FINITE GROUPS ADMITTING A FIXED-POINT-FREE AUTOMORPHISM OF ORDER 4.*

By Daniel Gorenstein and I. N. Herstein.

Recently, in a remarkable piece of work [4, 5] John Thompson has proved a result which implies as an immediate corollary the well-known Frobenius conjecture, namely that a finite group admitting a fixed-point-free automorphism (i. e., leaving only the identity element fixed) of prime order must be nilpotent. However, non-nilpotent groups are known which admit fixed-point-free automorphisms of composite order. In all these cases one notices that the groups in question are solvable. Although the sample is rather restricted, it is not too unnatural to ask whether the condition that a finite group admit such an automorphism is strong enough to force solvability of the group. This question is related to another problem, which seems equally difficult, which asks whether a finite group containing a cyclic subgroup which is its own normalizer must be composite.

In the present paper we shall prove that a group G possessing a fixed-point-free automorphism of order 4 is solvable. Although many of the ideas used carry over to the case in which ϕ has order pq, and especially $2q$, our key lemmas use the fact that ϕ has order 4 in a crucial way.

The proof depends upon a theorem of Philip Hall which asserts that a finite group G is solvable if for every factorization of $o(G)$ into relatively prime numbers m and n, G contains a subgroup of order m. We show (Lemma 7) that a group G which has a fixed-point-free automorphism of order 4 satisfies the conditions of Hall's theorem.

Once we know that G is solvable it is not difficult to prove that its commutator subgroup is nilpotent (Theorem 2). This fact was also observed by Thompson.

Graham Higman has shown [3] that there is a bound to the class of a p-group P which possesses an automorphism ϕ of prime order q without fixed-points. This does not carry over to automorphisms of composite order, for at the end of the paper we give an example due to Thompson of a family of p-groups of arbitrary high class each of which admits a fixed-point-free automorphism of order 4.

* Received July 8, 1960; Minor revision December 8, 1960.

1. We begin by recalling a few well-known elementary results concerning a finite group G which admits a fixed-point-free automorphism ϕ of order n and in particular when $n=4$. First of all, for any prime $p \mid o(G)$ there is a unique p-Sylow subgroup P of G which is invariant under ϕ. We shall call P the *canonical* p-Sylow subgroup of G (with respect to ϕ). Furthermore, for any x in G we have the relation $x\phi(x)\phi^2(x)\cdots\phi^{n-1}(x)=1$.

If $n=4$, each orbit under ϕ except for that consisting of the identity contains either 2 or 4 elements, hence G is necessarily of odd order. The set of elements of G left fixed by ϕ^2 is a ϕ-invariant subgroup of G, which we denote by F. If $F \neq 1$, the restriction of ϕ to F is an automorphism of F of order 2 without non-trivial fixed elements. This implies that F is Abelian and that $\phi(f)=f^{-1}$ for all f in F. Finally, we shall denote by I the set of all h in G for which $\phi^2(h)=h^{-1}$. It is worth observing that I need not be a subgroup of G.

Throughout the paper G will denote a finite group having a fixed-point-free automorphism ϕ of order 4, F will denote the subgroup left elementwise fixed by ϕ^2 and I the subset consisting of those elements of G which are mapped into their inverses by ϕ^2.

LEMMA 1. $G=FI=IF$.

Proof. If $z=x^{-1}\phi^2(x)$ for some x in G, then $\phi^2(z)=\phi^2(x^{-1})\phi^4(x) =\phi^2(x^{-1})x=z^{-1}$, whence $z\in I$. Furthermore, $x^{-1}\phi^2(x)=y^{-1}\phi^2(y)$ implies that $\phi^2(xy^{-1})=xy^{-1}$ and hence that $xy^{-1}\in F$. Thus I contains at least $[G:F]$ elements.

To complete the proof, it will clearly suffice to show that distinct elements of I lie in distinct right (or left) cosets of F. If $h_2=fh_1$, $h_1, h_2\in I$, $f\in F$, it follows by applying ϕ^2 that $h_2^{-1}=fh_1^{-1}$. Combining this with the previous relation gives $h_1^{-1}fh_1=f^{-1}$. Since G is of odd order, this forces $f=1$ and hence $h_1=h_2$. Similarly, we show that $h_2=h_1f$ implies $h_1=h_2$.

LEMMA 2. *If f_1, f_2 in F are conjugate in G, then $f_1=f_2$.*

Proof. Suppose $xf_1x^{-1}=f_2$. Since F is Abelian, we may assume without loss, in view of Lemma 1, that $x\in I$. Applying ϕ^2 gives $x^{-1}f_1x=f_2$, whence x^2 centralizes f_1. Since G is of odd order, x centralizes f_1, and consequently $f_1=f_2$.

As an immediate corollary, we obtain

LEMMA 3. *Any subgroup of F is in the center of its normalizer.*

LEMMA 4. *If $h\in I$, h commutes with $\phi(h)$.*

Proof. This lemma follows at once from the relations $h\phi(h)\phi^2(h)\phi^3(h) = 1$ and $\phi^2(h) = h^{-1}$.

LEMMA 5. *For any $p|o(G)$, F normalizes the canonical p-Sylow subgroup P of G.*

Proof. If $F \cap P = 1$, ϕ^2 is an automorphism of P of order 2 without non-trivial fixed elements, whence $\phi^2(x) = x^{-1}$ for all $x \in P$. Thus $P \subset I$. Let $f \in F$ and consider $P' = fPf^{-1}$. If $y = fxf^{-1}$, with $x \in P$, $\phi^2(y) = fx^{-1}f^{-1} = y^{-1}$, which implies that $P' \subset I$.

Suppose $P' \neq P$; choose y in P' and not in P. The subgroup generated by y and its image under ϕ is ϕ-invariant and, since $y \in I$, it follows from the preceding lemma that this subgroup is a p-group. Let P_1 be a maximal ϕ-invariant p-group containing y. If P_1 were not a p-Sylow subgroup of G, the unique ϕ-invariant p-Sylow subgroup P_2 of $N_G(P_1)$ would have order greater than $o(P_1)$ and would contain P_1 and consequently y. Since this would contradict our choice of P_1, P_1 must be a p-Sylow subgroup of G. Since P is the only ϕ-invariant p-Sylow subgroup of G, $P_1 = P$, which is impossible since $y \in P_1$, $y \notin P$. We conclude that $P' = fPf^{-1} = P$. Since f was arbitrary, $F \subset N_G(P)$.

Suppose, on the other hand, that $F \cap P \neq 1$. In this case we shall prove the lemma by induction on $o(G)$. Since F is Abelian, $F \cap P$ is a ϕ-invariant p-group which is normalized by F. If P_1 is a maximal ϕ-invariant p-group which is normalized by F, it follows first of all as in the preceding paragraph that $P_1 \subset P$. Suppose $P_1 < P$. We must have $N_G(P_1) = G$, for otherwise by induction F normalizes the unique ϕ-invariant p-Sylow subgroup P_2 of $N_G(P_1)$ and $o(P_2) > o(P_1)$. Thus $P_1 \lhd G$. Set $\bar{G} = G/P_1$ and let $\bar{\phi}$ be the image of ϕ on $\bar{G}$. $\bar{\phi}$ has no non-trivial fixed elements and is of order 2 or 4. If $\bar{P}$, $\bar{F}$ denote the images of P, F in $\bar{G}$, it follows by induction (or from the fact that $\bar{G}$ is Abelian in the case $\bar{\phi}^2 = 1$) that $\bar{F} \subset N_{\bar{G}}(\bar{P})$. Thus $F \subset N_G(P)$.

LEMMA 6. *If A, B are two ϕ-invariant subgroups of G which are each normalized by F, then ABF is a ϕ-invariant subgroup of G of order dividing $o(A)o(B)o(F)$.*

Proof. Since BF is a subgroup, ABF will be a subgroup if $(BF)A = A(BF)$. Since F normalizes A, it will suffice to show that $BA \subset ABF$.

Since A is ϕ-invariant, it follows from Lemma 1 applied to A that for any a in A, $a = a'f_1$, where $a' \in I \cap A$ and $f_1 \in F \cap A$. Similarly, for any b

in B, $b=f_2b'$, $f_2\in F\cap B$ and $b'\in I\cap B$. Clearly, $ba=f_2b'a'f_1\in ABF$ if and only if $b'a'\in ABF$.

Now $b'^{-1}a'^{-1}=fh$ for some f in F, h in I; applying ϕ^2 gives $b'a'=fh^{-1}$. Since $h^{-1}=a'b'f$ from the first relation, $b'a'=fa'b'f=a''b''f^2$, where $a''\in A$, $b''\in B$. Thus ABF is a subgroup as asserted. The remaining parts of the lemma are immediate.

LEMMA 7. *Let $p_1,p_2,\cdots,p_k$ be a set of primes dividing $o(G)$ and let $P_1,P_2,\cdots,P_k$ be the corresponding canonical Sylow subgroups of G. Then $P_1P_2\cdots P_k$ is a subgroup of G.*

Proof. By induction on k we may assume that $H=P_1P_2\cdots P_{k-1}$ is a subgroup of G. Clearly H is ϕ-invariant. By Lemma 5 $F\subset N_G(H)$ and $F\subset N_G(P_k)$, so that $S=HP_kF$ is a ϕ-invariant subgroup of G by Lemma 6. Since $o(S)\,|\,o(H)o(P_k)o(F)$, a q-Sylow subgroup Q of F for any prime $q\neq p_i$, $i=1,2,\cdots,k$, is a q-Sylow subgroup of S. By Lemma 3 Q is in the center of its normalizer in S, so that by a well-known theorem of Burnside S possesses a normal q-complement L_q. Since L_q consists of the elements of S of order prime to q, L_q contains H and P_k. Repeating this argument for each such prime $q\,|\,o(F)$, we readily conclude that $\bigcap_{\substack{q|o(F)\\ q\neq p_i}} L_q=HP_k=P_1P_2\cdots P_k$, which, being an intersection of subgroups, is a subgroup.

Lemma 7 leads at once to our main result.

THEOREM 1. *If G is a finite group admitting an automorphism of order 4 leaving only the identity element of G fixed, then G is solvable.*

Proof. It follows from Lemma 7 that for any factorization of $o(G)$ into the product of relatively prime numbers m and n, G contains a subgroup of order m. By a theorem of Philip Hall ([2], Theorem 9.3.3, p. 144), this implies that G is solvable.

2. We shall now examine the structure of G more closely, For our main result we need several lemmas.

LEMMA 8. *If $G=HM$, where H is nilpotent, normal in G, $(o(H),o(M))=1$, M is invariant under ϕ and $M\cap F=1$, then $G=H\times M$.*

Proof. Let $\Phi(H)$ be the Frattini subgroup of H and set $\bar{G}=G/\Phi(H)=\bar{H}\bar{M}$. Since $(o(H),o(M))=1$, it follows from the properties of the Frattini subgroup that $\bar{G}=\bar{H}\times\bar{M}$ implies $G=H\times M$. Hence, without loss, we may assume that H is elementary Abelian. Since ϕ^2 leaves only the identity element of M fixed, M is Abelian. If either H contains two disjoint ϕ-invariant subgroups normal in G or ϕ does not act irreducibly on M, the lemma follows easily by induction. Hence we may assume that ϕ acts irreducibly on M and no proper ϕ-invariant subgroup of H is normal in G. In particular, this implies that H is an elementary Abelian p-group for some prime p.

The holomorph of ϕ and M is represented irreducibly on H regarded as a vector space over the prime field K_p with p elements. Let H^* be the corresponding vector space over the algebraic closure K^*_p of K_p. If M does not centralize H, it follows from Lemma 3.1 of [1] that with respect to a suitable basis of H^* the matrix of ϕ assumes the form

$$\begin{bmatrix} \phi_1 & & & & 0 \\ & \phi_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ 0 & & & & \phi_s \end{bmatrix},$$

where

$$\phi_i = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ b_i & 0 & 0 & 0 \end{bmatrix}$$

with $b_i \in K^*_p$. Since $\phi^4 = 1$, $\phi_i{}^4 = 1$ and hence $b_i = 1$ for all i. But this means that 1 is a characteristic root of ϕ and hence that ϕ leaves some element of H other than the identity fixed. This contradiction forces M to centralize H, and consequently $G = H \times M$, as asserted.

LEMMA 9. *If $G = HM$, where H is nilpotent, normal in G, $(o(H), o(M)) = 1$, M is invariant under ϕ and $C_G(H) \subset H$, then $M \subset F$.*

Proof. By Theorem 1 G and hence M is solvable. Let K be a maximal ϕ-invariant normal subgroup of M. By induction applied to HK, $K \subset F$. Let $\bar{M} = M/K$ and let $\bar{\phi}$ be the image of ϕ on $\bar{M}$. If $\bar{\phi}^2 = 1$ on $\bar{M}$, it follows readily that $M \subset F$. Hence we may assume that $\bar{\phi}$ has order 4 on $\bar{M}$. Since $\bar{M}$ is elementary Abelian and $\bar{\phi}$ acts irreducibly on $\bar{M}$, $\bar{\phi}^2(\bar{y}) = \bar{y}^{-1}$ for all $\bar{y}$ in $\bar{M}$. Thus for all y in M, $\phi^2(y) = y^{-1}z$, $z \in K$. Now if $x \in K$, $yxy^{-1} = x'$ for some $x' \in K$. Applying ϕ^2 gives $y^{-1}zxz^{-1}y = x'$. Since K is abelian we easily conclude that y^2 and consequently y centralizes x. Hence K is in the center of M.

As in the previous lemma we may assume without loss of generality that

H is elementary Abelian. By Lemma 1 applied to M, $M=(F\cap M)(I\cap M)$, and under our present assumptions $I\cap M\neq 1$. By induction we may suppose that no ϕ-invariant proper subgroup of H is normal in H; and we shall then derive a contradiction by showing that $I\cap M$ centralizes H.

Now $C_G(K)$ is ϕ-invariant and contains M, since K is in the center of M. Since $H_1=H\cap C_G(K)\lhd C_G(K), N_G(H_1)$ contains M and H, whence $H_1\lhd G$. Since H_1 is invariant under ϕ, the minimality of H implies that either $H_1=1$ or $H_1=H$.

Suppose first that $H_1=1$. Since $K\subset F$ and F is Abelian $H\cap F\subset C_G(K)$, whence $H\cap F=1$ and consequently $H\subset I$. If $y\in M\cap I$, $x\in H$, $yxy^{-1}=x'$ for some x' in H. Applying ϕ^2, we obtain $y^{-1}x^{-1}y=x'^{-1}$, which together with the preceding relation implies that x and y commute. Thus $I\cap M\subset C_G(H)$ as asserted.

On the other hand, if $H_1=H$, K centralizes H, whence $K=1$ and $I\cap M=M$. Since $M\cap F=1$, $G=H\times M$ by Lemma 8. Thus $I\cap M$ centralizes H, completing the proof.

LEMMA 10. *G has p-length 1 for all $p\,|\,o(G)$.*

Proof. Since G is solvable by Theorem 1, the statement of the lemma is meaningful. The proof will be by induction on $o(G)$. Let M be the maximal normal subgroup of G of order prime to p, and assume first that $M\neq 1$. M is ϕ-invariant since it is characteristic in G. Let $\bar{\phi}$ be the image of ϕ on $\bar{G}=G/M$. If $\bar{\phi}^2=1$ on $\bar{G}$, $\bar{G}$ is Abelian. If $\bar{\phi}$ has order 4 on $\bar{G}$, it follows by induction that $\bar{G}$ has p-length 1 and hence that a p-Sylow subgroup $\bar{P}$ of $\bar{G}$ is normal in $\bar{G}$. In either case we conclude that G has p-length 1. We may therefore suppose that $M=1$.

Let P_1 be the maximal normal p-group of G and consequently ϕ-invariant. Let P be the canonical p-Sylow subgroup of G and $\tilde{P}$ its image in $\tilde{G}=G/P_1$. If $\tilde{K}$ is the maximal normal subgroup of $\tilde{G}$ of order prime to p, it follows by induction that the image of $\tilde{P}$ in $\tilde{G}/\tilde{K}$ is normal in $\tilde{G}/\tilde{K}$ whence $\tilde{P}\tilde{K}\lhd\tilde{G}$. If $\tilde{P}\tilde{K}<\tilde{G}$, its inverse image $G_0<G$, and hence by induction has p-length 1.

Since P_1 contains its own centralizer in G ([2], Theorem 18.4.4, p. 332), G_0 contains no non-trivial normal subgroups of order prime to p and hence $P\lhd G_0$. But then $\tilde{P}\lhd\tilde{P}\tilde{K}$, and since $\tilde{P}$ is characteristic in $\tilde{P}\tilde{K}$, we conclude that $\tilde{P}\lhd\tilde{G}$, whence $P\lhd G$.

We may therefore assume that $\tilde{G}=\tilde{P}\tilde{K}$. The inverse image G_1 of $\tilde{K}$ is of the form P_1K, where K has order prime to p. Since G_1 is solvable, any two subgroups of G_1 of order $o(K)$ are conjugate ([2], Theorem 9.3.1, p. 141). One can now show by the same argument which proves the existence of canonical p-Sylow subgroups that there exists a unique conjugate of K in G, which is invariant under ϕ. Without loss we may assume K itself is ϕ-invariant. Since $C_{G_1}(P_1) \subset P_1$, the previous lemma implies that $K \subset F$. But then by the argument of the first paragraph of the lemma $\tilde{K}$ is in the center of $\tilde{G}$, whence $\tilde{P} \lhd \tilde{G}$ and $P \lhd G$.

THEOREM 2. *If G possesses an automorphism ϕ of order 4 leaving only the identity element fixed, then the commutator subgroup of G is nilpotent.*

Proof. G is solvable by Theorem 1. Assume first that G contains two minimal ϕ-invariant normal subgroups N_1 and N_2. Since the image of ϕ on G/N_1 and G/N_2 has no non-trivial fixed elements, the commutator subgroups $[G/N_i, G/N_i]$ of G/N_i, $i = 1, 2$, are nilpotent by induction. Let H_i be the inverse image of $[G/N_i, G/N_i]$ in G and set $H = H_1 \cap H_2$. Clearly, $H \lhd G$ and $[G, G] \subset H$. Furthermore, if x and y are elements of relatively prime order in H, their images in G/N_i, $i = 1, 2$, commute, and hence $y^{-1}xyx^{-1} \in N_1 \cap N_2$. Since N_1 and N_2 are distinct minimal normal ϕ-invariant subgroups of G, $N_1 \cap N_2 = 1$, and consequently x, y commute. Thus H and hence $[G, G]$ is nilpotent.

We may therefore suppose that G contains a unique minimal normal ϕ-invariant subgroup N_1. N_1 is a p-group for some prime p and G contains no non-trivial normal subgroups of order prime to p. Since G has p-length 1 by Lemma 10, a p-Sylow subgroup P of G is normal in G. Now $C_G(P) \lhd G$ and $C_G(P) = Z(P) \times K$, where K has order prime to p. Since K is characteristic in $C_G(P)$, K is normal in G, whence $K = 1$ and $C_G(P) \subset P$. Furthermore, $G = PM$ for some subgroup M of G, and we may assume M is invariant under ϕ. Since $(o(P), o(M)) = 1$, we can apply Lemma 9 to conclude that $M \subset F$. Thus M is Abelian, and consequently $[G, G] \subset P$ is nilpotent.

3. We conclude with an example of a family of p-groups of arbitrarily high class each of which has a fixed-point free automorphism of order 4. Let p be any prime such that $p \equiv 1 \pmod 4$ and let P_1 be an elementary Abelian p-group of order p^t, where $t = p^d$, d an arbitrary integer, and let $x_1, x_2, \cdots, x_t$ be a basis for P_1. We construct an extension of P_1 by adjoining a new letter y satisfying the relations:

$$(*) \qquad y^t = 1, \ yx_iy^{-1} = x_ix_{i+1}, \ i = 1, 2, \cdots, t-1, \ yx_ty^{-1} = x_t.$$

These relations define a p-group of order tp^t and of class t.

Since $p \equiv 1 \pmod 4$, there is an integer α such that $\alpha^2 \equiv -1 \pmod p$.

We define an automorphism θ of P by setting $\theta(y)=y^{-1}$, $\theta(x_t)=x_t^{\alpha}$. For θ to be an automorphism, its value on x_i must be such that

$$(**) \qquad y^{-1}\theta(x_i)y=\theta(x_i)\theta(x_{i+1}).$$

Assume θ has been defined on x_j for $j>i$ and that $\theta(x_j)$ is in the subgroup generated by $x_j, x_{j+1},\cdots,x_t$. We shall show that $\theta(x_i)$ can be defined satisfying (**) and subject to the restriction $\theta(x_i)=x_i^{a_i}x_{i+1}^{a_{i+1}}\cdots x_t^{a_t}$. It follows at once from (**) that we have $x_{i+1}^{-a_i}x_{i+2}^{-a_{i+1}}\cdots x_t^{-a_{t-1}}=y\theta(x_{i+1})y^{-1}$. Since these relations have a solution for $a_i, a_{i+1},\cdots,a_{t-1}$ (for any choice of a_t), the automorphism θ exists.

Regarding P_1 as a vector space, it is easy to see that the matrix of θ with respect to the basis $x_1, x_2,\cdots,x_t$ has the form $\alpha D+N$, where $D=\operatorname{diag}(1,-1,1,-1,\cdots,1)$ and N is a strictly triangular matrix. It follows that the order of θ on P_1 is $4p^s$ for some $s\leqq d$. Setting $\phi=\theta^{p^s}$, ϕ has order 4 on P_1 and since $\phi(y)=y^{-1}$, ϕ has order 4 on P. The characteristic roots of ϕ are $\pm\alpha$, the same as those of θ. Since $\alpha\neq\pm 1$, ϕ leaves only the identity element of P_1 fixed. Since $\phi(y)=y^{-1}$, this implies that ϕ leaves only the indentity element of P fixed.

CLARK UNIVERSITY,
CORNELL UNIVERSITY.

REFERENCES.

[1] Daniel Gorenstein, "Finite groups which admit an automorphism with few orbits," *Canadian Journal of Mathematics*, vol. 12 (1960), pp. 73-100.

[2] Marshall Hall, *The Theory of Groups*, New York, 1959.

[3] Graham Higman, "Groups and rings having automorphisms without trivial fixed elements," *Journal of the London Mathematical Society*, vol. 32 (1957), pp. 321-334.

[4] John G. Thompson, "Finite groups with fixed-point-free automorphisms of prime order," *Proceedings of the National Academy of Sciences*, vol. 45 (1959), pp. 578-581.

[5] ———, "Normal p-complements for finite groups," *Mathematische Zeitschrift*, vol. 72 (1960), pp. 332-354.