Canad. Math. Bull.Vol. 34 (1), 1991 pp. 136–140

DIMENSION-PRESERVING EXTENSIONS OF PRO-p-GROUPS

TILMANN WÜRFEL

ABSTRACT. We investigate extensions of pro-p-groups $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ where N is pro-p-free and N_{ab} is a free $\mathbb{Z}_p[\![\Gamma]\!]$-module. In case Γ is finite we show that such an extension splits modulo the second derived group N''.

This note is a continuation of [6] where we studied certain presentations of pro-p-groups of cohomological dimension two, generalizing Brumer's characterization of such groups [1]. Here, we remove any condition of finite dimensionality and come up with a type of extension characterized by two properties of its kernel: it is pro-p-free and its abelianization is a free module over the cokernel, in the profinite sense. We then use some Lie algebra technique as in [5] to show that if the cokernel is finite then the extension with the kernel made metabelian splits. We work with the usual cohomology for profinite groups and discrete modules (cf. [3]) and use standard notations.

PROPOSITION 1. *Let $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ be an exact sequence of pro-p-groups (p a prime) and let $i^k : H^k(\Gamma, X^N) \longrightarrow H^k(G, X)$ denote the inflation maps. The following conditions are equivalent:*

(a) i^2 is surjective and i^3 is injective with $X = \mathbb{Z}/(p)$.

(b) i^2 is surjective and i^k is an isomorphism for all discrete torsion Γ-modules X and for all $k \geq 3$.

(c) N is pro-p-free and $H^1(\Gamma, H^1(N)) = 0$.

COROLLARY. If $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ satisfies the conditions of Proposition 1 then

(a) $cd(G) = cd(\Gamma)$ unless G is pro-p-free in which case $cd(\Gamma) \leq 2$,

(b) $N_{ab} \simeq \mathbb{Z}_p[\![\Gamma]\!]^d$ as Γ-modules where $\mathbb{Z}_p[\![\Gamma]\!]$ is the completed p-adic group ring and d is the $\mathbb{Z}/(p)$-dimension of $H^1(N)^\Gamma$.

PROOF. (a) follows from (b) of Proposition 1. The proof of (b) is contained in [2], Satz 7.7.

PROOF OF PROPOSITION 1. Let X be a finite p-primary left Γ-module. Embedding X into an induced G-module or Γ-module, respectively, yields the following two exact

Received by the editors September 8, 1988, revised October 5, 1989.
AMS subject classification: Primary: 20E18, 20J06.

sequences of Γ-modules:

(1) $$0 \longrightarrow X \longrightarrow M_G(X) \longrightarrow A \longrightarrow 0$$

(2) $$0 \longrightarrow X \longrightarrow M_\Gamma(X) \longrightarrow B \longrightarrow 0$$

Next apply $H^*(N,-)$ to (1), together with $M_G(X)^N \simeq M_\Gamma(X)$ and (2), so as to obtain the exact sequence of Γ-modules

(3) $$0 \longrightarrow B \longrightarrow A^N \longrightarrow H^1(N,X) \longrightarrow 0$$

$H^*(\Gamma,-)$ applied to (3) and the connecting isomorphism $H^k(\Gamma,B) \simeq H^{k+1}(\Gamma,X)$ now give, for every $k \geq 1$, the exact sequence

(4) $$H^{k+1}(\Gamma,X) \xrightarrow{j^k} H^k(\Gamma,A^N) \longrightarrow H^k(\Gamma,H^1(N,X)) \longrightarrow H^{k+2}(\Gamma,X) \xrightarrow{j^{k+1}} H^{k+1}(\Gamma,A^N)$$

If we now define $h^k\colon H^k(\Gamma,A^N) \longrightarrow H^k(G,A) \simeq H^{k+1}(G,X)$, then

(5) $$h^k j^k = i^{k+1}$$

(a)$\Rightarrow$(c): let $X = \mathbb{Z}/(p)$. Since i^2 is surjective, so is h^1 by (5). Hence h^1 is an isomorphism and j^1 is surjective. Since i^3 is injective, so is j^2. Sequence (4) now implies $H^k(\Gamma,H^1(N)) = 0$ for $k = 1$ and hence for all $k \geq 1$ which, for $k = 2$, makes j^2 surjective and hence an isomorphism. Therefore h^2 is injective. From the exact Hochschild-Serre sequence for the module A,

$$0 \longrightarrow H^1(\Gamma,A^N) \xrightarrow{h^1} H^2(G) \longrightarrow H^2(N)^\Gamma \longrightarrow H^2(\Gamma,A^N) \xrightarrow{h^2} H^3(G),$$

it now follows that $H^2(N)^\Gamma = 0$. So $H^2(N) = 0$ and N is pro-p-free.
(c)$\Rightarrow$(b): we have $H^k(N,A) \simeq H^{k+1}(N,X) = 0$ for all $k \geq 1$ because N is pro-p-free. So the Hochschild-Serre sequence reduces to

$$0 \longrightarrow H^k(\Gamma,A^N) \longrightarrow H^k(G,A) \longrightarrow 0$$

and h^k is an isomorphism for all $k \geq 1$. Moreover, freeness of N and the vanishing of $H^1(\Gamma,H^1(N))$ imply $H^k(\Gamma,H^1(N,X)) = 0$ for all $k \geq 1$ because N acts trivially on X. So, by (4), j^1 is surjective and j^k is an isomorphism if $k \geq 2$ which, by (5), establishes the properties of i^k. ∎

REMARK. Let $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ satisfy the conditions of Proposition 1 and assume Γ is finite. Then i^2 is an isomorphism for all torsion Γ-modules.

PROOF. It suffices to show that i^2 is injective for X finite, annihilated by some power p^m. We then have an epimorphism $S \longrightarrow X$ where S is some finite direct sum of copies of $\mathbb{Z}/(p^m)[\Gamma]$. This induces a morphism between the two exact Hochschild-Serre sequences:

$$\begin{array}{ccccccc} H^1(G,S) & \longrightarrow & H^1(N,S)^\Gamma & \longrightarrow & 0 & & \\ \downarrow & & \downarrow \pi & & & & \\ H^1(G,X) & \longrightarrow & H^1(N,X)^\Gamma & \longrightarrow & H^2(\Gamma,X) & \xrightarrow{i^2} & H^2(G,X) \end{array}$$

https://doi.org/10.4153/CMB-1991-022-3 Published online by Cambridge University Press

By (b) of the Corollary, the Γ-module N_{ab} is projective with respect to (discrete) Γ-modules and continuous homomorphisms. Therefore, π is surjective and i^2 is injective. ∎

We are now concerned with the question whether an extension satisfying the conditions of Proposition 1 and where Γ is finite, splits; if it does, then G is a free pro-p-product of the form $G \simeq F \amalg \Gamma$ with F pro-p-free ([6], Remark 1). By a theorem of Serre [4] one knows that G contains torsion (if $\Gamma \neq 1$), so the answer is "yes" for $\Gamma \simeq \mathbb{Z}/(p)$.

PROPOSITION 2. *Let $1 \longrightarrow N \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$ be an exact sequence of pro-p-groups satisfying the conditions of Proposition 1 and assume Γ is finite and G is finitely generated. Let N'' denote the second derived group of N. Then the induced extension $1 \longrightarrow N/N'' \longrightarrow G/N'' \longrightarrow \Gamma \longrightarrow 1$ splits.*

PROOF. We shall make use of the module structure of the free metabelian $\mathbb{Z}_p$-Lie algebra $M = \oplus_{i\geq 1} M_i$, derived from N, upon which Γ acts and whose first homogenous component M_1 is a free $\mathbb{Z}_p[\Gamma]$-module. We follow Stöhr's work [5] which was suggested to us by the referee of an earlier version of this paper.

By (b) of the Corollary $N_{ab} = N/N'$ is a finitely generated free $\mathbb{Z}_p[\Gamma]$-module. Therefore, $1 \longrightarrow N_{ab} \longrightarrow G/N' \longrightarrow \Gamma \longrightarrow 1$ splits and there is a closed subgroup $S \leq G$ such that $G = NS$ and $N \cap S = N'$. So N'/N'' becomes a $\mathbb{Z}_p[\Gamma]$-module by restricting the action of G to S. It suffices to show that $H^2(\Gamma, N'/N'') = 0$, for then $1 \longrightarrow N'/N'' \longrightarrow S/N'' \longrightarrow \Gamma \longrightarrow 1$ will split and hence so will $1 \longrightarrow N/N'' \longrightarrow G/N'' \longrightarrow \Gamma \longrightarrow 1$. Let N_i denote the lower central series of N and put $Q_i = N'/N_iN''$. Then $N'/N'' \simeq \lim Q_i$. We show in the Remark below that $H^2(\Gamma, \lim Q_i) \simeq \lim H^2(\Gamma, Q_i)$. Also let $M_i = N_iN''/N_{i+1}N''$. Then $1 \longrightarrow M_i \longrightarrow Q_{i+1} \longrightarrow Q_i \longrightarrow 1$ is exact and $Q_2 = 1$. So it remains to show that $H^2(\Gamma, M_i) = 0$ for all $i \geq 2$. This will follow from the Lemma below because $M_i \simeq N_i/N_{i+1}(N_i \cap N'')$ is isomorphic to the ith homogenous component of L/L'' where $L = \oplus_{i\geq 1} L_i$ with $L_i = N_i/N_{i+1}$ is the Lie algebra of the finitely generated free pro-p-group N and is thus a free $\mathbb{Z}_p$-Lie algebra over a $\mathbb{Z}_p$-basis of L_1.

REMARK. Let Γ be a finite group and Q_i an inverse system of compact Γ-modules upon which Γ acts continuously. Then $H^k(\Gamma, \lim Q_i) \simeq \lim H^k(\Gamma, Q_i)$ for all $k \geq 1$.

PROOF. Since the inverse limit of compact groups is exact and the induced module $M_\Gamma(-)$ preserve compactness and continuity, one may apply dimension shifting. So it suffices to give the proof for $k = 1$.

Consider the exact sequence of inverse systems of compact groups

$$0 \longrightarrow Q_i \longrightarrow M_\Gamma(Q_i) \longrightarrow C_i \longrightarrow 0$$

and put $Q = \lim Q_i, C = \lim C_i$. Then

$$0 \longrightarrow Q \longrightarrow M_\Gamma(Q) \longrightarrow C \longrightarrow 0$$

is exact. Application of the long exact cohomology sequence yields the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q/Q^{\Gamma} & \longrightarrow & C^{\Gamma} & \longrightarrow & H^1(\Gamma, Q) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \lim(Q/Q^{\Gamma}) & \longrightarrow & \lim(C_i^{\Gamma}) & \longrightarrow & \lim H^1(\Gamma, Q_i) & \longrightarrow & 0 \end{array}$$

where the bottom row is exact by compactness (Q_i^{Γ} and C_i^{Γ} are closed subgroups, $H^1(\Gamma, Q_i)$ gets the quotient topology). The middle vertical map is an isomorphism. The lefthand vertical map is surjective because it comes from the exact sequence of systems of compact groups

$$0 \longrightarrow Q_i^{\Gamma} \longrightarrow Q_i \longrightarrow Q_i/Q_i^{\Gamma} \longrightarrow 0$$

So the snake lemma establishes the desired isomorphism. ∎

LEMMA. *Let $M = \oplus_{n \geq 1} M_n$ be a finitely generated free metabelian $\mathbb{Z}_p$-Lie algebra upon which the finite p-group Γ acts (diagonally) such that M_1 is a free $\mathbb{Z}_p[\Gamma]$-module. Then each homogenous component M_n is a direct sum of a free $\mathbb{Z}_p[\Gamma]$-module and of ideals of the form $\mathbb{Z}_p[\Gamma]I\Delta$ where $\Delta \leq \Gamma$ and $I\Delta$ is the augmentation ideal of $\mathbb{Z}_p[\Delta]$. (If $(n,p) = 1$, then $\Delta = 1$.) Hence $H^2(\Gamma, M_n) = 0$.*

PROOF. We refer to [5], Sections 2, 3 and use the strategy of the proof of Theorem 3.11, loc. cit.. Let $R = \mathbb{Z}_p[\Gamma]$. The $\mathbb{Z}_p$-module M_n is generated by the left-normed commutators $[x_1, \ldots, x_n]$ ($x_i \in M_1$) and these satisfy the following relations:

$$\begin{aligned} &[x_1, x_2, \ldots] = -[x_2, x_1, \ldots] \\ (6) \qquad &[x_1, x_2, x_3, \ldots] + [x_3, x_2, x_1, \ldots] + [x_1, x_3, x_2, \ldots] = 0 \\ &[x_1, \ldots, x_j, x_{j+1}, \ldots] = [x_1, \ldots, x_{j+1}, x_j, \ldots] \text{ where } j \geq 3 \end{aligned}$$

Let $e_1, \ldots, e_d$ be an R-basis of M_1, put $E = \Gamma e_1 \cup \cdots \cup \Gamma e_d$, and choose a total ordering on E. The basic commutators $[x_1, \ldots, x_n]$ with $x_i \in E$ and $x_1 > x_2 \leq \cdots \leq x_n$ then form a $\mathbb{Z}_p$-basis of M_n.

Let $E^{(n)}$ denote the nth symmetric power of E, the general element of which is denoted by $\underline{x} = x_1 \circ \cdots \circ x_n$. Γ acts on $E^{(n)}$ by left multiplication and the stabilizer Δ of $\underline{x} \in E^{(n)}$ is characterized as follows: ($\delta \in \Gamma$)

$$\delta \underline{x} = \underline{x} \Leftrightarrow \begin{cases} \{\delta x_1, \ldots, \delta x_n\} = \{x_1, \ldots, x_n\} \\ \delta x_i \text{ and } x_i \text{ occur with the same multiplicity in } \underline{x} \, (i = 1, \ldots, n) \end{cases}$$

Therefore, the order of Δ divides n.

For $\underline{x} \in E^{(n)}$ let $M_n^{\underline{x}}$ denote the $\mathbb{Z}_p$-submodule generated by all left-normed commutators $[x_{\pi(1)}, \ldots, x_{\pi(n)}]$ (π a permutation). By (6), the basic ones among these commutators form a $\mathbb{Z}_p$-basis of $M_n^{\underline{x}}$. If $\gamma \in \Gamma$ and $\gamma \underline{x} \neq \underline{x}$, then basic commutators coming from $\gamma \underline{x}$ or $\underline{x}$, respectively, are different. Therefore, we have

$$\sum_{\gamma \in \Gamma} M_n^{\gamma \underline{x}} = \bigoplus_{\bar{\gamma} \in \Gamma/\Delta} M_n^{\gamma \underline{x}} \text{ where } \Delta \leq \Gamma \text{ is the stabilizer of } \underline{x}.$$

Moreover, since multiplication by γ induces a $\mathbb{Z}_p$-isomorphism $M_n^{\underline{x}} \longrightarrow M_n^{\gamma \underline{x}}$, we have

$$R \bigotimes_{R'} M_n^{\underline{x}} \simeq \bigoplus_{\bar{\gamma} \in \Gamma / \Delta} M_n^{\gamma \underline{x}} \text{ where } R' = \mathbb{Z}_p[\Delta].$$

We now show that $M_n^{\underline{x}} \simeq R'^{k-1} \oplus i\Delta$ as R'-modules where $\{x_1, \ldots, x_n\}$ is the disjoint union $\Delta x_1 \cup \cdots \cup \Delta x_k$. For this choose the ordering on E so that $\Delta x_1 < \cdots < \Delta x_k$ and that each Δx_i is ordered according to an ordering of Δ with 1 as the smallest element. The following basic commutators then form a $\mathbb{Z}_p$-basis of $M_n^{\underline{x}}$:

$$b_{\alpha,i} = [\alpha x_i, x_1, *] \text{ with } 1 \leq i \leq k, \alpha \in \Delta, \alpha \neq 1 \text{ if } i = 1,$$

and where $*$ stands for the remaining $n-2$ entries of $\underline{x}$. Using (6) one easily verifies that the action of $\delta \in \Delta$ on $b_{\alpha,i}$ is given by

$$\delta b_{\alpha,i} = b_{\delta\alpha,i} - b_{\delta,1} \text{ (where } b_{1,1} = 0) \tag{7}$$

The $\mathbb{Z}_p$-isomorphism $I\Delta \longrightarrow \oplus_{1 \neq \alpha \in \Delta} \mathbb{Z}_p b_{\alpha,1}$ given by $\alpha - 1 \longmapsto b_{\alpha,1}$ is therefore R'-linear. Let F be a free R'-module with basis $u_2, \ldots, u_k$ and define an R'-linear map $F \oplus I\Delta \longrightarrow M_n^{\underline{x}}$ by $u_i \longmapsto b_{1,i}$ and $\alpha - 1 \longmapsto b_{\alpha,1}$. This map is then surjective by (7) and hence is an isomorphism because the $\mathbb{Z}_p$-rank of $M_n^{\underline{x}}$ is $|\Delta|(k-1) + |\Delta| - 1$.

We have thus shown that $\sum_{\gamma \in \Gamma} M_n^{\gamma \underline{x}} \simeq R^{k-1} \oplus (R \otimes_{R'} I\Delta)$ where $R \otimes_{R'} I\Delta \simeq RI\Delta$. Therefore, $H^2(\Gamma, \sum_\gamma M_n^{\gamma \underline{x}}) \simeq H^2(\Delta, I\Delta) \simeq H^1(\Delta, \mathbb{Z}_p) = 0$. Decomposing $E^{(n)}$ into Γ-orbits yields that M_n is a direct sum of R-submodules of the form $\sum_\gamma M_n^{\gamma \underline{x}}$ and this completes the proof. ∎

REFERENCES

1. A. Brumer, *Pseudocompact algebras, profinite groups, and class formations*, J. Algebra **4**(1966), 442–470.
2. H. Koch, *Galoissche Theorie der p-Erweiterungen*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
3. J.-P. Serre, *Cohomolgie Galoisienne*, Springer LNM **5** (4th ed.), Berlin, 1973.
4. ———, *Sur la dimension des groupes profinis*, Topology **3**(1965), 413–420.
5. R. Stöhr, *On torsion in free central extensions of some torsion-free groups*, J. Pure Appl. Algebra **46**(1987), 249–289.
6. T. Würfel, *Extensions of pro-p-groups of cohomological dimension two*, Math. Proc. Camb. Phil. Soc. **99**(1986), 209–211.

Pennsylvania State University
Delaware Co. Campus
Media, PA 19063
USA

Current address:
Universität der Bundeswehr München
Fakultät für Informatik
D-8014 Neubiberg
West Germany

https://doi.org/10.4153/CMB-1991-022-3 Published online by Cambridge University Press