BULL. AUSTRAL. MATH. SOC. 20D15
VOL. 12 (1975), 363-369.

Secretive prime-power groups of large rank

G.E. Wall

A question of L.G. Kovács, Joachim Neubüser, B.H. Neumann (*J. Austral. Math. Soc.* 12 (1971), 287-300) on the existence of 'secretive' prime-power groups of large rank is settled affirmatively by proving the following result: given a prime p and integer $d \geq 2$, there exists a finite p-group P with cyclic centre and minimal number of generators d and having the property that every element not in its Frattini subgroup has a non-trivial power in its centre.

1. Introduction

In their paper, [2], Kovács, Neubüser, Neumann introduce certain (finite) 'secretive' groups, which conspire to 'hide' primes. The reader is referred to the original paper for the precise definition. A general impression of what secretive groups are like may be gained from the following result.

(I) ([2], Theorem 5.2). *Let B be a finite, non-cyclic group. If B has a representation over the field of complex numbers such that no element outside the Frattini subgroup $\phi(B)$ has an eigenvalue 1, then B is secretive.*

In fact, for present applications, only the following special case is needed.

Received 23 December 1974. This paper was presented at the 366th Pure Mathematics Seminar at the Australian National University on 13 December 1974 as the last of a series of three to mark the retirement of Professor B.H. Neumann from the Chair and headship of the Department of Mathematics in the Institute of Advanced Studies of the Australian National University.

(II) ([2], Corollary 5.4). *Let B be a finite, non-cyclic group. If the centre $\zeta(B)$ is cyclic and if every element outside $\phi(B)$ has a non-identity power in $\zeta(B)$, then B is secretive.*

The minimum number of generators of a group G is called the *rank* of G and denoted by $d(G)$. For each prime p, Kovács, Neubüser, Neumann construct examples of secretive p-groups of rank 2; and they refer to the construction of a secretive 2-group of rank 3 by I.D. Macdonald. The purpose of the present paper is to settle the question, raised by the same authors, of the existence of secretive p-groups of larger rank. The following result will be proved.

THEOREM. *Let p be a prime and let d, m be integers such that 2 $d \leq p^m$. Then there is a finite p-group B of rank d and exponent p^{m+1} which satisfies the hypotheses of* (II).

The Theorem and (II) yield an immediate answer to the question posed above.

COROLLARY. *For each prime p and integer $d \geq 2$, there exists a (finite) secretive p-group of rank d.*

2. A preliminary reduction

We assume henceforth that p, m, d are as in the Theorem. If G is a finite p-group, let $\pi_m(G)$ denote the subgroup generated by the p^m-th powers of the elements of G.

We prove in this section that it is sufficient to construct a finite p-group P with the following two properties:

(2.1) $d(P) = d$;

(2.2) $\pi_m(P)$ *has a subgroup Q of index p which is normal in P and does not contain the p^m-th power of any element of P outside $\phi(P)$.*

This assertion is an immediate consequence of the following result.

LEMMA 1. *If the finite p-group P satisfies* (2.1) *and* (2.2) *but no* *proper quotient group of* P *does, then* P *satisfies the hypotheses of* (II).

Proof. It is evident that P/Q satisfies (2.1) and (2.2). Therefore, by the hypothesis of the Lemma, $Q = \{1\}$. Thus, $\pi_m(P)$ has order p and so is a subgroup of $\zeta(P)$. It now follows from (2.2) that every element of P outside $\phi(P)$ has a non-identity power (namely, the p^m-th) in $\zeta(P)$. Clearly, P has rank d and exponent p^{m+1}; and since $d \geq 2$, P is non-cyclic.

It remains to prove that $\zeta(P)$ is cyclic. If this were not the case, then $\zeta(P)$ would have a subgroup M of order p different from $\pi_m(P)$. By (2.2), $M \subseteq \phi(P)$. It is now easily verified that P/M satisfies (2.1) and (2.2), contrary to the hypothesis of the Lemma. Thus, $\zeta(P)$ is cyclic and the proof is complete.

3. Definite q-forms

Let F be the field of p elements. Let q be a positive integer (in Section 4, we shall take $q = p^m$). Let A be the associative algebra (with identity) over F obtained by adjoining to F non-commuting elements $a_1, \ldots, a_d$ such that the monomials in the a_i of total degree $\leq q$ are linearly independent while all monomials of degree $> q$ are zero. In the present section, we study q-th powers in A.

Let V_1 denote the subspace spanned by the a_i and V_q the subspace spanned by the q-th powers of the elements of V_1. Then we have the q-th power mapping

$$\mu : V_1 \to V_q , \quad \mu(a) = a^q .$$

By a *q-form* on V_1, we shall mean a function $f : V_1 \to F$ of the form

$$f\left(\sum_1^d \lambda_i a_i\right) = \sum_{i_1+\ldots+i_d=q} \omega_{i_1,\ldots,i_d} \lambda_1^{i_1} \ldots \lambda_d^{i_d} ,$$

or, in simpler notation,

https://doi.org/10.1017/S000497270002400X Published online by Cambridge University Press

(3.1) $$f(a) = \sum_{|\underline{\underline{i}}|=q} \omega_{\underline{\underline{i}}} \lambda^{\underline{\underline{i}}} ,$$

where $\omega_{\underline{\underline{i}}} \in F$.

LEMMA 2. *$f^* \mapsto f = f^* \circ \mu$ defines an isomorphism from the dual space of V_q to the space of q-forms on V_1 .*

Proof. Using the relations $\lambda_i^p = \lambda_i$, we may reduce each $\lambda^{\underline{\underline{i}}}$ in (3.1) to the form $\lambda^{\underline{\underline{j}}}$, where the index row $\underline{\underline{j}}$ is *reduced*; that is,

$$0 \le j_i \le p-1 \quad (i = 1, \ldots, d) .$$

Thus,

$$f(a) = \sum_{\underline{\underline{j}} \in S} \theta_{\underline{\underline{j}}} \lambda^{\underline{\underline{j}}}$$

for a certain set S of reduced index rows. Now, the monomial functions

$$f_{\underline{\underline{j}}}(a) = \lambda^{\underline{\underline{j}}}$$

corresponding to the p^d reduced index rows are linearly independent (indeed, they form a basis for the vector space of *all* functions $V_1 \to F$). It follows that

(3.2) $$f_{\underline{\underline{j}}} \quad (\underline{\underline{j}} \in S)$$

form a basis for the space of q-forms.

We have

$$\mu(a) = a^q = \sum_{|\underline{\underline{i}}|=q} a_{\underline{\underline{i}}} \lambda^{\underline{\underline{i}}} ,$$

where $a_{\underline{\underline{i}}}$ denotes the sum of all monomials in $a_1, \ldots, a_d$ having partial degree i_k in a_k for $k = 1, \ldots, d$. Applying the same kind of reduction as before, we see that

$$\mu(a) = \sum_{\underline{\underline{j}} \in S} A_{\underline{\underline{j}}} \lambda^{\underline{\underline{j}}} .$$

Since the functions (3.2) are linearly independent, it follows that

(3.3) $$A_{\underline{i}} \quad (\underline{i} \in S)$$

span V_q . However, these elements are clearly linearly independent and so from a basis of V_q .

Now that we have constructed explicit bases for V_q and the space of q-forms, the rest of the proof is plain sailing and may be omitted.

DEFINITION. The q-form f is called *definite* when $f(a) = 0$ implies $a = 0$.

LEMMA 3.[1] *If* $q \geq d$ *, there exists a definite* q*-form on* V_1 .

Proof. Let K be an extension field of F of degree q . Embed V_1 (in any way) as subspace of K . Then the norm mapping

$$f(a) = N_{K/F}(a) \quad \left(a \in V_1\right)$$

is a definite q-form.

4. Completion of proof

Consider again the algebra A of the previous section and let $\underline{a}$ denote the ideal of A generated by $a_1, \ldots, a_d$. If $u \in \underline{a}$, then $(1+u)^{p^t} = 1 + u^{p^t} = 1$ for sufficiently large t . Thus, $1 + \underline{a}$ is a (finite) p-group under multiplication. Let P be the subgroup generated by the elements $x_i = 1 + a_i \quad (i = 1, \ldots, d)$.

An element x of P is expressible in the form

(4.1) $$x = x_1^{\lambda_1} \ldots x_d^{\lambda_d} y$$

with y in the derived group, $\delta(P)$; and it is easily proved that

(4.2) $$x \equiv 1 + a \left(\bmod \underline{a}^2\right) ,$$

where $a = \lambda_1 a_1 + \ldots + \lambda_d a_d$. It follows from (4.2) that the integers λ_i in (4.1) are uniquely determined $(\bmod p)$. We conclude that

[1] A well known result of Chevalley, [1], shows, on the other hand, that there are *no* definite q-forms on V_1 when $q < d$.

https://doi.org/10.1017/S000497270002400X Published online by Cambridge University Press

$$(4.3) \qquad x \in \phi(P) \Leftrightarrow a = 0 ,$$

$$(4.4) \qquad |P : \phi(P)| = |V_1| = p^d .$$

Assuming now that

$$(4.5) \qquad q = p^m ,$$

we shall verify that P satisfies (2.1) and (2.2).

That P satisfies (2.1) follows immediately from (4.4). The proof for (2.2) is less evident. The element x in (4.2) has the form $1 + a + b$, where $b \in \underline{\underline{a}}^2$. Then $x^q = 1 + (a+b)^q = 1 + a^q$ because $\underline{\underline{a}}^{q+1} = 0$. It follows easily that

$$\pi_m(P) = \{1+v \mid v \in V_q\} \subseteq \zeta(P) .$$

Suppose now that f is a definite q-form; such exist by Lemma 3 because of our initial assumption that $d \le p^m$. Then, by Lemma 2, there exists a linear functional f^* on V_q such that $f(a) = f^*(a^q)$ for all $a \in V_1$. Let

$$Q = \{1+v \mid v \in \ker f^*\} .$$

It is evident that Q is a subgroup of $\pi_m(P)$ of index p and, since $\pi_m(P) \subseteq \zeta(P)$, Q is normal in P. Suppose the element x in (4.2) is not in $\phi(P)$. Then $a \ne 0$ and so, since f is definite, $f^*(a^q) = f(a) \ne 0$. It follows that $x^q = 1 + a^q \notin Q$. This completes the verification that P satisfies (2.2).

We have now constructed a finite p-group P satisfying (2.1), (2.2) and this, by the considerations of Section 2, establishes our Theorem.

References

[1] C. Chevalley, "Démonstration d'une hypothèse de M. Artin", *Abh. Math. Sem. Univ. Hamburg* 11 (1936), 73-75.

[2] L.G. Kovács, Joachim Neubüser, B.H. Neumann, "On finite groups with 'hidden' primes", *J. Austral. Math. Soc.* 12 (1971), 287-300.

Department of Pure Mathematics,
University of Sydney,
Sydney,
New South Wales.

https://doi.org/10.1017/S000497270002400X Published online by Cambridge University Press