Algebra Seminar
Rutgers - 25 October 2002

Explicit norm one elements for ring actions of finite abelian groups

Christian Kassel

Institut de Recherche Mathématique Avancée
Strasbourg

Joint work with Eli Aljadeff (Technion, Haifa)

E. Aljadeff, C. Kassel, *Explicit norm one elements for ring actions of finite abelian groups*, preprint IRMA Strasbourg 2001/31, to appear in Israel J. Math.

www-irma.u-strasbg.fr/irma/publications/2001/00031.shtml

A simple-minded problem:

Let σ an automorphism σ of order 4 of a ring R and $x \in R$ such that

$$x + \sigma^2(x) = 1.$$

Find $y \in R$ such that

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

Answer: $y = x\sigma(x)$. Indeed, we have

$$\begin{aligned}
y + \sigma(y) + \sigma^2(y) + \sigma^3(y) = \\
&= x\sigma(x) + \sigma(x)\sigma^2(x) + \sigma^2(x)\sigma^3(x) + \sigma^3(x)x \\
&= x\sigma(x) + \sigma(x)(1 - x) \\
&\qquad + (1 - x)(1 - \sigma(x)) + (1 - \sigma(x))x \\
&= 1 + 2\big(x\sigma(x) - \sigma(x)x\big) \\
&= 1 \qquad \text{if } R \text{ is commutative.}
\end{aligned}$$

Surjectivity of the norm map:

Let G be a finite group acting on a ring R by ring automorphisms. The norm (sometimes called trace)

$N_G : R \to R^G$ (subring of invariant elements)

is defined for all $x \in R$ by

$$N_G(x) = \sum_{g \in G} g(x).$$

Question: When is $N_G : R \to R^G$ surjective?

• If $\mathrm{card}(G)$ is invertible in R (*e. g.*, $R \supset \mathbf{Q}$).

• Let L be a finite Galois extension of a number field K ($\supset \mathbf{Q}$) with Galois group G.

$$\begin{array}{ccccl} L & \supset & \mathcal{O}_L & & \text{(ring of algebraic integers in } L\text{)} \\ \uparrow & & \uparrow & & \\ K & \supset & \mathcal{O}_K & & \text{(ring of algebraic integers in } K\text{)} \end{array}$$

The group G acts on $\mathcal{O}_L$ and $\mathcal{O}_L^G = \mathcal{O}_K$. The norm $N_G : \mathcal{O}_L \to \mathcal{O}_L^G = \mathcal{O}_K$ is surjective if and only if the extension L/K is "tame".

A theorem by Aljadeff and Ginosar (1994):

Theorem. *$N_G : R \to R^G$ is surjective if and only if $N_U : R \to R^U$ is surjective for any elementary abelian subgroup U of G.*

• U is *elementary abelian* if $U \cong \mathbf{Z}/p \times \ldots \times \mathbf{Z}/p$ for some prime p

• Aljadeff (1992): If R is *commutative*, one may replace "elementary abelian subgroup" by "cyclic subgroup of prime order" ($\cong \mathbf{Z}/p$ for some prime p) in previous theorem.

Counterexample. The group $G = \mathbf{Z}/2\langle\sigma\rangle \times \mathbf{Z}/2\langle\tau\rangle$ acts on $R = M_2(\mathbf{F}_2(X))$ such that, for any $U \cong \mathbf{Z}/2 \subset G$, $N_U : R \to R^U$ is surjective, but $N_G : R \to R^G$ is not surjective.

The action is given by

$$\sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & cX \\ b/X & a \end{pmatrix}$$

$$\tau \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{(c+d)X+(a+b)}{X+1} & \frac{(a+cX)X+(b+dX)}{X+1} \\ \frac{a+b+c+d}{X+1} & \frac{(a+c)X+(b+d)}{X+1} \end{pmatrix}$$

An effective version of the surjectivity problem:

- The norm map is R^G-linear:

$$N_G(xy) = xN_G(y) \quad \text{if } x \in R^G \text{ and } y \in R.$$

Hence,

$N_G : R \to R^G$ surjective $\Leftrightarrow \exists\, x_G \in R$ with $N_G(x_G) = 1$.

- By Aljadeff-Ginosar's theorem

$$\exists\, x_G \in R : N_G(x_G) = 1 \Leftrightarrow \exists\, x_U \in R : N_U(x_U) = 1$$

for any elementary abelian subgroup U of G.

Problem: Given a family $(x_U)_U$ such that $N_U(x_U) = 1$ for any elementary abelian subgroup U of G, find $x_G \in R$ such that $N_G(x_G) = 1$.

What was known about the problem:

- In 1992 Aljadeff gave a formula for x_G when R is *commutative.*

- When R is not commutative, not much was known:

(a) Shelah: there is always a formula $x_G = F(g(x_U))$ where F is a noncommutative polynomial with integer coefficients in the variables $g(x_U)$.

(b) Problem solved by Aljadeff-Ginosar when R is a noncommutative $\mathbf{F}_2$-algebra and G is an abelian 2-group

(c) For an arbitrary noncommutative ring R and the group $G = \mathbf{Z}/4$ Péter P. Pálfy gave the formula

$$x_G = x_U \sigma(x_U) + x_U \sigma(x_U) x_U - x_U^2 \sigma(x_U). \qquad (1)$$

Remark: When R is commutative, we can take

$$x_G = x_U \sigma(x_U). \qquad (2)$$

The difference between (1) and (2) shows that the non-commutative case is much more difficult.

Our results:

We solved the problem for *noncommutative* rings when G is any *abelian* group.

Three steps in our proof:

(a) $G = \mathbf{Z}/p^n$ with p prime number and $n \geq 2$

(b) From cyclic p-groups to abelian p-groups

(c) From abelian p-groups to arbitrary abelian groups

The difficulty lies in Step (a).

Plan of lecture:

- Theorem for $G = \mathbf{Z}/p^n$

- Idea of proof in the p-cyclic case

- How to deduce the general case from the p-cyclic case

Our formula for $G = \mathbf{Z}/9$:

For a ring automorphism σ of order 9 of the ring R and an element $x \in R$ such that

$$x + \sigma^3(x) + \sigma^6(x) = 1,$$

we have

$$\sum_{i=0}^{8} \sigma^i(y) = 1$$

for

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

(RHS has 22 monomials)

The case of cyclic p-groups

• $G = \mathbf{Z}/p^n$ with generator σ (p prime number)

• $U \cong \mathbf{Z}/p^{n-k} \subset G$ generated by σ^{p^k}, where n, k are integers such that $n \geq 2$ and $1 \leq k \leq n/2$, *i. e.*,

$$\mathrm{card}(U) \geq \sqrt{\mathrm{card}(G)}.$$

Theorem 1.— *Let $x \in R$ satisfy $N_U(x) = 1$. Define z, $w_1, \ldots, w_{p^{n-k}-1}$, and $a \in R$ by*

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

$$w_i = \left(1 + \sigma^{p^k} + \sigma^{2p^k} + \cdots + \sigma^{(i-1)p^k}\right)\left(x\sigma^{-ip^k}(z)\right),$$

$$a = p^{n-2k}x + (1 - \sigma)\left(\sum_{i=1}^{p^{n-k}-1} w_i\right),$$

and $y = ax$. Then $N_G(y) = 1$.

Idea of proof of Theorem 1

1. *Natural idea:* Follow the proof of Aljadeff-Ginosar's theorem and make each step explicit.

• Aljadeff-Ginosar's proof relies on the following result by Chouinard (1976):

A finitely generated $R[G]$-module is projective if and only if it is projective as a $R[U]$-module for every elementary abelian subgroup U of G.

• Chouinard's theorem relies on the following result by Serre (1965). Denote

$$\beta : H^1(G, \mathbf{Z}/p) \to H^2(G, \mathbf{Z}/p) \quad \text{(Bockstein)}$$

the boundary map in the long exact cohomology sequence associated to the short exact sequence of trivial G-modules $0 \to \mathbf{Z}/p \to \mathbf{Z}/p^2 \to \mathbf{Z}/p \to 0$.

If G is a p-group that is not *elementary abelian, there exist nonzero $x_1, \ldots, x_k \in H^1(G, \mathbf{Z}/p)$ such that*

$$\beta(x_1) \cup \cdots \cup \beta(x_k) = 0 \in H^{2k}(G, \mathbf{Z}/p).$$

If G is an elementary abelian p-group, then the vector space $\beta(H^1(G, \mathbf{Z}/p))$ generates a polynomial algebra (without zero-divisors) in $H^{**}(G, \mathbf{Z}/p)$.

2. Our actual proof is based on two facts:

- A general fact inspired from Proposition XII.1.3 in Cartan-Eilenberg's book "Homological algebra"

- The explicit computation of the cohomology groups of a cyclic group

Lemma 1. *Let U be a finite group acting on a ring R. If $\exists\, x \in R$ satisfying $N_U(x) = 1$, then every element $z \in R$ such that $N_U(z) = 0$ can be written as*

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

Proof.

$$\begin{aligned} \text{RHS} &= \sum_{g \in U} g(x)\, g\big(g^{-1}(z)\big) - \sum_{g \in U} xg^{-1}(z) \\ &= N_U(x)\, z - x\, N_U(z) = z. \end{aligned}$$

Corollary 1. *If U is cyclic and $N_U : R \to R^U$ is surjective, then $H^q(U, R) = 0$ for all $q > 0$.*

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

$$H^1(U, R) = \text{Ker } N_U / I_U(R)$$

where $I_U(R) \subset R$ is spanned by $(g - 1)R$ $(g \in R)$.

New idea: Replace surjectivity of the norm, *i. e.*, vanishing of $H^2(-, R)$, by vanishing of some H^1 using cohomological exact sequence.

Embed R into the co-induced G-module

$$B = \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], R)$$

by $x \mapsto (\varphi_x : g \mapsto g(x))$. The group G acts on B by $(g\varphi)(s) = \varphi(sg)$ for $g, s \in G$ and $\varphi \in B$. We have

$$H^i(G, B) = 0 \quad (i > 0).$$

Define G-module C by short exact sequence

$$0 \to R \to B \to C \to 0. \tag{3}$$

The boundary map $\delta : H^1(G, C) \to H^2(G, R)$ is an isomorphism.

Applying $H^*(U, -)$ to (3) yields an exact sequence of $\mathbf{Z}[G/U]$-modules

$$0 \to R^U \to B^U \to C^U \to H^1(U, R) = 0. \tag{4}$$

$B^U \cong \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G/U], R)$ is a co-induced G/U-module. Hence $H^i(G/U, B^U) = 0$ for $i > 0$ and boundary map $\delta : H^1(G/U, C^U) \to H^2(G/U, R^U)$ is an isomorphism.

Commutative square

$$\begin{array}{ccc} H^1(G/U, C^U) & \xrightarrow{\text{Inf}} & H^1(G, C) \\ \delta \downarrow \cong & & \delta \downarrow \cong \\ H^2(G/U, R^U) & \xrightarrow[\text{Inf}]{\cong} & H^2(G, R) \end{array} \qquad (5)$$

• "Inflation maps" Inf : $E_2^{n0} \to H^n(G, M)$ come up in Hochschild-Serre's spectral sequences

$$E_2^{pq} = H^p(G/U, H^q(U, M)) \Longrightarrow H^*(G, M).$$

$H^q(U, R) = 0$ for all $q > 0$ (Cor. 1) implies that Inf : $H^2(G/U, R^U) \to H^2(G, R)$ is an isomorphism.

• All groups in (5) vanish: they are isomorphic to $H^2(G, R) = R^G/N_G(R)$, which is zero by Aljadeff-Ginosar's theorem. We now work in

$$H^1(G/U, C^U) = \text{Ker}(N_{G/U} : C^U \to C^U)/(\sigma - 1)(C^U).$$

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

defines $\varphi \in B^U$ with $N_{G/U}(\varphi) = 1$. Its image $\bar{\varphi}$ in C^U induces an element $[\bar{\varphi}]$ in $H^1(G/U, C^U)$.

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

Proof. Lift $\bar{\varphi}$ to $\varphi \in B^U$ and apply $N_{G/U}$.

From cyclic p-groups to abelian p-groups

- G abelian p-group (p prime number)
- $G = G_0 \times G_1$ with G_1 cyclic of order p^n $(n \geq 2)$
- $U = G_0 \times U_1$ with $U_1 \subset G_1$ cyclic of order p

- If $x_U \in R$ such that $N_U(x_U) = 1$, then

$$N_{U_1}\big(N_{G_0}(x_U)\big) = N_U(x_U) = 1.$$

- By repeated use of Theorem 1, we get $x_{G_1} \in R$ (explicit in terms of $N_{G_0}(x_U)$) with $N_{G_1}(x_{G_1}) = 1$.

- Set $x_G = x_{G_1} N_{U_1}(x_U)$. Then $N_G(x_G) = 1$.

From abelian p-groups to general abelian groups

- G finite abelian group of order $n = p_1^{a_1} \dots p_r^{a_r}$ $(r \geq 2)$
- S_i the Sylow subgroup of G of order $p_i^{a_i}$
- $d_1, \dots, d_r$ such that $d_1 n/p_1^{a_1} + \cdots + d_r n/p_r^{a_r} = 1$

Lemma 2. *For $x_1, \dots, x_r \in R$ such that $N_{S_i}(x_i) = 1$ for each $i = 1, \dots, r$, set*

$$x_G = d_1 x_1 + \cdots + d_r x_r.$$

Then $N_G(x_G) = 1$.

References

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

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

• E. Aljadeff, C. Kassel, *Explicit norm one elements for ring actions of finite abelian groups*, preprint IRMA Strasbourg 2001/31, to appear in Israel J. Math.

www-irma.u-strasbg.fr/irma/publications/2001/00031.shtml

• L. G. Chouinard, *Projectivity and relative projectivity over group rings* J. Pure Appl. Algebra 7 (1976), 278–302.

• J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology 3 (1965), 413–420.