Rend. Sem. Mat. Univ. Padova, Vol. 135 (2016), 251–258
DOI 10.4171/RSMUP/135-14

A simple construction for a class of p-groups with all of their automorphisms central

Andrea Caranti (*)

Abstract – We exhibit a simple construction, based on elementary linear algebra, for a class of examples of finite p-groups of nilpotence class 2 all of whose automorphisms are central.

Keywords. Finite p-groups, automorphisms, central automorphisms, endomorphisms.

Mathematics Subject Classification (2010). 20D15, 20D45.

1. Introduction

In June 2014, Marc van Leeuwen [18] inquired on Mathematics Stack Exchange whether there is a group P with an element $a \in P$ such that there is no automorphism of P taking a to its inverse.

In our answer, we noted that an example was provided by any of the many constructions in the literature [11, 13, 7, 10, 5, 1, 2, 16, 17] of finite p-groups of nilpotence class two in which all automorphisms are central, for p an odd prime. For, if P is such a group, and $a \in P \setminus Z(P)$, then an image of a under automorphisms is of the form az, with $z \in Z(P)$. If $az = a^{-1}$, then $a^2 \in Z(P)$, and thus $a \in Z(P)$, as p is odd.

Marc van Leeuwen commented that "indeed giving a concrete example is not so easy". This made us realize that examples of finite p-groups in which all automorphisms are central, although not conceptually difficult, usually rely on a fair amount of calculations with generators and relations. The goal of this paper is to give a class of examples of such groups for which calculations can be kept to a minimum, whereas a central role is played by linear algebra.

(*) *Indirizzo dell'A.*: Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Trento, Italy
E-mail: andrea.caranti@unitn.it

The examples are based on one of the cases of [1, Section 4]. They are constructed according to the linear algebra techniques employed in [11, 6, 1, 9], as described in [3], which we review in Section 2. The examples themselves are presented in Section 3, while in Section 4 we mention an extension to endomorphisms.

2. Preliminaries

Let P be a group. Since the centre $Z(P)$ is a characteristic subgroup of P, there is a natural morphism $\mathrm{Aut}(P) \to \mathrm{Aut}(P/Z(P))$ whose kernel $\mathrm{Aut}_c(P)$ consists of the central automorphisms of P, that is, those automorphisms of P that take every $a \in P$ to an element of $aZ(P)$.

We review the setup of [3]. Let V be a vector space of dimension $n+1$ over the field $\mathbf{F} = \mathrm{GF}(p)$, where p is a prime. Let $W = \Lambda^2 V$ be the exterior square of V. If $f \colon V \to W$ is a linear map, we will consider the group G of the elements of $\mathrm{GL}(V)$ that commute with f,

$$G = \{ g \in \mathrm{GL}(V) \colon (vg)f = (vf)\hat{g}, \text{ for all } v \in V \}, \tag{2.1}$$

where $\hat{g}$ is the automorphism of W induced by g. Note that we write maps on the right, so our vectors are row vectors.

Choose now a basis $v_0, v_1, \dots, v_n$ of V, and the corresponding basis $v_j \wedge v_k$ of W, for $j < k$. Write f in coordinates, that is,

$$v_i f = \sum_{j<k} a_{i,j,k} \cdot v_j \wedge v_k.$$

If p is odd, we can construct a finite p-group P via the following presentation

$$\begin{aligned} P = \Big\langle x_0, x_1, \dots, x_n \colon & [[x_i, x_j], x_k] = 1 \text{ for all } i, j, k, \\ & x_i^p = \prod_{j<k} [x_j, x_k]^{a_{i,j,k}} \text{ for all } i, \\ & [x_i, x_j]^p = 1 \text{ for all } i, j \Big\rangle. \end{aligned} \tag{2.2}$$

Note that here the third line of relations follows from the first two. In fact the first two lines of relations say that commutators and p-th powers of generators are central, so that we have $1 = [x_i^p, x_j] = [x_i, x_j]^p$, as x_i commutes with $[x_i, x_j]$.

Note that P is a group of nilpotence class two and order $|P| = p^{n+1+\binom{n+1}{2}}$, with $P' = \Phi(P) = Z(P)$ of order $p^{\binom{n+1}{2}}$, and P/P' of order p^{n+1}. Moreover P^p has order $p^{\dim(Vf)}$.

If $p = 2$, we appeal to an idea of Zurek [20], and modify (2.2), replacing p-th powers of generators with 4-th powers. The presentation thus becomes

$$P = \Big\langle x_0, x_1, \dots, x_n \colon [[x_i, x_j], x_k] = 1 \text{ for all } i, j, k, \\ x_i^4 = \prod_{j<k} [x_j, x_k]^{a_{i,j,k}} \text{ for all } i, \\ [x_i, x_j]^2 = 1 \text{ for all } i, j \Big\rangle.$$

Here we have $|P| = 2^{2(n+1)+\binom{n+1}{2}}$, P' has order $2^{\binom{n+1}{2}}$, P/P' has order $2^{2(n+1)}$, P^4 has order $2^{\dim(Vf)}$, and $P' \leq \Phi(P) = Z(P)$. This time, the relations $[x_i, x_j]^2 = 1$ are necessary.

Now it is shown in [3, Section 3] that the following result holds.

Theorem 2.1. *In the notation above,*

$$\mathrm{Aut}(P)/\,\mathrm{Aut}_c(P) \cong G.$$

The point of this, as explained in [3], is that for an automorphism g of $P/Z(P) = P/\Phi(P)$ to be induced by an automorphism of P, one needs g to preserve the p-th (respectively, 4-th) power relations, that is, the linear map f.

3. The examples

We will now construct a class of linear maps f, as in the previous section, for which the group G of (2.1) is $\{1\}$. According to Theorem 2.1, this will provide examples of finite p-groups P of nilpotence class 2 with $\mathrm{Aut}(P) = \mathrm{Aut}_c(P)$.

Let V be a vector space of dimension $n + 1 \geq 4$ over $\mathbf{F} = \mathrm{GF}(p)$, where p is a prime. (See Remark 3.4 for an explanation of the bound on the dimension.) Fix a basis $v_0, v_1, \dots, v_n$ of V, and let

$$U = \langle v_1, \dots, v_n \rangle.$$

On the exterior square $W = \Lambda^2 V$, consider a basis which begins with

$$v_0 \wedge v_1, v_0 \wedge v_2, \dots, v_0 \wedge v_n,$$

and continues with the $v_i \wedge v_j$, for $1 \leq i < j \leq n$.

We now make our choice for f.

Assumption 3.1. Consider the linear map $f\colon V \to W$ which, with respect to the given bases, has blockwise matrix

$$\begin{bmatrix} b & c \\ A & 0 \end{bmatrix}, \tag{3.1}$$

where b is a $1 \times n$ vector, c is a $1 \times \binom{n}{2}$ vector, A is an $n \times n$ matrix, and 0 is an $n \times \binom{n}{2}$ zero matrix. Moreover, we take

- $b, c \neq 0$, and
- A to be the companion matrix [12, p. 197] of the minimal polynomial m over $\mathbf{F}$ of a primitive element α of $\mathrm{GF}(p^n)$.

We collect a few elementary facts about the matrix A.

Lemma 3.2. *Let A be as in Assumption 3.1. Then the following hold:*

(1) *The roots of m, i.e. the eigenvalues of A, are*

$$\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}.$$

(2) *A has multiplicative order $p^n - 1$.*

(3) *$\mathbf{F}[A]$ is a field of order p^n, and $\mathbf{F}[A] = \{0\} \cup \{A^i : 0 \le i < p^n - 1\}$.*

(4) *$\mathbf{F}^n$ is a one-dimensional $\mathbf{F}[A]$-vector space.*

(5) *The centralizer*

$$C_{\mathrm{End}(\mathbf{F}^n)}(A)$$

of A in $\mathrm{End}(\mathbf{F}^n)$ is $\mathbf{F}[A]$.

Proof. (1) follows from the fact that α is a root of m, and m is irreducible in $\mathbf{F}[x]$, of degree n.

(2) follows immediately from the previous point.

(3) follows from $\mathbf{F}[A] \cong \mathbf{F}[x]/(m)$, and (2).

(4) follows from the fact that A is a companion matrix, and thus $\mathbf{F}^n$ is a cyclic $\mathbf{F}[A]$-module.

(5) now follows from the previous point, as the given centralizer is the ring of endomorphisms of the $\mathbf{F}[A]$-vector space $\mathbf{F}^n$. $\square$

We now collect a few facts about f and the group G of (2.1).

LEMMA 3.3. *Let f be as in Assumption 3.1, the group G as in (2.1), and U, V, W as in the notation above. Then the following hold*:

(1) *f is injective.*

(2) *$Uf = v_0 \wedge V = v_0 \wedge U$, and this is a subspace of W of dimension n.*

(3) *If $u \in U$ satisfies $u \wedge V \leq Vf$, then $u = 0$.*

(4) *$\langle v_0 \rangle = \{ x \in V : x \wedge V \leq Vf \}$.*

(5) *$\langle v_0 \rangle$ is left invariant by G.*

(6) *$U = \{ x \in V : xf \in v_0 \wedge V \}$.*

(7) *U is left invariant by G.*

PROOF. (1) follows from Assumption 3.1, since A is invertible, and $c \neq 0$ in (3.1).

The formula of (2) now follows from the shape of the matrix for f in Assumption 3.1.

To prove (3), let $u = c_1 v_1 + \cdots + c_n v_n$ satisfy $u \wedge V \leq Vf$. We will show that $c_1 = 0$, but a similar argument yields that all c_i have to be zero. Let us look at the coordinates of $u \wedge v_2$ and $u \wedge v_3$ with respect to $v_1 \wedge v_2$ and $v_1 \wedge v_3$, which yield the 2×2 matrix

$$\begin{bmatrix} c_1 & 0 \\ 0 & c_1 \end{bmatrix}.$$

By (1) and (2), the dimension of $Vf/Uf = Vf/(v_0 \wedge V)$ is 1. Thus this matrix must have rank at most 1, so that $c_1^2 = 0$.

To prove (4), let $0 \neq x \in V$ be such that $x \wedge V \leq Vf$. By (3), $x = cv_0 + u$, for some $c \neq 0$, and $u \in U$. But then by (2) $u \wedge V \leq Vf$, so that $u = 0$ again by (3).

(5) follows from the previous point.

(6) follows from (1) and (2), and implies (7), because of (5). □

REMARK 3.4. Note that the argument in the proof of (3) fails when $n = 2$, see [6], and this is the reason we have taken $n + 1 \geq 4$.

We can now state our main result.

THEOREM 3.5. *Let f be as in Assumption 3.1 and G as in (2.1). Then the group G is $\{ 1 \}$.*

PROOF. Items (5) and (7) of Lemma 3.3 allow us to write an element $g \in G$ in matrix form, with respect to the given basis of V, as

$$g = \begin{bmatrix} \gamma & 0 \\ 0 & \Delta \end{bmatrix},$$

where $\gamma \in \mathbf{F}^\star$ and $\Delta \in \mathrm{GL}(n, \mathbf{F})$. By the definition (2.1) of G, and Assumption 3.1, we have

$$\begin{bmatrix} \gamma & 0 \\ 0 & \Delta \end{bmatrix} \begin{bmatrix} b & c \\ A & 0 \end{bmatrix} = \begin{bmatrix} b & c \\ A & 0 \end{bmatrix} \begin{bmatrix} \gamma\Delta & 0 \\ 0 & \hat{\Delta} \end{bmatrix}, \tag{3.2}$$

where $\hat{\Delta}$ is the matrix induced by Δ on $U \wedge U$. We will only need to consider the following two consequences of (3.2):

$$\Delta A \Delta^{-1} = \gamma A, \tag{3.3}$$

and

$$b\Delta = b. \tag{3.4}$$

To deal with (3.3), we could appeal to [19], but prefer to give a simple direct argument. As noted in Lemma 3.2.(1), the eigenvalues of A are

$$\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}, \tag{3.5}$$

with α a primitive element, so that those of γA are

$$\gamma\alpha, \gamma\alpha^p, \dots, \gamma\alpha^{p^{n-1}}.$$

By (3.3) we have $\gamma\alpha = \alpha^{p^t}$ for some t. If $t > 0$, then

$$\alpha^{p^t - 1} = \gamma \in \mathrm{GF}(p)^\star,$$

with $p^t - 1 > 0$, so that the order

$$\frac{p^n - 1}{p - 1} = 1 + p + \cdots + p^{n-1}$$

of α in $\mathrm{GF}(p^n)^\star / \mathrm{GF}(p)^\star$ divides $p^t - 1 < p^{n-1}$, a contradiction. Thus $t = 0$ and $\gamma = 1$.

It follows that Δ is in the centralizer of A in $\mathrm{GL}(n, \mathbf{F})$, and thus, according to Lemma 3.2, Δ is a power of A.

But once more since the eigenvalues of A are as in (3.5), with α a primitive element, the only power of A to have an eigenvalue 1 is 1. Since we have (3.4), with $b \neq 0$ by Assumption 3.1, we obtain that $\Delta = 1$ and thus $G = \{1\}$ as claimed. ☐

4. Endomorphisms

The arguments of the previous section can be slightly extended to show that the set

$$G = \{ g \in \mathrm{End}(V) \colon (vg)f = (vf)\hat{g}, \text{ for all } v \in V \}$$

of the endomorphisms of V that commute with f consists of 0 and 1. Now in our examples P the centre $Z(P)$ is fully invariant, as it equals $\Phi(P)$. Thus an immediate extension of Theorem 2.1 yields that an endomorphism of P either maps P into $Z(P)$, or is a central automorphism, so that P is an E-group [8, 14, 15, 2, 4], that is, a group in which each element commutes with all of its images under endomorphisms.

To prove this, we proceed as in the previous section, except that we make no assumptions on γ and Δ. We have from (3.2)

$$\Delta A = \gamma A \Delta. \tag{4.1}$$

If $\gamma = 0$, then $\Delta = 0$. If $\gamma \neq 0$, it follows from (4.1) that $\ker(\Delta)$ is A-invariant, that is, a $\mathbf{F}[A]$-vector subspace of the one-dimensional $\mathbf{F}[A]$-vector space $\mathbf{F}^n$. Therefore we have either $\ker(\Delta) = \{0\}$, that is, Δ is invertible, and we proceed as above, or $\ker(\Delta) = \mathbf{F}^n$, that is, $\Delta = 0$. Now (3.2) yields $\gamma b = 0$, a contradiction to $\gamma \neq 0$ and $b \neq 0$.

Acknowledgements. The author gratefully acknowledges the support of the Department of Mathematics, University of Trento. The author is a member of GNSAGA–Indam.

References

[1] A. Caranti, *Automorphism groups of p-groups of class 2 and exponent p^2: a classification on 4 generators*, Ann. Mat. Pura Appl. (4) **134** (1983), pp. 93–146.

[2] A. Caranti, *Finite p-groups of exponent p^2 in which each element commutes with its endomorphic images*, J. Algebra **97** (1985), no. 1, pp. 1–13.

[3] A. Caranti, *A module-theoretic approach to abelian automorphism groups*, Israel J. Math. **205** (2015), 235–246.

[4] A. Caranti – S. Franciosi – F. de Giovanni, *Some examples of infinite groups in which each element commutes with its endomorphic images*, Group theory (Bressanone, 1986), Lecture Notes in Math., vol. 1281, Springer, Berlin, 1987, pp. 9–17.

[5] A. Caranti – P. Legovini, *On finite groups whose endomorphic images are characteristic subgroups*, Arch. Math. (Basel) **38** (1982), no. 5, pp. 388–390.

[6] G. Daues – H. Heineken, *Dualitäten und Gruppen der Ordnung p^6*, Geometriae Dedicata **4** (1975), no. 2/3/4, pp. 215–220.

[7] B. E. Earnley, *On finite groups whose group of automorphisms is abelian*, Ph. D. Thesis, Wayne State University, 1975, Dissertation Abstracts, V. 36, p. 2269 B.

[8] R. Faudree, *Groups in which each element commutes with its endomorphic images*, Proc. Amer. Math. Soc. **27** (1971), pp. 236–240.

[9] S. P. Glasby – P. P. Pálfy – C. Schneider, *p-groups with a unique proper non-trivial characteristic subgroup*, J. Algebra **348** (2011), pp. 85–109.

[10] H. Heineken, *Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch sind*, Arch. Math. (Basel) **33** (1979/80), no. 6, 497–503.

[11] H. Heineken – H. Liebeck, *The occurrence of finite groups in the automorphism group of nilpotent groups of class* 2, Arch. Math. (Basel) **25** (1974), pp. 8–16.

[12] N. Jacobson, *Basic algebra.* Vol. **I**, 2^{nd} ed., W. H. Freeman and Company, New York, 1985.

[13] D. Jonah – M. Konvisser, *Some non-abelian p-groups with abelian automorphism groups*, Arch. Math. (Basel) **26** (1975), pp. 131–133.

[14] J. J. Malone, *More on groups in which each element commutes with its endomorphic images*, Proc. Amer. Math. Soc. **65** (1977), no. 2, pp. 209–214.

[15] J. J. Malone, *A nonabelian 2-group whose endomorphisms generate a ring, and other examples of E-groups*, Proc. Edinburgh Math. Soc. (2) **23** (1980), no. 1, pp. 57–59.

[16] M. Morigi, *On p-groups with abelian automorphism group*, Rend. Sem. Mat. Univ. Padova **92** (1994), pp. 47–58.

[17] J. J. Malone, *On the minimal number of generators of finite non-abelian p-groups having an abelian automorphism group*, Comm. Algebra **23** (1995), no. 6, pp. 2045–2065.

[18] M. van Leeuwen, *Can a group have a subset that is stable under all automorphisms, but not under inverse*?, Mathematics StackExchange, June 2014. http://math.stackexchange.com/q/834082

[19] G. E. Wall, *Conjugacy classes in projective and special linear groups*, Bull. Austral. Math. Soc. **22** (1980), no. 3, pp. 339–364.

[20] G. Zurek, *A comment on a work by H. Heineken and H. Liebeck*: *"The occurrence of finite groups in the automorphism group of nilpotent groups of class* 2*"* [Arch. Math. (Basel) **25** (1974), 8–16; MR **50** #2337], Arch. Math. (Basel) **38** (1982), no. 3, pp. 206–207.

Manoscritto pervenuto in redazione l'8 luglio 2014.