Iwasawa Modules up to Isomorphism

Uwe Jannsen

Dedicated to Kenkichi Iwasawa

In classical Iwasawa theory one considers modules over the completed group ring \( A = \mathbb{Z}_p[[G]] \) 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 \( A \)-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 \( A \)-modules, recalled in §1. It amounts to considering \( A \)-modules up to projective factors (which is no serious restriction in view of Krull-Schmidt theorem), and has a formalism quite analogous to the one in topology: one has a loop space functor \( \Omega \), a suspension \( \Sigma \), fibrations, cofibrations etc., and a certain analogue of homotopy groups in form of the \( A \)-modules \( E'(M) = \text{Ext}_A(M, A) \).

There is also an analogue of the Postnikov tower describing how a module \( M \) is "glued together" from the modules \( E'(M) \). 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 \( A \)-module \( M \) is determined up to isomorphism by \( E^0(M) \cong A^{\text{rank}_A M}, E^1(M), E^2(M) \), and a class in \( \text{Ext}_A^2(E^2(M), E^1(M)) \). We then discuss the modules \( E'(M) \) in some detail. For example, we express various properties of \( M \)—like the existence of finite submodules or the freeness of \( M/\text{Tor}_A M \)—in terms of the \( E'(M) \). We also give some formulæ for the \( E' \), in terms of inverse limits often encountered in the applications.

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

Received February 1, 1988.
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 $\mathfrak{G}$ of $p$-cohomological dimension two. If $\mathfrak{H} \subseteq \mathfrak{G}$ is a closed normal subgroups and $G = \mathfrak{G} / \mathfrak{H}$, we show how to describe the $A$-module $\mathfrak{H}/[\mathfrak{H}, \mathfrak{H}](p)$ in terms of the dualizing module $E_2^p(\mathfrak{G}) = \lim_m D_2(Z/p^m)$ of $\mathfrak{G}$.

In § 5 this is applied to study the $A$-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:

**Theorem.** If $k$ is local, then the $A$-module $X = \text{Gal}(M/K)$, $M$ the maximal abelian pro-$p$-extension of $K$, is determined by $\mu_X(p)$—the group of $p$-power roots of unity in $K$—and a canonical class $\zeta \in H^2(G, \mu_p(k))^\vee$ (where $\vee$ denotes the Pontrjagin dual).

**Theorem.** If $k$ is global, let $S \supseteq \{p | p\}$ 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 $A$-module $X_S = \text{Gal}(M^S/K)$ is determined by $W_S = E_2^p(\text{Gal}(K^S/K))$—where $E_2^p$ is the dualizing module of $\text{Gal}(K^S/k)$—and a canonical class $\zeta \in H^2(G, W_S)^\vee$.

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

In the global case we show that $W_S$ is closely related to $X' = \text{Gal}(L'/K)$, 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

$$0 \rightarrow X'(-1) \rightarrow W'_S \rightarrow \bigoplus_{\nu \in S} \text{Ind}_{G_\nu}^G (Z_p(-1)) \rightarrow Z_p(-1) \rightarrow 0,$$

where $G_s \subseteq G$ is a decomposition group at $p$ and $\text{Ind}_{G_\nu}^G$ is the compact induction. If $K = k(\mu_{p^\infty})$, then $W'_S \cong E^1(X_S)$, and by the quasi-isomorphism $\text{Tor}_1(X_S) \cong E^1(X_S)^\circ$ (where $M^\circ$ 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 $A$-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 go already 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 $A$ 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 $A$-modules considered are assumed to be finitely generated.

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

$$f: M \to P \to N$$

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

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

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

b) $f$ is a homotopy equivalence if and only if $f^*: \text{Ext}^i_A(N, R) \to \text{Ext}^i_A(M, R)$ is an isomorphism for all $A$-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 $H_i(A)$) if and only if $M \oplus P \cong N \oplus Q$ with projective $A$-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.

1.3 Lemma. Let \( f, g : M \to N \) be surjective \( A \)-morphisms. If \( f \simeq g \), then \( \ker f \simeq \ker g \).

Proof. Let \( f - g = \pi \circ \varphi : M \xrightarrow{\varphi} P \xrightarrow{\pi} N \) with \( P \) projective, then we get a commutative exact diagram

\[
\begin{array}{ccccccc}
0 & \to & K & \to & M \oplus P & \xrightarrow{f+\pi} & N & \to & 0 \\
& \downarrow & & \downarrow \Phi & & \downarrow & & \\
0 & \to & L & \to & M \oplus P & \xrightarrow{g+\pi} & N & \to & 0,
\end{array}
\]

where \( \Phi : (m, p) \mapsto (m, p + \varphi(m)) \) is the mapping cylinder of \( \varphi \). But \( K \simeq \ker f \oplus P \) by the commutative exact diagram

\[
\begin{array}{ccccccc}
0 & \to & \ker f & \to & M & \xrightarrow{f} & N & \to & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
& & K & \to & M \oplus P & \xrightarrow{f+\pi} & N & \to & 0,
\end{array}
\]

and similarly \( L \simeq P \oplus \ker g \).

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

1.4. Definition. Let \( E^0(M) = M^+ = \text{Hom}_A(M, A) \) be the \( A \)-dual, and more generally, let \( E^i(M) = \text{Ext}^i_A(M, A) \) for \( i \geq 0 \). If \( M \) is a left \( A \)-module, say, these are right \( A \)-modules by functoriality and the right \( A \)-structure of the bi-module \( A \).

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

1.5. Definition and theorem.

a) The loop space functor \( M \mapsto \Omega M \) is defined as follows:

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

ii) Let \( \Omega M = \ker \pi \).

Thus, \( \Omega M \) is characterized by an exact sequence
with \( P \) projective (i.e., \( \Omega M \) is “the” first syzygy-module).

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

i) Choose a surjection \( \pi: P \rightarrow M^+ \) with \( P \) projective.

ii) Let \( \Sigma M = \text{Coker}(M - \varphi M \rightarrow M^{++} - \pi^+ \rightarrow P^+) \), where \( \varphi_M: M \rightarrow M^{++} \)
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

\[
(1.5.2) \quad M - \varphi \rightarrow Q \rightarrow \Sigma M \rightarrow 0
\]

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

c) The transpose \( DM \) is defined as follows

i) Choose \( P_1 - \pi_1 \rightarrow P_0 \rightarrow M \rightarrow 0 \) exact with projectives \( P_1 \) and \( P_0 \).

ii) Let \( DM = \text{Coker}(P_0^+ - \pi_1^+ \rightarrow P_1^+) \).

In other words, \( DM \) is defined by the exact sequence

\[
(1.5.3) \quad 0 \rightarrow M^+ \rightarrow P_0^+ \rightarrow P_1^+ \rightarrow DM \rightarrow 0.
\]

Then one has \( D^2 = \text{Id} \) 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 \( \varphi_P: P \rightarrow P^{++} \) is an isomorphism. For example, the last facts immediately imply \( D^2 = \text{Id} \), and the functoriality of \( \Omega \) is obtained by a commutative diagram

\[
\begin{array}{c}
0 \rightarrow \Omega M \rightarrow P \rightarrow M \rightarrow 0 \\
\Omega f \downarrow \quad \quad \quad \downarrow f \\
0 \rightarrow \Omega N \rightarrow Q \rightarrow N \rightarrow 0,
\end{array}
\]

where the dotted lifting of \( f \) exists by the projectivity of \( P \), and \( \Omega f \) is the induced map.

The reader should be aware of the fact that \( D \) and the \( E_1 \) interchange left and right \( A \)-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 \( A \)-module structures of \( A \) to give the \( E_1(M) \) and hence \( DM \) left \( A \)-module structures again, if \( M \) is a left \( A \)-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 \( A \)-modules or if a functor interchanges left and
right \( A \)-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 \( \text{pd}_A(M) \) of a \( A \)-module \( M \) is the
infimum over the numbers \( n \geq 0 \) such that there exists a resolution of
length \( n \)

\[
0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0
\]

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

1.6 Theorem. The functor \( M \mapsto E^1(M) \) induces an equivalence of
categories

\[
\{ \text{\( A \)-modules \( M \) with \( \text{pd}_A(M) \leq 1 \) \} \} \sim \{ \text{\( A \)-modules \( N \) with \( N^+ = 0 \) \} \}
\]

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

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 \( T_i(M) = \ker \varphi_M \) as above and \( T_1(M) = \operatorname{Coker} \varphi_M \), so that

(1.8.1) \[
0 \rightarrow T_1(M) \rightarrow M \xrightarrow{\varphi_M} M^+ \rightarrow T_i(M) \rightarrow 0
\]

is exact. Then canonically \( T_i(M) \cong E^i(DM) \) and \( T_i(M) \cong E^2(DM) \). In
view of this let

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

(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 \( \Omega M \) or \( \Sigma M \)
for a \( A \)-module \( M \). Obviously some information on \( M \) is lost (e.g., \( \Omega M \)
\( \cong 0 \) if \( \text{pd}_A(M) \leq 1 \)); 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:
1.9 Theorem. A $\Lambda$-module $M$ is determined up to homotopy by

a) $\Sigma M$, $T_1(M)$, and a class $\chi_M \in \text{Ext}_A^1(\Omega \Sigma M, T_1(M))$, or by

b) $\Omega M$, $E^1(M)$, and a class $\psi_M \in \text{Ext}_A^1(D\Sigma \Omega M, E^1(M))$.

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

Proof. a) Let $\chi_M$ be the class of the extension

\[
0 \rightarrow T_1(M) \rightarrow M \rightarrow \text{Im } \varphi_M \rightarrow 0,
\]

via the canonical identification

\[
\text{Im } \varphi_M \simeq \Omega \Sigma M,
\]

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

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

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

1.10 Theorem. The functors $\Sigma$ and $\Omega$ induce quasi-inverse equivalences of categories

\[
\begin{cases}
\text{A-modules } M \text{ with } T_1(M) = 0 \\
\text{up to homotopy}
\end{cases}
\xrightarrow{\sim}
\begin{cases}
\text{A-modules } N \text{ with } E^1(N) = 0 \\
\text{up to homotopy}
\end{cases}
\]

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

1.11 Corollary.

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 $\Lambda$-modules $N$. 
iv) The adjunction map $M \to \Omega \Sigma M$ is a homotopy equivalence.

b) The following statements are equivalent:
   i) $E^i(N) = 0$.
   ii) $N \simeq \Sigma M$ for some $A$-module $N$.
   iii) The adjunction map $\Sigma \Omega N \to N$ is homotopy equivalence.

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

§ 2. Group rings of profinite groups

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

$$A = A(G) = \mathbb{Z}_p[[G]] = \lim_{U \leq G} \mathbb{Z}_p[G/U],$$

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

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

where $B^* = \text{Hom}(B, \mathbb{Q}/\mathbb{Z})$ 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

$$D_r(A) = D_r([1], A) \quad (r \geq 0).$$

In the following assume that $A$ 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 $A$-module $M$ has a natural compact topology as a pseudo-compact module over the pseudo-compact algebra $A$ (cf. [Br]), and its Pontrjagin dual $M^\vee = \text{Hom}_{cont}(M, \mathbb{Q}_p/\mathbb{Z}_p) = \lim_{U} M_U^\vee$ (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 $A$-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 $\iota B = \{ b \in B \mid nb = 0 \}$.  

2.1 Theorem. Let $M$ be a finitely generated $A$-module.

a) There are functorial exact sequences

$$0 \rightarrow D_r(M^\vee) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow E^*(M)^\vee \rightarrow \text{Tor} D_{r-1}(M^\vee) \rightarrow 0$$

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

b) There is a long exact sequence

$$\cdots \rightarrow E^*(M)^\vee \rightarrow \lim_m D_r(p_m(M^\vee)) \rightarrow \lim_m D_{r-2}(M^\vee/p^m)$$

$$\rightarrow E^{*-1}(M)^\vee \rightarrow \cdots ,$$

functorial in $M$ and in $G$.

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

$$M^+ = \text{Hom}_A(M, A) \cong \lim_{U \leq G} \text{Hom}_A(M, \mathbb{Z}_p[G/U])$$

$$\cong \lim_{U \leq G} \text{Hom}_{\mathbb{Z}_p[G/U]}(M_U, \mathbb{Z}_p[G/U])$$

$$\cong \lim_{U \leq G} \text{Hom}_{\mathbb{Z}_p}(M_U, \mathbb{Z}_p),$$

where the limit is taken via the norms. Hence

$$(M^+)^\vee \cong \lim_{U \leq G} \text{Hom}_{\mathbb{Z}_p}(M_U, \mathbb{Z}_p)^\vee$$

$$\cong \lim_{U \leq G} M_U \otimes \mathbb{Z}_p/\mathbb{Z}_p,$$

where we have used the relation

$$(\lim_m \text{Hom}_{\mathbb{Z}_p}(N/p^m, \mathbb{Z}/p^m))^\vee \cong \lim_m N/p^m$$

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

(2.1.1) $$(M^+)^\vee = (\lim_{U \leq G} ((M^\vee)^*) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

or as

(2.1.2) $$(M^+)^\vee = \lim_m ((M/p^m)^\vee)^*).$$
In other words, 2.1.1 describes \( \mathcal{M}^{(M^+)} \) as the composition of the right exact functors \( \mathcal{M}^\rightarrow \rightarrow \mathcal{D}_0(M^\vee) \) and \( N^\rightarrow \rightarrow N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p / \mathbb{Z}_p \), while 2.1.2 describes it as the composition of the right exact functors \( \mathcal{M}^\rightarrow \rightarrow \mathcal{C}_{\mathbb{Q}_p}(M) \) and \( (M_m)^\rightarrow \rightarrow \lim_m \mathcal{D}_m(M_m^\vee) \), where \( \mathcal{C}_{\mathbb{Q}_p} \) 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 \( \mathcal{M}^\rightarrow \rightarrow \mathcal{D}_0(M^\vee) \) is \( \mathcal{M}^\rightarrow \rightarrow \mathcal{D}_r(M^\vee) \), and the first functors in the compositions map projectives to acyclics for the second functors. Since \( \mathcal{M}^\rightarrow \rightarrow \mathcal{M}^\vee \) and filtering direct limits are exact, we get two Grothendieck spectral sequences of homological type

\[
E^2_{r,s} = \text{Tor}^r_{\mathbb{Z}_p}(D_s(M^\vee), \mathbb{Q}_p / \mathbb{Z}_p) \Longrightarrow E^r_{r+s} = \mathcal{E}^{r+s}(M)^\vee
\]

\[
E^2_{r,s} = \lim_n D_n(L_sC_{\mathbb{Q}_p}(M)^\vee) \Longrightarrow E^r_{r+s} = \mathcal{E}^{r+s}(M)^\vee.
\]

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

\[
\text{Tor}^r_{\mathbb{Z}_p}(N, \mathbb{Q}_p / \mathbb{Z}_p) = \begin{cases} N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p / \mathbb{Z}_p & r=0, \\ \text{Tor}_{\mathbb{Z}_p}(N) & r=1, \\ 0 & r \geq 2, \end{cases}
\]

and the left derivatives of \( C_{\mathbb{Q}_p} \) are

\[
L^sC_{\mathbb{Q}_p}(M) = \begin{cases} (M/p^m) & s=0, \\ (p^mM) & s=2, \\ 0 & s \geq 2, \end{cases}
\]

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

2.2 Remark. a) The above can be extended to the case of an arbitrary profinite group \( G \), i.e., to non-noetherian \( \Lambda \), as follows. Call a \( \Lambda \)-module \( \text{noetherian} \), if it has a resolution by finitely projective \( \Lambda \)-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 \( \text{Tor}_{\mathbb{Z}_p}(M) \) and \( M/\text{Tor}_{\mathbb{Z}_p}(M) \) (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

\[
\cdots \longrightarrow \mathcal{E}^r(M)^\vee \longrightarrow \mathcal{E}^r(M/\text{Tor}_{\mathbb{Z}_p}(M))^\vee \longrightarrow \mathcal{E}^{r-1}(\text{Tor}_{\mathbb{Z}_p}(M))^\vee \\
\longrightarrow \mathcal{E}^{r-1}(M)^\vee \longrightarrow \cdots.
\]

2.3 Lemma. If \( U \leq G \) is an open subgroup of \( G \), then the restriction
induces a functorial isomorphism of $A_G$-modules

$$E^r_G(M) := \text{Ext}^r_{A(G)}(M, A(G)) \cong \text{Ext}^r_{A(U)}(M, A(U)) =: E^r(U)$$

for every $A(G)$-module $M$.

**Proof.** Since $A(G)$ is projective as a $A(U)$-module, this follows from the obvious case $r=0$ by looking at a free resolution of $M$.

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

**Proof.** Recall that $\text{vcd}_p(G) \leq n$ means that there is an open subgroup $U$ of $G$ with $p$-cohomological dimension $\text{cd}_p(U) \leq n$. 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.

**2.5 Corollary.** Let $G$ be a finite group, then $E^0(M) = \text{Hom}_{Z_p}(M, Z_p)$. $E^r(M) = \text{Tor}_{Z_p}(M)^\vee$, and $E^r(M) = 0$ for $r \geq 2$.

**Proof.** One has $\text{vcd}_p(G) = 0$, so the result follows with 2.4 and 2.1 a). One may also use 2.3 and the isomorphisms

$$\text{Ext}^r_{Z_p}(M, Z_p) \cong \text{Tor}^r_{Z_p}(M, Q_p/Z_p)^\vee.$$

**2.6 Corollary.** Assume that $G$ is virtually strict Cohen-Macaulay at $p$ (i.e., that an open subgroup has this property, see [S1] V4.1), with $\text{vcd}_p(G) = n$. (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 $Q_p$, e.g., $G = Z_p^n$). Then

a) $E^r(Z_p^\vee) = 0$ for $r \geq n$, and $E^n(Z_p^\vee) \cong E^0_p(G)$, the $p$-torsion dualizing module.

b) If $N$ is a finite $G$-module, then $E^r(N) = 0$ for $r \geq n + 1$, and $E^{n+1}(N)^\vee \cong \text{Hom}_{Z_p}(N^\vee, E^0_p(G))$.

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

**Proof c.** By 2.1 b) we get

$$E^r(M)^\vee \cong \lim_{\rightarrow} D_n((M/p^n)^\vee).$$

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

\[ D_n(A) = \lim_{U \subseteq G_{\text{rres}}} H^n(U, A)^* \]

(2.6.1)

\[ \cong \lim_{U \subseteq G_{\text{rres}}} H^0(U, \text{Hom}_{\mathbb{Z}_p}(A, E_n^{(p)}(G))) = \text{Hom}_{\mathbb{Z}_p}(A, E_n^{(p)}(G)) \]

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

\[ \lim_{m} D_n((M/p^m)^{\vee}) = \lim_{m} \text{Hom}_{\mathbb{Z}_p}((M/p^m)^{\vee}, E_n^{(p)}(G)) \cong M \otimes_{\mathbb{Z}_p} E_n^{(p)}(G), \]

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

\[ E^*(N) \cong D_{r-1}(N^{\vee}), \]

hence the claim by the previous considerations.

2.7 Remarks. 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 \( \text{vcd}_p(G) < \infty \), 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 \( (af)(a) = f(a^{-1}a) \) for \( f: A \rightarrow \mathbb{Q}/\mathbb{Z} \), \( a \in G \) and \( a \in A \), similarly for compact \( G \)-modules \( M \) and \( M^{\vee} \). If we do so, we have to give \( E^*(M) \) 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 \( ((af)(a) = f(aa) \) 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 \( \Lambda \), e.g., that it is a noetherian local ring with projective dimension \( \text{pd} (\Lambda) = 2 \) (recall that \( \text{pd} (\Lambda) = \sup \text{pd}_M(M) \), where \( M \) runs over all finitely generated \( \Lambda \)-modules). This implies that \( E^*(M) = 0 = T_i(M) \) for \( i \geq 3 \). We now investigate these groups for \( i \leq 2 \); for this let \( T_i(M) \) be the maximal finite submodule of \( M \).

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

a) \( T_1(M) \) is the \( \Lambda \)-torsion submodule of \( M \).

b) \( E^1(M) \) is a \( \Lambda \)-torsion module. If \( M \) is \( \Lambda \)-torsion, then \( E^1(M) \) is the Iwasawa adjoint \( \alpha(M) \) of \( M \) ([Iw] 1.3) and has no non-zero finite sub-
Iwasawa Modules

Finally, \( E^i(N) = 0 \) for a finite module \( N \).

c) \( T^\delta_1(M) \) is finite. One has \( T^\delta_1(M) = 0 \) if and only if \( M/T^\delta_1(M) \) is free, i.e., if and only if \( M \cong T^\delta_1(M) \oplus \Lambda^r \) for some \( r \geq 0 \). In particular, \( T^\delta_1(M) = 0 \) for \( \Lambda \)-torsion modules.

d) \( E^3(M) \) is finite, one has \( E^3(M) \cong E^3(T^\delta_1(M)) \cong T^\delta_1(M)^{\vee} \), and the following properties are equivalent:

i) \( E^3(M) = 0 \),

ii) \( \text{pd}_A(M) \leq 1 \),

iii) \( T^\delta_0(M) = 0 \),

iv) \( M \) is a submodule of an elementary \( \Lambda \)-module.

Proof. a) is clear by tensoring with the field of fractions of \( \Lambda \). The first statement in b) follows from a) since \( E^i(M) = T^i(DM) \). For the second statement see [P-R] I.2.2 and [Bi] 1.2 and remarque, and \( T^\delta_0(\alpha(M)) = 0 \) follows from Iwasawa's first description of \( \alpha(M) \) in [Iw] 1.3.

By the exact sequence \( 0 \rightarrow A \rightarrow A \rightarrow Z/p \rightarrow 0 \), where \( \gamma \) is a topological generator of \( G \), we immediately deduce \( E^i(Z/p) \cong Z/p \) (this always denotes the module \( Z/p \) with trivial action of \( G \)). The exact sequence

\[
0 \rightarrow E^i(Z/p) \rightarrow E^i(Z/p) \rightarrow E^i(Z/p) \rightarrow E^i(Z/p) \rightarrow 0
\]

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

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

\[
0 \rightarrow A \rightarrow M \rightarrow E \rightarrow C \rightarrow 0,
\]

where \( E \) is elementary and \( A \) and \( C \) are finite. One has \( \text{pd}_A(E) \leq 1 \) and \( T_0(E) = 0 \). The last property implies \( A_0 = T_0(M) \), the first one implies \( E^2(\text{Im } f) = 0 \), since this is a quotient of \( E^2(E) = 0 \), hence we get \( E^3(M) \cong E^2(A) \). The isomorphism

\[
E^3(A) \cong \text{Hom}(A, Q/\Lambda)
\]

now follows from the local duality for the regular local ring \( A \) of dimension 2 with residue field \( Z/p \) (cf. [Bi] 1.2). The rest is clear: \( f \) is injective if and only if \( T_0(M) = 0 \), i.e., if and only if \( T_0(M)^{\vee} = E^2(T_0(M)) \cong E^3(M) \) is zero, i.e., if and only if \( \text{pd}_A(M) \leq 1 \); look at a resolution

\[
0 \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0;
\]
if \( E^2(M) = 0 \), then \( \pi_2 \) has a left inverse.

c) now easily follows from the relation \( T_\omega(M) = E^2(DM) \), the exact sequence 1.8.1 and the well-known fact that \( M^{++} \) is projective for \( \text{cd} \ (A) \leq 2 \) (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 \( A \)-module \( M \) is determined by the above invariants. This result is valid more generally for rings \( A \) with \( \text{pd} \ (A) \leq 2 \).

**3.2 Theorem.** A \( A \)-module \( M \) is determined up to homotopy by

a) \( T_\omega(M), T_\omega^2(M) \) and a class \( \chi_M \in \text{Ext}_1^2(T_\omega^2(M), T_\omega(M)) \), or by

b) \( E^1(M), E^2(M) \) and a class \( \psi_M \in \text{Ext}_1^2(E^2(M), E^1(M)) \).

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

\[
0 \rightarrow \text{Im} \varphi_M \rightarrow M^{++} \rightarrow T_\omega^2(M) \rightarrow 0
\]

we obtain an isomorphism

\[
\text{Ext}_1^2(\text{Im} \varphi_M, T_\omega(M)) \cong \text{Ext}_1^2(T_\omega^2(M), T_\omega(M)).
\]

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

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

We now further investigate \( E^1 \) and \( T_1 \).

**3.3 Lemma.** a) One has \( E^1(M) \cong E^1(M/T_\omega^2(M)) \), and equivalence of the following statements:

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

ii) \( M/T_\omega^2(M) \) is free, i.e., \( M \cong T_\omega^2(M) \oplus A^r \) for some \( r \geq 0 \).

b) the following statements are equivalent:

i) \( T_1(M) = 0 \).

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

**Proof.** a) The first claim follows from the exact sequence

\[
0 = E^0(T_\omega^2(M)) \rightarrow E^1(M/T_\omega^2(M)) \rightarrow E^1(M) \rightarrow E^1(T_\omega^2(M)) = 0.
\]
But by 3.1 d) we have \( \text{pd}_d(M/T_0(M)) \leq 1 \), hence \( M/T_0(M) \cong 0 \) if and only if \( E^i(M/T_0(M)) = 0 \) by 1.6.

b) The implication \( \text{ii)} \Rightarrow \text{i)} \) 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

\[
\begin{array}{cccccc}
0 & \to & M & \to & P & \to & C & \to & 0 \\
\downarrow & & \downarrow \alpha & & \downarrow \beta \\
0 & \to & M & \to & M^{++} & \to & T_1(M) & \to & 0
\end{array}
\]

with canonical isomorphisms \( \alpha \) and \( \beta \).

**Proof.** The map \( i: M \to P \) induces an isomorphism \( i^*: P^+ \cong M^+ \), since \( C^+ = 0 = E^1(C) \). The commutative diagram

\[
\begin{array}{cccccc}
0 & \to & M & \overset{i}{\to} & P & \to & C & \to & 0 \\
\varphi_M \downarrow & & \varphi_P \downarrow & & \varphi_P \\
0 & \to & M^{++} & \cong & P^{++}
\end{array}
\]

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

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

A) free modules,

B) \( \Lambda \)-torsion modules with \( \text{pd}_d(M) \leq 1 \),

C) finite modules,

and two extension classes. For a \( \Lambda \)-module \( M \) the modules in question are

\[
\begin{array}{cccccc}
A) & M^{++} \\
B) & T_1(M)/T_0(M) \\
C) & T_0(M), T_2(M)
\end{array}
\]

with the extension classes \( \chi_M \) 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
The three types of \(A\)-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 \(A\)-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 \(E^2(E^2(N)) \cong E^2(\overline{N}) \cong \overline{N} = N\) 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 \(P \cong P^+\) for a complex \(P\) of projective \(A\)-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 modules in 3.5.2 and 3.5.3 are in fact the same.

3.7 Lemma. a) There is an exact sequence

\[ 0 \longrightarrow E^2(T_2(M)) \longrightarrow E^1(M) \longrightarrow E^1(T_1(M)) \longrightarrow 0 \]

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) \(E^2(E^1(M)) \cong T_0(M)\),

iii) \(E^2(E^2(M)) \cong T_0(M)\).
Proof. a): By splitting the sequence

$$0 \longrightarrow T_0(M) \longrightarrow M \overset{\phi_M}{\longrightarrow} M^+ \longrightarrow T_0(M) \longrightarrow 0$$

into two short exact sequences containing $B = \text{Im } \phi_M = M/T_0(M)$ we obtain exact sequences

$$0 = E^1(M^+) \longrightarrow E^1(B) \longrightarrow E^2(T_0(M)) \longrightarrow E^2(M^+) = 0$$
$$0 = E^0(T_0(M)) \longrightarrow E^1(B) \longrightarrow E^1(M) \longrightarrow E^1(T_0(M)) \longrightarrow E^2(B) = 0$$

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

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

$$E^3(E^1(M)) \cong E^3(T_0E^1(M)) \cong E^3(E^2(T_0(M))) \cong T_2(M),$$

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

3.8 Corollary. $E^1(M)$ is finite $\iff T_1(M)$ is finite $\iff E^1(E^1(M)) = 0$.

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

3.9 Lemma. Let $M$ be a finitely generated $A$-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) $E^0(M) = \varprojlim_{n,m} (M^\delta)_{G_n}$ is free of the same rank as $M$,

b) $E^r(T_0(M)) \cong \varprojlim_{n,m} (M^\delta/p^m)_{G_n},$

c) $E^r(M/T_0(M)) \cong \varprojlim_{n,m} (M^\delta)_{G_n},$

d) $E^0(M^\delta) \cong \varprojlim_{n,m} (M^\delta)_{G_n} \cong \text{Hom}_{Z_p}(M^\delta, Z_p),$

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

where the transition maps are the obvious ones.

Proof. 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

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

The cokernel obviously is isomorphic to $\text{Hom}_{Z_p}(M^\delta, Z_p)$, while the kernel vanishes for $M = M^\delta$. On the other hand one has an exact sequence
because \((M^4)^+ = 0 = E^2(M/M^4)\) (cf. 3.1 d)). Since the first exact sequence is functorial in \(M\), we deduce that it must be isomorphic to the second one, by applying it to \(M^2\) and \(M/M^4\).

§ 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 \(\text{cd}_p(\mathcal{G}) \leq 2\) 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 \(X = \mathcal{H}(p)^{\text{ab}} = \mathcal{H}^{\text{ab}}(p)\) as a module over the completed group algebra \(A = \mathbb{Z}_p[[G]]\), where \(\mathcal{H}^{\text{ab}} = \mathcal{H}/[\mathcal{H}, \mathcal{H}]\) 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 \(x_1, \ldots, x_d\). We obtain a commutative exact diagram

\[
\begin{array}{ccccccccc}
1 & \rightarrow & \mathcal{H} & \rightarrow & \mathcal{F} & \rightarrow & G & \rightarrow & 1 \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \rightarrow & \mathcal{H}/[\mathcal{H}, \mathcal{H}] & \rightarrow & \mathcal{F}/[\mathcal{F}, \mathcal{F}] & \rightarrow & G & \rightarrow & 1 \\
\end{array}
\]

and it follows easily with the methods of Fox and Lyndon that one has an exact sequence of \(A\)-modules

\[
0 \rightarrow \mathcal{H}(p)^{\text{ab}} \rightarrow A^d \rightarrow A^{\text{aug}} \rightarrow \mathbb{Z}_p \rightarrow 0
\]

where \(\text{aug}\) is the usual augmentation, \(\{e_i\}_{i=1}^d\) is a basis of \(A^d\), and \(x_i\) is the image of \(x_i\) in \(G \subseteq A\) (cf. [W1] for the case of a finite \(p\)-group).

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

4.2 Definition. Let \(Y = I(\mathcal{G})_{\pi}\), where \(I(\mathcal{G})\) is the augmentation ideal of \(\mathbb{Z}_p[[\mathcal{G}]] = A(\mathcal{G})\).

4.3 Lemma (cf. [NQD] 1.7). a) There is a commutative exact diagram of \(A\)-modules
where $I$ is the augmentation ideal of $A$.

b) $\mathcal{N}'/[\mathcal{N}', \mathcal{R}](p)$ is a projective $A$-module.

**Proof.** a) follows as in [NQD] 1.7, by taking the $\mathcal{K}$-homology of the two exact sequences

\[
\begin{align*}
0 & \rightarrow I(\mathcal{G}) \rightarrow Z_p[[\mathcal{G}]] \rightarrow Z_p \rightarrow 0 \\
0 & \rightarrow H^1(\mathcal{H}, \mathcal{Q}_p|Z_p)^{\vee} \rightarrow \mathcal{N}'/[\mathcal{N}', \mathcal{R}](p) \rightarrow \Lambda^d \rightarrow Y \rightarrow 0 \\
0 & \rightarrow H^1(\mathcal{H}, \mathcal{Q}_p|Z_p)^{\vee} \rightarrow \mathcal{N}'/[\mathcal{N}', \mathcal{R}](p) \rightarrow \mathcal{A}^{ab}(p) \rightarrow X \rightarrow 0 \\
0 & \rightarrow 0
\end{align*}
\]

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

\[
\begin{align*}
H_1(\mathcal{G}, Z_p) & = H^1(\mathcal{G}, \mathcal{Q}_p|Z_p)^{\vee} = \mathcal{K}^{ab}, \\
H_2(\mathcal{G}, I(\mathcal{G})) & = I(\mathcal{G}) = Y, \\
H_1(\mathcal{G}, I(\mathcal{G})) = H_2(\mathcal{G}, Z_p) & = H^1(\mathcal{G}, \mathcal{Q}_p|Z_p)^{\vee}.
\end{align*}
\]

b): $\mathcal{N}^{ab}(p)$ is a projective $A(\mathcal{G})$-module, since $\text{cd}_p(\mathcal{G}) \leq 2$, see [Br] 5.2. Hence $\mathcal{N}^{ab}(p)_{\mathfrak{m}} = \mathcal{N}'/[\mathcal{N}', \mathcal{R}](p)$ is a projective $A$-module.

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

**4.5 Theorem.** Let $E^1_z(\mathcal{G}) = \varprojlim_{m,n} H^2(\mathcal{U}, Z/p^n)^{\ast}$ be defined as in §2, let $W = (E^1_z(\mathcal{G}))^{\ast}$ and $Z = W^{\vee}$, and assume that $\mathcal{N}^{ab}(p)$ is a finitely generated $A(\mathcal{G})$-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 $\chi \in H^2(G, W)^{\ast} = H_2(G, Z) \cong [Y, I]$, via Lemma 1.3 and the exact sequence
(χ corresponds to the homotopy class of f). As an alternative description, there is an exact sequence

\[ 0 \rightarrow X \rightarrow Y \xrightarrow{f} I \rightarrow 0 \]

whose extension class is the image of χ under the injection

\[ [Y, I] \rightarrow \text{Ext}^1_A(Y, \mathcal{R}(p)^{ab}). \]

c) Let \( \chi_0 \in H^3(\mathcal{G}, E_2^{(p)})^* \) be the canonical class: this is the class corresponding to the identity map under the canonical isomorphism (cf. [S1] I–8.1).

\[ H^3(\mathcal{G}, E_2^{(p)})^* \cong \text{Hom}_{\mathcal{G}}(E_2^{(p)}, E_2^{(p)}). \]

Then χ is the image of \( \chi_0 \) under the map

\[ H^3(\mathcal{G}, E_2^{(p)})^* \rightarrow H^3(\mathcal{G}, W)^*, \]

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 \( \mathcal{N}/[\mathcal{N}, \mathcal{R}](p) \).

**Proof.**

a) By the projectivity of \( \mathcal{N}^{ab}(p) \), 4.3.2 induces an exact sequence

\[ (4.5.1) \quad (\mathcal{N}^{ab}(p))^+ \rightarrow (\mathcal{N}^{ab}(\mathcal{G}))^+ \rightarrow E_\sigma^1(I(\mathcal{G})) \rightarrow 0. \]

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

\[ E_\sigma^1(I(\mathcal{G})) \cong E_\sigma^3(\mathbb{Z}_p) \cong (\lim_m D_\sigma(\mathbb{Z}/p^m))^\vee = (E_2^{(p)})^\vee, \]

hence, by taking \( \mathcal{H} \)-coinvariants, an exact sequence

\[ (4.5.2) \quad (\mathcal{A}^d)^+ \rightarrow (\mathcal{N}/[\mathcal{N}, \mathcal{R}](p))^+ \rightarrow \mathbb{Z} \rightarrow 0, \]

where we have used the canonical isomorphisms

\[ \mathcal{N}^{ab}(p)_\mathcal{S} \cong \mathcal{N}/[\mathcal{N}, \mathcal{R}](p), \]

\[ \text{Hom}_{\mathcal{A}(\mathcal{G})}(M, \mathcal{A}(\mathcal{G}))_\mathcal{S} \cong \text{Hom}_A(M_\mathcal{S}, \mathcal{A}), \]

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

\[ \mathcal{N}/[\mathcal{N}, \mathfrak{R}](p) \longrightarrow A^d \longrightarrow Y \longrightarrow 0. \]

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

\[ 0 \longrightarrow \mathfrak{R}^{ab}(p) \longrightarrow A^d \longrightarrow I \longrightarrow 0 \]

by 4.6 a) below induces an exact sequence

\[ 0 \longrightarrow [Y, I] \xrightarrow{\partial} \text{Ext}^1_\mathfrak{R}(Y, \mathfrak{R}^{ab}(p)) \longrightarrow E^1(Y)^d. \]

Now by definition \( \partial \) maps the class of \( f \) to the class of the pull-back extension

\[ 0 \longrightarrow \mathfrak{R}^{ab}(p) \longrightarrow A^d \longrightarrow I \longrightarrow 0 \]

\[ 0 \longrightarrow \mathfrak{R}^{ab}(p) \longrightarrow X' \longrightarrow Y \longrightarrow 0 \]

\[ f \]

\[ X = X', \]

and obviously \( X' \cong X \oplus A^d \).

c) This follows from the functoriality in 4.6 c) below: the above discussion is also valid for \( G = \mathcal{G} \), and the class of \( f: Y \rightarrow I \) is the image of the identity map under

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

It remains to show that the identity map corresponds to \( \chi_0 \) via the isomorphism 4.6 b) for \( \mathcal{G} \) and \( M = E^\mathfrak{g}_\mathfrak{p}(Z_p) \), via the identification \( DM = DE^\mathfrak{g}_\mathfrak{p}(Z_p) = DE^\mathfrak{g}(I(\mathcal{G})) = I(\mathcal{G}) \). Looking at the diagram

\[ A(\mathcal{G})^+ \longrightarrow (A(\mathcal{G})^d)^+ \longrightarrow (\mathcal{N}^{ab}(p))^+ \longrightarrow E^\mathfrak{g}_\mathfrak{p}(Z_p) \longrightarrow 0 \]

\[ 0 \longrightarrow I(\mathcal{G})^+ \longrightarrow (A(\mathcal{G})^d)^+ \longrightarrow (\mathcal{N}^{ab}(p))^+ \longrightarrow E^\mathfrak{g}_\mathfrak{p}(Z_p) \longrightarrow 0, \]

with exact bottom row, one easily checks that both classes correspond to the class of the natural inclusion \( I(\mathcal{G}) \rightarrow A(\mathcal{G}) \) in \( H_\mathfrak{g}(\mathcal{G}, E^\mathfrak{g}_\mathfrak{p}(\mathcal{G})) = \text{Ker } ((I(\mathcal{G})^+)_\mathfrak{p} \rightarrow ((A(\mathcal{G})^d)^+)_\mathfrak{p}) \).

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

$$
\begin{align*}
A' & \xrightarrow{g} P \rightarrow Z \rightarrow 0 \\
\end{align*}
$$

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

$$
\text{Coker } (P^+ \xrightarrow{g^+} (A')^+) \cong \text{Coker } (Q^+ \xrightarrow{h^+} (A')^+).
$$

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 $0 \rightarrow R \xrightarrow{\alpha} P \xrightarrow{\beta} N \rightarrow 0$ be an exact sequence of $A$-modules, with $P$ finitely generated projective, and let $M$ be another finitely generated $A$-module. In the long exact Ext-sequence

$$
\begin{align*}
\text{Hom}_A(M, P) & \xrightarrow{\beta^*} \text{Hom}_A(M, N) \rightarrow \text{Ext}_A(M, R) \xrightarrow{\alpha_*} \text{Ext}_A(M, P)
\end{align*}
$$

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

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

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

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

$$
\begin{align*}
H_*(G, M) & \xrightarrow{\sim} [DM, I(G)]
\end{align*}
$$

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

Proof. a) Obviously for $f: M \rightarrow N$ one has $f \in \text{Im } \beta_* \Rightarrow f \sim 0$. For the converse implication note that every map $Q \rightarrow N$, with $Q$ projective, factorizes through $\beta$. 
b) Choose an exact sequence (of right $\Lambda$-modules, say)

\[ 0 \rightarrow N^{\ell} \rightarrow F^{1} \rightarrow F^{0} \rightarrow M \rightarrow 0, \]

with finitely generated free modules $F_{0}, F_{1}$, so that $DM$ is defined by exactness of

\[ F_{0}^{+} \rightarrow F_{1}^{+} \rightarrow DM \rightarrow 0. \]

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

\[
\begin{array}{c}
0 
\rightarrow 
N 
\rightarrow 
F^{1} 
\rightarrow 
F^{0} \\
\downarrow \varphi_{F^{1}} \\
0 
\rightarrow 
DM^{+} 
\rightarrow 
F^{++} 
\rightarrow 
F^{++}.
\end{array}
\]

On the other hand we have

\[ H_{2}(G, M) \cong \text{Ker} (N_{0} \rightarrow (F_{1})_{0}) \cong \varepsilon^{-1}(F_{1}I)/NI. \]

Now it is readily checked that

\[ F_{1}I \cong F_{1}^{++}I = \text{Hom}_{\Lambda}(F_{1}^{+}, \Lambda)I \cong \text{Hom}_{\Lambda}(F_{1}^{+}, I), \]

and so we may identify

\[ \varepsilon^{-1}(F_{1}I) \cong \text{Hom}_{\Lambda}(DM, I) \cong \text{Hom}_{\Lambda}(DM, \Lambda). \]

On the other hand the exact sequence

\[
\begin{array}{c}
\text{Hom}_{\Lambda}(DM, \Lambda^{d}) \\
\text{Hom}_{\Lambda}(DM, \Lambda)
\end{array}
\rightarrow
\text{Hom}_{\Lambda}(DM, I) 
\rightarrow
[DM, I] 
\rightarrow
0
\]

coming from a) and 4.1.2 shows

\[ NI = \text{Hom}_{\Lambda}(DM, \Lambda)I = \{ f \in \text{Hom}_{\Lambda}(DM, I) \mid f \sim 0 \}. \]

Putting everything 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

\[ H_{2}(G, M) = M_{\Delta} \cong (M_{H})_{0/1} = H_{0}(G|H, M_{H}) \]
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.

**4.7 Remarks.** a) Obviously, 4.6 a) holds for any ring \(A\), while 4.6
b) and c) remain true for any profinite group \(G\) with finitely many topo-
logical generators. More generally, one can show isomorphisms

\[ [DZ_p, \Omega^i M] \cong H_{i+1}(G, M), \quad i \geq 0, \]

under the assumption that \(\Omega^i M\) is finitely generated. This implies 4.6 b)
by an isomorphism \([DZ_p, \Omega M] \cong [DM, I]\), which for finitely generated
\(R^{ab}(p)\) coincides with

\[ [DZ_p, \Omega M] \cong [\Sigma DZ_p, M] \cong [\Omega Z_p, M] \cong [DM, \Omega Z_p]. \]

b) From 4.5.2 and 4.3 we obtain an isomorphism

\[ Z^+ \cong H^2(\mathcal{H}, Q_p/Z_p)^\vee. \]

c) Assume that \(H^2(\mathcal{H}, Q_p/Z_p) = 0\). Then \(pd_A(Y) \leq 1\), and we

can compare 4.5 with the general method 1.9 b) as follows: Choosing a sur-
jection \(P \twoheadrightarrow R^{ab}(p)\) with \(P\) projective we get a commutative exact diagram

\[ 0 \twoheadrightarrow \mathcal{N}/[\mathcal{N}, R](p) \twoheadrightarrow R^{ab}(p) \twoheadrightarrow X \twoheadrightarrow 0 \]

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

\[ \text{Ext}^1_1(D\Sigma\Omega X, E^1(X)) \simeq \text{Ext}^1_1(D\Sigma\Omega^2 I, E^1(X)) \]

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

with \(\alpha\) induced by the Ext-sequence for

\[ 0 \twoheadrightarrow \Omega D\Sigma\Omega^2 I \twoheadrightarrow Q \twoheadrightarrow D\Sigma\Omega^2 I \twoheadrightarrow 0 \]

(\(Q\) projective), and \(\beta\) by the adjunction of \(\Omega\) and \(\Sigma\). One easily checks

that under the composition \(\psi_X\) (from 1.9 b)) is mapped to the same class
as \(\chi = \chi(X)\) (from 4.5 b)) under
Iwasawa Modules

\[ [Y, I] = [DI, DY] = [DI, E'(Y)] \xrightarrow{\gamma} [DI, E'(X)]. \]

If \( E'(A^{ab}(p)) \approx E'(I) \approx E'(Z_p) \) vanishes, then \( \Sigma \Omega A^{ab}(p) \approx A^{ab}(p) \) by 1.10 and thus \( \alpha \) is an isomorphism. If both \( E'(Z_p) \) and \( E'(I) \approx E'(Z_p) \) vanish (e.g., if \( G \) is virtually strict \( p \)-Cohen-Macaulay with \( \vcd_p (G) = n \), then \( \Sigma \mathcal{Q}^2 I \approx I \) and so \( \beta \) is an isomorphism, and \( \gamma \) is an isomorphism by the exact sequence from 4.3

\[ E'(I) \longrightarrow E'(Y) \longrightarrow E'(X) \longrightarrow E'(I). \]

§ 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 \( \mathcal{O}/k \) be a \( p \)-closed Galois extension, i.e., an extension that has no non-trivial \( p \)-extension. For a global field \( k \) let \( S \) be a finite set of places containing those above \( p \cdot \infty \), and let \( \mathcal{O}/k \) be a \((p, S)\)-closed Galois extension, i.e., \( \mathcal{O}/k \) is unramified outside \( S \) (S-ramified) and \( \mathcal{O} \) has no non-trivial \( S \)-ramified \( p \)-extension. Let \( K/k \) be a Galois subextension and set \( \mathcal{G} = \text{Gal}(\mathcal{O}/k) \), \( \mathcal{H} = \text{Gal}(\mathcal{O}/K) \), and \( G = \text{Gal}(K/k) \). For any field \( L \) denote by \( \mu_{\ell}(p) \) the group of \( p \)-power roots of unity in \( L \).

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

5.1 Theorem. Let \( k \) be a finite extension of \( \mathbb{Q}_p \), \( n = [k: \mathbb{Q}_p] \).

a) There is an isomorphism of \( A \)-modules

\[ X = \lim_{L} A(L), \]

where \( L \) runs over all finite extensions \( L/k \), \( L \subseteq K \), and \( A(L) = \lim_{\pi} L^\times/(L^\times)^{\pi^n} \) is the \( p \)-completion of \( L^\times \).

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

\[ E_2^{(p)}(\mathcal{G}) \cong \mu_d(p). \]

c) \( \mathcal{G} \) is generated by \( d = n + 2 \) elements as a profinite group. Let \( \mathcal{G} \rightarrow \mathcal{N}, \mathcal{R}, Y \) etc. be as in §4, with \( d = n + 2 \), then

\[ \mathcal{N}^{ab}(p) \cong Z_p[[\mathcal{G}]]. \]

d) Let \( \sigma_1, \ldots, \sigma_{n+2} \) be topological generators of \( G \), and let \( a_i \in Z_p \) with \( \sigma_i(\zeta) = \zeta^{a_i} \) for all \( \zeta \in \mu_k(p) \), \( i = 1, \ldots, n+2 \). Then there is an exact sequence
\[0 \rightarrow A \rightarrow A^{n+2} \rightarrow Y \rightarrow 0\]

\[1 \rightarrow (\sigma_1 - \mu_1, \ldots, \sigma_{n+2} - \mu_{n+2})\]

(5.1.1)

\(e) \ X \text{ is determined up to isomorphism by } A_{\mathbb{K}}(p) \text{ and the image of } H^2(\mathcal{G}, \mu_\mathcal{O}(p)) \rightarrow H^2(G, \mu_\mathcal{O}(p))^*\).

**Proof.**  
\(\text{a) is clear from class field theory.}\)

\(\text{b) If } A \text{ is a } p\text{-torsion } \mathcal{G}\text{-module, then the inflation}\)

\[(5.1.2) \quad H(\mathcal{G}, A) \rightarrow H(k, A)\]

\(\text{is an isomorphism for all } r \geq 0, \text{ since } \text{cd}_p(\text{Gal}(\overline{k}/\Omega)) \leq 1 \text{ for an algebraic}\)

\(\text{closure } \overline{k} \text{ of } k \text{ (same argument as in [S1] II 5.6). The first two claims thus}\)

\(\text{follow from the fact that } \text{scd}_p(\text{Gal}(\overline{k}/k)) = 2 \text{ (loc. cit. 5.3). Applying 5.1.2}\)

\(\text{to a finite extension } L/k, \ L \subseteq \Omega, \text{ we get an isomorphism}\)

\[H^2(\text{Gal}(\Omega/L), Z/p^m)^* \cong H^2(L, Z/p^m)^* \cong \mu_{L, p^m},\]

\(\text{with the group of } p^m\text{-th roots of unity in } L, \text{ by Tate's local duality theorem}\)

\(\text{(loc. cit. 5.2). By passing to the limit over } m \text{ and } L \text{ we obtain the last claim.}\)

\(\text{c) This follows from [J1] 3.1 and 3.2. Note that it suffices to prove}\)

\(N'/N, \mathcal{A}(p) \cong Z_p[G] \text{ in the case of finite } G, \text{ since two pseudocompact}\)

\(Z_p[[\mathcal{G}]]\text{-modules } M \text{ and } M', \text{ with } M \text{ finitely generated, are isomorphic if}\)

\(M_\mathcal{G} \cong M'_\mathcal{G} \text{ for every open normal subgroup } \mathcal{G} \text{ of } \mathcal{G} \text{ (use that an inverse}\)

\(\text{limit of non-empty compact sets is non-empty). By Swan's theorem (see}\)

\(\text{[S3] 16.1 Corollary 2) and the projectivity of } N'^{ab}(p) \text{ it suffices to show the}\)

\(\text{above isomorphism after tensoring with } Q_p, \text{ which follows from [J1] 3.1}\)

\(\text{and 4.3 above, together with the vanishing of } H^2(\mathcal{H}, Q_p/Z_p).\)

\(\text{d) With the notations of §4 we have } W = \mu_{\mathcal{K}}(p) \text{ and } Z = \mu_{\mathcal{K}}(p)^\vee.\)

\(\text{Since } Y \cong DZ \text{ and } H^2(\mathcal{H}, Q_p/Z_p) = 0, \text{ we immediately get 5.1.1 from transposing}\)

\(\text{the exact sequence}\)

\[(5.1.3) \quad A^{n+2} \rightarrow A \rightarrow \mu_{\mathcal{K}}(p)^\vee \rightarrow 0\]

\[e_i \rightarrow \sigma_i - a_i^{-1}\]

\(\text{where } \{e_1\}_{i=1}^{n+2} \text{ is a basis of } A^{n+2} \text{ and } \rho \text{ sends } 1 \text{ to a generator of } \mu_{\mathcal{K}}(p)^\vee\)

\(\text{(given the left action of } G, \text{ once we have shown that } (\mu_{\mathcal{K}}(p)^\vee)_U = 0. \text{ This is}\)

\(\text{clear, because } (\mu_{\mathcal{K}}(p)^\vee)_U \text{ is finite for every open normal subgroup } U \text{ of } G.\)

\(\text{e) This is clear from 4.5 b) and d), since } \chi_0 \text{ generates the pro-cyclic}\)

\(\text{group } H^2(\mathcal{G}, \mu_\mathcal{O}(p))^* \cong \text{End } (\mu_\mathcal{O}(p)) \text{ and any two generators differ bymul-}
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

\[
\xymatrix{
H^2(G, \mu_k(p)) \ar[r]^-{\inf} & H^2(G, \Omega^\times) \\
\hat{H}^0(G, \mu_k(p)) \ar[r] & \hat{H}^0(G, K^\times) \ar[u] \ar[r]^-{\inf} & H^2(G, K^\times)
}
\]

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

b) If \( \text{cd}_p(G) \leq 1 \), then \( I \) is projective (cf. [Br] 5.1), hence \( Y \cong X \oplus I \), and in particular, \( X \cong D(\mu_k(p)^\vee) \) has projective dimension \( \leq 1 \) and is determined by \( E^1(X) \cong \mu_k(p)^\vee \). For example, assume that \( G \cong \mathbb{Z}_p \times A \) with a finite group \( A, p \nmid |A| : 1 \), 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

\[
0 \rightarrow X \rightarrow \Lambda^n \rightarrow \mu_k(p) \rightarrow 0.
\]

(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 \( U \cong \mathbb{Z}_p^n \), with \( p \nmid |U| : U \), and if \( \mu_k(p) \) is infinite, then \( H^2(G, \mu_k(p))^\ast \cong \text{Hom}_\sigma(\mu_k(p), \mathbb{Q}_p/Z_p) = 0 \), and one easily shows \( \mathfrak{g}^{ab}(p) \cong \Lambda^{d-1} \). Thus

\[
X \oplus \Lambda \cong Y
\]

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

\[
0 \rightarrow \Lambda \rightarrow \Lambda^2 \rightarrow M' \rightarrow 0
\]

\[
1 \rightarrow (\sigma - \chi(\sigma), \tau - \chi(\tau))
\]

with \( \sigma, \tau \) generators of \( G \) and \( \chi : G \rightarrow \mathbb{Z}_p^\times \) the cyclotomic character.

d) If \( G \) is a \( p \)-adic Lie group, then the methods of [S2] sometimes show that \( H^2(G, \mu_k(p)) \) is finite. In this case there is an injection

\[
X \oplus \Lambda^d \rightarrow \mathfrak{g}^{ab}(p) \oplus Y
\]
with cokernel of finite exponent.

Now let $k$ be a finite extension of $Q$, and let $\mathcal{O}$ be as above. Let $k_S$ be the maximal $S$-ramified extension of $k$, and set $\mathcal{H}_S = \text{Gal}(k_S/k)$, $\mathcal{H}_S^p = \text{Gal}(k_S^p/K)$. Then $X = X_S = \mathcal{H}_S^{ab}(p) = \mathcal{H}_S^{ab}(p)$ 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 $\text{cd}_p (\mathcal{H}) \leq 2$.

b) If an open subgroup of $\mathcal{H}$ is a pro-$p$-group, then $\mathcal{H}$ is finitely generated as a profinite group.

Proof. a) For a $p$-torsion $\mathcal{H}$-module $A$ the inflation

\[
(5.3.1) \quad H^r(\mathcal{H}, A) \rightarrow H^r(\mathcal{H}_S, A)
\]

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 $\text{cd}_p (\mathcal{H}) \leq 2$ and that $\mathcal{H}$ has finitely many topological generators. Let — for a suitable $d - \mathcal{F}$, $\mathcal{R}$ and $\mathcal{N}$ be chosen as in § 4, and let $Y = Y_s = I(\mathcal{H})_s$ as in 4.2. It is easy to see that $Y \cong I(\mathcal{H}_S)_s$, in particular this $\Lambda$-module only depends on $K$ and $S$, and by 4.3 we have a diagram of $\Lambda$-modules

\[
\begin{array}{ccc}
0 & \rightarrow & H_\ast(\mathcal{H}_S, Z_p) \rightarrow \mathcal{N} \rightarrow \mathcal{R}(p) \rightarrow \Lambda \rightarrow Y_s \rightarrow 0 \\
0 & \rightarrow & H_\ast(\mathcal{H}_S, Z_p) \rightarrow \mathcal{N} \rightarrow \mathcal{R}(p) \rightarrow \mathcal{R}^{ab}(p) \rightarrow X_s \rightarrow 0,
\end{array}
\]

since $H_\ast(\mathcal{H}_S, Z_p) = H_\ast(\mathcal{H}_S, \mathcal{Q}_p/Z_p) \cong H_\ast(\mathcal{H}, \mathcal{Q}_p/Z_p)$ by the argument of 5.3 a). Here $I$ and $\mathcal{R}^{ab}(p)$ 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 $H_\ast(\mathcal{H}_S, \mathcal{Q}_p/Z_p)$ 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 $Z_p$-extension of $k$ (cf. [Sch] 4.7).

Let $X_S = \text{Gal}(L/K)$ and $X_S = \text{Gal}(L'/K)$ 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 $S_j(K)$ be the set of finite primes in $K$ lying above $S$, and for $\mathfrak{P} \in S_j(K)$ let $K_\mathfrak{P}$ be the completion of $K$ at $\mathfrak{P}$. Then define
Iwasawa Modules

\[ A = A_S = \prod_{\mathfrak{p} \in S_f(K)} A_{\mathfrak{p}}, \]
\[ U = U_S = \prod_{\mathfrak{p} \in S_f(K)} U_{\mathfrak{p}}, \]
where \( A_{\mathfrak{p}} \) (resp. \( U_{\mathfrak{p}} \)) is the \( p \)-completion 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
\[ E = E_K = \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p, \]
\[ E_S = E_{S, K} = \mathcal{O}_S^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p. \]

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 \( L/k, L \subseteq K \).

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

**5.4 Theorem.**

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

\[
\begin{array}{ccccccc}
0 & \rightarrow & H^2(\mathcal{G}_S, Q_p/\mathbb{Z}_p) & \rightarrow & E & \rightarrow & X_S & \rightarrow & X_2 & \rightarrow & 0 \\
0 & \rightarrow & H^2(\mathcal{G}_S, Q_p/\mathbb{Z}_p) & \rightarrow & E_S & \rightarrow & X_S & \rightarrow & X_2 & \rightarrow & 0 \\
\end{array}
\]

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

\[ N'(N, \mathcal{G})(p) \cong \bigoplus_{v \in S_\infty} \Lambda_{(\mathcal{O}_v)} \otimes \Lambda^d - r_1' - r_2 - 1. \]

Here \( S'_{\infty} \) is the set of real places of \( k \) which ramify (i.e., become complex) in \( K \), \( r_1' \) is the cardinality of \( S'_{\infty} \), 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 \( \Lambda_{(\mathcal{O}_v)} = \Lambda/\Lambda(\sigma_v - 1) \) is the module of coinvariants for the right \( G_v \)-module structure of \( \Lambda \), regarded as a left \( \Lambda \)-module.

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

\[
0 \rightarrow \mu(p) \rightarrow \bigoplus_{\mathfrak{p} \in S_f} \text{Ind}^\mathcal{G}_{\mathfrak{p}}(\mu(p)) \rightarrow E^{[p]}(\mathcal{G}) \rightarrow 0
\]

where, for each \( \mathfrak{p} \in S_f = S_f(K), \mathfrak{G}_\mathfrak{p} \) is a decomposition group at \( \mathfrak{p} \) in \( \mathcal{G} \), \( \text{Ind}^\mathcal{G}_{\mathfrak{p}} \) means induction from \( \mathfrak{G}_\mathfrak{p} \) to \( \mathcal{G} \), \( \mu(p) \) is the \( \mathcal{G} \)-module of \( p \)-power roots of unity in an algebraic closure \( \overline{Q} \) of \( Q \), and \( \iota \) is the natural map.
Let $W = W_8 = E_{iP}(\mathcal{G})^{\infty}$ and $Z = Z_8 = W_8'$ so that $Y_8 \simeq DZ_8$ by 4.5 a). Then $W_8 \simeq E_{iP}(\mathcal{G})^{\infty}$, in particular, $W_8$ and $Z_8$ only depend on $K$ and $S$. There is an exact sequence

$$0 \to \mu_K(p) \to \bigoplus_{\mathfrak{p} \in S_f} \text{Ind}^G_{\mathbb{G}_m}(\mu_{K_\mathfrak{p}}(p)) \to W_8 \to H^1(\mathcal{H}_S, \mu(p)) \to 0$$

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

$$0 \to X(1) \to Z_8 \to \bigoplus_{\mathfrak{p} \in S_f} \mathbb{A} \otimes_{A_{G_\mathfrak{p}}} Z_p(-1) \to Z_p(-1) \to 0,$$

where $Z_p(1) = \lim_m \mu_{p^m}$, and $X(1) = X(1) \otimes_{\mathbb{Z}_p} Z_p(-1)$ for $Z_p(-1) = \text{Hom}_{\mathbb{Z}_p}(Z_p(1), Z_p)$ is the usual Tate twist of $X_8$.

**Proof.** 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

$$0 \to H^1(\mathcal{H}_S, \mathbb{Q}_p/Z_p)^\vee \to H^1(\mathcal{H}_S, Z_p(1)) \to \bigoplus_{\mathfrak{p} \in S_f(K)} H^1(K_\mathfrak{p}, Z_p(1)) \to H^1(\mathcal{H}_S, \mathbb{Q}_p/Z_p)^\vee \to \text{Gal}(L'/K) \to 0 \to 0$$

coming from Tate's duality theorem ([Ta] 3.1, compare [Sch] 2.5) and the fact that $H^1(K_\mathfrak{p}, \mathbb{Q}/Z_p) = 0$; here $H^1(-, Z_p(1)) = \lim H^1(-, \mu_{p^m})$. 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 $H^2(\mathcal{H}_S, \mathbb{Q}_p/Z_p)^\vee$ is taken via the duals of the restriction maps (cf. [Mi] I 4.19).

b) We already know that $\mathcal{N}/[\mathcal{N}, \mathcal{R}](p)$ is a projective $A$-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 $\mathcal{N}/[\mathcal{N}, \mathcal{R}](p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. From a) we get the equality

$$[\mathcal{N}/[\mathcal{N}, \mathcal{R}](p) \otimes \mathbb{Q}_p] = [\mathcal{R}^{ab}(p) \otimes \mathcal{Q}] + [H^2(\mathcal{H}_S, \mathbb{Q}_p/Z_p)^\vee \otimes \mathbb{Q}_p] - [X_8 \otimes \mathbb{Q}_p]$$

in the Grothendieck group $K_0(\mathbb{Q}_p[G])$ of finitely generated $\mathbb{Q}_p[G]$-modules,
[A] denoting the class of such a module $A$. From a) we have

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

and we may proceed as in [J1].

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

$$0 \rightarrow \mu_k(p) \rightarrow \bigoplus_{\Psi \in S_f(K)} \mu_{K_p}(p) \rightarrow H^2(\mathcal{A}_s, \mathbb{Z}_p)^\vee$$

$$\rightarrow H^1(\mathcal{A}_s, \mu(p)) \rightarrow \bigoplus_{\Psi \in S_f(K)} H^1(K_p, \mu(p)).$$

(5.4.3)

By passing to the direct limit over all finite layers $K/k$ contained in $\Omega/k$ we obtain the result, since for $H^2(\mathcal{A}_s, \mathbb{Z}_p)^\vee = \lim_m H^2(\mathcal{A}_p, \mathbb{Z}/p^m)^\vee = \lim_m H^2(\mathcal{A}, \mathbb{Z}/p^m)^\vee$ the limit is taken via the duals of the corestrictions, while for $H^1(\mathcal{A}_s, \mu(p)) \cong H^1(\mathcal{A}, \mu(p))$ 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 $\mathcal{A}_s$-cohomology of a similar sequence for $E^i_p(\mathcal{A}_s)$ as the one for $E^i_p(\mathcal{A})$ in c). The second sequence is obtained by taking the Pontrjagin dual of the first one. Finally we immediately obtain $E^i_2(\mathcal{A}) \cong E^i_3(\mathcal{A}_s)^{(2n/3)}$ 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 $I(G) \cong A$. Hence $Y \cong X \oplus A$, and in particular, $X \cong DZ$ 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 $H^2(\mathcal{A}, \mathbb{Q}_p / \mathbb{Z}_p) = 0$. If $cd_p(G) \leq 3$, then $pd_d(X) \leq 1$ (since $pd_d(R^{ab}(p)) \leq 1$, cf. [Br] 4.4, and hence $0 \cong \Omega R^{ab}(p) \cong \Omega X$, cf. 4.7 c)). Thus $X \cong DE^i(X)$ by Theorem 1.6, and by the arguments in 4.5 d) $X$ is determined up to isomorphism by $E^i(X)$. By 4.3 we have an exact sequence

$$E^i(I) \rightarrow E^i(Y) \rightarrow E^i(X) \rightarrow E^i(I) \rightarrow 0.$$

If $cd_p(G) = 2$, then $E^i(X)$ is the cokernel of $E^i_2(G)^{\vee} = E^3(Z_p) \rightarrow Z$, and, in fact this map is just the element $\chi \in H^2(G, W)^{\vee} \cong \text{Hom}_G(W, E^3(G)) \cong \text{Hom}_G(E^3(Z_p), Z)$. For example, if $G \cong Z_p^2$, then $E^3(Z_p) \cong Z_p$, and the map corresponds to an element in $Z^q \cong \text{Hom}_G(W, Q_p / Z_p)$. If $k$ is global and $\mu_k(p)$ is infinite, then the second exact sequence in 5.4 d) shows $Z^q \cong$
If \( \text{cd}_p(G) = 3 \) and \( G \) is strict \( p \)-Cohen-Macaulay, then we obtain an exact sequence

\[
0 \rightarrow \mathbb{Z} \rightarrow E^1(X) \rightarrow E^3(\mathbb{Z}_p) \rightarrow 0,
\]
whose extension class now is given by the element \( \chi \in H^3(G, W)^\vee \cong H^1_{\text{cont}}(G, \text{Hom}(W, E^3_p(G))) \cong H^1_{\text{cont}}(G, \text{Hom}(E^3(\mathbb{Z}_p), \mathbb{Z})). \)

c) The invariant \( \chi \in H^3(G, W)^\vee \) is zero if and only if every \( p \)-embedding problem is solvable for \( K/k \), i.e., if every diagram with exact row

\[
0 \rightarrow A \rightarrow E^0 \rightarrow G \rightarrow 1,
\]
with finite abelian \( p \)-group \( A \), can be completed by a homomorphism \( s: G \rightarrow E \) with \( \rho s = \pi \). This follows from the injection

\[
H^2(G, A) \rightarrow \prod_{\rho \in \text{Hom}_{\mathbb{Z}_p}(A, E^3_p)} H^2(G, E^3_p(\rho)),
\]
by the same arguments as in [JW].

5.6 Remark. In this and the following sections it is convenient to give all modules the left Galois module structures. In view of the discussion in 2.7 b) this means that \( C^\vee = \text{Hom}_{\text{cont}}(C, \mathbb{Q}_p/\mathbb{Z}_p) \), \( \text{Hom}_{\mathbb{Z}_p}(C, D) \) etc. have the action given by \( (af)(c) = af(\sigma^{-1}c) \), only then Tate's sequences 5.4.2, 5.4.3 are Galois equivariant. 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

\[
0 \rightarrow X_5(-1) \overset{\alpha_1}{\rightarrow} Z^5 \overset{\alpha_2}{\rightarrow} \bigoplus_{p \in \mathcal{S}_f} \text{Ind}_{\mathcal{G}_p}(Z_p(-1)) \overset{\alpha_3}{\rightarrow} Z_p(-1) \rightarrow 0.
\]

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
induced from the exact sequence

\[ 0 \rightarrow E_s \rightarrow A \rightarrow X_s \rightarrow X_3 \rightarrow 0. \]

**Proof.** Splitting the latter sequence into two short ones

\[ 0 \rightarrow E_s \rightarrow A \rightarrow B \rightarrow 0 \]

\[ 0 \rightarrow B \rightarrow X_s \rightarrow X_3 \rightarrow 0, \]

we get a commutative exact diagram

\[
\begin{array}{c}
E'(X_s) \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
E'(X_s) \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
E'(E_s)
\end{array}
\]

(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), \( \beta \) can be identified with the map \( \alpha_2 \) in 6.1. On the other hand, by the well-known local theory (compare 5.2 b)) we have

\[ A \cong T_1(A) \oplus A^{[k:Q]}, \quad T_1(A) \cong \bigoplus_{v \in \mathcal{S}_f} \text{Ind}^g_v(Z_p(1)). \]

Hence we get a commutative diagram

\[
\begin{array}{c}
\vdash \end{array}
\]
in which \( E_1(E_8) \to E_1(T_1(E_8)) \) and \( E_1(E_8) \to E_1(Z_p(1)) \) are surjective, since \( E_2(M/T_1(M)) = 0 \) for any \( A \)-module and \( E_2(E_8/Z_p(1)) = 0 \), since \( E_8/Z_p(1) \) 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.

\( E_8 \cong \bigoplus_{v \in S_\infty} A_{(G_v)} \oplus Z_p(1) \), where \( S_\infty \) 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, \( T_1(E_8) = Z_p(1) \).

**Proof.** The exact sequence

\[
0 = Z_p(1) \to E_1(E_8/Z_p(1)) \to E_1(E_8) \to E_1(Z_p(1))
\]

shows \( E_1(E_8/Z_p(1)) = 0 \). Since on the other hand \( \text{pd}_{A}(E_8/Z_p(1)) \leq 1 \), because this module does not contain any non-trivial finite submodule, we deduce from Theorem 1.6 that \( E_8/Z_p(1) \) is projective. Its isomorphism class is easily computed by the methods already used in the proof of 5.4 b), by computing \( E_8 \otimes Q_p \) for finite intermediate layers.

### 6.4 Corollary.

There is an exact sequence

\[
0 \to T_1(E_8) \to T_1(A_8) \to T_1(X_8) \to E_1(X_8(-1)) \to 0,
\]

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

\[
0 \to \bigoplus_{v \in T \setminus S} \text{Ind}_{G_v}^{G} (Z_p(1)) \to T_1(X_T) \to T_1(X_S) \to 0.
\]

**Proof.** Define \( Z'_S \) by the exact sequence

\[
0 \to Z_p(1) \to T_1(A_8) \to T_1(X_8) \to Z'_S \to 0.
\]

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

\[
0 \to E_1(Z'_S) \to E_1(T_1(X_8)) \to E_1(R) \to E_2(Z'_S) \to 0
\]

(6.4.1)

\[
E_1(T_1(X_8)) \to E_1(T_1(A)) \to E_1(Z_p(1)) \to 0
\]

\[
E_1(Z_p(1))
\]
where we have used the facts that $R^+ = 0 = Z_p(1)^+$ (since these are $A$-torsion modules) and $0 = E^2(T_1(X_S)) \rightarrow E^2(R)$. 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 $E^1(A) \simeq E^1(T_1(A))$ is torsion-free, a comparison of 6.4.1 with 6.2 now shows

$$E^1(Z'_S) \simeq X_0(-1)/T_0(X_S(-1)),$$

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

In particular, $\text{pd}_A(Z'_S) \leq 1$, and $Z'_S \simeq E^1(E^1(Z'_S))$ 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

$$Z'_S \simeq E^1(X_S(-1)/T_0(X_S(-1))) \simeq E^1(X_S(-1)),$$

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

$$0 \rightarrow \bigoplus_{\nu \in T_1 S} \text{Ind}_{\sigma^\nu}^S((1)) \rightarrow T_1(A_T) \rightarrow T_1(A_S) \rightarrow 0.$$

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

6.5 Corollary. a) $E^0(X_S) = \bigoplus_{\sigma \in S^\infty} A(\sigma)$, where $S^\infty$ is the set of complex archimedean places of $k$, $E^1(X_S) = Z_S$, $E^2(X_S) = 0$.

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

c) $T_0(X_0) \cong \lim_n H^1(G_n, S(K)), \text{ where } G_n = \text{Gal}(K/k(\mu_{p^n+1})), S(K) = \sigma^\nu_0, k$ 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 $X_S \cong DZ_S$, except for the claim in c). For this let $k_n = k(\mu_{p^n+1})$ and let $\text{Cl}_S(k_n)$ (resp. $\text{Cl}_S(K)$) be the $S$-class group of $k_n$ (resp. $K$). There is a well-known commutative diagram of finite groups

$$0 \rightarrow H^1(G_{n+1}, S(K)) \rightarrow \text{Cl}_S(k_{n+1}) \rightarrow \text{Cl}_S(K)^{\sigma_{n+1}}$$

$$0 \rightarrow H^1(G_n, S(K)) \rightarrow \text{Cl}_S(k_n) \rightarrow \text{Cl}_S(K)^{\sigma_n},$$

where cor is the corestriction, $N$ the norm, and $\text{tr}$ the trace of $G_n/G_{n+1}$. By passing to the inverse limit over $n$ we obtain an exact sequence of $G$-modules
Now \( \lim_n H^1(G_n, \mathcal{O}_G(K)) \) is finite, since the order of \( H^1(G_n, \mathcal{O}_G(K)) \) 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 \( A \cong 0 \) one has \( A^{G_0} \cong 0 \). But

\[
\left( \lim_n \operatorname{Cl}_G(K)^{G_0} \right) = \lim_n \operatorname{Cl}_G(K)^{G_0},
\]

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

6.6 Example. There is an exact sequence

\[
0 \to E^1(Z_G) \to X_S \to \bigoplus_{v \in S} A_{G_v} \to \operatorname{Hom}(\lim_n H^1(G_n, \mathcal{O}_G(K)), \mu(p)) \to 0.
\]

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

References


[Se] 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)).


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

Universität Regensburg
NWF I — Mathematik
Universitätsstraße 31
D-8400 Regensburg
West Germany