# FINITE GROUPS WHICH ADMIT AN AUTOMORPHISM WITH FEW ORBITS

DANIEL GORENSTEIN

**1. Introduction.** In the course of investigating the structure of finite groups which have a representation in the form $ABA$, for suitable subgroups $A$ and $B$, we have been forced to study groups $G$ which admit an automorphism $\phi$ such that every element of $G$ lies in at least one of the orbits under $\phi$ of the elements $g$, $g\phi^r(g)$, $g\phi^r(g)\phi^{2r}(g)$, $g\phi^r(g)\phi^{2r}(g)\phi^{3r}(g)$, etc., where $g$ is a fixed element of $G$ and $r$ is a fixed integer.

In a previous paper on $ABA$-groups written jointly with I. N. Herstein **(4)**, we have treated the special case $r = 0$ (in which case every element of $G$ can be expressed in the form $\phi^i(g^j)$), and have shown that if the orders of $\phi$ and $g$ are relatively prime, then $G$ is either Abelian or the direct product of an Abelian group of odd order and the quaternion group of order 8. In another paper **(3)**, the author has shown that if each element of $G$ lies in exactly one of these orbits, then $G$ must be an elementary Abelian group of type $(p, p, \ldots, p)$. The purpose of this paper is to prove more generally that any finite group $G$ which admits an automorphism whose orbits are of the above form is necessarily solvable (Theorem 5). The burden of the proof rests on the case in which $\phi$ leaves only the identity element of $G$ fixed, and in this case we shall show that $G$ is in fact nilpotent (Theorem 4).

In the course of the proof we first establish the nilpotency of $G$ in the so-called non-exceptional case (in particular, if $G$ is solvable) (Theorem 1). For this case our statement and argument resemble a result of Feit **(2)** and Higman **(5)**, which asserts that a solvable group having an automorphism of prime order which leaves only the identity element fixed is necessarily nilpotent.* Their argument actually applies if $G$ is assumed to be $p$-normal for all $p|o(G)$. Recently it has been announced by J. G. Thompson that $G$ must in fact be $p$-normal for all $p|o(G)$ whenever $G$ admits an automorphism of prime order leaving only the identity element of $G$ fixed, from which it follows that an arbitrary group $G$ admitting such an automorphism is necessarily nilpotent.†

However, not much is known concerning the structure of $G$ if $\phi$ is of composite order. It is not difficult to construct a solvable non-nilpotent group $G$ admitting an automorphism $\phi$ of composite order leaving only the identity

Received October 22, 1958.

*Feit proves the nilpotency of $G$ under the weaker hypothesis that no subgroup of $G$ has an exceptional group as a composition factor.

†A.M.S. Notices, *5* (6) (November, 1958), 695.



https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

element of $G$ fixed; and it is an open question whether $G$ must be solvable to admit such an automorphism even when $\phi$ has order 4.

We see then that our assumption on the orbits of $G$ is a strong one since no other conditions on $G$ or the order of $\phi$ are needed to prove that $G$ is nilpotent if $\phi$ leaves only the identity element of $G$ fixed. A direct consequence of this assumption is a simple inequality (Lemma 2.3) which exists between the order of $\phi$ and the order of $G$; and it is this inequality which lies at the heart of many of our arguments.

In §§ 10 and 11 we shall determine the structure of groups of prime power order which admit an automorphism $\phi$ without non-trivial fixed elements satisfying our special condition on orbits, and shall show that such a group is either Abelian or of class 2 (Theorem 8). Combining this result with Theorem 4, it will follow that any group $G$ admitting such an automorphism $\phi$ without non-trivial fixed elements is either Abelian or nilpotent of class 2 (Theorem 9).

In the final section we shall determine the precise connection between groups whose orbits satisfy this condition and groups of the form $ABA$. As an application we shall prove the solvability of a certain class of $ABA$-groups (Theorem 10).

The author wishes to thank Prof. Herstein for his considerable help in the preparation of this paper, particularly with the proof of Lemma 3.1.

**2. $\phi$-groups.** We shall call a group $G$ a $\phi$-group if $G$ admits an automorphism $\phi$ such that every element of $G$ can be expressed in the form $\phi^i(g\phi^r(g)\ldots\phi^{r(j-1)}(g))$ for some fixed integer $r$ and some fixed element $g$ in $G$, $i$ and $j$ being arbitrary. The element $g$ will be called a *generator* of $G$ under $\phi$, and $r$ will be called the *index* of $G$ with respect to $g$, or simply the index of $G$.

For simplicity we exclude the trivial case in which the order $h$ of $\phi$ is 1. This implies, in particular, that $o(G) > 1$. We may further assume that $r|h$ for otherwise set $r_1 = (r, h)$ and define $\phi_1 = \phi^{r/r_1}$. Then clearly $\phi_1$ has order $h$, $G$ is a $\phi_1$-group of index $r_1$ with respect to $g$, and we have $r_1|h$. In the special case in which $h = r$, and hence in which every element of $G$ can be expressed in the form $\phi^i(g^j)$, we shall say that $G$ is a $\phi$-group *of index* 0.

We can imbed $G$ as a normal subgroup of a group $G^*$, which contains an element $a$ of order $h$ such that $aga^{-1} = \phi(g)$ for all $g$ in $G$ and such that $G^* = GA$, where $A$ denotes the subgroup generated by $a$. If $\phi$ is of prime order and leaves only the identity element of $G$ fixed, it is easy to show that $G^*$ is a Frobenius group and that $G$ is the regular subgroup of $G^*$. By analogy with this case, we shall say, whenever $\phi$ leaves only the identity element of $G$ fixed, that $G$ is a *regular* $\phi$-group, and that $\phi$ is a *Frobenius* automorphism of $G$.

For brevity we also introduce the symbol $[g]_r^j$ for the element $g\phi^r(g)\ldots\phi^{r(j-1)}(g)$. For completeness we set $[g]_r^0 = 1$. This symbol has several formal properties which we shall use repeatedly throughout the ensuing discussion, and which for convenience we incorporate into the following lemma:

LEMMA 2.1. *Let $\phi$ be an automorphism ofo rder $h$ of a group $G$. For any $g$ in $G$ and any integers $i, j, k, r$, we have $[[g]_r{}^j]_{rj}{}^k = [g]_r{}^{jk}$ and $[g]_r{}^{j+k} = [g]_r{}^j\phi^{rj}([g]_r{}^k)$. Furthermore, if $h|r$, $[g]_r{}^j = g^j$; while if $r|h$ and $\phi^r$ is Frobenius, $[g]_r{}^{h/r} = 1$.*

*Proof.* All these relations except the last follow immediately from the definition of the symbol $[g]_r{}^j$. On the other hand, if $\phi^r$ leaves only the identity element of $G$ fixed, it is easy to see that $g$ can be written in the form $x^{-1}\phi^r(x)$ for some $x$ in $G$. But then $[g]_r{}^{h/r} = (x^{-1}\phi^r(x))(\phi^r(x^{-1}\phi^r(x)) \ldots \phi^{h-r}(x^{-1}\phi^r(x)) = x^{-1}\phi^h(x) = 1$.

The following lemma shows that the property of being a $\phi$-group carries over to subgroups and factor groups of $G$.

LEMMA 2.2. *Let $G$ be a $\phi$-group of index $r$ with respect to the generator $g$, and let $H$ be a subgroup of $G$ invariant under $\phi$. Then $H$ is a $\phi$-group of index $rs$ with respect to the generator $[g]_r{}^s$ for some integer $s$. If $H$ is normal in $G$ and $\bar{G} = G/H$ then $\bar{G}$ is a $\bar{\phi}$-group of index $r$ with respect to the generator $\bar{g}$, where $\bar{\phi}, \bar{g}$ denote respectively the image of $\phi$ on $\bar{G}$ and the residue of $g$ in $\bar{G}$. Furthermore, no proper subgroup of $G$ invariant under $\phi$ contains $g$.*

*Proof.* The last two statements of the lemma follow at once from the definition of a $\phi$-group. To prove the first assertion, let $s$ be the least positive integer such that $g_1 = [g]_r{}^s$ is in $H$. Since $H$ is invariant under $\phi$, every element of $G$ of the form $\phi^i([g_1]_{rs}{}^j)$ is in $H$. Conversely, if $[g]_r{}^k \in H$, write $k = sj + t$ and use Lemma 2.1 to get

$$[g]_r^k = [g]_r^{sj}\, \phi^{rsj}([g]_r^t) = [g_1]_{rs}^j \phi^{rsj}([g]_r^t),$$

whence $[g]_r{}^t \in H$. Since $s$ is the least positive integer with this property, $t = 0$, and it follows that every element of $H$ is of the form $\phi^i([g_1]_{rs}{}^j)$. Thus $H$ is a $\phi$-group of index $rs$ with generator $[g]_r{}^s$.

Finally, we shall establish a simple, but extremely important, relation between the order of $\phi$ and the order of $G$.

LEMMA 2.3. *Let $G$ be a $\phi$-group of index $r$ with respect to a generator $g$ of $G$; let $h$ be the order of $\phi$ and let $k$ be the least integer such that $[g]_r{}^k = 1$. Then $hk > o(G)$. In particular, if $\phi^r$ is Frobenius, $k = h/r$.*

*Proof.* Since every element of $G$ must be in the orbit under $\phi$ of one of the $k$ elements $[g]_r{}^j$, $j = 1, 2, \ldots, k$, since each of these orbits contains at most $h$ elements, and since the last one of them consists of only the identity element of $G$, the inequality $hk > o(G)$ is immediate.

If $\phi^r$ is Frobenius, Lemma 2.1 shows that $[g]_r{}^{h/r} = 1$. The proof of this equality shows also that for any value of $j < h/r$, $[g]_r{}^j \neq 1$. Thus $k = h/r$.

**3. Automorphisms of a class of groups of order $p^m q^n$.** In the next three sections we shall show that a regular $\phi$-group in which no subgroup has an exceptional group as a composition factor is nilpotent. The heart of

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

the problem is to prove this result for certain $\phi$-groups of order $p^m q^n$; §§ 3 and 4 are devoted to this special case.

LEMMA 3.1. *Let $G$ be a group of order $p^m q^n$, $p$ and $q$ being primes, in which the $p$-Sylow subgroup $P$ is normal in $G$ and Abelian of type $(p, p, \ldots, p)$, while the $q$-Sylow subgroups are Abelian of type $(q, q, \ldots, q)$; and assume that the centre of $G$ is trivial. Suppose $\phi$ is an automorphism of $G$ of order $h$ such that no proper subgroup of $P$ which is invariant under $\phi$ is normal in $G$ and such that some $q$-Sylow subgroup $Q$, but no proper subgroup of $Q$, is invariant under $\phi$. Then if $d$ is the order of $\phi$ on $Q$, we have $d|m$ and $h|d(p^{m/d} - 1)$.*

*Proof.* Since $G$ has no centre, $p \neq q$ and $m, n > 0$.

Since each element $y$ in $Q$ induces by conjugation an automorphism $\psi_y$ of $P$, there exists a group of automorphisms $A$ acting on $P$ which can be expressed in the form $\bar{Q}R$, where $\bar{Q}$ is normal in $A$ and is isomorphic to $Q$ under the correspondence $\psi_y \leftrightarrow y$, where $R$ is the cyclic subgroup generated by $\phi$, and where

$$(1) \qquad \phi^{-1}\psi_y\phi = \psi_{\phi(y)} \text{ for all } y \text{ in } Q.$$

For all $y$ in $Q$, we have $\phi^d(y) = y$, and hence $\phi^{-d}\psi_y\phi^d = \psi_y$. Thus $\phi^d$ is in the centre of $A$, and since $Q$ is Abelian, the subgroup $A_0$ generated by $\phi^d$ and $\bar{Q}$ is Abelian.

We shall regard $P$ as an $m$-dimensional vector space over the prime field $K$ with $p$-elements, and $A$ as a group of linear transformations acting on $P$. If $K^*$ denotes the algebraic closure of $K$ and $P^*$, the $m$-dimensional vector space over $K^*$, we may also consider $A$ as a group of linear transformations on $P^*$.

Now let $W$ be a minimal subspace of $P$, invariant under $\phi$, and of dimension $t$, and let $f(x)$, of degree $t$ and irreducible over $K$, be the minimal polynomial of $\phi^d$ on $W$. Since $\phi^d$ is in the centre of $A$, the subspaces $\phi^i\psi_y(W)$ are invariant under $\phi^d$ for all $i$ and all $y$ in $Q$, and $\phi^d$ has the same minimal polynomial $f(x)$ on each of these subspaces. Let

$$P_0 = \sum_{i,y} \phi^i\psi_y(W).$$

It follows immediately from (1) that $P_0$ is left fixed by every element of $A$. Regarded as a subgroup of $P$, $P_0$ is thus normal in $G$ and invariant under $\phi$, whence by our hypotheses $P_0 = P$. Since now $P$ is the sum of minimal subspaces invariant under $\phi^d$, it follows that $P$ is the direct sum of subspaces $W_1, W_2, \ldots, W_s$, each of dimension $t$, each invariant under $\phi^d$, and on each of which the minimal polynomial of $\phi^d$ is $f(x)$. Thus

$$(2) \qquad m = st \text{ and } f(x)^s \text{ is the characteristic polynomial of } \phi^d \text{ on } P.$$

The order $w$ of $\phi^d$ on $P$ is the same as its order on each of the subspaces $W_i$, and since $f(x)$ is irreducible, it follows that $w|p^t - 1$. In particular, this implies $(w, p) = 1$, and hence that the order of $A_0$ is relatively prime to $p$. It follows that the representation of $A_0$ in $P^*$ is completely reducible.

Now $A_0$ is Abelian and $P^*$ has coefficients in an algebraically closed field; hence we can find a vector $x_1 \neq 0$ in $P^*$ which is a common characteristic vector of every element in $A_0$. We shall show that for $0 \leqslant i < d$ the vectors $\phi^i(x_1)$ are also common characteristic vectors of $A_0$ and that they generate a $d$-dimensional subspace of $P^*$, invariant under $A$.

For each $y$ in $Q$, we have

$$\psi_{\phi^i(y)}(x_1) = a_{iy}x_1 \tag{3}$$

for some element $a_{iy}$ in $K^*$. Thus $\phi^{-i}\psi_y\phi^i(x_1) = \psi_{\phi^i(y)}(x_1) = a_{iy}x_1$, so that $\psi_y(\phi^i(x_1)) = a_{iy}\phi^i(x_1)$, proving that $\phi^i(x_1)$ is a common characteristic vector of the elements of $\bar{Q}$. Since $\phi^{dj}$ and $\phi^i$ commute, $\phi^i(x_1)$ is also a characteristic vector of $\phi^{dj}$, and hence of every element of $A_0$.

Let $P^*_1$ be the subspace of $P^*$ generated by the vectors $\phi^i(x_1)$. Since $\phi^d(x_1) = b_1x_1$ for some $b_1$ in $K^*$, $P^*_1$ is invariant under $A$; furthermore, the vectors $x_1, \phi(x_1), \ldots, \phi^d(x_1)$ are linearly dependent and hence $\dim P^*_1 \leqslant d$.

Suppose if possible that $\dim P^*_1 = k < d$. Then for $0 \leqslant i < k$ the vectors $\phi^i(x_1)$ are linearly independent, and furthermore

$$\phi^k(x_1) = c_0x_1 + c_1\phi(x_1) + \ldots + c_{k-1}\phi^{k-1}(x_1),\ c_j \in K^*, \tag{4}$$

and $c_0 \neq 0$. Apply $\psi_y$ to (4) and use (3) to obtain

$$a_{ky}\phi^k(x_1) = c_0a_{0y}x_1 + c_1a_{1y}\phi(x_1) + \ldots + c_{k-1}a_{k-1y}\phi^{k-1}(y). \tag{5}$$

Now multiply (4) by $a_{ky}$ and subtract from (5), obtaining

$$c_0(a_{0y} - a_{ky})x_1 + c_1(a_{1y} - a_{ky})\phi(x_1) + \ldots + c_{k-1}(a_{k-1y} - a_{ky})\phi^{k-1}(x_1) = 0.$$

Since $x_1, \phi(x_1), \ldots, \phi^{k-1}(x_1)$ are linearly independent and since $c_0 \neq 0$, we conclude that

$$a_{ky} = a_{0y}. \tag{6}$$

But (6) implies

$$\phi^{-k}\psi_y^{-1}\phi^k\psi_y(x_1) = a_{0y}\phi^{-k}\psi_y^{-1}\phi^k(x_1) = a_{0y}a_{ky}^{-1}x_1 = x_1.$$

Thus $x_1$ is a common characteristic vector of all commutators $\phi^{-k}\psi_y{}^{-1}\phi^k\psi_y$, $y \in Q$, with the common characteristic root 1. Since these linear transformations are defined over $K$ and 1 is in $K$, it is easy to show that they have a common characteristic vector $z_1 \neq 0$ in $P$ with a common characteristic root 1. But then

$$\phi^{-k}\psi_y^{-1}\phi^k\psi_y(x_1) = \phi^{-k}(y(\phi^k(y^{-1}z_1y))y^{-1}) = z_1,$$

and it follows that $\phi^{-k}(y)y^{-1}$ is in the centralizer of $\phi^k(z_1)$ for all $y$ in $Q$. But $Q$ is Abelian and hence the set of elements $\phi^{-k}(y)y^{-1}$ form a subgroup $Q_0$ of $Q$, which is clearly invariant under $\phi$. Since $k < d$ and $d$ is the order of $\phi$

on $Q$, $Q_0 \neq 1$ and our hypotheses imply that $Q_0 = Q$. Thus $\phi^k(z_1)$ commutes elementwise with $Q$, and since $P$ is Abelian, lies in the centre of $G$, contrary to the fact that $G$ has a trivial centre. Thus dim $P^*_1 = d$, as asserted, and with respect to this basis, $\phi$ is represented on $P^*_1$ by the companion matrix

$$\Phi_1 = \begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & . & . & . & 0 \\ & & & & & & \\ 0 & 0 & 0 & . & . & . & 1 \\ b_1 & 0 & 0 & . & . & . & 0 \end{pmatrix}. \tag{7}$$

Since $A_0$ is completely reducible and leaves $P^*$ invariant, we can write $P^* = P_1 \oplus P'$, where $P'$ is invariant under $A_0$. If $P' \neq 0$, we can construct as above a $d$-dimensional subspace $P^*_2 \subset P'$, invariant under $A$, and with respect to a suitable basis of $P^*_2$, $\phi$ will be represented by a companion matrix $\Phi_2$, of the same form as $\Phi_1$, with possibly a different element $b_2$ in the $d$th row, 1st column. Continuing this process, we can represent $P^*$ as the direct sum of subspaces $P^*_1, P^*_2, \ldots, P^*_\lambda$, each invariant under $A$ and of dimension $d$, and with respect to a suitable basis of $P^*$, $\phi$ is represented by the matrix

$$\phi = \begin{pmatrix} \Phi_1 & & & & \\ & \Phi_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & \Phi_\lambda \end{pmatrix} \tag{8}$$

where each $\Phi_i$ is a companion matrix of the form (7), having some element $b_i$ of $K^*$ in its $d$th row, 1st column. In particular,

$$m = d\lambda. \tag{9}$$

From (8) we see that the characteristic polynomial of $\phi$ over $P^*$ is $g(x) = (x^d - b_1)(x^d - b_2) \ldots (x^d - b_\lambda)$ and that the characteristic polynomial of $\phi^d$ is $h(x)^d = [(x - b_1)(x - b_2) \ldots (x - b_\lambda)]^d$. Since $\phi$ is defined over $P$, the coefficients of $g(x)$ and hence of $h(x)$ are in $K$. A comparison with (2) now yields

$$f(x)^s = h(x)^d. \tag{10}$$

But $f(x)$ is irreducible, and hence $d|s$ and $h(x) = f(x)^{s/d}$. It follows that the roots $b_1, \ldots, b_\lambda$ of $h(x)$ are roots of $f(x)$ and hence lie in the field with $p^t$ elements. Since $ts = m$ and $d|s$ the quantities $b_i$ lie in the field with $p^{m/d}$ elements, and hence have orders dividing $p^{m/d} - 1$. But by (8) $\phi^d$ is a diagonal matrix with $b_1, b_2, \ldots, b_\lambda$ as diagonal entries, and it follows that the order of $\phi^d$ divides $p^{m/d} - 1$, which completes the proof of the lemma.

LEMMA 3.2. *If $G$ satsifies the hypotheses of the preceding lemma, let $F$ denote* *the set of elements of $G$ left fixed by $\phi^r$, for some fixed integer $r$. Then either $F \subset P$, $F = Q$, or $F = G$.*

*Proof.* If $F \not\subset P$, there exists an element $z$ in $F$ with $z = xy$, $x$ in $P$, and $y \neq 1$ in $Q$. We have $xy = z = \phi^r(z) = \phi^r(x)\phi^r(y)$, whence $x\phi^r(x^{-1}) = y\phi^r(y^{-1})$. Since the left side of this equation is an element of $P$, while the right is an element of $Q$, each is the identity, and so $\phi^r(y) = y$. Thus $y \in Q \cap F$, which is invariant under $\phi$. But $Q \cap F \neq 1$ and it follows from the hypotheses of Lemma 3.1 that $Q \cap F = Q$. Thus either $F \subset$ P or $Q \subset F$.

Suppose now that $F > Q$, whence $F \cap P \neq 1$. If $x \in F \cap P$, $\phi^r(yxy^{-1}) = \phi^r(y)\phi^r(x)\phi^r(y^{-1}) = yxy^{-1}$, and hence $yxy^{-1}$ is in $F \cap P$ for any $y$ in $Q$. Thus $F \cap P$ is normal in $G$, and being invariant under $\phi$, must equal $P$. Thus $F$ contains $P$ as well as $Q$, and we conclude that $F = G$.

**4. $\phi$-groups of order $p^m q^n$.** We shall need a preliminary lemma.

LEMMA 4.1. *Let $G$ be an Abelian $\phi$-group of index $r$, of order $p^m$ and of type $(p, p, \ldots, p)$ and let $h$ be the order of $\phi$. Suppose $d|r$, $d|m$, and $h|d(p^{m/d} - 1)$. Then either $d = 1$ or $d = 2$, $r \neq 0$, and the subgroup $F$ left elementwise fixed by $\phi^r$ has order $p$.*

*Proof.* Let $s = m/d$. Since $o(\phi^d)|p^s - 1$, $\phi^d$ is completely reducible when considered as a linear transformation, and each of its irreducible constituents has dimension $\leqslant s$. Thus $G$ is the direct product of subgroups $G_1, G_2, \ldots, G_k$ invariant under $\phi^d$, each of order $\leqslant p^s$ and $k \geqslant d$.

Let $g$ be a generator of $G$ under $\phi$ of index $r$ and write $g = g_1 g_2 \ldots g_k$, $g_i \in G_i$, $i = 1, 2, \ldots, k$. Since $G$ is Abelian, we have

$$[g]_r^j = \prod_{i=1}^{d} [g_i]_r^j. \tag{11}$$

Since $\phi^d$ leaves $G_i$ invariant and since $d|r$, it follows that $[g_i]_r^j \in G_i$ for all $i, j$.

Suppose first that $r = 0$. Then $[g]_r^p = 1$ and we have $hp > o(G)$, whence $d(p^s - 1) > p^{sd-1}$, which implies $d = 1$ or $d = 2$, $s = 1$, and $h = 2(p - 1)$.

On the other hand, if $r \neq 0$, the element

$$[g_i]_r^{p^s - 1}$$

has order 1 or $p$ and is invariant under $\phi^r$, whence by (11) the same is true of

$$[g]_r^{p^s-1}.$$

It follows in either case that

$$[g]_r^{p(p^s-1)} = 1$$

and hence that $h(p(p^s - 1)) > o(G)$. Thus

$$d(p^s - 1)^2 > p^{sd-1}. \tag{12}$$

The only solutions of (12) are $d = 1$, $d = 2$, or $d = 3$, $s = 1$, and $h = 3(p-1)$.

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

In the third case the $G_i$ are cyclic of order $p$, for $i = 1, 2, 3$ and are permuted cyclically by $\phi$. But then if the subgroup $F$ left elementwise fixed by $\phi^r$ were to contain some $G_i$, it would follow that $F = G$, whence $G$ would be of index 0 which is not the case. It follows that $F = 1$ and hence that $[g]_r^{p-1} = 1$. This leads, as in (12), to the inequality $3(p - 1)^2 > p^3$, which is impossible.

We show next that $d = 2$, $h = 2(p^s - 1)$ is impossible. In this case $G = G_1 \otimes G_2$ where $G_1, G_2$ are invariant under $\phi^2$, of order $p^s$, and are permuted by $\phi$. If either $g_1 = 1$ or $g_2 = 1$ $\phi^i([g]_r^j) \in G_1 \cup G_2$, which is a proper subset of $G$. Thus we must have $g = g_1 g_2$ with $g_1 \neq 1$, $g_2 \neq 1$. But now $\phi^2$ has order $p^s - 1$ on both $G_1$ and $G_2$ and so $[g_2]_r^j = 1$ implies $[g_1]_r^j = 1$. Thus the identity is the only element of $G_1$ which is of the form $\phi^i([g]_r^j)$, contrary to the fact that $G$ is a $\phi$-group.

Suppose next that $d = 2$ and $h < 2(p^s - 1)$. Since $h | 2(p^s - 1)$, we conclude that $h < p^s - 1$. But now $[g]_r^{h/r} = 1$ implies $h^2/r > p^{2s}$ which is clearly impossible. Thus $[g]_r^{h/r} = x \neq 1$. Since $\phi^r(x) = x$, the subgroup $F$ left elementwise fixed by $\phi^r$ is not the identity. On the other hand, $[g]_r^{ph/r} = 1$ and so $h(h/r)p > p^{2s}$. It follows that $r < p$. Now $F$ is of index 0, and hence every element of $F$ is of the form $\phi^i(y^j)$ for some element $y$ in $F$. But $\phi$ has order $r$ on $F$, and consequently $rp > o(F)$. Since $r < p$, we conclude that $F$ is cyclic, and the lemma is proved.

We are now ready to prove our main result concerning $\phi$-groups of order $p^m q^n$.

LEMMA 4.2. *If a $\phi$-group satisfies the conditions of Lemma* 3.1, *then $\phi$ leaves some element other than the identity fixed.*

*Proof.* Let $g$ be a generator of $G$ under $\phi$ of index $r$, and let $F$ be the subgroup of $G$ of fixed elements under $\phi^r$. According to Lemma 3.2 either $F \subset P$, $F = Q$, or $F = G$.

*Case* 1. $F \subset P$. Write $g = xy$, with $x$ in $P$, $y$ in $Q$. $P$ is normal in $G$, and hence $[g]_r^j = x_j[y]_r^j$ for some $x_j$ in $P$. If $t$ is the least integer such that $[y]_r^t = 1$, then $t$ is the least integer such that $[g]_r^t$ is in $P$, and hence $P$ is a $\phi$-group of index $rt$. Moreover, since $Q$ is Abelian, it follows that $\phi^{rt}(y) = y$. But now the subgroup of $Q$ left fixed elementwise by $\phi^{rt}$ is invariant under $\phi$ and contains $y$, whence by our hypotheses it must equal $Q$. Thus the order $d$ of $\phi$ on $Q$ divides $rt$, the index of $P$. In view of Lemma 3.1, $P$ now satisfies all the conditions of Lemma 4.1, and hence either $d = 1$, in which case $\phi$ is the identity on $Q$, or $d = 2$ and the subgroup $F_1$ of $P$ left elementwise fixed by $\phi^{rt}$ is cyclic.

In the latter case, $\phi^r$ leaves only the identity element of $Q$ fixed, since $F \subset P$, and hence $\phi^r$ has order 2 on $Q$. It follows that $\phi^r(z) = z^{-1}$ for all $z$ in $Q$. In particular this implies $t = 2$. Furthermore if $\psi_z$ denotes the automorphism of $P$ induced by conjugation by an element $z$ in $Q$, we also have

$\phi^{2r}\psi_z\phi^{-2r} = \psi_z$. If $F_1 = (x_1)$, we conclude at once that $\phi^{2r}(\psi_z(x_1)) = \psi_z(x_1)$, whence $\psi_z(x_1) \in F_1$ for all $z$ in $F_1$. Thus $F_1$ is normal in $G$, and being invariant under $\phi$, $F_1 = P$, whence $o(P) = p$. Hence $m = 1$, contrary to the fact that $d|m$ by Lemma 3.1.

*Case* 2. $F = Q$. Since $F \neq G$, $r \neq 0$. If $r = 1$, every element of $Q$ is left fixed by $\phi$. Hence we may assume $r > 1$. We have $[y]_r{}^q = y^q = 1$, and hence $x_q = [g]_r{}^q \in P$. Since $\phi^r$ is without non-trivial fixed elements on $P$, $[x_q]_r{}^{h/r} = 1$, $[g]_r{}^{qh/r} = 1$, and $h^2q > ro(G)$ by Lemma 2.3. Since $h|d(p^{m/d} - 1)$, we have

$$d^2(p^{m/d} - 1)^2 > rp^mq^{n-1}. \tag{13}$$

The only solutions of (13) are $d = 1$, in which case the lemma follows, or $d = 2$ and $r = 2, 3$. If $d = 2$, $\phi^2$ leaves $Q$ elementwise fixed, while if $r = 3$, $\phi^3$ leaves $Q$ elementwise fixed. Hence the case $d = 2$, $r = 3$ implies $\phi$ is the identity on $Q$. In the remaining case $d = 2$, $r = 2$, we have $d|r$ and hence by Lemma 4.1, the subgroup $F_1$ of $P$ left elementwise fixed by $\phi^{2q}$ is cyclic (since $P$ is of index $2q$). This leads to a contradiction as in Case 1.

*Case* 3. $F = G$. This is the case $r = 0$. $P$ is also of index 0, so that $d$ divides the index of $P$, whence by Lemma 4.1, $d = 1$. Thus $\phi$ is the identity on $Q$, and the lemma is established.

We wish to point out that there do exist $\phi$-groups satisfying the conditions of Lemma 3.1 in which $\phi$ leaves some non-trivial element of $G$ fixed. Perhaps the simplest example is the symmetric group $S_3$ on three letters, which can be defined by the relations $x^3 = y^2 = 1$ and $y\,xy^{-1} = x^{-1}$. It is easily checked that $S_3$ is a $\phi$-group of index 1 with respect to the automorphism $\phi$ defined by: $\phi(x^iy^j) = x^{-i}y^j$, the element $xy$ being a generator of $S_3$ under $\phi$.

**5. Solvable and non-exceptional $\phi$-groups.** A group $G$ is called *exceptional* if $G$ is a non-cyclic simple group in which the normalizer of every characteristic subgroup $\neq 1$ of a $p$-Sylow subgroup $P$ of $G$ is $P$, for all primes $p|o(G)$. It is easily shown that if $G$ is solvable or if every Sylow subgroup of $G$ is Abelian, then no subgroup of $G$ has a composition factor which is an exceptional group (**2**, Lemma 4.1).

THEOREM 1. *Let $G$ be a regular $\phi$-group and assume that no subgroup of $G$ has a composition factor which is an exceptional group. Then $G$ is nilpotent.*

*Proof.* The proof is by induction on the order of $G$, and consists in reducing to the case in which $G$ satisfies the conditions of Lemma 3.1. This reduction is almost identical with that given by Feit (**2**, Lemma 4.2 and Theorem). However, as our group $G$ need not be the regular subgroup of a Frobenius group, we shall outline the steps in this portion of the proof.

We first show that $G$ contains a normal subgroup of prime power order invariant under $\phi$. If $G$ has a proper characteristic subgroup $H$, $H$ is nilpotent by induction, and any of its Sylow subgroups are normal in $G$ and invariant under $\phi$. Otherwise $G$ is the direct product of isomorphic non-exceptional simple groups. There exists then some $p|o(G)$ such that a $p$-Sylow subgroup $P$ of $G$ contains a characteristic subgroup $T$ such that $N(T) > P$. Since $\phi$ is a Frobenius automorphism, some $p$-Sylow subgroup of $G$ is invariant under $\phi$, and we may assume it to be $P$. Either $T$ is normal in $G$ (and $\phi(T) = T$) or by induction $N(T)$ is nilpotent, $P$ is normal in $N(T)$, and hence $N(P) > P$. Either the centre $C$ of $P$ is normal in $G$, and invariant under $\phi$ or $N(C)$ is nilpotent.

If neither $C$ nor $T$ is normal in $G$, we have $N(C) \supset N(P) > P$. If $Q$ is the unique $q$-Sylow subgroup of $N(C)$ for some prime $q \neq p$, and if $Q$ is not normal in $G$, $N(Q)$ is nilpotent and contains $P$, whence $P$ and $Q$ commute elementwise. If $C \supset x Px^{-1}$, then $Q \supset N(x^{-1}Cx)$, which is nilpotent, so that $Q$ commutes elementwise with $x^{-1}Px$ as well as $P$. Since $N(Q)$ is nilpotent, $x^{-1}Px = P$, and it follows that $G$ is $p$-normal. But $N(P)$ is also nilpotent, so that by a theorem of Grün (**6**, p. 171) $G$ contains a normal subgroup $H$ such that $G/H \cong C$, contradicting the fact that $G$ is its own commutator subgroup. Thus $G$ contains a normal subgroup of prime power order, invariant under $\phi$.

Let $P$ be a minimal such subgroup so that $P$ is Abelian of type $(p, p, \ldots, p)$. By induction $G/P$ is nilpotent. If $G$ is not a $p$-group, suppose $q$ is a prime dividing $o(G)$, $q \neq p$; and let $Q$ be a minimal subgroup invariant under $\phi$ of a $q$-Sylow subgroup of $G$. If $PQ < G$, $PQ$ is nilpotent and this, together with the fact that $G/P$ is nilpotent, implies that $Q$ is in the centre of $G$. But then $G/Q$ and hence $G$ is nilpotent.

We may suppose therefore that $G = PQ$, the centre of $G$ is trivial, no subgroup of $P$ invariant under $\phi$ is normal in $G$, and no subgroup of $Q$ is invariant under $\phi$—precisely the hypotheses of Lemma 3.1. But now Lemma 4.2 implies that there is no regular $\phi$-group which satisfies these conditions, and hence $G$ is nilpotent.

COROLLARY. *If the Sylow subgroups of a regular $\phi$-group are $G$ Abelian, then $G$ is Abelian.*

## 6. The fixed subgroup of $\phi^r$.

The subgroup left elementwise fixed by $\phi^r$ plays an important role in determining the structure of a $\phi$-group of index $r$. In this section we shall determine some of the properties of this subgroup for $\phi$-groups of prime power order. We shall need the following lemma:

LEMMA 6.1. *Let $G$ be a $\phi$-group of index 0 of order $p^a$ having a generator $g$ of order $p^n$. Then $G$ contains a sequence of characteristic subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$ where $G_i$ is generated by the elements of order $p^i$ in $G$. Moreover, the subgroups $G_i$ are the only subgroups of $G$ invariant under $\phi$.*

*Proof.* Since $G$ is a $\phi$-group of index 0, the elements $\phi^i(g^{p^{n-1}j})$ clearly include all elements of order $p$ in $G$. Since no proper subset of these elements form a

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

subgroup invariant under $\phi$, they must form the characteristic subgroup $G_1$ of elements of order dividing $p$ in the centre of $G$. As pointed out, no proper subgroup of $G_1$ is invariant under $\phi$.

The lemma follows now easily by applying induction to the group $G/G_1$.

THEOREM 2. *Let $G$ be a regular $\phi$-group of index $r$ and order $p^a$, and let $F$ be the subgroup of $G$ left elementwise fixed by $\phi^r$. Then every subgroup of $F$ invariant under $\phi$ is normal in $G$.*

*Proof.* Since $\phi^r$ leaves $F$ elementwise fixed, $F$ is of index 0, and hence by the preceding lemma the elements of order $p$ in $F$ form a characteristic subgroup $F_1$ of $F$. If $F_1$ is normal in $G$, the theorem follows by induction. For if we set $\bar{G} = G/F_1$, $\bar{F} =$ the residue of $F$ in $\bar{G}$, and $\bar{F}'$ the subgroup of elements left elementwise fixed by the image $\bar{\phi}^r$ of $\phi^r$, $\bar{F} \subset \bar{F}'$ and $\bar{F}'$ is normal in $\bar{G}$ by induction. Since $\bar{F}$ is invariant under $\bar{\phi}$, $\bar{F}$ is characteristic in $\bar{F}'$ by the preceding lemma, and hence normal in $\bar{G}$. Thus $F$ is normal in $G$ and the theorem follows at once.

We shall actually prove that $F_1$ lies in the centre of $G$. Let $h$ be the order of $\phi$, let $g$ be a generator of $G$ under $\phi$, and let

$$g_1 = [g]_r^{h_1/r}$$

be a generator of $F_1$, so that $F_1$ is of index $h_1$. To our induction hypothesis we shall add the assertion that either $h/h_1$ or $h_1/h$ is a power of $p$.

Let us begin by verifying this statement under the assumption that $F_1$ is in the centre of $G$. Let $k$ be the order of $\bar{\phi}$ of $\bar{G}$ and let $\bar{g}$ be the residue of $g$ in $\bar{G}$. Let $H$ be the set of elements of $G$ left fixed by $\phi^k$ and suppose first the $H \not\supset F_1$. Then $H \cap F_1 = 1$ and hence $\phi^k$ is Frobenius on $F_1$. Thus $\phi^k(g) = xg$, $x \in F_1$ and $x = y^{-1}\phi^k(y)$ for some $y$ in $F_1$. It follows that $\phi^k(gy^{-1}) = gy^{-1}$, whence $gy^{-1} \in H$. Thus $g \in F_1H$. Since $F_1H$ is invariant under $\phi$ and contains $g$, $G = F_1H$. Since $H \cong \bar{G}$, $\phi$ has order $k$ on $H$. If $(r, k) = s$, it follows that

$$h = \frac{rk}{s}. \tag{14}$$

On the other hand, let $H_1$ be the subgroup of $H$ generated by the elements of order $p$ left elementwise fixed by $\phi^r$. Then $F_1H_1$ is left elementwise fixed by $\phi^r$ and its elements all have order dividing $p$. It follows that $F_1H_1 = F_1$. Since $F_1 \cap H_1 = 1$, we conclude that $H_1 = 1$. Hence $\phi^r$ leaves only the identity element of $H$ fixed, and consequently $\bar{\phi}^r$ leaves only the identity element of $\bar{G}$ fixed. But this implies $k/s$ is the least integer such that $[\bar{g}]_r^{k/s} = 1$, and hence $g_1 = [g]_r^{k/s}$. Thus $rk/s$ is the index of $F_1$, and in view of (14) we conclude that $h_1 = h$.

Hence we may suppose $H \supset F_1$. In this case, the relation $\phi^k(g) = xg$ implies $\phi^{kp}(g) = g$, and we have

$$k|h|kp. \tag{15}$$

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

Since $r|h$, it follows that either $r = s$ or $r = sp$. If $\bar{\phi}^r$ leaves only the identity element of $\bar{G}$ fixed, it follows as above that $h_1 = kr/s$, and hence $k|h_1|kp$. We conclude from (15) that either $h/h_1$ or $h_1/h$ is a power of $p$.

If $\bar{\phi}^r$ is not Frobenius, let $\bar{F}_1$ be the subgroup of $\bar{G}$ generated by the elements of order $p$ left elementwise fixed by $\bar{\phi}^r$. If $k_1$ is the index of $\bar{F}_1$, then by induction either $k/k_1$ or $k_1/k$ is a power of $p$. By definition of $k_1$,

$$[\bar{g}]_r^{k_1/r}$$

is a generator of $\bar{F}_1$, and hence

$$g_2 = [g]_r^{k_1/r}$$

is a generator of the inverse image $F_2$ of $\bar{F}_1$. Since $\bar{\phi}^r$ leave $\bar{F}_1$ elementwise fixed and $r|k_1$,

$$\phi^{k_1}(g_2) = zg_2$$

for some $z$ in $F_1$. Since $F_1$ is in the centre of $F_2$, this implies

$$(16) \qquad [g_2]_{k_1}^j = z^{j(j-1)/2} g_2^j.$$

As $p$ is the least power of $j$ for which $g_2{}^p \in F_1$, it follows at once that $h_1 = k_1 p$. Thus $h_1 = kp^\epsilon$ for some integer $\epsilon$. This together with (15) implies that either $h/h_1$ or $h_1/h$ is a power of $p$.

Finally we must show that $F_1$ does in fact lie in the centre of $G$. Let $C$ be a minimal subgroup of the centre of $G$ invariant under $\phi$. Because of the minimality of $F_1$, either $C = F_1$ or $C \cap F_1 = 1$. In the latter case, let $\tilde{G}$, $\tilde{F}_1$, $\tilde{g}$, $\tilde{\phi}$ be respectively $G/C$, the image of $F_1$ and $g$ in $G/C$, and the image of $\phi$ on $G/C$. Let $m$ be the order of $\tilde{G}$ on $\tilde{F}$, and define $M$ to be the subgroup of $G$ left elementwise fixed by $\phi^m$.

Now by induction, if $m_1$ is the index of $\bar{F}_1$, we have

$$(17) \qquad \frac{m}{m_1} = p^\epsilon$$

for some integer $\epsilon$.

By definition of $m_1$, $r|m_1$. If we write $r = r_1 p^\delta$, where $(r_1, p) = 1$, it follows that

$$(18) \qquad r_1|m.$$

Since every element of $F_1$ is of the form $\phi^i(g_1{}^j)$, the order of $\phi$ on $F_1$ is relatively prime to $p$, and hence $\phi^{r_1}$ leaves $F_1$ elementwise fixed. It follows therefore from (18) that $F_1 \subset M$.

Assume first that $C \subset M$, in which case $CF_1 \subset M$. Now the index of $CF_1 =$ index of $\bar{F}_1 = m_1$. Let $g'$ be a generator of $CF_1$ of index $m_1$ and write $g' = xy$, $x \in C$, $y \in F_1$. If $m|m_1$,

$$[g']_{m_1}^j = g'^j = x^j y^j,$$

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

and every element of $CF_1$ is of the form $\phi^i(x^j y^j)$, which is clearly impossible since $C \cap F_1 = 1$. On the other hand, if $m \nmid m_1$ (17) holds with $\epsilon \supset 0$, and in this case

$$[g']^j_{m_1} = [x]^j_{m_1} y^j. \tag{19}$$

To obtain an element of $F_1$, we must have

$$[x]^j_{m_1} = 1,$$

and this implies $\phi^{m_1 j}(x) = x$ since $C$ is Abelian. If $j = 1$,

$$[g']^j_{m_1} = x^j y^j,$$

which is impossible as above. Since

$$\phi^{m_1 p^\epsilon}(x) = x,$$

$j \neq 1$ implies $p|j$ and hence 1 is the only element of $F_1$ which can be written in the form

$$\phi^i([g']^j_{m_1}),$$

contrary to the fact that $g'$ is a generator of $CF_1$ under $\phi$.

On the other hand, if $C \cap M = 1$, it follows as in an earlier part of the proof that $G = CM$. But $M \prec G$ and $F_1 \subset M$ so that by induction $F_1$ is in the centre of $M$. Since $C$ is in the centre of $G$, it follows that $F_1$ is in the centre of $G$, and the proof is complete.

COROLLARY. *If $F_1$ denotes the subgroup of $F$ generated by the elements of order $p$ in $F$, then $F_1$ lies in the centre of $G$.*

## 7. $\phi$-groups in which $\phi^r$ leaves only the identity fixed.

We shall also need some properties of $\phi$-groups of index $r$ in which $\phi^r$ is a Frobenius automorphism. To this end, we first establish the following lemma.

LEMMA 7.1. *Let $G$ be a regular $\phi$-group of prime power order, and let $C$ be a subgroup of the centre of $G$, invariant under $\phi$ and of least possible order. Then either $C = G$ or $[o(C)]^2 \leqslant o(G)$.*

*Proof.* We may suppose $G > C$. If $\bar{G} = G/C$, we may restrict our attention to a minimal subgroup of the centre of $\bar{G}$, and hence without loss of generality we may assume that $\bar{G}$ is Abelian of type $(p, p, \ldots, p)$ and that no proper subgroup of $\bar{G}$ is invariant under the image $\bar{\phi}$ of $\phi$ on $\bar{G}$.

Let $g$ be a generator of $G$, $\bar{g}$ its image in $\bar{G}$, $k$ the order of $\bar{\phi}$, and $H$ the subgroup of $G$ left elementwise fixed by $\phi^k$. If $H \cap C = 1$, it follows as in the preceding section that $G = CH$. Since $G/C \cong H$, $H$, and hence $G$, is Abelian. But by definition of $C$, $o(C) \leqslant o(H)$ and therefore $[o(C)]^2 \leqslant o(G)$.

If, on the other hand, $H \supset C$, the equation $\phi^k(g) = yg$ implies $\phi^{kp}(g) = g$ so that $h|kp$, where $h$ is the order of $\phi$. If $h = k$ and $\phi^r$ leaves only the identity element fixed, it follows as in the preceding section that the identity is the only element $C$ which can be written in the form $\phi^i([g]_r{}^j)$, which is a contradiction.

If $h = k$ and some proper subgroup $F$ of $G$ is left elementwise fixed by $\phi^k$, either $F \cap C = 1$ or $F \supset C$. In the first case, since no proper subgroup of $\bar{G}$ is invariant under $\bar{\phi}$, it follows that $G = CF$, and hence $G$ is Abelian since $F \cong \bar{G}$ is Abelian; and we have $[o(C)]^2 \leqslant o(G)$.

If $F > C$, then $F = G$ is of index 0, and hence $C$ contains all elements of $G$ of order $p$. If $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m$ are a basis of $\bar{G}$, let $x_1, x_2, \ldots, x_m$ be a set of representatives such that $\phi(x_i) = x_{i+1}, i = 1, 2, \ldots, m - 1$. Then

$$\phi(x_m) = zx_1^{\alpha_1}x_2^{\alpha_2} \ldots x_m^{\alpha_m}.$$

Since $x_i^p \in C$ for all $i$, it follows at once that $x_1^p, x_2^p, \ldots, x_m^p$ generate a subgroup $C_1$ of $C$ invariant under $\phi$. Since $C$ is minimal, $C_1 = C$, and hence $o(C) \leqslant p^m = o(\bar{G})$, which implies $[o(C)]^2 \leqslant o(G)$.

Finally if $F = C$, $C$ is of index 0, whence the order of $\phi$ on $G$ is a multiple of $p^n - 1/p - 1$, where $p^n = o(C)$. This implies $(p^n - 1)/(p - 1)|k$. But $\bar{G}$ is an Abelian group of type $(p, p, \ldots, p)$ and hence $k < o(\bar{G})$. Thus $o(C) = p^n \leqslant o(\bar{G})$ and $[o(C)]^2 \leqslant o(G)$, as desired.

We now prove

THEOREM 3. *Let $G$ be a regular $\phi$-group of index $r$ and assume $\phi^r$ leaves only the identity element of $G$ fixed. Then either some Sylow subgroup of $G$ is Abelian or there exists a proper subgroup $G_1$ in $G$, invariant under $\phi$, which contains a non-trivial subgroup of the centre of some $p$-Sylow subgroup of $G$ for every prime $p|o(G)$.*

*Proof.* If $g$ is a generator of $G$ under $\phi$, and if $h$ denotes as usual the order of $\phi$, we have first of all $[g]_r^{h/r} = 1$ and hence by Lemma 2.3

$$h^2 > o(G). \tag{20}$$

Let $p_1, \ldots, p_t$ be the distinct primes dividing $o(G)$, and let $P_1, \ldots, P_t$ be the corresponding Sylow subgroups of $G$ invariant under $\phi$. Let $C_i$ be a minimal subgroup of $P_i$, invariant under $\phi$, and of lowest possible order. Then if no Sylow subgroup of $G$ is Abelian, the preceding lemma gives

$$[o(C_i)]^2 \leqslant o(P_i), \qquad i = 1, 2, \ldots, t. \tag{21}$$

Define $s_i$ by the condition that

$$g_i = [g]_r^{s_i}$$

be a generator of $Ci$, and let $h_i$ be the order of $\phi$ on $C_i$, $i = 1, 2, \ldots, t$. Since $C_i$ is an Abelian group of type $(p_i, p_i, \ldots, p_i)$, we have

$$h_i < o(C_i), \qquad i = 1, 2, \ldots, t. \tag{22}$$

Now let $\lambda$ be the greatest common divisor of $s_1, s_2, \ldots, s_t$. We may assume the $s_i$ are so numbered that

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

$$(23) \qquad \lambda = \sum_{i=1}^{m} a_i s_i - \sum_{i=m+1}^{t} b_i s_i, \qquad \text{where } a_i, b_i \geqslant 0.$$

We now consider the elements

$$(24) \qquad \begin{aligned} x &= [g_1]_{rs_1}^{a_1} \phi^{ra_1s_1}([g_2]_{rs_2}^{a_2}) \ldots \phi^{r(a_1s_1+\ldots+a_{m-1}s_{m-1})}([g_m]_{rs_m}^{a_m}) \\ y &= [g_{m+1}]_{rs_{m+1}}^{b_{m+1}} \phi^{rb_{m+1}s_{m+1}}([g_{m+2}]_{rs_{m+2}}^{b_{m+2}}) \ldots \phi^{r(b_{m+1}s_{m+1}+\ldots+b_{t-1}s_{t-1}}([g_t]_{rs_t}^{b_t}). \end{aligned}$$

By repeated use of Lemma 2.1, we find that

$$(25) \qquad x = [g]_r^u \text{ and } y = [g]_r^v, \qquad \text{where } u = \sum_{i=1}^{m} a_i s_i, v = \sum_{i=m+1}^{t} b_i s_i,$$

and hence that $z = y^{-1}x = \phi^{rv}(g)\phi^{r(v+1)}(g) \ldots \phi^{r(u-1)}(g)$. It follows that

$$(26) \qquad z = \phi^{rv}([g]_r^\lambda).$$

By construction $z$ is a power product of elements of $C_1, C_2, \ldots, C_t$, and hence we have $\phi^k(z) = z$ for some integer $k|\Pi_1{}^t h_i$. Therefore

$$(27) \qquad \phi^k([g]_r^\lambda) = [g]_r^\lambda \quad \text{with} \quad k \Bigg| \prod_{i=1}^{t} h_i.$$

Now let $G_1$ be the subgroup of $G$ invariant under $\phi$ which is generated by $[g]_r^\lambda$. We prove that $G_1$ is a proper subgroup of $G$. Suppose, on the contrary, that $G_1 = G$. Then $\phi^k$ is the identity on $G$ by (27) and hence $h|k$.

But then combining (21), (22), and (23), we get

$$(28) \qquad h^2 \leqslant \prod_{i=1}^{t} h_i^2 < \prod_{i=1}^{t} [o(C_i)]^2 \leqslant \prod_{i=1}^{t} (o(P_i)) = o(G),$$

in contradiction to (20).

Since $\lambda|s_i$ for all $i$, $[g]_r{}^{s_i}$ and hence $C_i$ is contained in $G_1$ for all $i = 1, 2, \ldots, t$, and the theorem is proved.

Corollary. *The same conclusion holds if we assume that $h^2/r > o(G)$ instead of that $\phi^r$ leaves only the identity element of $G$ fixed.*

**8. The structure of regular $\phi$-groups.** We are now in a position to prove our main result

Theorem 4. *Every regular $\phi$-group is nilpotent.*

*Proof.* Let $G$ be a regular $\phi$-group of index $r$, $g$ a generator of $G$ under $\phi$, and let $k$ be the least integer such that $[g]_r{}^k = 1$. The proof will be by induction on $k$.

If $H$ is a proper subgroup of $G$ invariant under $\phi$, and $s$ the least integer such that $z = [g]_r{}^s \in H$, then clearly $s|k$, $z$ is a generator of $H$ of index $rs$ and $[z]_{rs}{}^{k/s} = 1$. Hence by induction $H$ is nilpotent.

It suffices therefore, in view of Theorem 1, to prove that the normalizer of a characteristic subgroup of some Sylow subgroup $P$ of $G$ contains $P$ properly. As in Theorem 1, we may suppose $G$ contains no proper characteristic subgroup; and hence that $G$ is the direct product of isomorphic non-cycle simple groups, no subset of which is invariant under $\phi$.

Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing $o(G)$, and let $P_1, P_2, \ldots, P_t$ be the corresponding Sylow subgroups of $G$ invariant under $\phi$. If, first of all, some $P_i$ is Abelian, $N(P_i) \prec G$, and hence is nilpotent. Thus $P_i$ is in the centre of its normalizer, and it follows by a theorem of Burnside that $G$ contains a normal subgroup $H$ such that $G/H \cong P_i$, contrary to the fact that $G$ is its own commutator subgroup.

Thus no Sylow subgroup of $G$ is Abelian. If $\phi^r$ left only the identity element of $G$ fixed, it would follow from Theorem 3 that there exists a proper subgroup $G_1$ in $G$, invariant under $\phi$ which contains for each $i = 1, 2, \ldots, t$ a subgroup $C_i'$ of the centre of $P_i$. Since $G_1$ is nilpotent by induction and $G$ is not a $p$-group, $N(C_i') \succ P_i$. Now $N(C_i') \prec G$ and so is nilpotent. If $C_i$ denotes the centre of $P_i$, it follows that $N(C_i) \succ P_i$, $i = 1, 2, \ldots, t$, and by a previous remark this is sufficient to prove the nilpotency of $G$. Hence if $F$ denotes the subgroup of $G$, left elementwise fixed by $\phi^r$, $F \succ 1$.

Let $g_i = [g]_r^{s_i}$ be a generator of $P_i$, $i = 1, 2, \ldots, t$ and define $F_i$ to be the subgroup of $G$ left elementwise fixed by $\phi^{rs_i}$. Clearly $F \subset F_i$ for all $i$. Suppose first there is an index $i$, say $i = 1$, for which $o(F_1)$ is divisible by at least two distinct primes.

If $F_1 \prec G$, then $F_1$ is nilpotent by induction. Let $P_i'$ be the $p_i$-Sylow subgroup of $F$ invariant under $\phi$. As is easily seen, $P_i' \subset P_i$. Suppose for some $i$ $p_i | o(F)$. By Theorem 2, $F_i \cap P_i$ is normal in $P_i$ and $F \cap P_i$ being invariant under $\phi$, is a characteristic subgroup of $F_i \cap P_i$, and hence is normal in $F_i \cap P_i$ Thus $N(F \cap P_i) \supset P_i$ Since $F_1$ is nilpotent, it follows that $F \cap P_i$ is normal in $F_1$, and hence $N(F \cap P_i) \supset F_1$. It follows from our assumption on $o(F_1)$ that $N(F \cap P_i) \succ P_i$. Since $N(F \cap P_i)$ is nilpotent by induction, we conclude that $N(C_i) \succ P_i$ which is sufficient to prove the nilpotency of $G$.

Suppose instead that $F_1 = G$, so that $\phi^{rs_1}$ is the identity on $G$. If $g_1$ has order $p^n$, it follows that

$$[g_1]_{rs_1}^{p^n} = g_1^{p^n} = 1, \text{ whence } [g]_r^{s_1 p^n} = 1,$$

and consequently

$$k = s_1 p^n. \tag{29}$$

Since $G$ is not solvable, the well-known theorem of Burnside implies $t \geqslant 3$. It follows from (29) that $s_2 | s_1 p^n$ and $s_3 | s_1 p^n$. However $s_2 \nmid s_1$, for this would imply that $[g]_r^{s_1} \in P_1 \cap P_2 = 1$, which is not the case. Similarly $s_3 \nmid s_1$, and hence

$$p_1 | s_2, \qquad p_1 | s_3. \tag{30}$$

Let $G_1$ be the subgroup generated under $\phi$ by

$$g' = [g]_r^{p_1}.$$

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

By (30), $G_1 \supset P_2$ and $G_1 \supset P_3$. If $G_1 < G$, $G_1$ is nilpotent by induction, and consequently $N(C_2) > P_2$, from which the nilpotency of $G$ follows. On the other hand, if $G_1 = G$, $g'$ is a generator of $G$ under $\phi$ of index $rp_1$ and

$$[g']_{rp_1}^{k'} = 1, \text{ where } k' = k/p_1.$$

Since $k' < k$, the nilpotency of $G$ follows by induction.

Finally we must consider the case in which each $F_i$ is of prime power. Since $F \subset F_i$ for all $i$, $o(F_i)$ is a power of a single prime, say $p_1$, for all $i = 1, 2, \ldots, t$. In particular, this implies $F_i \cap P_i = 1$, $i = 2, 3, \ldots, t$, and $\phi^{rs_i}$ leaves only the identity element of $P_i$ fixed. Once again $t \geqslant 3$.

It follows at once from the fact that $[g]_r{}^k = 1$ that $\phi^{rk}(g) = g$, and hence that $(h/r)|k$. Thus

$$k = mh/r \tag{31}$$

for some integer $m$.

If $m = 1$, $h(h/r) > o(G)$, and it follows from the corollary of Theorem 3 that either some Sylow subgroup of $G$ is Abelian or $G$ contains a proper subgroup $G_1$ satisfying the conditions of Theorem 3. Since both of these cases have been treated above, we may assume $m > 1$.

On the other hand, since $\phi^{rs_i}$ leaves only the identity element of $P_i$ fixed,

$$[g_i]_{rs_i}^{h/r} = 1, \qquad i = 2, 3;$$

and hence

$$[g]_r^{hs_i/r} = 1.$$

It follows that

$$m|s_i, \qquad i = 2, 3. \tag{32}$$

If now $G^*_1$ is the subgroup of $G$ generated under $\phi$ by $g^* = [g]_r{}^m$, $G^*_1 \supset P_2$ and $G^*_1 \supset P_3$ in view of (32). If $G^*_1 < G$, it follows as above that $N(C_2) > P_2$ and that $G$ is nilpotent; while if $G^*_1 = G$, $g^*$ is a generator of $G$ of index $rm$,

$$[g^*]_{rm}^{k^*} = 1,$$

where $k^* = k/m$, and $G$ is nilpotent by induction.

**9. The solvability of $\phi$-groups.** We now prove

THEOREM 5. *Every $\phi$-group is solvable.*

*Proof.* Let $G$ be a $\phi$-group of index $r$ with respect to a generator $g$, and let $h$ be the order of $\phi$. As in § 2, we imbed $G$ as a normal subgroup of a group $G^*$ which satisfies the following conditions:

$$G^* = GA \text{ with } G \cap A = 1, \; aya^{-1} = \phi(y) \tag{33}$$

for some element $a$ in $G^*$ of order $h$ and all $y$ in $G$.

If

$$y = \phi^i([g]_r^j)$$

is an arbitrary element of $G$, we can represent $y$ in $G^*$ in the form

$$y = a^i[g(a^r g a^{-r})(a^{2r} g a^{-2r}) \ldots (a^{(j-1)r} g a^{-(j-1)r})a^{-i},$$

which reduces to

$$(34) \qquad y = a^i (ga^r)^j a^{-jr-i}$$

Setting $b = ga^r$, every element of $G$ can thus be expressed in the form $a^i b^j a^{-jr-i}$ for suitable choice of $i$ and $j$. If $x \in G^*$, $x = ya^k$ for some $y$ in $G$ and some integer $k$. It follows that

$$(35) \qquad \text{if } x \in G^*,\ x = a^u b^v a^w \text{ for suitable integers } u, v, w.$$

If $\phi$ leaves only the identity element of $G$ fixed, $G$ is nilpotent by Theorem 4; and so we may assume that there is a subgroup $H \neq 1$ in $G$ which is left elementwise fixed by $\phi$.

Let $g_1 = [g]_r{}^s$ be a generator of $H$, so that by (34)

$$(36) \qquad g_1 = b^s a^{-rs}.$$

Since $\phi(g_1) = g_1$, we have $ag_1a^{-1} = ab^s a^{-rs} a^{-1} = b^s a^{-rs}$, whence

$$(37) \qquad ab^s a^{-1} = b^s.$$

Thus $b^s$ commutes with $a$. Since $b^s$ obviously commutes with $b$, it follows from (35) that $b^s$ is in the centre of $G^*$. Let $C^*$ be the subgroup generated by $b^s$, and set $\bar{G}^* = G^*/C^*$. Denoting the images of $a$, $b$, $g$, $G$ in $\bar{G}^*$ respectively by $\bar{a}$, $\bar{b}$, $\bar{g}$, $\bar{G}$, it follows first of all that $\bar{G}$ is normal in $G^*$, and secondly that every element of $\bar{G}$ is of the form $\bar{a}^i \bar{b}^j \bar{a}^{-jr-i}$, while every element of $\bar{G}^*$ is of the form $\bar{a}^u \bar{b}^v \bar{a}^w$. If $\bar{\phi}$ denotes the automorphism of $\bar{G}$ induced by conjugation by $\bar{a}$, we can reverse the steps in the derivation of (34) to conclude that every element of $\bar{G}$ is of the form $\bar{\phi}^i([\bar{g}]_r{}^j)$. Thus $\bar{G}$ is a $\bar{\phi}$-group; and by definition of $\bar{\phi}$, we have

$$(38) \qquad \bar{\phi}(\bar{y}) = \bar{a}\bar{y}\bar{a}^{-1}, \qquad \bar{y} \in \bar{G}.$$

Either $\bar{\phi}$ leaves only the identity element of $\bar{G}$ fixed or we may repeat the process. Continuing this process we can always construct a sequence of groups

$$G_i^*,\ i = 1, 2, \ldots, n \quad \text{with} \quad G^* = G_1^*, \qquad \bar{G}^* = G_2^*,$$

satisfying the following conditions:

(1) $G_{i+1}^* = G_i^*/C_i^*$, where $C_i^*$ is a cyclic subgroup of the centre of $G_i^*$, $i = 1, 2, \ldots, n-1$;

(2) $G_n^*$ is either the identity or contains a normal subgroup $G_n$ such that $G/G_n$ is cyclic;

(3) $G_n$ is a $\phi_n$-group in which $\phi_n$ leaves only the identity element of $G_n$ fixed.

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

By Theorem 4, $G_n$ is nilpotent. Hence $G^*_n$ and conseqently $G^*$ is solvable. Since $G \subset G^*$, it follows that $G$ is solvable.

*Remark.* Not every $\phi$-group is nilpotent. An example of a non-nilpotent $\phi$-group is the symmetric group on 3 letters, which was discussed at the end of § 4.

**10. $\phi$-groups of index 0.** In the next two sections we shall show that a regular $\phi$-group of prime power order is either Abelian or metabelian. In view of Theorem 4 this will imply that a regular $\phi$-group is nilpotent of class $\leqslant 2$.

In **(4**, Lemma 2**)**, it has been shown that a regular $\phi$-group of index 0 is Abelian if the order of $\phi$ is relatively prime to the order of a generator of $G$ under $\phi$. In this section we shall establish the same result without making any restrictions on the order of $\phi$.

We have seen in Lemma 6.1 that a $\phi$-group $G$ of index 0 and of prime power order contains a sequence of subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$, where the $G_i$ are the only subgroups of $G$ invariant under $\phi$, where each $G_i$ is normal in $G$, and where $x^{-1}\phi^r(x) = 1$ if $x \in G_i$, $i = 0, 1, 2, \ldots, n$. For later purposes we need to investigate $\phi$-groups of prime power order which contain such a sequence of subgroups $G_i$ satisfying the first two of these conditions together with following weaker third conditions: if $x \in G_i$, then

$$x^{-1}\phi^r(x) \in G_{i-1}, \qquad i = 0, 1, 2, \ldots, n.$$

We begin with the following lemma.

LEMMA 10.1. *Let $G$ be an Abelian $\phi$-group of index $r$, of order $p^{nm}$ and type $(p^n, p^n, \ldots, p^n)$. Denote by $G_i$ the subgroup generated by the elements of order $p^i$, and assume that for every $x$ in $G_i$, $x^{-1}\phi^r(x)$ is in $G_{i-1}$. Then if $h$ is the order of $\phi$, we have $h|p^{n-1}(p^m - 1)$ and either $n = 1$ or $m \leqslant 2$.*

*Proof.* Let $g$ be a generator of $G$ under $\phi$. If $n = 1$, $G$ is of order $p^m$, of type $(p, p, \ldots, p)$, and $g^{-1}\phi^r(g) = 1$, so that $G$ is of index 0, and every element of $G$ is of the form $\phi^i(g^j)$. Hence the orbit under $\phi$ of $g^j$ contains exactly $h$ elements, if $0 < j < p$; if the number of distinct such orbits is $k$, we have $hk + 1 = p^m$, whence $h|p^m - 1$.

If $n > 1$, we proceed by induction to prove the first part of the lemma. $G_{n-1}$ is of type $(p^{n-1}, p^{n-1}, \ldots, p^{n-1})$, of order $p^{(n-1)m}$, and is invariant under $\phi$. Since $\phi^r(g) = gy$, $y \in G_{n-1}$ and $\phi^r(y) = yy'$, $y' \in G_{n-2}$, it follows by a direct computation that

$$(39) \qquad [g]_r^j = y_j y^{j(j-1)/2} g^j, \qquad \text{where } y_j \in G_{n-2}.$$

From (39) it follows that the least value of $j$ for which $[g]_r{}^j$ is in $G_{n-1}$ is $j = p$, and that $G_{n-1}$ is of index $rp$ with respect to the generator $[g]_r{}^p$. Since

$$[x^{-1}\phi^r(x)]_r^p = x^{-1}\phi^{rp}(x),$$

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

$x \in G_i$ implies

$$x^{-1}\phi^{rp}(x) \in G_{i-1}.$$

Hence we may apply induction to $G_{n-1}$ to conclude that the automorphism

$$\phi_1 = \phi^{p^{n-2}(p^m-1)}$$

leaves $G_{n-1}$ elementwise fixed.

But then

$$(\phi_1(g))^p = \phi_1(g^p) = g^p,$$

whence $\phi_1(g) = gz$, with $z^p = 1$. But then $z \in G_{n-1}$, $\phi_1(z) = z$ and $\phi_1{}^p(g) = g$. It follows that

$$\phi_1^p = \phi^{p^{n-1}(p^m-1)}$$

is the identity on $G$.

For the second part of the lemma we need the statement:

(40) $$[g]_r^j \in G_{n-1} \qquad \text{if and only if } p^i | j.$$

We have proved (40) above for $i = 1$. If $i > 1$, set $g_1 = [g]_r{}^p$. Since $g_1$ is a generator of $G_{n-1}$ of index $rp$, it follows by induction that

$$[g_1]_{rp}^k \in G_{n-i}$$

if and only if $p^{i-1}|k$. But now by Lemma 2.1,

$$[g_1]_{rp}^k = [g]_r^{pk},$$

and (40) follows at once.

In particular, (40) implies that

$$[g]_r^{p^n} = 1$$

and that there are exactly $p^n - p^{n-1}$ values of $j < p^n$ for which $[g]_r{}^j$ has order $p^n$. For these values of $j$ the elements $\phi^i([g]_r{}^j)$ must exhaust the $p^{mn} - p^{m(n-1)}$ elements of $G$ of order $p^n$. Hence

$$h(p^n - p^{n-1}) \geqslant p^{mn} - p^{m(n-1)}.$$

But $h|p^{n-1}(p^m - 1)$, whence

(41) $$p^{n-1}(p^m - 1)(p^n - p^{n-1}) \geqslant p^{mn} - p^{m(n-1)}.$$

It follows that $p - 1 \geqslant p^{m(n-1)-2n+2}$, and we conclude from this inequality that either $n = 1$ or $m \leqslant 2$.

The following theorem will be of considerable importance in determining the structure of a regular $\phi$-group.

THEOREM 6. *Assume that a regular $\phi$-group $G$ of index $r$ and order $p^a$ contains a sequence of normal subgroups $G = G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = 1$, invariant under $\phi$, such that no subgroup of $G$ invariant under $\phi$ lies properly between $G_i$ and $G_{i-1}$ and such that if $x \in G_i$, $x^{-1}\phi^r(x) \in G_{i-1}$, $i = 1, 2, \ldots, n$. Then $G$ is Abelian.*

*Proof.* We shall first show that all the elements of order $p$ in $G$ are contained in $G_1$, and hence that $G_1$ lies in the centre of $G$. $\bar{G} = G/G_1$ satisfies all the conditions of the lemma, and hence by induction the elements of order $p$ in $\bar{G}$ are contained in the subgroup $\bar{G}_2 = G_2/G_1$, which is Abelian of type (p, p, . . . , p). Hence the elements of order $p$ in $G$ are contained in $G_2$. Since $G_1$ is a minimal subgroup of $G$ invariant under $\phi$, it is also Abelian of type (p, p, . . . , $p$).

We have $G_2$ of index $rs$ with respect to some generator $g_2$, $g_2^p \in G_1$, and $\phi^r(g_2) = yg_2$ for some $y$ in $G_1$. Since $G_1$ is normal in $G_2$, it follows directly that

$$[g_2]^j_{rs} = z_j g_2^j, \qquad z_j \text{ in } G_1.$$

If $g_2$ has order $p^2$, we conclude at once from this relation that the elements of order $p$ in $G_2$ are contained in $G_1$.

On the other hand, suppose $g_2^p = 1$. First of all, if $G_1$ were not in the centre $C$ of $G_2$, we would have $G_1 \cap C = 1$ and $G_1C/G_1 \cong \bar{G}_2$, since no proper subgroup of $\bar{G}_2$ is invariant under $\phi$. But then $G_2 = G_1C$, and so $G_2$ is Abelian. $G_1$ must therefore lie in the centre of $G_2$. But now if $\phi^{rs}(g_2) = zg_2$, $z \in G_1$, it follows that

$$[g_2]^j_{rs} = z^{j(j-1)/2} g_2^j,$$

If $p$ is odd, we conclude that $[g_2]_{rs}{}^p = g_2^p = 1$, a contradiction to the fact that $G_1$ is spanned by the elements of the form

$$\phi^i([g]^{pj}_{rs}).$$

If $p = 2$, (42) gives $[g_2]_{rs}{}^4 = 1$, and so the orbits of the four elements $[g_2]_{rs}{}^j$, $j = 1, 2, 3, 4$ must span $G_2$. But

$$[g_2]^3_{rs} = zg_2 = \phi^{rs}(g_2)$$

since $g_2^2 = 1$, and hence $[g_2]_{rs}{}^1$ and $[g_2]_{rs}{}^3$ determine the same orbit. It follows that the orbit of $g_2$ under $\phi$ must include every element of $G_2 - G_1$, whence

$$h \geqslant o(G_2) - o(G_1). \tag{43}$$

Since our assumptions imply that every element of $G_2$ is of order 2, $G_2$ is Albelian and we may regard $\phi$ as a linear transformation of an $n$-dimensional vector space $(2^n = o(G_2))$, over the field with 2 elements, which leaves some $t$-dimensional subspace invariant $(2^t = o(G_1))$. But the maximum order of such a linear transformation is easily computed to be $(2^t - 1)(2^{n-t} - 1)$, which is less than $2^n - 2^t$, in contradiction to (43). Hence $G_1$ consists of the elements of order dividing $p$ in $G$, as asserted.

If $o(G_1) = p$, $G$ therefore has a unique subgroup of order $p$, and as is well-known, this implies that $G$ is either cyclic or isomorphic to the generalized quaternion group of order $2^a$. But this last group has a unique element of order 2, which is necessarily fixed by every automorphism of the group.

Hence $G$ is Abelian if $G_1$ is cyclic. We assume therefore that $o(G_1) = p^t$ with $t \geqslant 2$.

We consider the group $\bar{G} = G/G_1$, and suppose $k$ to be the order of the image $\bar{\phi}$ of $\phi$ on $\bar{G}$. If $F$ denotes the subgroup of $G$ left elementwise fixed by $\phi^k$, we have $F \cap G_1 = 1$ or $F \cap G_1 = G_1$, since $G_1$ is a minimal subgroup of $G$ invariant under $\phi$ and since $F$ is also invariant under $\phi$. Since $G_1$ contains every element of order $p$ in $G$, $F \cap G_1 = 1$ implies $F = 1$.

Consider the case $F = 1$. If $g$ is a generator of $G$, $\phi^k(g) = z_1 g$, $z_1$ in $G_1$; and since $\phi^k$ leaves only the identity element of $G_1$ fixed, $z_1 = x^{-1}\phi^k(x)$ for some $x$ in $G_1$, and $\phi^k(x^{-1}g) = x^{-1}g$. Thus $x^{-1}g \in F$, whence $g = x$. Thus $G = G_1$ is Abelian. We may thus suppose $F \supset G_1$.

Now $\bar{G}$ satisfies all the hypotheses of the theorem and is Abelian by induction. But then it satisfies the conditions of Lemma 6.1, and consequently is either cyclic, of type $(p^{n-1}, p^{n-1})$ or of type $(p, p, \ldots, p)$ and order $p^m$ with $k | p^m - 1$. If $\bar{G}$ is cyclic, $G$ is of course Abelian, since $G_1$ is in its centre. In the second case, it follows that every element of $G$ is of the form $xg^i\phi(g)^j$ for some element $x$ in $G_1$ and suitable integers $i, j$. Suppose now that

$$\phi(g)g = yg\phi(g), \qquad y \text{ in } G_1. \tag{44}$$

Since $\bar{G}$ is of type $(p^{n-1}, p^{n-1})$, $\bar{\phi}^2(\bar{g}) = \bar{g}^\alpha \bar{\phi}(\bar{g}^\beta)$ for some integers $\alpha, \beta$, where $\bar{g}$ denotes the image of $g$ in $\bar{G}$. Hence

$$\phi^2(g) = zg^\alpha\phi(g^\beta), \qquad z \in G_1. \tag{45}$$

Now apply $\phi$ to (44) and use (45) to obtain

$$\begin{aligned} \phi^2(g)\phi(g) &= \phi(y)\phi(g)\phi^2(g) = \phi(y)\phi(g)zg^\alpha\phi(g^\beta) \\ &= \phi(y)y^\alpha(zg^\alpha\phi(g^\beta))\phi(g) = \phi(y)y^\alpha\phi^2(g)\phi(g). \end{aligned} \tag{46}$$

Hence $\phi(y) = y^{-\alpha}$, and the subgroup $H$ generated by $y$ is invariant under $\phi$. Since $H \subset G_1$, we have $H = G_1$ or $H = 1$. In the first case, $o(G_1) = p$, contrary to our present assumption. Hence $y = 1$ and it follows at once from (44) that $G$ is Abelian.

There remains the case $F \supset G_1$, $\bar{G}$ Abelian of type $(p, p, \ldots, p)$ and order $p^m$, with $k | p^m - 1$. In this case the relation $\phi^k(g) = z_1 g$ implies $\phi^{kp}(g) = g$, whence

$$h | kp | (p^m - 1)p. \tag{47}$$

On the other hand, as in the proof of Lemma 10.1

$$[g]_r^{p^2} = 1,$$

and hence

$$hp^2 > o(G) = o(G_1)o(\bar{G}) = p^{t+m}. \tag{48}$$

Combining (22) and (23), we get the inequality $(p^m - 1)p^3 > p^{t+m}$, which implies $t \leqslant 2$. We are assuming $t > 1$ and hence $t = 2$.

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

The theorem has already been proved if $m \leqslant 2$. Hence we may assume $m \geqslant 3$. Let $\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_m$ be a basis for $\bar{G}$ and $y_1, y_2, \ldots, y_m$ a set of representatives in $G$. Since $G_1$ contains all elements of $G$ of order $p$, $y_i^p \neq 1$ for all $i$. Since $y_i^p \in G_1$ and $G_1$ is of type $(p, p)$, there exists integers $\gamma_1$ and $\gamma_2$ such that

$$y_3^p = y_1^{p\gamma_1}y_2^{p\gamma_2}. \tag{49}$$

On the other hand, if

$$y_3(y_1^{\gamma_1}y_2^{\gamma_2}) = x_1y_1^{\gamma_1}y_2^{\gamma_2}y_3 \qquad \text{and} \qquad y_2^{\gamma_2}y_1^{\gamma_1} = x_2y_1^{\gamma_1}y_2^{\gamma_2},$$

then

$$(y_2^{-\gamma_2}y_1^{-\gamma_1}y_3)^p = x_1^{p(p+1)/2}(y_2^{-\gamma_2}y_1^{-\gamma_1})^py_3^p = (x_1x_2)^{p(p+1)/2}y_2^{-\gamma_2p}y_1^{-\gamma_1p}y_3^p. \tag{50}$$

If $p$ is odd, it follows at once from (49) and (50) that $y_2^{-\gamma_2}y_1^{-\gamma_1}y_3$ has order $p$ and hence is in $G_1$. We conclude that $\bar{y}_3 = \bar{y}_1^{\gamma_1}\bar{y}_2^{\gamma_2}$, which implies $m \leqslant 2$, a contradiction.

On the other hand, if $p = 2$, and $\bar{g}$ is the residue of $g$ in $\bar{G}$, it follows as in the first part of the proof that $[g]_r^4 = 1$, that $[g]_r^3$ and $[g]_r^1$ determine the same orbits, and hence that the orbit of $g$ under $\phi$ must include all $2^2(2^m - 1)$ elements of $G - G_1$, and hence

$$h \geqslant 2^2(2^m - 1). \tag{51}$$

On the other hand, since every element of $G_1$ is of the form $\phi^i(g_1^j)$, $\phi$ has order 3 on $G_1$. Since $F \supset G_1$, $3|k$. But then $\phi^k(g) = xg$, $x \in G_1$, implies $\phi^{2k}(g) = g$, whence $h|2k$. Since $k \leqslant 2^m - 1$, $h \leqslant 2(2^m - 1)$ in contradiction to (51).

COROLLARY. *A regular $\phi$-group of index 0 and of prime power order is Abelian.*

The structure of $\phi$-groups of index 0 is now easily obtained.

THEOREM 7. *A regular $\phi$-group of index 0 is Abelian.*

*Proof.* If $G$ is of index 0, so is every one of its subgroups. Since $\phi$ is regular, $\phi$ leaves some $p$-Sylow subgroup of $G$ invariant for every $p|o(G)$. It follows from the preceding corollary that the Sylow subgroups of $G$ are all Abelian. and hence by the corollary of Theorem 1, that $G$ is Abelian.

## 11. The structure of regular $\phi$-groups of prime power order.

THEOREM 8. *A regular $\phi$-group of prime power order is either Abelian or metabelian.*

*Proof.* Let $G$ be a regular $\phi$-group of index $r$ and order $p$. We shall first prove that $G$ contains a normal subgroup $F^*$ invariant under $\phi$ and of index $rs$ such that

(a) $F^*$ satisfies the hypotheses of Theorem 6.
(*b*) $\tilde{G} = G/F^*$ is Abelian of type $(p, p, \ldots, p)$.
(*c*) The image $\tilde{\phi}^r$ of $\phi^r$ leaves only the identity element of $\tilde{G}$ fixed.
(*d*) If $k$ = order of $\tilde{\phi}$, then $(k, p) = 1$ and $k|rs$.

We shall then show that $F^*$ is actually in the centre of $G$.

Suppose first that $\phi^r$ leaves some proper subgroup $F$ of $G$ elementwise fixed. By Theorem 2, $F$ is normal in $G$. Let $\bar{G} = G/F$. By induction $\bar{G}$ contains a subgroup $\bar{F}^*$ of index $rs$ such that $\bar{F}^*$, $\tilde{G} = \bar{G}/\bar{F}^*$, and the image $\tilde{\phi}$ of $\phi$ on $\tilde{G}$ satisfy conditions (a) to (d). If $F^*$ denotes the inverse image of $\bar{F}^*$ in $G$, $F^*$ is of index $rs$. Since $F$ is of index 0, it follows readily from Lemma 6.1 and condition (a) for $\bar{F}^*$ that $F^*$ satisfies (a). Since $G/F^* \cong \tilde{G}$, the remaining conditions follow at once.

We may therefore assume that $\phi^r$ leaves only the identity element of $G$ fixed. If $G$ is Abelian of type $(p, p, \ldots, p)$ and $(h, p) = 1$, where $h$ = order of $\phi$, set $F^* = 1$.

If $G$ is not of this form, let $C_1$ be a minimal subgroup of the centre of $G$, invariant under $\phi$, and set $\bar{G} = G/C_1$, $\bar{\phi}$ = image of $\phi$ on $\bar{G}$. If $\bar{G}$ is Abelian of type $(p, p, \ldots, p)$ and the order $m$ of $\bar{\phi}$ is relatively prime to $p$, we let $H$ be the subgroup of elements of $G$ left elementwise fixed by $\phi^m$. If $H \cap C_1 = 1$, it follows by the usual argument that $G = C_1H$, that $H \cong \bar{G}$, and consequently that $G$ is Abelian of type $(p, p, \ldots, p)$. Since $C_1$ is a minimal subgroup of $G$ invariant under $\phi$, the order of $\phi$ on $C_1$ is relatively prime to $p$, and it follows at once that $(h, p) = 1$, a contradiction. Thus $H \supset C_1$.

Let $g$ be a generator of $G$ of index $r$ and $g_1 = [g]_r{}^s$ a generator of $C_1$ of index $rs$. If $\bar{g}$ is the residue of $g$ in $\bar{G}$, $[\bar{g}]_r{}^s = 1$, and since $\bar{\phi}$ leaves only the identity element of $\bar{G}$ fixed, it follows that $\bar{\phi}^{rs}(\bar{g}) = \bar{g}$. Thus $m|rs$.Since $H \supset C_1$ we conclude that $x^{-1}\phi^{rs}(x) = 1$ for all $x$ in $C_1$. If we put $F^* = C_1$, it is clear that conditions (a) to (d) hold.

Consider then the case in which either $\bar{G}$ is not Abelian of type $(p, p, \ldots, p)$ or $(m, p) \neq 1$ so that $\bar{G}$ contains at least one proper normal subgroup invariant under $\phi$. By induction $\bar{G}$ contains a proper normal subgroup $\bar{F}^*$ of index $rs$ such that if $\tilde{G} = \bar{G}/\bar{F}^*$, $\tilde{\phi}$ = image of $\bar{\phi}$ on $\tilde{G}$, and $k$ = order of $\tilde{\phi}$, then $\bar{F}^*$ satisfies the conditions of Theorem 6, $\tilde{G}$ is Abelian of type $(p, p, \ldots, p)$, $(k, p) = 1$ and $k|rs$, and $\tilde{\phi}^r$ is Frobenius. Our conditions imply that $\bar{\phi}^{rs}(\bar{g}) = \bar{x}\bar{g}$, $\bar{x} \in \bar{F}^*$. It follows as in the derivation of (39) and (40) that

$$\bar{\phi}^{rsp^n}(\bar{g}) = \bar{g}$$

for some integer $n$, and hence

$$m|rsp^n. \tag{52}$$

Let $H$ be the subgroup of $G$ left elementwise fixed by $\phi^{rsp^n}$, and suppose first that $H \supset C_1$. Let $F^*$ be the inverse image of $\bar{F}^*$ in $G$. The index of $F^*$ = index of $\bar{F}^* = rs$. Furthermore $\phi^{rsp^n}(x) = x$ for all $x$ in $C_1$. Since $C_1$ is a minimal subgroup of $G$ invariant under $\phi$, the order of $\phi$ on $C_1$ is relatively

https://doi.org/10.4153/CJM-1960-008-6 Published online by Cambridge University Press

prime to $p$, and hence $x^{-1}\phi^{rs}(x) = 1$ for all $x$ in $C_1$. It follows immediately that $F^*$ satisfies (a). Since $G/F^* \cong \bar{G}/\bar{F}^*$, (b), (c), and (d) also hold.

On the other hand, if $H \cap C_1 = 1$, it follows once again that $G = C_1H$ and that $\bar{G} \cong H$ under an isomorphism $\tau$ such that $(\tau\bar{\phi}(\bar{x})) = \phi(\tau(\bar{x}))$ for all $\bar{x}$ in $\bar{G}$. Let $F'$ be the normal subgroup of $H$ which corresponds to $\bar{F}^*$ under $\tau$. Then $F'$ is invariant under $\phi$, $\phi$ has order $m$ on $H$ and $m|rsp$. Let $F_1$ be a minimal subgroup of $F'$ invariant under $\phi$. Since every subgroup of $F'$ invariant under $\phi$ is characteristic in $F'$, $F_1$ is normal in $H$ and hence also in $G$. Let $G' = G/F_1$, $\phi'$ = image of $\phi$ on $G'$, $m'$ = order of $\phi'$. By induction $G'$ contains a normal subgroup $F'^*$ of index $rs'$ such that conditions (a), (b), (c) hold for $F'^*$ and $\tilde{G} = G/F'^*$. In particular, $m' = rs'p^{n'}$ for some integer $n'$. Let $H_1$ be the subgroup of $G$ invariant under

$$\phi^{rs'p^{n'}}.$$

Since $\bar{F}^*$ is the homomorphic image of $C_1F'$, $C_1F'$ is of index $rs$. Since $F_1 \subset C_1F'$, it follows that $rs|rs'$, and hence $H_1 \supset F_1$. Our desired conclusion now follows as in the preceding paragraph.

It remains to prove that $F^*$ lies in the centre of $G$. By construction $F^*$ contains a sequence of normal subgroups $F^* = F_n \supset F_{n-1} \supset \ldots \supset F_1 \supset F_0 = 1$ invariant under $\phi$ such that

$$x^{-1}\phi^{rs}(x) \in F_{i-1} \text{ if } x \in F_i$$

and such that no proper subgroup of $F^*$ invariant under $\phi$ lies properly between $F_i$ and $F_{i-1}$. By Theorem 6, $F^*$ is Abelian. It is easy to see that this implies that $F^*$ is of type $(p^n, p^n, \ldots, p^n)$ and that $F_i$ is the subgroup generated by the elements of order $p^i$ in $F^*$. Thus $F_1$ is characteristic in $F^*$, and consequently normal in $G$. Since $F^*$ is a minimal subgroup of $G$ invariant under $\phi$, we conclude that $F_1$ lies in the centre of $G$.

Since $\tilde{G}$ is Abelian of type $(p, p, \ldots, p)$ we can decompose $\tilde{G}$ into the direct product of subgroups $\tilde{G}_j$, $j = 1, 2, \ldots, t$ invariant under $\tilde{\phi}^{rs}$ and none of which can be further decomposed into proper subgroups invariant under $\tilde{\phi}^{rs}$. If $G_j$ denotes the inverse image of $\tilde{G}_j$, it suffices to prove that $F^*$ lies in the centre of each $G_j$. For definiteness, take $j = 1$.

First of all, if $\tilde{\phi}^{rs}$ has non-trivial fixed elements on $\tilde{G}_1$, it follows from the minimality of $\tilde{G}_1$ that $\tilde{\phi}^{rs}$ is in fact the identity on $\tilde{G}_1$. Hence if $x \in G_1$, $x^{-1}\phi^{rs}(x) \in F^*$. It follows at once that $G_1$ is a group of index $rs$ satisfying the conditions of Theorem 6, and hence is Abelian. Thus $F^*$ is in the centre of $G_1$ in this case.

Consider then the case in which $\tilde{\phi}^{rs}$ leaves only the identity element of $\tilde{G}_1$ fixed. $\tilde{G}_1$ has a basis $\tilde{y}_1, \ldots, \tilde{y}_q$ such that

$$\tilde{\phi}^{rs}(\tilde{y}_i) = y_{i+1}, \qquad i = 1, 2, \ldots, q-1$$

and

$$\tilde{\phi}^{rs}(y_q) = \tilde{y}_1^{\alpha_1}\tilde{y}_2^{\alpha_2} \ldots \tilde{y}_q^{\alpha_q} \tag{53}$$

for suitable integers $\alpha_1, \alpha_2, \ldots, \alpha_q$.

If

$$\tilde{y}_1^{i_1}\tilde{y}_2^{i_2}\ldots\tilde{y}_q^{i_q}$$

is a fixed element of $\tilde{\phi}^{rs}$, then it is easily checked that the integers $i_1, i_2, \ldots, i_q$ are a solution of the congruences.

$$\alpha_1 i_q \equiv i_1; \alpha_2 i_q + i_1 \equiv i_2; \ldots; \alpha_q i_q + i_{q-1} \equiv i_q \qquad (\text{mod } p), \tag{54}$$

and conversely. It follows readily from (54) that $\tilde{\phi}^{rs}$ is Frobenius on $\tilde{G}_1$ if and only if

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_q - 1, p) = 1. \tag{55}$$

Let $y_i$ be a representative of $\tilde{y}_i$ in $G_1$ such that

$$\phi^{rs}(y_i) = y_{i+1}, \qquad i = 1, 2, \ldots, q-1.$$

Then

$$\phi^{rs}(y_q) = x_0 y_1^{\alpha_1} y_2^{\alpha_2}\ldots y_q^{\alpha_q},$$

$x_0 \in F^*$. If $\psi$ denotes the automorphism of $F^*$ induced by conjugation by $y_1$, $\psi$ leaves $F_1$ elementwise fixed since $F_1$ lies in the centre of $G_1$. We shall prove by induction on $n$ that $\psi$ leaves $F^*$ elementwise fixed. This will suffice to prove that $F^*$ is in the centre of $G_1$, and will complete the proof of the theorem.

By induction $F^*/F_1$ lies in the centre of $G/F_1$, whence

$$\text{if } x \in F^*, \quad \psi(x) = zx, \quad z \in F_1. \tag{56}$$

Suppose $\psi$ is the identity on $F_k$ with $1 \leqslant k < n$. We shall prove $\psi$ is the identity on $F_{k+1}$. Applying $\phi^{rsi}$ to (56), we obtain

$$\phi^{rsi}(\psi(x)) = \phi^{rsi}(y_1)\phi^{rsi}(x)\phi^{rsi}(y_1^{-1}) = \phi^{rsi}(z)\phi^{rsi}(x) = z\phi^{rsi}(x). \tag{57}$$

But if $x \in F_{k+1}$, $\phi^{rsi}(x) = xz_i$, $z_i \in F_k$. Since $F_k$ is in the centre of $G_1$, we conclude from (57) that

$$\phi^{rsi}(\psi(x)) = zx = \psi(x) \quad \text{for all } i \text{ and all } x \text{ in } F_{k+1}. \tag{58}$$

By repeated use of (58) we now obtain

$$\psi(x) = \phi^{rsq}(\psi(x)) = (x_0 y_1^{\alpha_1} y_2^{\alpha_2}\ldots y_q^{\alpha_q})(x)(x_0 y_1^{\alpha_1} y_2^{\alpha_2}\ldots y_q^{\alpha_q})^{-1} = \psi^{\alpha_1+\alpha_2+\ldots+\alpha_q}(x),$$

whence

$$\psi^{\alpha_1+\alpha_2+\ldots+\alpha_q-1}(x) = x, \qquad x \in F_{k+1}. \tag{59}$$

On the other hand, (56) implies $\psi^p(x) = x$. But then (55) and (59) together imply $\psi(x) = x$ for all $k$ in $F_{k+1}$. Q.E.D.

Theorem 8 and Theorem 4 together imply

THEOREM 9. *A regular $\phi$-group is either Abelian or nilpotent of class* 2.

We conjecture that a regular $\phi$-group is Abelian if $\phi^r$ is Frobenius. This result would follow easily from the following conjecture concerning fixed-point free automorphisms of $p$-groups.

CONJECTURE. *Let $G$ be a non-Abelian $p$-group which admits an automorphism $\phi$ of order $h$ leaving only the identity element of $G$ fixed, and assume that $G$ cannot be expressed as the direct product of two proper subgroups invariant under $\phi$. Then $h^2 < o(G)$.*

## 12. The relation between $\phi$-groups and groups of the form ABA.

In the proof of the preceding theorem we have already seen that a $\phi$-group $G$ can be imbedded as a normal subgroup of an $ABA$-group $G^*$ satisfying $G^* = GA$ and $G \cap A = 1$. The converse is also true, and consequently we have

THEOREM 10. *$G$ is a $\phi$-group if and only if it can be imbedded as a normal subgroup of a group $G^*$ of the form $ABA$, where $A$ and $B$ are cyclic subgroups of $G^*$, such that $G^* = GA$ and $A \cap G = 1$.*

*Proof.* It suffices to prove that if an $ABA$-group $G^*$ in which $A, B$ are cyclic contains a normal subgroup $G$ such that $G^* = GA$ and $G \cap A = 1$, then $G$ is a $\phi$-group.

If $a, b$ are generators of $A, B$ respectively, we have $b = ga^r$ for some element $g$ in $G$ and some integer $r$. Since $G$ is normal, the elements

$$b^j a^{-jr} = (ba^{-r})(a^r b a^{-2r}) \ldots (a^{(j-1)r} b a^{-jr}) = g(a^r g a^{-r}) \ldots a^{(j-1)r} g a^{-(j-1)r} \tag{60}$$

are in $G$ for all $i, j$.

Suppose for some $j$, $b^j a^k \in G$; then $a^{-k-jr} = (b^j a^k)^{-1}(b^j a^{-jr}) \in G \cap A$. Since $G \cap A = 1$, $a^k = a^{-jr}$. It follows at once that $G$ consists precisely of the elements of $G^*$ of the form $a^i b^j a^{-jr-i}$. If we now define $\phi$ to be an automorphism of $G$ induced by conjugation by $a$, it follows as in the proof of Theorem 5 that every element of $G$ is of the form $\phi^i([g]_r{}^j)$. Thus $G$ is a $\phi$-group of index $r$ and with generator $g$.

Combining Theorems 5 and 10, we obtain our final result:

THEOREM 11. *A group $G^*$ which is of the form $ABA$, where $A$ and $B$ are cyclic subgroups, and which contains a normal subgroup $G$ such that $G^* = GA$* and $G \cap A = 1$ *is solvable.*

In a subsequent paper we shall show that an $ABA$ group $G^*$ with a trivial centre in which $A$ is its own normalizer and $A$ is of odd order always contains a normal subgroup $G$ such that $G^* = GA$ and $G \cap A = 1$. We shall also determine the structure of $G^*$ when $o(A)$ is even and, in particular, shall show that $G^*$ is solvable.

## References

**1.** W. Burnside, *Theory of groups of finite order* (Dover, New York, 1955).
**2.** W. Feit, *On the structure of Frobenius groups*, Can. J. Math., *9* (1957), 587–96.
**3.** D. Gorenstein, *A class of Frobenius groups*, Can. J. Math., *11* (1959), 39–42.
**4.** D. Gorenstein and I. N. Herstein, A *class of solvable groups*, Can. J. Math., *11* (1959), 311–20.
**5.** G. Higman, *Groups and rings which have automorphisms without non-trivial fixed elements*, J. London Math. Soc., *32* (1957), 321–334.
**6.** H. Zassenhaus, *The theory of groups* (Chelsea, New York, 1958).

*Clark University*