SOLVABLE GROUPS ADMITTING A FIXED-POINT-FREE AUTOMORPHISM OF PRIME POWER ORDER

FLETCHER GROSS

1. **Introduction.** The purpose of the paper is to prove the following:

THEOREM 1. *Suppose G is a finite group which admits an automorphism σ of order p^n, where p is an odd prime, such that σ fixes only the identity element of G.*
(a) *If G is solvable, then $h(G) \leqq n$.*
(b) *If G is π-solvable, then $l_\pi(G) \leqq [(n+1)/2]$.*
Furthermore, both these inequalities are best-possible.

Here $h(G)$, the Fitting height (also called the nilpotent length) of G, is as defined in [**7**]. $l_\pi(G)$, the π-length of G, is defined in an obvious analogy to the definition of p-length in [**2**].

Higman [**3**] proved Theorem 1 in the case $n=1$ (subsequently, without making any assumptions on the solvability of G, Thompson [**6**] obtained the same result). Hoffman [**4**] and Shult [**5**] proved Theorem 1 provided that either p is not a Fermat prime or a Sylow 2-group of G is abelian.

For $p=2$, Gorenstein and Herstein [**1**] obtained Theorem 1 if $n \leqq 2$, and Hoffman and Shult both obtained Theorem 1 provided that a Sylow q-group of G is abelian for all Mersenne primes q which divide the order of G. Shult, who considers a more general situation of which Theorem 1 is a special case, recently extended his results to include all primes, but his bound on $h(G)$ is not best-possible in the special case of Theorem 1. It also should be noted that Thompson [**7**] obtained a bound for $h(G)$ under a much more general hypothesis than that considered in the other papers mentioned.

Theorem 1 is a consequence of

THEOREM 2. *Let G be a finite group admitting a fixed-point-free automorphism σ of order p^n, p an odd prime, and let H be a normal Hall subgroup of G such that H contains its centralizer in G. Then the automorphism of G/H induced by $\sigma^{p^{n-1}}$ is the identity automorphism.*

Here again, the papers of Hoffman and Shult imply Theorem 2 if either p is not a Fermat prime or a Sylow 2-group of G is abelian. Thus what is new about the present paper is that no condition is imposed upon the Sylow 2-groups of G if p is a Fermat prime.

Received by the editors February 15, 1966.

The restriction to odd primes is essential since Theorem 2 is false for $p=2$, $n>2$. To see this let $q=2^m-1$ be some Mersenne prime and let M be the nonabelian group of exponent q and order q^3. M admits a fixed-point-free automorphism σ of order 2^{m+1}. Let K be the semidirect product of M and the group generated by σ^2, and choose F to be any finite field such that (1) the characteristic of F is not 2 or q, and (2) F is a splitting field for K. There is a faithful irreducible representation ρ of K over F such that $\rho(\sigma^2)$ has no nonzero fixed vectors. Now for $x\in M$, define $\rho^*(x)$ by $\rho^*(x)=\rho(x)\oplus\rho(x^\sigma)$. Then choose $\rho^*(\sigma)$ to be

$$\begin{pmatrix} 0 & \rho(\sigma^2) \\ I & 0 \end{pmatrix}.$$

$\rho^*(\sigma)$ is of order 2^{m+1} and $\rho^*(\sigma)^{-1}\rho^*(x)\rho^*(\sigma)=\rho^*(x^\sigma)$. Thus ρ^* is a faithful representation of the semidirect product of M and $\langle\sigma\rangle$, the group generated by σ. If H is the space on which $\rho^*(M\langle\sigma\rangle)$ operates, then $\rho^*(\sigma)$ induces a fixed-point-free automorphism of the semidirect product HM. This automorphism is of order 2^{m+1} on both HM and HM/H.

2. **Proofs.** First we need some elementary number theoretic results which we state without proof.

(2.1) LEMMA. *Let $p=2^s+1$ be an odd Fermat prime. Then p^k divides (2^n-1) if and only if $2s\, p^{k-1}$ divides n.*

(2.2) LEMMA. *Suppose $p=2^s+1$ is an odd Fermat prime and $p^a=2^b+1$ for some positive integers a, b. Then $a=1$, $b=s$ unless $p=3$, in which case $a=2$, $b=3$ is also possible.*

We now proceed to prove Theorem 2 by induction on the order of G. H is a characteristic subgroup of G so H certainly admits σ. By induction, if G_1 is a proper subgroup of G such that G_1 admits σ and $G_1\geqq H$, then $\sigma^{p^{n-1}}$ must be the identity on G_1/H. According to [2, Theorem C], this implies that

(1) G/H is a q-group for some prime q.

(2) Either $\phi(G/H)=1$ or $(G/H)'=\phi(G/H)=Z(G/H)$.

(3) $\langle\sigma\rangle$ is faithfully and irreducibly represented by the automorphisms induced on $(G/H)/\phi(G/H)$.

(Here $\phi(G)$ and $Z(G)$ denote the Frattini subgroup and center, respectively, of G.) Now there must be a Sylow q-group M of G such that M admits σ. Clearly $G=HM$ and $M\cong G/H$. Thus we must show that $\sigma^{p^{n-1}}$ fixes M elementwise. For convenience we set $\sigma^{p^{n-1}}=\sigma'$.

Now suppose x is an element of M not fixed by σ'. Let $y=(x,\sigma')$

$=x^{-1}x^{\sigma'}\neq 1$. Now since H contains its centralizer in G, it follows that there is a Sylow r-group K of H such that M normalizes K, K admits σ, and $(y, K)\neq 1$. Now let N be the centralizer of K in M, and consider the group KM/N. This group satisfies the hypothesis of Theorem 2, and so, if $H\neq K$, we must have σ' is the identity on M/N. But N is a proper subgroup of M (since $y\notin N$) so that σ' must fix N elementwise. Since p cannot divide the order of M, this would imply that σ' is the identity on M.

Thus we assume that H is an r-group for some prime r. Now $G/\phi(H)$ satisfies the hypothesis of the theorem, so by induction we may assume that $\phi(H)=1$. From now on we consider H as a vector space over a field F of characteristic r and we consider $M\langle\sigma\rangle$, the semidirect product of M and $\langle\sigma\rangle$, as a linear group operating on H. Since σ is fixed-point-free on G, σ, as a linear transformation, cannot have 1 as an eigenvalue. Now extending the field F does not change the structure of $\langle\sigma\rangle M$ nor the eigenvalues of σ. Accordingly we consider $\langle\sigma\rangle M$ as a linear group over a field F of characteristic r, and we assume that F is a splitting field for $\langle\sigma\rangle M$.

Now let V be an irreducible $F-\langle\sigma\rangle M$ submodule such that $(M, \sigma^{p^{n-1}})$ is not the identity on V. Next decompose V into the sum $V=V_1\oplus V_2\oplus\cdots$ of minimal characteristic $F-M$ submodules V_i. Since V is irreducible, σ must permute the V_i transitively. Let $\tau=\sigma^{p^m}$ be the first power of σ which fixes all the V_i, and number the V_i so that $V_i\sigma=V_{i+1\ (\mathrm{mod}\,p^m)}$. Next let N be the restriction of M to V, K_i the kernel of the representation of N afforded by the module V_i, and $Q_i=N/K_i$. Since $Z(Q_i)$ is represented by a scalar matrix on V_i, τ must fix $Z(Q_i)$ elementwise. Now $m=0$ would imply that $\tau=\sigma$, $V=V_1$, and $K_1=1$. Since σ must induce a fixed-point-free automorphism of $Z(N)$, this implies that $m>0$.

Now the argument in [5, pp. 704–708] shows that 1 must be an eigenvalue of σ unless $p^{n-m}=q^d+1$, Q_i is of order q^{2d+1}, and Q_i is an extra-special q-group. We now proceed to finish the proof of Theorem 2 by showing that under the conditions just stated, σ cannot be fixed-point-free on N'.

First $p^{n-m}=q^d+1$ implies that $q=2$ (since p is odd) and p is a Fermat prime $=2^s+1$. Thus either $d=s$, $n-m=1$ or, if $p=3$, we could have $d=3$, $n-m=2$. In any event d is the smallest positive integer such that $(2^{2d}-1)$ is divisible by p^{n-m}. Now $\sigma^{p^{n-1}}$ is not the identity on any V_i since $(M, \sigma^{p^{n-1}})$ is not the identity on V. For the same reason N/N' is a faithful $GF(q)-\langle\sigma\rangle$ module and Q_i/Q_i' is a faithful $GF(q)-\langle\tau\rangle$ module. But since $M/\phi(M)$ is an irreducible module for $\langle\sigma\rangle$ and since Q_i/Q_i' is of order 2^{2d}, it follows that N/N'

and Q_i/Q_i' are irreducible modules for $\langle\sigma\rangle$ and $\langle\tau\rangle$, respectively. From (2.1) it follows that the smallest integer k such that p^n divides (2^k-1) is $k=2sp^{n-1}=2dp^m$. Thus N/N' is of order 2^{2dp^m}. Now $Q_i=N/K_i$ and so Q_i/Q_i' is operator isomorphic as a $\langle\tau\rangle$-module to $N/(K_iN')$.

(2.3) LEMMA. (1) *For all* i, k *such that* $1\leqq i\leqq p^m$, $1\leqq k\leqq p^m$,

$$\left(\bigcap_{j=i}^{i+k-1} K_jN'\right)\Big/ N'$$

is of order $2^{2d(p^m-k)}$.

(2) *For all* i, k *such that* $1\leqq i\leqq p^m$, $1\leqq k<p^m$,

$$\left(\bigcap_{j=i}^{i+k-1} K_jN'\right)(K_{i+k}N') = N.$$

PROOF. Throughout, the indices j on the subgroups K_j are to be taken modulo p^m. Now if $k=1$, then

$$|K_iN'/N'| = |N/N'|/|N/K_iN'| = 2^{2d(p^m-1)}.$$

Now assume the first assertion of the lemma is true for a given $k<p^m$. Now

$$\left(\bigcap_{j=i}^{i+k-1} K_jN'\right)K_{i+k}N'/K_{i+k}N'$$

is a $\langle\tau\rangle$-submodule of $N/K_{i+k}N'$. Since $N/K_{i+k}N'$ is an irreducible $\langle\tau\rangle$-module, we conclude that either the second part of the lemma holds or

$$\bigcap_{j=i}^{i+k-1} K_jN' \leqq K_{i+k}N'.$$

In the latter case we certainly have

$$\bigcap_{j=i}^{i+k-1} K_jN' \leqq \bigcap_{j=i+1}^{i+k} K_jN' = \left(\bigcap_{j=i}^{i+k-1} K_jN'\right)^{\sigma}.$$

Since

$$N > \left(\bigcap_{j=i}^{i+k-1} K_jN'\right) > N'$$

from (1), this implies that

$$\left(\bigcap_{j=i}^{i+k-1} K_jN'\right)\Big/ N'$$

is a nontrivial proper $\langle\sigma\rangle$-submodule of the irreducible $\langle\sigma\rangle$-module N/N'. This contradiction establishes the second part of the lemma for the given value of k.

But then

$$N/K_{i+k}N' \cong \left(\bigcap_{j=i}^{i+k-1} K_jN'\right) \Big/ \left(\bigcap_{j=i}^{i+k} K_jN'\right).$$

But since

$$\left|\left(\bigcap_{j=i}^{i+k-1} K_jN'\right) \Big/ N'\right| = 2^{2d(p^m-k)} \quad \text{and} \quad \left| N/K_{i+k}N' \right| = 2^{2d},$$

this implies that

$$\left|\left(\bigcap_{j=i}^{i+k} K_jN'\right) \Big/ N'\right| = 2^{2d(p^m-k-1)}.$$

Thus part (1) of the lemma is proved for $k+1$. Then, by induction, the lemma is proved.

Now let $L_i = \bigcap_{j\neq i} K_jN'$ for all i, $1 \leqq i \leqq p^m$. From the lemma, $L_iK_i = L_iK_iN' = N$ for all i. Also since $L_i^\sigma = L_{i+1 \pmod{p^m}}$, $L_1L_2 \cdots L_{p^m}/N'$ is a nontrivial $\langle\sigma\rangle$-module. Thus $L_1L_2 \cdots L_{p^m} = N$. Our goal now is to show that N' is the direct product

$$L_1' \times L_2' \times \cdots \times L_{p^m}'.$$

To do this, we first need

(2.4) LEMMA. $(L_i, L_k) = 1$ *if* $i \neq k$.

PROOF. Suppose $(x, y) \neq 1$ for $x \in L_i$, $y \in L_k$. Choose t such that (x, y) is not the identity on V_t. Now at least one of L_i and L_k is contained in K_tN'. Without loss of generality assume that $L_i \leqq K_tN'$. Therefore $x = gh$ where $g \in K_t$, $h \in N'$. Now $N' \leqq Z(N)$. Therefore $(gh, y) = (g, y)$. But g is the identity on V_t which implies that (g, y) is also the identity on V_t. This proves the lemma.

As an immediate consequence of the lemma we have $N' = L_1'L_2' \cdots L_{p^m}'$. Now as in the proof just given, $L_i \leqq K_tN'$ implies that (L_i, N) is the identity on V_t. Since N is faithfully represented on V, this implies that L_i' is faithfully represented on V_i. Thus

$$| L_i' | = | Q_i' | = 2 \qquad \text{for all } i.$$

Now suppose $L_i' \cap \Pi_{j\neq i} L_j' \neq 1$. Then we would have $\Pi_{j\neq i} L_j'$ not the identity on V_i. But $j \neq i$ implies that $L_j' \leqq (L_j, N)$ is the identity on V_i. Thus $L_i' \cap \Pi_{j\neq i} L_j' = 1$ for all i. This implies that

$$N' = L_1' \times L_2' \times \cdots \times L'_{p^m}$$

and thus $|N'| = 2^{p^m}$. Since $|N'| \not\equiv 1 \pmod p$, N' cannot have a fixed-point-free automorphism whose order is a power of p. This concludes the proof of Theorem 2.

The proof of Theorem 1 now follows by induction on the order of G. First suppose G has two distinct minimal σ-admissible normal subgroups H_1, H_2. Then G is isomorphic to a subgroup of the direct product of G/H_1 and G/H_2 and both G/H_1 and G/H_2 satisfy the theorem. It then follows that G would satisfy the theorem.

Thus, for part (a) of the theorem, we may assume that the Fitting group $F_1(G)$ is a q-group for some prime q. Then $O_{qq'}(G)$ satisfies the conditions of Theorem 2. Therefore $\sigma^{p^{n-1}}$ is the identity on $O_{qq'}(G)/F_1(G)$. By [4, Lemma 4], this implies that $\sigma^{p^{n-1}}$ is the identity on $G/F_1(G)$. Then, by induction, we have

$$h(G) = 1 + h(G/F_1(G)) \leqq 1 + (n-1) = n.$$

For part (b) of Theorem 1, we may assume that $O_{\pi'}(G) = 1$. Then by one application of Theorem 2, $\sigma^{p^{n-1}}$ is the identity on $O_{\pi\pi'}(G)/O_\pi(G)$, and by a second application, $\sigma^{p^{n-2}}$ is the identity on $O_{\pi\pi'\pi}(G)/O_{\pi\pi'}(G)$. Thus, again using [4, Lemma 4], $\sigma^{p^{n-2}}$ is the identity on $G/O_{\pi\pi'}(G)$. Induction now implies that

$$l_\pi(G) = 1 + l_\pi(G/O_{\pi\pi'}(G)) \leqq 1 + [(n-1)/2] = [(n+1)/2].$$

All that remains now is to show that the inequalities in Theorem 1 are best-possible. For part (a), this follows from examples constructed by Shult [5, Theorem 5]. For part (b), however, Shult's construction has to be modified somewhat. Working by induction, Shult assumes that G_k is a solvable group of Fitting height k which admits a fixed-point-free automorphism of order p^k. Then if q_k is any prime such that $q_k \equiv 1 \pmod p$ and q_k does not divide the order of G, Shult proceeds to construct a new group G_{k+1} such that $F_1(G_{k+1})$ is a q-group, $G_{k+1}/F_1(G_{k+1})$ is isomorphic to G_k, $h(G_{k+1}) = k+1$, and G_{k+1} admits a fixed-point-free automorphism of order p^{k+1}. A close look at Shult's procedure reveals that it is only necessary that q_k does not divide the order of $F_1(G)$. Thus if q, r are distinct primes such that $q \equiv r \equiv 1 \pmod p$, Shult's procedure can be used to construct groups G_k with the following properties.

(1) G_k is a q, r-group.

(2) $F_1(G_k)$ is either a q- or an r-group.

(3) G_k admits a fixed-point-free automorphism of order p^k.

(4) $h(G_k) = k$.

It now follows that $l_q(G_k)$ and/or $l_r(G_k)$ is equal to $[(k+1)/2]$. Thus the inequality in part (b) is best-possible.

REFERENCES

1. D. Gorenstein and I. Herstein, *Finite groups admitting a fixed-point-free automorphism of order* **4**, Amer. J. Math. **83** (1961), 71–78.

2. P. Hall and G. Higman, *On the p-length of p-soluble groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc. (3) **6** (1956), 1–42.

3. G. Higman, *Groups and rings having automorphisms without non-trivial fixed elements*, J. London Math. Soc. **32** (1958), 321–334.

4. F. Hoffman, *Nilpotent height of finite groups admitting fixed-point-free automorphisms*, Math. Z. **85** (1964), 260–267.

5. E. Shult, *On groups admitting fixed point free abelian groups*, Illinois J. Math. **9** (1965), 701–720.

6. J. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad Sci. U.S.A. **45** (1959), 578-581.

7. ———, *Automorphisms of solvable groups*, J. Algebra **1** (1964), 259–267.

UNIVERSITY OF ALBERTA, EDMONTON