JOURNAL OF ALGEBRA **190,** 163–171 (1997)
ARTICLE NO. JA966879

A Note on p'-Automorphism of p-Groups P of Maximal Class Centralizing the Center of P

Bardo Wolf

Received October 25, 1995

The main subject of this paper is the proof of the following observations (Theorems A and B are contained in the authors dissertation [Wo] written at the University of Mainz in 1994 under the direction of Professor Dr. K. Doerk.)

THEOREM A. *Let P be a p-group of maximal class with $|P| = p^n$, $n \geq 4$, and p an odd prime. Let H be a Hall p'-subgroup of the automorphism group of P. Then*

(i) $C_H(Z(P))$ *is cyclic.*

(ii) $|C_H(Z(P))|$ *divides* $p - 1$ *and if* $|H| = (p-1)^2$, *then* $|C_H(Z(P))| = p - 1$.

THEOREM B. *Let P be a p-group of maximal class with $|P| = p^n$, $n \geq 4$, and p an odd prime. Let q be an odd prime with $q \mid (p-1)$ and let R be a Sylow q-subgroup of the automorphism group of P. Then*

(i) $C_R(Z(P))$ *is cyclic.*

(ii) $C_R(Z(P))$ *acts regularly on* $P/Z(P))$ *if and only if* $|P| \leq p^{q+1}$. (*The use of* regularly *is as in* [DH, A.4.23].)

0021-8693/97 $25.00

Remark C. (a) The interest in this subject stems from an application of these theorems in the theory of Fitting classes. In a variation of a result of Trevor Hawkes (see [DH, IX.6.19]), the following is shown in [Wo]:

> Let P be a p-group of maximal class with $|P| \leq p^{q+1}$ and q an odd prime such that $q \mid (p-1)$. If α is an automorphism of P of order q with $[Z(P), \alpha] = 1$ and $G = P\langle \alpha \rangle$ denotes the semidirect product, then the smallest Fitting class containing G consists only of supersoluble groups, but is not contained in the class of nilpotent groups.

(b) It is known, that p-groups P of maximal class need not have any p'-automorphism (see, for example, [CaSco90]), so it is no surprise that usually $C_H(Z(P))$ is not too big, where H is a Hall p'-subgroup of the automorphism group of P. However, there are two families of p-groups of maximal class with $|H| = (p-1)^2$, such that for Theorems A and B and part (a) of this remark, nontrivial examples exist:

(i) the p-groups of maximal class of exponent p with an abelian maximal subgroup (see, for instance, [BaWoe76]);

(ii) the p-groups of maximal class constructed by Blackburn (see [Hu, III.14.24] and [Hart84]), which are extensions of an extraspecial p-group by a group of order p (that $|H| = (p-1)^2$ in this case is shown in [Wo]).

PRELIMINARIES

A p-group P of order p^n with $n \geq 2$ and nilpotency class $n-1$ is said to be of maximal class. The cornerstone in the theory of p-groups of maximal class is the paper by Blackburn [Bb58] (see also Huppert's book [Hu, III.14]).

Consider a p-group P of maximal class with $p \geq 3$ and $n \geq 4$. Let $1 = P_n \lhd P_{n-1} \lhd \cdots \lhd P_2 \lhd P$ be the lower central series of P. It is customary to set $P_1 = C_P(P_2/P_4)$. This subgroup of index p plays a fundamental role in the study of these groups. The degree of commutativity of P is the largest integer l, such that $[P_i, P_j] \leq P_{i+j+l}$ for all $i, j \geq 1$, unless P_1 is abelian, in which case $l = n-3$. If P_1 is not abelian, then the degree of commutativity of P is $\geq l$ if and only if $[P_1, P_i] \leq P_{i+1+l}$ for all $i \geq 1$ (see [Hart84]).

A p-group P of maximal class is called *exceptional* if the degree of commutativity is zero. One of the main results of Blackburn's paper is the following.

THEOREM D (Blackburn [Hu, III.14.6]). *Let P be a p-group of maximal class with $|P| = p^n$ and $n \geq 5$. Then*

(i) *P/P_{n-1} is not exceptional and $P_1 = C_P(P_i/P_{i+2})$ for $i \leq n-3$.*

(ii) *If P is exceptional, then $p > 3$ and $6 \leq n \leq p+1$; also n is even and $P_E = C_P(P_{n-2})$ is a characteristic subgroup of index p in P different from P_1.*

The following elementary lemma is fundamental:

LEMMA E. *Let P be a p-group of maximal class with $|P| = p^n$, $n \geq 4$. Then the automorphism group of P is soluble. If H is a Hall p'-subgroup of* Aut(P), *then one can choose elements, $s, s_1 \in P$ with the following properties*:

(i) *$P = \langle s, P_1 \rangle$. If P is exceptional, so $P_E = C_P(P_{n-2}) = \langle s, P_2 \rangle$ and $P_1 = \langle s_1, P_2 \rangle$. Set $s_i = [s_{i-1}, s]$ for $i = 2, \ldots, n-2$ and*

$$s_{n-1} := \begin{cases} [s_{n-2}, s], & \text{if } P \text{ is not exceptional}, \\ [s_{n-2}, s_1], & \text{if } P \text{ is exceptional}. \end{cases}$$

Then

$$P = \langle s, s_1 \rangle \quad \text{and} \quad P_i = \langle s_i, P_{i+1} \rangle \qquad \text{for } i = 1, \ldots, n-1,$$
$$Z(P) = \langle s_{n-1} \rangle.$$

(ii) *For $\alpha \in H$ there exists $a, c \in \mathrm{GF}(p)$ with*

$$s\alpha = s^a \bmod P_2 \quad \text{and} \quad s_1\alpha \equiv s_1^c \bmod P_2$$

such that

$$\mu: H \to D,$$
$$\alpha \mapsto (a, c),$$

is a monomorphism, where D is a direct product of two copies of the multiplicative group of $\mathrm{GF}(p)$. $|H| \mid (p-1)^2$. *Furthermore,*

$$s_i\alpha \equiv s_i^{a^{i-1} \cdot c} \bmod P_{i+1} \qquad \text{for } i = 2, 3, \ldots, n-2.$$

The operation on $Z(P)$ depends on whether P is exceptional or not:

$(Z\cdot)$ *If P is not exceptional, then*

$$(s_{n-1})\alpha = s_{n-1}^{a^{n-2} \cdot c}.$$

$[Z(P), \alpha] = 1$ *if and only if* $a^{n-2} \cdot c = 1 \in \mathrm{GF}(p)$.

$(Z \cdot \cdot)$ *If P is exceptional, then*

$$(s_{n-1})\alpha = s_{n-1}^{a^{n-3} \cdot c^2}.$$

$[Z(P), \alpha] = 1$ *if and only if* $a^{n-3} \cdot c^2 = 1 \in \mathrm{GF}(p)$.

Remark. In other contexts it is convenient to choose $s \in P \setminus \{P_1 \cup C_P(P_{n-2})\}$. It should be clear that in dealing with p'-automorphisms the choice in (i) is appropriate.

Proof of Lemma E. $|P/P_2| = |P/\Phi(P)| = p^2$ since P is of maximal class. So $C_{\mathrm{Aut}(P)}(P/P_2)$ is a p-group (see [Hu, III.3.18]). P_1 is a characteristic subgroup of P. Therefore P_1/P_2 is invariant under $\mathrm{Aut}(P)$ and $\mathrm{Aut}(P)/C_{\mathrm{Aut}(P)}(P/P_2)$ is isomorphic to a subgroup of the upper triangular matrices in $\mathrm{GL}(2, p)$. This shows the solubility of $\mathrm{Aut}(P)$. Let H be a Hall p'-subgroup of $\mathrm{Aut}(P)$. Obviously $|H| \mid (p-1)^2$. P_1/P_2 is H-invariant. By Maschke's theorem there exists an H-invariant one-dimensional complement S/P_2 to P_1/P_2. Choose $s, s_1 \in P$ such that $S = \langle s, P_2 \rangle$ and $P_1 = \langle s_1, P_2 \rangle$. With this choice in mind the rest of (i) and (ii) are easy consequences. ∎

Proof of Theorem A. Assume that P is exceptional (the other case, i.e., P is not exceptional, can be treated in a similar way). Let $s, s_1 \in P$ and μ: $H \mapsto D$ be as in the last Lemma. Let D operate on a cyclic group $X = \langle x \rangle$ of order p following $(Z \cdot \cdot)$ from Lemma E:

$$x \mapsto x^d = x^{a^{n-3} \cdot c^2} \qquad \text{for } d = (a, c) \in D.$$

Notice that n is even and $6 \leq n \leq p+1$ since P is exceptional.

Then $(C_H(Z(P)))\mu \leq C_D(\langle x \rangle)$ and so it suffices to prove $|C_D(X)| = p - 1$.

Because D is abelian, one only needs to show that each Sylow q-subgroup Q of $C_D(X)$ is a cyclic group of order q^k, where $q^k \,\|\, (p-1)$.

q odd: Let q be an odd prime dividing $p-1$ with $q^k \,\|\, (p-1)$ and let Q be a Sylow q-subgroup of D. Let y denote a primitive q^kth root of unity in $\mathrm{GF}(p)$. Let

$$d = (y^v, y^w) \in Q.$$

Assume $d \in C_D(X)$. This is equivalent to

$$x^{(y^v)^{n-3} \cdot (y^w)^2} = x \quad \text{or} \quad y^{v(n-3)+2w} = 1 \in \mathrm{GF}(p)$$

and

$$(n-3) \cdot v + 2 \cdot w \equiv 0 \bmod q^k.$$

Especially with $v = 1$, $w_1 = \frac{1}{2}(q^k - n + 3)$ it follows that

$$d_1 := (y, y^{w_1}) \in C_Q(X).$$

The order of d_1 is q^k and so $\langle d_1 \rangle = Q_1 \leq C_Q(X)$.

With $v_2 = 1$, $w_2 = (4 - n)/2$, and

$$d_2 := (y, y^{w_2}),$$

it follows that

$$(n - 3) \cdot v_2 + 2 \cdot w_2 \equiv 1 \bmod q^k.$$

Therefore $x^{d_2} = x^y$ and $x^{d_2^i} = x^{y^i}$ for $i = 1, \ldots, q^k$. So the cyclic group $Q_2 = \langle d_2 \rangle$ is of order q^k. As a consequence of the construction of Q_2,

$$Q_2 \cap C_Q(X) = 1.$$

However, Q is abelian and so $Q = Q_1 \times Q_2$. This shows $Q_1 = C_Q(X)$ and $|Q_1| = q^k$.

$q = 2$: Now $q = 2$ and $2^k \,||\, (p - 1)$. Let Q be a Sylow 2-subgroup of the abelian group D. Set $S := \mathrm{Soc}_2(Q)$. The first step is to show that the group $C_S(X)$ is a cyclic group of order 2. This has as an immediate consequence, that $C_Q(X)$ is cyclic, since Q is abelian.

For $d = (a, c) \in S$ with $a, c \in \{1, -1\}$,

$$x^d = x \text{ is equivalent to } x^{a^{n-3} \cdot c^2} = x.$$

Since n is even and $(n - 3)$ is odd it follows that the only nontrivial solution of this equation for $a, c \in \{1, -1\}$ is given with $a = 1$ and $c = -1$. Therefore, $|C_S(X)| = 2$. It remains to show, that $|C_Q(X)| = 2^k$.

Let $y \in \mathrm{GF}(p)$ denote a primitive 2^kth root of unity in $\mathrm{GF}(p)$. Let

$$d := (y^v, y^w) \in Q \qquad \text{with integers } v, w.$$

Count the number of different solutions of

$$x^d = x, \qquad \text{respectively, } x^{(y^v)^{n-3} \cdot (y^w)^2} = x.$$

This is equivalent to

$$y^{v(n-3) + 2w} = 1 \in \mathrm{GF}(p)$$

and

$$2 \cdot w \equiv -(n - 3) \cdot v \bmod 2^k.$$

Count for each v with $0 \leq v < 2^k$ the number of different solutions of this linear congruence. It is $(n-3)$ odd. Therefore, if v is odd, this congruence has no solution; otherwise, if v is even, it has exactly. $(2, 2^k) = 2$ different solutions. So the number of different solutions of this linear congruence is 2^k. This shows $|C_Q(X)| = 2^k$. ∎

LEMMA F. *Let P be a p-group of maximal class with $|P| = p^n$, $n \geq 4$. Let H be a Hall p'-subgroup of the automorphism group of P. Let $s, s_1 \in P$ and $\mu\colon H \to D$ be as in Lemma* E. *If $\alpha \in C_H(Z(P))$ is of odd order and*

$$(\alpha)\mu = (a, c)$$

or

$$s\alpha \equiv s^a \bmod P_2 \quad \textit{and} \quad s_1\alpha \equiv s_1^c \bmod P_2,$$

then the multiplicative order of a in $\mathrm{GF}(p)$ *is the same as the order of α. In particular, if $|\alpha| = q$ for an odd prime q, then a is a primitive qth root of unity in* $\mathrm{GF}(p)$ *and $c = a^r$ for an integer r.*

Proof. Let $\alpha \in H$ be an element of order q for an odd prime q with $[Z(P), \alpha] = 1$ and $s\alpha = s^a \bmod P_2$. Then $a \neq 1 \in \mathrm{GF}(p)$. Assume not. Then $c \neq 1$, since α is a nontrivial p'-automorphism.

(i) If P is not exceptional it follows from Lemma E with $(Z\,\cdot\,)$ that

$$(s_{n-1})\alpha = s_{n-1}^c \neq s_{n-1},$$

since $c \neq 1$. However, this contradicts $[Z(P), \alpha] = 1$.

(ii) If P is exceptional it follows from $(Z\,\cdot\,\cdot\,)$ in Lemma E that

$$(s_{n-1})\alpha = s_{n-1}^{c^2} \neq s_{n-1},$$

since $c \neq 1$ and α is of odd order. Again this contradicts $[Z(P), \alpha] = 1$.

Therefore $\alpha \neq 1$. The same argument for each $i \in \{1, \ldots, q-1\}$ yields $a^i \neq 1$ and so a is a primitive qth root of unity in $\mathrm{GF}(p)$, since the order of α is q. Therefore $c = a^r$ for some integer r.

Now let $\alpha \in C_H(Z(P))$ be an element of odd order m. Assume $s\alpha \equiv s^a \bmod P_2$ and the multiplicative order of a in $\mathrm{GF}(p)$ is $t < m$. Then t divides m and $\alpha^t \in C_{\mathrm{Aut}(P)}(sP_2)$. As a consequence an odd prime q dividing m/t exists, such that $\beta := \alpha^{m/q}$ is a nontrivial automorphism of P of order q centralizing the center of P. From $t \mid (m/q)$ it follows with an appropriate integer k that

$$\beta = \alpha^{m/q} = \alpha^{tk} = (\alpha^t)^k \in C_{\mathrm{Aut}(P)}(sP_2).$$

However, this is a contradiction. This shows that the multiplicative order of a in $GF(p)$ is m. ∎

Proof of Theorem B. Part (i) of this theorem is an immediate consequence of Theorem A.

Assume $|C_R(Z(P))| = q$ in a first step for part (ii). Let $1 \neq \alpha \in C_R(Z(P))$. With Lemmata E and F one has

$$s\alpha \equiv s^y \bmod P_2 \quad \text{and} \quad s_1\alpha \equiv s_1^{y^w} \bmod P_2,$$

where y is an qth root of unity and $w \in \{0, \dots, q-1\}$. From Lemma E one gets, for $i = 2, \dots, n-2$,

$$s_i\alpha \equiv s_i^{y^{i-1+w}} \bmod P_{i+1}.$$

(a) If $n > q + 1$, then α has a fixed point on $P/Z(P)$ and so $C_R(Z(P))$ does not act regularly on $P/Z(P)$: It is $n - 2 > q - 1$. Therefore, $i_0 \in \{1, \dots, n-2\}$ exists with $i_0 - 1 \equiv -w \bmod q$ and so $s_{i_0}\alpha \equiv s_{i_0} \bmod P_{i_0+1}$. This essentially shows with [Hu, I.18.6] that α has a fixed point on $P/Z(P)$.

(b) If $n \leq q + 1$, then α has no fixed points on $P/Z(P)$ and so $C_R(Z(P))$ acts regularly on $P/Z(P)$: There are two cases to examine.

(i) Let P be not exceptional. From $(Z\,\cdot\,)$ (Lemma E) one gets

$$y^{n-2+w} = 1 \in GF(p).$$

This is equivalent to

$$n - 2 + w \equiv 0 \bmod q$$

and this congruence determines w.

For $i \in \{1, 2, \dots, n-2\}$ it follows that

$$i - 1 + w \equiv -(n - 1 - i) \bmod q.$$

It is

$$n - 1 - i \in \{1, 2, \dots, n-2\} \subseteq \{1, 2, \dots, q-1\},$$

since $n \leq q + 1$. Therefore $i - 1 + w \not\equiv 0 \bmod q$ for $i = 1, 2, \dots, n-2$ and

$$s_i\alpha \equiv s_i^{y^{i-1+w}} \not\equiv s_i \bmod P_{i+1} \qquad \text{for } i = 1, 2, \dots, n-2.$$

Furthermore, $s\alpha \equiv s^y \not\equiv s \bmod P_2$. So α has no fixed points on every section of the lower central series of $P/Z(P)$ and as an immediate consequence no fix points on $P/Z(P)$.

(ii) Let P be exceptional. From Blackburn's Theorem D it follows that $n \geq 6$ and n is even. With Lemma E $(Z \cdot \cdot)$ one gets

$$y^{n-3+2w} = 1 \in \mathrm{GF}(p).$$

This is equivalent to

$$n - 3 + 2w \equiv 0 \bmod q$$

and this congruence determines w.

Assume

$$n - i_0 - 2 + w \equiv 0 \bmod q$$

for an appropriate $i_0 \in \{1, 2, \ldots, n-2\}$. Therefore $w \equiv -n + i_0 + 2 \bmod q$. Since $\alpha \in C_R(Z(P))$ it follows from $(Z \cdot \cdot)$ in Lemma E that

$$n - 3 + 2w \equiv 0 \bmod q$$

and

$$(\star) \qquad n - 3 + 2(-n + i_0 + 2) \equiv -n + 1 + 2i_0 \equiv 0 \bmod q.$$

It is $n - 3 < q$, since $n \leq q + 1$. Therefore one gets, with $1 \leq i_0 \leq n - 2$,

$$-q < -n + 3 \leq -n + 1 + 2i_0 \leq -n + 1 + 2(n-2) = n - 3 < q.$$

To fulfill $(\star)$ it is necessary that $-n + 2i_0 + 1 = 0$. However, n is even and so $-n + 2i_0 + 1 \neq 0$. This contradicts $(\star)$. This contradiction shows

$$n - i_0 - 2 + w \not\equiv 0 \bmod q.$$

Therefore α has no fixed points on every section of the lower central series of $P/Z(P)$ and as an immediate consequence no fixed points on $P/Z(P)$.

Now it remains to prove in the case $n \leq q + 1$ and $|C_R(Z(P))| > q$ that $C_R(Z(P))$ acts regularly on $P/Z(P)$. By (i), $C_R(Z(P))$ is cyclic. From the first part of the proof it follows that $\mathrm{Soc}(C_R(Z(P)))$ acts regularly on $P/Z(P)$.

Let $C_R(Z(P)) = \langle \alpha \rangle$ with $|\langle \alpha \rangle| = q^t > q$. Assume, that $m \not\equiv 0 \bmod (q^t)$ exists, such that α^m has a fixed point $x_0 Z(P) \neq Z(P)$ on $P/Z(P)$. Then $1 \neq (\alpha^m)^r \in C_R(Z(P))$ is an element of order q for some appropriate r with fixed point $x_0 Z(P) \neq Z(P)$. However, this is a contradiction ∎

REFERENCES

[BaWoe76] A. H. Baartmans and J. J. Woeppel, The automorphism group of a p-group of maximal class with an abelian maximal subgroup, *Fund. Math.* **93** (1976), 41–46

[Bb58] N. Blackburn, On a special class of p-groups, *Acta Math.* **100** (1958), 45–92

[CaSco90] A. Caranti and C. M. Scoppola, A remark on the orders of p-groups that are automorphism groups, *Boll. Un. Mat. Ital. A*(7) **4** (1990), 201–207

[DH] K. Doerk and T. O. Hawkes, "Finite Soluble Groups," de Gruyter Verlag, Berlin, 1992

[Hart84] B. Hartley, Topics in the theory of nilpotent groups, "Group Theory, Essays for Philip Hall," pp. 61–120, Academic Press, London, 1984.

[Hu] B. Huppert, "Endliche Gruppen I," Springer-Verlag, Berlin, 1967

[Wo] B. Wolf, Überauflösbare Fittingklassen, die durch gewisse Erweiterungen von p-Gruppen von maximaler Klasse erzeugt werden, Dissertation, Universität Mainz, 1994