PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 3, 1968

p-AUTOMORPHIC p-GROUPS AND HOMOGENEOUS ALGEBRAS

LARRY DORNHOFF

A p-group was called p-automorphic by Boen, if its automorphism group is transitive on elements of order p. Boen conjectured that if p is odd, then such a p-group is abelian. Let P be a nonabelian p-automorphic p-group, p odd, generated by n elements. Boen proved that $n > 3$, and in joint work with Rothaus and Thompson proved that $n > 5$. Kostrikin then showed that $n > p + 6$, as a corollary of results on homogeneous algebras. In this paper it is shown that $n > 2p + 3$, using Kostrikin's methods, and his proof is somewhat simplified by eliminating special case considerations for small values of p.

The above results and the following terminology may be found in [1], [2], and [4]. Let A be a finite-dimensional algebra over the field K, where if $x, y \varepsilon A$ and $\lambda \varepsilon K$, we assume bilinearity and the law $(\lambda x) \circ y = \lambda(x \circ y) = x \circ (\lambda y)$, but associativity is not assumed. Following [4], A is said to be *homogeneous* if the automorphism group Γ of A is transitive on $A^{\#} = A - \{0\}$, *anticommutative* if $x \circ y + y \circ x = 0$, and *nil* if all endomorphisms $K_a: x \rightarrow x \circ a$ are nilpotent.

For a fixed odd prime p, suppose that P is a nonabelian p-automorphic p-group with minimal number n of generators. It is shown in [1] that P has a p-automorphic quotient group $\bar{P}$ with the same number of generators, where the Frattini subgroup $\Phi(\bar{P})$ is central and is the direct product of n cyclic groups of equal order p^m. If we consider $A = \bar{P}/\Phi(\bar{P})$ as a vector space over $GF(p)$, we define a multiplication in A as follows: for $x = a\Phi(\bar{P}), y = b\Phi(\bar{P})$ in A, a coset $z = c\Phi(\bar{P})$ is uniquely determined, such that $[a, b] = c^{p^m}$. Define $x \circ y = z$. Then it is clear that A becomes an anticommutative homogeneous algebra, and Theorem 1 of [2] asserts that A is nil.

It is proved in [4] that if A is a finite-dimensional homogeneous algebra with nontrivial multiplication over a field K of characteristic not 2, then A is an anticommutative nil algebra and K is a finite field of q elements, where $q < \dim A - 6$. In this paper we shall prove:

THEOREM. *Let A be a homogeneous anticommutative nil algebra with nontrivial multiplication of dimension n over the field K of q elements, q odd. Then $n > 2q + 3$.*

This result immediately implies the corresponding result for p-

automorphic p-groups.

2. In proving the theorem, we use the following notation. A is a homogeneous anticommutative nil algebra of dimension n over the field K of q elements, q odd, and Γ its automorphism group. We choose integers m and r such that

$$\dim AR_x = m, R_x^r = 0, R_x^{r-1} \neq 0, \text{ all } x \neq 0 \text{ in } A .$$

Of course $r \leqq m + 1$. Since Γ is transitive on $A - \{0\}$, $q^n - 1$ divides the order of Γ. Let s be a prime dividing $q^n - 1$, but not dividing $q^t - 1$ for any $t < n$; the existence of s is proved in [3]. (We may assume $n > 2$; for the case $n = 2$, the theorem follows from the relation $r > q$, soon to be proved.) Let $\sigma \in \Gamma$ have order s; then σ is irreducible on the vector space A. Fix a nonzero element $e \in A$. Then A is spanned by $e, e\sigma, \cdots, e\sigma^{n-1}$; let

$$e\sigma^n = \sum_{j=1}^{n} a_j e\sigma^{n-j}, \ a_j \in K ,$$

where σ satisfies the irreducible polynomial $P(X) = X^n - \sum_{j=1}^{n} a_j X^{n-j}$.

Consider the vectors $e\sigma^i \circ e$, $0 \leqq i \leqq n - 1$. We see that

$$\begin{aligned}(e\sigma^i \circ e)\sigma^{n-i} &= e\sigma^n \circ e\sigma^{n-i} = \left(\sum_{j=1}^{n} a_j e\sigma^{n-j}\right) \circ e\sigma^{n-i} \\ &= \sum_{j=1}^{n} a_j(e\sigma^{n-j} \circ e\sigma^{n-i}) = \sum_{j \leqq i} a_j(e\sigma^{i-j} \circ e)\sigma^{n-i} \\ &\quad - \sum_{j > i} a_j(e\sigma^{j-i} \circ e)\sigma^{n-j} = \sum_{0 \leqq k < i} a_{i-k}(e\sigma^k \circ e)\sigma^{n-i} \\ &\quad - \sum_{k=1}^{n-i} a_{i+k}(e\sigma^k \circ e)\sigma^{n-i-k} .\end{aligned}$$

Transferring all terms to the right-hand side, we have a relation

$$AR_e B = 0 ,$$

where $B = (b_{ij})_{0 \leqq i, j \leqq n-1}$, as a matrix over $\bar{K} = K(\sigma)$, say, with row index j and column index i, is given as follows: Define $a_0 = -1$, $a_k = 0$ if $k < 0$ or $k > n$. Then

$$b_{ij} = a_{i-j}\sigma^{n-i} - a_{i+j}\sigma^{n-i-j} .$$

We look at this matrix B quite closely. If n is even, let B_1 be the lower right-hand $(n/2) \times (n/2)$ minor. B_1 is a triangular matrix with

$$\operatorname{Det} B_1 = (-1)^{n/2}\sigma^{1+2+\cdots+\{(n-2)/2\}}(\sigma^{n/2} + a_n) \neq 0 ,$$

so rank $B \geqq n/2$. If n is odd, let B_1 be the lower right-hand

$(n+1)/2 \times (n+1)/2$ minor. B_1 is no longer triangular, but we easily compute

$$\operatorname{Det} B_1 = (-1)^{(n-3)/2}\sigma^{1+2+\cdots+\{(n-3)/2\}}(\sigma^n + a_{n-1}\sigma^{(n+1)/2} + a_1 a_n \sigma^{(n-1)/2} - a_n^2) .$$

If this is 0 and $n > 3$, we see that $P(X)$ reduces to $P(X) = X^n - 1$, so $\sigma^{2n} = 1$, a contradiction to the fact $s \equiv 1 \pmod n$ (see [3]). If $n = 3$, then $P(X) = X^3 - aX^2 + aX - 1$ and $P(X)$ is reducible. Hence rank $B \geqq (n+1)/2$. We conclude that in any case

$$\operatorname{rank} R_e = \dim AR_e = m \leqq \frac{n}{2} .$$

The next step in the proof is to show that $r > q + 1$; this is done in [4], but we repeat it here, as the final case simplifies.

First suppose $r \leqq q$. Then we can linearize the identity

$$(R_x + \alpha R_z)^r = R^r_{x+\alpha z} = 0 ,$$

all $\alpha \in K$, obtaining

$$\sum_{i=0}^{r-1} R_x^i R_z R_x^{r-1-i} = 0 .$$

Applying to $y \in A$ and using anticommutativity,

$$y \cdot \sum_{i=0}^{r-1} R_x^i R_z R_x^{r-1-i} = -\sum_{i=0}^{r-1} z R_{yR_x^i} R_x^{r-1-i} = 0 ,$$

and hence

$$\sum_{i=0}^{r-1} R_{yR_x^i} R_x^{r-1-i} = 0 .$$

The equation $e = a \circ e$ is not possible, since otherwise $eR_a^k = (-1)^k e \neq 0$, and R_a is not nilpotent. Hence $a \notin AR_e$. We choose a basis $\{e_1, \cdots, e_{r_1}; e_{r_1+1}, \cdots, e_{r_1+r_2}; \cdots e_n\}$, $e = e_n$, such that the nilpotent transformation R_e is in Jordan canonical form. Thus we have

$$r = r_1 \geqq r_2 \geqq \cdots ; e_i R_{e_n} = e_{i+1} \text{ if}$$

$r_1 + \cdots + r_{k-1} + 1 \leqq i < r_1 + \cdots + r_k$, some k; $e_{r_1+\cdots+r_k} R_{e_n} = 0$.

Setting $y = e_1$, $x = e_n$ in the last identity, we have

$$R_{e_r} + \Big(\sum_{i=0}^{r-2} R_{e_{i+1}} R_{e_n}^{r-2-i}\Big) R_{e_n} = 0 .$$

Hence $AR_{e_r} \subseteqq AR_{e_n}$; but $\dim AR_{e_r} = \dim AR_{e_n}$, so $AR_{e_r} = AR_{e_n}$. Thus $e_r = e_1 R_{e_n}^{r-1} \in AR_{e_n} = AR_{e_r}$, a contradiction. We conclude $r > q$.

Now suppose $r = q + 1$. The identity $R_x^r = 0$ cannot be linearized, but the linearization process does enable us to prove

$$R_y R_x^{q-1} R_z + R_z R_x^{q-1} R_y + f(R_x, R_y, R_z) R_x + R_x g(R_x, R_y, R_z) = 0 \ ,$$

where f and g are homogeneous polynomials, linear in R_y and R_z. (Expand $(R_x + \alpha R_y + \beta R_z)^{q+1} = 0$, use $\alpha = \alpha^q$, $\beta = \beta^q$ to combine two terms, and then use van der Monde determinants as in the usual linearization to show all terms are 0. The coefficient of $\alpha\beta$ is the left side of the desired equation.) Applying this to x and using anticommutativity,

$$0 = zR_{yR_x^q} - zR_x^q R_y - z\bar{f}(R_x, R_y)R_x, \text{ some } \bar{f},$$

showing that

$$R_{yR_x^q} - R_x^q R_y - \bar{f}(R_x, R_y) R_x = 0 \ .$$

We choose a canonical basis for R_{e_n} as before and set $x = e_n$, $y = e_1$ in the last identity, obtaining

$$R_{e_r} = R_{e_n}^q R_{e_1} + f(R_{e_n}, R_{e_1}) R_{e_n} \ .$$

For $i \notin \{1, r_1 + 1, r_1 + r_2 + 1, \cdots\}$, we see

$$e_i R_{e_r} = e_i \bar{f}(R_{e_n}, R_{e_1}) Re_n \in AR_{e_n} \ .$$

Also,

$$e_1 R_{e_r} = e_r R_{e_1} + e_1 \bar{f}(Re_n, R_{e_1}) R_{e_n} \ ,$$

so since the characteristic is odd, $e_1 R_{e_r} \in AR_{e_n}$. If $r_2 < r_1$, then $e_i R_{e_n}^q = 0$ for $i \geqq r$, and we conclude that $AR_{e_r} = AR_{e_n}$, which we know to be impossible. Hence $r_2 = r_1 = r$. Then $n \geqq 2r + 1 = 2q + 3$. If we have equality, then the canonical form shows $m = \dim AR_{e_n} = 2r - 2 = 2q > (n/2)$, a contradiction. Hence $n > 2q + 3$, and we are done in this case.

Thus we now may assume $r \geqq q + 2$, $r \leqq m + 1$, $m \leqq n/2$. If n is even, we have $q + 2 \leqq r \leqq m + 1 \leqq (n/2) + 1$, or $n \geqq 2q + 2$, so we may assume $n = 2q + 2$; then equality holds everywhere, and $r = q + 2$, $m = q + 1$. If n is odd, we have

$$q + 2 \leqq r \leqq m + 1 \leqq \frac{n-1}{2} + 1, \text{ or } n \geqq 2q + 3 \ ,$$

so we may assume $n = 2q + 3$; then equality holds everywhere, and $r = q + 2$, $m = q + 1$. In either case, we note $n \leqq 2m + 1$.

Since q is odd and $q^n - 1$ divides the order of Γ, we can choose an element $\tau \in \Gamma$ of order 2. Define

$$B = \{a \in A \mid \tau(a) = a\}, C = \{a \in A \mid \tau(a) = -a\} \ .$$

Then A is a direct sum $A = B \oplus C$ of its subspaces B and C. Certainly

$C \neq 0$. If $B = 0$, choose $C_1, C_2 \in C$ with $c_1 \circ c_2 \neq 0$. Then $c_1 \circ c_2 = (-c_1) \circ (-c_2) = \tau(c_1) \circ \tau(c_2) = \tau(c_1 \circ c_2) = -c_1 \circ c_2$, a contradiction. Define $\dim B = k > 0, \dim C = n - k$. It is clear that $B \circ B \subseteqq B, C \circ C \subseteqq B$, $B \circ C \subseteqq C$. Hence if $b \in B$, then $BR_b \subseteqq B, CR_b \subseteqq C$; of course the nilpotency index r of R_b is the maximum of its nilpotency indexes on the subspaces B and C.

Suppose first $B \circ C = 0$. Then for any $b \in B^\#, AR_b = BR_b$ has dimension $m; b \notin BR_b$, so $\dim B \geqq m + 1$, proving $\dim C \leqq m$. For any $c \in C^\#, c \circ c = 0$, so since $AR_c = CR_c$, we have

$$\dim AR_c = \dim CR_c < \dim C \leqq m ,$$

a contradiction.

We have thus proved $B \circ C \neq 0$. Pick $b \in B$ with $CR_b \neq 0$; $CR_b \subseteqq C$, so $AR_b = BR_b \oplus CR_b$, and $\dim BR_b \leqq m - 1$. We look at the canonical form of R_b on B and on C, and use the fact

$$r = m + 1; \dim BR_b \leqq m - 1$$

implies $(R_b \mid B)^m = 0$, so $(R_b \mid C)^m \neq 0$, and $\dim CR_b \geqq m$. Hence $\dim CR_b = m, \dim C \geqq m + 1, \dim B \leqq m$. This means that for *any* $b' \in B^\#, \dim BR'_b < m$, so $CR'_b \neq 0$; the same argument then applies for b' as for b. We conclude that $B \circ B = 0$.

Let c be any element of $C^\#$. Since $R_c^m \neq 0$ and $\dim AR_c = m$, we have $\dim AR_c^2 = m - 1$. Since $BR_c \subseteqq C$ and $CR_c \subseteqq B$, we have

$$\dim AR_c = m = \dim BR_c + \dim CR_c .$$

Also,

$$AR_c^2 = (BR_c + CR_c)R_c \subseteqq CR_c + BR_c .$$

Let $\beta_i = \dim BR_c^i, \gamma_i = \dim CR_c^i, i = 1, 2$. We see that $\beta_1 + \gamma_1 = m$, $\beta_2 + \gamma_2 = m - 1, \beta_2 \leqq \gamma_1, \gamma_2 \leqq \beta_1$, and of course $\beta_2 \leqq \beta_1, \gamma_2 \leqq \gamma_1$. Since $m = q + 1$ is even, let $m = 2l$; the only solutions for the β_i and γ_i have $\beta_1 = \gamma_1 = l$. So $\dim BR_c = l$, for any $c \in C^\#$.

We now consider separately the cases $n = 2q + 2$ and $n = 2q + 3$. Let S denote the set of all ordered pairs $\langle b, c \rangle, b \in B, c \in C$, with $b \circ c = 0$. In each case we compute the order $|S|$ in two different ways to obtain a contradiction.

When $n = 2q + 2 = 2m = 4l$, we know that for any

$$b \in B^\#, \dim CR_b = m ,$$

so

$$\dim \{c \in C \mid b \circ c = 0\} = (n - k) - m = m - k ,$$

and for any

$$c \in C^{\#}, \dim BR_c = l, \text{ so } \dim\{b \in B \mid b \circ c = 0\} = k - l .$$

Hence

$$| S | = (q^k - 1)q^{m-k} + q^{n-k}$$

and

$$| S | = (q^{n-k} - 1)q^{k-l} + q^k .$$

Therefore

$$q^{n-k} + q^m - q^{m-k} = q^{n-l} + q^k - q^{k-l} .$$

We know $\dim C = n - k \geqq m + 1$, so $k < m$. Equating highest terms, the equation must imply $k = l$. But now the left side is divisible by q and the right is not, a contradiction.

When $n = 2q + 3 = 2m + 1 = 4l + 1$, then for any

$$b \in B^{\#}, \dim\{c \in C \mid b \circ c = 0\} = (n - k) - m = m - k + 1 ,$$

and for any

$$c \in C^{\#}, \dim\{b \in B \mid b \circ c = 0\} = k - l .$$

Hence

$$| \mathrm{S} | = (q^k - 1)q^{m-k+1} + q^{n-k}$$

and

$$| S | = (q^{n-k} - 1)q^{k-l} + q^k ,$$

showing that

$$q^{m+1} - q^{m+1-k} + q^{n-k} = q^{n-l} - q^{k-l} + q^k .$$

The largest terms on the two sides are necessarily equal, so $n - k = n - l, k = l$. But then the left side is divisible by q and the right is not, the final contradiction.

REMARK. Following [5], one can also consider *semi-p-automorphic* p-groups, in which the automorphism group is transitive on subgroups of order p, and the corresponding notion of *spa-algebras*, in which the automorphism group is transitive on one-dimensional subspaces. The arguments above then show $n > 2p + 1$. To prove $n > 2p + 3$, we require the involution τ in the automorphism group Γ; τ does exist, since otherwise Γ would be of odd order and hence solvable, and the case of a solvable Γ is treated in [5].

Added in proof. Ernest Schult has announced a complete solution of Boen's problem in Bull. Amer. Math. Soc. 74 (1968), 268–270.

REFERENCES

1. J. R. Boen, *On p-automorphic p-groups*, Pacific J. Math. **12** (1962), 813-815.
2. J. R. Boen, O. Rothaus, and J. Thompson, *Further results on p-automorphic p-groups*, Pacific J. Math. **12** (1962), 817-821.
3. L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly **12** (1905), 86-89.
4. A. I. Kostrikin, *On homogeneous algebras*, Izvestia Acad. Nauk SSSR **29** (1965), 471-483.
5. E. Schult, *On semi-p-automorphic groups I* (to appear)

Received August 28, 1967. This research partially supported by Army Contract SAR/Da-31-124-ARO-D-336.

YALE UNIVERSITY