\mu_K(p)$ is infinite, then $H^2(G, \mu_K(p))^* \cong \mathrm{Hom}_G(\mu_K(p), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, and one easily shows $R^{ab}(p) \cong \Lambda^{d-1}$. Thus

$$X \oplus \Lambda \cong Y$$

by the second description of 4.5 b). For example, if $G \cong \mathbb{Z}_p^2$, then $X \cong M' \oplus \Lambda^{n-1}$, where M' is given by the exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \Lambda^2 \longrightarrow M' \longrightarrow 0$$

$$1 \longmapsto (\sigma - \chi(\sigma) \ , \ \tau - \chi(\tau))$$

with σ , τ generators of G and $\chi : G \longrightarrow \mathbb{Z}_p^\times$ the cyclotomic character.

d) If G is a p-adic Lie group, then the methods of [S2] show that $H^2(G, \mu_K(p))$ is always finite. Hence there is always an injection

$$X \oplus \Lambda^d \hookrightarrow R^{ab}(p) \oplus Y$$

with cokernel of finite exponent.

Now let k be a finite extension of $\mathbb{Q}$, and let Ω be as above. Let k_S be the maximal S-ramified extension of k , and set $G_S = \mathrm{Gal}(k_S/k)$, $H_S = \mathrm{Gal}(k_S/K)$. Then $X = X_S = H^{ab}(p)$ $= H_S^{ab}(p)$ is the Galois group over K of the maximal abelian S-ramified pro-p-extension of K .

5.3. Lemma

a) If $p \neq 2$ or if $p = 2$ and k is totally imaginary, then $cd_p(G) \leq 2$.

b) If an open subgroup of G is a pro-p-group , then G is finitely generated as a profinite group.

Proof

a) For a p-torsion G-module A the inflation

(5.3.1) $$H^r(G\,,A) \xrightarrow{\inf} H^r(G_S\,,A)$$

is an isomorphism for all $r \geq 0$, and this implies the claim (see [Neu]).

b) This follows, e.g., from [J1] 3.2 b).

In the following we shall assume that $cd_p(G) \leq 2$ and that G has finitely many topological generators. Let - for a suitable d - F , R and N be chosen as in § 4, and let $Y = Y_S = I(G)_H$ as in 4.2. It is easy to see that $Y \cong I(G_S)_{H_S}$, in particular this Λ-module only depends on K and S , and by 4.3 we have a diagram of Λ-modules

(5.4.1)
$$\begin{tikzcd}
 & & & I \arrow[r, equal] & I \\
0 \arrow[r] & H_2(H_S, \mathbb{Z}_p) \arrow[r] & N/[N,R](p) \arrow[r] & \Lambda^d \arrow[r] \arrow[u, two heads] & Y_S \arrow[r] \arrow[u, two heads] & 0 \\
0 \arrow[r] & H_2(H_S, \mathbb{Z}_p) \arrow[r] \arrow[u, equal] & N/[N,R](p) \arrow[r] \arrow[u, equal] & R^{ab}(p) \arrow[r] \arrow[u, hook] & X_S \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$
,

since $H_2(H_S, \mathbb{Z}_p) = H^2(H_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong H^2(H, \mathbb{Q}_p/\mathbb{Z}_p)$ by the argument of 5.3 a). Here I and $R^{ab}(p)$ only depend on the structure of G as an abstract group and X_S and Y_S on the invariants described in theorem 4.5. It is conjectured that $H^2(H_S, \mathbb{Q}_p/\mathbb{Z}_p)$ vanishes; for a finite extension K/k this is equivalent to the Leopoldt conjecture for K and p (compare 5.4 a) below), on the other hand this vanishing is known, if K contains the cyclotomic $\mathbb{Z}_p$-extension of k (cf. [Sch] 4.7).

Let $X_2 = \mathrm{Gal}(L/K)$ and $X_3 = \mathrm{Gal}(L'/K)$ where L is the maximal abelian unramified pro-p-extension of K and L'/K is the maximal subextension in which every prime above S is completely decomposed. For K/k finite let $S_f(K)$ be the set of finite primes in K lying above S, and for $\mathfrak{P} \in S_f(K)$ let $K_\mathfrak{P}$ be the completion of K at $\mathfrak{P}$. Then define

$$A = A_S = \prod_{\mathfrak{P}\in S_f(K)} A_\mathfrak{P} \quad ,$$

$$U = U_S = \prod_{\mathfrak{P}\in S_f(K)} U_\mathfrak{P} \quad ,$$

where $A_\mathfrak{P}$ (resp. $U_\mathfrak{P}$) is the p-complection of $K_\mathfrak{P}^\times$ (resp. of the group of units in $K_\mathfrak{P}$). Let $\mathcal{O}_K$ (resp. $\mathcal{O}_S$) be the ring of integers (resp. S-integers) in K and set

$$E = E_K = \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad ,$$

$$E_S = E_{S,K} = \mathcal{O}_S^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad .$$

For arbitrary K/k define the groups $A_{\mathfrak{p}}$, $U_{\mathfrak{p}}$, A, U, E and E_S as the inverse limits - via the norms - of the above groups for all finite intermediate layers L/k, $L \leq K$.

The next theorem extends results of Kuz'min [Kuz], Nguyen-Quang-Do [NQD] and the author [J1].

5.4. Theorem

a) With the notations as above, there is a commutative exact diagram of Λ-modules

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & H^2(\mathcal{H}_S,\mathbb{Q}_p/\mathbb{Z}_p)^{\vee} & \longrightarrow & E & \longrightarrow & U_S & \longrightarrow & X_S & \longrightarrow & X_2 & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & H^2(\mathcal{H}_S,\mathbb{Q}_p/\mathbb{Z}_p)^{\vee} & \longrightarrow & E_S & \longrightarrow & A_S & \longrightarrow & X_S & \longrightarrow & X_3 & \longrightarrow & 0 .
\end{array}$$

b) If $d \geq r_1' + r_2 + 1$, there is an isomorphism

$$\mathcal{N}/[\mathcal{N}, R](p) \cong \bigoplus_{v \in S_\infty'} \Lambda_{(G_v)} \oplus \Lambda^{d-r_1'-r_2-1} .$$

Here 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. For each $v \in S_\infty'$, $G_v = \langle\sigma_v\rangle$ is a chosen decomposition group at v in G, and $\Lambda_{(G_v)} = \Lambda/\Lambda(\sigma_v - 1)$ is the module of coinvariants for the right

G_v-module structure of Λ , regarded as a left Λ-module.

c) Let $E_2^{(p)}(G)$ be the dualizing module of G . If $\mu_p \subseteq \Omega$, then there is an exact sequence

$$0 \longrightarrow \mu(p) \xrightarrow{\iota} \bigoplus_{\mathfrak{p}\in S_f} \mathrm{Ind}_{G_{\mathfrak{p}}}^{G}(\mu(p)) \longrightarrow E_2^{(p)}(G) \longrightarrow 0$$

where, for each $\mathfrak{p} \in S_f = S_f(k)$, $G_{\mathfrak{p}}$ is a decomposition group at $\mathfrak{p}$ in G , $\mathrm{Ind}_{G_{\mathfrak{p}}}^{G}$ means induction from $G_{\mathfrak{p}}$ to G , $\mu(p)$ is the G-module of p-power roots of unity in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, and ι is the natural map.

d) Let $W = W_S = E_2^{(p)}(G)^{H}$ and $Z = Z_S = W_S^{\vee}$ as in § 4 - so that $Y_S \simeq DZ_S$ by 4.5 a). Then $W_S \cong E_2^{(p)}(G_S)^{H_S}$, in particular, W_S and Z_S only depend on K and S . There is an exact sequence

$$0 \longrightarrow \mu_K(p) \longrightarrow \bigoplus_{\mathfrak{p}\in S_f} \mathrm{Ind}_{G_{\mathfrak{p}}}^{G}(\mu_{K_{\mathfrak{p}}}(p)) \longrightarrow W_S \longrightarrow H^1(H_S,\mu(p)) \xrightarrow{\mathrm{res}} \bigoplus_{\mathfrak{p}\in S_f} H^1(K_{\mathfrak{p}},\mu(p)) ,$$

where, for each $\mathfrak{p} \in S_f$, $G_{\mathfrak{p}}$ is the image of $G_{\mathfrak{p}}$ in G , $K_{\mathfrak{p}}$ is the completion of K at the prime $\mathfrak{P}/\mathfrak{p}$ belonging to $G_{\mathfrak{p}}$, and res is induced by $H^2(H_S, \mu(p)) \xrightarrow{\mathrm{inf}} H^2(K, \mu(p)) \longrightarrow H^1(K_{\mathfrak{p}}, \mu(p))$. In particular, if $\mu_K(p)$ is infinite, then there is an exact sequence

$$0 \longrightarrow X_3(-1) \longrightarrow Z_S \longrightarrow \bigoplus_{\mathfrak{p}\in S_f} \Lambda \otimes_{\Lambda(G_{\mathfrak{p}})} \mathbb{Z}_p(-1) \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0 ,$$

where $\mathbb{Z}_p(1) = \varprojlim_m \mu_{p^m}$, and $X_3(-1) = X_3 \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1)$ for $\mathbb{Z}_p(-1) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1), \mathbb{Z}_p)$ is the usual Tate twist of X_3 .

<u>Proof</u>

a) This is clear from the cited references; we only remark that for K/k finite the lower sequence by Kummer theory can be identified with the exact sequence

$$0 \longrightarrow H^2(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow H^1(\mathcal{H}_S, \mathbb{Z}_p(1)) \longrightarrow \bigoplus_{\mathfrak{p}\in S_f(K)} H^1(K_{\mathfrak{p}}, \mathbb{Z}_p(1))$$

(5.4.2)

$$\longrightarrow H^1(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \longrightarrow \mathrm{Gal}(L'/K) \longrightarrow 0$$

coming from Tate's duality theorem ([Ta] 3.1, compare [Sch] 2.5) and the fact that $H^2(K_{\mathfrak{p}}, \mathbb{Q}/\mathbb{Z}_p) = 0$; here $H^1(-, \mathbb{Z}_p(1)) = \varprojlim H^1(-, \mu_{p^m})$. The upper sequence is an easy consequence by class field theory, and the general case follows by passing to the limit over the intermediate finite layers, since this limit for $H^2(\mathcal{H}_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$ is taken via the duals of the restriction maps (cf. [Mi] I 4.19).

b) We already know that $N/[N, R](p)$ is a projective Λ-module, and for its description it suffices to consider the case of finite G (same argument as for 5.1 c)). For finite G the claim follows with the arguments in [J1] 3.3: By Swan's theorem it suffices to consider $N/[N, R](p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. From a) we get the equality

$$[N/[N,R](p) \otimes \mathbb{Q}_p] = [R^{ab}(p) \otimes \mathbb{Q}] + [H^2(H_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \otimes \mathbb{Q}_p] - [X_S \otimes \mathbb{Q}_p]$$

in the Grothendieck group $K_o(\mathbb{Q}_p[G])$ of finitely generated $\mathbb{Q}_p[G]$-modules, $[A]$ denoting the class of such a module A. From a) we have

$$[X_S \otimes \mathbb{Q}_p] - [H^2(H_S, \mathbb{Q}_p/\mathbb{Z}_p)^\vee] = [U \otimes \mathbb{Q}_p] - [E \otimes \mathbb{Q}_p] ,$$

and we may proceed as in [J1].

c) From Tate's duality theorem we get an exact sequence for finite K/k, $K \subseteq k_S$:

$$(5.4.3) \qquad \begin{aligned} 0 \longrightarrow \mu_K(p) \longrightarrow \bigoplus_{\mathfrak{p} \in S_f(K)} \mu_{K_\mathfrak{p}}(p) \longrightarrow H^2(H_S, \mathbb{Z}_p)^\vee \\ \longrightarrow H^1(H_S, \mu(p)) \longrightarrow \bigoplus_{\mathfrak{p} \in S_f(K)} H^1(K_\mathfrak{p}, \mu(p)) . \end{aligned}$$

By passing to the direct limit over all finite layers K/k contained in Ω/k we obtain the result, since for $H^2(H_S, \mathbb{Z}_p)^\vee = \varinjlim_m H^2(H_S, \mathbb{Z}/p^m)^\vee = \varinjlim_m H^2(H, \mathbb{Z}/p^m)^\vee$ the limit is taken via the duals of the corestrictions, while for $H^1(H_S, \mu(p)) \cong H^1(H, \mu(p))$ and the last group it is taken via the restrictions.

The first exact sequence in d) now follows either by only passing to the limit over all finite layers in K/k, or by taking the H_S-cohomology of a similar sequence for $E_2^{(p)}(G_S)$ as the one for $E_2^{(p)}(G)$ in c). The second sequence is obtained by taking the Pontrjagin dual of the first one. Finally we immediatly obtain $E_2^{(p)}(G) \cong E_2^{(p)}(G_S)^{\mathrm{Gal}(k_S/\Omega)}$ from 5.3.1.

5.5. Examples (valid for the global and the local case)

a) If $G \cong \mathbb{Z}_p$, it is well-known that $I(G) \cong \Lambda$. Hence $Y \cong X \oplus \Lambda$, and in particular, $X \simeq DZ$ is completely determined by Z (compare [J1] p. 123, 124, where this was proved under too restrictive assumptions - and where the $\mathbb{Z}_p(1)$'s in (43) have to be replaced by $\mathbb{Z}_p(-1)$'s). A similar discussion holds for $cd_p(G) \leq 1$ (cf. 5.2 b)).

b) Assume that $H^2(H, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. If $cd_p(G) \leq 3$, then $pd_\Lambda(X) \leq 1$ (since $pd_\Lambda(R^{ab}(p)) \leq 1$, cf. [Br] 4.4, and hence $0 \simeq \Omega R^{ab}(p) \simeq \Omega X$, cf. 4.7 c)). Thus $X \simeq DE^1(X)$ by theorem 1.6, and by the arguments in 4.5 d) X is determined up to isomorphism by $E^1(X)$. By 4.3 we have an exact sequence

$$\begin{array}{ccccccccc}
E^1(I) & \longrightarrow & E^1(Y) & \longrightarrow & E^1(X) & \longrightarrow & E^2(I) & \longrightarrow & 0 \\
\wr\| & & \wr\| & & & & \wr\| & & \\
E^2(\mathbb{Z}_p) & & Z & & & & E^3(\mathbb{Z}_p) & &
\end{array}$$

If $cd_p(G) = 2$, then $E^1(X)$ is the cokernel of $E_2^{(p)}(G)^\vee = E^2(\mathbb{Z}_p) \longrightarrow Z$, and, in fact this map is just the element

$\chi \in H^2(G, W)^\vee \cong \mathrm{Hom}_G(W, E_2^{(p)}(G)) \cong \mathrm{Hom}_G(E^2(\mathbb{Z}_p), Z)$. For example, if $G \cong \mathbb{Z}_p^2$, then $E^2(\mathbb{Z}_p) \cong \mathbb{Z}_p$, and the map corresponds to an element in $Z^G \cong \mathrm{Hom}_G(W, \mathbb{Q}_p/\mathbb{Z}_p)$. If k is global and $\mu_K(p)$ is infinite, then the second exact sequence in 5.4 d) shows $Z^G \cong X_3(-1)^G$.

If $cd_p(G) = 3$ and G is strict p-Cohen-Macaulay, then we obtain an exact sequence

$$0 \longrightarrow Z \longrightarrow E^1(X) \longrightarrow E^3(\mathbb{Z}_p) \longrightarrow 0 ,$$

whose extension class now is given by the element $\chi \in H^2(G, W)^\vee \cong H^1_{cont}(G, \mathrm{Hom}(W, E_3^{(P)}(G))) \cong H^1_{cont}(G, \mathrm{Hom}(E^3(\mathbb{Z}_p), Z))$.

c) The invariant $\chi \in H^2(G, W)^\vee$ is zero if and only if every p-embedding problem is solvable for K/k and $\mathcal{G}$, i.e., if every diagram with exact row

$$\begin{array}{ccccccccc} & & & & & & \mathcal{G} & & \\ & & & & & & \downarrow{\scriptstyle \pi} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\rho} & G & \longrightarrow & 1 , \end{array}$$

with finite abelian p-group A , can be completed by a homomorphism $s : \mathcal{G} \longrightarrow E$ with $\rho s = \pi$. This follows with the injection

$$H^2(G\,,A) \hookrightarrow \prod_{\mu\in \mathrm{Hom}_G(A,E_2^{(p)})} H^2(G\,,E_2^{(p)})\ ,$$

with the same arguments as in [JW].

5.6. Remark In this and the following section it is convenient to give all modules the left Galois module structures. In view of the discussion in 2.7 b) this means that $C^\vee = \mathrm{Hom}_{\mathrm{cont}}(C,\mathbb{Q}_p/\mathbb{Z}_p)$, $\mathrm{Hom}_{\mathbb{Z}_p}(C\,,D)$ etc. have the action given by $(\sigma f)(c) = \sigma f(\sigma^{-1}c)$, only then Tate's sequences 5.4.2, 5.4.3 are Galois equivarient. In particular, the action on the Iwasawa adjoint $E^1(X)$ is the one of [W2] and different from the one in [Iw].

§ 6. Some results for the cyclotomic $\mathbb{Z}_p$-extensions

We consider a situation as in the previous section, with k a global field and $K = k(\mu(p))$. Since there are only finitely many primes in K over every prime of k , the sequence of 5.4 d) becomes

$$(6.1) \qquad 0 \longrightarrow X_3(-1) \xrightarrow{\alpha_1} Z_S \xrightarrow{\alpha_2} \bigoplus_{\mathfrak{p}\in S_f} \mathrm{Ind}_{G_\mathfrak{p}}^{G}(\mathbb{Z}_p(-1)) \xrightarrow{\alpha_3} \mathbb{Z}_p'(-1) \longrightarrow 0 .$$

The following result was proved by K. Wingberg in [W2] up to quasi-isomorphisms.

6.2 Theorem. The sequence 6.1 can be identified with an exact sequence

$$0 \longrightarrow X_3(-1) \longrightarrow E^1(X_S) \longrightarrow E^1(A) \longrightarrow E^1(E_S) \longrightarrow 0$$

induced from the exact sequence

$$0 \longrightarrow E_S \longrightarrow A \longrightarrow X_S \longrightarrow X_3 \longrightarrow 0 .$$

Proof. Splitting the latter sequence into two short ones

$$0 \longrightarrow E_S \longrightarrow A \longrightarrow B \longrightarrow 0$$

$$0 \longrightarrow B \longrightarrow X_S \longrightarrow X_3 \longrightarrow 0 ,$$

we get a commutative exact diagram

II

$$
\begin{tikzcd}
E^1(X_3) \arrow[r] & E^1(X_S) \arrow[r] \arrow[d, equal] & E^1(B) \arrow[r] \arrow[d, dash] & E^2(X_3) \\
& E^1(X_S) \arrow[r, "\beta"] & E^1(A) \arrow[d] & \\
& & E^1(E_S) \arrow[d] & \\
& & 0 &
\end{tikzcd}
\tag{6.2.1}
$$

where we have used that $E^2(B)$ vanishes as quotient of $E^2(X_S) = 0$. Now by the considerations in 4.5 and example 5.5 a), β can be identified with the map α_2 in 6.1. On the other hand, by the well-known local theory (compare 5.2 b)) we have

$$A \cong T_1(A) \oplus \Lambda^{[k:\mathbb{Q}]} ,$$

$$T_1(A) \cong \bigoplus_{\mathfrak{p} \in S_f} \mathrm{Ind}_{G_{\mathfrak{p}}}^{G} (\mathbb{Z}_p(1)) .$$

Hence we get a commutative diagram

$$
\begin{tikzcd}
& & \mathrm{Coker}\,\beta \arrow[r] \arrow[d, two heads, "5.2.1"] & 0 \\
E^1(X_S) \arrow[r, "\beta"] \arrow[dddd, "\wr"] & E^1(A) \arrow[ur] \arrow[r] \arrow[d, "\wr"] & E^1(E_S) \arrow[d, two heads] & \\
& E^1(T_1(A)) \arrow[r] \arrow[ddd, "\wr"] & E^1(T_1(E_S)) \arrow[dd, two heads] & \\
& & & \\
& & E^1(\mathbb{Z}_p(1)) \arrow[d, "\wr"] & \\
Z_S \arrow[r, "\alpha_1"] & \bigoplus_{\mathfrak{p} \in S_f} \mathrm{Ind}_{G_{\mathfrak{p}}}^{G} (\mathbb{Z}_p(-1)) \arrow[r, "\alpha_3"] & \mathbb{Z}_p(-1) \arrow[r] & 0 ,
\end{tikzcd}
$$

in which $E^1(E_S) \longrightarrow E^1(T_1(E_S))$ and $E^1(E_S) \longrightarrow E^1(\mathbb{Z}_p(1))$ are surjective, since $E^2(M/T_1(M)) = 0$ for any Λ-module and $E^2(E_S/\mathbb{Z}_p(1)) = 0$, since $E_S/\mathbb{Z}_p(1)$ has no non-zero finite submodule.

Hence the surjections on the right are all isomorphisms which proves the claim.

The next consequence has also been obtained by K. Wingberg (unpublished) by somewhat different means.

6.3 Corollary. $E_S \cong \bigoplus_{v \in S_\infty} \Lambda_{(G_v)} \oplus \mathbb{Z}_p(1)$, where S_∞ is the set of archimedean places of k and G_v, for each $v \in S_\infty$, is the decomposition group of v in G. In particular, $T_1(E_S) = \mathbb{Z}_p(1)$.

Proof. The exact sequence

$$0 = \mathbb{Z}_p(1)^+ \longrightarrow E^1(E_S/\mathbb{Z}_p(1)) \longrightarrow E^1(E_S) \xrightarrow{\sim} E^1(\mathbb{Z}_p(1))$$

shows $E^1(E_S/\mathbb{Z}_p(1)) = 0$. Since on the other hand $pd_\Lambda(E_S/\mathbb{Z}_p(1)) \leq 1$, because this module does not contain any non-trivial finite submodule, we deduce from theorem 1.6 that $E_S/\mathbb{Z}_p(1)$ is projective. Its isomorphism class is easily computed by the methods already used in the proof of 5.4 b), by computing $E_S \otimes \mathbb{Q}_p$ for finite intermediate layers.

6.4 Corollary. There is an exact sequence

$$0 \longrightarrow T_1(E_S) \longrightarrow T_1(A_S) \longrightarrow T_1(X_S) \longrightarrow E^1(X_3(-1)) \longrightarrow 0\,,$$

in particular, for $T \supset S$ a finite set of primes one has an exact sequence

$$0 \longrightarrow \bigoplus_{\mathfrak{p} \in T \smallsetminus S} \mathrm{Ind}_{G_{\mathfrak{p}}}^{G}(\mathbb{Z}_p(1)) \longrightarrow T_1(X_T) \longrightarrow T_1(X_S) \longrightarrow 0 \ .$$

<u>Proof</u>. Define Z'_S by the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_p(1) \arrow[r] & T_1(A_S) \arrow[rr] \arrow[dr, two heads] & & T_1(X_S) \arrow[r] & Z'_S \arrow[r] & 0 \\
& & & R \arrow[ur, hook] & & &
\end{tikzcd}$$

Splitting this sequence into two short exact sequences as indicated, we obtain a commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & E^1(Z'_S) \arrow[r] & E^1(T_1(X_S)) \arrow[r] \arrow[d, equal] & E^1(R) \arrow[r] \arrow[d, hook] & E^2(Z'_S) \arrow[r] & 0 \\
& & E^1(T_1(X_S)) \arrow[r] & E^1(T_1(A)) \arrow[r] \arrow[d] & E^1(\mathbb{Z}_p(1)) \arrow[r] & 0 \\
& & & E^1(\mathbb{Z}_p(1)) & &
\end{tikzcd} \qquad (6.4.1)$$

where we have used the facts that $R^+ = 0 = \mathbb{Z}_p(1)^+$ (since these are Λ-torsion modules) and $0 = E^2(T_1(X_S)) \longrightarrow\!\!\!\!\!\rightarrow E^2(R)$. The exactness of the second row follows from the proof of 6.3 since $E^1(T_1(X_S)) = E^1(X_S)/T_0(E^1(X_S))$ by 3.6 ii). Since $E^1(A) \xrightarrow{\sim} E^1(T_1(A))$ is torsion-free, a comparison of 6.4.1 with 6.2 now shows:

$$E^1(Z'_S) \cong X_3(-1)/T_0(X_3(-1)) \ ,$$

$$E^2(Z'_S) = 0 \ .$$

V

In particular, $pd_\Lambda(Z_S') \le 1$, and $Z_S' \cong E^1(E^1(Z_S'))$ by theorem 1.6, since $(Z_S')^+ = 0$ (cf. also the statement about the self-duality for modules of type B) in § 3). We conclude

$$Z_S' \cong E^1(X_3(-1)/T_0(X_3(-1))) \cong E^1(X_3(-1)) ,$$

cf. 3.3 a), hence the first claim. The obtained sequence is functorial in S , hence the second claim is an obvious consequence, by the exact sequence

$$0 \longrightarrow \bigoplus_{\rho \in T \setminus S} \mathrm{Ind}_{G_\rho}^{G}(\mathbb{Z}_p(1)) \longrightarrow T_1(A_T) \longrightarrow T_1(A_S) \longrightarrow 0 .$$

We finish by calculating for X_S the Λ-modules associated to it by the general discussion in § 3.

6.5 Corollary. a) $E^0(X_S) = \bigoplus_{v \in S_\infty^c} \Lambda(G_v)$, where S_∞^c is the set of complex archimedean places of k , $E^1(X_S) = Z_S$, $E^2(X_S) = 0$.

b) $T_0(X_S) = 0$, $T_1(X_S) = E^1(Z_S)$, $T_2(X_S) = T_0(X_3(-1))^\vee$.

c) $T_0(X_3) \cong \varprojlim_n H^1(G_n, \mathcal{E}_S(K))$, where $G_n = \mathrm{Gal}(K/k(\mu_{p^{n+1}}))$,

$\mathcal{E}_S(K) = \mathcal{O}_{S,K}^{\times}$ is the group of S-units in K , and the limit is taken via the corestrictions.

Proof. All formulae are clear from the previous discussion and the fact that $X_S \simeq DZ_S$, except for the claim in c). For this let $k_n = k(\mu_{p^{n+1}})$ and let $Cl_S(k_n)$ (resp. $Cl_S(K)$) be the S-class group of k_n (resp. K). There is a well-known commutative diagram of finite groups

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_{n+1}, E_S(K)) \arrow[r] \arrow[d, "\mathrm{cor}"] & Cl_S(k_{n+1}) \arrow[r] \arrow[d, "N"] & Cl_S(K)^{G_{n+1}} \arrow[d, "\mathrm{tr}"] \\
0 \arrow[r] & H^1(G_n, E_S(K)) \arrow[r] & Cl_S(k_n) \arrow[r] & Cl_S(K)^{G_n}
\end{tikzcd} ,$$

where cor is the corestriction, N the norm, and tr the trace of G_n/G_{n+1}. By passing to the inverse limit over n we obtain an exact sequence of G-modules

$$0 \longrightarrow \varprojlim_n H^1(G_n, E_S(K)) \longrightarrow X_3 \longrightarrow \varprojlim_n Cl_S(K)^{G_n} .$$

Now $\varprojlim_n H^1(G_n, E_S(K))$ is finite, since the order of $H^1(G_n, E_S(K))$ is bounded independently of n [Iw] 5.2. Hence it suffices to show that the last group has no non-trivial finite G-submodule. It suffices to show the same for the fixed module under the pro-p-group G_0, since for a finite G_0-module $A \neq 0$ one has $A^{G_0} \neq 0$. But

$$\left(\varprojlim_n Cl_S(K)^{G_n}\right)^{G_0} = \varprojlim_n Cl_S(K)^{G_0} ,$$

where the inverse limit is taken via the p-multiplication, so this group is uniquely p-divisible.

<u>6.6 Example</u>. There is an exact sequence

$$0 \longrightarrow E^1(Z_S) \longrightarrow X_S \longrightarrow \bigoplus_{v \in S_\infty^c} \Lambda(G_v) \longrightarrow \mathrm{Hom}\left(\varprojlim_n H^1(G_n, E_S(K)), \mu(p)\right) \longrightarrow 0 .$$

This should be compared with Iwasawa's results in [Iw] 8.3.

References

[AB] M. Auslander, M. Bridger, Stable Module Theory, Memoirs of the Amer. Math. Soc., vol.94 (1969).

[Bi] P. Billot, Quelques aspects de la descente sur une courbe elliptique dans le cas de réduction supersingulière, Comp. Math. 58 (1986), 341-369.

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

[Du] D. Dummit, On the cyclicity of a Galois module in local fields, J. reine angew. Math. 342 (1983), 212-220.

[Ger] E.L. Gerlovin, Completion of the multiplicative group of a cyclic p-extension of a local field, Vestnik Leningrad Univ. 24, No. 7 (1969), 14-22.

[Gr] A. Grothendieck, Local Cohomology, Lecture Notes in Math. 41, Springer Berlin-Heidelberg-New York 1967.

[Hi] P. Hilton, Homotopy theory of modules and duality, Symp. Int. de Top. Alg., Mexico (1956), p.273-281.

[HS] P. Hilton, U. Stammbach, A Course in Homological Algebra, Graduate Texts in Math. 4, Springer New York-Heidelberg-Berlin 1970.

[Iw] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, Ann. of Math.98 (1973), 246-326.

[Jak] A.V. Jakovlev, Homological determinacy of p-adic representations of rings with power basis, Math. USSR-Izv.4, No.5 (1970), 1001-1016 (transl. from Izv. Akad. Nauk SSR 34, No.5 (1970)).

[J1] U. Jannsen, On the structure of Galois groups as Galois modules, Number Theory Noordwijkerhout 1983, p.109-126, Lecture Notes in Math. 1068, Springer Berlin-Heidelberg-New York-Tokyo 1984.

[J2] U. Jannsen, Homotopy theory for modules over a ring; preprint (1985).

[JW] U. Jannsen, K. Wingberg, Einbettungsprobleme und Galoisstruktur lokaler Körper, J. reine angew. Math.319 (1980), 196-212.

[Ko] N.M. Kopelevich, P-adic representations of rings with power basis, Math. Notes 17 (1975) 154-159 (transl. from Mat. Zametki 17 (1975)).

[Kun] E. Kunz, Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg Braunschweig/Wiesbaden 1980.

[Kuz] L.V. Kuz'min, Homology of profinite groups, Schur multipliers, and class field theory, Math. USSR - Izv.3, No.6 (1969), 1149-1181 (transl. from Izv. Akad. Nauk. SSSR 33, No.6 (1969)).

[La] M. Lazard, Groupes Analytiques P-adiques, Publ. Math. I.H.E.S. 26 (1965).

[Mi] J.S. Milne, Arithmetic Duality Theorems, Perspectives in Math. Vol.1, Academic Press Boston 1986.

[Neu] O. Neumann, On p-closed algebraic number fields with restricted ramification, Math. USSR Izv. 9, No.2 (1975), 243-254 (transl. from Izv. Akad. Nauk. SSSR 39, No.2 (1975), 259-271, 471).

[NQD] T. Nguyen-Quang-Do, Formations de classes et modules d'Iwasawa, Number Theory Noordwijkerhout 1983, p.167-185, Lecture Notes in Math. 1068, Springer Berlin-Heidelberg-New York-Tokyo 1984.

[P-R] B. Perrin-Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa, Soc. Math. de France. Memoire 17 (1984).

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

[Še] G.P. Šestakova, Homological determination of modules with torsion, Math. USSR-Sb. 37, No. 3 (1980), 441-449 (transl. from Matem. Sbornik 109 (151), No.3 (1979)).

[S1] J-P. Serre, Cohomologie Galoisienne, Lecture Notes in Math.5, Springer Berlin-Heidelberg-New York 1973.

[S2] J-P. Serre, Sur les groupes de congruence de variétés abéliennes, II, Izv. Akad. Nauk. SSSR 35 (1971), 731-737.

[S3] J-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Math. 42, Springer New York-Heidelberg-Berlin 1977.

[Ta] J. Tate, Duality theorems in Galois cohomology over number fields, Proc. ICM Stockholm 1962, p.288-295, Institut Mittag-Leffler 1963.

[W1] K. Wingberg, Die Einseinheitengruppe von p-Erweiterungen regulärer $\mathfrak{p}$-adischer Zahlkörper als Galoismodul, J. reine angew. Math. 305 (1979), 206-214.

[W2] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, Comp. Math. 55 (1985), 333-381.

[W3] K. Wingberg, Duality theorems for abelian varieties over $\mathbb{Z}_p$-extensions, this volume.