BULL. AUSTRAL. MATH. SOC. 20D30, 20E15
VOL. 68 (2003) [141–153]

SOME FINITE SOLVABLE GROUPS WITH NON-TRIVIAL LATTICE ENDOMORPHISMS

S.E. STONEHEWER AND G. ZACHER

The main purpose of this paper is to exhibit a doubly-infinite family of examples which are extensions of a p-group by a cyclic p'-group, with the action satisfying some conditions of Zappa (1951), arising from his study of dual-standard (meet-distributive) subgroups. The examples show that Zappa's conditions do not bound the nilpotency class (or even the derived length) of the p-group. The key to this work is found in closely related conditions of Hartley (published here for the first time). The examples use some exceptional relationships between primes.

1. INTRODUCTION

In a group G the map $X \mapsto X \cap D$ defines a subgroup-lattice endomorphism as soon as D is a *meet-distributive* (*dual-standard*) subgroup of G, that is, $\langle X \cap D, Y \cap D\rangle = \langle X, Y\rangle \cap D$ for all subgroups X, Y of G. The dual-standard subgroups in finite groups have been characterised by Zappa [**12**] (see also [**11**, Theorem 11 in Section 7 of Chapter III]); he proves the following result.

THEOREM. *Let D be a dual-standard subgroup of a finite group G. Then D is normal in G and there are Hall subgroups M, H, L of G with H nilpotent, such that G is a split extension of $M \times L$ by H, $L \leqslant D \leqslant HL$ and $\pi(HL/D) = \pi(D/L)$. Also the Sylow subgroups of H are cyclic or generalised quaternion.*

Here $\pi(G)$ denotes the set of primes dividing the order of G. Further details are given in [**10**], where it is proved that the commutator subgroup $[H, L]$ is nilpotent. In this connection the action of a p'-group Q on a p-group P (H and L respectively in Zappa's Theorem) becomes relevant when there is a subgroup Q_1 of Q such that

(Z1) for $X \leqslant P$, Q_1 normalises X implies that Q normalises X; and
(Z2) $C_P(Q) = C_P(Q_1)$.

Here $C_P(Q)$ is the centraliser of Q in P. We refer to (Z1) and (Z2) by saying that *the action of Q on P satisfies Zappa's conditions with respect to Q_1*. The following properties are closely related:

(H1) P has a Q-composition series

Received 13th January, 2003
The authors are grateful to CNR and MIUR for financial support during the preparation of this paper.

$$1 = P_0 \lhd P_1 \lhd P_2 \cdots \lhd P_r = P, \tag{1}$$

which is also a Q_1-composition series;

(H2) if V_i and V_j are composition factors of (1), then V_i and V_j are Q-isomorphic whenever they are Q_1-isomorphic; and

(H3) either $C_P(Q_1) = 1$ or $C_P(Q) \neq 1$.

We refer to (H1), (H2) and (H3) by saying that *the action of Q on P satisfies Hartley's conditions with respect to Q_1*.

In this context it is natural to ask if the nilpotency class or derived length of P is restricted by Zappa's conditions. In private communications in 1990, Brian Hartley showed that neither the class nor the derived length is bounded and, in order to do this, he introduced the conditions (H1), (H2) and (H3).

The present paper is divided in four sections. In the second we give Hartley's previously unpublished work, which is in two parts. Theorem 2.1 proves that Hartley's conditions imply Zappa's conditions when Q is Abelian. Then examples are constructed to show that Zappa's conditions do *not* imply the existence of a bound on the derived length of P, again when Q is Abelian. Section 3 deals with the relationship between Zappa's and Hartley's conditions, showing that in certain situations the former imply the latter. We also give more examples showing that (Z1) and (Z2) do not bound the nilpotency class of P. Finally in section 4 we give examples to show that Zappa's conditions do not imply Hartley's conditions in general.

We should point out that when Q is cyclic or generalised quaternion and Q_1 is not equal to 1 or Q and has order 2 if Q is not cyclic, then Zappa shows that (Z1) and (Z2) are necessary and sufficient for PQ_1 to be a dual-standard subgroup of PQ.

All groups considered here are finite.

2. Hartley's results

We note first of all that if (H1) and (H2) hold for a given Q-composition series of P, then, by the Jordan-Hölder Theorem, they hold for every composition series of P. In particular we may always assume that (1) is a refinement of a central series of P.

Theorem 2.1. (Hartley) *Let P be a p-group acted on by an Abelian p'-group Q and let Q_1 be a subgroup of Q. Then*

(i) *with respect to Q_1,* (H1) *and* (H2) *imply* (Z1).

Moreover

(ii) *if in addition* (H3) *holds, then* (Z2) *also holds.*

Proof: (i) Let P have order p^n. We may assume that $n \geqslant 2$ and we proceed by induction on n. Let X be a proper non-trivial subgroup of P and suppose that Q_1

normalises X. Then we have to show that Q normalises X. If $\Phi(P) \neq 1$, then, by induction, $X\Phi(P)$ is Q-invariant, and since

$$X \leqslant X^Q \leqslant X\Phi(P) \neq P,$$

again by induction it follows that X is Q-invariant. Thus we may assume that P is elementary Abelian.

Decompose P under the action of Q into its homogeneous components:

$$P = W_1 \oplus \cdots \oplus W_r.$$

By (H1) and (H2), the W_i here are also the homogeneous components for the action of Q_1. So there exists i such that $X \cap W_i \neq 0$. If $r > 1$, then, by induction, $X \cap W_i$ is Q-invariant. So factoring by $X \cap W_i$, we see, again by induction, that X is Q-invariant. Therefore we may assume that $r = 1$ and $X \leqslant P = W_1$.

Let $P = V_1 \oplus \cdots \oplus V_t$ be a decomposition into F_pQ-modules. (Here F_p is the field of p elements.) For $1 \leqslant i, j \leqslant t$, V_i and V_j are Q-isomorphic and so they are Q_1-isomorphic. By (H1), V_i and V_j are irreducible Q_1-modules. Let V_i have dimension m over F_p. Since Q is Abelian, it follows from [**3**, Proposition 8.2 on p. 154] that P has $(p^{mt} - 1)/(p^m - 1)$ irreducible F_pQ- as well as F_pQ_1-modules. But the first set is contained in the second, by (H1), hence the two sets coincide. Therefore X is Q-invariant.

(ii) Let $C_P(Q)$ have order p^β. We may assume that $\beta \geqslant 1$. Also β is the number of composition factors in a Q-composition series of P on which Q acts trivially. (This can be seen by choosing a Q-composition series of P through $C_P(Q)$ and arguing by induction on the order of P. If Q centralises a composition factor above $C_P(Q)$, then we may assume that it is P/P_{r-1} and $P_{r-1} = \Phi(P)$. But then Q centralises P.) Viewing such a series as a Q_1-composition series, it follows from (H2) that the number of trivial Q_1-composition factors cannot increase. Hence $C_P(Q_1) = C_P(Q)$. ∎

Before we come to the construction of examples showing that there is no bound on the derived length of P when Zappa's conditions are satisfied, we recall some known facts about faithful irreducible Q-modules V over F_p when Q is a cyclic q-group and q is a prime different from p. Let $Q = \langle \eta \rangle$ be a cyclic group of order q^e. Then $\dim V = |p \bmod q^e| = m$, say. If ε is a primitive q^e-th root of 1 in F_{p^m}, then the map

$$\eta^i : \nu \mapsto \nu\varepsilon^i$$

defines a faithful irreducible $\langle \varepsilon \rangle$-module structure on the vector space $V_\varepsilon = F_p[\varepsilon]$ with basis $B = \{\varepsilon, \varepsilon^p, \ldots, \varepsilon^{p^{m-1}}\}$. If ε' is another primitive q^e-th root of 1, then V_ε and $V_{\varepsilon'}$ are Q-isomorphic if and only if ε' belongs to B. The module V is Q-isomorphic to some V_ε.

We need a combinatorial result concerning finite fields.

LEMMA 2.2. *Let e be a positive integer and let p and q be primes such that*

$$|p \bmod q^e| = m, \text{ where } q^{e+1} \text{ divides } p^m - 1.$$

Then $F_{p^m}^*$ contains a subgroup Q_1 of order q^e. Let Γ be the Galois group of F_{p^m} over F_p. Suppose that r is a positive integer such that

$$(m+1)^{2(r-1)} < q^{e-1}(q-1)/(q^{e-1}+1) \quad \text{if } m \geqslant 2$$

and

$$2^{2(r-1)} < q-1 \quad \text{if } m = 1.$$

Then there exist generators $\lambda_1, \lambda_2, \ldots, \lambda_r$ of Q_1 such that the elements $\mu_{i_1}\mu_{i_2}\ldots\mu_{i_s}$, where $\{i_1, i_2, \ldots, i_s\}$ ranges over all subsets (including the empty set) of $\{1, 2, \ldots, r\}$ and each μ_j ranges over the Γ-orbit of λ_j, are all distinct.

PROOF: The Lemma is clear if $r = 1$. So suppose that $r \geqslant 2$ and that we have found $\lambda_1, \lambda_2, \ldots, \lambda_t$, $1 \leqslant t < r$. The number of elements $\mu_{i_1}\mu_{i_2}\ldots\mu_{i_s}$, with $\{i_1, i_2, \ldots, i_s\}$ a subset of $\{1, 2, \ldots, t\}$ and μ_j belonging to the Γ-orbit of λ_j, is at most

$$\sum_{s=0}^{t} \binom{t}{s} m^s = (1+m)^t.$$

If Λ_t is this set of products, then we need to choose $\lambda_{t+1} = \lambda$ of order q^e in Q_1, such that, for σ in Γ, we have $\lambda^\sigma \notin \Lambda_t\Lambda_t^{-1}$, or equivalently $\lambda \notin \Lambda_t\Lambda_t^{-1}$ (since $\Lambda_t\Lambda_t^{-1}$ is Γ-invariant), and for $1 \neq \sigma \in \Gamma$,

$$\lambda^\sigma\lambda^{-1} = \lambda^{p^i-1} \notin \Lambda_t\Lambda_t^{-1}$$

$0 \leqslant i \leqslant m-1$. Recall that q^e does not divide $p^{m-1}-1$. Thus raising to the power p^i-1 in $\langle\lambda\rangle$ is an endomorphism with kernel of order at most q^{e-1}. It follows that we must avoid at most $(m+1)^{2t}$ values for λ if $m = 1$ and at most $(m+1)^{2t} + q^{e-1}(m+1)^{2t}$ values if $m \geqslant 2$. Thus if $m = 1$, then the number to avoid is at most $2^{2(r-1)}$ and this is less than $q-1$ and therefore less that $q^e - q^{e-1}$. So we can choose a suitable λ. On the other hand, if $m \geqslant 2$, then we require

$$(m+1)^{2(r-1)} + q^{e-1}(m+1)^{2(r-1)} < q^{e-1}(q-1),$$

that is

$$(m+1)^{2(r-1)} < q^{e-1}(q-1)/(q^{e-1}+1),$$

which is the case. Again we can find λ. □

https://doi.org/10.1017/S0004972700037497 Published online by Cambridge University Press

Now let p, q be primes and let e be a positive integer. Assume that p has multiplicative order m modulo q^e and that q^n is the highest power of q dividing $p^m - 1$, with $n > e$. In the finite field $F = F_{p^m}$, let Q be the cyclic subgroup of F^* of order q^f, where $e < f \leqslant n$; and let Γ be the Galois group of F over F_p. We have $\Gamma = \langle\sigma\rangle$, where σ has order m. With this notation we can prove the following result.

THEOREM 2.3. (Hartley) *Let r be a positive integer such that*

$$(m+1)^{2(r-1)} < q^{e-1}(q-1)/(q^{e-1}+1) \quad \text{if } m \geqslant 2$$

and

$$2^{2(r-1)} < q-1 \quad \text{if } m = 1.$$

Then there exists a p-group P of nilpotency class r and derived length $\lceil \log_2(r+1) \rceil$, acted upon faithfully by Q, such that Zappa's conditions are satisfied with respect to the subgroup Q_1 of order q^e.

PROOF: By Lemma 2.2, we can find r generators $\lambda_1, \lambda_2, \ldots, \lambda_r$ in Q_1 such that the elements $\mu_{i_1}\mu_{i_2}\ldots\mu_{i_s}$, where $\{i_1, i_2, \ldots, i_s\}$ ranges over all subsets of $\{1, 2, \ldots, r\}$ and each μ_j ranges over the Γ-orbit of λ_j, are distinct.

Choose elements $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ in Q such that $\varepsilon_i^{q^{f-e}} = \lambda_i$ and let V_i be the faithful irreducible m-dimensional $\langle\lambda_i\rangle$-module given by the action $\nu \mapsto \nu\lambda_i$, whose eigenvalues are the elements μ_i in the Γ-orbit of λ_i. Thus for $i_1 < i_2 < \cdots < i_s$ in $\{1, 2, \ldots, r\}$, the eigenvalues of the Q_1-module

$$V_{i_1} \otimes \cdots \otimes V_{i_s}, \tag{2}$$

where a generator of Q_1 acts as multiplication on each V_i by λ_i, are the elements $\mu_{i_1}\mu_{i_2}\ldots\mu_{i_s}$. These are pairwise distinct, by Lemma 2.2. Consequently the module (2) splits into non-isomorphic irreducible Q_1-modules and, for different subsets of $\{1, 2, \ldots, r\}$, they have no common constituents.

Let $P = H(V)$ be the Hartley p-group constructed from $V = \{V_1, V_2, \ldots, V_r\}$ (see [**3**, pp. 197–203]). Then Q acts on P as multiplication on each V_i by ε_i. By [**3**, Theorem 12.8 on p. 202], the nilpotency class of P is r and the derived length is $\lceil \log_2(r+1) \rceil$. Under the action of Q, Hartley's conditions are satisfied with respect to Q_1. Therefore the result follows by Theorem 2.1. ∎

COROLLARY 2.4. *Let r be a positive integer and let q be a prime greater than $2^{2(r-1)}$. Let p be a prime such that q^2 divides $p-1$. Then there exists a p-group P of nilpotency class r and derived length $\lceil \log_2(r+1) \rceil$, acted on faithfully by a cyclic group Q of order q^2, such that Zappa's conditions are satisfied with respect to $Q_1 = Q^q$.*

https://doi.org/10.1017/S0004972700037497 Published online by Cambridge University Press

PROOF: Here $m = 1$ and $e = 1$. Note that by Dirichlet's Theorem, there are infinitely many primes p satisfying our hypotheses. □

Again with $e = 1$, Theorem 2.3 also shows that there exists a 2-group P, of class r and derived length $\lceil \log_2(r+1) \rceil$, acted upon faithfully by a cyclic group Q of order q^2 such that Zappa's conditions hold with respect to Q^q, provided q^2 divides $2^m - 1$ and $2(m+1)^{2(r-1)} < q - 1$, where m is the order of 2 modulo q and may be a proper divisor of $q - 1$.

Costantini has kindly pointed out to us that the existence of the prime q is closely related to the so-called Wieferich primes, that is, primes q such that q^2 divides $2^{q-1}-1$. The only Wieferich primes below 16.10^{12} are 1093 and 3511 ([1]). In our case we can take either of these values for q when $r = 1$.

3. When Zappa's conditions imply Hartley's conditions

The situation when P is elementary Abelian is easy to deal with.

LEMMA 3.1. *Let P be an elementary Abelian p-group on which a p'-group Q acts and let Q_1 be a subgroup of Q. Then with respect to Q_1, (Z1) implies (H1) and (H2).*

PROOF: Clearly (Z1) implies (H1). To show that (H2) holds, let

$$P = V_1 \oplus \cdots \oplus V_t$$

be a decomposition of P into irreducible Q-modules, therefore by (Z1) also irreducible Q_1-modules. Assume that for some $i \neq j$, $1 \leqslant i, j \leqslant t$, there exists a Q_1-isomorphism $\gamma : V_i \to V_j$ and let D_γ be the corresponding diagonal subgroup of $V_i \oplus V_j$. Since D_γ is Q_1-invariant, it follows from (Z1) that it is also Q-invariant. Thus

$$V_i \underset{Q}{\cong} (V_i \oplus V_j)/D_\gamma \underset{Q}{\cong} V_j,$$

that is V_i and V_j are Q-isomorphic. So (H2) holds. □

We shall see in the next section that Zappa's conditions do not imply Hartley's conditions in general. However, other cases where (Z1) does imply (H1) and (H2) are contained in our next results.

A p-group P is said to be *powerful* if p is odd and P/P^p is Abelian, or if $p = 2$ and P/P^4 is Abelian. We recall from [2, Chapter 2] that when P is powerful of exponent p^e, the Frattini series, defined by $P_0 = P$, $P_{i+1} = \Phi(P_i)$ for $i \geqslant 0$, is a central series of P of length e. Moreover, each term P_i is also powerful and

$$P_{i+1} = P_i^p = P^{p^{i+1}}.$$

https://doi.org/10.1017/S0004972700037497 Published online by Cambridge University Press

Also P has a *basis* $\{x_1, \ldots, x_d\}$ in the sense that each element of P can be expressed uniquely in the form $x_1^{r_1} \cdots x_d^{r_d}$. Here d is the minimal number of generators of P. (See [**2**, Exercise 9, Chapter 2].) By order considerations, the non-trivial elements of

$$\{x_1^{p^i}, \ldots, x_d^{p^i}\}$$

form a basis of P_i. Similarly $\{x_1P_i, \ldots, x_dP_i\}$ is a basis of P/P_i, for $1 \leqslant i \leqslant e$. For each j we have

$$\langle x_j \rangle \cap P_i = \langle x_j^{p^i} \rangle.$$

Also $y = x_1^{r_1} \ldots x_d^{r_d}$ implies $|x_i^{r_i}| \leqslant |y|$, by [**2**, Lemma 2.4, (ii)].

THEOREM 3.2. *Let P be a powerful p-group of exponent p^e and suppose that $\Omega(P/P_i)$ is Abelian for $1 \leqslant i \leqslant e$. Let Q be a p'-group acting on P and let Q_1 be a proper, non-trivial subgroup of Q. If* (Z1) *holds with respect to Q_1, then* (H1) *and* (H2) *also hold with respect to Q_1.*

PROOF: As always, (Z1) implies (H1). Thus suppose that (H2) does not hold and let P be a counterexample of minimal exponent p^e. By Lemma 3.1, $e \geqslant 2$. Let

$$1 = X_r \lhd X_{r-1} \lhd \cdots \lhd X_1 \lhd X_0 = P$$

be a Q-composition series of P that refines the Frattini series. By choice of P, (H2) follows for P_i and for P/P_i, for $1 \leqslant i \leqslant e-1$. Hence there are i and j, with $P_1 \leqslant X_i$ and $X_j \leqslant P_{e-1}$, such that X_{i-1}/X_i and X_j/X_{j+1} are Q_1-isomorphic, but not Q-isomorphic. Since P/P_1 and P_{e-1} are completely reducible Q-modules, without loss of generality we may assume that $X_i = P_1$ and $j = r-1$.

Write $M = X_{i-1}$. Then M/P_1 is Q-irreducible. Let yP_1 be any non-trivial element of M/P_1. Let $\{x_1, \ldots, x_d\}$ be a basis of P and let $y = x_1^{r_1} \ldots x_d^{r_d}$. Since $x_i^{r_i} \in P_1$ if p divides r_i, we may (without changing yP_1) assume that

$$y = x_{i_1}^{s_1} \cdots x_{i_k}^{s_k},$$

where p does not divide s_i, $1 \leqslant i \leqslant k$. We distinguish two cases.

CASE 1. *Suppose that y has order p^s, where $s \geqslant 2$.* The map $x \mapsto x^p$ induces a Q-epimorphism $\sigma : P/P_1 \to P_1/P_2$, by [**2**, Lemma 2.4 (ii)]. Thus

$$(yP_1)^\sigma = x_{i_1}^{ps_1} \cdots x_{i_k}^{ps_k} P_2 \neq P_2. \tag{3}$$

For, those elements $x_{i_j}^{ps_j}$, which are non-trivial, are (modulo P_2) part of a basis of P_1/P_2, as we observed above. They cannot all be trivial, otherwise y has order p, which is not the case. Therefore (3) is true. Denoting the kernel of σ by K/P_1, it follows that $K \cap M = P_1$. Thus M/P_1 is Q-isomorphic to a Q-composition factor lying between P_1 and P_2, which is a contradiction.

https://doi.org/10.1017/S0004972700037497 Published online by Cambridge University Press

CASE 2. *Suppose that y has order p.* Here y belongs to $\Omega(P)$, which is Abelian by hypothesis. Let $T = P_1 \cap \Omega(P)$ and let $\Omega(P) = K \oplus T$ be a Q-decomposition. Now

$$M/P_1 \leqslant \Omega(P)P_1/P_1 \underset{Q}{\cong} \Omega(P)/T \underset{Q}{\cong} K.$$

Hence M/P_1 is Q-isomorphic to some Q-invariant subgroup B of K. Then B and P_{e-1} are Q_1-isomorphic, hence also Q-isomorphic, by Lemma 3.1. Thus M/P_1 and P_{e-1} are Q-isomorphic, a contradiction. □

COROLLARY 3.3. *Let P be a p-group acted on by a p'-group Q and let Q_1 be a proper, non-trivial subgroup of Q. If* (Z1) *holds with respect to Q_1, then* (H1) *and* (H2) *hold with respect to Q_1 whenever P satisfies one of the following conditions:*

(i) *P is a powerful group with a homogeneous basis $\{x_1, \ldots, x_d\}$, that is, x_i and x_j have the same order for all i, j;*

(ii) *P is a modular group.*

PROOF: (i) By Theorem 3.2, it suffices to show that $\Omega(P/P_i)$ is Abelian for all i. Thus suppose that this is not the case and let P be a counterexample of minimal exponent p^e. Clearly $e \geqslant 2$. For each $i < e$, P/P_i also has a homogeneuos basis and exponent p^i. Hence $\Omega(P/P_i)$ is Abelian, by choice of P. Thus $\Omega(P)$ is not Abelian. Note that if y has order p, then $y = x_1^{r_1} \cdots x_d^{r_d}$ and $x_i^{r_i} = 1$ or p, as we observed above. Therefore $\Omega(P) = P_{e-1} = \langle x_1^{p^{e-1}}, \ldots, x_d^{p^{e-1}} \rangle$ is Abelian. a contradiction.

(ii) Now we suppose that P is modular. Then $\Omega(P/P_i)$ is Abelian for all i, and it follows from Iwasawa's structure theorem (see [**9**, Theorem 2.3.1]) that if P is not Hamiltonian, then P is powerful. Thus Theorem 3.2 applies. On the other hand, if P is Hamiltonian, then P' has order 2 and P/P' is elementary Abelian. Thus P' is centralised by Q and so Lemma 3.1 applies. □

REMARK. In [**6**] it is shown that a p-group P is modular and non-Hamiltonian if and only if every subgroup of P is powerful.

As applications of these results, we construct classes of p-groups P, acted upon by p'-groups Q, in which Hartley's conditions are satisfied with respect to some proper, non-trivial subgroup Q_1 of Q.

EXAMPLE 3.4. Let P be a special p-group (see [**4**, Kapitel 3, Section 13]), and let Q be a p'-group acting on P. Let Q_1 be a proper, non-trivial subgroup of Q. Suppose that (Z1) and (Z2) hold with respect to Q_1 and suppose also that $C_P(Q) \geqslant Z(P)$ if $P' \neq 1$. Then, by Lemma 3.1, all of Hartley's conditions hold. When p is odd, P here is certainly powerful, but the hypothesis of Theorem 3.2 may not be satisfied. When $p = 2$, then P may not be powerful, but $C_P(Q) \geqslant Z(P)$ when P is extraspecial.

Finally we show that the nilpotency class of P is not restricted in these situations.

EXAMPLE 3.5. Let p be a prime $\geqslant 5$ and let A be an Abelian p-group of exponent p^m, $m \geqslant 2$. Consider the group Π of power automorphisms of A. So Π is cyclic, generated by α, say, and

$$\langle\alpha\rangle \cong C_{p^{m-1}} \times C_{p-1}.$$

Let P be the split extension of A by $\langle\alpha\rangle_p$ and let Q be the p'-component of $\langle\alpha\rangle$. With Q_1 a proper, non-trivial subgroup of Q, one sees easily that when Q acts on P, (Z1) and (Z2) are satisfied with respect to Q_1. So Theorem 3.2 applies.

4. EXAMPLES WHERE ZAPPA'S CONDITIONS DO NOT IMPLY HARTLEY'S CONDITIONS

Let p be a prime and let n and c be integers $\geqslant 2$. Then let P be a relatively free p-group of exponent p, rank n and class c. So $P' = \Phi(P)$ and $|P : \Phi(P)| = p^n$. Moreover, given a p'-automorphism of P/P', it can be lifted to an automorphism η of P of the same order ([8]). Let $Q = \langle\eta\rangle$ and suppose that Q has order q^m, where $m > 1$ and q is a prime different from p. Assume that $V_1 = P/P'$ is a faithful irreducible Q-module, so that F_{p^n} is a splitting field over F_p of the polynomial $x^{q^m} - 1$. For some primitive q^mth root ε of 1 in F_{p^n}, we have $V_1 \underset{Q}{\cong} V_\varepsilon$. Since the p^ith powers of ε (i going from 1 to $n-1$) form a basis of V_ε, it follows that there are $q^{m-1}(q-1)/n$ distinct faithful irreducible Q-modules. If we set $Q_1 = \langle\eta^q\rangle$, then V_1 is also a faithful Q_1-module and it is irreducible if and only if p has order n modulo q^{m-1}.

Let $P = \gamma_1(P) > \gamma_2(P) > \gamma_3(P) > \cdots$ be the lower central series of P. Then $V_i = \gamma_i(P)/\gamma_{i+1}(P)$ is an F_pQ- as well as an F_pQ_1-module. The map γ from $V_1 \times V_i$ to V_{i+1} defined by

$$\gamma : \big(x\gamma_2(P), y\gamma_{i+1}(P)\big) \mapsto [x, y]\gamma_{i+2}(P)$$

is $\mathbb{Z}$-bilinear ([5, p. 286]). Hence there exists an epimorphism γ' from $V_1 \otimes V_i$ to V_{i+1} mapping $\nu \otimes \nu_i$ to $(\nu, \nu_i)^\gamma$. We apply this construction in the next result.

PROPOSITION 4.1. *Let p be an odd prime and let P be a 2-generator relatively free p-group of exponent p and nilpotency class 3. Let $Q = \langle\eta\rangle$ be a group of automorphisms of P of order q^2, where q is a prime different from p. If P/P' is a faithful irreducible Q-module as well as an irreducible $\langle\eta^q\rangle$-module, then P satisfies Hartley's conditions with respect to $Q_1 = \langle\eta^q\rangle$. Also q is odd.*

PROOF: We have $P' = \Phi(P) > Z(P) > 1$. Here, in the above notation, $n = 2$, the dimension of V_2 is 1 and the dimension of V_3 is 2. By assumption $|p \bmod q^2| = |p \bmod q| = 2$. It follows that q^2 divides $p^2 - 1$ and q does not divide $p - 1$. Hence q^2 divides $p + 1$. Also q must be odd.

Both $V_1 \otimes V_2$ and V_3 have dimension 2. Hence $\gamma' : V_1 \otimes V_2 \to V_3$ is an isomorphism and since q does not divide $p - 1$, Q acts trivially on V_2. Therefore V_1 and V_3 are

isomorphic Q-modules. Then (H1) and (H2) hold. Since $C_P(Q)$ and $C_P(Q_1)$ are equal (of order p), (H3) also holds. □

Note that, by Theorem 2.1, Zappa's conditions also hold in the above situation.

In the remaining part of this paper we construct examples satisfying (Z1), (Z2), (H1) and (H3), but not (H2).

EXAMPLE 4.2. Let p and q be primes such that

$$n = |p \bmod q^2| = |p \bmod q| > 1.$$

Let P be a relatively free p-group of exponent p, class 2 and rank n. With $V_1 = P/P'$ and $V_2 = P'/1$, we know that there exists an epimorphism γ from $V_1 \otimes V_1$ to V_2, namely $(xP' \otimes yP') \mapsto [x, y]$, whose kernel is $W = \langle \nu \otimes \nu \mid \nu \in V_1 \rangle$. Thus

$$V_2 \cong (V_1 \otimes V_1)/W = V_1 \wedge V_1.$$

By choice of p and q, there exists an automorphism η of P of order q^2 such that, with $Q = \langle \eta \rangle$ and $Q_1 = \langle \eta^q \rangle$, V_1 is a faithful irreducible Q- as well as Q_1-module. Assume that $n = q - 1$, which means that there exists only one faithful irreducible Q_1-module. Suppose also that there is no solution of the congruence

$$p^j \equiv p^i + 1 \bmod q^2, \tag{4}$$

for non-negative integers i and j, with i not divisible by n. For example $q = 5$, $p = 7$ will do.

Choose a Q-invariant subgroup T of P' such that $V_3 = P'/T$ is a faithful irreducible Q-module. Let $V_1 \underset{Q}{\cong} V_\varepsilon$ for some primitive q^2th root ε of 1 in F_{p^n}. Then there exists t, with $0 < t < n/2$, such that with $s = p^t + 1$ and $\lambda = \varepsilon^s$, $V_\varepsilon \underset{Q}{\cong} V_\lambda$ ([7, p. 50]). Since the congruence relation (4) has no solution, V_1 and V_3 cannot be Q-isomorphic. It follows that the Q-group P/T does not satisfy condition (H2) with respect to Q_1. Since the only Q-invariant subgroups in the interval $[P/T]$ are P, P' and T, and since $C_{P/T}(Q) = C_{P/T}(Q_1) = 1$, Zappa's conditions are satisfied, while Hartley's condition (H2) fails to hold.

EXAMPLE 4.3. For our last example, take $p = 67$ and let P be a relatively free 3-generator p-group of exponent p and class 3. Let $Q = \langle \eta \rangle$ be a cyclic group of automorphisms of P of order q^2, with $q = 7$. Let $Q_1 = \langle \eta^7 \rangle$.

We have $|67 \bmod 7^2| = |67 \bmod 7| = 3$, P' is an elementary Abelian p-group, and with $V_1 = P/P'$, $V_2 = P'/Z(P)$ and $V_3 = Z(P)/1$, V_1 and V_2 have dimension 3, while V_3 has dimension 8 (over F_p). In $GL(V_1)$ we choose an element of order q^2, acting

irreducibly, and lift it to an automorphism η of P, still of order q^2. Then V_1 and V_2 are faithful irreducible Q- as well as Q_1-modules, and they are not isomorphic (see [7, p. 52]). For a suitable primitive q^2th root ε of 1 in F_{p^3}, we have

$$F_{p^3} = F_p[\varepsilon] = F_p[\varepsilon^q]$$

and V_1 and V_ε are Q-isomorphic, while with $\lambda = \varepsilon^q$, V_1 and V_λ are Q_1-isomorphic. To get the minimal polynomial of ε and λ in $F_p[x]$, we factorise $x^{49}-1$ and x^7-1 into irreducible components. Thus

$$\begin{aligned} x^{49}-1 = {} & (x-1)(x^3+13x^2+x-1)(x^3+11x^2+43x-1)(x^3+40x^2+33x-1) \\ & \times (x^3+7x^2+24x-1)(x^3+32x^2+62x-1)(x^3+66x^2+54x-1) \\ & \times (x^3+43x^2+60x-1)(x^3+24x^2+56x-1)(x^3+5x^2+35x-1) \\ & \times (x^3+45x^2+29x-1)(x^3+34x^2+27x-1)(x^3+7x^2+30x-1) \\ & \times (x^3+37x^2+60x-1)(x^3+38x^2+22x-1)(x^3+12x^2+11x-1) \\ & \times (x^3+56x^2+55x-1) \end{aligned}$$

and

$$x^7-1 = (x-1)(x^3+12x^2+11x-1)(x^3+56x^2+55x-1).$$

Let $f = x^3+13x^2+x-1$. Then a root ε of $f = f_\varepsilon$ in F_{p^3} has order 49. Choose an automorphism η of P of order 49 and with the F_pQ-module V_1 Q-isomorphic to V_ε. Then trace $(\eta \mid V_1) = -13$.

If x_1 is a free generator of P, then $\{x_1, x_2(=x_1^\eta), x_3(=x_2^\eta)\}$ is a basis of P and with $\nu_i = x_i P'$ (in V_1), we get $\nu_1^\eta = \nu_2 = \varepsilon\nu_1$, $\nu_2^\eta = \nu_3 = \varepsilon\nu_2$ and

$$\nu_3^\eta = (-13\varepsilon^2 - \varepsilon + 1)\nu_1 = \nu_1 - \nu_2 - 13\nu_3 = x_1 x_2^{-1} x_3^{-13} P'.$$

Let $w_1 = [x_1, x_2]Z(P)$, $w_2 = [x_2, x_3]Z(P)$, and $w_3 = [x_3, x_1]Z(P)$. Then $\{w_1, w_2, w_3\}$ is a basis of V_2 and we have $w_1^\eta = w_2$, $w_2^\eta = w_2 + w_3$ and $w_3^\eta = w_1 + 13w_2$. Therefore trace $(\eta \mid V_2) = 1$, while trace $(\eta^7 \mid V_1) = -12$ or -56. (Using the Girard-Newton formulas, the exact value can be calculated from f_ε.) Now, as F_pQ-module, V_3 is a proper Q-epimorphic image of $V_1 \otimes V_2$, since the dimension of $V_1 \otimes V_2$ is 9.

We have

$$\text{trace}\,(\eta \mid V_1 \otimes V_2) = \text{trace}\,(\eta \mid V_1) \times \text{trace}\,(\eta \mid V_2) = -13,$$

while

$$\text{trace}\,(\eta^7 \mid V_1 \otimes V_2) = \text{trace}\,(\eta^7 \mid V_1) \times \text{trace}\,(\eta^7 \mid V_2) = (-12)(-56) = 2,$$

since V_1 and V_2 are not Q_1-isomorphic. We conclude that the decomposition of V_3 into irreducible Q_1-modules is as follows:

$$V_3 = 2 \times 1 \oplus U_{-12} \oplus U_{-56}.$$

(The indices here denote the trace of η^7 on these modules.) It follows that the only possibilities for the decomposition of the Q-module V_3 into a sum of irreducible submodules are

$$2 \times 1 \oplus W_{-5} \oplus W_{-11}, \quad 2 \times 1 \oplus W_{-45} \oplus W_{-38}, \quad 2 \times 1 \oplus W_{-40} \oplus W_{-43},$$

where the W here are also faithful. From trace considerations, W is not Q-isomorphic to V_1 or V_2. Thus one of the above 3 decompositions must be $V_3 = 2 \times 1 \oplus W \oplus U$, with $W \underset{Q_1}{\cong} U_{-12}$ and $U \underset{Q_1}{\cong} U_{-56}$. Hence, while V_1 is not Q-isomorphic to W or U, V_1 is Q_1-isomorphic to W or U. Therefore condition (H2) is not satisfied.

To see that Zappa's conditions hold, let $N = 2 \times 1 \oplus U$ if $V_1 \underset{Q_1}{\cong} U_{-12}$ and let $N = 2 \times 1 \oplus W$ if $V_1 \underset{Q_1}{\cong} U_{-56}$. Then N is a normal Q-invariant subgroup of P. Also either $P'/N \underset{Q}{\cong} V_2 \oplus W$, $P'/N \underset{Q_1}{\cong} V_2 \oplus U_{-12}$ and $V_2 \underset{Q_1}{\cong} U_{-12}$ or $P'/N \underset{Q}{\cong} V_2 \oplus U$, $P'/N \underset{Q_1}{\cong} V_2 \oplus U_{-56}$ and $V_2 \underset{Q_1}{\cong} U_{-56}$. In the interval $[P/N]$, every Q- and Q_1-invariant subgroup different from P and P' is properly contained in $[P'/N]$, and this interval has exactly two Q_1-invariant subgroups, which are both Q-invariant. Hence Zappa's condition (Z1) is satisfied for P/N. Since $C_P(Q) = C_P(Q_1)$ is an elementary Abelian subgroup of order p^2 contained in N, condition (Z2) also holds for P/N. Thus finally we see that the Q-group P/N satisfies Zappa's, but not Hartley's conditions, with respect to Q_1.

References

[1] R. Crandall, C. Pomerance, *Prime numbers, a computational perspective* (Springer-Verlag, Berlin, 2001).

[2] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups*, London Mathematical Society Lecture Notes Series **157** (Cambridge University Press, Cambridge, 1991).

[3] K. Doerk and T.O. Hawkes, *Finite soluble groups* (de Gruyter, Berlin, New York, 1992).

[4] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[5] B. Huppert and N. Blackburn, *Finite groups II* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[6] A. Lubotzky and A. Mann, 'Powerful p-groups I, finite groups', *J. Algebra* **105** (1987), 484–505.

[7] S. Mattarei, *Retrieving information about a group from its character table*, (Ph.D. Thesis) (University of Warwick, Warwick, 1992).

[8] H. Neumann, *Varieties of groups* (Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[9] R. Schmidt, *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics **14** (de Gruyter, Berlin, New York, 1994).

[10] S.E. Stonehewer, G. Zacher, 'Dual-standard subgroups of finite and locally finite groups', *Manuscripta Math.* **70** (1991), 115–132.

[11] M. Suzuki, *Structure of a group and the structure of its lattice of subgroups* (Springer-Verlag, Berlin, Gottingen, Heidelberg, 1967).

[12] G. Zappa, 'Sulla condizione perché un emitrofismo inferiore tipico tra due gruppi sia un emotropismo', *Giorn. Mat. Battaglini* **80** (1951), 80–101.

Mathematics Institute
University of Warwick
Coventry CV4 7AL
England
Stewart@stonehewer.freeserve.co.uk

Dipartimento di Matematica Pura ed Applicata
Università di Padova
via Belzoni 7
35131 Padova
Italy
zacher@math.unipd.it

https://doi.org/10.1017/S0004972700037497 Published online by Cambridge University Press