FURTHER RESULTS ON p-AUTOMORPHIC p-GROUPS

J. BOEN, O. ROTHAUS, AND J. THOMPSON

Graham Higman [3] has shown that a finite p-group, p an odd prime, with an automorphism permuting the subgroups of order p cyclically is abelian. In [1] a p-group was defined to be p-automorphic if its automorphism group is transitive on the elements of order p. It was conjectured that a p-automorphic p-group ($p \neq 2$) is abelian and proved that a counterexample must be generated by at least four elements. In this present paper we prove that a counterexample generated by n elements must be such that $n > 5$ and, if $n \neq 6$, then $p < n3^{n^2}$ (Theorem 3). We also show that the existence of a counterexample implies the existence of a certain algebraic configuration (Theorem 1). All groups considered are finite.

Notation. $\Phi(P)$ is the Frattini subgroup of the p-group P and P' is its commutator subgroup. $\Omega_i(P)$ is the subgroup generated by the elements of P whose orders do not exceed p^i. $Z(P)$ is the center of P. $F(m, n, p)$ denotes the set of p-automorphic p-groups P which enjoy the additional properties:

1. $P' = \Omega_1(P)$ is elementary abelian of order p^n.
2. $\Phi(P) = Z(P) = \Omega_m(P)$ is the direct product of n cyclic groups of order p^m.
3. $|P: \Phi(P)| = p^n$.

In [1] it was shown that a counterexample generated by n elements has a quotient group in $F(m, n, p)$. Hence, in arguing by contradiction, we may assume that a counterexample P is in $F(m, n, p)$.

Let $A = A(P) = \text{Aut } P$ and let $A_0 = \ker(\text{Aut } P \to \text{Aut } P/\Phi(P))$. Thus $A/A_0 = B$ is faithfully represented as linear transformations of $V = P/\Phi(P)$, considered as a vector space over $GF(p)$.

Since p is odd and $cl(P) = 2$, the mapping $\eta: x \to x^{p^m}$ is an endomorphism of P which commutes with each σ of Aut P. Since $\Omega_m(P) = \Phi(P)$, ker $\eta = \Phi(P)$, so η induces an isomorphism of V into $W = P'$. Since dim $V = \dim W$, η is onto.

The commutator function induces a skew-symmetric bilinear map of $V \times V$ onto W, (onto since P is p-automorphic) and since $\Phi(P) = Z(P)$, $(,)$ is nondegenerate. Associated with $(,)$ is a nonassociative product $\circ$, defined as follows: If $\alpha, \beta \in V$, say $\alpha = x\Phi(P)$, $\beta = y\Phi(P)$, then $[x, y]$ is an element of W which depends only on α, β, and so $[x, y] = z^{p^m}$ where the coset $\gamma = z\Phi(P)$ depends only on α, β. We write $\alpha \circ \beta = \gamma$. An immediate consequence of this condition is the statement that $\alpha \to \alpha \circ \beta$

Received December 6, 1961. Boen's work on this paper was partly supported by N.S.F Grant G-9504.

is a linear map ϕ_β of V into V. Thus, $\circ$ induces a map θ of V into End V, the ring of linear transformations of V to V.

If $\bar{\sigma}$ is the inner automorphism of End V induced by $\sigma \in B$, then the diagram

$$\begin{array}{ccc} V & \xrightarrow{\theta} & \text{End } V \\ \sigma \downarrow & & \downarrow \bar{\sigma} \\ V & \xrightarrow{\theta} & \text{End } V \end{array}$$

commutes, that is $\phi_{\beta^\sigma} = \sigma^{-1}\phi_\beta\sigma$. Since P is p-automorphic, if α, β are nonzero elements of V, then $\alpha = \beta^\sigma$ for suitable $\sigma \in B$, so that $\phi_\alpha = \sigma^{-1}\phi_\beta\sigma$.

THEOREM 1. *If $\alpha \in V$, then ϕ_α is nilpotent.*

Proof. We can suppose $\alpha \neq 0$. Since $\alpha \circ \alpha = 0$, ϕ_α is singular. Let $f(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots$ be the characteristic equation of ϕ_α. $f(x)$ is independent of the nonzero element α of V, and $c_n = 0$ since ϕ_α is singular.

Let $\alpha_1, \cdots, \alpha_n$ be a basis for V, and identify ϕ_α with the matrix which is associated with ϕ_α and the basis $\alpha_1, \cdots, \alpha_n$. Then c_i is the sum of all i by i principal minors of ϕ_α, so if $\alpha = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n$, c_i is a homogeneous polynomial of degree $i\,(\leqq n-1)$ in the n variables $\lambda_1, \cdots, \lambda_n$. By a Theorem of Chevalley [2], there are values $\lambda_1, \cdots, \lambda_n$ of $GF(p)$ which are not all zero, such that $c_i = 0$. Since c_i is independent of the non-zero tuple $(\lambda_1, \cdots, \lambda_n)$, it follows that $c_i = 0$ so ϕ_α is nilpotent.

Theorem 1 states that $\theta(V)$ is a linear variety of End (V) consisting only of nilpotent matrices such that any two nonzero $x, y \in \theta(V)$ are similar. If one could show that the algebra generated by $\theta(V)$ were nilpotent, an easy argument would show that all p-automorphic p-groups (p odd) are abelian.

THEOREM 2. *Let r be the rank of ϕ_α. If $n > 3$, then $2 < r < n-1$.*

Proof. We assume $n > 3$ because $n \leqq 3$ was treated in [1]. Clearly $r \neq 0$ because P is non-abelian and $r \neq n$ by Theorem 1.

Case I. $r \neq n-1$. Suppose $r = n-1$. Then, for $\alpha \neq 0$, $\beta \circ \alpha = \beta\phi_\alpha = 0$ implies that $\beta \in \{\alpha\}$ where $\{\alpha\}$ is the subspace of V spanned by α. If $\gamma\phi_\alpha^2 = (\gamma\phi_\alpha)\phi_\alpha = 0$, then $\gamma\phi_\alpha \in \{\alpha\}$, say $\gamma\phi_\alpha = k\alpha$. But $\gamma\phi_\alpha + \alpha\phi_\gamma = 0$ by the skew-symmetry of $\circ$, so $\alpha\phi_\gamma = -k\alpha$. By Theorem 1, $k = 0$ and thus $\gamma \in \{\alpha\}$. Hence rank $\phi_\alpha^2 =$ rank ϕ_α, a contradiction to Theorem 1.

Case II. $r \neq 1$. Choose a basis of V, say $\alpha_1, \cdots, \alpha_n$, and suppose that $\phi_\alpha = (a_{ij})$ with respect to this basis; End (V) has the obvious matrix representation with $\phi_\alpha \in \theta(V) \subset \mathrm{End}(V)$. Recall that $\theta(V)$ becomes an n-space of n by n nilpotent matrices over $GF(p)$ in which any two nonzero matrices are similar. If $r = 1$, then we may assume without loss of generality that ϕ_α has a 1 in the (1, 2) position and zeros elsewhere.

If every $(x_{ij}) = X \in \theta(V)$ satisfies $x_{ij} = 0$ for $i > 1$, then we are done because the nilpotency of X implies that $x_{11} = 0$ for every $X \in \theta(V)$, which implies that $\dim \theta(V) < n$. If, on the other hand, there exists $X \in \theta(V)$ with a nonzero entry below the first row, then we may use the fact that every 2 by 2 subdeterminant of every element of $\theta(V)$ vanishes to show that every X has its nonzero elements in the second column only. But the nilpotency of X implies that $x_{22} = 0$. Hence $\dim \theta(V) < n$, a contradiction.

Case III. $r \neq 2$. *If* $r = 2$, we may assume without loss of generality that

(a) ϕ_α has 1's in the (1, 2), (2, 3) positions and zeros elsewhere or else

(b) ϕ_α has 1's in the (1, 2), (3, 4) positions and zeros elsewhere.

First consider (a).

If every $(x_{ij}) = X \in \theta(V)$ satisfies $x_{ij} = 0$ for $i > 2$, then $Z(P) \subsetneqq \Phi(P)$, a contradiction. If every $X \in \theta(V)$ satisfies $x_{ij} = 0$ for $j \neq 2, 3$, then $x_{32} = 0$ because $X + k\phi_\alpha$ is nilpotant for every $k \in GF(p)$ and $p > 2$. But then $\dim \theta(V) < n$, a contradiction. Hence we need consider only the subcase of (a) in which some $X \in \theta(V)$ has a nonzero entry below the third row and a nonzero entry that is not in columns two or three. Consider such an X. Unless $x_{ij} = 0$ when $i \neq 1, 2$ and $j \neq 2, 3$, it is easy to see that there exists a nonzero 3 by 3 determinant in $X + k\phi_\alpha$ for some k. It is also easy to see that any two rows of X below the second row are dependent, and that any two columns other than the second and third are dependent. Using the fact that every 3 by 3 subdeterminant of every element of $\theta(V)$ is zero, it is straightforward to show that there exist nonsingular matrices R and S such that RXS has 1's in the (1, 4), (3, 2) posititions and zeroes elsewhere and $R\phi_\alpha S$ has 1's in the (1, 3), (2, 2) positions and zeroes elsewhere.

Set $X' = RXS$, $\phi'_\alpha = R\phi_\alpha S$. It is now straightforward to show that that if $Y = (y_{ij}) \in R\theta(V)S$ is linearly independent from $\{X', \phi'_\alpha\}$, then $y_{ij} = 0$ for $i \neq 1$ and $j \neq 2$. This implies that $\dim R\theta(V)S < n$, a contradiction, since $\dim R\theta(V)S = \dim \theta(V) = n$.

Subcase (b), in which $\phi_\alpha^2 = 0$, is handled in a similar fashion except that we exclude the case in which every $X \in \theta(V)$ satisfies $x_{ij} = 0$, $j \neq 2, 4$, by noting the following: In such a case $(X + k\phi_\alpha)^2 = 0$ for every k implies that $x_{22} = 0$, which in turn implies that $\dim \theta(V) < n$.

COROLLARY. *$F(m, n, p)$ is empty for all m and odd p unless $n > 5$.*

Proof. Theorem 2 implies that $n > 4$ and that if $n = 5$, then rank $\phi_\alpha = 3$. Let S_n denote the projective $(n-1)$-space whose points are the 1-subspaces of V. If $n = 5$ and rank $\phi_\alpha = 3$, then it follows that S_5 is partitioned into lines according to the rule that $\{\alpha\}$, $\{\beta\}$ $(0 \neq \alpha, \beta \in V)$ lie on the same line if and only if $\alpha \circ \beta = 0$. But S_5 has $p^4 + p^3 + p^2 + p + 1$ points and cannot be partitioned into disjoint subsets of $p + 1$ points each.

THEOREM 3. *If $p \geqq n3^{n^2}$ and $n \neq 6$, then $F(m, n, p)$ is empty for all positive integers m.*

Proof. If $GL\,(n, p)$ denotes the invertible elements of End V, then

$$|GL(n, p)| = p^{n(n-1)/2} \cdot k(n, p), \text{ where } k(n, p) = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1).$$

If we consider $GF(p^n)$ as a vector space over $GF(p)$, the right-regular representation shows that $GL(n, p)$ contains a cyclic group of order $p^n - 1$.

Let $\Phi_d(x)$ be the monic polynomial whose complex roots are the primitive dth roots of unity. Then $p^n - 1 = \prod_{d|n} \Phi_d(p)$. By an elementary number-theoretic theorem [4], $\Phi_n(p)$ and $k(n, p)/\Phi_n(p)$ are relatively prime, or their greatest common divisor is q where q is the largest prime divisor of n, in which case $\Phi_n(p)/q$ is relatively prime to $k(n, p)/\Phi_n(p)$. Thus, we determine $\varepsilon = 0$ or 1 so that $\Phi_n(p)/q^\varepsilon$ is relatively prime to $k(p, n)/\Phi_n(p)$.

Let $p \in F(m, n, p)$. Since P is p-automorphic, $|B|$ is divisible by $p^n - 1$ and in particular is divisible by $\Phi_n(p)/q^\varepsilon$. Let r^α be the largest power of the prime r which divides $\Phi_n(p)/q^\varepsilon$, $\alpha \geqq 1$, and let S_r be a Sylow r-subgroup of B. By Sylow's theorem and the preceding paragraph, S_r is cyclic with generator σ_r.

Since P belongs to the exponent n modulo r, it follows that $\lambda, \lambda^p, \cdots, \lambda^{p^{n-1}}$ are the characteristic roots of σ_r, λ being a primitive r^αth root of unity in $GF(p^n)$.

Since η commutes with σ_r, λ is also a characteristic root of σ_r on W. Since $(\alpha, \beta)^\sigma = (\alpha^\sigma, \beta^\sigma)$, the characteristic roots of σ_r on W are to be found among the $\lambda^{p^i + p^j}$, $0 \leqq i < j \leqq n - 1$, as can be seen by diagonalizing σ_r over $V \otimes GF(p^n)$. Hence, $\lambda = \lambda^{p^i + p^j}$ for suitable i, j and so

$$p^i + p^j - 1 \equiv 0 \pmod{r^\alpha}. \tag{1}$$

Since r was any prime divisor of $\Phi_n(p)/q^\varepsilon$, we have

$$\prod_{0 \leqq i < j \leqq n-1} (p^i + p^j - 1) \equiv 0 \pmod{\Phi_n(p)/q^\varepsilon}. \tag{2}$$

The polynomials $\Phi_n(x)$, $n \neq 6$, and $x^i + x^j - 1$ are relatively prime, a fact which can be seen geometrically, as pointed out by G. Higman. Namely, if $\varepsilon, \varepsilon'$ are complex numbers of absolute value one, and $\varepsilon + \varepsilon' = 1$, then the points $0, 1, \varepsilon$ are the vertices of an equilateral triangle, so that ε is a primitive sixth root of unity. Since $n \neq 6$, we can therefore find integral polynomials $f(x)$, $g(x)$, such that

$$f(x)\Phi_n(x) + g(x)\prod_{0 \leqq i < j \leqq n-1}(x^i + x^j - 1) = |N| \,, \tag{3}$$

where

$$\begin{aligned} N &= \textstyle\prod_\zeta \prod_{i,j}(\zeta^i + \zeta^j - 1) \\ \Phi_n(\zeta) &= 0 \end{aligned} \tag{4}$$

is the resultant of $\Phi_n(x)$ and $\prod(x^i + x^j - 1)$.

From (4) we see that $N \leqq 3^{\phi(n)n^2}$, since there are at most $\phi(n)n^2$ triples (ζ, i, j). Now (2) and (3), the fact that $\Phi_n(p)/q^\varepsilon$ divides $|N|$, imply that

$$\Phi_n(p)/q^\varepsilon \leqq 3^{\phi(n)n^2} \,. \tag{5}$$

One sees geometrically that $\Phi_n(p) \geqq (p-1)^{\phi(n)}$, so with (5) and $q^\varepsilon \leqq n$ we find

$$p \leqq 1 + n^{1/\phi(n)} 3^{n^2} < n 3^{n^2} \,. \tag{6}$$

REMARK. Theorem 3 of [3] provides a certain motivation for the detailed examination of $\Phi_n(p)$ in the preceding theorem.

BIBLIOGRAPHY

1. J. Boen, *On p-Automorphic p-Groups*, (to appear in Pacific Journal of Mathematics).
2. C. Chevalley, *Demonstration d'une hypothese de M. Artin*, Abh. Math. Seminar U. Hamburg, **11** (1936).
3. G. Higman, *Suzuki 2-groups*, (to appear).
4. T. Nagell, *Introduction to Elementary Number Theory*, Wiley (1951).

UNIVERSITY OF CHICAGO AND UNIVERSITY OF MICHIGAN
INSTITUTE FOR DEFENSE ANALYSES
UNIVERSITY OF CHICAGO