# ON $p$-AUTOMORPHIC $p$-GROUPS

J. R. BOEN

In a paper to appear, G. Higman has "classified" the finite 2-groups whose involutions are permuted cyclically by their automorphism groups [1]. He found that such a group is either generalized quaternion, abelian of type $(2^n, \cdots, 2^n)$, or of exponent four and class two. He also proved that a finite $p$-group with an automorphism permuting its subgroups of order $p$ cyclically is abelian if $p$ is odd. We say that a group is $\pi$-automorphic if it has the property that any two of its elements of order $k$ are conjugate under an automorphism where $\pi$ is a set of positive integers and $k \in \pi$. In this paper we conjucture that a finite $p$-automorphic $p$-group is abelian for odd $p$, and prove that a counterexample cannot be generated by fewer than four elements.

We use the following notation. Let $p^{n+1}$ be the exponent of the $p$-group $G$; $H_k(G)$ denotes the set of elements of $G$ whose orders do not exceed $p^k$; $G'$ is the commutator subgroup of $G$; $(x, y) = x^{-1}y^{-1}xy$; $Z(G)$ is the center of $G$ and $Z_2(G)$ is the preimage of $Z(G/Z)$ in the cannonical homomorphism of $G$ onto $G/Z$; $\Phi(H)$ is the Frattini subgroup of the group $H$; $|H|$ is the order of $H$; $|x|$ is the order of the element $x$. $GL(3, p)$ is the full linear group of degree three over the prime Galois field $GF(p)$.

Henceforth let $G$ denote a finite $p$-automorphic non-abelian $p$-group for odd $p$. Note that $H_1(G) = H_1 \subseteqq Z = Z(G)$, so $H_1$ is a subgroup.

LEMMA 1. *$G/H_1$ is $p$-automorphic.*

*Proof.* Clearly there exists $x \in Z_2(G)$ such that $|x| = p^2$ because $G$ cannot be of exponent $p$. Consider $y \in G$ where $|y| = p^2$. By the definition of $G$ there exists $\alpha \in \mathrm{Aut}(G)$ such that $(y^p)^\alpha = x^p$. Let $y^\alpha = wx$. Thus $(y^\alpha)^p = (wx)^p = w^p x^p (x, w)^{\binom{p}{2}}$ by the choice of $x$. If $Z$ has an element of order $p^2$, choose $x$ to be it. Then $(x, w) = 1$. If $Z = H_1$, then $(x, w) \in H_1$ and $(x, w)^{\binom{p}{2}} = 1$. In either case $(y^\alpha)^p = (y^p)^\alpha = x^p = w^p x^p$ so $w \in H_1$ and $(yH_1)^\alpha = xH_1$. Q.E.D.

LEMMA 2. *If $G' = H_1$, then $H_n(G) = \Phi(G) = Z$.*

*Proof.* $\Phi(G) = \Phi = G'P$ where $P$ is the subgroup of $G$ generated by $p$th powers. $G' = H_1$ implies that $G$ is of class two, so $(x^p, y) = (x, y^p) = (x, y)^p = 1$. Hence $\Phi \subseteqq Z$. In the canonical homomorphism of $G$

Received March 31, 1961, and in revised form August 31, 1961. This paper was sponsored in part by NSF Grant G-9504.

onto $G/G' = K$, $H_n(G) = H_n$ is the preimage of $H_{n-1}(K) = \Phi(K)$. ($H_n$ is a subgroup because $G$ is regular; $K$ is abelian and has equal invariants). If there exists $x \in Z$ such that $|x| = p^{n+1}$ then for any $y \in G$ where $|y| = p^{n+1}$ we have $(y^{p^n})^\alpha = x^{p^n}$ for some $\alpha \in \mathrm{Aut}(G)$. By the same reasoning used in Lemma 1 it follows that $y^\alpha = wx$ where $w \in H_n$. Hence $y^\alpha \in Z$ so $y \in Z$ and $G$ is abelian, a contradiction. Q.E.D.

LEMMA 3. *If $G' = H_1$, then $\varphi: x \to x^{p^n}$ is an isomorphism of $G/Z$ onto $G'$.*

*Proof.* Since $G$ is of class two, $(xy)^m = x^m y^m (y, x)^{\binom{m}{2}}$ where $m = p^n$. But $\binom{m}{2}$ is a multiple of $p$ so $(y, x)^{\binom{m}{2}} = 1$ and $\varphi$ is an endomorphism of $G$. Clearly $H_n = Z$ is the kernel of $\varphi$. At least one nonidentity element of $G'$ is an $m$th power, hence every one is and thus $G/Z \cong G'$. Q.E.D.

THEOREM. *A finite non-abelian p-automorphic p-group $G$ cannot be generated by fewer than four elements.*

*Proof.* It is easily seen that $H_1 \subseteqq \Phi$. By repeated application of Lemma 1 we arrive at a $G_1$ such that $G_1' = H_1(G_1)$ where $G_1$ has the same number of generators as $G$. Since we argue by contradiction we may assume without loss of generality that $G' = H_1$.

Clearly $G$ cannot be cyclic. If $G$ can be generated by two elements, the fact that $G$ is of class two implies that $G'$ is cyclic; this contradicts Lemma 3. Hence we assume $G$ to be a three-generator group, say $G = \{u_1, u_2, u_3\}$. Lemma 2 implies the following identities.

(i) $(u_1^{x_1} u_2^{x_2} u_3^{x_3} h, u_1^{y_1} u_2^{y_2} u_3^{y_3} h') = \prod_{i<j} s_{ij}^{x_i y_j - x_j y_i}$ where $h, h' \in Z$ and $s_{ij} = (u_i, u_j)$.

(ii) $$(u_1^{x_1} u_2^{x_2} u_3^{x_3} h)^{p^n} = \prod t_i^{x_i} \text{ where } t_i = u_i^{p^n}.$$

Now every element of $G'$ is a commutator. Thus there exist relations $t_i = s_{12}^{a_{i1}} s_{13}^{a_{i2}} s_{23}^{a_{i3}}$, $i = 1, 2, 3$, where $|A| = |(a_{ij})| \neq 0$. Let $\alpha$ be an automorphism of $G$, say $u_i^\alpha = u_1^{x_{i1}} u_2^{x_{i2}} u_3^{x_{i3}} h_i$, $i = 1, 2, 3$, where $h_i \in Z$ and $x_{ij} \in GF(p)$. (i) implies that $s_{ij}^\alpha = \prod_{k<l} s_{kl}^{\bar{x}_{kl}}$ where $\bar{x}_{kl} = x_{ik} x_{jl} - x_{jk} x_{il}$. Hence

$$t_i^\alpha = (s_{12}^{a_{i1}} s_{13}^{a_{i2}} s_{23}^{a_{i3}})^\alpha = (s_{12}^{a_{i1}})^\alpha (s_{13}^{a_{i2}})^\alpha (s_{23}^{a_{i3}})^\alpha = s_{12}^{\Sigma a_{ij} \bar{x}_{j1}} s_{13}^{\Sigma a_{ij} \bar{x}_{j2}} s_{23}^{\Sigma a_{ij} \bar{x}_{j3}} .$$

But (ii) implies that

$$t_i^\alpha = \prod t_j^{x_{ij}} = s_{12}^{\Sigma x_{ij} a_{j1}} s_{13}^{\Sigma x_{ij} a_{j2}} s_{23}^{\Sigma x_{ij} a_{j3}} .$$

Equating these two representations of $t_i^\alpha$ and noting that $s_{12}$, $s_{13}$, and $s_{23}$ are independent, we have

$$\text{(iii)} \qquad A\bar{X} = XA$$

where $A = (a_{ij})$, $X = (x_{ij})$, and $\bar{X} = (\bar{x}_{ij})$ are nonsingular 3-square matrices over $GF(p)$. It is clear that $\bar{X} = |X| B^{-1}X^{-T}B$ where $X^{-T}$ is the transpose of $X^{-1}$ and $B = (b_{ij})$ has the entries $b_{13} = b_{31} = -b_{22} = 1$ and the remaining $b_{ij} = 0$. Thus, substituting for $\bar{X}$ in (iii), we equate the determinants of the two sides of (iii) and find that $|X| = 1$. (iii) then takes the form:

$$\text{(iv)} \qquad CX^{-T}C^{-1} = X \text{ where } C = AB^{-1}\,.$$

It follows that (iv) holds for all $X$ in some transitive (on the nonzero vectors of the 3-space $V$) subgroup $T$ of $GL(3, p)$. Thus $|T|$ is divisible by $p^3 - 1$. $|GL(3, p)| = p^3(p-1)(p^2-1)(p^3-1)$. Let $q$ be a prime divisor of $p^2 + p + 1$ where $q > 3$. It is easily shown that such a $q$ exists and that $q$ is relatively prime to $p - 1$ and $p + 1$. Thus a Sylow $q$-subgroup of $T$ is a Sylow $q$-subgroup $GL(3, p)$. $GL(3, p)$ contains a cyclic transitive subgroup of order $p^3 - 1$, the multiplicative group of the right-regular representation of $GF(p^3)$ considered as a vector space over $GF(p)$. Hence a Sylow $q$-subgroup of $GL(3, p)$ is cyclic, so an $X \in T$ of order $q$ is conjugate to

$$Y = \begin{pmatrix} \omega & & \\ & \omega^p & \\ & & \omega^{p^2} \end{pmatrix} \text{ where } \omega^q = 1$$

in $GL(3, p^3)$. But $Y$ is certainly not conjugate to $Y^{-T}$ in $GL(3, p^3)$ from which it follows that $X$ will not satisfy (iv), a contradiction. Q.E.D.

The author is indebted to G. Higman and G. E. Wall for their suggestions, and to the referee for correcting an error.

## Reference

1. G. Higman, *Suzuki 2-groups*, to appear.

University of Chicago