Université Grenoble Alpes

ANNALES DE L'INSTITUT FOURIER

Daciberg Lima Gonçalves, John Guaschi & Oscar Ocampo

Embeddings of finite groups in $B_n/\Gamma_k(P_n)$ for $k = 2, 3$

Tome 70, nº 5 (2020), p. 2005-2025.
<http://aif.centre-mersenne.org/item/AIF_2020__70_5_2005_0>

Ann. Inst. Fourier, Grenoble
70, 5 (2020) 2005-2025

EMBEDDINGS OF FINITE GROUPS IN $B_n/\Gamma_k(P_n)$ FOR $k = 2, 3$

by Daciberg LIMA GONÇALVES,
John GUASCHI & Oscar OCAMPO

Abstract. — Let $n \geqslant 3$ and $k \in \{2, 3\}$. We study the embedding of a given finite group G in the quotient $B_n/\Gamma_k(P_n)$, where B_n is the n^{th} Artin braid group, $\{\Gamma_l(P_n)\}_{l \in \mathbb{N}}$ is the lower central series of the n^{th} pure braid group P_n, and $|G|$ denotes the order of G. If such an embedding exists, it is known that $\gcd(|G|, k!) = 1$. In this paper, we show that if G is a finite group for which $\gcd(|G|, k!) = 1$, then G embeds into $B_{|G|}/\Gamma_k(P_{|G|})$. If $k = 2$, the result was proved independently by Beck and Marin. If $G = \mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_d$, where the action θ is injective, p is an odd prime, $p \geqslant 5$ if $k = 3$, and d divides $p-1$ and satisfies $\gcd(d, k!) = 1$, we show that G embeds into $B_{p^r}/\Gamma_k(P_{p^r})$. If $k = 2$, this is a special case of another result of Beck and Marin. We also construct explicit embeddings in $B_9/\Gamma_2(P_9)$ of the two non-Abelian groups of order 27.

Résumé. — Soient $n \geqslant 3$ et $k \in \{2, 3\}$. Nous étudions le plongement d'un groupe fini donné G dans le quotient $B_n/\Gamma_k(P_n)$, où B_n est le n^{e} groupe de tresses d'Artin, $\{\Gamma_l(P_n)\}_{l \in \mathbb{N}}$ est la série centrale descendante du n^{e} groupe de tresses pures P_n, et $|G|$ désigne l'ordre de G. Si un tel plongement existe, on sait que $\operatorname{pgcd}(|G|, k!) = 1$. Si G est un groupe fini pour lequel $\operatorname{pgcd}(|G|, k!) = 1$, nous montrons dans cet article que G se plonge dans $B_{|G|}/\Gamma_k(P_{|G|})$. Si $k = 2$, ce résultat a été démontré indépendamment par Beck et Marin. Si $G = \mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_d$, où l'action θ est injective, p est un nombre premier impair, $p \geqslant 5$ si $k = 3$, et d divise $p-1$ et vérifie $\operatorname{pgcd}(d, k!) = 1$, nous montrons que G se plonge dans $B_{p^r}/\Gamma_k(P_{p^r})$. Si $k = 2$, c'est un cas particulier d'un autre résultat de Beck et Marin. Nous construisons également des plongements explicites des deux groupes non-abéliens d'ordre 27 dans $B_9/\Gamma_2(P_9)$.

1. Introduction

If $n \in \mathbb{N}$, let B_n denote the *(Artin) braid group* on n strings. It is well known that B_n admits a presentation with generators $\sigma_1, \ldots, \sigma_{n-1}$ that

Keywords: Braid groups, quotients, embedding of finite groups.
2020 *Mathematics Subject Classification:* 20F36, 20F18, 20F14, 20B35, 16S34.

are subject to the relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ for all $1 \leqslant i < j \leqslant n-1$ for which $|i-j| \geqslant 2$, and $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for all $1 \leqslant i \leqslant n-2$. Let $\sigma\colon\ B_n \to S_n$ denote the surjective homomorphism onto the symmetric group S_n defined by $\sigma(\sigma_i) = (i, i+1)$ for all $1 \leqslant i \leqslant n-1$. The *pure braid group* P_n on n strings is defined to be the kernel of σ, from which we obtain the following short exact sequence:

$$1 \to P_n \to B_n \xrightarrow{\sigma} S_n \to 1. \tag{1.1}$$

If G is a group, recall that its *lower central series* $\{\Gamma_k(G)\}_{k\in\mathbb{N}}$ is defined by $\Gamma_1(G) = G$, and $\Gamma_k(G) = [\Gamma_{k-1}(G), G]$ for all $k \geqslant 2$ (if H and K are subgroups of G, $[H, K]$ is defined to be the subgroup of G generated by the commutators of the form $[h, k] = hkh^{-1}k^{-1}$, where $h \in H$ and $k \in K$). Note that $\Gamma_2(G)$ is the commutator subgroup of G, and that $\Gamma_k(G)$ is a normal subgroup of G for all $k \in \mathbb{N}$. In our setting, since P_n is normal in B_n, it follows that $\Gamma_k(P_n)$ is also normal in B_n, and the extension (1.1) induces the following short exact sequence:

$$1 \to P_n/\Gamma_k(P_n) \to B_n/\Gamma_k(P_n) \xrightarrow{\overline{\sigma}} S_n \to 1, \tag{1.2}$$

obtained by taking the quotient of P_n and B_n by $\Gamma_k(P_n)$. It follows from results of Falk and Randell [3] and Kohno [7] that the kernel of (1.2) is torsion free (see Proposition 2.1 for more information). The quotient groups of the form $B_n/\Gamma_k(P_n)$ have been the focus of several recent papers. First, the quotient $B_n/\Gamma_2(P_n)$ belongs to a family of groups known as *enhanced symmetric groups* [8, page 201] that were analysed in [11]. Secondly, in their study of pseudo-symmetric braided categories, Panaite and Staic showed that this quotient is isomorphic to the quotient of B_n by the normal closure of the set $\left\{\sigma_i\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}^{-1}\sigma_i\sigma_{i+1}^{-1} \,\middle|\, i = 1, 2, \ldots, n-2\right\}$ [10]. Thirdly, in [4], we showed that $B_n/\Gamma_2(P_n)$ is a crystallographic group, and that up to isomorphism, its finite Abelian subgroups are the Abelian subgroups of S_n of odd order. In particular, the torsion of $B_n/\Gamma_2(P_n)$ is the odd torsion of S_n. We also gave an explicit embedding in $B_7/\Gamma_2(P_7)$ of the Frobenius group $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ of order 21, which is the smallest finite non-Abelian group of odd order. As far as we know, this is the first example of a finite non-Abelian group that embeds in a quotient of the form $B_n/\Gamma_2(P_n)$. Almost all of the results of [4] were subsequently extended to the generalised braid groups associated to an arbitrary complex reflection group by Marin [9]. If $p > 3$ is a prime number for which $p \equiv 3 \bmod 4$, he showed that the Frobenius group $\mathbb{Z}_p \rtimes \mathbb{Z}_{(p-1)/2}$ embeds in $B_p/\Gamma_2(P_p)$. Observe that this group cannot be embedded in $B_n/\Gamma_2(P_n)$ for any $n < p$, since $\mathbb{Z}_p$ cannot be embedded in S_n in this case. In another direction, the authors studied some aspects of the quotient $B_n/\Gamma_k(P_n)$ for all $n, k \geqslant 3$, and proved that it is an almost-crystallographic group [5]. For the case $k=3$, it was shown that the torsion of $B_n/\Gamma_3(P_n)$ is the torsion of S_n that is relatively prime with 6. For future reference, we summarise some of these results in the following theorem.

THEOREM 1.1 ([4, Corollary 4], [5, Theorems 2 and 3]). — *Let $n \geqslant 3$.*

(a) *The torsion of the quotient $B_n/\Gamma_2(P_n)$ is equal to the odd torsion of S_n.*

(b) *The group $B_n/\Gamma_3(P_n)$ has no elements of order 2 or 3, and if $m \in \mathbb{N}$ is relatively prime with 6 then $B_n/\Gamma_3(P_n)$ possesses elements of order m if and only if S_n does.*

Almost nothing is known about the torsion and the finite subgroups of $B_n/\Gamma_k(P_n)$ in the case where $k > 3$.

Suppose that $n \geqslant 3$ and $k \geqslant 2$. The results of [4, 5, 9] lead to a number of interesting problems involving the quotients $B_n/\Gamma_k(P_n)$. Given a finite group G, a natural question in our setting is whether it can be embedded in some $B_n/\Gamma_k(P_n)$. In order to formulate some of these problems, we introduce the following notation. Let $|G|$ denote the order of G, let $m(G)$ denote the least positive integer r for which G embeds in the symmetric group S_r, and if $k \geqslant 2$, let $\ell_k(G)$ denote the least positive integer s, if such an integer exists, for which G embeds in the group $B_s/\Gamma_k(P_s)$. The integer $\ell_k(G)$ is not always defined. For example, if G is of even order, Theorem 1.1 (a) implies that G does not embed in any group of the form $B_n/\Gamma_k(P_n)$. However, if $\ell_k(G)$ is defined, then $m(G) \leqslant \ell_k(G)$ using (1.2) and the fact that $P_n/\Gamma_k(P_n)$ is torsion free.

The main aim of this paper is to study the embedding of finite groups in the two quotients $B_n/\Gamma_k(P_n)$, where $k \in \{2,3\}$. In Section 2, we start by recalling some results from [4, 5] about the action of S_n on certain bases of the free Abelian groups $P_n/\Gamma_2(P_n)$ and $\Gamma_2(P_n)/\Gamma_3(P_n)$, which we use to obtain information about the cycle structure of elements of S_n that fix elements of these bases. In Proposition 2.3, using cohomological arguments, we show that a short exact sequence splits if its quotient is a finite group G and its kernel is a free $\mathbb{Z}[G]$-module. This provides a fundamental tool for embedding G in our quotients. In Section 3, we prove the following result.

THEOREM 1.2. — *Let G be a finite group, and let $k \in \{2,3\}$. Then the group G embeds in $B_{|G|}/\Gamma_k(P_{|G|})$ if and only if $\gcd(|G|, k!) = 1$.*

The statement of Theorem 1.2 has been proved independently by Beck and Marin in the case $k=2$ [1] using different methods within the setting of real reflection groups. This result may be viewed as a Cayley-type result for $B_n/\Gamma_k(P_n)$ since the proof makes use of the embedding of G in the symmetric group $S_{|G|}$, as well as Proposition 3.1 that provides sufficient conditions on the fixed points in the image of an embedding of G in S_m for G to embed in $B_n/\Gamma_k(P_n)$. If $\gcd(|G|, k!) = 1$, it follows from this theorem that $\ell_k(G) \leqslant |G|$ by Theorem 1.2, from which we obtain:

$$m(G) \leqslant \ell_k(G) \leqslant |G|. \tag{1.3}$$

The analysis of the inequalities of (1.3) is itself an interesting problem. Using Theorem 1.1, if G is a cyclic group of prime order at least 5 and k is equal to either 2 or 3 then $m(G) = \ell_k(G) = |G|$. In [1, Corollary 13], Beck and Marin show that $m(G) = \ell_2(G)$ for any finite group of odd order in a broader setting. This result may also be obtained by applying [1, Corollary 7] to [4, Corollary 4 and its proof]. We do not currently know whether there exist groups for which $m(G) < \ell_3(G)$.

In Section 4, we study the embedding of certain finite groups in the quotient $B_n/\Gamma_k(P_n)$, where $k \in \{2, 3\}$. In the case $k = 2$, our results are special cases of [1, Corollary 13], but the methods that we use are rather different from those of [1], and they are also valid for the case $k = 3$. In Section 4.1, we consider certain semi-direct products of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$ for which the action θ is injective, and we analyse their possible embedding in $B_n/\Gamma_k(P_n)$. Our main result in this direction is the following.

Theorem 1.3. — *Let $m, n \geqslant 3$, let $G = \mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$, where $\theta\colon \mathbb{Z}_m \to \mathbb{Z}_n$ is the associated action, and let $1 \leqslant t < n$ be such that $\theta(1_m)$ is multiplication by t in $\mathbb{Z}_n$. Assume that $\gcd(t^l - 1, n) = 1$ for all $1 \leqslant l \leqslant m-1$. If mn is odd (resp. $\gcd(mn, 6) = 1$) then G embeds in $B_n/\Gamma_2(P_n)$ (resp. in $B_n/\Gamma_3(P_n)$).*

Using Lemma 4.2 (a), we remark that the hypotheses of Theorem 1.3 imply that the action $\theta\colon \mathbb{Z}_m \to \operatorname{Aut}(\mathbb{Z}_n)$ is injective. As an application of this theorem, we obtain the following corollary.

Corollary 1.4. — *Let p be an odd prime, let $p - 1 = 2^j d$, where d is odd, let d_1 be a divisor of d, and let G be a group of the form $\mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_{d_1}$, where $\theta\colon \mathbb{Z}_{d_1} \to \operatorname{Aut}(\mathbb{Z}_{p^r})$ is injective.*

(a) *If $p \geqslant 3$ then G embeds in $B_{p^r}/\Gamma_2(P_{p^r})$.*

(b) *If $p \geqslant 5$ and d_1 satisfies $\gcd(d_1, 3) = 1$ then G embeds in $B_{p^r}/\Gamma_3(P_{p^r})$.*

Since the group $\mathbb{Z}_{p^r}$ cannot be embedded in S_m for any $m < p^r$, the groups of Corollary 1.4 satisfy $m(G) = \ell_k(G) = p^r$, where $k \in \{2, 3\}$, so the results of this corollary are sharp in this sense, and are coherent with those of [1, Corollary 13] in the case $k = 2$. Further, the groups that appear in [9, Corollary 3.11] correspond to the case where $r = 1$, $p \equiv 3 \bmod 4$, and

$d_1 = (p-1)/2$ is odd. Hence Corollary 1.4 generalises Marin's result to the case where p is any odd prime and d_1 is the greatest odd divisor of $p-1$, and more generally, in the case $k=2$, the family of groups obtained in Theorem 1.3 extends even further that of the Frobenius groups of [9, Corollary 3.11].

At the end of the paper, in Section 4.2, we give explicit embeddings of the two non-Abelian groups of order 27 in $B_9/\Gamma_2(P_9)$. Neither of these groups satisfies the hypotheses of Theorem 1.3. The fact that they embed in $B_9/\Gamma_2(P_9)$ follows from the more general result of [1, Corollary 13], but our approach is different to that of [1]. Within our framework, it is natural to study these two groups, first because with the exception of the Frobenius group of order 21 analysed in [4], they are the smallest non-Abelian groups of odd order, and secondly because they are of order 27, so are related to the discussion in Section 4.1 on groups whose order is a prime power. The direct embedding of these groups in $B_9/\Gamma_2(P_9)$ is computationally difficult due to the fact that the kernel $P_9/\Gamma_2(P_9)$ of (1.2) is of rank 36, but we get round this problem by first considering an embedding in a quotient where the corresponding kernel is free Abelian of rank 9, and then by applying Proposition 2.3. We believe that this technique will prove to be useful for other groups.

If $n \geqslant 3$, it follows from [1, Corollary 13] that the isomorphism classes of the finite subgroups of $B_n/\Gamma_2(P_n)$ are in bijection with those of the subgroups of S_n of odd order. The study of the finite non-cyclic subgroups of $B_n/\Gamma_3(P_n)$ constitutes work in progress.

Acknowledgements

The work on this paper took place during several visits to the Departamento de Matemática, Universidade Federal de Bahia, the Departamento de Matemática do IME – Universidade de São Paulo and to the Laboratoire de Mathématiques Nicolas Oresme UMR CNRS 6139, Université de Caen Normandie. The first and the third authors were partially supported by the FAPESP Projeto Temático “Topologia Algébrica, Geométrica e Diferencial” 2016/24707-4 (Brazil), and the first two authors were partially supported by the CNRS/FAPESP PRC project n° 275209 (France) and n° 2016/50354-1 (Brazil). The third author was initially supported by a project grant n° 151161/2013-5 from CNPq. We would also like to thank Vincent Beck and Ivan Marin for sharing their results with us.

2. Preliminaries

In this section, we recall several results concerning the torsion of the groups $B_n/\Gamma_k(P_n)$, where $k \in \{2,3\}$, as well as some group-cohomological facts from [2] that will be used in this paper. We first state the following result from [5] that we will require.

Proposition 2.1 ([5, Lemma 11]).

(a) *Let $n, k \geqslant 2$. Then the group $P_n/\Gamma_k(P_n)$ is torsion free.*
(b) *Let $n \geqslant 3$, let $k \geqslant l \geqslant 1$, and let G be a finite group. If $B_n/\Gamma_k(P_n)$ possesses a (normal) subgroup isomorphic to G then $B_n/\Gamma_l(P_n)$ possesses a (normal) subgroup isomorphic to G. In particular, if p is prime, and if $B_n/\Gamma_l(P_n)$ has no p-torsion then $B_n/\Gamma_k(P_n)$ has no p-torsion.*

Note that the first part of Proposition 2.1 follows from papers by Falk and Randell [3, Theorem 4.2] and Kohno [7, Theorem 4.5] who proved independently that for all $n \geqslant 2$ and $k \geqslant 1$, the group $\Gamma_k(P_n)/\Gamma_{k+1}(P_n)$ is free Abelian of finite rank, the rank being related to the Poincaré polynomial of certain hyperplane complements.

It is well known that a set of generators for P_n is given by the set $\{A_{i,j}\}_{1\leqslant i<j\leqslant n}$ [6]. If $j > i$ then we take $A_{j,i} = A_{i,j}$. By abuse of notation, for $k \geqslant 2$ and $1 \leqslant i < j \leqslant n$, we also denote the image of $A_{i,j}$ under the canonical projection $P_n \to P_n/\Gamma_k(P_n)$ by $A_{i,j}$. The groups $P_n/\Gamma_2(P_n)$ and $\Gamma_2(P_n)/\Gamma_3(P_n)$ are free Abelian groups of finite rank $n(n-1)/2$ and $n(n-1)(n-2)/6$ respectively [3, Theorem 4.2]. By [4, Section 3, p. 399] (resp. [5, equation (17)]), a basis for $P_n/\Gamma_2(P_n)$ (resp. $\Gamma_2(P_n)/\Gamma_3(P_n)$) is given by:

$$\mathcal{B} = \{A_{i,j} \mid 1 \leqslant i < j \leqslant n\} \text{ (resp. by } \mathcal{B}' = \{\alpha_{i,j,k} \mid 1 \leqslant i < j < k \leqslant n\}), \tag{2.1}$$

where $\alpha_{i,j,k} = [A_{i,j}, A_{j,k}]$. The action by conjugacy of $B_n/\Gamma_2(P_n)$ (resp. of $B_n/\Gamma_3(P_n)$) on $P_n/\Gamma_2(P_n)$ (resp. on $P_n/\Gamma_3(P_n)$) is defined in [4, Proposition 12] (resp. in [5, equation (8)]), and induces an action of S_n on $P_n/\Gamma_2(P_n)$ (resp. on $\Gamma_2(P_n)/\Gamma_3(P_n)$) that we now describe. If $\tau \in S_n$, $A_{i,j} \in \mathcal{B}$ and $\alpha_{i,j,k} \in \mathcal{B}'$ then by [4, Proposition 12] and [5, equation (8)], we have:

$$\begin{cases} \tau \cdot A_{i,j} = A_{\tau^{-1}(i),\tau^{-1}(j)} \text{ and} \\ \tau \cdot \alpha_{i,j,k} = \tau \cdot [A_{i,j}, A_{j,k}] = [A_{\tau^{-1}(i),\tau^{-1}(j)}, A_{\tau^{-1}(j),\tau^{-1}(k)}]. \end{cases} \tag{2.2}$$

The following lemma implies that S_n acts on $\mathcal{B}$ and $\widehat{\mathcal{B}'}$ respectively, where $\widehat{\mathcal{B}'} = \mathcal{B}' \cup \mathcal{B}'^{-1}$. In each case, the nature of the action gives rise by linearity to an action of S_n on the whole group. We also obtain some information about the stabilisers of the elements of $\mathcal{B}$ and $\widehat{\mathcal{B}'}$. This will play a crucial role in the proof of Proposition 3.1.

Lemma 2.2. — *Let $n \geqslant 2$, and let $\tau \in S_n$.*

(a) *Let $A_{i,j}$ be an element of the basis $\mathcal{B}$ of $P_n/\Gamma_2(P_n)$, where $1 \leqslant i < j \leqslant n$. Then the element $\tau \cdot A_{i,j}$ given by the action of S_n on $P_n/\Gamma_2(P_n)$ belongs to $\mathcal{B}$. Further, if $\tau \cdot A_{i,j} = A_{i,j}$ then the cycle decomposition of τ either contains a transposition, or at least two fixed elements.*

(b) *Let $\alpha_{i,j,k}$ be an element of the basis $\mathcal{B}'$ of $\Gamma_2(P_n)/\Gamma_3(P_n)$, where $1 \leqslant i < j < k \leqslant n$. Then the element $\tau \cdot \alpha_{i,j,k}$ given by the action of S_n on $\Gamma_2(P_n)/\Gamma_3(P_n)$ belongs to $\widehat{\mathcal{B}'}$. Further, if $\tau \cdot \alpha_{i,j,k} \in \{\alpha_{i,j,k}, \alpha_{i,j,k}^{-1}\}$ then the cycle decomposition of τ contains either a transposition, or a 3-cycle, or at least three fixed elements.*

Proof.

(a). — The first part follows from (2.2). If $1 \leqslant i < j \leqslant n$ and $\tau \in S_n$ are such that $\tau \cdot A_{i,j} = A_{i,j}$ then $\tau(\{i,j\}) = \{\tau(i), \tau(j)\} = \{i,j\}$, which implies the second part of the statement.

(b). — The first part is a consequence of [5, equation (16)]. Now suppose that $\tau \cdot \alpha_{i,j,k} \in \{\alpha_{i,j,k}, \alpha_{i,j,k}^{-1}\}$, where $1 \leqslant i < j < k \leqslant n$ and $\tau \in S_n$. By [5, equation (18)], we have $\tau(\{i,j,k\}) = \{\tau(i), \tau(j), \tau(k)\} = \{i,j,k\}$, from which we deduce the second part. □

Lemma 2.2 implies that if $G = S_n$ then $\mathcal{B}$ and $\widehat{\mathcal{B}'}$ are G-sets, and the action of G on each of these sets extends to a $\mathbb{Z}$-linear action of G on the free $\mathbb{Z}$-modules $\mathbb{Z}\mathcal{B}$ and $\mathbb{Z}\mathcal{B}'$ respectively, with respect to the embedding of $\widehat{\mathcal{B}'}$ in $\mathbb{Z}\mathcal{B}'$ given by $\alpha_{i,j,k} \longmapsto \alpha_{i,j,k}$ and $\alpha_{i,j,k}^{-1} \longmapsto (-1).\,\alpha_{i,j,k}$, the underlying free Abelian groups being naturally identified with $P_n/\Gamma_2(P_n)$ and $\Gamma_2(P_n)/\Gamma_3(P_n)$ respectively. It follows that $P_n/\Gamma_2(P_n)$ and $\Gamma_2(P_n)/\Gamma_3(P_n)$ each admit a G-module structure inherited from the action of S_n on $\mathcal{B}$ and $\widehat{\mathcal{B}'}$ respectively.

Given a group G, let $\mathbb{Z}[G]$ denote its group ring. The underlying Abelian group, also denoted by $\mathbb{Z}[G]$, may be regarded as a $\mathbb{Z}[G]$-module (or as a G-module) via the multiplication in the ring $\mathbb{Z}[G]$ (see [2, Chapter I, Sections 2 and 3] for more details), namely:

$$g \cdot \sum_{i=1}^{m} n_i g_i = \sum_{i=1}^{m} n_i (g g_i) \tag{2.3}$$

for all $m \in \mathbb{N}$, $g, g_1, \ldots, g_m \in G$ and $n_1, \ldots, n_m \in \mathbb{Z}$. The cohomology of the group G with coefficients in $\mathbb{Z}[G]$ regarded as a G-module is well understood. In the case that G is finite, we have the following result concerning its embedding in certain extensions whose kernel is a free $\mathbb{Z}[G]$-module. First recall that if M is an Abelian group that fits into an extension of the following form:

$$1 \to M \to E \to G \to 1, \tag{2.4}$$

then M is also a $\mathbb{Z}[G]$-module, the action being given by (2.4).

Proposition 2.3. — *Let G be a finite group. Given an extension of the form* (2.4)*, suppose that M is a free $\mathbb{Z}[G]$-module. Then the short exact sequence* (2.4) *splits. In particular, G embeds in E as a subgroup, and the restriction of the projection $E \to G$ to the embedded copy of G is an isomorphism.*

Proof. — First suppose that $M \cong \mathbb{Z}[G]$. By [2, equation 6.5, p. 73], the group $H^*(G, \mathbb{Z}[G])$ is trivial for all $* \geqslant 1$. In particular, $H^2(G, \mathbb{Z}[G]) = 0$, which implies that any extension of the form (2.4) with $M = \mathbb{Z}[G]$ is split [2, Chapter IV, Theorem 3.12], where the action of the quotient on the kernel turns $\mathbb{Z}[G]$ into a $\mathbb{Z}[G]$-module that is isomorphic to the one-dimensional free $\mathbb{Z}[G]$-module. Now suppose that M is an arbitrary free $\mathbb{Z}[G]$-module whose $\mathbb{Z}[G]$-module structure is defined by (2.4). So $M \cong \oplus_J \mathbb{Z}[G]$ as a $\mathbb{Z}[G]$-module for some set J, and:

$$H^2(G, M) \cong H^2\Bigg(G, \bigoplus_J \mathbb{Z}[G]\Bigg) \cong \bigoplus_J H^2(G, \mathbb{Z}[G]) = 0$$

by the first part of the proof. The short exact sequence (2.4) splits as in the case $M \cong \mathbb{Z}[G]$. □

3. Cayley-type results for subgroups of $B_n/\Gamma_k(P_n)$, $k = 2, 3$

Let $k \in \{2, 3\}$. In this section, we prove Theorem 1.2 that may be viewed as an analogue of Cayley's theorem for $B_n/\Gamma_k(P_n)$. The following proposition will be crucial in the proofs of Theorems 1.2 and 1.3.

Proposition 3.1. — *Let $k \in \{2, 3\}$, let G be a finite group whose order is relatively prime with $k!$, let $m \geqslant 3$, and let $\varphi\colon\ G \to S_m$ be an embedding. Assume that for all $g \in G \setminus \{e\}$, $\varphi(g)$ fixes at most $k-1$ elements. Then the group G embeds in $B_m/\Gamma_k(P_m)$.*

Proof. — Assume first that $k=2$, so $|G|$ is odd. Let $\widetilde{G}$ be the (isomorphic) image of G by φ in S_m. Taking the inverse image by $\overline{\sigma}$ of $\widetilde{G}$ in (1.2) with $n=m$ and $k=2$ gives rise to the following short exact sequence:

$$1 \to P_m/\Gamma_2(P_m) \to \overline{\sigma}^{-1}(\widetilde{G}) \xrightarrow{\overline{\sigma}|_{\overline{\sigma}^{-1}(\widetilde{G})}} \widetilde{G} \to 1. \tag{3.1}$$

From Section 2, G, and hence $\widetilde{G}$, acts on the free Abelian group $P_m/\Gamma_2(P_m)$ of rank $m(m-1)/2$, and the restriction of this action to the basis $\mathcal{B}$ is given by (2.2). Let $1 \leqslant i < j \leqslant m$, and let $g \in G$ be such that $\varphi(g)\cdot A_{i,j} = A_{i,j}$. Since $|G|$ is odd, the cycle decomposition of $\varphi(g)$ contains no transposition, and by Lemma 2.2 (a) and the hypothesis on the fixed points of $\varphi(g)$, we see that $g=e$. So for all $1 \leqslant i < j \leqslant m$, the orbit of $A_{i,j}$ contains exactly $|G|$ elements. In particular, $|G|$ divides $m(m-1)/2$, and $\mathcal{B}$ may be decomposed as the disjoint union of the form $\coprod_{k=1}^{m(m-1)/2|G|} \mathcal{O}_k$, where each $\mathcal{O}_k$ is an orbit of length $|G|$. For $k=1,\ldots,m(m-1)/2|G|$, let $e_k \in \mathcal{O}_k$, and let H_k denote the subgroup of $P_m/\Gamma_2(P_m)$ generated by $\mathcal{O}_k$. Then $P_m/\Gamma_2(P_m) \cong \bigoplus_{k=1}^{m(m-1)/2|G|} H_k$, and for all $x \in \mathcal{O}_k$, there exists a unique element $g \in G$ such that $\varphi(g)\cdot e_k = x$. Thus the map that to x associates g defines a bijection between $\mathcal{O}_k$ and G. Since $\mathcal{O}_k$ is a basis of H_k, if $h \in H_k$, there exists a unique family of integers $\{q_g\}_{g\in G}$ such that $h = \prod_{g\in G}(\varphi(g)\cdot e_k)^{q_g}$, and the map $\Phi\colon H_k \to \mathbb{Z}[G]$ defined by $\Phi(h) = \sum_{g\in G} q_g g$ may be seen to be an isomorphism. Further, via Φ, the action of G on H_k corresponds to the usual action of G on $\mathbb{Z}[G]$. More precisely, if $\gamma \in G$, then:

$$\begin{aligned}\Phi(\varphi(\gamma)\cdot h) &= \Phi\left(\varphi(\gamma)\cdot \prod_{g\in G}(\varphi(g)\cdot e_k)^{q_g}\right) = \Phi\left(\prod_{g\in G}(\varphi(\gamma g)\cdot e_k)^{q_g}\right)\\ &= \sum_{g\in G} q_g \gamma g = \gamma\cdot\Phi(h),\end{aligned}$$

the action of γ on $\Phi(h)$ being given by (2.3). Hence $P_m/\Gamma_2(P_m)$ is isomorphic to $\bigoplus_1^{m(m-1)/2|G|} \mathbb{Z}[G]$ as $\mathbb{Z}[G]$-modules, and by Proposition 2.3, we conclude that the extension (3.1) splits. Thus G is isomorphic to a subgroup $\widehat{G}$ of $\overline{\sigma}^{-1}(\widetilde{G})$, which in turn is a subgroup of $B_m/\Gamma_2(P_m)$, and this proves the result in the case $k=2$. Now suppose that $k=3$. Since $\gcd(|G|,6)=1$, $|G|$ is odd, and as above, G is isomorphic to the subgroup $\widehat{G}$ of $B_m/\Gamma_2(P_m)$. Consider the following extension:

$$1 \to \Gamma_2(P_m)/\Gamma_3(P_m) \to B_m/\Gamma_3(P_m) \xrightarrow{\rho} B_m/\Gamma_2(P_m) \to 1,$$

where $\rho\colon B_m/\Gamma_3(P_m) \to B_m/\Gamma_2(P_m)$ denotes the canonical projection. Taking the inverse image of $\widehat{G}$ by ρ gives rise to the following short exact sequence:

$$1 \to \Gamma_2(P_m)/\Gamma_3(P_m) \to \rho^{-1}(\widehat{G}) \xrightarrow{\rho|_{\rho^{-1}(\widehat{G})}} \widehat{G} \to 1. \tag{3.2}$$

Let $\varphi'\colon \widehat{G} \to S_m$ denote the embedding of $\widehat{G}$ in S_m given by composing φ by an isomorphism between $\widehat{G}$ and G. Then $\widehat{G}$ acts on the kernel $\Gamma_2(P_m)/\Gamma_3(P_m)$ of (3.2) via (2.2). Since $\gcd(|\widetilde{G}|, 6) = 1$, for all $\widehat{g} \in \widehat{G} \setminus \{e\}$, the cycle decomposition of $\varphi'(\widehat{g})$ contains neither a transposition nor a 3-cycle, and by hypothesis, $\varphi'(\widehat{g})$ contains at most 2 fixed elements. It follows from Lemma 2.2 (b) that if $\varphi'(\widehat{g}) \cdot \alpha_{i,j,k} \in \{\alpha_{i,j,k}, \alpha_{i,j,k}^{-1}\}$, where $1 \leqslant i < j < k \leqslant n$ and $\widehat{g} \in \widehat{G}$, then $\widehat{g} = e$. In particular, the orbits of $\alpha_{i,j,k}$ and $\alpha_{i,j,k}^{-1}$ are disjoint, every orbit contains exactly $|G|$ elements, and thus $|G|$ divides $m(m-1)(m-2)/6$. So there exists a basis of $\Gamma_2(P_m)/\Gamma_3(P_m)$ that is the disjoint union of $m(m-1)(m-2)/6|G|$ orbits of elements of $\widehat{\mathcal{B}}'$, and that for all $1 \leqslant i < j < k \leqslant n$, contains exactly one element of $\{\alpha_{i,j,k}, \alpha_{i,j,k}^{-1}\}$. As in the case $k = 2$, we conclude that the short exact sequence (3.2) splits, and that G embeds in $B_m/\Gamma_3(P_m)$. □

Remark 3.2. — An efficient way to use Proposition 3.1 is as follows. Let $\varphi\colon G \to S_n$ be an embedding, and for an order-preserving inclusion $\iota\colon \{1, 2, \ldots, m\} \hookrightarrow \{1, 2, \ldots, n\}$, where $m < n$, consider the embedding $S_m \to S_n$. Suppose that the homomorphism φ factors through S_m, and let $\varphi'\colon G \to S_m$ be the factorisation. It may happen that the hypotheses of Proposition 3.1 hold for φ' but not for φ. In this case, we may apply this proposition to φ' to conclude the existence of an embedding of G in $B_m/\Gamma_k(P_m)$, which in turn implies that G embeds in $B_n/\Gamma_k(P_n)$.

We are now able to prove Theorem 1.2.

Proof of Theorem 1.2. — Let G be a finite group, and let $k \in \{2, 3\}$. If G embeds in the group $B_{|G|}/\Gamma_k(P_{|G|})$ then Theorem 1.1 implies that $\gcd(|G|, k!) = 1$. Conversely, suppose that $\gcd(|G|, k!) = 1$. Consider the classical embedding of G in $S_{|G|}$ that is used in the proof of Cayley's theorem (note that we identify S_G with $S_{|G|}$). More precisely, let $\psi\colon G \times G \to G$ denote the action of G on itself given by left multiplication. For all $g \in G$, the map $\psi_g\colon G \to G$ defined by $\psi_g(h) = \psi(g, h) = gh$ is a permutation of G, and the map $\Psi\colon G \to S_{|G|}$ defined by $\Psi(g) = \psi_g$ is an injective homomorphism, so $\widetilde{G} = \{\psi_g \mid g \in G\}$ is a subgroup of $S_{|G|}$ that is isomorphic to G. The action ψ is free: if $h \in G$ then $h = \psi_g(h)$ if and only if $g = e$. In particular, if $g \neq e$ then ψ_g is fixed-point free, and so the permutation $\Psi(g)$ is fixed-point free for all $g \in G \setminus \{e\}$. Taking $m = |G|$, the hypotheses of Proposition 3.1 are satisfied for the embedding $\Psi\colon G \to S_{|G|}$, and we conclude that G embeds in $B_{|G|}/\Gamma_k(P_{|G|})$. □

4. Embeddings of some semi-direct products in $B_n/\Gamma_k(P_n)$, $k \in \{2,3\}$

Let $m, n \in \mathbb{N}$, and let $k \in \{2,3\}$. In this section, we study the problem of embedding groups of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$ in $B_n/\Gamma_k(P_n)$, where the representation $\theta\colon \mathbb{Z}_m \to \operatorname{Aut}(\mathbb{Z}_n)$ is taken to be injective. With additional conditions on θ, in Section 4.1, we prove Theorem 1.3. In Section 4.2, we study the two non-Abelian groups of order 27. The first such group is of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$, where θ is injective, but the additional conditions of Theorem 1.3 are not satisfied. The second such group is not of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$. We prove that both of these groups embed in $B_9/\Gamma_2(P_9)$. In the case of the first group, this shows that the hypotheses of Theorem 1.3 are sufficient to embed $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$ in $B_n/\Gamma_k(P_n)$, but not necessary. With respect to (1.3), these groups also satisfy $m(G) = \ell_k(G) < |G|$, which is coherent with [1, Corollary 13] in the case $k = 2$.

4.1. Proof of Theorem 1.3

Let $m, n \in \mathbb{N}$. In this section, G will be a group of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$. We study the question of whether G embeds in $B_n/\Gamma_k(P_n)$, where $k \in \{2,3\}$. By Theorem 1.1, when $G = \mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$ for such an embedding to exist, $\gcd(|G|, k!) = 1$, and so we shall assume from now on that this is the case. In order to apply Proposition 3.1, we will make use of a specific embedding of G in S_n studied by Marin in the case where n is prime and $m = (n-1)/2$ [9], as well as the restriction to G of the action of S_n on $P_n/\Gamma_2(P_n)$ and $\Gamma_2(P_n)/\Gamma_3(P_n)$ described by equation (2.2). If $q \in \mathbb{N}$, we will denote the image of an integer r under the canonical projection $\mathbb{Z} \to \mathbb{Z}_q$ by r_q, or simply by r if no confusion is possible.

Following [9, proof of Corollary 3.11], we start by describing a homomorphism from K to S_A, for groups of the form $K = A \rtimes_\theta H$, where A and H are finite, A is Abelian, and S_A denotes the symmetric group on the set A. Let $(u, v) \in K$, where the elements of K are written with respect to the semi-direct product $A \rtimes_\theta H$, and let $\varphi_{(u,v)}\colon A \to A$ be the affine transformation defined by:

$$\varphi_{(u,v)}(z) = \theta(v)(z) + u \text{ for all } z \in A. \tag{4.1}$$

Lemma 4.1.

(a) *For all* $(u,v) \in K$*, the map* $\varphi_{(u,v)}\colon A \to A$ *defined in* (4.1) *is a bijection.*
(b) *Let* $\varphi\colon K \to S_A$ *be the map defined by* $\varphi(u,v) = \varphi_{(u,v)}$ *for all* $(u,v) \in K$*. Then* φ *is a homomorphism. Further, if the action* $\theta\colon H \to \operatorname{Aut}(A)$ *is injective then* φ *is too.*

Proof.

(a). — If $(u,v) \in K$, the statement follows from the fact that $\theta(v)$ is an automorphism of A.

(b). — Part (a) implies that the map φ is well defined. We now prove that φ is a homomorphism. If $(u_1,v_1),(u_2,v_2) \in K$, then for all $z \in A$, we have:

$$\begin{aligned}
(\varphi_{(u_2,v_2)} \circ \varphi_{(u_1,v_1)})(z) &= \varphi_{(u_2,v_2)}(\theta(v_1)(z) + u_1)\\
&= \theta(v_2)(\theta(v_1)(z) + u_1) + u_2\\
&= \theta(v_2)(\theta(v_1)(z)) + \theta(v_2)(u_1) + u_2\\
&= \theta(v_2v_1)(z) + \theta(v_2)(u_1) + u_2\\
&= \varphi_{(u_2+\theta(v_2)(u_1),v_2v_1)}(z)\\
&= \varphi_{(u_2,v_2)(u_1,v_1)}(z),
\end{aligned}$$

so $\varphi_{(u_2,v_2)} \circ \varphi_{(u_1,v_1)} = \varphi_{(u_2,v_2)(u_1,v_1)}$, and φ is a homomorphism. Finally, suppose that θ is injective, and let $(u,v) \in \operatorname{Ker}(\varphi)$. Then $z = \varphi(u,v)(z) = \varphi_{(u,v)}(z) = \theta(v)(z) + u$ for all $z \in A$. Taking z to be the trivial element e_A of A yields $u = e_A$. Hence $\theta(v) = \mathrm{Id}_A$, and it follows that v is the trivial element H by the injectivity of θ, which completes the proof of the lemma. □

As above, let G be a semi-direct product of the form $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_m$, where $\theta\colon \mathbb{Z}_m \to \operatorname{Aut}(\mathbb{Z}_n)$ is the associated action. Note that we can apply the construction of equation (4.1) to G, and so the conclusions of Lemma 4.1 hold for G. The element 1_m generates the additive group $\mathbb{Z}_m$, so $\theta(1_m)$ is an automorphism of $\mathbb{Z}_n$ whose order divides m, and since any automorphism of $\mathbb{Z}_n$ is multiplication by an integer that is relatively prime with n, there exists $1 \leqslant t < n$ such that $\gcd(t,n) = 1$, $\theta(1_m)$ is multiplication by t, and $t^m \equiv 1 \bmod n$. If θ is injective, the order of the automorphism $\theta(1_m)$ is equal to m, and so $t^l \not\equiv 1 \bmod n$ for all $1 \leqslant l < m$, but this does not imply that $t^l - 1$ is relatively prime with n. However, the condition that $\gcd(t^l - 1, n) = 1$ for all $1 \leqslant l < m$ is the hypothesis that we require in order to prove Theorem 1.3, and as we shall now see, implies that θ is injective.

Lemma 4.2. — *Let $n,m\in\mathbb{N}$, let G be a semi-direct product of the form $\mathbb{Z}_n\rtimes_\theta\mathbb{Z}_m$, and let $1\leqslant t<n$ be such that $\theta(1_m)$ is multiplication in $\mathbb{Z}_n$ by t. Suppose that $\gcd(t^l-1,n)=1$ for all $1\leqslant l\leqslant m-1$.*

(a) *The action $\theta\colon \mathbb{Z}_m\to \operatorname{Aut}(\mathbb{Z}_n)$ is injective, and the homomorphism $\varphi\colon G\to S_{\mathbb{Z}_n}$ defined in Lemma 4.1 is injective.*
(b) *For all $(u,v)\in G\backslash\{(0_n,0_m)\}$, the permutation $\varphi(u,v)$ fixes at most one element, and if $v\neq 0_m$ then $\varphi(u,v)$ fixes precisely one element.*

Proof.

(a). — To prove the first part, we argue by contraposition. Suppose that θ is not injective. Then there exists $1\leqslant l<m$ such that $\theta(l_m)=\mathrm{Id}_{\mathbb{Z}_n}$. Now $\theta(1_m)$ is multiplication by t, so $\theta(l_m)$ is multiplication by t^l, and thus $t^l\equiv 1 \bmod n$, which implies that $\gcd(t^l-1,n)\neq 1$. The second part of the statement follows from Lemma 4.1 (b).

(b). — Let $(u,v)\in G\backslash\{(0_n,0_m)\}$. If $v=0_m$ then $u\neq 0_n$, so $\varphi_{(u,0_m)}(z)=z+u\neq z$ for all $z\in\mathbb{Z}_n$, hence $\varphi_{(u,0_m)}$ is fixed-point free. So suppose that $v\neq 0_m$. Since $\theta(v)$ is multiplication by t^v, the corresponding affine transformation $\varphi_{(u,v)}\colon \mathbb{Z}_n\to\mathbb{Z}_n$ is given by $\varphi_{(u,v)}(z)=t^vz+u$ for all $z\in\mathbb{Z}_n$. By hypothesis, $\gcd(t^v-1,n)=1$, so t^v-1 is invertible in $\mathbb{Z}_n$, and if $z\in\mathbb{Z}_n$, we have:

$$\varphi_{(u,v)}(z)=z\iff t^vz+u=z\iff (t^v-1)z=-u\iff z=-u(t^v-1)^{-1}$$

in $\mathbb{Z}_n$. Hence $\varphi_{(u,v)}$ possesses a unique fixed point. □

The above framework enables us to prove Theorem 1.3 using Proposition 3.1.

Proof of Theorem 1.3. — Let $\varphi\colon G\to S_{\mathbb{Z}_n}$ be the embedding of G in $S_{\mathbb{Z}_n}$ of Lemma 4.1 (b). By Lemma 4.2 (b), for all $g\in G\setminus\{e\}$, $\varphi(g)$ fixes at most one point. So the embedding φ satisfies the hypotheses of Proposition 3.1, from which we conclude that G embeds in $B_n/\Gamma_2(P_n)$ (resp. in $B_n/\Gamma_3(P_n)$) if mn is odd (resp. if $\gcd(mn,6)=1$). □

As an application of Theorem 1.3, we consider groups of the form $\mathbb{Z}_n\rtimes_\theta H$, where H is finite, $n=p^r$ is a power of an odd prime p, where $r\in\mathbb{N}$, and the homomorphism $\theta\colon H\to\operatorname{Aut}(\mathbb{Z}_{p^r})$ is injective. Recall from [12, p. 146, lines 16–17] that:

$$\operatorname{Aut}(\mathbb{Z}_{p^r})\cong\mathbb{Z}_{(p-1)p^{r-1}}\cong\mathbb{Z}_{p-1}\oplus\mathbb{Z}_{p^{r-1}},\tag{4.2}$$

where the isomorphisms of (4.2) are described in [12, p. 145–146]. We shall now prove Corollary 1.4 by studying injective actions of the form

$\theta\colon H \to \mathbb{Z}_{(p-1)p^{r-1}}$, where H is a cyclic group whose order is an odd divisor of $p-1$. Note that for our purposes, it suffices to take H to be the (unique) subgroup of $\mathbb{Z}_{p-1} \leqslant \operatorname{Aut}(\mathbb{Z}_{p^r})$ of order d_1, and θ to be inclusion.

Proof of Corollary 1.4. — Let $p > 2$ be prime, let $p-1 = 2^j d$, where d is odd, and let d_1 be a divisor of d. So identifying $\operatorname{Aut}(\mathbb{Z}_{p^r})$ with $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{r-1}}$ via (4.2), and taking the subgroup H in the above discussion to be $\mathbb{Z}_{d_1}$, there exists an injective homomorphism $\theta\colon \mathbb{Z}_{d_1} \to \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{r-1}}$, where $\theta(1_{d_1})$ is an automorphism of $\mathbb{Z}_{p^r}$ given by multiplication by an integer t that is relatively prime with p, and the order d_1 of this automorphism is also relatively prime with p. In particular, the order of t in the group $\mathbb{Z}_{p^r}^*$ is equal to d_1. We claim that $\gcd(t^l - 1, p) = 1$ for all $0 < l < d_1$. Suppose on the contrary that $t^l - 1$ is divisible by p for some $0 < l < d_1$. Then $t^l = 1 + kp$, where $k \in \mathbb{N}$, and [12, p. 146, line 12] implies that the order of t^l in $\mathbb{Z}_{p^r}^*$ is a power of p, which contradicts the fact that t is of order d_1 and $\gcd(d_1, p) = 1$. This proves the claim. Part (a) (resp. part (b)) follows using the fact that the order of $\mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_{d_1}$ is odd (resp. relatively prime with 6) and by applying Theorem 1.3. □

Remark 4.3. — As we mentioned in the introduction, the results of Corollary 1.4 are sharp in the sense that if $k \in \{2, 3\}$, the groups $\mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_d$ satisfy $\ell_k(G) = m(G) = p^r$ if $d > 1$, where $k \in \{2, 3\}$. This result no longer holds if we remove the hypothesis that the order of the group being acted upon is a prime power. For example, if in the semi-direct product $G = \mathbb{Z}_n \rtimes \mathbb{Z}_d$, we take $n = 15$ and $d = 1$ then $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5$, and $\ell_2(G) = m(G) = 8 < 15$ using [4, Theorem 3 (b)] or [1, Corollary 13].

4.2. Further examples

In this final section, we give examples of two semi-direct products of the form $\mathbb{Z}_9 \rtimes_\theta \mathbb{Z}_3$ and $(\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_\theta \mathbb{Z}_3$ respectively that do not satisfy the hypotheses of Theorem 1.3, but that embed in $B_9/\Gamma_2(P_9)$. We start with some general comments. If p is an odd prime, consider the group $G = \mathbb{Z}_{p^r} \rtimes_\theta \mathbb{Z}_{p^{r-1}(p-1)}$, where with respect to the notation of [12, p. 146, line 8], the homomorphism $\theta\colon \mathbb{Z}_{p^{r-1}(p-1)} \to \operatorname{Aut}(\mathbb{Z}_{p^r})$ sends $1_{p^{r-1}(p-1)}$ to the element of $\operatorname{Aut}(\mathbb{Z}_{p^r})$ given by multiplication in $\mathbb{Z}_{p^r}$ by t', where $t' = (1+p)g_1$, and where the order of g_1 (resp. $1+p$) is equal to $p-1$ (resp. p^{r-1}) in the multiplicative group $\mathbb{Z}_{p^r}^*$. If d_1 is an odd divisor of $p^{r-1}(p-1)$, let $q = p^{r-1}(p-1)/d_1$, and consider the subgroup $\mathbb{Z}_{p^r} \rtimes_{\theta'} \mathbb{Z}_{d_1}$ of G, where $\mathbb{Z}_{d_1}$ is the subgroup of $\mathbb{Z}_{p^{r-1}(p-1)}$ of order d_1, and $\theta'\colon \mathbb{Z}_{d_1} \to \operatorname{Aut}(\mathbb{Z}_{p^r})$ is the restriction of θ to $\mathbb{Z}_{d_1}$. Then $\theta'(1_d)=\theta(q_{p^{r-1}(p-1)})$ is multiplication by $t=t'^q$ in $\mathbb{Z}_{p^r}$, and by injectivity, t is of order d_1 in $\mathbb{Z}_{p^r}^*$. If further d_1 is divisible by p then $t^{d_1/p}$ is of order p in $\mathbb{Z}_{p^r}^*$, and by [12, p. 146, line 12], $t^{d_1/p}\equiv(1+p)^{\lambda p^{r-2}} \bmod p^r$, where $\lambda\in\mathbb{N}$ and $\gcd(\lambda,p)=1$. It follows that $t^{d_1/p}-1$ is divisible by p, and since $0<d_1/p<d_1$, the hypotheses of Theorem 1.3 are not satisfied for the group $\mathbb{Z}_{p^r}\rtimes_{\theta'}\mathbb{Z}_{d_1}$. As Example 4.4 (a) below shows, if $p=3$ and $r=2$, such a group may nevertheless embed in $B_{p^r}/\Gamma_2(P_{p^r})$. In Example 4.4 (b), we show that the other non-Abelian group of order 27, which is of the form $(\mathbb{Z}_p\oplus\mathbb{Z}_p)\rtimes\mathbb{Z}_p$, also embeds in $B_9/\Gamma_2(P_9)$. It does not satisfy the hypotheses of Theorem 1.3 either.

Examples 4.4. — Suppose that G is a group of order 27 that embeds in S_9. If $k=2$ and $n=9$ in (1.2), taking the preimage of G by $\overline{\sigma}$ leads to the following short exact sequence:

$$1\to P_9/\Gamma_2(P_9)\to\overline{\sigma}^{-1}(G)\xrightarrow{\overline{\sigma}|_{\overline{\sigma}^{-1}(G)}} G\to 1, \tag{4.3}$$

where the rank of the free Abelian group $P_9/\Gamma_2(P_9)$ is equal to 36. As we shall now see, if G is one of the two non-Abelian groups of order 27, the action of S_9 on the basis $\mathcal{B}$ of $P_9/\Gamma_2(P_9)$ given by (2.2) restricts to an action of G on $\mathcal{B}$ for which there are two orbits, that of $A_{1,2}$, which contains 9 elements, and is given by:

$$\mathcal{O}=\{A_{1,2},A_{8,9},A_{5,6},A_{2,3},A_{7,8},A_{4,5},A_{1,3},A_{7,9},A_{4,6}\}, \tag{4.4}$$

and that of $A_{5,9}$, which contains the remaining 27 elements of $\mathcal{B}$. Let H be the subgroup of $P_9/\Gamma_2(P_9)$ generated by the orbit of $A_{5,9}$. Then $H\cong\mathbb{Z}^{27}$, and H is not normal in $B_9/\Gamma_2(P_9)$, but it is normal in the subgroup $\overline{\sigma}^{-1}(G)$ of $B_9/\Gamma_2(P_9)$ since the basis $\mathcal{B}\setminus\mathcal{O}$ of H is invariant under the action of G. We thus have an extension:

$$1\to H\to\overline{\sigma}^{-1}(G)\xrightarrow{\pi}\widetilde{H}\to 1, \tag{4.5}$$

where $\widetilde{H}=\overline{\sigma}^{-1}(G)/H$, and $\pi\colon\overline{\sigma}^{-1}(G)\to\widetilde{H}$ is the canonical projection. Equation (4.3) induces the following short exact sequence:

$$1\to(P_9/\Gamma_2(P_9))/H\to\widetilde{H}\xrightarrow{\widetilde{\sigma}} G\to 1, \tag{4.6}$$

where $\widetilde{\sigma}\colon\widetilde{H}\to G$ is the surjective homomorphism induced by $\overline{\sigma}$, and we also have an extension:

$$1\to H\to P_9/\Gamma_2(P_9)\xrightarrow{\rho}(P_9/\Gamma_2(P_9))/H\to 1, \tag{4.7}$$

obtained from the canonical projection $\rho\colon P_9/\Gamma_2(P_9)\to(P_9/\Gamma_2(P_9))/H$. From the construction of H, and using the fact that $P_9/\Gamma_2(P_9)$ (resp. H) is the free Abelian group of rank 36 (resp. 27) for which $\mathcal{B}$ (resp. $\mathcal{B}\setminus\mathcal{O}$)

is a basis, the kernel of (4.6) is isomorphic to $\mathbb{Z}^9$ and a basis is given by the H-cosets of the nine elements of $\mathcal{O}$. Further, the restriction of ρ to the subgroup of $P_9/\Gamma_2(P_9)$ generated by $\mathcal{O}$ is an isomorphism, and thus the set $\rho(\mathcal{O})$ is a basis of $(P_9/\Gamma_2(P_9))/H$, which we denote by $\mathcal{O}'$. In the examples below, we shall construct an explicit embedding $\iota\colon G \to \widetilde{H}$ of G in $\widetilde{H}$ for which the action of $\iota(G)$ is induced by the embedding of G in S_9 (in other words, the embedding of G in $\widetilde{H}$ is compatible with the action on H). This being the case, using (4.5), we thus obtain the following short exact sequence:

$$1 \to H \to \pi^{-1}(\iota(G)) \xrightarrow{\pi|_{\pi^{-1}(\iota(G))}} \iota(G) \to 1. \tag{4.8}$$

Now H is isomorphic to $\mathbb{Z}[G]$, and the action of $\iota(G)$ on H is given via (2.2). It follows from Proposition 2.3 that the short exact sequence (4.8) splits. Hence G embeds in $\pi^{-1}(\iota(G))$, which is a subgroup of $\overline{\sigma}^{-1}(G)$, and so it embeds in $B_9/\Gamma_2(P_9)$. We could have attempted to embed G in $B_9/\Gamma_2(P_9)$ directly via (4.3). However one of the difficulties with this approach is that the rank of the kernel is 36, whereas that of the kernel of (4.6) is much smaller, and this decreases greatly the number of calculations needed to show that G embeds in $\widetilde{H}$. We now give the details of the computations of this embedding in the two cases.

(a) Up to isomorphism, there is only one non-Abelian group G of order 27 that contains a cyclic group of order 9, so this group is isomorphic to the semi-direct product $\mathbb{Z}_9 \rtimes_{\theta'} \mathbb{Z}_3$ defined in the first paragraph of this subsection. We construct G as a subgroup of S_9 as follows. Consider the elements $\alpha = (1,2,3)(4,5,6)(7)(8)(9)$ and $\beta = (1,4,7,3,5,8,2,6,9)$ of S_9, and let $G = \langle \alpha, \beta \rangle$. Then $\alpha\beta\alpha^{-1} = (\alpha^{-1}(1), \ldots, \alpha^{-1}(9)) = (1,5,9,3,6,7,2,4,8) = \beta^4$, and it follows that the subgroup $\langle \beta \rangle$ of G is normal, and that $G \cong \mathbb{Z}_9 \rtimes \mathbb{Z}_3$, the action being multiplication by 4. With the above notation, one may check that $\mathcal{O}$ and $\mathcal{B} \setminus \mathcal{O}$ are the two orbits arising from the action of G on $\mathcal{B}$ given by (2.2) (for future reference, note that the order of the elements of $\mathcal{O}$ is that obtained by the action of successive powers of β). We define the map $\iota\colon G \to \widetilde{H}$ on the generators of G by $\iota(\alpha) = \widehat{\alpha}$ and $\iota(\beta) = \widehat{\beta}$, where $\widehat{\alpha} = \sigma_2\sigma_1^{-1}\sigma_5\sigma_4^{-1}$ and $\widehat{\beta} = A_{1,2}A_{8,9}^{-1}w\sigma_8\sigma_7\sigma_6\sigma_5\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}w^{-1}$, and where $w = \sigma_3\sigma_6\sigma_2\sigma_3\sigma_4\sigma_5\sigma_4\sigma_3\sigma_7\sigma_6$. By abuse of notation, we will denote an element of $B_9/\Gamma_2(P_9)$ in the same way as its projection on the quotient $(B_9/\Gamma_2(P_9))/H$. We claim that $\widehat{\alpha}\widehat{\beta}\widehat{\alpha}^{-1}\widehat{\beta}^{-4} = 1$ in $\widetilde{H}$, from which we may conclude that ι extends to a group homomorphism.

To prove the claim, using [4, Proposition 12] and the action of β on the orbit of $A_{1,2}$ mentioned above, first note that:

$$\begin{aligned}\widehat{\alpha}\widehat{\beta}\widehat{\alpha}^{-1}\widehat{\beta}^{-4} &= \widehat{\alpha}A_{1,2}A_{8,9}^{-1}b\widehat{\alpha}^{-1}(A_{1,2}A_{8,9}^{-1}b)^{-4}\\ &= A_{1,3}A_{8,9}^{-1}\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}.\, b^3A_{1,2}^{-1}A_{8,9}b^{-3}\\ &\quad .\, b^2A_{1,2}^{-1}A_{8,9}b^{-2}.\, bA_{1,2}^{-1}A_{8,9}b^{-1}.\, A_{1,2}^{-1}A_{8,9}\\ &= A_{1,3}A_{8,9}^{-1}.\, \widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}.\, A_{2,3}^{-1}A_{7,8}.\, A_{5,6}^{-1}A_{2,3}.\, A_{8,9}^{-1}A_{5,6}.\, A_{1,2}^{-1}A_{8,9}\\ &= A_{1,2}^{-1}A_{7,8}A_{1,3}A_{8,9}^{-1}\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}. \end{aligned}\tag{4.9}$$

To obtain the last equality, we have also used the fact that $\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}$ belongs to the quotient $(P_9/\Gamma_2(P_9))/H$, so commutes with the other terms in the expression. To compute $\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}$ in terms of the basis $\mathcal{O}'$ of $(P_9/\Gamma_2(P_9))/H$, we make use of the method of crossing numbers given in [4, Proposition 15], with the difference that since we are working in $(P_9/\Gamma_2(P_9))/H$, using the isomorphism $\rho\big|_{\langle\mathcal{O}\rangle} : \langle\mathcal{O}\rangle \to (P_9/\Gamma_2(P_9))/H$ induced by (4.7), it suffices to compute the crossing numbers of the pairs of strings corresponding to the elements of $\mathcal{O}$ given in (4.4). Using the braid $\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4}$ illustrated in Figure 4.1, one may verify that:

$$\widehat{\alpha}b\widehat{\alpha}^{-1}b^{-4} = A_{1,2}A_{1,3}^{-1}A_{7,8}^{-1}A_{8,9}\tag{4.10}$$

in $(P_9/\Gamma_2(P_9))/H$.

It follows from equations (4.9) and (4.10) that $\widehat{\alpha}\widehat{\beta}\widehat{\alpha}^{-1}\widehat{\beta}^{-4} = 1$ in $\widetilde{H}$, which proves the claim. Thus $\langle\, \widehat{\alpha}, \widehat{\beta}\,\rangle$ is a quotient of G, but since it is non Abelian, and the only non-Abelian quotient of G is itself, we conclude that $\langle\, \widehat{\alpha}, \widehat{\beta}\,\rangle \cong G$, and hence ι is an embedding. It follows from the discussion at the beginning of these examples that G embeds in $\pi^{-1}(\iota(G))$, and therefore in $B_9/\Gamma_2(P_9)$.

(b) We now give an explicit example of a non-Abelian group G of the form $A \rtimes \mathbb{Z}_m$ that embeds in $B_{|A|}/\Gamma_2(P_{|A|})$, where A is a non-cyclic finite Abelian group. To our knowledge, this is the first explicit example of a finite group that embeds in such a quotient but that is not a semi-direct product of two cyclic groups. In particular, this subgroup does not satisfy the hypothesis of Theorem 1.3 either. Let G be the Heisenberg group mod p of order p^3, where p is an odd prime. There exists an extension of the form:

$$1 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \oplus \mathbb{Z}_p \to 1,\tag{4.11}$$

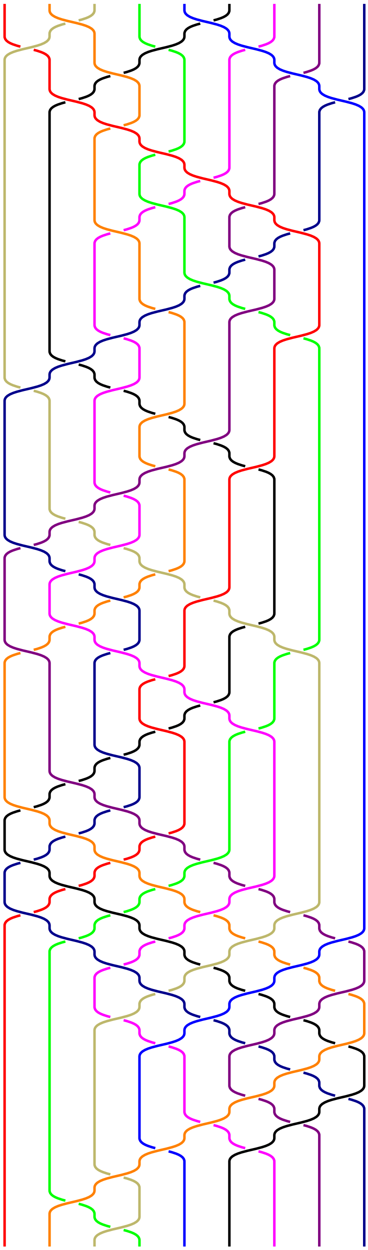
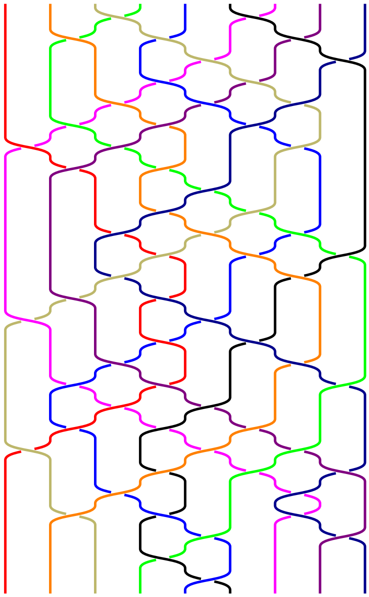
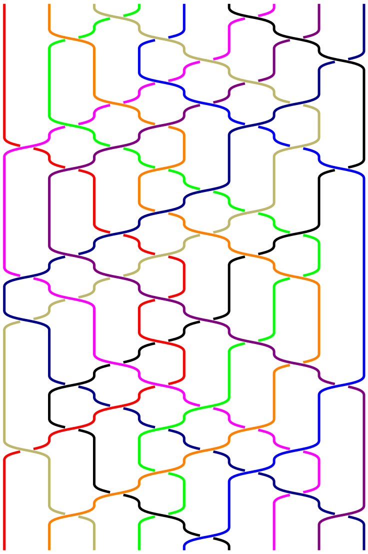


Figure 4.1. The braid $\widehat{\alpha} b \widehat{\alpha}^{-1} b^{-4}$



(a) The braid $[\widehat{\alpha}, \widehat{\beta}].\widehat{\gamma}^{-1}$



(b) The braid $[\widehat{\alpha}, \widehat{\gamma}]$

Figure 4.2. The braids $[\widehat{\alpha}, \widehat{\beta}].\widehat{\gamma}^{-1}$ and $[\widehat{\alpha}, \widehat{\gamma}]$

and a presentation of G is given by:

$$\langle a, b, c \mid a^p = b^p = c^p = 1,\ c = [a, b] \text{ and } [a, c] = [b, c] = 1 \rangle\,, \tag{4.12}$$

where c is an element of G emanating from a generator of the kernel $\mathbb{Z}_p$ of the extension (4.11), and a and b are elements of G that project to the generators of the summands of the quotient. This group is also isomorphic to $(\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes_\theta \mathbb{Z}_p$, where the action $\theta\colon \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ is given by $\theta(1_p) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. From now on, we assume that $p = 3$. Consider the map from G to S_9 that sends a to $\alpha = (1, 4, 7)(2, 5, 8)(3, 6, 9)$ and b to $\beta = (1)(2)(3)(4, 5, 6)(7, 9, 8)$, so c is sent to $\gamma = [\alpha, \beta] = (1, 2, 3)(4, 5, 6)(7, 8, 9)$. The relations of (4.12) hold for the elements α, β and γ, and since the only non-Abelian quotient of G is G itself, it follows that this map extends to an embedding of G in S_9. Once more, one may check that $\mathcal{O}$ and $\mathcal{B} \setminus \mathcal{O}$ are the orbits arising from the action of G on $\mathcal{B}$. It remains to show that G embeds in $\widetilde{H}$. Let $\iota\colon\ G \to \widetilde{H}$ be the map defined by $\iota(\alpha) = \widehat{\alpha}$, $\iota(\beta) = \widehat{\beta}$ and $\iota(\gamma) = \widehat{\gamma}$, where:

$$\widehat{\alpha} = w'\sigma_2\sigma_1^{-1}\sigma_5\sigma_4^{-1}\sigma_8\sigma_7^{-1}w'^{-1}, \quad \widehat{\beta} = \sigma_5\sigma_4^{-1}\sigma_7\sigma_8^{-1}$$
$$\text{and} \quad \widehat{\gamma} = \sigma_2\sigma_1^{-1}\sigma_5\sigma_4^{-1}\sigma_8\sigma_7^{-1},$$

and where

$$w' = \sigma_3\sigma_2\sigma_4\sigma_6\sigma_5\sigma_4\sigma_3\sigma_7\sigma_6.$$

Using the notation of [4, equations (14) and (16)], we have:

$$\widehat{\alpha} = w'\delta_{0,3}\delta_{3,3}\delta_{6,3}w'^{-1} = w'\delta(0, 3, 3, 3)w'^{-1}$$
$$\widehat{\beta} = \delta_{3,3}\delta_{6,3}^{-1} \quad \text{and} \quad \widehat{\gamma} = w'\widehat{\alpha}w'^{-1}.$$

So these three elements are of order 3 in $B_9/\Gamma_2(P_9)$ by the argument of [4, line 4, p. 412], and hence they satisfy the first three relations of (4.12) in $\widetilde{H}$, a, b and c being taken to be $\widehat{\alpha}, \widehat{\beta}$ and $\widehat{\gamma}$ respectively. One may check in a straightforward manner that $[\widehat{\beta}, \widehat{\gamma}] = 1$ as elements of B_9, hence $[\widehat{\beta}, \widehat{\gamma}] = 1$ in $\widetilde{H}$. To see that the two remaining relations of (4.12) hold, as in the first example, we use the method of crossing numbers of the strings given in [4, Proposition 15], but in $\widetilde{H}$ rather than $P_9/\Gamma_2(P_9)$. In this way, we see from Figures 4.2 (a) and (b) that $[\widehat{\alpha}, \widehat{\beta}].\,\widehat{\gamma}^{-1} = 1$ and $[\widehat{\alpha}, \widehat{\gamma}] = 1$ in $\widetilde{H}$. It thus follows that $\langle\, \widehat{\alpha}, \widehat{\beta}, \widehat{\gamma}\,\rangle$ is a quotient of G, but since this subgroup is non-Abelian, and the only non-Abelian quotient of G is itself, we conclude that $\langle\, \widehat{\alpha}, \widehat{\beta}\,\rangle \cong G$, and hence ι is an embedding.

Once more, it follows from the discussion at the beginning of these examples that G embeds in $\pi^{-1}(\iota(G))$, and therefore in $B_9/\Gamma_2(P_9)$.

Remarks 4.5.

(a) Let G be one of the two groups of order 27 analysed in Examples 4.4. With the notation introduced at the beginning of Section 4, the fact that G embeds in $B_9/\Gamma_2(P_9)$ implies that $\ell_2(G) \leqslant 9$. On the other hand, if G embeds in S_r then $r \geqslant 9$ by Lagrange's Theorem. Hence $m(G) \geqslant 9$, and it follows from (1.3) that $m(G) = \ell_2(G) = 9$, which is coherent with [1, Corollary 13] in the case $k = 2$.

(b) The finite groups of the form $A \rtimes_\theta H$, where A is a finite Abelian group, H is an arbitrary finite group, and $\theta\colon\ H \to \operatorname{Aut}(A)$ is injective, embed in S_A by Lemma 4.1. From [1, Corollary 13], if the order of $A \rtimes_\theta H$ is odd then it embeds in $B_{|A|}/\Gamma_2(P_{|A|})$. We would like to be able to determine which of these groups embed in $B_{|A|}/\Gamma_3(P_{|A|})$.

BIBLIOGRAPHY

[1] V. Beck & I. Marin, "Torsion subgroups of quasi-Abelianized braid groups", *J. Algebra* **558** (2020), p. 3-23.

[2] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer, 1982.

[3] M. Falk & R. Randell, "The lower central series of a fiber-type arrangement", *Invent. Math.* **82** (1985), p. 77-88.

[4] D. L. Gonçalves, J. Guaschi & O. Ocampo, "A quotient of the Artin braid groups related to crystallographic groups", *J. Algebra* **474** (2017), p. 393-423.

[5] ———, "Almost-crystallographic groups as quotients of Artin braid groups", *J. Algebra* **524** (2019), p. 160-186.

[6] V. L. Hansen, *Braids and coverings: selected topics*, London Mathematical Society Student Texts, vol. 18, Cambridge University Press, 1989, x+191 pages.

[7] T. Kohno, "Série de Poincaré–Koszul associée aux groupes de tresses pures", *Invent. Math.* **82** (1985), p. 57-75.

[8] I. Marin, "On the representation theory of braid groups", *Ann. Math. Blaise Pascal* **20** (2013), no. 2, p. 193-260.

[9] ———, "Crystallographic groups and flat manifolds from complex reflection groups", *Geom. Dedicata* **182** (2016), p. 233-247.

[10] F. Panaite & M. D. Staic, "A quotient of the braid group related to pseudosymmetric braided categories", *Pac. J. Math.* **244** (2010), no. 1, p. 155-167.

[11] J. Tits, "Normalisateurs de tores. I: Groupes de Coxeter étendus", *J. Algebra* **4** (1966), p. 96-116.

[12] H. J. Zassenhaus, *The theory of groups*, Dover Publications, 1999, reprint of the 2nd (1958) edition, x+265 pages.

Manuscrit reçu le 28 octobre 2018,
révisé le 9 avril 2019,
accepté le 21 mai 2019.

Daciberg LIMA GONÇALVES
Departamento de Matemática – IME-USP
Rua do Matão 1010
CEP: 05508-090 – São Paulo – SP (Brazil)
dlgoncal@ime.usp.br

John GUASCHI
Normandie Univ., UNICAEN, CNRS, LMNO
14000 Caen (France)
john.guaschi@unicaen.fr

Oscar OCAMPO
Universidade Federal da Bahia
Departamento de Matemática – IME
Av. Adhemar de Barros S/N
CEP: 40170-110 – Salvador – BA (Brazil)
oscaro@ufba.br