Winter School on Galois Theory
Luxembourg, 15 - 24 February 2012

INTRODUCTION TO PROFINITE GROUPS

Luis Ribes
Carleton University, Ottawa, Canada

LECTURE 3

3.1 G-MODULES

Let G be a profinite group. A *left G-module* or simply a *G-module* is a topological abelian group M on which G operates continuously. Specifically, a G-module is a topological abelian group M together with a continuous map $G \times M \to M$, denoted by $(g, a) \mapsto ga$, satisfying the following conditions

(i) $$(gh)a = g(ha),$$

(ii) $$g(a + b) = ga + gb,$$

(iii) $$1a = a,$$

for $a, b \in M$ and $g, h \in G$, where 1 is the identity of G.

If the topology of M is discrete, then M is called a *discrete G-module*; and if the topology of M is profinite, we say that M is a *profinite G-module. Right G-modules* are defined analogously.

The following lemma is proved easily.

3.1.1 Lemma *Let G be a profinite group and let M be a discrete abelian group. Let $G \times M \longrightarrow M$ be an action of G on M satisfying conditions* (i), (ii), (iii) *as above. Then, the following are equivalent:*

(a) *$G \times M \longrightarrow M$ is continuous;*

(b) *For each a in M, the stabilizer,*
$$G_a = \{g \in G \mid ga = a\}$$
of a is an open subgroup of G;

(c)
$$M = \bigcup_U M^U,$$
where U runs through the set of all open subgroups of G, and where
$$M^U = \{a \in M \mid ua = a,\ u \in U\},$$
is the subgroup of fixed points of M under the action of U.

3.1..2 Examples of Discrete G-modules.

(1) Let G be any profinite group and M any discrete abelian group. Define an action of G on M by $ga = a$, for all $a \in M$ and $g \in G$. Then M is a discrete G-module. This action is called the *trivial action* on M, and we refer to M with this action as a *trivial G-module*.

(2) Let N/K be a Galois extension of fields and $G = G_{N/K}$ its Galois group. For $\sigma \in G$ and $x \in N$, define $\sigma x = \sigma(x)$. Under this action the following are examples of discrete G-modules:

   (2a) $N^\times$ (the multiplicative group of N);

   (2b) N^+ (the additive group of N);

   (2c) The roots of unity in N (under multiplication).

NOTE that with the exception of (2c), the examples above are not torsion abelian groups.

Let M and N be G-modules. A *G-morphism*$\varphi : A \longrightarrow B$ is a continuous G-homomorphism, i.e., an abelian group homomorphism for which

$$\varphi(ga) = g\varphi(a), \quad \text{for all } g \in G, a \in M.$$

The class of G-modules and G-morphisms constitutes an abelian category which we denote by $\mathbf{Mod}(G)$. The profinite G-modules form an abelian subcategory of $\mathbf{Mod}(G)$, denoted $\mathbf{PMod}(G)$, while the discrete

G-modules form an abelian subcategory denoted $\mathbf{DMod}(G)$. In turn, the discrete torsion G-modules form a subcategory of $\mathbf{DMod}(G)$.

3.2 THE COMPLETE GROUP ALGEBRA

Consider a commutative profinite ring R (for example $R = \hat{\mathbf{Z}}$) and a profinite group H. We denote the usual abstract group algebra (or group ring) by $[RH]$. Recall that it consists of all formal sums $\sum_{h\in H} r_h h$ ($r_h \in R$), where r_h is zero for all but a finite number of indices $h \in H$), with natural addition and multiplication. As an abstract R-module, $[RH]$ is free on the set H.

Assume that H is a finite group. Then $[RH]$ is (as a set) a direct product $[RH] \cong \prod_H R$ of $|H|$ copies of R. If we impose on $[RH]$ the product topology, then $[RH]$ becomes a topological ring, in fact a profinite ring (since this topology is compact, Hausdorff and totally disconnected). Suppose now that G is a profinite group. Define the *complete group algebra* to be the inverse limit

$$[\![RG]\!] = \varprojlim_{U\in\mathcal{U}} [R(G/U)]$$

of the ordinary group algebras $[R(G/U)]$, where $\mathcal{U}$ is the collection of all open normal subgroups of G.

NOTATION: $\mathbf{DMod}([\![RG]\!])$ Is the category of discrete $[\![RG]\!]$-modules and continuous module homomorphisms $\mathbf{PMod}([\![RG]\!])$ Is the category of profinite $[\![RG]\!]$-modules (and continuous module homomorphisms).

Duality Between Discrete and Profinite Modules

Put $\Lambda = [\![RG]\!]$. Given a Λ-module M (discrete or profinite), consider the abelian group

$$M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$$

of all continuous homomorphism from M to $\mathbf{Q}/\mathbf{Z}$ (as abelian groups) with the compact open topology. Then M^* is profinite if M discrete torsion, and it is discrete torsion if M is profinite. Define a right action of Λ on M^* by $(\varphi\Lambda)(m) = \varphi(\Lambda m)$. This action is continuous and so M^* becomes a right that the contravariant functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$ establishes a "duality" between the categories $\mathbf{PMod}(\Lambda)$ and $\mathbf{DMod}(\Lambda^{op})$. In our context duality can be described as follows: every (elementary) statement, definition, theorem, etc., that one makes in either the category $\mathbf{PMod}(\Lambda)$ or $\mathbf{DMod}(\Lambda^{op})$ involving modules and morphisms (that we represent by arrows), can be translated into a dual statement, definition, theorem, etc. in the other category by applying the functor $\mathrm{Hom}(-, \mathbf{Q}/\mathbf{Z})$, i.e., replacing each module M by $\mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ and reversing the arrows; if a statement, theorem, etc., holds in one of these categories, then the dual statement, theorem, etc. holds true in the other category.

3.2.1 Proposition *Let G be a profinite group and R a commutative profinite ring.*

(a) *Every $[\![RG]\!]$-module is naturally a G-module.*

(b) *Every profinite abelian group and every discrete torsion abelian group has a unique $\widehat{\mathbf{Z}}$-module structure.*

(c) *Profinite G-modules coincide with profinite $[\![\widehat{\mathbf{Z}}G]\!]$-modules.*

(d) *If A is both a G-module and an R-module with commuting actions (i.e., if $r \in R$, $g \in G$ and $a \in A$, then $r(ga) = g(ra)$), then A is in a natural way an $[\![RG]\!]$-module.*

(e) *The category $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$ coincides with the subcategory of $\mathbf{DMod}(G)$ consisting of the discrete torsion G-modules.*

Proof. The most interesting part is (e): Put $\Lambda = [\![RG]\!]$. Let M be discrete and let $m \in M$. Since there exists a fundamental system of neighborhoods of 0 in Λ consisting of open ideals of Λ, there is an open ideal T of Λ such that $Tm = 0$; therefore, Λm is a submodule with finitely many elements. Thus (e) follows. □

3.3 PROJECTIVE AND INJECTIVE MODULES

Let $\mathcal{A}$ be a category. An object P in $\mathcal{A}$ is called *projective* if for every diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow{\scriptstyle\varphi} \\ B & \xrightarrow{\alpha} & A \end{array}$$

of objects and morphisms in $\mathcal{A}$, where α is an epimorphism, there exists a morphism $\beta : P \longrightarrow B$ making the diagram commutative, i.e., $\alpha\beta = \varphi$. We refer to β as a *lifting* (of φ). If $\mathcal{A}$ is an abelian category, one has equivalently, that P is projective in $\mathcal{A}$ if the functor $\mathrm{Hom}(P, -)$ is exact, i.e., whenever

$$0 \longrightarrow C \longrightarrow B \longrightarrow A \longrightarrow 0$$

is an exact sequence in $\mathcal{A}$, so is the corresponding sequence

$$0 \longrightarrow \mathrm{Hom}(P, C) \longrightarrow \mathrm{Hom}(P, B) \longrightarrow \mathrm{Hom}(P, A) \longrightarrow 0$$

of abelian groups.

One says that a category $\mathcal{A}$ has *enough projectives* if for every object M in $\mathcal{A}$, there exists a projective object P of $\mathcal{A}$ and an epimorphism $P \longrightarrow M$.

3.3.1 Proposition *Let* $\Lambda = [\![RG]\!]$.

(a) *Every free profinite* Λ*-module is projective in the category* $\mathbf{PMod}(\Lambda)$ *of all profinite* Λ*-modules.*

(b) *The category* $\mathbf{PMod}(\Lambda)$ *has enough projectives.*

(c) *The projective objects in* $\mathbf{PMod}(\Lambda)$ *are precisely the direct summands of free profinite* Λ*-modules.*

The dual concept of a projective object in a category $\mathcal{A}$ is that of an injective object. An object Q in $\mathcal{A}$ is called *injective* if whenever

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\varphi}\downarrow & & \\ Q & & \end{array}$$

is a diagram of objects and morphisms in $\mathcal{A}$, where α is a monomorphism, there exists a morphism $\bar{\varphi} : B \longrightarrow Q$ making the diagram commutative, i.e., $\bar{\varphi}\alpha = \varphi$. We refer to $\bar{\varphi}$ as an *extension* of φ. If $\mathcal{A}$ is an abelian category, one has equivalently, that Q is injective in $\mathcal{A}$ if the functor $\mathrm{Hom}(-, Q)$ is exact, i.e., whenever

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence in $\mathcal{A}$, so is the corresponding sequence

$$0 \longrightarrow \mathrm{Hom}(C, Q) \longrightarrow \mathrm{Hom}(B, Q) \longrightarrow \mathrm{Hom}(A, Q) \longrightarrow 0$$

of abelian groups.

One says a category $\mathcal{A}$ has *enough injectives* if for every object M in $\mathcal{A}$, there exists an injective object Q of $\mathcal{A}$ and a monomorphism $M \longrightarrow Q$.

An object M in $\mathbf{DMod}(\Lambda)$ is called *cofree* if it satifies a universal property dual to that of free objets, i.e., if its dual M^* is free in $\mathbf{PMod}(\Lambda)$. Applying duality, Proposition 3.3.1 yields

3.3.2 Proposition *Let* $\Lambda = [\![RG]\!]$.

(a) *Every cofree discrete* Λ*-module is injective in the category* $\mathbf{DMod}(\Lambda)$ *of all discrete* Λ*-modules.*

(b) *The category* **DMod**(Λ) *has enough injectives.*

(c) *The injective objects in* **DMod**(Λ) *are precisely the direct factors of cofree discrete* Λ*-modules.*

Let G be a profinite group. Next we show that the category **DMod**(G) of discrete G-modules also has enough injectives. As we indicated in Proposition 3.2.1, **DMod**$([\![\widehat{\mathbf{Z}}G]\!])$ is the subcategory of **DMod**(G) consisting of those modules that are torsion.

3.3.3 Proposition *Let G be a profinite group. Then* **DMod**(G) *has enough injectives, i.e., for every $A \in$* **DMod**(G)*, there exists a monomorphism*

$$A \longrightarrow M_A$$

in **DMod**(G) *with M_A injective.*

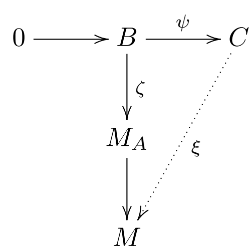
Proof. Denote by G_0 the abstract group underlying G. Let A be a discrete G-module; then obviously $A \in$ **Mod**(G_0), the category of abstract G_0-modules. It is well known that **Mod**(G_0) has enough injectives. Let

$$0 \longrightarrow A \stackrel{\varphi}{\longrightarrow} M$$

be an exact sequence in **Mod**(G_0), with M injective in **Mod**(G_0). Define

$$M_A = \bigcup_U M^U,$$

where U runs through all open normal subgroups of G. Clearly $M_A \in$ **DMod**(G). Let $a \in A$, and let U be an open normal subgroup of G such that $a \in A^U$. Then $\varphi(a) \in M^U$. Hence $\varphi(A) \subseteq M_A$. Finally M_A is injective in **DMod**(G) because any diagram



where ψ, ζ are mappings in **DMod**(G), with ψ a monomorphism, can be completed to a commutative diagram by a G_0-homomorphism $\xi : C \longrightarrow M$. However, since C is a discrete G-module, one has $\xi(C) \subseteq M_A$. □

3.4 COMPLETE TENSOR PRODUCT

Let $\Lambda = [\![RG]\!]$. Let A be a profinite right Λ-module, B a profinite left Λ-module, and M an R-module. A continuous map

$$\varphi : A \times B \longrightarrow M$$

is called *middle linear* if $\varphi(a+a', b) = \varphi(a, b)+\varphi(a', b)$, $\varphi(a, b+b') = \varphi(a, b)+\varphi(a, b')$ and $\varphi(a\lambda, b) = \varphi(a, \lambda b)$ for all $a, a' \in A,\ b, b' \in B,\ \lambda \in \Lambda$.

We say that a profinite R-module T together with a middle linear map $A \times B \longrightarrow T$, denoted $(a, b) \mapsto a\widehat{\otimes}b$, is a *complete tensor product* of A and B over Λ if the following universal property is satisfied:

If M is a profinite R-module and $\varphi : A \times B \longrightarrow M$ a continuous middle linear map, then there exists a unique map of R-modules $\bar{\varphi} : T \longrightarrow M$ such that $\bar{\varphi}(a\widehat{\otimes}b) = \varphi(a, b)$.

It is easy to see that if the complete tensor product exists, it is unique up to isomorphism. We denote it by $A\widehat{\otimes}_\Lambda B$. Furthermore, it is clear that $\{a\widehat{\otimes}b \mid a \in A, b \in B\}$ is a set of topological generators for the R-module $A\widehat{\otimes}_\Lambda B$.

Note that it suffices to check the above universal property only for finite R-modules M, since every R-module is the inverse limit of its finite R-quotient modules.

3.4.1 Lemma *With the above notation, the complete tensor product $A\widehat{\otimes}_\Lambda B$ exists. In fact, if*

$$A = \varprojlim_{i\in I} A_i \quad \text{and} \quad B = \varprojlim_{j\in J} B_j,$$

where each A_i (respectively, B_i) is a finite right (respectively, left) Λ-module, then

$$A\widehat{\otimes}_\Lambda B = \varprojlim_{i\in I, j\in J} (A_i \otimes_\Lambda B_j) \ ,$$

where $A_i \otimes_\Lambda B_j$ is the usual tensor product as abstract Λ-modules. In particular, $A\widehat{\otimes}_\Lambda B$ is the completion of $A \otimes_\Lambda B$, where $A \otimes_\Lambda B$ has the topology for which a fundamental system of neighborhoods of 0 are the kernels of the natural maps

$$A \otimes_\Lambda B \longrightarrow A_i \otimes_\Lambda B_j \quad (i \in I, j \in J).$$

3.5 COHOMOLOGY OF PROFINITE GROUPS

Let G be a profinite group and let $A \in \mathbf{DMod}(G)$. For each natural number n we consider an R-module

$$H^n(G, A),$$

the *nth cohomology group of G with coefficients in A*. We shall give explicit definitions of these cohomology groups later in Section 3.6. Here, instead, we mention some of their fundamental properties (cf. Proposition 6.2.2 in [RZ]), which in fact characterize them:

(a) $H^n(G, A)$ are functors in the variable A;

(b) $H^0(G, A) = \{a \mid a \in A, ga = a, \forall g \in G\} = A^G$;

(c) $H^n(G, Q) = 0$ for every discrete injective G-module Q and $n \geq 1$;

(d) For each short exact sequence $0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$ in $\mathbf{DMod}(G)$, there exist 'connecting homomorphisms'

$$\delta : H^n(G, A_3) \longrightarrow H^{n+1}(G, A_1)$$

for all $n \geq 0$, such that the sequence

$$0 \to H^0(G, A_1) \to H^0(G, A_2) \to H^0(G, A_3) \xrightarrow{\delta}$$
$$H^1(G, A_1) \to H^1(G, A_2) \to \cdots$$

is exact; and

(e) For every commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A'_1 & \longrightarrow & A'_2 & \longrightarrow & A'_3 & \longrightarrow & 0 \end{array}$$

in $\mathbf{DMod}(G)$ with exact rows, the following diagram commutes for every $n \geq 0$

$$\begin{array}{ccc} H^n(G, A_3) & \xrightarrow{\delta} & H^{n+1}(G, A_1) \\ {\scriptstyle H^n(G,\gamma)}\downarrow & & \downarrow{\scriptstyle H^{n+1}(G,\alpha)} \\ H^n(G, A'_3) & \xrightarrow{\delta} & H^{n+1}(G, A'_1) \end{array}$$

The existence of these cohomology groups follows from the existence of 'enough injectives' in $\mathbf{DMod}(G)$. The sequence $H^0(G,-), H^1(G,-), H^2(G,A), \ldots$ is the "sequence of right derived functors of the functor $A \mapsto A^G$ " (cf. [RZ], Section 6.1).

3.6 EXPLICIT CALCULATION OF COHOMOLOGY GROUPS

For each $n \geq 0$, define L_n as the left free profinite R-module on the free profinite G-space $G^{n+1} = G \times \overset{n+1}{\cdots} \times G$ with diagonal action (i.e., $x(x_1, \ldots, x_n) = (xx_1, \ldots, xx_n)$, for $x, x_1, \ldots, x_n \in G$). Then L_n is a free profinite $[\![RG]\!]$-module on the profinite space

$$\{(1, x_1, \ldots, x_n) \mid x_i \in G\}.$$

Define a sequence $\mathbf{L}(G)$:

$$\cdots \longrightarrow L_n \xrightarrow{\partial_n} L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \xrightarrow{\epsilon} R \longrightarrow 0, \tag{1}$$

where

$$\partial_n(x_0, x_1, \ldots, x_n) = \sum_{i=0}^{n} (-1)^i (x_0, \ldots, \hat{x}_i, \ldots, x_n)$$

(the symbol $\hat{x}_i$ indicates that x_i is to be omitted), and ϵ is the augmentation map

$$\epsilon(x) = 1.$$

It is easy to check that ϵ and each ∂_n are $[\![RG]\!]$-homomorphisms, and that (1) is in fact an exact sequence, a *free* $[\![RG]\!]$*-resolution of* R.

If one applies the functor $\mathrm{Hom}_{[\![RG]\!]}(-, A) = -^G$ to (1), excluding the first term R, one gets the following cochain complex, $\mathbf{C}(G, A)$:

$$0 \longrightarrow C^0(G,A) \longrightarrow \cdots \longrightarrow C^n(G,A) \xrightarrow{\partial^{n+1}} C^{n+1}(G,A) \longrightarrow \cdots \ , \tag{2}$$

where $C^n(G, A)$ consists of all continuous maps $f : G^{n+1} \longrightarrow A$ such that

$$f(xx_0, xx_1, \ldots, xx_n) = xf(x_0, x_1, \ldots, x_n) \quad \text{for all } x, x_i \in G.$$

And

$$(\partial^{n+1} f)(x_0, x_1, \ldots, x_{n+1}) = \sum_{i=0}^{n+1} (-1)^i f(x_0, \ldots, \hat{x}_i, \ldots x_{n+1}) \ .$$

Then one has the following explicit description:

3.6.1 Theorem *$H^n(G, A)$ is the n-th cohomology group of the cochain complex* (2)*, i.e.,*

$$H^n(G, A) = \mathrm{Ker}(\partial^{n+1})/\mathrm{Im}(\partial^n) \ .$$

(cf. [RZ], Theorem 6.2.4).

3.7 HOMOLOGY OF PROFINITE GROUPS

The 'dual' of cohomology is homology [we make this precise later]. For a right profinite $[\![RG]\!]$-module B (we write this as $B \in \mathbf{PMod}([\![RG]\!]^{op})$), define

$$B_G = B/\overline{\langle bg - b \mid b \in B, g \in G \rangle}.$$

Then one defines the *n-th homology group $H_n(G,B)$ of G with coefficients in B*. These are in fact R-modules. They have the following basic properties.

$\{H_n(G,-)\}_{n\in\mathbf{N}}$ is the sequence of left derived functors of the functor $B \mapsto B_G$ from $\mathbf{PMod}([\![RG]\!]^{op})$ to $\mathbf{PMod}(R)$. In other words, this sequence is the unique sequence of covariant functors from $\mathbf{PMod}([\![RG]\!]^{op})$ to $\mathbf{PMod}(R)$ such that

(a) $H_0(G,B) = B_G$ (as functors on $\mathbf{PMod}([\![RG]\!]^{op})$),

(b) $H_n(G,P) = 0$ for every projective profinite right $[\![RG]\!]$-module P and $n \geq 1$.

(c) For each short exact sequence $0 \longrightarrow B_1 \longrightarrow B_2 \longrightarrow B_3 \longrightarrow 0$ in $\mathbf{PMod}([\![RG]\!]^{op})$, there exist connecting homomorphisms

$$\delta : H_{n+1}(G,B_3) \longrightarrow H_n(G,B_1),$$

for all $n \geq 0$, such that the sequence

$$\cdots \to H_1(G,B_2) \to H_1(G,B_3) \stackrel{\delta}{\to} H_0(G,B_1) \to$$

$$H_0(G,B_2) \to H_0(G,B_3) \to 0$$

is exact; and

(d) For every commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & B_1' & \longrightarrow & B_2' & \longrightarrow & B_3' & \longrightarrow & 0 \end{array}$$

in $\mathbf{PMod}([\![RG]\!]^{op})$ with exact rows, the diagram

$$\begin{array}{ccc} H_{n+1}(G,B_3) & \stackrel{\delta}{\longrightarrow} & H_n(G,B_1) \\ {\scriptstyle H_{n+1}(G,\gamma)}\downarrow & & \downarrow{\scriptstyle H_n(G,\alpha)} \\ H_{n+1}(G,B_3') & \stackrel{\delta}{\longrightarrow} & H_n(G,B_1') \end{array}$$

commutes for every $n \geq 0$.

3.7.1 One can calculate explicitly $H_n(G,B)$ (see for example [RZ], Theorem 6.3.1) as the n-th homology group of the sequence

$$\cdots \longrightarrow B\widehat{\otimes}_{[\![RG]\!]}L_{n+1} \longrightarrow B\widehat{\otimes}_{[\![RG]\!]}L_n \stackrel{\partial_n}{\longrightarrow} \cdots \longrightarrow B\widehat{\otimes}_{[\![RG]\!]}L_0 \longrightarrow 0\ .$$

3.7.2 Proposition (Duality of homology-cohomology) *Let G be a profinite group and let B be a profinite right $[\![\widehat{\mathbf{Z}}G]\!]$-module. Then*

$$H_n(G,B) \quad \text{and} \quad H^n(G,B^*) \quad (n \in \mathbf{N})$$

are Pontryagin dual, where B^* denotes the Pontryagin dual of B.

3.8 HOMOLOGY AND COHOMOLOGY IN LOW DIMENSIONS

3.8.1

$$H^0(G,A) = \{a \in A \mid xa = a, \forall x \in G\} = A^G$$

is the subgroup of elements of A invariant under the action of G.

3.8.2

$$H^1(G, A) = \mathrm{Der}(G, A)/\mathrm{Ider}(G, A)$$

where

$$\mathrm{Der}(G, A) = \{d : G \longrightarrow A \mid d(xy) = xd(y) + d(x), \quad \text{for all} \quad x, y \in G\}$$

(the *group of derivations*) , and $\mathrm{Ider}(G, A)$ is the *group of inner derivations* $d_a : G \to A$ defined for each $a \in A$ as $d_a(x) = xa - a$.

3.8.3 Given a finite G-module A, $H^2(G, A)$ is in $1 - 1$ correspondence with the (equivalence classes of) extensions of A by G, i.e., exact sequences

$$0 \longrightarrow A \longrightarrow E \stackrel{\varphi}{\longrightarrow} G \longrightarrow 1$$

where the action of G on A is precisely the natural action determined by this sequence.

3.8.4

$$H_0(G, B) = B_G$$

3.8.5

$$H_1(G, \widehat{\mathbf{Z}}) \cong G/\overline{[G, G]},$$

the abelianized group of G (here the action of G on $\widehat{\mathbf{Z}}$ is assumed to be trivial)

3.8.6 If G is a pro-p group and the action of G on $\mathbf{F}_p$ is trivial, one has

$$H_1(G, \mathbf{F}_p) \cong G/G^p\overline{[G, G]}.$$

Note that $G^p\overline{[G, G]} = \Phi(G)$ is the Frattini subgroup of G.

For proofs of the above results see [RZ], Section 6.8.

3.9 INDUCED AND COINDUCED MODULES

Let G be a profinite group and let $H \leq_c G$. For $A \in \mathbf{DMod}(H)$ consider the abelian group

$$\mathrm{Coind}_H^G(A) =$$

$$\{f : G \longrightarrow A \mid f \text{ continuous, with } f(hy) = hf(y) \text{ for all } h \in H,\ y \in G\}.$$

The compact-open topology makes $\mathrm{Coind}_H^G(A)$ into a discrete abelian group. Define an action of G on $\mathrm{Coind}_H^G(A)$ by

$$(xf)(y) = f(yx) \quad (x, y \in G,\ f \in \mathrm{Coind}_H^G(A)).$$

This action is in fact continuous. So $\mathrm{Coind}_H^G(-)$ transforms modules in $\mathbf{DMod}(H)$ into modules in $\mathbf{DMod}(G)$. The G-module $\mathrm{Coind}_H^G(A)$ is called a *coinduced* module. Its most important property is

3.9.1 Theorem (Shapiro's Lemma) *Let G be a profinite group, H a closed subgroup of G and $A \in$ $\mathbf{DMod}(H)$. Then there exist natural isomorphisms*

$$H^n(G, \mathrm{Coind}_H^G(A)) \cong H^n(H, A) \quad (n \geq 0).$$

3.9.2 Corollary *Let G be a profinite group and let A be an abelian group. Then* $\mathrm{Coind}_1^G(A) = C(G, A)$ *(the group of all continuous functions from G to A), and $H^n(G, C(G, A)) = 0$ for $n > 0$.*

Because of this last property, the coinduced modules of the form $C(G, A)$ play an important role that allows a 'shift of dimension' (using the properties in Section 3.5).

Dually one has *induced modules*: Let $H \leq G$ be profinite groups and let B be a profinite right $[\![\widehat{\mathbf{Z}}H]\!]$-module. Define a right G-module structure on the profinite group

$$\mathrm{Ind}_H^G(B) = B \widehat{\otimes}_{[\![\widehat{\mathbf{Z}}H]\!]} [\![\widehat{\mathbf{Z}}G]\!]$$

3.9.3 Theorem Let G be a profinite group, H a closed subgroup of G and $B \in \mathbf{PMod}([\![\widehat{\mathbf{Z}}H]\!])$.

(a) (Shapiro's Lemma) There exist natural isomorphisms

$$H_n(G, \mathrm{Ind}_H^G(B)) \cong H_n(H, B), \quad (n \geq 0).$$

(b) Let M be a profinite abelian group. Then $\mathrm{Ind}_1^G(M) = M \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\widehat{\mathbf{Z}}G]\!]$, and

$$H_n(G, M \widehat{\otimes}_{\widehat{\mathbf{Z}}} [\![\widehat{\mathbf{Z}}G]\!]) = 0$$

for $n > 0$.

(cf. [RZ], Section 6.10).

3.10 COHOMOLOGICAL DIMENSION

Let G be a profinite group and let p be a prime number. The *cohomological p-dimension* $cd_p(G)$ of G is the smallest non-negative integer n such that $H^k(G, A)_p = 0$ for all $k > n$ and $A \in \mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, if such an n exists. Otherwise we say that $cd_p(G) = \infty$.

Similarly, the *strict cohomological p-dimension* $scd_p(G)$ of G is the smallest non-negative number n such that $H^k(G, A)_p = 0$ for all $k > n$ and $A \in \mathbf{DMod}(G)$.

Define

$$cd(G) = \sup_p cd_p(G),$$

and

$$scd(G) = \sup_p scd_p(G).$$

3.10.1 Proposition *Let G be a profinite group and let p be a prime. Then*

$$cd_p(G) \leq scd_p(G) \leq cd_p(G) + 1.$$

Proof. The first inequality is clear. For the second we may suppose that $cd_p(G) < \infty$. Let $n = cd_p(G) + 1$. Assume $A \in \mathbf{Mod}(G)$ and let $p : A \longrightarrow A$ be multiplication by p. Denote the kernel of this map $A[p]$; in other words,

$$A[p] = \{a \in A \mid pa = 0\}.$$

Consider the short exact sequences

$$0 \longrightarrow A[p] \longrightarrow A \xrightarrow{p} pA \longrightarrow 0,$$

$$0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA \longrightarrow 0.$$

Then $A[p]$ and A/pA are in $\mathbf{DMod}([\![\widehat{\mathbf{Z}}G]\!])$, in fact they are annihilated by p. So, if $k \geq n$,

$$H^k(G, A[p]) = H^k(G, A/pA) = 0.$$

Therefore, from the long exact sequences corresponding to the short exact sequences above,

$$\cdots \longrightarrow H^k(G, A[p]) \longrightarrow H^k(G, A) \xrightarrow{\varphi} H^k(G, pA) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^{k-1}(G, A/pA) \longrightarrow H^k(G, pA) \xrightarrow{\psi} H^k(G, A) \longrightarrow \cdots,$$

one obtains that the maps φ and ψ are injections if $k > n$. Hence their composition

$$\psi\varphi : H^k(G, A) \longrightarrow H^k(G, A)$$

is again an injection. On the other hand, it is clear that $\psi\varphi$ is multiplication by p. Thus

$$H^k(G, A)_p = 0, \quad \text{if } k > n.$$

Hence the second inequality follows. □

Example Let $G = \widehat{\mathbf{Z}}$. Then it is not hard to see that $cd_p(G) = 1$, while $scd_p(G) = 2$ (see [RZ], Example 7.1.3).

3.11 COHOMOLOGICAL DIMENSION AND SUBGROUPS

Let H be a closed subgroup of a profinite group G. Then every G-module A is automatically an H-module. From the explicit definition of $H^n(G, A)$ in terms of cochains (see Section 3.6 above) one sees that there are natural homomorphisms (called 'restrictions')

$$\mathrm{Res} = \mathrm{Res}^G_H : H^n(G, A) \longrightarrow H^n(H, A) \quad (n \geq 0).$$

On the other hand, if H is an open subgroup of a profinite group G, and $A \in \mathbf{DMod}(G)$, then there are natural homomorphisms (called 'corestrictions')

$$\mathrm{Cor} = \mathrm{Cor}^H_G : \mathbf{H}^n(H, A) \longrightarrow \mathbf{H}^n(G, A) \quad (n \geq 0).$$

At level 0, corestriction is just the map:

$$\mathrm{N}_{G/H} : A^H \longrightarrow A^G$$

given by

$$\mathrm{N}_{G/H}(a) = \sum ta,$$

where $a \in A^H$ and t runs through a left transversal of H in G.

The fundamental connection between restriction and corestriction is (see [RZ], Theorem 6.7.3)

3.11.1 Theorem *Let H be an open subgroup of a profinite group G. Then the composition* CorRes *is multiplication by the index $[G : H]$ of H in G, i.e.,*

$$\mathrm{Cor}^H_G \mathrm{Res}^G_H = [G : H] \cdot \mathrm{id},$$

where id *is the identity on $H^n(G, -)$ $(n \geq 0)$.*

From this one obtains (see [RZ], Theorem 7.3.1 and Corollary 7.3.3)

3.11.2 Theorem *Let G be a profinite group, H a closed subgroup of G and p a prime number. Then*

(a)

$$cd_p(H) \leq cd_p(G).$$

Moreover, equality holds in either of the following cases

(1) $p \nmid [G:H]$,

(2) $cd_p(G) < \infty$ and the exponent of p in the supernatural number $[G:H]$ is finite (this is the case, e.g., if H is open in G).

(b) *Let G_p be a p-Sylow group of G. Then*

$$cd_p(G) = cd_p(G_p) = cd(G_p).$$

3.12 PROJECTIVE PROFINITE GROUPS

A pro-$\mathcal{C}$ group G is called *$\mathcal{C}$-projective* if it is a projective object in the category of pro-$\mathcal{C}$ groups, i.e., if every diagram

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 1 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & 1 \end{array} \qquad (3)$$

of pro-$\mathcal{C}$ groups has a weak solution. We say that G is *projective* if it is projective in the category of profinite groups (i.e., $\mathcal{C}$-projective and $\mathcal{C}$ is the class of all finite groups).

The following lemma simplifies the criteria to decide whether G is projective.

3.12.1 Lemma *Let $\mathcal{C}$ and $\mathcal{C}'$ be varieties of finite groups, and let G be a profinite group. The following conditions are equivalent.*

(a) *Every embedding problem* (3) *for G where K is pro-$\mathcal{C}'$ and A is pro-$\mathcal{C}$ has a weak solution;*

(b) *Every embedding problem* (3) *for G such that $A \in \mathcal{C}$ and $K \in \mathcal{C}'$ is an abelian minimal normal subgroup of A, has a weak solution.*

Example A free pro-$\mathcal{C}$ group is $\mathcal{C}$-projective.

3.12.2 Lemma *Let $\mathcal{C}$ be a variety of finite groups and let G be a pro-$\mathcal{C}$ group.*

(a) *If G is $\mathcal{C}$-projective, then it is isomorphic to a closed subgroup of a free pro-$\mathcal{C}$ group.*

(b) *Assume in addition that the variety $\mathcal{C}$ is extension closed. Then G is $\mathcal{C}$-projective if and only if G is a closed subgroup of a free pro-$\mathcal{C}$ group.*

Proof.

(a) By Proposition 2.2.6, there exists a free pro-$\mathcal{C}$ group F and a continuous epimorphism $\alpha : F \longrightarrow G$. Since G is $\mathcal{C}$-projective, there exists a continuous homomorphism $\sigma : G \longrightarrow F$ such that $\alpha\sigma = \mathrm{id}_G$. Hence σ is an embedding.

(b) Assume that $G \leq_c F$, where F is a free pro-$\mathcal{C}$ group. Consider an embedding problem (3) as above with $A \in \mathcal{C}$. Then $\mathrm{Ker}(\varphi)$ is an open normal subgroup of G. Hence there exists $V \triangleleft_o F$ such that

$V \cap G \leq \mathrm{Ker}(\varphi)$. Since GV is open in F and the variety $\mathcal{C}$ is extension closed, it follows that GV is a free pro-$\mathcal{C}$ group (see Theorem 2.6.1). Therefore we may assume that $F = GV$. Put $U = V\mathrm{Ker}(\varphi)$. Then $U \triangleleft_o F$ and $U \cap G = \mathrm{Ker}(\varphi)$. Define an epimorphism $\varphi_1 : F \longrightarrow B$ to be the composite of the natural maps

$$F \longrightarrow F/U = GU/U \longrightarrow G/G \cap U = G/\mathrm{Ker}(\varphi) \longrightarrow B.$$

Note that φ is the restriction of φ_1 to G. Since F is $\mathcal{C}$-projective, there exists a continuous homomorphism $\bar{\varphi}_1 : F \longrightarrow A$ such that $\alpha\bar{\varphi}_1 = \varphi_1$. Therefore, the restriction of $\bar{\varphi}_1$ to G is a weak solution of the embedding problem (3), as needed. □

For certain varieties $\mathcal{C}$ (the so called 'saturated' varieties of finite groups: G finite and $G/\Phi(G) \in \mathcal{C} \Rightarrow G \in \mathcal{C}$), e.g., extension-closed varieties, the distinction between 'projective' and '$\mathcal{C}$-projective' is non-existent. In fact we have (see [RZ], Proposition 7.6.7)

3.12.3 Proposition *Let $\mathcal{C}$ be a saturated variety of finite groups and let G be a pro-$\mathcal{C}$ group. Then the following conditions on G are equivalent:*

(a) *G is a $\mathcal{C}$-projective group;*

(b) *G is a projective group;*

(c) *$cd(G) \leq 1$.*

3.12.4 Theorem (cf. [RZ], Theorem 7.7.4) *Let G be a pro-p group. Then, the following statements are equivalent*

(a) $\mathrm{cd}_p(G) \leq 1$*;*

(b) $H^2(G, \mathbf{F}_p) = 0$*;*

(c) *G is a free pro-p group;*

(d) *G is a projective group.*

3.12.5 Corollary (cf. [RZ], Corollary 7.7.5) *Every closed subgroup H of a free pro-p group G is a free pro-p group.*