ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 2, Number 2, Spring 1972

THE AUTOMORPHISM GROUP OF AN EXTRASPECIAL p-GROUP

DAVID L. WINTER

1. Let p be a prime. The finite p-group P is called special if either (i) P is elementary abelian or (ii) the center, commutator subgroup and Frattini subgroup of P all coincide and are elementary abelian. A nonabelian special p-group whose center has order p is called an extraspecial p-group. It is possible to give a uniform treatment of the subject of automorphisms for all the possible isomorphism types of extraspecial p-groups and so some cases that are more or less known are included here. The result when p is odd and P has exponent p^2 leads to an interesting subgroup of the symplectic group $\mathrm{Sp}(2n, q)$, q a power of p, $n > 1$. This subgroup is the semidirect product of $\mathrm{Sp}(2n-2, q)$ and a normal special p-group of order q^{2n-1} whose center has order q.

THEOREM 1. *Let p be a prime and let P be an extraspecial p-group of order p^{2n+1}. Let I be the group of inner automorphisms and let H be the normal subgroup of* $\mathrm{Aut}\,P$ *consisting of all elements of* $\mathrm{Aut}\,P$ *which act trivially on $Z(P)$. Then* $\mathrm{Aut}\,P = \langle \theta \rangle H$ *where θ has order $p-1$, $H \cap \langle \theta \rangle = \langle 1 \rangle$ and H/I is isomorphic to a subgroup of* $\mathrm{Sp}(2n, p)$. *Furthermore,*

(a) *If p is odd and P has exponent p, $H/I \cong \mathrm{Sp}(2n, p)$ of order $p^{n^2}\prod_{i=1}^{n}(p^{2i}-1)$.*

(b) *If p is odd and P has exponent p^2, H/I is the semidirect product of* $\mathrm{Sp}(2n-2, p)$ *and a normal extraspecial group of order p^{2n-1}. (If $n = 1$, H/I has order p.)*

(c) *If $p = 2$, H/I is isomorphic to the orthogonal group $O_\epsilon(2n, 2)$ of order $2^{n(n-1)+1}(2^n - \epsilon)\prod_{i=1}^{n-1}(2^{2i}-1)$. Here $\epsilon = 1$ if P is isomorphic to the central product of n dihedral groups of order 8 and $\epsilon = -1$ if P is isomorphic to the central product of $n-1$ dihedral groups of order 8 and a quaternion group.*

COROLLARY 1. *Let p be an odd prime and let P be an extraspecial p-group of exponent p^2. There is a nonidentity element of $P/Z(P)$ left fixed by every automorphism of P.*

Received by the editors June 16, 1970.
AMS 1970 *subject classifications.* Primary 20D45; Secondary 20F55, 20D05.

COROLLARY 2. *Let P be an extraspecial p-group of order p^{2n+1} and let ϕ be an automorphism of P which acts trivially on $Z(P)$ and irreducibly on $P/Z(P)$. Then the order of ϕ modulo I, the group of inner automorphisms, is a divisor of p^n+1. If p is odd, P has exponent p.*

2. As usual, Aut P denotes the automorphism group of P, $Z(P)$ the center of P. If $x \in P$, $\bar{x}$ means the coset $Z(P)x$. If a is a rational integer $\bar{a}$ means its image under the natural map of the integers onto $GF(p)$. Since P has class 2, for p odd,

$$(xy)^p = x^p y^p, \tag{2.1}$$

$x, y \in P$ [3, 5.3.9]. The terminology and concepts of symplectic spaces are taken from [1] and [4, II, §9]. The results on extraspecial p-groups stated below are from [3] and [4].

Let P be an extraspecial p-group. Then P has order p^{2n+1} for some positive integer n. P is the central product of n nonabelian subgroups of order p^3. In all cases, P has generators $x_1, \cdots, x_{2n}$ satisfying the following relations once a suitable generator z of $Z(P)$ is chosen.

$$[x_{2i-1}, x_{2i}] = z, \qquad i = 1, \cdots, n.$$

$$[x_j, x_k] = 1 \quad \textit{unless } \{j, k\} \textit{ is one of the pairs } \{2i-1, 2i\} \textit{ or}$$

$$\{2i, 2i-1\} \textit{ for some } i,\ 1 \leqq i \leqq n.$$

$$x_i^p \in \langle z \rangle \quad \textit{for all } i,\ z^p = 1.$$

If p is odd, there are two isomorphism classes; one with P of exponent p and one with P of exponent p^2. In the latter case, we may take x_1 of order p^2, x_i of order p if $i \neq 1$ and $x_1^p = z$ [3, 5.5.2].

If $p = 2$, P may be the central product of n dihedral groups of order 8 in which case we may take $x_{2i-1}^2 = x_{2i}^2 = 1$, $i = 1, \cdots, n$. If $p = 2$, the only other possibility is that P is isomorphic to the central product of $n-1$ dihedral groups of order 8 and a quaternion group. In this case, we take $x_{2i-1}^2 = x_{2i}^2 = 1$, $i = 1, \cdots, n-1$, $x_{2n-1}^2 = x_{2n}^2 = z$.

Let $x, y \in P$. If one sets $(\bar{x}, \bar{y}) = \bar{a}$ where $[x, y] = z^a$, $P/Z(P)$ becomes a nondegenerate symplectic space over $GF(p)$. The first two relations above may be expressed as $(\bar{x}_{2i-1}, \bar{x}_{2i}) = 1$, $i = 1, \cdots, n$, $(\bar{x}_j, \bar{x}_k) = 0$, unless $\{j, k\}$ is one of the pairs $\{2i-1, 2i\}$ or $\{2i, 2i-1\}$, $1 \leqq i \leqq n$.

If $p = 2$, we may also set $q(\bar{x}) = \bar{c}$ where $x^2 = z^c$ ($c = 0$ or 1). Then q is a quadratic form on $P/Z(P)$. If P is the central product of

n dihedral groups of order 8, then [4, III, §13]

$$(2.2)\qquad q(\bar{x}_1^{\xi_1}\bar{x}_2^{\xi_2}\cdots\bar{x}_{2n}^{\xi_{2n}}) = \xi_1\xi_2 + \cdots + \xi_{2n-1}\xi_{2n}.$$

If P is the central product of $n-1$ dihedral groups of order 8 and a quaternion group, then

$$(2.3)\qquad \begin{aligned} q(\bar{x}_1^{\xi_1}\bar{x}_2^{\xi_2}\cdots\bar{x}_{2n}^{\xi_{2n}}) = {} & \xi_1\xi_2 + \cdots + \xi_{2n-3}\xi_{2n-2} + \xi_{2n-1}^2 \\ & + \xi_{2n-1}\xi_{2n} + \xi_{2n}^2. \end{aligned}$$

These are precisely the two possible normal forms of a nondegenerate quadratic form over $GF(2)$ [2, Chapter VIII]. In both cases the quadratic form and the bilinear form are related by $q(\bar{x}\bar{y}) = q(\bar{x}) + q(\bar{y}) + (\bar{x}, \bar{y})$.

3. (3A) *Let $\phi \in \operatorname{Aut} P$. ϕ induces on $P/Z(P)$ an element of* $\operatorname{Sp}(2n, p)$ *if and only if ϕ acts trivially on* $Z(P)$. If $p = 2$, $q(\phi(\bar{x})) = q(\overline{\phi(x)}) = q(\bar{x})$ *for all $x \in P$.*

Proof. For $x, y \in P$, $(\phi(\bar{x}), \phi(\bar{y})) = (\overline{\phi(x)}, \overline{\phi(y)}) = (\bar{x}, \bar{y})$ if and only if $[x, y] = [\phi(x), \phi(y)] = \phi([x, y])$. Since $Z(P) = P'$, this proves the first assertion. If $p = 2$, the second follows since $\phi(x)^2 = \phi(x^2) = x^2$ for all $x \in P$.

From now on H denotes the subgroup of $\operatorname{Aut} P$ consisting of all members of $\operatorname{Aut} P$ which act trivially on $Z(P)$. If $\alpha \in \operatorname{Aut} P$ and $h \in H, (\alpha^{-1}h\alpha)(z) = \alpha^{-1}[h(\alpha(z))] = \alpha^{-1}[\alpha(z)] = z$. Hence, $H \lhd \operatorname{Aut} P$. Of course if $p = 2$, $\operatorname{Aut} P = H$.

(3B) *Let m be a primitive root* mod p *with* $0 < m < p$. *Let θ be defined by $\theta(x_{2i-1}) = x_{2i-1}^m$, $\theta(x_{2i}) = x_{2i}$, $i = 1, \cdots, n$, $\theta(z) = z^m$. Then θ can be extended to an automorphism of P of order $p-1$. Furthermore,* $\operatorname{Aut} P = \langle\theta\rangle H$ *and* $\langle\theta\rangle \cap H = \langle 1\rangle$.

Proof. The first statement follows since $[x_{2i-1}^m, x_{2i}] = z^m$ (also if p is odd and P has exponent p^2, $x_1^{mp} = z^m$) and so x_{2i-1}^m, x_{2i}, z^m satisfy the same relations as x_{2i-1}, x_{2i}, z. That $\operatorname{Aut} P = \langle\theta\rangle H$ is also clear since if $\alpha \in \operatorname{Aut} P$, $\theta^a\alpha \in H$ for a suitable power a. From the definitions $\langle\theta\rangle \cap H = \langle 1\rangle$.

(3C) *The group M of all automorphisms which act trivially on both $Z(P)$ and $P/Z(P)$ is equal to the group I of inner automorphisms. It consists of the p^{2n} automorphisms ϕ determined by $\phi(x_i) = x_i z^{d_i}$, $\phi(z) = z$, $0 \leqq d_i < p$.*

Proof. Clearly I of order p^{2n} is contained in M. Each element of M must be determined by one of the p^{2n} functions mentioned in the lemma. All statements now follow.

(3D) *Each element of P can be expressed uniquely in the form* $(\prod_{i=1}^{2n} x_i^{a_i})\, z^c$, $0 \leqq a_i, c < p$.

PROOF. This is true because $\{\bar{x}_i\}_{i=1}^{2n}$ is a basis of the vector space $P/Z(P)$.

We now regard $\mathrm{Sp}(2n, p)$ as operating on $P/Z(P)$ and preserving the skew-symmetric bilinear form $(\bar{x}, \bar{y})$. Let $T \in \mathrm{Sp}(2n, p)$ and let $A = (\overline{a_{ij}})$ be the matrix of T relative to the basis $\{\bar{x}_i\}_{i=1}^{2n}$ where the a_{ij} are integers with $0 \leqq a_{ij} < p$ for all i and j. Define a function ϕ from P to P by

$$\phi(x) = \left[\prod_{i=1}^{2n} \left(\prod_{j=1}^{2n} x_j^{a_{ij}}\right)^{a_i}\right] z^c \tag{3.1}$$

where $(\prod_{i=1}^{2n} x_i^{a_i})z^c$, $0 \leqq a_i$, $c < p$, is the expression for x given in (3D). Call ϕ *the function determined by* T. ϕ is well defined, acts trivially on $Z(P)$ and induces T on $P/Z(P)$. Since T is nonsingular the range of ϕ generates P modulo $Z(P)$ so the range of ϕ generates P since $Z(P)$ is the Frattini subgroup. Therefore, ϕ is an automorphism of P if and only if ϕ preserves multiplication. In this direction it is immediate that

$$\phi(x_i^{a_i}) = \left(\prod_j x_j^{a_{ij}}\right)^{a_i} = \phi(x_i)^{a_i} \quad \text{and}$$
$$\phi\left(\left[\prod_{i=1}^{2n} x_i^{a_i}\right] z^c\right) = \left[\prod_{i=1}^{2n} \phi(x_i)^{a_i}\right] z^c \quad \text{for } 0 \leqq a_i, c < p. \tag{3.2}$$

Furthermore, $(\overline{\phi(x)}, \overline{\phi(y)}) = (T(\bar{x}), T(\bar{y})) = (\bar{x}, \bar{y})$. Hence

$$[\phi(x), \phi(y)] = [x, y] \quad \text{for all } x, y \in P. \tag{3.3}$$

(3E) *H/I is isomorphic to the subgroup G of* $\mathrm{Sp}(2n, p)$ *consisting of all transformations which determine automorphisms of P by* (3.1).

PROOF. By (3A) each $\phi \in H$ induces a transformation $T \in \mathrm{Sp}(2n, p)$ on $P/Z(P)$. The map $\phi \to T$ is a homomorphism of H into $\mathrm{Sp}(2n, p)$ whose kernel is I by (3C). The image of the homomorphism obviously contains the set G of all transformations which determine automorphisms of P. On the other hand, let T be the image of ϕ and let ϕ_1 be the function on P determined by T. We shall show that $\phi = \alpha\phi_1$ for some inner automorphism α.

Let $\phi(x_i) = (\prod_j x_j^{a_{ij}})z^{c_i}$, $0 \leqq a_{ij}$, $c_i < p$. Then the matrix of T relative to $\{\bar{x}_i\}$ is $(\overline{a_{ij}})$. There exists a unique set of integers $d_1, \cdots, d_{2n}$, $0 \leqq d_i < p$ such that $\sum_j a_{ij} d_j \equiv c_i \pmod p$, $i = 1, \cdots, 2n$. By (3C) there is an inner automorphism α such that $\alpha(x_i) = x_i z^{d_i}$, $i = 1, \cdots, 2n$. Let $x \in P$ and let $x = (\prod x_i^{a_i})z^c$, $0 \leqq a_i$, $c < p$. Then

$$(\alpha\phi_1)(x) = \alpha\Big(\Big[\prod_i \Big(\prod_j x_j^{a_{ij}}\Big)^{a_i}\Big] z^c \Big)$$
$$= \Big[\prod_i \Big(\prod_j \alpha(x_j)^{a_{ij}}\Big)^{a_i}\Big] z^c$$
$$= \Big[\prod_i \Big(\prod_j x_j^{a_{ij}} z^{a_{ij} d_j}\Big)^{a_i}\Big] z^c$$
$$= \Big[\prod_i \Big(\prod_j x_j^{a_{ij}}\Big)^{a_i} z^{a_i c_i}\Big] z^c.$$

Hence

$$\phi(x) = \phi\Big[\Big(\prod x_i^{a_i}\Big) z^c\Big]$$
$$= \Big[\prod_i \Big(\Big(\prod_j x_j^{a_{ij}}\Big) z^{c_i}\Big)^{a_i}\Big] z^c = (\alpha\phi_1)(x).$$

Therefore, $\phi_1 = \alpha^{-1}\phi$ is an automorphism and the image of H under the homomorphism is G. Thus G is a group and $H/I \cong G$.

(3F) *Let $T \in \mathrm{Sp}\,(2n, p)$ and let ϕ be the function on P determined by T. Then $\phi \in \mathrm{Aut}\, P$ if and only if $\phi(x_i)^p = x_i^p$, $i = 1, \cdots, 2n$.*

PROOF. Since ϕ acts trivially on $Z(P)$, the condition is necessary. Conversely, assume $\phi(x_i)^p = x_i^p = z^{\gamma_i}$, $0 \leqq \gamma_i < p$, $i = 1, \cdots, 2n$. Let

$$x = \Big(\prod_{i=1}^{2n} x_i^{a_i}\Big) z^{c_1}, \qquad y = \Big(\prod_{i=1}^{2n} x_i^{b_i}\Big) z^{c_2}, \quad 0 \leqq a_i, b_i, c_i < p.$$

We have

$$\prod_i x_i^{a_i} \prod_i x_i^{b_i} = \Big(\prod_{i=1}^{2n} x_i^{a_i+b_i}\Big) \prod_{j=1}^{2n-1} \prod_{k=j+1}^{2n} [x_k^{a_k}, x_j^{b_j}]$$
$$= \Big(\prod_{i=1}^{2n} x_i^{a_i+b_i}\Big) z^e$$

for some e. By (3.2) and (3.3),

$$\prod \phi(x_i)^{a_i} \prod \phi(x_i)^{b_i} = \Big[\prod \phi(x_i)^{a_i+b_i}\Big] z^e.$$

Thus, $\phi(xy) = \phi[(\prod x_i^{a_i+b_i}) z^{c_1+c_2+e}]$. Now set $a_i + b_i = r_i + \delta_i p$ and $c_1 + c_2 + e + \sum \gamma_i \delta_i = r + tp$ with $0 \leqq r_i$, $r < p$, $i = 1, \cdots, 2n$. Then $\phi(xy) = \phi[(\prod x_i^{r_i}) z^r] = [\prod \phi(x_i)^{r_i}] z^r$. On the other hand,

$$\begin{aligned}\phi(x)\phi(y) &= [\prod\phi(x_i)^{a_i}]\,[\prod\phi(x_i)^{b_i}]\,z^{c_1+c_2}\\ &= [\prod\phi(x_i)^{a_i+b_i}]\,z^{c_1+c_2+e}\\ &= [\prod\phi(x_i)^{r_i}]\,[\prod z^{\gamma_i\delta_i}]z^{c_1+c_2+e}.\end{aligned}$$

Hence, $\phi(xy) = \phi(x)\phi(y)$ as desired.

4. If p is odd and P has exponent p, the condition of (3F) is always satisfied. Therefore, in this case, $H/I \cong \mathrm{Sp}\,(2n, p)$.

If $p = 2$, the condition is $\phi(x_i)^2 = x_i^2$, $i = 1, \cdots, 2n$. This is equivalent to $q(\phi(\bar{x}_i)) = q(T(\bar{x}_i)) = q(\bar{x}_i)$ for all i. Thus the necessary condition $q(\phi(\bar{x})) = q(T(\bar{x})) = q(\bar{x})$ given by (3A) is also sufficient to guarantee that T determines an automorphism. Hence, H/I is the orthogonal group associated with the appropriate quadratic form (2.2) or (2.3). The orders as well as other properties of these groups have been given by Dickson [2, Chapter VIII].

Assume now that p is odd and P has exponent p^2. As stated in §2 we may take $x_1{}^p = z$, $x_i{}^p = 1$ for $i > 1$. Then $\phi(x_i)^p = (\prod_j x_j{}^{a_{ij}})^p = \prod_j x_j{}^{pa_{ij}} = z^{a_{i1}}$ by (2.1). Hence the group G of (3E) consists of all elements of $\mathrm{Sp}\,(2n, p)$ whose matrices relative to $\{\bar{x}_i\}$ satisfy $\bar{a}_{11} = 1$, $\bar{a}_{i1} = 0$ for $i > 1$. The structure of G can be studied in a more general context.

Let $q = p^r$ where p is any prime. Regard $\mathrm{Sp}\,(2n, q)$ as transformations of a nondegenerate symplectic space V over $GF(q)$ preserving its skew-symmetric form. Let $x_1, \cdots, x_{2n}$ be a basis of V such that x_{2i-1}, x_{2i} is a hyperbolic pair for $i = 1, \cdots, n$ and

$$V = \langle x_1, x_2\rangle \perp \cdots \perp \langle x_{2n-1}, x_{2n}\rangle.$$

By the matrix of a linear transformation of V we shall mean the matrix relative to this basis. Let L be the subgroup of $\mathrm{Sp}\,(2n, q)$ of all transformations whose matrices have first column $(1, 0, \cdots, 0)$.

(4A) *For all* $T \in L$, $T(x_2) = x_2$.

Proof. Let $T \in L$ and let $T(x_i) = y_i$, $i = 1, \cdots, 2n$. Since T is an isometry, $V = \langle y_1, y_2\rangle \perp \cdots \perp \langle y_{2n-1}, y_{2n}\rangle$. Let $H_1 = \langle y_1, y_2\rangle$ and let $H_1^\perp$ denote its orthogonal complement. Then by the definition of L,

$$H_1^\perp = \langle y_3, y_4\rangle \perp \cdots \perp \langle y_{2n-1}, y_{2n}\rangle \subset \langle x_2, x_3, \cdots, x_{2n}\rangle. \tag{4.1}$$

Let $A = (a_{ij})$ be the matrix of T and suppose $a_{22} = 0$. Then $(y_1, x_1 + a_{12}x_2) = (x_1 + \sum_{i=2}^{2n} a_{1i}x_i, x_1 + a_{12}x_2) = -a_{12} + a_{12} = 0$ and $(y_2, x_1 + a_{12}x_2) = (\sum_{j=3}^{2n} a_{2j}x_j, x_1 + a_{12}x_2) = 0$. Therefore $(x_1 + a_{12}x_2) \in H_1^\perp$, contrary to (4.1). Hence $a_{22} \neq 0$.

Now $\sum c_i x_i \in \langle y_2\rangle^\perp$ if and only if

$$\left(\sum_{j=2}^{2n} a_{2j}x_j, \sum c_i x_i\right) = -c_1 a_{22} + \sum_{i,j=2}^{2n} a_{2j}c_i(x_j, x_i)$$

$$= -c_1 a_{22} + \sum_{j=2}^{2n} \left[\sum_{t=1}^{n} a_{2j}c_{2t}(x_j, x_{2t}) + \sum_{t=2}^{n} a_{2j}c_{2t-1}(x_j, x_{2t-1})\right]$$

$$= -c_1 a_{22} + \sum_{t=2}^{n} (a_{2,2t-1}c_{2t} - a_{2,2t}c_{2t-1}) = 0,$$

since $a_{21} = 0$. Hence $\sum c_i x_i \in \langle y_2 \rangle^\perp$ if and only if

$$c_1 = \left[\sum_{t=2}^{n} (a_{2,2t-1}c_{2t} - a_{2,2t}c_{2t-1})\right] / a_{22}.$$

On the other hand, $\sum c_i x_i \in \langle y_1 \rangle^\perp$ if and only if

$$\left(x_1 + \sum_{j=2}^{2n} a_{1j}x_j, \sum c_i x_i \right)$$
$$= c_2 - c_1 a_{12} + \sum_{t=2}^{n} (a_{1,2t-1}c_{2t} - a_{1,2t}c_{2t-1}) = 0.$$

This implies $\sum c_i x_i \in H_1^\perp$ if $c_3, c_4, \cdots, c_{2n}$ are chosen arbitrarily and c_1 and c_2 are taken as indicated above. But by (4.1) we know $c_1 = 0$ always and this requires $a_{2i} = 0$ for $i > 2$. We already know $a_{21} = 0$ and since $(y_1, y_2) = 1 = (x_1 + \sum_{j=2}^{2n} a_{1j}, a_{22}x_2) = a_{22}$, (4A) is proved.

We note at this point that if $n = 1$, then L is isomorphic to the group of all matrices of the form

$$\begin{pmatrix} 1 & a_{12} \\ 0 & 1 \end{pmatrix}$$

and hence is an elementary abelian p-group of order q. From now on let $n > 1$ hold.

Each of the q^{2n-1} pairs y_1, y_2 with $y_1 = x_1 + \sum_{j=2}^{2n} a_{1j}x_j$, $y_2 = x_2$ is a hyperbolic pair and the set of these pairs is invariant under L. Suppose $T \in L$ fixes all of these pairs. Then T fixes the pairs x_1, x_2 and $x_1 + x_i$, x_2, $i > 2$, which implies T is the identity. Therefore L is a permutation group on these pairs.

If y_1, y_2 is one such pair, the map $T(x_1) = y_1$, $T(x_2) = y_2$ has an extension to an element $S \in \mathrm{Sp}\,(2n, q)$ by Witt's theorem [4, II, 9.9]. But for each $i > 2$, $S(x_i)$ is in the orthogonal complement of $\langle x_2 \rangle$ which is $\langle x_2, \cdots, x_{2n} \rangle$ and therefore $S \in L$. Hence L acts transitively on the pairs.

It follows that $|L| = q^{2n-1}|K|$ where K is the subgroup fixing the pair x_1, x_2. But each element of K yields an isometry of $\langle x_3, x_4, \cdots, x_{2n}\rangle$ by restriction and conversely each such isometry can be extended in a unique way to an element of K. Hence $K \cong \mathrm{Sp}\,(2n-2, q)$. Therefore

$$|L| = q^{2n-1}q^{(n-1)^2}\prod_{i=1}^{n-1}(q^{2i}-1)$$

$$= q^{n^2}\prod_{i=1}^{n-1}(q^{2i}-1).$$

The group of matrices of elements of K is the set of all matrices

$$R_B = \begin{pmatrix} 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & & & & & \\ \cdot & \cdot & & & & & \\ \cdot & \cdot & & & B & & \\ \cdot & \cdot & & & & & \\ 0 & 0 & & & & & \end{pmatrix}$$

where B is the matrix of an arbitrary element of $\mathrm{Sp}\,(2n-2, q)$ relative to the basis $x_3, x_4, \cdots, x_{2n}$.

Let S be the group of transformations whose matrices relative to $x_1, \cdots, x_{2n}$ have the form

$$C = \begin{pmatrix} 1 & a_{12} & a_{13} & \cdot & \cdot & \cdot & a_{1,2n} \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & a_{14} & & & & & \\ 0 & -a_{13} & & & & & \\ \cdot & \cdot & & & & & \\ \cdot & \cdot & & & I & & \\ \cdot & \cdot & & & & & \\ 0 & a_{1,2n} & & & & & \\ 0 & -a_{1,2n-1} & & & & & \end{pmatrix}$$

where I is the identity matrix of rank $2n-2$. Since

$$C^m = \begin{pmatrix} 1 & ma_{12} & ma_{13} & \cdots & ma_{1,2n} \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & ma_{14} & & & \\ 0 & -ma_{13} & & & \\ \cdot & \cdot & & & \\ \cdot & \cdot & & I & \\ \cdot & \cdot & & & \\ 0 & ma_{1,2n} & & & \\ 0 & -ma_{1,2n-1} & & & \end{pmatrix}$$

S has exponent p. If p is odd, it is easily verified that S is a special p-group of order q^{2n-1} whose center has order q. If $p = 2$, S is elementary abelian. Clearly $K \cap S = \langle 1 \rangle$ and from the group orders $L = KS$.

Computing with the matrices above, we have

$$R_B{}^{-1} C R_B = \begin{pmatrix} 1 & a_{12} & (a_{13}, \cdots, a_{1,2n})\, B \\ 0 & 1 & 0 \cdots 0 \\ 0 & & \\ \cdot & B^{-1} \begin{pmatrix} a_{14} \\ -a_{13} \\ \cdot \\ \cdot \\ \cdot \\ -a_{2n-1} \end{pmatrix} & I \\ \cdot & & \\ \cdot & & \\ 0 & & \end{pmatrix}.$$

This shows that $S \lhd L$. This completes the proof of Theorem 1.

PROOF OF COROLLARY 1. For a coset decomposition of H relative to I we may write $H = \bigcup I\phi_i$ where ϕ_i runs over all automorphisms of P which are determined by transformations in G (refer to (3E)). If p is odd and P has exponent p^2, we have seen that $\phi_i(\bar{x}_2) = \bar{x}_2$ for each such ϕ_i. Thus $\phi(\bar{x}_2) = \bar{x}_2$ for all $\phi \in H$ and the same is true for all $\phi \in \operatorname{Aut} P$ by (3B).

PROOF OF COROLLARY 2. Let ϕ satisfy the hypotheses of Corollary 2. Then $\phi \in H$ and from the preceding paragraph $\phi = \alpha\phi_i$ where α is an inner automorphism and ϕ_i is an automorphism of P determined by some $T \in \mathrm{Sp}\,(2n, p)$. Thus the action of ϕ on $P/Z(P)$ is the same as T on $P/Z(P)$. Hence $\langle T \rangle$ acts irreducibly on $P/Z(P)$ and by [4, II, 9.23] if the order of T is m, $m \mid (p^n + 1)$. This m is the least positive integer such that ϕ^m acts trivially on $P/Z(P)$ and hence by (3C) the least positive integer such that $\phi^m \in I$.

If p is odd, P cannot have exponent p^2 by Corollary 1.

REFERENCES

1. E. Artin, *Geometric algebra*, Interscience, New York, 1957. MR **18**, 553.

2. L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York, 1958. MR **21** #3488.

3. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968. MR **38** #229.

4. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR **37** #302.

MICHIGAN STATE UNIVERSITY, EAST LANSING, MICHIGAN 48823