OUTER AUTOMORPHISMS OF CERTAIN p-GROUPS[1]

CHARLES GODINO

Introduction. By employing methods of Group Representation Theory, the main theorems in this paper establish the existence of outer automorphisms of certain types of p-groups. There is no doubt that the results obtained in §3 can also be obtained by familiar group theoretic techniques. However, the author feels that the representation theory approach to the problem is an interesting one in itself and is worthy of being explored. Finally, *throughout* this paper, we consider only *finite* groups.

1. Certain types of automorphisms of p-groups.

THEOREM 1.1. *Let G be a p-group, $p \neq 2$. Let $\rho^*(G)$ be a faithful representation[2] of G as a linear group having coefficient field $R(\epsilon)$ where R is the rational field and ϵ is a primitive p^nth root of unity. Suppose the center of $\rho^*(G)$ contains scalar matrices and suppose the maximal order among these scalar matrices is p^m where $m \leqq n$. Let ϕ be a linear character of G which maps G into the field of p^mth roots of unity and let $\bar{\phi}$ be the linear character conjugate to ϕ. Then, at least one of the mappings defined by $\alpha: \rho^*(g) \to \rho^*(g)\phi(g)$ for every $g \in G$, $\beta: \rho^*(g) \to \rho^*(g)\bar{\phi}(g)$ for every $g \in G$, determines an automorphism of G. (This automorphism of G will henceforth be called an automorphism of the $G \to G\phi$ type or of the $G \to G\bar{\phi}$ type.)*

PROOF. The proof is clear that both α and β are homomorphisms since $\rho^*(G)$ can be decomposed into cosets with respect to its center and order $\phi \leqq p^m$ implies the matrix $\phi(g)I$ is a scalar matrix in the center of $\rho^*(G)$ for every $g \in G$. Also, since order $\phi =$ order $\bar{\phi}$, the matrix $\bar{\phi}(g)I$ is a scalar matrix in the center of $\rho^*(G)$ for every $g \in G$.

Since our coefficient field is $R(\epsilon)$, it is clear that the scalar matrices in the center of $\rho^*(G)$ form a cyclic subgroup and this group is generated by the element $\epsilon^{p^{n-m}}I$. Denote this group by S and let $\mu = \epsilon^{p^{n-m}}$. Then order $\mu = p^m$ and μI generates S. In addition, order $\phi \leqq p^m$ implies for every $g \in G$, $\phi(g) = \mu^s$ where $0 \leqq s < p^m$.

Received by the editors February 10, 1963 and, in revised form, July 5, 1964.

[1] This paper is a revision of part of the author's Doctoral dissertation written at the University of Notre Dame under the direction of K. M. Kronstein.

[2] In the remainder of this paper, the expression "faithful representation of G" will always carry the same meaning as described here.

Now, to prove that either α or β is an automorphism, we must show that at least one of them has a trivial kernel. Let K_α and K_β denote the respective kernels. If $K_\alpha = I$, we are done. If $K_\alpha \neq I$, then there exists an element $g \in G$, $g \neq 1$, such that $\rho^*(g)\alpha = \rho^*(g)\phi(g) = I$. Hence, $\rho^*(g) = (\phi(g))^{-1} I = \phi(g^{-1})I$ and $\rho^*(g)$ must be a scalar matrix in S. Therefore, $K_\alpha \subseteq S$.

Case 1. $K_\alpha = S$. Then $(\mu I)\alpha = (\mu I)\phi(\mu I) = I$. This implies $\phi(\mu I) = \mu^{-1}$. Consequently, for any r, $0 \leqq r < p^m$, we have $(\mu^r I)\alpha = I$. Now, the conjugate character $\bar{\phi}$ must have the property that $\bar{\phi}(\mu I) = \mu$, since $\bar{\phi}(g) = \phi(g^{-1})$ for every $g \in G$. Therefore, $(\mu I)\beta = \mu^2 I \neq I$ since $p \neq 2$ implies no element can have order 2.

Now, if $K_\beta \neq I$, then we know $K_\beta \subseteq S$ (by an argument similar to the one used previously for K_α). Suppose for some r, $0 < r < p^m$, we have $(\mu^r I)\beta = (\mu^r I)\bar{\phi}(\mu^r I) = I$. This implies that $\bar{\phi}(\mu^r I) = \mu^{-r}$. However, $\bar{\phi}(\mu I) = \mu$ implies $\bar{\phi}(\mu^r I) = \mu^r$. Therefore, $\mu^r = \mu^{-r}$ and μ^r has order 2 which is impossible. Hence, $K_\beta = I$ and β is an automorphism. In fact, since β moves a central element, it must be an *outer* automorphism.

Case 2. $K_\alpha \neq S$. K_α is therefore a proper subgroup of the cyclic group S and must be generated by an element μ^{p^t} where $0 < t < m$ and $\phi(\mu^{p^t} I) = \mu^{-p^t}$. This implies that $\bar{\phi}(\mu^{p^t} I) = \phi(\mu^{-p^t} I) = \mu^{p^t}$ and so $(\mu^{p^t} I)\beta = \mu^{2p^t} I \neq I$ since order $\mu^{p^t} \neq 2$.

Now, if $K_\beta \neq I$, then K_β, which is also a subgroup of S, has a generator $\mu^r I$ where $0 < r < p^m$. Hence $(\mu^r I)\beta = I$ and this implies $\bar{\phi}(\mu^r I) = \mu^{-r}$. Now, if $(r, p) = 1$, then $\mu^r I$ generates S which implies $\bar{\phi}(\mu I) = \mu^{-1}$ and therefore $\bar{\phi}(\mu^{p^t} I) = \mu^{-p^t}$. But this means $\mu^{p^t} = \mu^{-p^t}$ which is impossible. If $(r, p) \neq 1$, then $r = p^w$ where $0 < w < m$. In this event, we have $\bar{\phi}(\mu^{p^t} I) = \mu^{p^t}$ and $\bar{\phi}(\mu^{p^w} I) = \mu^{-p^w}$. We shall show that the latter equation is incompatible with the former.

If $w = t$, then $\mu^{p^t} = \mu^{-p^t}$ which is impossible. If $w > t$, then $\mu^{p^w} I$ is in the subgroup of S generated by $\mu^{p^t} I$. Therefore, $\bar{\phi}(\mu^{p^w} I) = \mu^{p^w}$ which contradicts the statement that $\bar{\phi}(\mu^{p^w} I) = \mu^{-p^w}$. If $w < t$, then $\mu^{p^t} I$ is in the subgroup of S generated by $\mu^{p^w} I$. Therefore, $\bar{\phi}(\mu^{p^t} I) = \mu^{-p^t}$ which contradicts the statement that $\bar{\phi}(\mu^{p^t} I) = \mu^{p^t}$. Therefore, $K_\beta = I$ and β is an *outer* automorphism.

We conclude with one remark. *If the center of G is contained in the commutator subgroup of G, then $\phi(z) = \bar{\phi}(z) = 1$ for every z in the center of G and both α and β will be automorphisms.*

In the following, G is a finite p-group with a minimal generating system $x_1, x_2, \cdots, x_n$, with commutator subgroup G', center Z and Frattini subgroup D. For each i, let p^{d_i} equal the relative order of x_i modulo G'. Then, every element g in G can be uniquely expressed as

a product, $g=\prod_{i=1}^{n} x_i^{\beta_i} g'$ where $g' \in G'$ and for each i, $0 \leqq \beta_i < p^{d_i}$.

THEOREM 1.2. *Let z be an element of $Z \cap D$ with $o(z) \leqq p^{d_1}$. Then, the mapping*

$$\alpha: \quad \prod_{i=1}^{n} x_i^{\beta_i} g' \rightarrow (x_1 z)^{\beta_1} \prod_{i=2}^{n} x_i^{\beta_i} g'$$

is an automorphism of G.

PROOF. It is clear from the definition of α, that $g'\alpha = g'$ for every $g' \in G'$ and that the effect of α on the generating system of G is:

$$\alpha: \quad \begin{aligned} &x_1 \rightarrow x_1 z, \\ &x_i \rightarrow x_i \qquad \text{for } i \neq 1. \end{aligned}$$

Throughout the remainder of this paper, this notation will be used whenever we mean the mapping α defined in the hypothesis.

The actual details of the proof are fairly routine and hence are omitted.

COROLLARY. *If in the preceding Theorem, we choose $z \in Z \cap D$ such that $o(z) \leqq p^{d_i}$ for $i = 1, 2, 3, \cdots, m$, where $2 \leqq m \leqq n$, then*

$$\alpha: \quad \begin{aligned} &x_i \rightarrow x_i z \qquad \text{for } i = 1, 2, 3, \cdots, m, \\ &x_i \rightarrow x_i \qquad \text{for } i > m, \end{aligned}$$

is an automorphism of G.

2. **Main results.** *In what follows, $\rho^*(G)$ is a faithful representation of a p-group G, $p \neq 2$, the center of $\rho^*(G)$ contains scalar matrices and ϵI is a scalar matrix of maximal order p^m in the center of $\rho^*(G)$.*

THEOREM 2.1. *Let ϕ be a linear character of G which maps G into the field of p^mth roots of unity. Then, at least one of the mappings $\alpha: G \rightarrow G\phi$, $\beta: G \rightarrow G\bar{\phi}$ determines an outer automorphism of G provided there exists $h \in G$ such that* (1) $\operatorname{Tr} \rho^*(h) \neq 0$ *and* (2) $\phi(h) \neq 1$.

PROOF. It is clear from Theorem 1.1 that either α or β is an automorphism of G. Suppose α is an automorphism. Then under α, $\rho^*(h)$ is mapped to $\rho^*(h)\phi(h)$. But conditions (1) and (2) imply that $\operatorname{Tr} \rho^*(h) \neq \operatorname{Tr}(\rho^*(h)\phi(h))$. Hence $\rho^*(h)$ is *not* conjugate to $\rho^*(h)\phi(h)$ and α must be outer. Now, if β is an automorphism, it must be outer since $\phi(h) \neq 1$ implies that $\bar{\phi}(h) \neq 1$ and, therefore, $\rho^*(h)$ is *not* conjugate to $\rho^*(h)\bar{\phi}(h)$.

COROLLARY 1. *If* (1) $\operatorname{Tr} \rho^* \not\equiv 0$ *outside G' and* (2) $\exp G/G' \leqq p^m$,

then G has an outer automorphism of the type $G \to G\phi$ or $G \to G\bar{\phi}$.

PROOF. By condition (1), there exists $h \in G$, $h \notin G'$ such that $\operatorname{Tr} \rho^*(h) \neq 0$. Now G' is the intersection of the kernels of all the linear characters of G, hence $h \notin G'$ implies there exists a linear character ϕ of G such that $\phi(h) \neq 1$. But by condition (2), the order of ϕ in the character group is less than or equal to p^m (since G/G' is isomorphic to the group of linear characters of G) and, therefore, ϕ maps G into the field of p^mth roots of unity. Now h and ϕ satisfy the conditions of Theorem 2.1 and we are done.

COROLLARY 2. *If $\operatorname{Tr} \rho^* \not\equiv 0$ outside the Frattini group D of G, then G has an outer automorphism of the type $G \to G\phi$ or $G \to G\bar{\phi}$.*

PROOF. Since $\operatorname{Tr} \rho^* \not\equiv 0$ outside D, there exists $x \in G$, $x \notin D$ such that $\operatorname{Tr} \rho^*(x) \neq 0$. Since $x \notin D$, there exists a minimal generating system of G containing x. Let $G = \{x_1, x_2, \cdots, x_n\}$. (The notation $G = \{x_1, x_2, \cdots, x_n\}$ will always denote a minimal generating system (see [5, p. 176]).)

Now $x \notin D \Rightarrow x \notin G' \Rightarrow$ relative $o(x)$ modulo G' is at least equal to p. Hence, we may define the following linear character ϕ' on G/G',

$$\phi' : \begin{array}{l} x \to \epsilon^{p^{m-1}}, \\ x_i \to 1 \qquad \text{for } i = 2, \cdots, n. \end{array}$$

Then, ϕ' may be extended to a linear character ϕ of G such that

$$\phi : \begin{array}{l} x \to \epsilon^{p^{m-1}}, \\ x_i \to 1 \qquad \text{for } i = 2, \cdots, n. \end{array}$$

Then, x and ϕ satisfy the conditions of Theorem 2.1 and we are done.

LEMMA. *Let G be a p-group ($p \neq 2$). If G is the semidirect product (see [5, p. 88]) of a normal abelian subgroup A and any other subgroup B, then G has an outer automorphism.*

PROOF. Every element g of G can be uniquely expressed as a product $g = ba$ where $b \in B$ and $a \in A$ (since G is a semidirect product). Choose any integer k, $1 < k < p$, and define on G the mapping $\alpha : ba \to ba^k$. Now, since A is abelian, it can be shown by routine methods that α is an automorphism. Also, since G is a p-group and A is normal in G, we have $A \cap Z \neq 1$. Therefore, a central element of G is mapped to its kth power and hence α is an outer automorphism.

REMARK. The preceding Lemma is valid for $p = 2$ provided $\exp(A \cap Z) > 2$ and we choose $k = 3$.

THEOREM 2.2 (K. KRONSTEIN). *If H is an irreducible*[3] *linear p-group contained as a normal subgroup in the irreducible monomial linear p-group H^* with the property that the coefficient field of H^* equals the coefficient field of the center $Z(H)$ of H, then H has an outer automorphism.*

PROOF. Let the coefficient field of H^* equal $R(\epsilon)$ where ϵ is a primitive p^nth root of unity. Now, since H is irreducible and the coefficient field of H^* equals the coefficient field of $Z(H)$, H must have a cyclic center generated by the scalar matrix ϵI.

Case 1. $H \neq H^*$.

Choose an element $g \in H^*$ such that $g \notin H$. Define on H, the mapping α: $h \to g^{-1}hg$ for every $h \in H$. Clearly, α is an automorphism of H. Now, suppose α is an inner automorphism. Then, there exists an element $a \in H$ such that $g^{-1}hg = aha^{-1}$ for every $h \in H$. This implies that $(ga)^{-1}h(ga) = h$ for every $h \in H$ and hence, by Schur's Lemma, (ga) must be a scalar matrix $\epsilon^k I$ where $1 \leqq k < p^n$. But $\epsilon^k I \in Z(H)$ and, therefore, $g = (\epsilon^k I)a^{-1}$ must also be an element of H. But this contradicts our choice of g and hence α must be an outer automorphism of H.

Case 2. $H = H^*$.

Let d be the degree of the linear p-group H. Form all possible $d \times d$ monomial matrices with entries which are p^nth roots of unity. Then, this finite set of matrices forms a group M^* which must contain H as a subgroup. But H is a p-group and hence H must in fact be contained in a Sylow subgroup M of M^*. Now, if $H \neq M$, we may use the same argument as in Case 1. Therefore, we assume $H = M$. But M is a Sylow subgroup of M^* and must therefore be the semidirect product of A and P where A is the normal abelian subgroup consisting of all the diagonal matrices in M^* and where P is some Sylow subgroup of the subgroup P^* of all permutation matrices in M^*. (Among all the subgroups of M^* having p-power order, this group clearly is of maximal order and hence must be a Sylow group.) We may now apply the preceding lemma and we are done.

3. **Applications.** In this section, we apply the preceding results to the case of p-groups of class 2 and we establish that *every finite nilpotent group G having its commutator subgroup contained in its center has an outer automorphism.*

The proof of this result as presented by Eugene Schenkman (see

[3] Here and in the remainder of this paper the term "irreducible" will always mean *absolutely* irreducible.

[1]) is invalid due to an error in his Lemma 3 which destroys the accuracy of the counting process used in the proof of his Theorem 1.

LEMMA. *Let G be a p-group with $Z \not\subset D$. Then, G has an outer automorphism.*

PROOF. $Z \not\subset D$ implies the existence of an element $a \in Z$ with the property that $G = \{a, x_2, \cdots, x_n\}$. Since $Z \cap D \neq 1$, we may choose an element $z \in Z \cap D$ having order p. Then, by Theorem 1.2, the mapping

$$\alpha: \begin{array}{ll} a \to az, & \\ x_i \to x_i & \text{for } i \neq 1 \end{array}$$

is an automorphism of G and α must be outer since it maps the central element a to az.

THEOREM 3.1. *Let G be a p-group such that the center Z of G is not contained in the commutator group G' of G. Then, G has an outer automorphism.*

PROOF. By the preceding lemma, if $Z \not\subset D$, we are done. Hence, we may assume that $Z \subset D$. Let $G = \{x_1, x_2, \cdots, x_n\}$. Let $a \in Z$ such that $a \notin G'$. Let the order of $a = p^m$. Let the exponent of the factor group G/G' equal p^r.

Case 1. $p^r \geqq p^m$.

$\exp G/G' = p^r$ implies for some k, the relative order of x_k modulo G' is equal to p^r. Then the mapping

$$\alpha: \begin{array}{ll} x_k \to x_k a, & \\ x_i \to x_i & \text{for all } i \neq k \end{array}$$

is an automorphism of G (by Theorem 1.2) and α is outer since $a \notin G'$.

Case 2. $p^r < p^m$.

On the cyclic group generated by the element a, define the linear character $\rho: a \to \epsilon$, where ϵ is a primitive p^mth root of unity. Consider the representation ρ^* on G induced by ρ (see [5, p. 283]). ρ^* is faithful on G and $\rho^*(a) = \epsilon I$. Hence $\operatorname{Tr} \rho^*(a) \neq 0$ and since $a \notin G'$, $\operatorname{Tr} \rho^* \neq 0$ outside G'. Now, $p^r < p^m$ implies $\exp G/G' < p^m$. Therefore, the conditions of Corollary 1 of Theorem 2.1 are satisfied and we are done. Also, in this case, the $G \to G\phi$ mappings give automorphisms when $p = 2$. Hence, the preceding argument is valid for $p = 2$.

COROLLARY. *Let G be any p-group with its commutator group G' contained in but not equal to its center Z. Then G has an outer automorphism.*

THEOREM 3.2. *Let G be a p-group having $G'=Z$. If Z is not cyclic, then G has an outer automorphism.*

PROOF. Let $G=\{x_1, x_2, \cdots, x_n\}$. Let the relative order of x_i modulo G' equal p^{d_i}. Let B_i equal the subgroup of Z consisting of all the elements of Z having order less than or equal to p^{d_i}. Now, if Z has m generators, then it is clear that each B_i must have precisely m generators.

Let A' equal the group of automorphisms of G generated by mapping each x_i to every element of x_iB_i (see the Corollary of Theorem 1.2). Then A' is a subgroup of the group A of automorphisms of G and $A'\cong B_1\otimes B_2\otimes \cdots \otimes B_n$. Hence A' must have mn generators.

Since $Z=G'$, we have $G/Z=G/G'$ and therefore G/Z has n generators. Now, suppose G has no outer automorphisms. Then, $A\cong G/Z$ and hence A has n generators. But A' is a subgroup of the abelian group A and therefore A' can have at most n generators. Hence $m=1$ and Z must be cyclic thereby contradicting the hypothesis.

LEMMA. *Let G be any p-group having a cyclic center Z. Let P be the cyclic subgroup of Z of order p. Let K be any conjugate class of G. Then, if $PK=K$, every faithful irreducible character of G vanishes on K.*

PROOF. Let $R(G)$ be any faithful irreducible representation of G having degree d. Let t be the character of $R(G)$. We will show that t vanishes on K. Let $y\in K$. Since $PK=K$, there exists $z\in P$ and $x\in K$ such that $y=zx$ where $z\neq 1$. Now $t(y)=t(zx)=t(z)t(x)/d$. (Since $z\in Z$ and $R(G)$ irreducible imply $R(z)$ is the scalar matrix $(t(z)/d)I$.) But x and y are in the same conjugate class, hence $t(y)=t(x)$. Now if $t(y)\neq 0$, then $t(z)/d=1$. But this is impossible since $R(z)$ is not the identity matrix (since $z\neq 1$). Therefore, $t(y)=0$ and t vanishes on K.

THEOREM 3.3. *Let G be a p-group with $G'=Z$. If Z is cyclic, then G has an outer automorphism.*

PROOF. Let $Z=\{a\}$ where $o(a)=p^n$ and let $P=\{a^{p^{n-1}}\}$. Let X be any faithful irreducible character of G and let K be any conjugate class of G not contained in Z.

If $y\in K$, then $y\notin Z$ and there exists $h\in G$ such that $y^{-1}h^{-1}yh=g'$ where $g'\in G'$ and $g'\neq 1$. But $G'=Z=\{a\}$ implies $g'=a^q$ where $1\leq q<p^n$. Therefore, we have $h^{-1}yh=ya^q$ and it is clear that y must be conjugate to yy' where $y'\in\{a^{p^{n-1}}\}$. Therefore, $PK=K$ and, by the preceding lemma, X vanishes on K and hence X vanishes outside Z.

Now if the degree of X is d, then $X(a)=d\epsilon$ where ϵ is a primitive

p^nth root of unity. But this means that the coefficient field of X equals $R(\epsilon)$ (since X vanishes outside Z) and since $R(\epsilon)$ is also the coefficient field of Z, we have that the coefficient field of X equals the coefficient field of Z.

However, by a fairly well-known result (a proof of which may be found in [2]), G must have a faithful irreducible monomial representation $\rho^*(G)$ with coefficient field equal[4] to the coefficient field of X with the property that $X(g)=\mathrm{Tr}(\rho^*(g))$ for every $g\in G$ and in particular $X(a)=\mathrm{Tr}(\rho^*(a))=d\epsilon$. Therefore, the coefficient field of $\rho^*(G)$ equals the coefficient field of the center of $\rho^*(G)$ and we may apply Theorem 2.2.

REMARK. For $p=2$, the preceding argument is valid if $\exp Z>2$. A separate argument is needed for the case $\exp Z=2$, but no new ideas are involved and hence it is omitted.

THEOREM 3.4. *Every finite nilpotent group G having $G'\subseteq Z$ has an outer automorphism.*

PROOF. This result clearly follows from the preceding theorems in this section and from the fact that every finite nilpotent group is the direct product of p-groups.

REFERENCES

1. E. Schenkman, *The existence of outer automorphisms of some nilpotent groups of class* 2, Proc. Amer. Math. Soc. **6** (1955), 6.

2. P. Roquette, *Realisierung von Darstellungun Endlicher Nilpotenter Gruppen*, Arch. Math. **9** (1958), 241–250.

3. H. Zassenhaus, *The theory of groups*, Chelsea, New York, 1949.

4. C. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.

5. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

6. W. Burnside, *Theory of groups of finite order*, Dover, New York, 1955.

COLUMBIA UNIVERSITY AND
UNIVERSITY OF NOTRE DAME

[4] This result, for $p=2$, states that the coefficient field of $\rho^*(G)$ is *contained* in the *smallest cyclotomic* field containing the coefficient field of X (except for the case when $o(Z)=2$). But in *this* discussion, X vanishes outside Z and hence the character field is already cyclotomic. Therefore, when $p=2$ and $n\neq 1$, the coefficient field of $\rho^*(G)$ *equals* the coefficient field of X.