Norm formulas for finite groups and induction from elementary abelian subgroups

Eli Aljadeff and Christian Kassel

Abstract. *It is known that the norm map N_G for a finite group G acting on a ring R is surjective if and only if for every elementary abelian subgroup E of G the norm map N_E for E is surjective. Equivalently, there exists an element $x_G \in R$ with $N_G(x_G) = 1$ if and only for every elementary abelian subgroup E there exists an element $x_E \in R$ such that $N_E(x_E) = 1$. When the ring R is noncommutative, it is an open problem to find an explicit formula for x_G in terms of the elements x_E. In this paper we present a method to solve this problem for an arbitrary group G and an arbitrary group action on a ring. Using this method, we obtain a complete solution of the problem for the quaternion and the dihedral 2-groups, and for a group of order 27. We also show how to reduce the problem to the class of almost extraspecial p-groups.*

Mathematics Subject Classification (2000): 16W22, 16U99, 20C10, 20D15, 20J05

Key Words: *noncommutative ring, group action, norm map, p-group, quaternion group, dihedral group, extraspecial group, group cohomology*

Let G be a finite group acting by ring automorphisms on an arbitrary (not necessarily commutative) ring R with unit. For any subgroup U of G the *norm map* $N_U : R \to R^U$ is defined for all $x \in R$ by

$$N_U(x) = \sum_{g \in U} g(x).$$

Here $g(x)$ denotes the value in R of the action of g on x and R^U the subring of U-invariant elements in R.

The question of the surjectivity of the map N_G onto R^G has well-known interpretations in topics such as Galois theory, algebraic number fields and, most importantly for this paper, integral group representations.

In [2, Theorem 1] the first-named author and Ginosar proved that N_G is surjective onto R^G if and only if N_E is surjective onto R^E for every elementary abelian subgroup E of G. This generalizes Chouinard's theorem [7] that asserts that a $\mathbf{Z}[G]$-module is projective if and only if for every elementary abelian subgroup E of G it is projective as a $\mathbf{Z}[E]$-module.

The map N_U being R^U-linear, it is surjective onto R^U if and only if the unit 1 of R belongs to the image of N_U. We can therefore rephrase Aljadeff and Ginosar's result as follows: there is an element $x_G \in R$ such that $N_G(x_G) = 1$ if and only if there is an element $x_E \in R$ such that $N_E(x_E) = 1$ for every elementary abelian subgroup E of G. Using this statement, Shelah observed (see [2, Proposition 6]) that there exist formulas expressing x_G polynomially in terms of the elements x_E and the elements of G.

The aim of this paper is to find such a formula for any given finite group G. We would like to point out that such a formula should be defined over $\mathbf{Z}$ and be independent of the ring on which the group acts. In this way it has a universal character though it may not be unique. With such a formula it is possible to construct a projective G-basis for any finitely generated projective $\mathbf{Z}[G]$-module M out of given projective E-bases of M, one for each elementary abelian subgroup E of G.

We assume that G is not an elementary abelian group (otherwise the problem is trivial). The smallest group that is not elementary abelian is the cyclic group C_4 of order 4. This case was solved by Péter P. Pálfy who found the formula

$$x_G = x_E\sigma(x_E) + x_E\sigma(x_E)x_E - x_E^2\sigma(x_E), \tag{0.1}$$

where σ denotes a generator of C_4. The meaning of this formula is the following: if C_4 acts on some ring R and there is an element $x_E \in R$ such that $x_E + \sigma^2(x_E) = 1$ (i.e., $N_E(x_E) = 1$ for the (unique) elementary abelian subgroup E of G), then for $x_G \in R$ given by (0.1) we have

$$N_G(x_G) = x_G + \sigma(x_G) + \sigma^2(x_G) + \sigma^3(x_G) = 1.$$

This was the first formula of this kind to be found.

The next step is due to the authors: they showed in [3] how to obtain formulas for *all abelian groups*. Such formulas can be complicated even in simple cases. For instance, if $G = C_9$ is a cyclic group of order 9 (with generator σ) and $x_E \in R$ is an element of norm one for the subgroup of order 3, then

$$\begin{aligned} x_G = & - x_E^2 + 2\sigma(x_E)x_E - \sigma^3(x_E)x_E + \sigma^4(x_E)x_E \\ & + x_E\sigma^3(x_E)x_E + x_E\sigma^4(x_E)x_E + x_E\sigma^5(x_E)x_E \\ & + x_E\sigma^6(x_E)x_E + x_E\sigma^7(x_E)x_E + x_E\sigma^8(x_E)x_E \\ & - \sigma(x_E)\sigma^4(x_E)x_E - \sigma(x_E)\sigma^5(x_E)x_E - \sigma(x_E)\sigma^6(x_E)x_E \\ & - \sigma(x_E)\sigma^7(x_E)x_E - \sigma(x_E)\sigma^8(x_E)x_E - \sigma(x_E)x_E^2 \\ & + \sigma^3(x_E)\sigma^6(x_E)x_E + \sigma^3(x_E)\sigma^7(x_E)x_E + \sigma^3(x_E)\sigma^8(x_E)x_E \\ & - \sigma^4(x_E)\sigma^7(x_E)x_E - \sigma^4(x_E)\sigma^8(x_E)x_E - \sigma^4(x_E)x_E^2 \end{aligned} \tag{0.2}$$

is a formula (with 22 monomials) for an element of norm one for G. It should also be noted that the first-named author obtained formulas for arbitrary groups acting on *commutative* rings (see [1]).

We are thus left with the case of *nonabelian groups acting on noncommutative rings* (noncommutative rings are important for us because we want to be able to apply the formulas to ring of endomorphisms). In this paper we present a general method that allows to solve the problem for arbitrary groups and arbitrary ring actions. The idea is to translate the task of finding formulas for norm one elements x_G for a group G acting on a ring R into a more accessible system of equations in R, where the variables are symbols $b(\sigma)$, one for each generator σ in a presentation of G. The equations are obtained from the relations in the presentation. Such a system has solutions, and we will show how each solution yields a formula for x_G. We illustrate this method by solving this system of equations for the quaternion and dihedral families of 2-groups, and a group of order 27. This provides the first examples of norm one formulas for nonabelian groups acting on noncommutative rings.

We also show that the problem for a general group G can be reduced to a smaller class of groups, namely the class of extraspecial and almost extraspecial p-groups that are subquotients of G. For instance, in order to solve the problem for the quaternion and dihedral groups mentioned above, it is sufficient to solve it for the quaternion group Q_8 and the dihedral group D_8 of order 8.

The paper is organized as follows. In Section 1 we explain precisely what we mean by a formula for a group G and we introduce a ring that is universal for the situation under consideration.

In Section 2 we present three reductions, first a straightforward one to p-groups, then a reduction to extraspecial and almost extraspecial p-groups. Finally we show how to solve the problem for the product of two p-groups once we have solutions for each of them.

After some cohomological preliminaries in Section 3 we explain our method to solve the problem for an arbitrary p-group in Section 4. This involves solving the above-mentioned system of equations and a further problem that we solve in Section 5. More precisely, assuming we are given an element $x \in R$ such that $N_U(x) = 1$, we will show in Section 5 how to express any 1-cocycle $\beta : U \to R$ explicitly as a 1-coboundary, i.e., how to find an explicit formula for an element $w \in R$ such that $\beta(g) = g(w) - w$ for all $g \in U$. Once we have solved the above-mentioned system of equations and we have a formula for w, we obtain a complete explicit solution to the problem of finding a formula for a norm one element for G.

In Sections 6–8 we apply our method to two important families of nonabelian groups, namely the quaternion groups Q_{2^n} and the dihedral groups D_{2^n}, and to a group of order 27.

All groups considered in this paper are finite, and all rings have units. We denote a cyclic group of order n by C_n.

1. Formulas for a group

For any group G we denote $\mathcal{E}_G$ the set of elementary abelian subgroups of G. Recall that a group E is elementary abelian if it is isomorphic to C_p^r for some prime number p and some integer $r \geq 1$. Clearly, $\mathcal{E}_H \subset \mathcal{E}_G$ if H is a subgroup of G.

Definition 1.1.— *A formula for a finite group G is a polynomial Φ_G in noncommuting variables $g(x_E)$, where $g \in G$ and $E \in \mathcal{E}_G$, and with coefficients in $\mathbf{Z}$, satisfying the following condition: whenever G acts by automorphisms on a ring R and $(x_E)_{E \in \mathcal{E}_G}$ is a family of elements of R such that $N_E(x_E) = 1$ for all $E \in \mathcal{E}_G$, then the element $x_G \in R$ obtained by replacing in Φ_G each variable $g(x_E)$ by the value of the action of g on the element $x_E \in R$ satisfies $N_G(x_G) = 1$.*

In this definition we use the same letter for the symbol x_E and its value in R. We shall write x_E instead of $g(x_E)$ in a formula when $g = 1$ is the neutral element of G.

In order to clarify Definition 1.1, we consider the free noncommutative ring

$$R_{\text{free}}(G) = \mathbf{Z}\,\langle g(X_E) \,|\, g \in G,\, E \in \mathcal{E}_G \rangle$$

generated by symbols of the form $g(X_E)$, where g runs over all elements of G and E runs over all elements of $\mathcal{E}_G$. To simplify notation, we set $e(X_E) = X_E$ when e is the neutral element of G. The group G acts by ring automorphisms on $R_{\text{free}}(G)$ as follows: if $h \in G$ and $g(X_E)$ is a generator of $R_{\text{free}}(G)$, then

$$h(g(X_E)) = (hg)(X_E)$$

for g, $h \in G$, and $E \in \mathcal{E}_G$. Let I be the two-sided ideal of $R_{\text{free}}(G)$ generated by all elements of the form

$$\sum_{h \in E} (gh)(X_E) - 1$$

for any $g \in G$ and any $E \in \mathcal{E}_G$. The ideal is preserved by the G-action on $R_{\text{free}}(G)$.

Let $R_{\text{univ}}(G)$ be the quotient ring

$$R_{\text{univ}}(G) = R_{\text{free}}(G)/I$$

with the induced G-action. By definition of $R_{\text{univ}}(G)$, for any $E \in \mathcal{E}_G$ we have

$$N_E(X_E) = \sum_{h \in E} h(X_E) = 1. \tag{1.1}$$

Proposition 1.2.— *Any element $\Phi_G \in R_{\text{univ}}(G)$ such that $N_G(\Phi_G) = 1$ is a formula for the group G.*

Proof.— First observe that Φ_G is a polynomial with integer coefficients in noncommutative variables $g(X_E)$ indexed by $G \times \mathcal{E}_G$. Suppose that G acts on a ring R and that $(x_E)_{E \in \mathcal{E}_G}$ is a family of elements of R such that $N_E(x_E) = 1$ for all $E \in \mathcal{E}_G$. Set $f(g(X_E)) = g(x_E)$ for all $g \in G$ and $E \in \mathcal{E}_G$. Since for all $g \in G$ and $E \in \mathcal{E}_G$,

$$\sum_{h \in E} (gh)(x_E) = gN_E(x_E) = g(1) = 1$$

in R, there is a unique homomorphism of G-rings $f : R_{\mathrm{univ}}(G) \to R$ such that $f(g(X_E)) = g(x_E)$ for all $g \in G$ and $E \in \mathcal{E}_G$. Set $x_G = f(\Phi_G)$. We then have

$$N_G(x_G) = N_G(f(\Phi_G)) = f(N_G(\Phi_G)) = f(1) = 1,$$

which proves the proposition. □

The proof above also shows that $R_{\mathrm{univ}}(G)$ is the universal G-ring with a family of elements $(X_E)_{E\in\mathcal{E}_G}$ such that $N_E(X_E) = 1$.

As we have already pointed out in the introduction, there is a formula for every finite group G. Let us give a quick proof of this fact using the ring $R_{\mathrm{univ}}(G)$: indeed by (1.1), we have $N_E(X_E) = 1$ for every elementary abelian subgroup E of G. Therefore by [2, Theorem 1] there exists $\Phi_G \in R_{\mathrm{univ}}(G)$ such that $N_G(\Phi_G) = 1$. By Proposition 1.2 this is a formula for G. Since finding such a formula for G amounts to constructing a norm-one element in $R_{\mathrm{univ}}(G)$, we see that the problem is a pure group-theoretical question.

The right-hand sides of (0.1) and (0.2) provide formulas for the cyclic groups C_4 and C_9, respectively. If E is an elementary abelian group, then $\Phi_E = x_E$ is clearly a formula for E.

In our search for formulas for a group G, the following rephrasing of [2, Theorem 1] will be useful. To state it, we need the following notation: $\mathcal{E}_G^{\max}$ denotes the set of maximal elements of $\mathcal{E}_G$ with respect to inclusion, and $\mathcal{E}_G^0$ a subset of $\mathcal{E}_G^{\max}$ such that any element of $\mathcal{E}_G^{\max}$ is conjugated in G to exactly one element of $\mathcal{E}_G^0$.

Proposition 1.3.— *Let G be a finite group acting on a ring R by ring automorphisms. We assume that G is not elementary abelian. Then the following statements are equivalent:*

1) There exists $x_G \in R$ such that $N_G(x_G) = 1$.

2) For each proper subgroup U of G there exists $x_U \in R$ with $N_U(x_U) = 1$.

3) For each $E \in \mathcal{E}_G$ there exists $x_E \in R$ such that $N_E(x_E) = 1$.

4) For each $E \in \mathcal{E}_G^{\max}$ there exists $x_E \in R$ such that $N_E(x_E) = 1$.

5) For each $E \in \mathcal{E}_G^0$ there exists $x_E \in R$ such that $N_E(x_E) = 1$.

Proof.— 1) ⇒ 2): Let $\{g_1, \ldots, g_r\}$ be a set of representatives for the right cosets of U in G. Define

$$x_U = g_1(x_G) + \cdots + g_r(x_G) \in R. \tag{1.2}$$

Then

$$N_U(x_U) = \sum_{u\in U} \sum_{i=1}^{r} (ug_i)(x_G) = N_G(x_G) = 1.$$

2) ⇒ 3) ⇒ 4) ⇒ 5): It is obvious. (Note that the assumption that G is not elementary abelian is needed for the implication 2) ⇒ 3).)

3) ⇒ 1): This is nontrivial; it follows from [2, Theorem 1].

5) ⇒ 4): Let $g \in G$ and $E \in \mathcal{E}_G$. For $x_E \in R$ such that $N_E(x_E) = 1$, define

$$x_{gEg^{-1}} = g(x_E). \tag{1.3}$$

Then

$$N_{gEg^{-1}}(x_{gEg^{-1}}) = N_{gEg^{-1}}(g(x_E)) = g\bigl(N_E(x_E)\bigr) = g(1) = 1.$$

4) ⇒ 3): Any $E \in \mathcal{E}_G$ is a subgroup of an element of $\mathcal{E}_G^{\max}$. Then proceed as for 1) ⇒ 2). □

It can be seen from (1.2) and (1.3) that the number of variables in a formula Φ_G for G can be reduced; we can restrict ourselves to the variables $g(x_E)$, where $g \in G$ and where $E \in \mathcal{E}_G^{\max}$ or $E \in \mathcal{E}_G^0$.

2. Three reductions

In this section we reduce in three steps the problem of finding a formula for G to the problem of finding formulas for smaller groups of a special type.

First reduction

We start by reducing the problem to p-groups, where p is a prime number. Given a group G, let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the factorization of the order n of G in prime factors, where $p_1, \dots, p_r$ are distinct prime numbers, $r \geq 2$, and the exponents $a_1, \dots, a_r$ are positive integers. Choose integers $d_1, \dots, d_r$ such that

$$d_1 n/p_1^{a_1} + \cdots + d_r n/p_r^{a_r} = 1.$$

For every $i = 1, \dots, r$, let S_i be a Sylow p_i-subgroup (of order $p_i^{a_i}$) of G.

The following result implies that, in order to find a formula for a group G, it is sufficient to find a formula for a Sylow p-subgroup of G for each prime number p dividing the order of G.

Proposition 2.1.— *For each $i = 1, \dots, r$, let Φ_{S_i} be a formula for S_i. If*

$$\Phi_G = d_1 \Phi_{S_1} + \cdots + d_r \Phi_{S_r},$$

then Φ_G is a formula for G.

Proof.— Suppose we are given a ring R on which G acts and elements $x_E \in R$ such that $N_E(x_E) = 1$, one for each elementary abelian subgroup E of G. Replacing each variable x_E ($E \in \mathcal{E}_{S_i} \subset \mathcal{E}_G$) in the polynomial Φ_{S_i} by the element $x_E \in R$, we obtain an element $x_i \in R$ such that $N_{S_i}(x_i) = 1$ for each $i = 1, \dots, r$. Let us check that $N_G(x_G) = 1$ for $x_G = d_1 x_1 + \cdots + d_r x_r$. Indeed,

$$N_G(x_i) = \sum_{g \in G} g(x_i) = \sum_{g \in G/S_i} g\bigl(N_{S_i}(x_i)\bigr) = \sum_{g \in G/S_i} g(1) = n/p_i^{a_i}.$$

Consequently, $N_G(x_G) = d_1 n/p_1^{a_1} + \cdots + d_r n/p_r^{a_r} = 1$. □

Let us illustrate Proposition 2.1 in the case of the symmetric group S_3. Let s be a transposition and t be a cyclic permutation in S_3. The subgroups E_s and E_t generated respectively by s and t are elementary abelian. Then by Proposition 2.1,

$$\Phi_{S_3} = x_{E_s} - x_{E_t}$$

is a formula for S_3.

Second reduction

We next reduce the problem from arbitrary p-groups to p-groups that are extraspecial or almost extraspecial. Recall that a p-group G is *extraspecial* (respectively *almost extraspecial*) if G fits into a central extension of the type

$$1 \to C_p \to G \to C_p^r \to 1,$$

where $r \geq 1$, and the center of G is isomorphic to C_p (respectively to C_{p^2}). For a complete description of (almost) extraspecial groups, see for instance [5] (see also [8, Chapter 5]). Note that with this definition no abelian group is extraspecial and that the only abelian almost extraspecial group is C_{p^2}.

For any p-group G we denote $\mathcal{F}_G$ the set of isomorphism classes of groups U satisfying the following conditions :

(i) U is a subquotient (i.e., a homomorphic image of a subgroup) of G and

(ii) U is extraspecial or almost extraspecial.

We have $\mathcal{F}_H \subset \mathcal{F}_G$ whenever H is a subquotient of G.

The following result states that, in order to find a formula for a finite p-group G, it is sufficient to have formulas for all groups in $\mathcal{F}_G$.

Theorem 2.2.— *For any finite p-group G there is an algorithm whose output is a formula Φ_G for G and whose inputs are formulas Φ_H for all $H \in \mathcal{F}_G$.*

Before we prove the theorem, we establish two intermediate results.

Lemma 2.3.— *If a p-group G is neither elementary abelian, nor extraspecial, nor almost extraspecial, then there is a central element $h \in G$ of order p such that the quotient group $G/\langle h \rangle$ is not an elementary abelian group.*

Proof.— If G is abelian, then G is of order $\geq p^3$. Take an element g of order p in G. If $G/\langle g \rangle$ is not elementary abelian, we are done. If $G/\langle g \rangle$ is elementary abelian, say $G/\langle g \rangle \cong C_p^r$ for some r that is necessarily at least 2, then by the classification of finite abelian p-groups we have $G \cong C_{p^2} \times C_p^{r-1}$. Let σ be an element of order p in C_p^{r-1} (it exists since $r-1 \geq 1$) and $h \in G$ be the element mapped to $(0, \sigma) \in C_{p^2} \times C_p^{r-1}$. Then $G/\langle h \rangle$ contains an element of order p^2, hence is not elementary abelian.

Now assume that G is not abelian. Let g be an element of order p in the center $Z(G)$ of G. If $G/\langle g \rangle$ is not elementary abelian, we are done. Therefore we may assume that $G/\langle g \rangle$ is elementary abelian. Observe that under this condition the commutator subgroup G' of G is the subgroup $\langle g \rangle$ generated by g. Since G is neither abelian, nor extraspecial, nor almost extraspecial, its center $Z(G)$ is not isomorphic to C_p or to C_{p^2}. Moreover, $Z(G)$ is not cyclic of order $\geq p^3$ since $G/\langle g \rangle$ is elementary abelian. Therefore there is an element $h \in Z(G)$ of order p such that $\langle h \rangle \neq \langle g \rangle = G'$, and so $G/\langle h \rangle$ is not abelian, hence not elementary abelian. □

Let G be a p-group that is neither elementary abelian, nor extraspecial, nor almost extraspecial. By Lemma 2.3 there is a subgroup U of order p in the center of G such that G/U is not elementary abelian. We fix such a subgroup U.

Let $\pi : G \to G/U$ be the natural projection. Let $\Phi_{G/U}$ be a formula for G/U, and for each $\bar{E} \in \mathcal{E}_{G/U}$ let $\Phi_{\pi^{-1}(\bar{E})}$ be a formula for the proper subgroup $\pi^{-1}(\bar{E})$ of G (it is a proper subgroup because G/U is not elementary abelian). Set

$$\Phi_G = \Phi_{G/U}\bigl(N_U(\Phi_{\pi^{-1}(\bar{E})})\bigr)x_U. \tag{2.1}$$

Equality (2.1) defines a noncommutative polynomial with integer coefficients in the variables $g(x_E)$, where $g \in G$ and $E \in \mathcal{E}_G$. This is a consequence of the following observations on the right-hand side of (2.1).

Firstly, $N_U(\Phi_{\pi^{-1}(\bar{E})})$ has the following meaning: we replace each monomial $h_1(x_{E_1}) \cdots h_s(x_{E_s})$ in $\Phi_{\pi^{-1}(\bar{E})}$, where $h_1, \ldots, h_s \in \pi^{-1}(\bar{E})$ and $E_1, \ldots, E_s \in \mathcal{E}_{\pi^{-1}(\bar{E})}$, by the polynomial

$$\sum_{u \in U} (uh_1)(x_{E_1}) \cdots (uh_s)(x_{E_s}).$$

Secondly, the expression $\Phi_{G/U}\bigl(N_U(\Phi_{\pi^{-1}(\bar{E})})\bigr)$ means that we replace each letter $x_{\bar{E}}$ ($\bar{E} \in \mathcal{E}_{G/U}$) in the polynomial $\Phi_{G/U}$ by the polynomial $N_U(\Phi_{\pi^{-1}(\bar{E})})$ whose meaning has just been explained. In this way, each variable $\bar{g}(x_{\bar{E}})$, where $\bar{g} \in G/U$ and $\bar{E} \in \mathcal{E}_{G/U}$, becomes a polynomial in the variables $g(x_E)$, where $g \in G$ and $E \in \cup_{\bar{E} \in \mathcal{E}_{G/U}} \mathcal{E}_{\pi^{-1}(\bar{E})}$ $(\subset \mathcal{E}_G)$.

Finally, the polynomial $\Phi_{G/U}\bigl(N_U(\Phi_{\pi^{-1}(\bar{E})})\bigr)$ is multiplied on the right by the variable x_U, which makes sense since $U \in \mathcal{E}_G$.

PROPOSITION 2.4.— *With the previous notation, Φ_G is a formula for G.*

PROOF.— Suppose G acts on a ring R and we have elements $x_E \in R$ such that $N_E(x_E) = 1$, one for each $E \in \mathcal{E}_G$. In particular, we have an element $x_U \in R$ such that $N_U(x_U) = 1$.

For each $\bar{E} \in \mathcal{E}_{G/U}$, let $x_{\pi^{-1}(\bar{E})}$ be the element of R obtained from the formula $\Phi_{\pi^{-1}(\bar{E})}$ by replacing each variable $h(x_E)$, where $h \in \pi^{-1}(\bar{E})$ and $E \in \mathcal{E}_{\pi^{-1}(\bar{E})}$ $(\subset \mathcal{E}_G)$, by the value of the action of h on the element $x_E \in R$. By definition of a formula, we have

$$N_{\pi^{-1}(\bar{E})}(x_{\pi^{-1}(\bar{E})}) = 1.$$

The element $N_U(x_{\pi^{-1}(\bar{E})})$ clearly belongs to the subring R^U. Let

$$z_{G/U} = \Phi_{G/U}\bigl(N_U(x_{\pi^{-1}(\bar{E})})\bigr)$$

be obtained by replacing each variable $\bar{g}(x_{\bar{E}})$ of $\Phi_{G/U}$ by $\bar{g}N_U(x_{\pi^{-1}(\bar{E})}) \in R^U$ (this makes sense since G/U acts on R^U). Since $\Phi_{G/U}$ is a formula for G/U, we have $N_{G/U}(z_{G/U}) = 1$. The element $z_{G/U}$ belongs to R^U because the inputs in its definition are in this subring. To conclude, let $x_G = z_{G/U}x_U \in R$. Using the R^U-linearity of N_U, we obtain

$$\begin{aligned} N_G(x_G) &= N_{G/U}(N_U(z_{G/U}x_U)) \\ &= N_{G/U}(z_{G/U}N_U(x_U)) \\ &= N_{G/U}(z_{G/U} \cdot 1) = 1. \end{aligned}$$

□

PROOF OF THEOREM 2.2.— We proceed by induction on the order of G.

Suppose G is of order p^3. If G is elementary abelian or extraspecial, we are done (note that G cannot be almost extraspecial). Otherwise, $G \cong C_{p^3}$ or $G \cong C_{p^2} \times C_p$, and in both cases $\mathcal{F}_G = \{C_{p^2}\}$. Fix a central subgroup U of order p such that G/U is not elementary abelian. Then G/U, being of order p^2, is isomorphic to C_{p^2}, which is almost extraspecial. The group G/U has a unique elementary abelian subgroup $\bar{E}$ of order p whose lifting $\pi^{-1}(\bar{E})$ to G, being of order p^2, is either isomorphic to C_p^2 (elementary abelian) or C_{p^2} (belonging to $\mathcal{F}_G$). In both cases, by Proposition 2.4, (2.1) yields a formula for Φ_G in terms of $\Phi_{C_{p^2}}$.

Let G be a group of order p^n with $n \geq 4$. Suppose we have proved the theorem for all groups of order at most p^{n-1}. As above, we may assume that G is neither elementary abelian, nor extraspecial, nor almost extraspecial. We again fix a central subgroup U of order p such that G/U is not elementary abelian. By the induction hypothesis, there is an algorithm whose output is a formula $\Phi_{G/U}$ for G/U and whose inputs are formulas for all groups in $\mathcal{F}_{G/U}$. The lifting $\pi^{-1}(\bar{E})$ to G of each $\bar{E} \in \mathcal{E}_{G/U}$ is a proper subgroup of G since G/U is not elementary abelian. By the induction hypothesis again, there is an algorithm whose output is a formula $\Phi_{\pi^{-1}(\bar{E})}$ for $\pi^{-1}(\bar{E})$ and whose inputs are formulas for all groups in $\mathcal{F}_{\pi^{-1}(\bar{E})}$. Therefore by Proposition 2.4, (2.1) yields an algorithm whose output is a formula Φ_G for G and whose inputs are formulas for all groups in the sets $\mathcal{F}_{\pi^{-1}(\bar{E})}$ or in $\mathcal{F}_{G/U}$. We conclude by observing that $\mathcal{F}_{G/U} \subset \mathcal{F}_G$ and $\mathcal{F}_{\pi^{-1}(\bar{E})} \subset \mathcal{F}_G$ for all $\bar{E} \in \mathcal{E}_{G/U}$. □

Third reduction

We now consider the case when G is the product of two groups.

THEOREM 2.5.— *Let $G = G_1 \times G_2$ be a product of two p-groups G_1 and G_2. There is an algorithm whose output is a formula Φ_G for G and whose inputs are formulas for all groups in $\mathcal{F}_{G_1} \cup \mathcal{F}_{G_2}$.*

Before we give the proof of this theorem, we establish a result similar to Proposition 2.4.

Consider the case when $G = H \times C$, where H is a p-group and C is an elementary abelian p-group of rank one, i. e., $C \cong C_p$. Set

$$\Phi_G = \Phi_H\big(N_C(x_{E' \times C})\big)x_C, \tag{2.2}$$

where Φ_H is a formula for H and $E' \in \mathcal{E}_H$ $(\subset \mathcal{E}_G)$. Observe that $E' \times C \in \mathcal{E}_G$. The right-hand side of (2.2) has the following meaning. Firstly,

$$N_C(x_{E' \times C}) = \sum_{u \in C} u(x_{E' \times C}).$$

Secondly, $\Phi_H\big(N_C(x_{E' \times C})\big)$ means that we replace each letter $x_{E'}$ $(E' \in \mathcal{E}_H)$ in the polynomial Φ_H by the polynomial $N_C(x_{E' \times C})$ defined above. In this way, each variable $h(x_{E'})$ of Φ_H, where $h \in H$ and $E' \in \mathcal{E}_H$, becomes a polynomial in the variables $g(x_{E' \times C})$, where $g \in G$ and $E' \times C \in \mathcal{E}_G$. Therefore, the right-hand side of (2.2) is a noncommutative polynomial with integer coefficients and in the right set of variables.

Proposition 2.6.— *With the previous notation, Φ_G is a formula for G.*

Proof.— Suppose G acts on a ring R and we have elements $x_E \in R$ such that $N_E(x_E) = 1$, one for each $E \in G$. In particular, we have $x_C \in R$ such that $N_C(x_C) = 1$. For each $E' \in \mathcal{E}_H$, the product $E' \times C$ is an elementary abelian subgroup of G, and we have an element $x_{E'\times C} \in R$ such that $N_{E'\times C}(x_{E'\times C}) = 1$. The element $N_C(x_{E'\times C})$ belongs to R^C and satisfies

$$N_{E'}\big(N_C(x_{E'\times C})\big) = 1.$$

Let $z = \Phi_H\big(N_C(x_{E'\times C})\big)$ be the element obtained by replacing each variable $h(x_{E'})$ of Φ_H by $hN_C(x_{E'\times C}) \in R^C$ (the group $H = G/C$ acts on R^C). Since Φ_H is a formula for H, we have $N_H(z) = 1$. Moreover, since the inputs belong to R^C, so does z. Now let $x_G = zx_C$. Then, using the R^C-linearity of N_C, we obtain

$$\begin{aligned} N_G(x_G) &= N_H(N_C(zx_C)) \\ &= N_H(zN_C(x_C)) \\ &= N_H(z \cdot 1) = 1. \end{aligned}$$

□

Proof of Theorem 2.5.— (a) Assume first that G_2 is elementary abelian. Let us prove by induction on the order of G_2 that there is an algorithm whose output is a formula Φ_G for G and whose inputs are formulas for all groups in $\mathcal{F}_{G_1}$. Since $\mathcal{F}_{G_2} = \emptyset$, it will prove Theorem 2.5 in this case.

If G_2 is of order p, we appeal to Proposition 2.6: Formula (2.2), in which we have replaced H by G_1 and C by G_2, yields an algorithm whose output is a formula Φ_G for the group G and whose input is a formula for G_1. Therefore, by Theorem 2.2 there is an algorithm whose output is a formula for G and whose inputs are formulas for all groups in $\mathcal{F}_{G_1}$.

If G_2 is of order $> p$, we write $G_2 = G_2' \times C$, where C is cyclic of order p (the subgroup G_2' is elementary abelian). Reasoning as above, we obtain an algorithm whose output is a formula for $G = G_1 \times G_2' \times C$ and whose input is a formula for $G_1 \times G_2'$. By induction there is an algorithm whose output is a formula for $G_1 \times G_2'$ and whose inputs are formulas for all groups in $\mathcal{F}_{G_1}$. Therefore there is an algorithm whose output is a formula for G and whose inputs are formulas for all groups in $\mathcal{F}_{G_1}$.

(b) Let G_2 be an arbitrary p-group of order p^n with $n \geq 2$ and suppose we have proved Theorem 2.5 for all groups $G = G_1 \times G_2'$ such that the order of G_2' is at most p^{n-1}. By Part (a) we may assume that G_2 is not elementary abelian.

Let U be a central subgroup of G_2 of order p and

$$\pi : G = G_1 \times G_2 \to G/U = G_1 \times G_2/U$$

be the natural projection. By Proposition 2.4, Formula (2.1) yields an algorithm whose output is a formula for G and whose inputs are formulas for G/U and for

$\pi^{-1}(\bar{E})$, where $\bar{E}$ runs over $\mathcal{E}_{G/U}$. By induction there is an algorithm whose output is a formula for $G/U = G_1 \times G_2/U$ and whose inputs are formulas for all groups in $\mathcal{F}_{G_1} \cup \mathcal{F}_{G_2/U}$.

Each elementary abelian subgroup $\bar{E}$ of $G/U = G_1 \times G_2/U$ is clearly contained in an elementary abelian subgroup of the form $E_1 \times E_2$, where E_1 is an elementary abelian subgroup of G_1 and E_2 is an elementary abelian subgroup of G_2/U. Its inverse image $\pi^{-1}(\bar{E})$ is therefore contained in a group of the form $E_1 \times N$, where N is a subgroup of G_2. Formula (1.2) shows how to obtain a formula for $\pi^{-1}(\bar{E})$ from a formula for $E_1 \times N$. By Part (a) there is an algorithm whose output is a formula for $E_1 \times N$ and whose inputs are formulas for all groups in $\mathcal{F}_N$. Summing up and observing that $\mathcal{F}_{G_2/U} \subset \mathcal{F}_{G_2}$ and $\mathcal{F}_N \subset \mathcal{F}_{G_2}$, we conclude that there is algorithm whose output is a formula for G and whose inputs are formulas for all groups in $\mathcal{F}_{G_1} \cup \mathcal{F}_{G_2}$. $\square$

REMARKS 2.7. (a) Lemma 2.3 can be used to show that $\mathcal{F}_G = \emptyset$ if and only if G is elementary abelian.

(b) By definition of $\mathcal{F}_G$, if G is an *abelian* p-group, then $\mathcal{F}_G$ is empty (if G is elementary abelian) or $\mathcal{F}_G = \{C_{p^2}\}$. By Theorem 2.2 it suffices to have a formula for C_{p^2} in order to obtain formulas for all abelian groups. A formula for C_{p^2} was obtained in [3, Corollary 1]. We recall it here for the sake of completeness: let σ be a generator of C_{p^2} and E be the unique abelian elementary subgroup of C_{p^2}. Then

$$\begin{aligned}\Phi_{C_{p^2}} = x_E^2 &+ \sum_{j=0}^{p-1}\sum_{k=1}^{p-1}\sum_{i=0}^{k-1} \sigma^{ip}(x_E)\,\sigma^{j-(k-i)p}(x_E)\,x_E \\ &- \sum_{j=0}^{p-1}\sum_{k=1}^{p-1}\sum_{i=0}^{k-1} \sigma^{ip+1}(x_E)\,\sigma^{j-(k-i)p+1}(x_E)\,x_E \\ &- \sum_{k=1}^{p-1}\sum_{i=0}^{k-1} \sigma^{ip}(x_E)\,x_E + \sum_{k=1}^{p-1}\sum_{i=0}^{k-1} \sigma^{ip+1}(x_E)\,x_E\end{aligned} \tag{2.3}$$

is a formula for C_{p^2}. Formula (0.2) is the special case of (2.3) when $p = 3$.

(c) Theorem 2.5 may help get a better reduction than Theorem 2.2 for non-abelian groups. For instance, take the product $G = Q_8 \times Q_8$ of two copies of the quaternion group of order 8. By [8, Chapter 5] the central product G_1 of Q_8 with itself, which is a quotient of G, is an extraspecial group; it belongs to $\mathcal{F}_G$. Theorem 2.2 therefore suggests that a formula for the group G_1 (of order 32) is needed to obtain a formula for G. Nevertheless, by Theorem 2.5 only formulas for the groups in $\mathcal{F}_{Q_8} = \{C_4, Q_8\}$ are needed.

3. Cohomological preliminaries

In this section we present two results needed in the sequel. The first one is an important consequence of the existence of a norm one element.

PROPOSITION 3.1.— *Let G be a finite p-group acting on a ring R. If there is an element $x \in R$ such that $N_G(x) = 1$, then $H^i(G, R) = 0$ for all $i > 0$.*

PROOF.— We proceed by induction on the order of G. Assume first that G is a cyclic group of order p with generator σ. Recall that the cohomology groups of a cyclic group are given for all $j \geq 1$ by

$$H^{2j}(G, R) = R^G/\mathrm{Im}\ N_G \quad \text{and} \quad H^{2j-1}(G, R) = \mathrm{Ker}\ N_G/(\sigma - 1)(R).$$

The even cohomology groups vanish since $N_G(R^G x) = R^G N_G(x) = R^G$. The vanishing of the odd cohomology groups follows from [3, Lemma 1].

Now let G be of order p^n with $n \geq 2$ and assume that the lemma holds for all p-groups of order $< p^n$. Take a normal subgroup U of G of index p (such a subgroup always exists). Using Formula (1.2), out of the element $x \in R$ satisfying $N_G(x) = 1$ we derive an element $x_U \in R$ such that $N_U(x_U) = 1$. The existence of x_U implies by induction that $H^i(U, R) = 0$ for all $i > 0$.

It then follows from the Lyndon-Hochschild-Serre spectral sequence that the inflation maps

$$\mathrm{Inf} : H^i(G/U, R^U) \to H^i(G, R)$$

are isomorphisms for all i. Now G/U is cyclic and the element $N_U(x) \in R^U$ satisfies

$$N_{G/U}(N_U(x)) = N_G(x) = 1.$$

Then by the first part of the proof the cohomology groups $H^i(G/U, R^U)$ vanish for all $i > 0$, and so do the groups $H^i(G, R)$. □

In the next sections we shall represent elements of the cohomology group $H^1(G, M)$, where G is a group and M is a left G-module, by 1-cocycles of G with values in M. Recall from [6, Chapter X, § 4] that such a 1-cocycle (also called a crossed homomorphism) is a map $\beta : G \to M$ satisfying

$$\beta(gh) = \beta(g) + g\beta(h) \tag{3.1}$$

for all g, $h \in G$. A 1-coboundary is a map $\beta : G \to M$ for which there exists $m \in M$ such that

$$\beta(g) = (g - 1)m \tag{3.2}$$

for all $\in G$. It is easy to check that a 1-coboundary is a 1-cocycle. 1-cocycles and 1-coboundaries are elements of the standard cochain complex whose cohomology is $H^*(G, M)$. If δ is the differential in the standard cochain complex, then (3.2) can be rewritten as $\beta = \delta(m)$.

The following identities are easy consequences of the functional equation (3.1).

LEMMA 3.2.— *Let $\beta : G \to M$ be a 1-cocycle of G with values in a left G-module M.*

(a) For the neutral element $1 \in G$, we have $\beta(1) = 0$.

(b) For $g \in G$ and $i \geq 2$, we have

$$\beta(g^i) = (1 + g + \cdots + g^{i-1})\beta(g).$$

(c) If $g \in G$ is of order N, then

$$(1 + g \cdots + g^{N-1})\beta(g) = 0.$$

(d) For any $g \in G$, we have $\beta(g^{-1}) = -g^{-1}\beta(g)$.

(e) If σ, $\tau \in G$ satisfy $\tau\sigma = \sigma^{-1}\tau$, then

$$(\sigma - 1)\beta(\tau) + (1 + \sigma\tau)\beta(\sigma) = 0.$$

4. A method for finding formulas for p-groups

We now present a method for finding a formula for a given p-group G. It consists in taking a presentation of G and deriving from it a system of equations whose indeterminates are elements $b(\sigma) \in R$, one for each generator σ in the presentation. There is an equation for each relation in the presentation. Group cohomology guarantees that this system of equations has a solution. Once we have a solution, we again use homological algebra to obtain an explicit formula for G.

In view of Propositions 1.3 and 2.1 we may assume that G is a finite p-group (not elementary abelian) and that we have formulas for all proper subgroups of G. Let G act on a ring R. We assume the existence of $x_H \in R$ such that $N_H(x_H) = 1$ for each proper subgroup H of G. Our aim is to give an explicit formula for $x_G \in R$ with $N_G(x_G) = 1$ in terms of the elements x_H and of the elements of G.

Fix a normal subgroup U of index p in G and choose an element $\sigma \in G$ whose class $\bar{\sigma}$ generates the cyclic group G/U. Set $x = x_U \in R$ (this is one of the elements x_H whose existence was assumed above); we have $N_U(x) = 1$.

PROPOSITION 4.1.— *Let $a \in R$ be a U-invariant element such that*

$$N_{G/U}(a) = (1 + \sigma + \cdots + \sigma^{p-1})(a) = 1.$$

Then $N_G(y) = 1$ if $y = ax$ or $y = xa$.

PROOF.— Let $y = ax$. By the R^U-linearity of N_U, we have

$$N_G(y) = N_{G/U}(N_U(ax)) = N_{G/U}(aN_U(x)) = N_{G/U}(a) = 1.$$

A similar proof holds for $y = xa$. □

To solve the problem for G, it is therefore sufficient to find an element $a \in R^U$ such that $N_{G/U}(a) = 1$. In the rest of the section we show how to find such an element.

We start as in [3, Section 2] by considering the group $B = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], R)$ of $\mathbf{Z}$-linear maps from the group ring $\mathbf{Z}[G]$ to R. The group G acts on the left on B by $(g\varphi)(s) = \varphi(sg)$ for all $g, s \in G$ and $\varphi \in B$. The ring R is a G-submodule of B, where an element $r \in R$ is identified with the element $\varphi_r \in B$ given by $\varphi_r(g) = g(r)$ for all $g \in G$. Let $C = B/R$ be the quotient G-module. We denote $q : B \to C$ the canonical surjection.

Consider the following commutative square:

$$\begin{tikzcd}
H^1(G/U, C^U) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\delta"'] & H^1(G, C) \arrow[d, "\delta"'] \\
H^2(G/U, R^U) \arrow[r, "\mathrm{Inf}"] & H^2(G, R)
\end{tikzcd} \tag{4.1}$$

The vertical maps δ in (4.1) are the connecting homomorphisms arising from the short exact sequences

$$0 \to R \to B \to C \to 0 \quad \text{and} \quad 0 \to R^U \to B^U \to C^U \to H^1(U, R) = 0.$$

By Proposition 3.1 the group $H^1(U, R)$ vanishes because of the existence of the element $x \in R$ satisfying $N_U(x) = 1$. The maps δ are isomorphisms because B is a co-induced G-module and B^U is a co-induced G/U-module, hence $H^i(G, B) = H^i(G/U, B^U) = 0$ for all $i > 0$.

The horizontal maps in (4.1) are inflation maps. By the Lyndon-Hochschild-Serre spectral sequence the vanishing of $H^i(U, R)$ for $i > 0$ (see Proposition 3.1) implies that the lower inflation map $\mathrm{Inf} : H^2(G/U, R^U) \to H^2(G, R)$ is an isomorphism. Therefore, the upper inflation map is an isomorphism as well. In view of this, of Proposition 1.3 and of Proposition 3.1, all groups in the square (4.1) vanish.

Next, define $\varphi \in B$ by

$$\varphi(g) = \begin{cases} 1 & \text{if } g \in U, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

It is clear that φ is invariant under the action of the subgroup U and that

$$N_{G/U}(\varphi) = (1 + \sigma + \cdots + \sigma^{p-1})(\varphi) = \varphi_1 = 1.$$

Consider the map $\alpha_0 : G/U \to B^U$ given by

$$\alpha_0(\bar{\sigma}^k) = \begin{cases} 0 & \text{if } k = 0, \\ \varphi & \text{if } k = 1, \\ (1 + \sigma + \cdots + \sigma^{k-1})(\varphi) & \text{if } 2 \leq k \leq p - 1. \end{cases} \tag{4.3}$$

Let $q\alpha_0 : G/U \to C^U$ be the composition of α_0 with $q_{|B^U} : B^U \to C^U$.

LEMMA 4.2.— *The map* $q\alpha_0 : G/U \to C^U$ *is a 1-cocycle.*

PROOF.— It suffices to check that

$$q\alpha_0(\bar{\sigma}^i) + \bar{\sigma}^i q\alpha_0(\bar{\sigma}^j) = q\alpha_0(\bar{\sigma}^{i+j})$$

for all $i, j \in \{0, 1, \ldots, p-1\}$. This follows from the definition of α_0 and the following equalities in C:

$$q((1 + \bar{\sigma} + \cdots + \bar{\sigma}^{p-1})(\varphi)) = q(N_{G/U}(\varphi)) = q(\varphi_1) = 0. \qquad \square$$

Define $\alpha : G \to B$ by $\alpha(g) = \alpha_0(\bar{g})$ for all $g \in G$, where $\bar{g}$ denotes the class of g in G/U. By (4.3) the value of α on the chosen element σ is $\alpha(\sigma) = \varphi$.

Let $q\alpha : G \to C$ be the composition of α with $q : B \to C$. By Lemma 4.2, $q\alpha_0 : G/U \to C^U$ represents an element in $H^1(G/U, C^U)$. It is easy to check that its image in $H^1(G, C)$ under the upper inflation map in the square (4.1) is represented by the map $q\alpha : G \to C$. Since $q\alpha_0$ is a 1-cocycle, so is $q\alpha$.

Our idea is to correct $\alpha : G \to B$ as follows.

LEMMA 4.3.— *There is a map* $b : G \to R$ *such that*

$$\alpha - b = \alpha - \varphi_b : G \to B$$

is a 1-*cocycle with values in* B.

PROOF.— We have seen above that $H^1(G, C) = 0$. Since $q\alpha$ is a 1-cocycle with values in C, it is a 1-coboundary; so there is $\bar{\psi} \in C$ such that $q\alpha = \delta(\bar{\psi})$. Lift $\bar{\psi}$ to an element $\psi \in B$ and set $b = \alpha - \delta(\psi)$. Then $\alpha - b = \delta(\psi)$ is a 1-coboundary with values in B, hence a 1-cocycle. $\square$

We now claim that it suffices to perform the following three tasks in order to find a formula for G.

Task 1: Write the set of equations satisfied by the values $b(g) \in R$ of the map b, obtained by expressing that $\alpha - b : G \to B$ is a 1-cocycle. We can reduce the number of unknowns by choosing a presentation $\langle \sigma_1, \ldots, \sigma_r \mid R_1, \ldots, R_s \rangle$ of G. Since the generators are of finite order, we may assume that each relation R_i is a word in $\sigma_1, \ldots, \sigma_r$ (i.e., the inverses of $\sigma_1, \ldots, \sigma_r$ do not appear in R_i).

Set $\beta = \alpha - b$. For each relation $R_i = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_t}$ define

$$\beta(R_i) = \beta(\sigma_{i_1}) + \sigma_{i_1}\beta(\sigma_{i_2}) + \cdots + \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_{t-1}}\beta(\sigma_{i_t}). \qquad (4.4)$$

By setting $\beta(R_i) = 0$ for all $i = 1, \ldots, s$, we obtain a system (Σ) of s equations whose unknowns are $b(\sigma_1), \ldots, b(\sigma_r)$. It is an easy exercise to show that the values $b(\sigma_1), \ldots, b(\sigma_r) \in R$ determine uniquely a map $b : G \to R$ such that $\alpha - b$ is a 1-cocycle.

Task 2: By Lemma 4.3 the system of equations (Σ) derived in Task 1 has a solution $b : G \to R$. Task 2 consists in writing down such a solution polynomially in terms of the given data.

Task 3: By Proposition 3.1 the existence of a norm one element $x \in R$ for U implies the vanishing of $H^1(U, R)$. Hence, for any 1-cocycle $\beta : U \to R$ there is an element $w \in R$ such that $\beta(g) = (g-1)w$ for all $g \in U$. Give an explicit expression of such an element w as a noncommutative polynomial with integer coefficients in the variables $u(x)$ and $u(\beta(v))$, where $u, v \in U$.

Once Tasks 1–3 are completed, we solve the problem for G as follows. Let $b : G \to R$ be a solution of the system (Σ) (in particular, we have an element $b(\sigma) \in R$). Then $\alpha - b$ is a 1-cocycle with values in B. Since B is cohomologically trivial, there is $\psi : G \to R$ such that $\alpha - b = \delta(\psi)$. In particular, since $\alpha(g) = \varphi$ for $g = \sigma$, we obtain

$$\varphi - b(\sigma) = (\sigma - 1)\psi. \tag{4.5}$$

Similarly, by (4.3),

$$0 - b(g) = (g - 1)\psi \tag{4.6}$$

for all $g \in U$. Equations (4.6) imply that the restriction of b to U is a 1-cocycle with values in R. After performing Task 3, we have an element $w \in R$ such that

$$b(g) = (g - 1)w \tag{4.7}$$

for all $g \in U$. Relations (4.6–4.7) together imply

$$(g - 1)(\psi + w) = 0$$

for all $g \in U$, which means that $\psi + w$ is U-invariant.

Proposition 4.4.— *With the previous notation the element*

$$a = b(\sigma) + (1 - \sigma)(w) \in R$$

is U-invariant and we have $N_{G/U}(a) = 1$.

Proof.— (a) Relation (4.5) allows us to express a under the form

$$a = \varphi - (\sigma - 1)(\psi + w).$$

To check the U-invariance of a, it is enough to check the U-invariance of

$$(\sigma - 1)(\psi + w)$$

since φ is U-invariant. For $u \in U$ let $u' \in U$ be such that $u\sigma = \sigma u'$ (recall that U is a normal subgroup of G). Therefore, in view of the U-invariance of $\psi + w$, for $u \in U$ we obtain

$$\begin{aligned} u(\sigma - 1)(\psi + w) &= u\sigma(\psi + w) - u(\psi + w) \\ &= \sigma u'(\psi + w) - u(\psi + w) \\ &= \sigma(\psi + w) - (\psi + w) \\ &= (\sigma - 1)(\psi + w). \end{aligned}$$

(b) Since σ^p belongs to U, the U-invariance of $\psi + w$ implies

$$\begin{aligned} N_{G/U}(a) &= N_{G/U}(\varphi) - (1 + \sigma + \cdots + \sigma^{p-1})(\sigma - 1)(\psi + w) \\ &= 1 - (\sigma^p - 1)(\psi + w) = 1. \end{aligned}$$

□

By Proposition 4.1, the element $y = ax \in R$ (or $y = xa$) then yields an explicit norm one element for G with the appropriate form. This solves the problem for G.

Remark 4.5. Before we close this section, let us evaluate the level of difficulty of Tasks 1–3. We explained above how to perform Task 1; this is easy. For Task 3 we have a general method to solve it; it will be detailed in the next section.

At the moment we do not have a general method to solve Task 2, which consists in solving the system of equations (Σ) defined above. The solutions given in Sections 6–8 have been found in an *ad hoc* way; we nevertheless observe that they are of a very simple form. If we could prove in full generality that the solutions of (Σ) are of the form

$$\sum_H A_H(x_H),$$

where H runs over all maximal proper subgroups of G, $A_H \in \mathbf{Z}[G]$, and $x_H \in R$ satisfies $N_H(x_H) = 1$, then solving (Σ) could be reduced to solving a system (Σ') of linear equations over the ring of integers $\mathbf{Z}$, whose number of unknowns and of equations can be bounded in terms of G. More precisely, if r is the number of generators and s is the number of relations in the chosen presentation of the group G, and if m is the number of maximal proper subgroups of G, then the number of unknowns in (Σ') is $rm|G|$ and the number of equations is $s|G|$. Note that the number of maximal proper subgroups of G is $m = (p^N - 1)(p - 1)$, where p^N is the order of the quotient of G by its Frattini subgroup.

5. Writing a 1-cocycle as an explicit 1-coboundary

We consider a finite p-group U acting on a ring R. Assume that we have an element $x \in R$ such that $N_U(x) = 1$. The cohomology group $H^1(U, R)$ vanishes by Proposition 3.1. Therefore, given a 1-cocycle $\beta : U \to R$, there exists $w \in R$ such that $\beta(g) = (g - 1)w$ for all $g \in U$. Our aim in this section is to explain how to obtain a formula for w in terms of $x \in R$, the elements of U, and the values of β (this is Task 3 of the previous section).

Let us start with the case when $U = C_p$ is a cyclic group of order p. We denote σ a generator of U. If $\beta : U \to R$ is a 1-cocycle of U with values in R, then by Lemma 3.2 (c)

$$N_U(\beta(\sigma)) = (1 + \sigma + \cdots + \sigma^{p-1})\beta(\sigma) = 0.$$

Now by Lemma 1 of [3] we have $\beta(\sigma) = (\sigma - 1)w$, where

$$w = \sum_{k=1}^{p-1} (1 + \sigma + \cdots + \sigma^{k-1})\big(x\sigma^{-k}\beta(\sigma)\big) \in R. \tag{5.1}$$

The right-hand side of (5.1) is a noncommutative polynomial with integer coefficients in the variables $u(x)$ and $u(\beta(\sigma))$, where $u \in U$. By Lemma 3.2 (b) we obtain for $g = \sigma^i$, where $1 \leq i \leq p-1$,

$$\begin{aligned}\beta(g) &= (1+\sigma+\cdots+\sigma^{i-1})\beta(\sigma)\\ &= (1+\sigma+\cdots+\sigma^{i-1})(\sigma-1)w\\ &= (\sigma^i-1)w = (g-1)w.\end{aligned}$$

With Formula (5.1) we have thus expressed any 1-cocycle as a 1-coboundary in the case when U is a cyclic group of order p. Formula (5.1) is the prototype of formulas we wish to obtain for w in the general case.

To deal with a general finite p-group U, we proceed by induction on the order of U. Fix a normal subgroup U' of U of index p and choose $\sigma \in U$ such that its class $\bar{\sigma}$ in U/U' generates U/U'. Following (1.2), set

$$x' = (1+\sigma+\cdots+\sigma^{p-1})(x). \tag{5.2}$$

Then $N_{U'}(x') = 1$. We assume that we know how to express any 1-cocycle $\gamma : U' \to R$ as the coboundary of an element of R expressed as a noncommutative polynomial with integer coefficients in $u'(x')$ and $u'(\gamma(v'))$ $(u', v' \in U')$.

In order to pass from U' to U we make use of a well-known construction due to Wall [9]. Let (C'_*, d') be the standard resolution of $\mathbf{Z}$ by free left $\mathbf{Z}[U']$-modules. In particular, $C'_0 = \mathbf{Z}[U']$, $C'_1 = \mathbf{Z}[U' \times U']$ and the differential $d' : C'_1 \to C'_0$ is given for all g, $h \in U'$ by

$$d'(g,h) = gh - g.$$

For each $q \geq 0$ we define a chain complex $C_{*,q}$ of free left $\mathbf{Z}[U]$-modules by setting

$$C_{p,q} = \mathbf{Z}[U] \otimes_{\mathbf{Z}[U']} C'_p.$$

We define a differential $d_0 : C_{p,q} \to C_{p-1,q}$ by $d_0 = \mathrm{id}_{\mathbf{Z}[U]} \otimes d'$. Observe that

$$C_{0,q} = \mathbf{Z}[U] \quad \text{and} \quad C_{1,q} = \mathbf{Z}[U \times U']$$

for all $q \geq 0$. The chain complex $C_{*,q}$ is a free resolution of $\mathbf{Z}[U] \otimes_{\mathbf{Z}[U']} \mathbf{Z}$, which can be identified with $\mathbf{Z}[U/U']$. By Lemma 2 and Theorem 1 of [9] there exist $\mathbf{Z}[U]$-linear maps

$$d_k : C_{p,q} \to C_{p+k-1,q-k} \qquad (k \geq 1, q \geq k)$$

such that

(i) when $p = 0$, then $d_1 : C_{0,q} = \mathbf{Z}[U] \to C_{0,q-1} = \mathbf{Z}[U]$ is given by

$$d_1(\xi) = \xi(1+\sigma+\cdots+\sigma^{p-1}) \ \text{ if } \xi \in C_{0,2i}, \tag{5.3}$$

$$d_1(\xi) = \xi(\sigma-1) \ \text{ if } \xi \in C_{0,2i-1} \tag{5.4}$$

(here $i \geq 1$), and

(ii)

$$\sum_{i=0}^{k} d_i d_{k-i} = 0. \tag{5.5}$$

Define a nonnegatively graded $\mathbf{Z}[U]$-module C_*^{W} for all $r \geq 0$ by

$$C_r^{\mathrm{W}} = \bigoplus_{p+q=r} C_{p,q}.$$

Observe that

$$C_0^{\mathrm{W}} = \mathbf{Z}[U] \quad \text{and} \quad C_1^{\mathrm{W}} = \mathbf{Z}[U \times U'] \oplus \mathbf{Z}[U].$$

The maps $d^{\mathrm{W}} = \sum_{k\geq 0} d_k$ define a degree -1 differential on C_*^{W} and turn it into a resolution of $\mathbf{Z}$ by free left $\mathbf{Z}[U]$-modules.

Let us apply the functor $\mathrm{Hom}_{\mathbf{Z}[U]}(-, R)$ to the resolution $(C_*^{\mathrm{W}}, d^{\mathrm{W}})$. Define

$$C^{p,q} = \mathrm{Hom}_{\mathbf{Z}[U]}(C_{p,q}, R) = \mathrm{Hom}_{\mathbf{Z}[U]}(\mathbf{Z}[U] \otimes_{\mathbf{Z}[U']} C'_p, R) = \mathrm{Hom}_{\mathbf{Z}[U']}(C'_p, R)$$

(the last isomorphism follows by adjunction). In particular,

$$C^{0,q} = R \quad \text{and} \quad C^{1,q} = \mathrm{Hom}(U', R)$$

for all $q \geq 0$. The differential d_0 turns into a degree $+1$ differential $\delta^0 : C^{p,q} \to C^{p+1,q}$. The maps d_k ($k \geq 1$) turn into maps $\delta^k : C^{p,q} \to C^{p-k+1,q+k}$, which by (5.5) satisfy

$$\sum_{i=0}^{k} \delta^i \delta^{k-i} = 0. \tag{5.6}$$

Set

$$C_{\mathrm{W}}^p = \bigoplus_{i=0}^{p} C^{i,p-i} \quad \text{and} \quad \delta_{\mathrm{W}} = \sum_{k\geq 0} \delta^k.$$

Then $(C_{\mathrm{W}}^*, \delta_{\mathrm{W}})$ is a cochain complex whose cohomology groups are the groups $H^*(U, R)$.

Any element of $H^1(U, R)$ can be represented by a 1-cocycle in the cochain complex $(C_{\mathrm{W}}^*, \delta_{\mathrm{W}})$, namely by a couple

$$(\gamma, s) \in C^{1,0} \times C^{0,1} = \mathrm{Hom}(U', R) \times R$$

satisfying

$$\delta^0(\gamma) = 0, \quad \delta^1(\gamma) + \delta^0(s) = 0, \quad \delta^2(\gamma) + \delta^1(s) = 0. \tag{5.7}$$

Here $\delta^1(s) = (1 + \sigma + \cdots + \sigma^{p-1})s$. A 1-coboundary in the complex $(C_{\mathrm{W}}^*, \delta_{\mathrm{W}})$ is a couple $(\gamma, s) \in C^{1,0} \times C^{0,1} = \mathrm{Hom}(U', R) \times R$ for which there exists $w \in C^{0,0} = R$ such that

$$\gamma = \delta^0(w) \quad \text{and} \quad s = \delta^1(w) = (\sigma - 1)w. \tag{5.8}$$

Let us explain how to find $w \in R$ for a given 1-cocycle (γ, s). For each $q \geq 0$, $(C^{*,q}, \delta^0)$ is the standard cochain complex whose cohomology groups are the groups $H^*(U', R)$. In particular, the kernel of $\delta^0 : R = C^{0,q} \to C^{1,q}$ is $R^{U'}$. By the first relation in (5.7) the element $\gamma \in C^{1,0}$ is a 1-cocycle for the cochain complex $(C^{*,0}, \delta^0)$. By assumption we know how to construct $w_1 \in R$ such that $\gamma = \delta^0(w_1)$ polynomially in terms of the norm one element x', the values of γ, and the elements of U'.

Set $s' = s - \delta^1(w_1) = s - (\sigma - 1)w_1 \in R$. Then by (5.6) and by the second relation in (5.7),

$$\delta^0(s') = \delta^0(s) - \delta^0\delta^1(w_1) = \delta^0(s) + \delta^1\delta^0(w_1) = \delta^0(s) + \delta^1(\gamma) = 0.$$

This proves that s' belongs to $R^{U'}$.

The element $x'' = N_{U'}(x)$ belongs to $R^{U'}$ and we have

$$(1 + \sigma + \cdots + \sigma^{p-1})x'' = (1 + \sigma + \cdots + \sigma^{p-1})N_{U'}(x) = N_U(x) = 1. \tag{5.9}$$

The third relation in (5.7), together with (5.3) and (5.6), implies

$$\begin{aligned}(1 + \sigma + \cdots + \sigma^{p-1})s' &= \delta^1(s') = \delta^1(s) - \delta^1\delta^1(w_1) \\ &= \delta^1(s) + \delta^2\delta^0(w_1) \\ &= \delta^1(s) + \delta^2(\gamma) = 0.\end{aligned}$$

Since σ^p belongs to the subgroup U', the element $\sigma^p - 1$ acts as 0 on $R^{U'}$, and σ generates a cyclic group of order p in the automorphism group of the ring $R^{U'}$. The element $s' \in R^{U'}$ is of norm zero for this cyclic group. Using Formula (5.1), we obtain an element $w_2 \in R^{U'}$ such that $s' = (\sigma - 1)w_2$, explicitly in terms of s', of σ, and of the element x'' appearing in (5.9).

We claim that $w = w_1 + w_2 \in R$ satisfies Equations (5.8). Indeed,

$$\delta^1(w) = (\sigma - 1)w = (\sigma - 1)w_1 + (\sigma - 1)w_2 = (\sigma - 1)w_1 + s' = s.$$

On the other hand, $\delta^0(w_2) = 0$ since w_2 belongs to $R^{U'}$. Therefore,

$$\delta^0(w) = \delta^0(w_1) = \gamma.$$

This proves our claim and shows how to construct w for the cochain complex $(C^*_{\mathrm{W}}, \delta_{\mathrm{W}})$.

In order to express a 1-cocycle $\beta : U \to R$ in the *standard* cochain complex as a 1-coboundary, we use the comparison lemma between the resolution $(C^{\mathrm{W}}_*, d^{\mathrm{W}})$ and the standard resolution (C_*, d) of $\mathbf{Z}$ by free left $\mathbf{Z}[U]$-modules (see, e.g., Proposition 1.2 in [6, Chapter V]).

Lemma 5.1.— *There exists a chain map*

$$\theta_* : (C_*^{\mathrm{W}}, d^{\mathrm{W}}) \to (C_*, d)$$

such that $\theta_0 : C_0^{\mathrm{W}} = \mathbf{Z}[U] \to C_0 = \mathbf{Z}[U]$ *is the identity map and*

$$\theta_1 : C_1^{\mathrm{W}} = \mathbf{Z}[U \times U'] \oplus \mathbf{Z}[U] \to C_1 = \mathbf{Z}[U \times U]$$

is the $\mathbf{Z}[U]$*-linear map whose restriction to the first summand* $\mathbf{Z}[U \times U']$ *is induced by the natural inclusion of* U' *into* U*, and the restriction to the second summand* $\mathbf{Z}[U]$ *is defined for all* $g \in U$ *by* $\theta_1(g) = (g, \sigma) \in C_1$*.*

Proof.— The existence of θ_* follows from the comparison lemma. Since $C_0^W = C_0 = \mathbf{Z}[U]$, we can take θ_0 to be the identity map. It now suffices to check that $d\theta_1 = d^{\mathrm{W}}$ for the map θ_1 described in the lemma. On the summand $\mathbf{Z}[U \times U']$ we have

$$d(\theta_1(g,h)) = d(g,h) = gh - g = d_0(g,h) = d^{\mathrm{W}}(g,h)$$

for $g \in U$ and $h \in U'$. On the summand $\mathbf{Z}[U]$, by (5.4) we have

$$d(\theta_1(g)) = d(g,\sigma) = g(\sigma - 1) = g\sigma - g = d_1(g) = d^{\mathrm{W}}(g)$$

for $g \in U$. □

When we apply the functor $\mathrm{Hom}_{\mathbf{Z}[U]}(-, R)$ to $\theta_* : (C_*^{\mathrm{W}}, d^{\mathrm{W}}) \to (C_*, d)$, we obtain a cochain map

$$\theta^* : C^*(U,R) = \mathrm{Hom}_{\mathbf{Z}[U]}(C_*, R) \to C_{\mathrm{W}}^* = \mathrm{Hom}_{\mathbf{Z}[U]}(C_*^{\mathrm{W}}, R)$$

inducing an isomorphism in cohomology. The cochain complex $(C^*(U,R), \delta)$ is the standard cochain complex computing $H^*(U,R)$. Now, let $\beta : U \to R$ be a standard 1-cocycle. This is an element of $C^1(U,R)$ such that $\delta(\beta) = 0$. Consider its image $\theta^1(\beta) \in C_{\mathrm{W}}^1$. It is a 1-cocycle in $(C_{\mathrm{W}}^*, \delta_{\mathrm{W}})$. By our investigation above we know how to construct $w \in R$ such that $\theta^1(\beta) = \delta_{\mathrm{W}}(w)$. We claim the following.

Lemma 5.2.— *We have* $\beta = \delta(w)$*.*

Proof.— By construction of θ_1 we have $d\theta_1 = d^{\mathrm{W}}$. Dualizing, we obtain $\theta^1\delta = \delta_{\mathrm{W}}$. Therefore,

$$\theta^1(\delta(w)) = \delta_{\mathrm{W}}(w) = \theta^1(\beta).$$

To conclude it suffices to check that θ^1 is injective. Using the string of natural isomorphisms

$$\begin{aligned} C_{\mathrm{W}}^1 &= \mathrm{Hom}_{\mathbf{Z}[U]}(C_1^{\mathrm{W}}, R) \\ &= \mathrm{Hom}_{\mathbf{Z}[U]}(\mathbf{Z}[U \times U'], R) \oplus \mathrm{Hom}_{\mathbf{Z}[U]}(\mathbf{Z}[U], R) \\ &= \mathrm{Hom}(U', R) \oplus R \end{aligned}$$

and Lemma 5.1, we easily see that the image $\theta^1(\beta)$ of any standard 1-cocycle $\beta \in \mathrm{Hom}(U, R)$ is given by

$$\theta^1(\beta) = (\beta', \beta(\sigma)) \in \mathrm{Hom}(U', R) \oplus R = C^1_{\mathrm{W}},$$

where β' is the restriction of β to U' and $\beta(\sigma)$ is its value on σ. If $\theta^1(\beta) = 0$, then the restriction of β to U' is zero and $\beta(\sigma) = 0$. It follows from Lemma 3.2 (b) that β vanishes on all powers of σ. The cocycle condition (3.1) then implies that β vanishes on all elements of U. This proves the injectivity of θ_1. □

Summing up, we thus have obtained an inductive way (starting from cyclic groups) to express any 1-cocycle of a finite p-group (with values in a ring R) as the coboundary of an element $w \in R$, polynomially in terms of x, the values of the 1-cocycle, and the elements of the group. This is a vast generalization of [3, Lemma 1].

Example 5.3. Let U be an elementary abelian group generated by two generators σ_1 and σ_2 of order two and acting on a ring R. Let U' be the subgroup generated by σ_1. We assume the existence of an element $x \in R$ such that $N_U(x) = 1$. The elements

$$x' = (1 + \sigma_2)(x) \quad \text{and} \quad x'' = (1 + \sigma_1)(x)$$

are of norm one for U' and U/U', respectively. Observe that $\sigma_2(x') = x'$.

A 1-cocycle in the complex $(C^*_{\mathrm{W}}, \delta_{\mathrm{W}})$ corresponding to this situation is a couple $(\gamma, s) \in \mathrm{Hom}(U', R) \times R$ satisfying Equations (5.7). In particular, $\gamma : U' \to R$ is a 1-cocycle for the subgroup U'. Set $r = \gamma(\sigma_1) \in R$. Then Equations (5.7) are equivalent to the following three equations:

$$(1 + \sigma_1)(r) = 0, \quad (\sigma_2 - 1)(r) + (\sigma_1 - 1)(s) = 0, \quad (1 + \sigma_2)(s) = 0.$$

(In this example as in any case when U is a semidirect product of U' and U/U', the map δ^2 in (5.7) vanishes.) By (5.1) we have $r = (\sigma_1 - 1)w_1$, where

$$w_1 = x'\sigma_1(r) = (1 + \sigma_2)(x)\, \sigma_1(r).$$

Consequently,

$$s' = s - (\sigma_2 - 1)w_1 = s - x'(\sigma_2\sigma_1)(r) + x'\sigma_1(r) = s - x'(\sigma_1(\sigma_2 - 1)(r)).$$

Following the procedure above, we have $s' = (\sigma_2 - 1)w_2$, where by (5.1)

$$\begin{aligned} w_2 &= x''\sigma_2(s') \\ &= x''\sigma_2\big(s - x'(\sigma_1(\sigma_2 - 1)(r))\big) \\ &= x''\sigma_2(s) - x''x'(\sigma_2\sigma_1(\sigma_2 - 1)(r)) \\ &= x''\sigma_2(s) + x''x'(\sigma_1(\sigma_2 - 1)(r)) \\ &= (1 + \sigma_1)(x) \cdot \sigma_2(s) + (1 + \sigma_1)(x) \cdot (1 + \sigma_2)(x) \cdot (\sigma_1(\sigma_2 - 1)(r)). \end{aligned}$$

Therefore, if we set

$$\begin{aligned} w &= w_1 + w_2 \\ &= (1+\sigma_2)(x)\cdot\sigma_1(r) + (1+\sigma_1)(x)\cdot\sigma_2(s) \\ &\quad + (1+\sigma_1)(x)\cdot(1+\sigma_2)(x)\cdot(\sigma_1(\sigma_2-1)(r)), \end{aligned} \tag{5.10}$$

we obtain $\gamma(\sigma) = r = (\sigma_1 - 1)w$ and $s = (\sigma_2 - 1)w$.

6. The quaternion 2-groups.

The smallest nonabelian p-groups are the two nonabelian groups of order 8, namely the quaternion group Q_8, which has a unique elementary abelian subgroup of order 2, and the dihedral group D_8, which has two nonconjugate maximal elementary abelian subgroups of order 4. Both Q_8 and D_8 are extraspecial groups.

In this section we apply the method of Section 4 in order to solve the problem for Q_8 and more generally for the generalized quaternion groups $Q_{2^{n+2}}$ $(n \geq 1)$.

The group $G = Q_{2^{n+2}}$ of order 2^{n+2} (with $n \geq 1$) has a presentation with two generators σ, τ and the relations

$$\sigma^{2^{n+1}} = 1, \quad \tau\sigma = \sigma^{-1}\tau, \quad \tau^2 = \sigma^{2^n}. \tag{6.1}$$

Any element of the group can be written as $\sigma^i\tau^j$, where $i = 0, 1, \ldots, 2^{n+1}-1$ and $j = 0, 1$. We take U to be the cyclic group generated by σ. The quotient group G/U is cyclic of order 2 and generated by the class of τ.

The group $Q_{2^{n+2}}$ has a unique elementary abelian subgroup, which is the group of order 2 generated by the central element $\tau^2 = \sigma^{2^n}$.

We follow the method presented in Section 4. Let us first perform Task 1.

Lemma 6.1.— *The values $b(\sigma)$ and $b(\tau) \in R$ satisfy the system of three equations*

$$\begin{cases} N_U(b(\sigma)) & = 0, \\ (\sigma - 1)b(\tau) + (1 + \sigma\tau)b(\sigma) & = 0, \\ (1+\tau)b(\tau) - (1 + \sigma + \cdots + \sigma^{2^n - 1})b(\sigma) & = 1. \end{cases}$$

Proof.— Since the restriction of b to U is a 1-cocycle, the first equation follows from Lemma 3.2 (c). Applying Lemma 3.2 (e) to $\beta = b - \alpha$, we obtain

$$(\sigma - 1)(b(\tau) - \varphi) + (1 + \sigma\tau)b(\sigma) = 0.$$

We derive the second equation of the lemma by recalling that φ is U-invariant. In order to prove the third equation, we use the third relation in (6.1). Since b is a 1-cocycle when restricted to U, we have

$$b(\sigma^{2^n}) = (1 + \sigma + \cdots + \sigma^{2^n - 1})b(\sigma) \tag{6.2}$$

by Lemma 3.2 (b). On the other hand, we have

$$b(\tau^2) = (1+\tau)(b(\tau) - \varphi) = (1+\tau)b(\tau) - N_{G/U}(\varphi) = (1+\tau)b(\tau) - 1. \tag{6.3}$$

The third equation then follows from $\tau^2 = \sigma^{2^n}$ and (6.2–6.3). □

To solve Task 2 , we need an element x of R such that

$$N_U(x) = (1 + \sigma + \cdots + \sigma^{2^{n+1}-1})(x) = 1.$$

Lemma 6.2.— *The elements*

$$b(\sigma) = (1 - \sigma\tau)(x) \quad \textit{and} \quad b(\tau) = (1 + \sigma + \cdots + \sigma^{2^n-1})(x)$$

of R are solutions of the system of equations of Lemma 6.1.

Proof.— For the first equation we have

$$\begin{aligned} N_U(b(\sigma)) &= N_U(1 - \sigma\tau)(x) = N_U(x) - N_U\tau(x) \\ &= N_U(x) - \tau N_U(x) = (1 - \tau)(1) = 0. \end{aligned}$$

We check the second equation:

$$\begin{aligned} (\sigma - 1)b(\tau) + (1 + \sigma\tau)b(\sigma) &= (\sigma - 1)(1 + \sigma + \cdots + \sigma^{2^n-1})(x) \\ &\quad + (1 + \sigma\tau)(1 - \sigma\tau)(x) \\ &= (\sigma^{2^n} - 1 + 1 - (\sigma\tau)^2)(x) = 0. \end{aligned}$$

For the third equation we have

$$\begin{aligned} &(1 + \tau)b(\tau) - (1 + \sigma + \cdots + \sigma^{2^n-1})b(\sigma) \\ &\quad = \big((1 + \tau)(1 + \sigma + \cdots + \sigma^{2^n-1}) - (1 + \sigma + \cdots + \sigma^{2^n-1})(1 - \sigma\tau)\big)(x) \\ &\quad = \tau(1 + \sigma + \cdots + \sigma^{2^{n+1}-1})(x) \\ &\quad = \tau(N_U(x)) = \tau(1) = 1. \end{aligned}$$

□

We now complete Task 3, which is to find an explicit $w \in R$ such that $b(g) = (g - 1)w$ for $g \in U$. By Lemmas 6.1–6.2 we have $N_U(b(\sigma)) = 0$ for $b(\sigma) = (1 - \sigma\tau)(x)$. Since U is cyclic, we may apply [3, Lemma 1]. We then obtain $b(\sigma) = (\sigma - 1)w$, where

$$\begin{aligned} w &= \sum_{k=1}^{2^{n+1}-1} (1 + \sigma + \cdots + \sigma^{k-1})\big(x\,\sigma^{-k} b(\sigma)\big) \\ &= \sum_{k=1}^{2^{n+1}-1} (1 + \sigma + \cdots + \sigma^{k-1})\big(x\,\sigma^{-k}(1 - \sigma\tau)(x)\big). \end{aligned} \tag{6.5}$$

Observe that w is a noncommutative polynomial with $2^{n+1}(2^{n+1} - 1)$ monomials of degree ≤ 2 in terms of x.

As a consequence of Proposition 4.4, the element $a = b(\tau) + (1-\tau)w \in R$ is U-invariant and we have $N_{G/U}(a) = 1$. Therefore, $N_G(ax) = 1$ for $G = Q_{2^{n+2}}$. It can be checked that $y = ax$ is a polynomial in the variables $g(x)$ $(g \in G)$ with $2^n(1 + 4(2^{n+1} - 1))$ monomials of degree ≤ 3.

For the special case when $n = 1$ and $G = Q_8$ is the quaternion group of order 8, we obtain the following element $y \in R$ satisfying $N_{Q_8}(y) = 1$:

$$\begin{aligned}
y = x^2 &+ \sigma(x)x \\
&+ x\sigma(x)x + x\sigma^2(x)x + x\sigma^3(x)x \\
&- x\tau(x)x - x(\sigma^2\tau)(x)x - x(\sigma^3\tau)(x)x \\
&+ \sigma(x)\sigma^2(x)x + \sigma(x)\sigma^3(x)x \\
&- \sigma(x)\tau(x)x - \sigma(x)(\sigma^3\tau)(x)x \\
&+ \sigma^2(x)\sigma^3(x)x - \sigma^2(x)\tau(x)x \\
&+ \tau(x)x^2 + \tau(x)\sigma^2(x)x + \tau(x)\sigma^3(x)x \\
&- \tau(x)(\sigma\tau)(x)x - \tau(x)(\sigma^2\tau)(x)x - \tau(x)(\sigma^3\tau)(x)x \\
&+ (\sigma^2\tau)(x)\sigma^2(x)x - (\sigma^2\tau)(x)(\sigma\tau)(x)x \\
&+ (\sigma^3\tau)(x)\sigma^2(x)x + (\sigma^3\tau)(x)\sigma^3(x)x \\
&- (\sigma^3\tau)(x)(\sigma\tau)(x)x - (\sigma^3\tau)(x)(\sigma^2\tau)(x)x.
\end{aligned} \tag{6.6}$$

The right-hand side of (6.6) contains 26 monomials of degree ≤ 3 in terms of x. If we wish to express y in terms of a norm one element x_E for the elementary abelian subgroup E of Q_8 generated by σ^2, it suffices by (0.1) to replace x in (6.6) by the polynomial $x_E\sigma(x_E)x_E + x_E\sigma(x_E) - x_E^2\sigma(x_E)$. We thus obtain a formula for Q_8 with 666 $(= 2 \cdot 3^2 + 24 \cdot 3^3)$ monomials of degree ≤ 9.

Remark 6.3. Observe that the group Q_8 is extraspecial, and if $G = Q_{2^{n+2}}$ $(n \geq 2)$, then $\mathcal{F}_G = \{C_4, Q_8, D_8\}$.

7. The dihedral 2-groups

The dihedral group $G = D_{2^{n+1}}$ of order 2^{n+1} (where $n \geq 2$) has a presentation with two generators σ, τ and the relations

$$\tau\sigma = \sigma^{-1}\tau \quad \text{and} \quad \tau^2 = \sigma^{2^n} = 1. \tag{7.1}$$

Any element of the group can be written uniquely as $\sigma^i\tau^j$, where $i = 0, 1, \ldots, 2^n - 1$ and $j = 0, 1$. Let U be the normal subgroup generated by σ^2 and τ. The quotient group G/U is the cyclic group of order 2 generated by the class of σ. Note that U is a dihedral group of order 2^n if $n \geq 3$ and an elementary abelian group if $n = 2$. It contains the elementary abelian subgroup U_1 generated by u and τ, where $u = \sigma^{2^{n-1}}$ is the unique non-trivial central element of $D_{2^{n+1}}$.

Let x be an element of R such that $N_U(x) = 1$. We denote H the cyclic group generated by σ (of order 2^n). We follow the method presented in Section 4. Let us first perform Task 1.

LEMMA 7.1.— *The values* $b(\sigma)$ *and* $b(\tau) \in R$ *satisfy the system of three equations*

$$\begin{cases} (1+\tau)b(\tau) & = & 0, \\ N_H(b(\sigma)) & = & 2^{n-1}, \\ (\sigma-1)b(\tau)+(1+\sigma\tau)b(\sigma) & = & 1. \end{cases}$$

PROOF.— Since $b : U \to R$ is a 1-cocycle, and τ and σ^2 belong to U, we have

$$(1+\tau)b(\tau) = 0 \quad \text{and} \quad (1+\sigma^2+\cdots+\sigma^{2^n-2})b(\sigma^2) = b(\sigma^{2^n}) = b(1) = 0. \quad (7.2)$$

This proves the first equation. We have

$$(\alpha - b)(\sigma^2) = (1+\sigma)(\alpha - b)(\sigma)$$

by Lemma 3.2 (b); hence

$$b(\sigma^2) = (1+\sigma)(b(\sigma)-\varphi) = (1+\sigma)b(\sigma) - N_{G/U}(\varphi) = (1+\sigma)b(\sigma) - 1. \quad (7.3)$$

The second relation in (7.2) and Relation (7.3) imply

$$\begin{aligned} N_H(b(\sigma)) &= (1+\sigma^2+\cdots+\sigma^{2^n-2})(1+\sigma)b(\sigma) \\ &= (1+\sigma^2+\cdots+\sigma^{2^n-2})b(\sigma^2) + (1+\sigma^2+\cdots+\sigma^{2^n-2})(1) \\ &= 2^{n-1}. \end{aligned}$$

The second equation of the lemma is thus proved. Applying Lemma 3.2 (e) to $\beta = b - \alpha$, we obtain

$$(\sigma-1)b(\tau) + (1+\sigma\tau)(b(\sigma)-\varphi) = 0,$$

which implies

$$(\sigma-1)b(\tau) + (1+\sigma\tau)b(\sigma) = (1+\sigma\tau)\varphi = N_{G/U}(\varphi) = 1.$$

This proves the last equation. □

Let U_2 be the elementary abelian subgroup of $G = D_{2^{n+1}}$ generated by u and $\sigma\tau$. (The subgroups U_1 and U_2 are not conjugate in G.) Let x_2 be an element of R satisfying

$$N_{U_2}(x_2) = (1+u+\sigma\tau+u\sigma\tau)(x_2) = (1+\sigma\tau)(1+u)(x_2) = 1. \quad (7.4)$$

Lemma 7.2.— *The elements*

$$b(\sigma) = (\sigma + u\tau)(x_2) \quad \textit{and} \quad b(\tau) = (\tau - 1)(1 + u)(x_2)$$

of R are solutions of the system of equations of Lemma 7.1.

Proof.— The first equation is clearly satisfied. For the second one, we have

$$\begin{aligned} N_H(b(\sigma)) &= (N_H\sigma)(x_2) + (N_H u\tau)(x_2) = N_H(1+\tau)(x_2) \\ &= N_G(x_2) = [G : U_2]\, N_{U_2}(x_2) = 2^{n-1}. \end{aligned}$$

We now check the third equation. Using (7.4) and the identities

$$(\sigma - 1)(\tau - 1) = (1 + \sigma\tau)(1 - \sigma) \quad \text{and} \quad N_{U_2} = (1 + \sigma\tau)(1 + u)$$

in $\mathbf{Z}[G]$, we obtain

$$\begin{aligned} (\sigma - 1)b(\tau) + (1 + \sigma\tau)b(\sigma) - 1 &= (1 + \sigma\tau)\big((1 - \sigma)(1 + u) + (\sigma + u\tau) - (1 + u)\big)(x_2) \\ &= (1 + \sigma\tau)(\tau - \sigma)u(x_2) \\ &= (1 + \sigma\tau)(\sigma\tau - 1)\sigma u(x_2) \\ &= ((\sigma\tau)^2 - 1)\sigma u(x_2) = 0. \end{aligned}$$

□

Proceeding as in Section 5, we can find $w \in R$ such that

$$b(\sigma^2) = (\sigma^2 - 1)w \quad \text{and} \quad b(\tau) = (\tau - 1)w.$$

The element w can be expressed (as a noncommutative polynomial with integer coefficients) in terms of the norm one element x, the elements of U, and the values $b(\sigma)$, $b(\tau)$ given in Lemma 7.2. Observe that here we need both x and $x_2 \in R$, which is not surprising since G has two nonconjugate maximal elementary abelian subgroups. As a consequence of Proposition 4.4, the element

$$a = b(\sigma) + (1 - \sigma)(w)$$

is U-invariant and $N_{G/U}(a) = 1$. Hence, $N_G(y) = 1$ for $y = ax$ by Proposition 4.1.

If $G = D_8$, then $U = U_1$ is elementary abelian of order 4, and we can use Example 5.3. Setting $\sigma_1 = \tau$, $\sigma_2 = \sigma^2$, $r = b(\tau)$, and $s = b(\sigma^2)$ in Formula (5.10), we obtain an explicit w with 48 monomials of degree at most 3. Hence for $G = D_8$ we have a norm one element y with 98 monomials of degree ≤ 4.

Remarks 7.3. (a) The group D_8 is extraspecial and, if $G = D_{2^{n+1}}$ $(n \geq 2)$, then $\mathcal{F}_G = \{C_4, D_8\}$.

(b) By Sections 2, 6, 7, we have solved the problem for all 2-groups G such that $\mathcal{F}_G = \{C_4, Q_8, D_8\}$, in particular for all metacyclic 2-groups. Note that by [4, Theorem 5.1] any 2-group every subgroup of which is generated by two elements is metacyclic.

8. A nonabelian group of order 27

Let p be an odd prime number and G_{p^3} be the group generated by σ, τ and the relations

$$\sigma^{p^2} = \tau^p = 1 \quad \text{and} \quad \tau\sigma = \sigma^{p+1}\tau. \tag{8.1}$$

This is the only nonabelian group of order p^3 containing a cyclic subgroup of index p. The center Z of G_{p^3} is the cyclic group generated by σ^p, and G_{p^3}/Z is elementary abelian of order p^2. Therefore, G_{p^3} is extraspecial.

Let U be the elementary abelian subgroup of G_{p^3} generated by σ^p and τ; it is the unique maximal elementary abelian subgroup of G_{p^3}. The quotient group G_{p^3}/U is the cyclic group of order p generated by the class of σ.

Let x be an element of R such that $N_U(x) = 1$. We denote H the cyclic group of order p^2 generated by σ. Following the method of Section 4, we undertake Task 1.

Lemma 8.1.— *The values $b(\sigma)$ and $b(\tau) \in R$ satisfy the system of three equations*

$$\left\{\begin{array}{ccc} (1+\tau+\cdots+\tau^{p-1})b(\tau) & = & 0, \\ N_H(b(\sigma)) & = & p, \\ (\sigma^{p+1}-1)b(\tau) + (1+\sigma+\ldots+\sigma^{p-1}+\sigma^p-\tau)b(\sigma) & = & 1. \end{array}\right.$$

Proof.— Since $b : U \to R$ is a 1-cocycle, and τ and σ^p belong to U, we have

$$(1+\tau+\cdots+\tau^{p-1})b(\tau) = 0 \quad \text{and} \quad (1+\sigma^p+\cdots+\sigma^{(p-1)p})b(\sigma^p) = 0. \tag{8.2}$$

This proves the first equation. By Lemma 3.2 (b) we have

$$(\alpha - b)(\sigma^p) = (1+\sigma+\cdots+\sigma^{p-1})(\alpha - b)(\sigma),$$

which implies

$$\begin{aligned} b(\sigma^p) &= (1+\sigma+\cdots+\sigma^{p-1})(b(\sigma)-\varphi) \\ &= (1+\sigma+\cdots+\sigma^{p-1})b(\sigma) - N_{G_{p^3}/U}(\varphi) \\ &= (1+\sigma+\cdots+\sigma^{p-1})b(\sigma) - 1. \end{aligned} \tag{8.3}$$

The second relation in (8.2), together with Relation (8.3), implies

$$\begin{aligned} N_H(b(\sigma)) &= (1+\sigma^p+\cdots+\sigma^{(p-1)p})(1+\sigma+\cdots+\sigma^{p-1})b(\sigma) \\ &= (1+\sigma^p+\cdots+\sigma^{(p-1)p})b(\sigma^p) + (1+\sigma^p+\cdots+\sigma^{(p-1)p})(1) \\ &= p. \end{aligned}$$

This proves the second equation. To prove the last one, we first compute $b(\sigma^{p+1})$. We have

$$b(\sigma^{p+1}) - \varphi = b(\sigma^p) + \sigma^p(b(\sigma) - \varphi),$$

hence

$$\begin{aligned} b(\sigma^{p+1}) &= b(\sigma^p) + \sigma^p b(\sigma) - (\sigma^p - 1)\varphi \\ &= (1 + \sigma + \cdots + \sigma^{p-1} + \sigma^p)b(\sigma) - 1 \end{aligned}$$

in view of (8.3) and the σ^p-invariance of φ. Applying the cocycle condition to the third relation in (8.1), we obtain

$$\begin{aligned} b(\tau) + \tau(b(\sigma) - \varphi) &= b(\tau\sigma) - \varphi = b(\sigma^{p+1}\tau) - \varphi \\ &= b(\sigma^{p+1}) - \varphi + \sigma^{p+1}b(\tau) \\ &= (1 + \sigma + \cdots + \sigma^{p-1} + \sigma^p)b(\sigma) - 1 - \varphi + \sigma^{p+1}b(\tau). \end{aligned}$$

This, together with the τ-invariance of φ, proves the third equation of the lemma. □

We will solve the system of equations of Lemma 8.1 when $p = 3$, i.e., for the group G_{27} of order 27, generated by σ, τ and the relations

$$\sigma^9 = \tau^3 = 1 \quad \text{and} \quad \tau\sigma = \sigma^4\tau. \tag{8.4}$$

The elementary abelian subgroup U considered above is generated by σ^3 and τ. We assume the existence of $x \in R$ such that $N_U(x) = 1$. The center Z of G_{27} is the cyclic group generated by σ^3; it is contained in U. Therefore, if we set $x_0 = (1 + \tau + \tau^2)(x) \in R$, we have $N_Z(x_0) = 1$.

Consider the cyclic group H' of order 9 generated by $\sigma\tau$. We have $(\sigma\tau)^3 = \sigma^3$. Hence H' contains Z as a subgroup of index 3. By [3, Corollary 1] we obtain an element $x' \in R$ such that $N_{H'}(x') = 1$. To have an explicit formula for x', replace σ by $\sigma\tau$, x_E by $x_0 = (1 + \tau + \tau^2)(x)$, and x_G by x' in Formula (0.2) of the introduction. The element $x' \in R$ is used in the next result.

Lemma 8.2.— *The elements* $b(\sigma) = (1 + \sigma\tau + (\sigma\tau)^2)(x')$ *and*

$$b(\tau) = (\tau - 1)[\sigma^6 - \sigma(1 + \sigma + \sigma^2 + \sigma^4)\tau](x')$$

of R *are solutions of the system of equations of Lemma 8.1.*

Proof.— Set $A = \sigma^6 - \sigma(1 + \sigma + \sigma^2 + \sigma^4)\tau \in \mathbf{Z}[G_{27}]$. Then $b(\tau) = (\tau - 1)A(x')$. The first equation in Lemma 8.1 is satisfied because

$$(1 + \tau + \tau^2)b(\tau) = (1 + \tau + \tau^2)(\tau - 1)A(x') = 0.$$

For the second equation we have

$$\begin{aligned} N_H(b(\sigma)) &= (1 + \sigma + \sigma^2)(1 + \sigma^3 + \sigma^6)(1 + \sigma\tau + (\sigma\tau)^2)(x') \\ &= (1 + \sigma + \sigma^2)(1 + (\sigma\tau)^3 + (\sigma\tau)^6)(1 + \sigma\tau + (\sigma\tau)^2)(x') \\ &= (1 + \sigma + \sigma^2)N_{H'}(x') = (1 + \sigma + \sigma^2)(1) = 3. \end{aligned}$$

The following identity in the group ring $\mathbf{Z}[G_{27}]$ can be checked directly:

$$(\sigma^4 - 1)(\tau - 1)A + (1 + \sigma + \sigma^2 + \sigma^3 - \tau)(1 + \sigma\tau + (\sigma\tau)^2) = N_{H'}. \tag{8.5}$$

(This identity was found using a computer.) Applying both sides of (8.5) to x', we obtain the third equation in Lemma 8.1. $\square$

Proceeding as in Example 5.3, we can find $w \in R$ such that

$$b(\sigma^3) = (\sigma^3 - 1)w \quad \text{and} \quad b(\tau) = (\tau - 1)w.$$

The element w can be expressed (as a noncommutative polynomial with integer coefficients) in terms of the norm one element x, the elements of U, and the values $b(\sigma)$, $b(\tau)$ given in Lemma 8.2. As a consequence of Proposition 4.4, the element $a = b(\sigma) + (1 - \sigma)(w)$ is U-invariant and $N_{G_{27}/U}(a) = 1$. Therefore, $N_{G_{27}}(y) = 1$ for $y = ax$ or $y = xa$ by Proposition 4.1.

As a consequence of Section 2, we have solved the problem for all 3-groups G such that $\mathcal{F}_G = \{C_9, G_{27}\}$.

ACKNOWLEDGEMENTS. We thank Patrick Dehornoy and Ron Holzman for useful discussions on the best way to write up the results of Section 2.

References

[1] E. Aljadeff, *On the surjectivity of some trace maps*, Israel J. Math. 86 (1994), 221–232.

[2] E. Aljadeff, Y. Ginosar, *Induction from elementary abelian subgroups*, J. of Algebra 179 (1996), 599–606.

[3] E. Aljadeff, C. Kassel, *Explicit norm one elements for ring actions of finite abelian groups*, Israel J. Math. 129 (2002), 99–108.

[4] N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. 11 (1961), 1–22.

[5] J. F. Carlson, J. Thévenaz, *Torsion endo-trivial modules*, Algebr. Represent. Theory 3 (2000), 303–335.

[6] H. Cartan, S. Eilenberg, *Homological algebra*, Princeton University Press, Princeton, 1956.

[7] L. G. Chouinard, *Projectivity and relative projectivity over group rings*, J. Pure Appl. Algebra 7 (1976), 287–302.

[8] D. Gorenstein, *Finite groups*, 2nd edition, Chelsea Publ. Co., New York, 1980.

[9] C. T. C. Wall, *Resolutions for extensions of groups*, Proc. Cambridge Phil. Soc. 57 (1961), 251–255.

Eli Aljadeff
Department of Mathematics
Technion - Israel Institute of Technology
32000 Haifa, Israel
E-mail: `aljadeff@techunix.technion.ac.il`
Fax: +972-4-832-4654

Christian Kassel
Institut de Recherche Mathématique Avancée
CNRS - Université Louis Pasteur
7 rue René Descartes
67084 Strasbourg Cedex, France
E-mail: `kassel@math.u-strasbg.fr`
Fax: +33 (0)3 90 24 03 28
http://www-irma.u-strasbg.fr/~kassel/

(Version of 18 April 2005)