Math. Res. Lett. **20** (2013), *no.* 3, 537–545

CYCLIC EXTENSIONS OF FREE PRO-P GROUPS AND P-ADIC MODULES

Anderson L. P. Porto and Pavel A. Zalesskii

Abstract. We prove a pro-p version of the classical decomposition of a $\mathbb{Z}_p$-torsion free $\mathbb{Z}_pC_p$-module into indecomposable modules. We also describe some pro-p $\mathbb{Z}_pC_{p^n}$-modules obtained from a semidirect product of a free pro-p group F and a cyclic group C_{p^n} of automorphisms by factoring out the (closed) commutator subgroup $[F, F]$.

1. Introduction

Let p be a prime number, C_p a group of order p, $\mathbb{Z}_p$ the ring of p-adic integers and $\mathbb{Z}_pC_p$ the group ring. Let M be a $\mathbb{Z}_p$-torsion free $\mathbb{Z}_pC_p$-module. If M is finitely generated, then a classical result that plays a fundamental role in the theory of integral representations (cf. [2] or [4]) describes M as a finite direct sum of cyclic modules of the form $\mathbb{Z}_pC_p$, $\mathbb{Z}_p$ and $J(\mathbb{Z}_pC_p)$, where $J(\mathbb{Z}_pC_p)$ is the augmentation ideal of $\mathbb{Z}_pC_p$.

Note that $\mathbb{Z}_pC_p$ is a local pro-p ring, so a $\mathbb{Z}_pC_p$-module M is finitely generated as a pro-p $\mathbb{Z}_pC_p$-module if and only if it is finitely generated as an abstract $\mathbb{Z}_pC_p$-module (see pp. 126–127 in Wilson [11]). If M is infinitely generated then this is no longer the case, since an abstract infinitely generated $\mathbb{Z}_pC_p$-module is not necessarily compact so need not be pro-p. For infinitely generated abstract $\mathbb{Z}_pC_p$-modules the above result is not valid; $\mathbb{Q}_p$ considered as a trivial $\mathbb{Z}_pC_p$-module is not decomposable (since $\mathbb{Q}_p$ is not decomposable as a $\mathbb{Z}_p$-module).

We prove in this paper that surprisingly the classical result mentioned above holds for infinitely generated $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC_p$-modules.

Theorem A. *Let $C = \langle x\rangle$ be a group of order p and let M be a $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC$-module. Then M decomposes as*

$$M = M_T \oplus M_{\theta_p} \oplus L,$$

where L is a free pro-p $\mathbb{Z}_pC$-submodule of M, M_T is a trivial $\mathbb{Z}_pC$-module, M_{θ_p} is a free pro-p $\mathbb{Z}_p[\theta_p]$-module, where $\mathbb{Z}_p[\theta_p]$ is the quotient ring of $\mathbb{Z}_pC$ modulo the ideal $(\phi_p(x))$ generated by the cyclotomic polynomial $\phi_p(x) = 1 + x + \ldots + x^{p-1}$ and θ_p is a root of $\phi_p(x)$. Moreover, $M_T \cong \bigoplus_\gamma \mathbb{Z}_p$, $M_{\theta_p} \cong \bigoplus_\beta J(\mathbb{Z}_pC)$ and $L \cong \bigoplus_\phi \mathbb{Z}_pC$ are profinite direct sums of pro-p $\mathbb{Z}_pC$-modules over Boolean spaces of indices γ, β, ϕ, respectively.

Note that Theorem A can not be proved simply by using the projective limit argument since it is not clear why M can be decomposed as an inverse limit of $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC_p$-modules. The existence of such a decomposition is a consequence of Theorem A.

Received by the editors May 21, 2012.
Key words and phrases. Virtually free pro-p groups. Pro-p modules.

Now let $G = F \rtimes C_{p^n}$ be a pro-p semidirect product of a free pro-p group F and a cyclic group C_{p^n} of order p^n. The continuous action of C_{p^n} on F induces the structure of a $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC_{p^n}$-module on the abelianization $F/[F,F]$. In the second part of the paper, we study the structure of such pro-p $\mathbb{Z}_pC_{p^n}$-modules.

Theorem B. *Let $G = U \rtimes H$ be a pro-p semidirect product of a free pro-p group U and a cyclic group H of order p^n. Suppose that the centralizers of all non-identity elements of finite order in G are finite. Then*

$$U^{ab} := U/[U,U] \cong \left(\bigoplus_{i \in (I,*)} J_{K_i}(H) \right) \bigoplus L$$

is a profinite direct sum of pro-p $\mathbb{Z}_pH$-modules, where $(I,*)$ is a Boolean pointed space of indices, each K_i is a subgroup of H, $J_{K_i}(H)$ is the kernel of the canonical epimorphism $\mathbb{Z}_pH \twoheadrightarrow \mathbb{Z}_p(H/K_i)$ and L is a free pro-p $\mathbb{Z}_pH$-module.

In the proof, we use essentially Theorem 2.2 in Herfort–Zalesskii [5], which describes certain free-by-cyclic pro-p groups as a free pro-p product of normalizers of subgroups of order p and some additional free factor.
If $n = 1$ then we use Theorem A to prove that the abelianization $F^{ab} = F/[F,F]$ gives all possible $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC_p$-modules.

Theorem C. *Let M be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_pC_p$-module. Then there exists a pro-p semidirect product $F \rtimes C_p$ of a free pro-p group F and a group C_p of order p such that F^{ab} is isomorphic to M as a pro-p $\mathbb{Z}_pC_p$-module.*

Note that for $n > 1$, F^{ab} does not give all possible $\mathbb{Z}_p$-torsion free pro-p $\mathbb{Z}_pC_p$-modules, see Remark 4.5 in [8].

Basic results about profinite groups, rings and modules used in the paper can be found in [9] or [11], and for an account of injective and divisible modules see [10]. All groups and modules in the paper are pro-p, so all subgroups and submodules are closed and all homomorphisms are continuous; generation always means topological generation. Throughout the paper p denotes a prime number, $\mathbb{Z}_p$ the ring of p-adic integers and C_{p^n} denotes a cyclic group of order p^n. For a finite group H we denote by $\mathbb{Z}_pH$ the group ring of H over $\mathbb{Z}_p$ and $J(H)$ denotes the augmentation ideal of $\mathbb{Z}_pH$. If K is a subgroup of H we denote by $J_K(H)$ the kernel of the natural homomorphism $\mathbb{Z}_pH \longrightarrow \mathbb{Z}_p(H/K)$, where $\mathbb{Z}_p(H/K)$ is the free $\mathbb{Z}_p$-module over the coset space H/K. We use $\mathbb{Z}_p[\theta_p]$ to denote the quotient ring of $\mathbb{Z}_pC_p$ modulo the ideal $(\phi_p(x))$ generated by the cyclotomic polynomial $\phi_p(x) = 1 + x + \cdots + x^{p-1}$ — that is, the ring obtained from $\mathbb{Z}_p$ by adding a primitive pth root of unity. If R is a ring with unity, denote by $R^{\times}$ its group of units. We shall denote by $[A,B]$ the topological closure of the mutual commutator subgroup of subgroups A and B of a given group and by $F^{ab} = F/[F,F]$ the abelianization of a group F.

2. Preliminary results

Let M be a pro-p $\mathbb{Z}_pH$-module. We say that a collection $\{M_t, t \in T\}$ of closed $\mathbb{Z}_pH$-submodules of M indexed by a Boolean space T is a continuous system of $\mathbb{Z}_pH$-submodules of M if for each open neighbourhood U of 0 in M, the set $T(U) = \{t \in T | M_t \subset U\}$ is open in T.

Definition 2.1 ([6])**.** Let M be a profinite $\mathbb{Z}_pH$-module, T a Boolean space and $\{M_t | t \in T\}$ a continuous system of $\mathbb{Z}_pH$-submodules of M. We say that M is a profinite direct sum of M_t, $t \in T$, notation $M = \bigoplus_{t\in T} M_t$ if:

(1) $M_s \cap M_r = \{0\} \, \forall \, r \neq s \in T$ and
(2) The following universal property holds: any given continuous map $\lambda : \bigcup_{t\in T} M_t \longrightarrow K$ to a profinite $\mathbb{Z}_pH$-module K such that each restriction $\lambda_{|M_t} : M_t \longrightarrow K$ is a continuous $\mathbb{Z}_pH$-homomorphism, extends to a unique continuous $\mathbb{Z}_pH$-homomorphism $\overline{\lambda} : \bigoplus_{t\in T} M_t \longrightarrow K$.

The concept of a free pro-p product of a continuous system of closed subgroups over a Boolean space is defined in a manner analogous to Definition 2.1.

Let G be a pro-p group having an open free pro-p subgroup F. Then the set $\mathcal{T}$ of all subgroups of order p in G is a profinite space of indices, since it is the projective limit of corresponding finite discrete spaces of quotients G/U, where U runs through the open normal subgroups of G which are contained in F. Moreover, G acts continuously on $\mathcal{T}$ by conjugation.

Theorem 2.2 (Theorem 2.2 [5])**.** *Let $G \cong F \rtimes C_{p^n}$ be a cyclic extension of a free pro-p group F. Suppose $\mathcal{T} \longrightarrow \mathcal{T}/G$ admits a continuous section σ. Then*

$$G \cong \left(\coprod_{T\in\sigma(\mathcal{T}/G)} C_G(T) \right) \coprod \widetilde{F}$$

is a free pro-p product of the centralizers $C_G(T)$ of groups T of order p over a Boolean space $\sigma(\mathcal{T}/G)$ of indices and a free pro-p subgroup $\widetilde{F}$ of F. Moreover, each $C_G(T)$ is a semidirect product of open free pro-p subgroup of F by a finite cyclic group of order p^k, where $1 \leq k \leq n$.

Corollary 2.3. *Suppose $C_F(t) = \{1\}$ for every torsion element $t \neq 1$ of G. Then $G = \left(\coprod_{i\in I} T_i\right) \amalg F(X)$ is a free pro-p product of groups $T_i \cong C_{p^{k_i}}$, where $1 \leq k_i \leq n$, $F(X)$ is a free pro-p group and I is a profinite space.*

Proof. Since in our case F acts freely on the profinite space $\mathcal{T}$ of subgroups of order p, $\mathcal{T} \longrightarrow \mathcal{T}/F$ admits a continuous section $\sigma : \mathcal{T}/F \longrightarrow \mathcal{T}$ (see Lemma 5.6.5 in [9]). Put $I = \mathrm{Im}(\sigma)$. Since by hypothesis $C_G(T)$ is finite cyclic for each T, by Theorem 2.2 we get the required decomposition. □

Remark 2.4. Since a torsion free abelian pro-p group is free abelian (see Chapter 4 in [9]), $\mathbb{Z}_p$-torsion freeness is equivalent to $\mathbb{Z}_p$-freeness, thus we shall use this shorter term in the rest of the paper.

3. The Heller–Reiner decomposition

Lemma 3.1. *The equation $(\theta_p - 1)x = pz$ has a solution in any quotient ring R of $\mathbb{Z}_p[\theta_p]$ for any $z \in R$.*

Proof. Since the maximal ideal of $\mathbb{Z}_p[\theta_p]$ is principal with $\theta_p - 1$ being a generator (see Proposition 7.13 [1]), the solution exists in $\mathbb{Z}_p[\theta_p]$. Let $\phi : \mathbb{Z}_p[\theta_p] \to R$ be the canonical epimorphism. Denote by $\tilde{z}$ an element of $\mathbb{Z}_p[\theta_p]$ such that $\phi(\tilde{z}) = z$. Then by the above $(\theta_p - 1)x = p\tilde{z}$ has a solution r in $\mathbb{Z}_p[\theta_p]$. Then $\phi(r)$ is a required solution. □

Lemma 3.2. *Let M be a $\mathbb{Z}_p[\theta_p]$-module. Suppose M is divisible as an abelian group. Then M is a divisible $\mathbb{Z}_p[\theta_p]$-module.*

Proof. It suffices to show that the multiplication by $\theta_p - 1$ is an automorphism of M. In other words we need to show that for any $y \in M$ the equation $(\theta_p - 1)x = y$ has a solution in M, since each element $a \in \mathbb{Z}_p[\theta_p]$ is of the form $(\theta_p - 1)^n \cdot \epsilon$, with $\epsilon \in (\mathbb{Z}_p[\theta_p])^\times$ for some non-negative integer n (see pp. 121 [1]). As M is p-divisible, $y = pz$ for some $z \in M$. Let $\langle z \rangle$ be the submodule of M generated by z. Then $\langle z \rangle$ as a cyclic module is isomorphic to some quotient ring of $\mathbb{Z}_p[\theta_p]$ (see Theorem 2.2 in [10]), so that the result follows from Lemma 3.1. □

Lemma 3.3. *Let $C = \langle x \rangle$ be a cyclic group of order p and let B be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_pC$-module. Suppose that B is annihilated by $\phi_p(x) = 1 + x + \cdots + x^{p-1}$. Then B is a free pro-p $\mathbb{Z}_p[\theta_p]$-module.*

Proof. Consider the dual module $B^* = \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$. Since B is $\mathbb{Z}_p$-free, by Theorem 4.3.3 in [9] $B \cong \prod \mathbb{Z}_p$ and so $B^* \cong \bigoplus_J \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong \bigoplus_J \mathbb{Q}_p/\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module, where J is some indexing set. Since $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible it follows from Exercise 3.17 in [10] that B^* is a divisible $\mathbb{Z}_p$-module. By Lemma 3.2 B^* is divisible as a $\mathbb{Z}_p[\theta_p]$-module and since $\mathbb{Z}_p[\theta_p]$ is a principal ideal domain (page 121 in [7]), it follows that B^* is injective as a $\mathbb{Z}_p[\theta_p]$-module (cf. Theorem 3.24 in [10]). Therefore B is a projective $\mathbb{Z}_p[\theta_p]$-module and as $\mathbb{Z}_p[\theta_p]$ is a local pro-p ring, B is a free pro-p $\mathbb{Z}_p[\theta_p]$-module (see [11], pp. 127). □

Lemma 3.4. *Let $C = \langle x \rangle$ be a cyclic group of order p and let M be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_pC$-module. Let $\phi_p : M \longrightarrow M$ be the $\mathbb{Z}_pC$-homomorphism $m \longmapsto \phi_p(x)m$ and let π be the canonical $\mathbb{Z}_pC$-epimorphism of M onto M/pM. Then the kernel of $\pi \circ \phi_p$ is equal to $\left(M^C \oplus M_{p-1}\right) + pM$, where M_{p-1} is the $\mathbb{Z}_pC$-submodule annihilated by the cyclotomic polynomial $\phi_p(x)$ and M^C is the $\mathbb{Z}_pC$-submodule of fixed points for the action of C on M.*

Proof. Clearly $M^C \subset \mathrm{Ker}(\pi \circ \phi_p)$, because for all $m \in M^C$, we have $\phi_p(x)m = pm$ whence $(\pi \circ \phi_p)(m) = 0$. On the other hand $\phi_p(x)M_{p-1} = \{0\}$, so M_{p-1} is contained in the kernel of $\pi \circ \phi_p$. Thus, we must prove the converse containment. Suppose on the contrary that $\mathrm{Ker}(\pi \circ \phi_p) \not\subset (M_{p-1} + M^C + pM)$. In this case, there is an element $m \in \mathrm{Ker}(\pi \circ \phi_p) \setminus (M^C + M_{p-1} + pM)$. Since cyclic modules are only of the form $\mathbb{Z}_p$, $\mathbb{Z}_p[\theta_p]$ and $\mathbb{Z}_pC$ (see Theorem 2.6 in [4]), one has $\langle m \rangle \cong \mathbb{Z}_pC_p$, and so $\phi_p(x)m = py$ for some $0 \neq y \in M$. It follows that $(x-1)\phi_p(x)m = (x-1)py = 0$, i.e. $py \in M^C$. Since M is $\mathbb{Z}_p$-free, it follows that $y \in M^C$. Then $\phi_p(x)(m - y) = py - py = 0$ and so $m = (m - y) + y \in M_{p-1} + M^C$ as needed. The proof is finished. □

Lemma 3.5. *Let $C = \langle x \rangle$ be a cyclic group of order p and let M be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_pC$-module. Let L be a free pro-p $\mathbb{Z}_pC$-submodule of M. Then $M^C/(M^C \cap L)$ is a free pro-p $\mathbb{Z}_p$-module and $M_{p-1}/(M_{p-1} \cap L)$ is a free pro-p $\mathbb{Z}_p[\theta_p]$-module.*

Proof. If $L = \{0\}$, there is nothing to prove. Suppose $L \neq \{0\}$. Since L is $\mathbb{Z}_pC$-free, $L \cap M^C = L^C = \phi_p(x)L$ and $L_{p-1} := L \cap M_{p-1} = (x-1)L$. Let $y \in M^C \setminus (M^C \cap L)$ be such that $py \in M^C \cap L$. Then we can find an element l of some free $\mathbb{Z}_pC$-basis for L such that py belongs to the free cyclic pro-p $\mathbb{Z}_pC$-submodule $\langle l \rangle$. Namely, if l_0 is a generator of L^C as a trivial $\mathbb{Z}_pC$-module and such that $py \in \langle l_0 \rangle$, then l can be chosen arbitrarily such that $l_0 = \phi_p(x)l$. Then the pro-p $\mathbb{Z}_pC$-submodule $\langle y, l \rangle$ of M is finitely generated and so by the classical Heller–Reiner decomposition (cf. [4]) it decomposes as a direct sum of $\mathbb{Z}_pC$-submodules: $\langle y, l \rangle = \langle l \rangle \oplus L_1$, where L_1 is a trivial $\mathbb{Z}_pC$-submodule of M^C. Hence $\langle y, l \rangle / (M^C \cap \langle y, l \rangle)$ is $\mathbb{Z}_p$-torsion free, contradicting our assumptions on y. Thus $M^C/(M^C \cap L)$ is $\mathbb{Z}_p$-torsion free and so by Remark 2.4 is a free pro-p $\mathbb{Z}_p$-module. Similarly let $z \in M_{p-1} \setminus (L \cap M_{p-1})$ be such that $pz \in L \cap M_{p-1}$. Then we can find an element l' of some free $\mathbb{Z}_pC$-basis for L such that pz belongs to the free cyclic pro-p $\mathbb{Z}_pC$-submodule $\langle l' \rangle$. Namely, taking l_0 to be an element outside of the product IM_{p-1} such that $pz \in \langle l_0 \rangle$, where I is the maximal ideal of $(x-1)\mathbb{Z}_pC$, one can choose l' to be any element element such that $(x-1)l' = l_0$. Then $\langle z, l' \rangle$ decomposes as a direct sum of $\mathbb{Z}_pC$-submodules: $\langle l' \rangle \oplus R$, where R is a free cyclic $\mathbb{Z}_p[\theta_p]$-module (see cf. [4]). Hence$\langle z, l' \rangle / (M_{p-1} \cap \langle z, l' \rangle)$ is $\mathbb{Z}_p$-torsion free, contradicting our assumptions on z. Thus, $M_{p-1}/(M_{p-1} \cap L)$ is $\mathbb{Z}_p$-torsion free and so by Lemma 3.3 is a free pro-p $\mathbb{Z}_p[\theta_p]$-module. □

Theorem A. *Let $C = \langle x \rangle$ be a group of order p and let M be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_pC$-module. Then M decomposes as*

$$M = M_T \oplus M_{\theta_p} \oplus L,$$

where L is a free pro-p $\mathbb{Z}_pC$-submodule of M, M_T is a trivial $\mathbb{Z}_pC$-module and M_{θ_p} is a free pro-p $\mathbb{Z}_p[\theta_p]$-module. Moreover, $M_T \cong \bigoplus_\gamma \mathbb{Z}_p$, $M_{\theta_p} \cong \bigoplus_\beta J(\mathbb{Z}_pC)$ and $L \cong \bigoplus_\phi \mathbb{Z}_pC$ as pro-p $\mathbb{Z}_pC$-modules, where γ, β, ϕ are Boolean space of indices.

Proof. Consider M/pM as a pro-p $\mathbb{F}_pC$-module. Then $\widetilde{M} := \mathrm{Hom}\,(M/pM, \mathbb{F}_p)$ is a discrete $\mathbb{F}_pC$-module. Consider the family of all injective $\mathbb{F}_pC$-submodules of M/pM partially ordered by inclusion. Since $\mathbb{F}_pC$ is a Noetherian ring, it follows from Theorem 4.10 in [10], that the direct limit of such injective $\mathbb{F}_pC$-submodules is injective, so that by Zorn's Lemma there exists a maximal injective $\mathbb{F}_pC$-submodule $\widetilde{L}$ in $\widetilde{M}$. Now $\widetilde{L}$ has a complement $\widetilde{K}$ in $\widetilde{M}$, i.e. $\widetilde{M} = \widetilde{L} \oplus \widetilde{K}$. By Pontryagin duality (see [3], pp. 332)

$$M/pM \cong \mathrm{Hom}(\widetilde{L} \oplus \widetilde{K}, \mathbb{F}_p) \cong \mathrm{Hom}(\widetilde{L}, \mathbb{F}_p) \oplus \mathrm{Hom}(\widetilde{K}, \mathbb{F}_p).$$

Put $\bar{L} := \mathrm{Hom}(\widetilde{L}, \mathbb{F}_p)$ and $\bar{K} := \mathrm{Hom}(\widetilde{K}, \mathbb{F}_p)$. We shall identify $\bar{L}$ with the copy of $\bar{L}$ in M/pM, and do the same with $\bar{K}$. Then $\bar{L}$ is projective $\mathbb{F}_pC$-submodule of M/pM. As $\mathbb{F}_pC$ is a local pro-p ring (see Proposition 7.5.3, pp.126 in [11]) $\bar{L}$ is a free $\mathbb{F}_pC$-submodule of M/pM (see Corollary 7.5.4, pp. 127 in [11]).

Let $\pi : M \longrightarrow M/pM$ be the natural epimorphism. By Proposition 2.2.2 in Ribes–Zalesskii [9], π admits a continuous section $\delta : M/pM \longrightarrow M$ with $\delta(0 + M) = 0$. Consider a profinite space Ω of free generators of $\bar{L}$ converging to 0. Put $\mathcal{X} = \delta(\Omega)$. Let L be the closed $\mathbb{Z}_pC$-submodule of M topologically generated by $\mathcal{X}$. Then L is a free pro-p $\mathbb{Z}_pC$-submodule on $\mathcal{X}$. Indeed, let A be a free pro-p $\mathbb{Z}_pC$-module on $\mathcal{X}$ and $f : A \longrightarrow L$ be the $\mathbb{Z}_pC$-epimorphism induced by sending $\mathcal{X}$ identically to its copy in L. Then as a pro-p group A is free pro-p abelian on the basis $C\mathcal{X}$. Since $\bar{L}$ is a free

$\mathbb{F}_pC$-module on Ω, it is an elementary abelian pro-p group on $C\Omega$. This shows that the kernel of f is contained in the Frattini subgroup $\Phi(A)$. But a homomorphism of free abelian pro-p groups with the kernel in the Frattini subgroup is an isomorphism. Thus f is an isomorphism.

Let M^C be the pro-p $\mathbb{Z}_pC$-submodule of fixed points in M, i.e., the closed $\mathbb{Z}_pC$-submodule of M, annihilated by $(x-1)$. Consider the natural epimorphism $s : M^C \longrightarrow M^C/(L\cap M^C)$. As by Lemma 3.5 $M^C/(L\cap M^C)$ is free pro-p as a $\mathbb{Z}_p$-module, it follows that $M^C = (L \cap M^C) \oplus U$, where U is a complement for $L \cap M^C$.

Now consider the pro-p $\mathbb{Z}_pC$-submodule M_{p-1} of M annihilated by $(\phi_p(x))$. By Lemma 3.3, M_{p-1} is a free pro-p $\mathbb{Z}_p[\theta_p]$-module. Consider the natural epimorphism $r : M_{p-1} \longrightarrow M_{p-1}/(L \cap M_{p-1})$. As by Lemma 3.5 $M_{p-1}/(L \cap M_{p-1})$ is a free pro-p $\mathbb{Z}_p[\theta_p]$-module, we have $M_{p-1} = (L \cap M_{p-1}) \oplus V$, where V is a pro-p $\mathbb{Z}_p[\theta_p]$-submodule of M_{p-1}.

Thus $L \cap V = \{0\}$ and so $L + V = L \oplus V$. As $M^C \cap M_{p-1} = \{0\}$ one has $U\cap(L+V) = \{0\}$ so that $L+U+V = L\oplus U\oplus V$. We want to show that $M = L\oplus U\oplus V$ as a pro-p $\mathbb{Z}_pC$-module.

It suffices to prove that $M = \langle M^C, M_{p-1}, L\rangle$ as a $\mathbb{Z}_pC$-module, since $U \oplus V \oplus L$ contains $L\cap M^C, U, V$, $L\cap M_{p-1}$ and $M_{p-1} = (L\cap M_{p-1})\oplus V$, $M^C = (L\cap M^C)\oplus U$.

Consider the following diagram:

$$\begin{array}{ccc} M & \xrightarrow{\phi_p} & M \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ M/pM & \xrightarrow[\bar{\phi}_p]{} & M/pM, \end{array}$$

where $\phi_p : M \longrightarrow M$ is a $\mathbb{Z}_pC$-homomorphism sending $m \longmapsto \phi_p(x)m$, π is the canonical $\mathbb{Z}_pC$-epimorphism of M to M/pM and $\overline{\phi_p} : M/pM \longrightarrow M/pM$ is a $\mathbb{Z}_pC$-homomorphism sending $\bar{m} \longmapsto \phi_p(x)\bar{m}$. Clearly the diagram is commutative.

Recall that $\bar{L}$ is a free $\mathbb{F}_pC$-submodule of M/pM and $M/pM \cong \bar{L} \oplus \bar{K}$, where $\bar{K}$ is a $\mathbb{F}_pC$-complement of $\bar{L}$ in M/pM. By the commutativity of the above diagram the preimage of $\bar{K}$ in M is contained in $\mathrm{Ker}(\pi \circ \phi_p)$. By Lemma 3.4, $M = \langle L, \mathrm{Ker}(\pi\circ\phi_p)\rangle = \langle L, M^C + M_{p-1} + pM\rangle$ as a free abelian pro-p group. As $pM = \Phi(M)$ is the Frattini subgroup of the abelian pro-p group M, we have $M = L + M^C + M_{p-1}$. Finally put $M_T = U$ and $M_{\theta_p} = V$.

The second part of the statement follows from the definition of a free module on a Boolean space of indices (see page 108 in [6]). □

4. Finite centralizers of torsion elements

Theorem B. *Let $G = U \rtimes H$ be a pro-p semidirect product of a free pro-p group U and a cyclic group H of order p^n. Suppose that the centralizers of all non-identity elements of finite order in G are finite. Then*

$$U^{ab} := U/[U,U] \cong \left(\bigoplus_{i\in(I,*)} J_{K_i}(H)\right) \bigoplus L$$

is a profinite direct sum of pro-p $\mathbb{Z}_pH$-modules, where $(I,*)$ is a Boolean pointed space of indices, the K_i are subgroupss of H, $J_{K_i}(H)$ is the kernel of the canonical epimorphism $\mathbb{Z}_pH \twoheadrightarrow \mathbb{Z}_p(H/K_i)$ and L is a free pro-p $\mathbb{Z}_pH$-module.

Proof. By Corollary 2.3, $G = \left(\coprod_{i\in I} T_i\right) \amalg F(X)$ is a free pro-p product of groups $T_i \cong C_{p^{k_i}}$, where $1 \le k_i \le n$, $F(X)$ is a free pro-p subgroup of U and I is a profinite index space. By Proposition 4.9 in [6], H is conjugate to some finite free factor in G. Thus, we may assume that $H = T_* \cong C_{p^n}$ for some $* \in I$. Let $\phi : G \longrightarrow H$ be the endomorphism identical on H and having U as the kernel.

By Corollary 3.3.10 in Ribes–Zalesskii [9], we have $F(X) = \varprojlim_{\beta\in B} F(X_\beta)$, where X_β runs through the collection of all finite quotient sets of X and $F(X_\beta)$ is a free pro-p group with finite base X_β. Let $I = \varprojlim_{\kappa\in K} I_\kappa$ be a decomposition of I as an inverse limit of finite spaces I_κ such that $\pi_\kappa(i) = \pi_\kappa(j)$ only if $\phi(T_i) = \phi(T_j)$, where $\pi_\kappa : I \longrightarrow I_\kappa$ is the κth projection. Choose a generator for every subgroup of H and let S be the set of these generators. Then for every $i \in I$, there is a unique generator t_i of T_i such that $\phi(t_i) \in S$ and the set of all these generators is homeomorphic to I. Note that a projection π_κ induces the homomorphisms $\coprod_{i\in I} T_i \longrightarrow \coprod_{i_\kappa\in I_\kappa} T_{i_\kappa}$ that identifies t_i with t_j whenever $\pi_\kappa(i) = \pi_\kappa(j)$.

This gives the inverse limit decomposition

$$\begin{aligned} G &\cong \left[\varprojlim_{\kappa\in K}\left(\coprod_{i_\kappa\in I_\kappa} T_{i_\kappa}\right)\right] \coprod \left(\varprojlim_{\beta\in B} F(X_\beta)\right) \\ &\cong \varprojlim_{\kappa\in K,\beta\in B}\left[\left(\coprod_{i_\kappa\in I_\kappa} T_{i_\kappa}\right)\coprod F(X_\beta)\right] \end{aligned}$$

(cf. Lemma 9.1.5 in Ribes–Zalesskii [9]).

Note that ϕ factors via the epimorphisms

$$f_{\kappa,\beta} : \left(\coprod_{i_\kappa\in I_\kappa} T_{i_\kappa}\right)\coprod F(X_\beta) \twoheadrightarrow H$$

and we denote by $U_{\kappa,\beta}$ its kernel.

Then by Corollary 1.1.8 in Ribes–Zalesskii [9], $U = \varprojlim_{K\times B} U_{\kappa,\beta}$. It follows that $U^{ab} \cong \varprojlim_{K\times B} U^{ab}_{\kappa,\beta}$, where $U^{ab}_{\kappa,\beta} := U_{\kappa,\beta}/[U_{\kappa,\beta}, U_{\kappa,\beta}]$.

Put $*_\kappa$ to be the image of $*$ in I_κ. By Proposition 3.3 in [8]

$$U^{ab}_{\kappa,\beta} \cong \left(\bigoplus_{i_\kappa\in I_\kappa\setminus\{*_\kappa\}} J_{K_{i_\kappa}}(H)\right)\bigoplus L_{\kappa,\beta}$$

as a pro-p $\mathbb{Z}_pH$-module, where $L_{\kappa,\beta}$ is a free pro-p $\mathbb{Z}_pH$-module with finite base, $J_{K_{i_\kappa}}(H)$ is the kernel of $\mathbb{Z}_pH \twoheadrightarrow \mathbb{Z}_p(H/K_{i_\kappa})$. Moreover, it follows from the proof there that $L_{\kappa,\beta}$ has the image of X_β in $U^{ab}_{\kappa,\beta}$ as a free $\mathbb{Z}_pH$-basis and that $J_{K_{i_\kappa}}(H)$ is generated by the images of the elements $t_{*_\kappa} t_{i_\kappa}^{-1}$ in the abelianization of $U_{\kappa,\beta}$, where

$t_{*_\kappa} \in T_{*_\kappa} \cong H$, $t_{i_\kappa} \in T_{i_\kappa}$ with $U_{\kappa,\beta} t_{i_\kappa} = U_{\kappa,\beta} t_{*_\kappa}$. Note that since I_κ is finite discrete space, $I_k \setminus \{*_k\} = (I_k, *_\kappa)$ and so

$$\bigoplus_{i_\kappa \in I_\kappa \setminus \{*_k\}} J_{K_{i_\kappa}}(H) = \bigoplus_{i_\kappa \in (I_\kappa, *_\kappa)} J_{K_{i_\kappa}}(H).$$

This means that the decomposition

$$U^{ab}_{\kappa,\beta} \cong \left(\bigoplus_{i_\kappa \in (I_\kappa, *_\kappa)} J_{K_{i_\kappa}}(H) \right) \bigoplus L_{\kappa,\beta}$$

is coherent with the inverse system for U^{ab} and so by the commutation property between projective limits and profinite direct sums (see Proposition 1.6 on pp. 100 combined with 3.1 on page 107 in [6]), we have

$$U^{ab} \cong \varprojlim_{\kappa \in K} \left[\bigoplus_{i_\kappa \in (I_\kappa, *_\kappa)} J_{K_{i_\kappa}}(H) \right] \bigoplus \varprojlim_{\beta \in B} L_{\kappa,\beta} \cong \bigoplus_{i \in (I,*)} J_{K_i}(H) \bigoplus L$$

which is the desired profinite direct sum, where L is a free pro-p $\mathbb{Z}_p H$-module and $(I, *) = \varprojlim_{\kappa \in K} (I_\kappa, *_\kappa)$. □

Remark 4.1. The proof shows that L is a free pro-p $\mathbb{Z}_p H$-module with closed free base $X[U,U]/[U,U]$.

The following corollary is a generalization of Lemma 3.1 in [8].

Corollary 4.2. *If $T_i \cong C_{p^n}$, for all $i \in I$, then*

$$U^{ab} \cong \bigoplus_{i \in (I,*)} J(H) \bigoplus L,$$

where L is a free pro-p $\mathbb{Z}_p H$-module and $J(H)$ is the augmentation ideal of $\mathbb{Z}_p H$.

Corollary 4.3. *With the hypotheses of Theorem B, H acts faithfully on $U^{ab} := U/[U,U]$.*

Proof. The proof is the same as in Corollary 3.4 in Porto–Zalesskii [8], pp. 229. □

Corollary 4.4. *The $\mathbb{Z}_p H$-module U^{ab} of Theorem B is indecomposable as a $\mathbb{Z}_p H$-module if and only if G has not more than two free factors and $|X| \leq 1$.*

Proof. By Proposition 2.1 in [8], $J_{K_i}(H)$ is indecomposable $\mathbb{Z}_p H$-module for every $i \in (I,*)$. Hence the result follows from Theorem B. □

Now we are ready to prove

Theorem C. *Let M be a $\mathbb{Z}_p$-free pro-p $\mathbb{Z}_p C_p$-module. Then there exists a pro-p semidirect product $F \rtimes C_p$ of a free pro-p group F and a group C_p of order p such that F^{ab} is isomorphic to M as a pro-p $\mathbb{Z}_p C_p$-module.*

Proof. Let c be a generator of C_p. By Theorem A, M decomposes as

$$M = M_T \oplus M_{\theta_p} \oplus L,$$

where L is a free pro-p $\mathbb{Z}_pC_p$-submodule of M, M_T is a trivial pro-p $\mathbb{Z}_pC_p$-module and M_{θ_p} is a free pro-p $\mathbb{Z}_p[\theta_p]$-module; let X, Y, Z be free profinite bases of M_T, M_{θ_p}, L, respectively. Put $Y_0 := \bigcup_{j=0}^{p-2} c^jY$, $Z_0 := \bigcup_{t=0}^{p-1} c^tZ$ and $W := X \cup Y_0 \cup Z_0$. Let $F = F(W)$ be the free pro-p group on W. Define a pro-p semidirect product $F \rtimes C_p$ putting for all $x \in X : x^c = x$; for each $y \in Y : (c^ky)^c = c^{k+1}y$ for $0 \leqslant k \leqslant p-3$ and $(c^{p-2}y)^c = \left(\prod_{r=0}^{p-2} c^ry\right)^{-1}$; and for all $z \in Z : (c^sz)^c = c^{s+1}z$ where $0 \leqslant s \leqslant p-1$; to be the action on the elements of the basis W and extending it to the action on F by the universal property of F. Then $F(X)^{ab} \cong M_T$, $F(Y_0)^{ab} \cong M_{\theta_p}$ and $F(Z_0)^{ab} \cong L$ as pro-p $\mathbb{Z}_pC_p$-modules, so that

$$F^{ab} \cong F(X)^{ab} \oplus F(Y_0)^{ab} \oplus F(Z_0)^{ab} \cong M. \qquad \square$$

Acknowledgments

The first author was partially supported by FAPEMIG, and the second author by CAPES and CNPq.

References

[1] J.W.S. Cassels and A. Frohlich, *Algebraic number theory*, Academic Press, London, New York, 1967.
[2] C.W. Curtis and I. Reiner, *Methods of representation theory — with applications to finite groups and ordes*, Wiley, New York, 1981.
[3] J. Flood, *Pontryagin duality for topological modules*, Proc. Amer. Math. Soc. **75**(2) (1979), 329–333.
[4] A. Heller and I. Reiner, *Representations of cyclic groups in ring of integers I*, Ann. Math. **76**(2) (1962), 73–92.
[5] W.N. Herfort and P.A. Zalesskii, *Cyclic extensions of free pro-p groups*, J. Algebra **216** (1999), 511–547.
[6] O.V. Mel'nikov, *Subgroups and homology of free products of profinite groups*, Math. USSR, Iz. **34** (1990), 97–119.
[7] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin–Heidelberg, New York, 1999.
[8] A.L.P. Porto and P.A. Zalesskii, *Free-by-finite pro-p groups and p-adic integral representations*, Arch. Math. **97** (2011), 225–235.
[9] L. Ribes and P.A. Zalesskii, *Profinite groups*, **40**, Springer-Verlag, Berlin–Heidelberg, New York, 2nd ed., 2010.
[10] J.J. Rotman, *An introduction to homological algebra*, Academic Press, University Illinois, Urbana, Illinois, 1979.
[11] J.S. Wilson, *Profinite groups*, Clarendon Press, Oxford, 1998.

Instituto de Ciência e Tecnologia (ICT), UFVJM, 39100-000, Diamantina-MG, Brazil
E-mail address: ander.porto@ict.ufvjm.edu.br

Departamento de Matemática, Universidade de Brasília, 70910-900, Brasília-DF, Brazil
E-mail address: pz@mat.unb.br