

EXPLICIT NORM ONE ELEMENTS FOR RING ACTIONS OF FINITE ABELIAN GROUPS*

BY

ELI ALJADIEFF

*Department of Mathematics, Technion — Israel Institute of Technology
32000 Haifa, Israel
e-mail: aljadeff@techunix.technion.ac.il*

AND

CHRISTIAN KASSEL

*Institut de Recherche Mathématique Avancée, C.N.R.S. — Université Louis Pasteur
7 rue René Descartes, 67084 Strasbourg Cedex, France
e-mail: kassel@math.u-strasbg.fr
Web: www-irma.u-strasbg.fr/kassel/*

ABSTRACT

It is known that the norm map N_G for the action of a finite group G on a ring R is surjective if and only if for every elementary abelian subgroup U of G the norm map N_U is surjective. Equivalently, there exists an element $x_G \in R$ satisfying $N_G(x_G) = 1$ if and only if for every elementary abelian subgroup U there exists an element $x_U \in R$ such that $N_U(x_U) = 1$. 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_U . We solve this problem when the group G is abelian. The main part of the proof, which was inspired by cohomological considerations, deals with the case when G is a cyclic p -group.

* Supported by TMR-Grant ERB FMRX-CT97-0100 of the European Union.
Received January 1, 2000 and in revised form August 20, 2001

Introduction

Let R be a ring (with unit element 1) and G a finite group acting on R by ring automorphisms. For any subgroup U of G define the norm map (sometimes called the trace map) $N_U: R \rightarrow R^U$ by

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

Ginsar and the first author reduced the surjectivity of the norm map N_G for a group G to the surjectivity of the norm maps for its elementary abelian subgroups; more precisely, they proved that $N_G: R \rightarrow R^G$ is surjective if and only if $N_U: R \rightarrow R^U$ is surjective for every elementary abelian subgroup U of G (see [2, Theorem 1]).

The R^U -linearity of N_U implies that it is surjective if and only there exists an element $x_U \in R$ such that $N_U(x_U) = 1$. Suppose we have such an element x_U for every elementary abelian subgroup U of G . Then by the result mentioned above there is a “global” element $x_G \in R$ such that $N_G(x_G) = 1$. Using this last statement, Shelah observed (see [2, Proposition 6]) that there exists a formula in which x_G is a finite sum of the form

$$x_G = \sum a g_{i_1}(x_{U_{j_1}}) g_{i_2}(x_{U_{j_2}}) \cdots g_{i_r}(x_{U_{j_r}}),$$

where $a \in \mathbf{Z}$, $g_{i_1}, g_{i_2}, \dots, g_{i_r} \in G$, and $U_{j_1}, U_{j_2}, \dots, U_{j_r}$ are elementary abelian subgroups of G .

Using a tensor induction argument, the first author found such a formula in case the ring R is commutative (see [1, Theorem 2.1]). When R is not commutative, the only formulas known so far hold in the following two cases:

- (a) G is an abelian 2-group and R is an algebra over the field \mathbf{F}_2 (cf. [2, Section 2]),
- (b) $G = \mathbf{Z}/4$ and R is any ring (see Formula (2) below).

The aim of this article is to show how to find an explicit formula of the above form in the case of a finite *abelian group* G acting on an arbitrary *noncommutative ring* R . The main and most involved part in the construction is to give a formula for a norm one element in case G is a cyclic p -group. More precisely, in Theorem 1 below, we express a norm one element for a cyclic group G of order p^n in terms of a norm one element for a proper subgroup of order $\geq p^{n/2}$. This allows us to find by induction a norm one element for a cyclic p -group in terms of a norm one element for its unique elementary abelian subgroup. Next, using the expression for cyclic p -groups, we show how to obtain an explicit formula for a norm one element for any abelian p -group in terms of a norm one element for its maximal elementary

abelian subgroup. Finally, we extend the formula to arbitrary abelian groups. We emphasize that a formula for abelian p -groups cannot be obtained simply by “gluing the cyclic components” since the existence of norm one elements for all cyclic subgroups does not imply the existence of a global element of norm one (see [1]).

Theorem 1 appears in Section 1; its proof is given in Section 2. In Section 3 we extend our result to arbitrary finite abelian groups, and in Section 4 we give some cohomological explanations for the proof of Theorem 1.

1. Statements for cyclic p -groups

We fix a prime number p , and integers n and k verifying $n \geq 2$ and $1 \leq k \leq n/2$. Consider the cyclic group $G = \mathbf{Z}/p^n$ of order p^n with a generator σ , and the cyclic subgroup U of order p^{n-k} , generated by σ^{p^k} . Let R be a (nonnecessarily commutative) ring on which G acts by ring automorphisms. Our main result is the following.

THEOREM 1: *Let $x \in R$ satisfy $N_U(x) = 1$. Define z and $a \in R$ by*

$$z = p^{n-2k}(1 + \sigma + \sigma^2 + \cdots + \sigma^{p^k-1})(x) - 1$$

and

$$(1) \quad a = p^{n-2k}x + (1 - \sigma) \left(\sum_{i=1}^{p^{n-k}-1} \left(1 + \sigma^{p^k} + \sigma^{2p^k} + \cdots + \sigma^{(i-1)p^k} \right) (x\sigma^{-ip^k}(z)) \right).$$

Then $N_G(ax) = 1$.

When $G = \mathbf{Z}/p^2$, the theorem can be reformulated as follows.

COROLLARY 1: *Let σ be an automorphism of order p^2 of a ring R , and $x \in R$ satisfying $(1 + \sigma^p + \sigma^{2p} + \cdots + \sigma^{(p-1)p})(x) = 1$. Define*

$$z = (1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1})(x) - 1$$

and

$$a = x + (1 - \sigma) \left(\sum_{i=1}^{p-1} \left(1 + \sigma^p + \sigma^{2p} + \cdots + \sigma^{(i-1)p} \right) (x\sigma^{-ip}(z)) \right).$$

Then

$$(1 + \sigma + \sigma^2 + \cdots + \sigma^{p^2-1})(ax) = 1.$$

For $p = 2, 3$, the corollary yields the following explicit formulas. When $p = 2$, starting from $x \in R$ such that $x + \sigma^2(x) = 1$, we obtain the norm one element

$$\begin{aligned} ax &= \sigma(x)x - \sigma(x)x^2 + x\sigma^2(x)x + x\sigma^3(x)x - \sigma(x)\sigma^3(x)x \\ &= 2x^2 - x^3 - x\sigma(x)x - \sigma(x)x^2 + \sigma(x)^2x. \end{aligned}$$

In this case, Péter P. Pálfi had shown the first author the following simpler formula:

$$(2) \quad x\sigma(x)x + x\sigma(x) - x^2\sigma(x).$$

When $p = 3$, starting now from $x \in R$ such that $x + \sigma^3(x) + \sigma^6(x) = 1$, we obtain the norm one element

$$\begin{aligned} ax &= -x^2 + 2\sigma(x)x - \sigma^3(x)x + \sigma^4(x)x \\ &\quad + x\sigma^3(x)x + x\sigma^4(x)x + x\sigma^5(x)x + x\sigma^6(x)x + x\sigma^7(x)x + x\sigma^8(x)x \\ &\quad - \sigma(x)\sigma^4(x)x - \sigma(x)\sigma^5(x)x - \sigma(x)\sigma^6(x)x \\ &\quad - \sigma(x)\sigma^7(x)x - \sigma(x)\sigma^8(x)x - \sigma(x)x^2 \\ &\quad + \sigma^3(x)\sigma^6(x)x + \sigma^3(x)\sigma^7(x)x + \sigma^3(x)\sigma^8(x)x \\ &\quad - \sigma^4(x)\sigma^7(x)x - \sigma^4(x)\sigma^8(x)x - \sigma^4(x)x^2. \end{aligned}$$

Using Theorem 1 repeatedly, we can find an explicit expression for an element $x_G \in R$ with $N_G(x_G) = 1$ as a noncommutative polynomial in the variables $\sigma^i(x_E)$ ($0 \leq i < p^n$), where $x_E \in R$ satisfies $N_E(x_E) = 1$ for the unique elementary abelian subgroup $E \cong \mathbf{Z}/p$ of G . Formula (1) also gives an upper bound for the number of monomials appearing in this polynomial. Indeed, the number of monomials for a in (1) is $\leq p^{n-k}(p^{n-k} - 1)(p^k + 1) + 1$. We obtain a crude upper bound by setting $k = 1$ and by summing from 2 to n . The upper bound we get in this way is

$$\frac{p(p+1)(p^{n-1} - 1)(p^n - 1)}{p^2 - 1} + n - 1 \sim \frac{p+1}{p^2 - 1} p^{2n}$$

when n becomes large. By taking k as the largest integer $\leq n/2$, we get a smaller upper bound, which is equivalent to $p^{1/2}p^{3n/2}$ ($n \gg 0$).

2. Proof of Theorem 1

We shall need a special case of the following lemma, directly inspired from Proposition 1.3 of [3, Chap. XII].

LEMMA 1: Let U be a finite group acting by ring automorphisms on a ring R . If there exists an element $x \in R$ such that $N_U(x) = 1$, then every element $z \in R$ such that $N_U(z) = 0$ can be written as

$$z = \sum_{g \in U} (g - 1)(xg^{-1}(z)).$$

Proof: Computing the right-hand side, we obtain

$$\begin{aligned} \sum_{g \in U} (g - 1)(xg^{-1}(z)) &= \sum_{g \in U} g(x)g(g^{-1}(z)) - \sum_{g \in U} xg^{-1}(z) \\ &= N_U(x)z - xN_U(z) = z. \quad \blacksquare \end{aligned}$$

Let us apply Lemma 1 to the case when U is a cyclic group of order r . If we denote a generator of U by t , then every element $z \in R$ such that $N_U(z) = 0$ is of the form $z = (t - 1)(w)$, where

$$(3) \quad w = \sum_{i=1}^{r-1} (1 + t + t^2 + \cdots + t^{i-1})(xt^{-i}(z)).$$

We now start the proof of Theorem 1. Recall that G is a cyclic group of order p^n , generated by σ , and U is the subgroup generated by σ^{p^k} , where $1 \leq k \leq n/2$.

Consider the group $B = \text{Hom}(\mathbf{Z}[G], R)$ of \mathbf{Z} -linear maps from the group ring $\mathbf{Z}[G]$ to R , and equip it with the G -action given by $(g\varphi)(s) = \varphi(sg)$ for all $g, s \in G$ and $\varphi \in B$. We embed R into B by considering an element $x \in R$ as the element $\varphi_x \in B$ determined by $\varphi_x(g) = g(x)$ for all $g \in G$. The embedding $R \subset B$ preserves the G -action.

Define $\varphi \in B$ by

$$\varphi(g) = \begin{cases} 1 & \text{if } g = \sigma^{ip^k} \text{ } (0 \leq i < p^{n-k}), \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that φ is invariant under the action of the subgroup U . Since the action of G on the group B^U of U -invariant elements of B factors through an action of the quotient cyclic group G/U , we may consider the action of

$$N_{G/U} = 1 + \sigma + \sigma^2 + \cdots + \sigma^{p^k-1}$$

on B^U . We clearly have

$$(4) \quad N_{G/U}(\varphi) = \varphi_1 \quad \text{and} \quad N_G(\varphi) = p^{n-k}\varphi_1.$$

On the other hand, $N_U(x) = 1$ implies $N_G(x) = p^k$. Therefore

$$(5) \quad N_G(\varphi - p^{n-2k}\varphi_x) = 0.$$

(Observe that p^{n-2k} is an integer since we assume $k \leq n/2$.) Define $\psi \in B$ inductively by $\psi(\sigma^0) = 0$ and for $1 \leq i < p^n$ by

$$\psi(\sigma^i) = \psi(\sigma^{i-1}) - \varphi(\sigma^{i-1}) + p^{n-2k}\sigma^{i-1}(x).$$

It follows from the definition of ψ and from (5) that

$$(6) \quad \varphi = (1 - \sigma)(\psi) + p^{n-2k}\varphi_x.$$

LEMMA 2: *The element $\psi \in B$ is U -invariant modulo R .*

Proof: By (4) and (6) we have

$$\begin{aligned} \varphi_1 &= N_{G/U}(\varphi) \equiv N_{G/U}((1 - \sigma)(\psi)) \\ &\equiv ((1 + \sigma + \sigma^2 + \cdots + \sigma^{p^k-1})(1 - \sigma))(\psi) \\ &\equiv (1 - \sigma^{p^k})(\psi) \quad \text{modulo } R. \end{aligned}$$

We conclude by observing that $\varphi_1 \equiv \varphi_0 \equiv 0$ modulo R . ■

It follows from Lemma 2 that there exists $z \in R$ such that

$$(7) \quad (\sigma^{p^k} - 1)(\psi) = \varphi_z.$$

In order to find z , it suffices to apply both sides of (7) to the unit element of G ; we thus obtain $z = \psi(\sigma^{p^k}) - \psi(\sigma^0)$, which, by definition of ψ , equals

$$(8) \quad z = p^{n-2k}(1 + \sigma + \sigma^2 + \cdots + \sigma^{p^k-1})(x) - 1.$$

We claim that the element $z \in R$ is killed by N_U . Indeed, by (7),

$$N_U(z) = N_U((\sigma^{p^k} - 1)(\psi)) = (\sigma^{p^n} - 1)(\psi) = 0.$$

Applying Formula (3), we have $z = (\sigma^{p^k} - 1)(w)$, where

$$(9) \quad w = \sum_{i=1}^{p^{n-k}-1} (1 + \sigma^{p^k} + \sigma^{2p^k} + \cdots + \sigma^{(i-1)p^k})(x\sigma^{-ip^k}(z)).$$

Formulas (7) and (9) imply

$$(10) \quad (\sigma^{p^k} - 1)(\psi - \varphi_w) = 0.$$

In other words, $\psi - \varphi_w$ is U -invariant.

LEMMA 3: The element $a = p^{n-2k}x + (1 - \sigma)(w) \in R$ is U -invariant and $N_{G/U}(a) = 1$.

Proof: By definition of a and w , and by (6), we have

$$\varphi_a = \varphi - (1 - \sigma)(\psi - \varphi_w),$$

which is U -invariant in view of (10). By (4) and (10), we obtain

$$\begin{aligned} N_{G/U}(a) &= N_{G/U}(\varphi) - N_{G/U}((1 - \sigma)(\psi - \varphi_w)) \\ &= \varphi_1 - (1 - \sigma^p)(\psi - \varphi_w) = 1. \quad \blacksquare \end{aligned}$$

We can now complete the proof of Theorem 1. First observe that the elements $a \in R^U$ and $z \in R$ of the theorem are exactly the ones introduced in this section. So it is enough to check that $N_G(ax) = 1$. Indeed, using the R^U -linearity of N_U , Lemma 3, and $N_U(x) = 1$, we have

$$\begin{aligned} N_G(ax) &= \sum_{g \in G} g(ax) = \sum_{t \in G/U} t \left(\sum_{s \in U} s(ax) \right) \\ &= \sum_{t \in G/U} t(N_U(ax)) = \sum_{t \in G/U} t(aN_U(x)) \\ &= \sum_{t \in G/U} t(a) = N_{G/U}(a) = 1. \quad \blacksquare \end{aligned}$$

3. Extension to finite abelian groups

In this section we show how to use Theorem 1 to obtain a formula for a norm one element for an arbitrary abelian group in terms of norm one elements for its maximal elementary abelian subgroups.

We start with the case of an abelian p -group G for some prime number p . Suppose that it is of the form $G = G_0 \times G_1$, where G_1 is cyclic of order p^n for some integer $n \geq 2$. Let H be the subgroup of G given by $H = G_0 \times H_1$, where H_1 is the subgroup of order p in G_1 . Suppose we have an element $x_H \in R$ such that $N_H(x_H) = 1$. We first give a formula for an element $x_G \in R$ of norm one for the whole group G in terms of x_H . If $z = N_{G_0}(x_H)$, then

$$N_{H_1}(z) = N_{H_1}(N_{G_0}(x_H)) = N_H(x_H) = 1.$$

By a repeated use of Theorem 1, we obtain an explicit element $x_{G_1} = f(z) \in R$ such that $N_{G_1}(x_{G_1}) = 1$. Note that z is G_0 -invariant; moreover, since G_0 centralizes G_1 , the element $x_{G_1} = f(z)$ is G_0 -invariant as well. Define $x_G \in R$ by $x_G = x_{G_1} N_{H_1}(x_H)$.

LEMMA 4: We have $N_G(x_G) = 1$.

Proof: By the G_0 -invariance of x_{G_1} we have

$$\begin{aligned} N_{G_0}(x_G) &= \sum_{g \in G_0} g(x_{G_1})g(N_{H_1}(x_H)) \\ &= x_{G_1}N_{G_0}(N_{H_1}(x_H)) \\ &= x_{G_1}N_H(x_H) = x_{G_1}. \end{aligned}$$

This implies $N_G(x_G) = N_{G_1}(N_{G_0}(x_G)) = N_{G_1}(x_{G_1}) = 1$. ■

Using repeatedly the above procedure, we obtain a formula for a norm one element for any abelian p -group in terms of a norm one element for its unique maximal elementary abelian subgroup.

We next consider the case of an arbitrary finite abelian group G . In order to obtain a formula for a norm one element for G in terms of norm one elements for the elementary abelian subgroups of G , it suffices in view of the previous extension to give a formula for a norm one element for G in terms of norm one elements for the Sylow subgroups of G .

Suppose that the order n of G has a factorization $n = p_1^{a_1} \cdots p_r^{a_r}$, where p_1, \dots, p_r are distinct prime numbers, the exponents a_1, \dots, a_r are positive and $r \geq 2$. For every $i = 1, \dots, r$, we denote the p_i -Sylow subgroup (of order $p_i^{a_i}$) of G by S_i . We choose integers d_1, \dots, d_r such that

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

The following yields a formula for a norm one element for G in terms of norm one elements for the Sylow subgroups S_i .

LEMMA 5: If $x_1, \dots, x_r \in R$ satisfy $N_{S_i}(x_i) = 1$ for each $i = 1, \dots, r$, then $N_G(x_G) = 1$ for $x_G = d_1 x_1 + \cdots + d_r x_r$.

Proof: For each $i = 1, \dots, r$, let T_i be a set of representatives for cosets of S_i in G . We have

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

Consequently,

$$N_G(x_G) = N_G(d_1 x_1 + \cdots + d_r x_r) = d_1 n / p_1^{a_1} + \cdots + d_r n / p_r^{a_r} = 1. \quad \blacksquare$$

4. Some cohomological considerations

In the proof of Theorem 1 as given in Section 2, the computations take place in the co-induced module $B = \text{Hom}(\mathbf{Z}[G], R)$, and the elements $\varphi, \psi \in B$ play a central rôle. This can be explained through the following cohomological considerations.

We first claim that the existence of $x \in R$ such that $N_U(x) = 1$ implies the vanishing of the cohomology of the group U with coefficients in R in positive degrees: $H^i(U, R) = 0$ for all $i > 0$. Indeed, since U is cyclic with generator σ^{p^k} , we have

$$H^1(U, R) = \text{Ker}(N_U: R \rightarrow R) / (\sigma^{p^k} - 1)(R),$$

which is zero by Lemma 1. The surjectivity of $N_U: R \rightarrow R^U$ implies the vanishing of

$$H^2(U, R) = R^U / N_U(R).$$

Then the claim follows from the periodicity of the cohomology of cyclic groups.

In view of [4, Section VII.6] (or of Hochschild–Serre’s spectral sequence), the vanishing of $H^i(U, R) = 0$ for $i > 0$ implies that the inflation maps

$$\text{Inf}: H^*(G/U, R^U) \rightarrow H^*(G, R)$$

are isomorphisms.

Now consider the short exact sequence of $\mathbf{Z}[G]$ -modules

$$(11) \quad 0 \rightarrow R \rightarrow B \rightarrow C \rightarrow 0,$$

where $C = B/R$. Applying $H^*(U, -)$ to (11), we obtain a sequence of $\mathbf{Z}[G/U]$ -modules

$$(12) \quad 0 \rightarrow R^U \rightarrow B^U \rightarrow C^U \rightarrow 0,$$

which is exact because of the vanishing of $H^1(U, R)$. Observe that $B^U \cong \text{Hom}(\mathbf{Z}[G/U], R)$ is a co-induced module for G/U .

The naturality of the inflation maps gives rise to the commutative square

$$(13) \quad \begin{array}{ccc} H^1(G/U, C^U) & \xrightarrow{\text{Inf}} & H^1(G, C) \\ \delta \downarrow & & \delta \downarrow \\ H^2(G/U, R^U) & \xrightarrow{\text{Inf}} & H^2(G, R) \end{array}$$

where the vertical maps δ are connecting maps for the short exact sequences (11) and (12). We claim that all maps in the square (13) are isomorphisms. We

have already proved this for the lower inflation map. The connecting maps δ are isomorphisms because co-induced modules are cohomologically trivial. It follows that the upper inflation map is an isomorphism as well. Moreover, by [2, Theorem 1], the surjectivity of $N_U: R \rightarrow R^U$ implies the surjectivity of $N_G: R \rightarrow R^G$. Therefore, $H^2(G, R) = R^G/N_G(R) = 0$, which implies the vanishing of all cohomology groups in (13).

The central rôle played by the element $\varphi \in B^U$ in the proof of Theorem 1 follows from the following two facts:

(i) If $\bar{\varphi}$ denotes the class of φ in C , then by (4) it induces an element

$$[\bar{\varphi}] \in H^1(G/U, C^U) = \text{Ker}(N_{G/U}: C^U \rightarrow C^U)/(\sigma - 1)(C^U).$$

(ii) The image $\delta([\bar{\varphi}])$ of $[\bar{\varphi}]$ under the connecting map for the short exact sequence (12) is computed as follows: lift $\bar{\varphi}$ to $\varphi \in B^U$ and apply $N_{G/U}$. By (4) again, we obtain

$$\delta([\bar{\varphi}]) = 1 \in H^2(G/U, R^U) = R^G/N_{G/U}(R^U).$$

The existence of ψ satisfying (6) follows from the vanishing of

$$H^1(G, C) = \text{Ker}(N_G: C \rightarrow C)/(\sigma - 1)(C)$$

and Lemma 2 follows from the injectivity of $\text{Inf}: H^1(G/U, C^U) \rightarrow H^1(G, C)$.

References

- [1] E. Aljadeff, *On the surjectivity of some trace maps*, Israel Journal of Mathematics **86** (1994), 221–232.
- [2] E. Aljadeff and Y. Ginosar, *Induction from elementary abelian subgroups*, Journal of Algebra **179** (1996), 599–606.
- [3] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, 1956.
- [4] J.-P. Serre, *Corps locaux*, Publications de l'Université de Nancago, Hermann, Paris, 1962 (English translation: *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, New York, Berlin, 1979).