Fong, P.
Osaka J. Math.
13 (1976), 483–489

ON ORDERS OF FINITE GROUPS AND CENTRALIZERS OF p-ELEMENTS

To the memory of Otto Grün

PAUL FONG[1]

(Received July 28, 1975)

Introduction

The following theorem was recently proved by R. Brauer and the author [1]:

Theorem. *Let p be a prime. Then at least one of the following hold:*
(a) *There exists a function $f(c)$ with the following property: If G is a finite group of order divisible by p, and if $c=max\ \{|C_G(x)|: x\in G, x$ of order $p\}$, then $|G:O_{p'}(G)|\leqslant f(c)$.*
(b) *There exist infinitely many sporadic simple groups of order divisible by p.*

In this paper we shall see that a similar theorem holds when c is allowed to be $|C_G(x)|$ for any element x in G of order p. Indeed, consider the following two statements for a fixed prime p:

(I) There exists a function $f(c)$ with the following property: If G is a finite group of order divisible by p, x is an element of order p, $c=|C_G(x)|$, and $S(G)$ is the solvable radical of G, then $|G:O_{p',p}(S(G))|\leqslant f(c)$.

(II) There exists a function $g(c)$ with the following property: If G is a finite non-abelian simple group, τ is an automrophism of order p of G, and $c=|C_G(\tau)|$, then $|G|\leqslant g(c)$.

Clearly (I) implies (II). We shall prove that (II) implies (I). In particular, (I) holds when $p=2$ since an argument of Brauer and Fowler easily establishes (II) for $p=2$. If the simple groups G in (II) are restricted to be alternating or Chevalley groups, then it can be verified that the function $g(c)$ in (II) exists, and in fact $g(c)=c^N$ for some integer N will do. Hence (II) and (I) fail only if there exist infinitely many sporadic simple groups admitting automorphisms of order p.

This work was done at the Group Theory Symposium at the University of Warwick 1972–1973. Thanks are due to the many participants there for

[1] This work was supported by grant GP-34626 of the National Science Foundation.

their helpful comments. The observation that (II) holds for $p=2$ is due to D. Goldschmidt.

1. The equivalence of (I) and (II)

Lemma 1. *Let G be a finite group and x an element of G. If $\bar{G}$ and $\bar{x}$ are the images of G and x under a homomorphism of G, then $|C_{\bar{G}}(\bar{x})| \leqslant |C_G(x)|$.*

Proof: Since the irreducible characters χ of $\bar{G}$ can be viewed as irreducible characters χ of G, $|C_{\bar{G}}(\bar{x})| = \sum_{\chi} |\chi(\bar{x})|^2 = \sum_{\chi} |\chi(x)|^2 \leqslant |C_G(x)|$.

We recall that a group H is quasisimple if $H=H'$ is perfect and $H/Z(H)$ is a non-abelian simple group. If G is any group, $E(G)$ is the join of all subnormal, quasisimple subgroups of G.

Lemma 2. *Let p be a prime, and let G be a group with $O_{p'}(S(G))=1$. Then $C_G(E(G)O_p(G)) \leqslant O_p(G)$.*

Proof. By assumption $E(G)O_p(G)$ is the generalized Fitting subgroup $F^*(G)$ of G. Since $C_G(F^*(G)) \leqslant F^*(G)$ ([3], Theorem 1 (i)), the result is immediate.

Theorem 1. *Let p be a prime. Then* (I) *and* (II) *are equivalent.*

Proof. That (I) implies (II) is trivial. Conversely, suppose a function $g(c)$ exists satisfying (II). We claim that a monotonic function $f_1(c)$ exists with the following property: If G is a finite quasisimple group, τ is an automorphism of order p of G, and $c=|C_G(\tau)|$, then $|G| \leqslant f_1(c)$. Indeed, the automorphism $\bar{\tau}$ of $\bar{G}=G/Z(G)$ induced by τ has order p since G is perfect. Hence $|\bar{G}| \leqslant g(\bar{c})$, where $\bar{c}=|C_G(\bar{\tau})|$. On the other hand, $Z(G)$ is isomorphic to a subgroup of the Schur multiplier of $\bar{G}$, and so $|Z(G)| \leqslant |\bar{G}|^2$ by a result of Green ([4], Lemma 6.2 and Corollary). Thus $|G| \leqslant g(\bar{c})^3$. Since $\bar{c} \leqslant c$ by Lemma 1, we may then define the function f_1 by setting

$$f_1(c) = \max_{1 \leqslant c \leqslant c} \{g(\bar{c})^3\} .$$

This establishes the claim.

Next let G be any finite group of order divisible by p with $O_{p'}(S(G))=1$. Let $C=C_G(E(G))$ and $C_0=C_C(O_p(G)/\phi(O_p(G)))$, so that $C_0 \leqslant O_p(G)$ by Lemma 2 and a theorem of Burnside. Now G/C and C/C_0 act faithfully on $E(G)$ and V respectively, where $V=O_p(G)/\phi(O_p(G))$. Since $|G:O_p(G)| \leqslant |G:C_0| = |G:C|\,|C:C_0|$, upper bounds by functions of c on $|E(G)|$ and $|V|$ imply one on $|G:O_p(G)|$.

Let x be an element of order p and let $c=|C_G(x)|$. The element x induces a linear transformation of order 1 or p on V. Since $|C_V(x)| \leqslant c$ by Lemma 1, it then follows that $|V| \leqslant c^p$. The element x also induces a permutation of the quasisimple components of $E(G)$. Let the orbits be $O_1, \cdots, O_s, O_{s+1}, \cdots, O_{s+t}$, arranged so that $|O_1| = \cdots = |O_s| = 1$ and $|O_{s+1}| = \cdots = |O_{s+t}| = p$. If $1 \leqslant i \leqslant s$, then O_i consists of a single quasisimple group G_i on which x induces an automorphism of order 1 or p. Since $|C_{G_i}(x)| \leqslant c$, it follows that

$$(1.1) \qquad |G_i| \leqslant max\ \{f_1(c), c\} \qquad \text{for} \quad 1 \leqslant i \leqslant s\,.$$

If $s+1 \leqslant i \leqslant s+t$, then the quasisimple components in O_i are permuted cyclically by x. Let these be $G_{i1}, G_{i2}, \cdots, G_{ip}$, where $G_{ij} = G_{i1}{}^{x^{j-1}}$. Then $D_i = \{hh^x \cdots h^{x^{p-1}} : h \in G_{i1}\}$ is a subgroup of $G_{i1} G_{i2} \cdots G_{ip}$ centralized by x. In particular, $|D_i| \leqslant c$. Since $D_i/Z(D_i) \simeq G_{i1}/Z(G_{i1})$, it follows that $|G_{i1}/Z(G_{i1})| \leqslant c$ as well. Thus

$$(1.2) \qquad |G_{i1}| \leqslant c^3 \qquad \text{for} \quad i > s$$

by the result of Green quoted earlier. The components in each orbit then have bounded orders by (1.1), (1.2). But the number of orbits $s+t$ is itself bounded by c. Indeed, let $\bar{G} = G/Z(E(G))$ and let $\bar{X}$ denote the image of X in $\bar{G}$ for any subset or element X of G. The orbits of $\bar{x}$ acting on the simple components of $\overline{E(G)}$ are the images of the orbits of x acting on the quasisimple components of $E(G)$. Moreover, $|C_{\overline{E(G)}}(\bar{x})| \leqslant |C_{E(G)}(x)| \leqslant c$ by Lemma 1. Now $\bar{x}$ centralizes a non-identity element of each $\bar{G}_i$ for $1 \leqslant i \leqslant s$ by a thoerem of Thompson [9], and $\bar{x}$ centralizes a non-identity element of each product $\bar{G}_{i1} \bar{G}_{i2} \cdots \bar{G}_{ip}$ for $s+1 \leqslant i \leqslant s+t$ since $[\bar{x}, \bar{D}_i] = 1$. Hence $s+t \leqslant c$. Thus $|E(G)| \leqslant$ max $\{f_1(c)^c, c^{3pc}\}.|$. A function $f_2(c)$ then exists such that $|G| \leqslant f_2(c)$.

Finally let G be any group of order divisible by p and let $\bar{G} = G/O_{p'}(S(G))$. Let x be an element of order p in G and $\bar{x}$ be its image in $\bar{G}$. Since $\bar{c} = |C_{\bar{G}}(\bar{x})| \leqslant |C_G(x)| \leqslant c$ by Lemma 1 and $|G : O_{p',p}(S(G))| = |\bar{G} : O_p(\bar{G})|$, we may then define the function $f(c)$ needed for (I) by

$$f(c) = \max_{1 \leqslant \bar{c} \leqslant c} \{{}_2f(\bar{c})\}\ .$$

This completes the proof.

Corollary. (I) *holds for* $p=2$.

Proof. We shall show that (II) holds for $p=2$ with $g(c) = (2c(2c+1))!$. The argument is essentially that of Brauer and Fowler [2]. Let G be the semidirect product of H and $\langle \tau \rangle$, and let $\{1\} = K_0, K_1, \cdots, K_s$ be the conjugacy classes of G containing an element inverted by τ. We note that $s \geqslant 1$ since $|G|$ is even. Also let K be that class among $K_1, \cdots, K_s$ which contains τ. Using the symbol for a class to denote the corresponding class sum in the group ring $Z[G]$ as well, we have

$$(1.3) \qquad K^2 = \sum_{i=0}^{s} m_i K_i ,$$

where the m_i are non-negative integers. Indeed, $m_0 = |K|$ and $m_i \leqslant |G|/|K_i|$ for $1 \leqslant i \leqslant s$, the latter inequality holding since $p=2$. Thus (1.3) implies

$$(1.4) \qquad |K|^2 = |K| + \sum_{i=1}^{s} m_i |K_i| \leqslant |K| + s|G| .$$

On the other hand, a count of the elements in $K_0, K_1, \cdots, K_s$ implies

$$(1.5) \qquad |G| \geqslant \sum_{i=1}^{s} |K_i| \geqslant s|K'| ,$$

where K' is chosen from $K_1, \cdots, K_s$ to minimize $|K_i|$. The inequalities (1.4) and (1.5) imply that

$$(1.6) \qquad |K|^2 |K'| \leqslant |K|\,|K'| + |G|^2 .$$

Setting $|K| = |G{:}C_G(\tau) = |G|/2c$ and $|K'| = |G|/c'$ into (1.6), we obtain $|G|/c' \leqslant 2c(2c+1)$. Since c' is the order of the subgroup $C_G(g')$, where $g' \in K'$, G then has a normal subgroup N contained in $C_G(g')$ such that G/N is isomorphic to a subgroup of the symmetric group on $2c(2c+1)$ symbols. Moreover, $N=G$ or 1 since H is simple. If $N=G$, then $G \cong H \times Z_2$ and τ must be an inner automorphism. The theorem of Brauer and Fowler applies to this situation and yields $|H| \leqslant (\frac{1}{2}c(c+2))!$. If $N=1$, then $|H| \leqslant (2c(2c+1))!$. Thus $|H| \leqslant g(c)$ in all cases.

2. (II) for alternating and Chevalley groups

Theorem 2. *Let p be prime. Then there exists a natural integer N with the following property: If G is a finite non-abelian simple alternating or Chevalley group, τ is an automorphism of order p of G, and $c = |C_G(\tau)|$, then $|G| \leqslant c^N$.*

Proof. We shall only give a cursory outline of the proof, since much more precise information on $C_G(\tau)$, when G is a Chevalley group, is currently being tabulated by N. Burgoyne and others. The groups and their automorphisms will be discussed in a finite number of cases. Clearly it suffices to prove the existence of the exponent in each case. Also in any given case, finitely many groups can be omitted from the discussion without affecting the proof.

If G is an alternating group of degree $n > 6$, then the automorphism τ is induced by an element x of order p in the corresponding symmetric group of degree n. Using estimates provided by Stirling's formula, we easily find an exponent for this case.

We need two arrangements of the Chevalley groups. The first is

(2.1a) $PSL_n(q)$, $PSU_n(q)$, $PSp_{2n}(q)$, $P\Omega_{2n+1}(q)$, $P\Omega_{2n}(\varepsilon, q)$

(2.1b) $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$, ${}^2C_2(q^2)$, ${}^3D_4(q^3)$,, ${}^2E_6(q^2)$, ${}^2F_4(q^2)$, ${}^2G_2(q^2)$,

and separates the families of classical type from the rest. The second is

(2.2a) $A_n(q)$, $B_n(q)$, $C_n(q)$, $D_n(q)$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$,

(2.2b) ${}^2A_n(q^2)$, ${}^2C_2(q^2)$, ${}^3D_4(q^3)$, ${}^2D_n(q^2)$, ${}^2E_6(q^2)$, ${}^2F_4(q^2)$, ${}^2G_2(q^2)$,

and separates the families of normal type from the rest. The Lie notation is that of [6], so that the characteristic power q need not be an integer.

The automorphism group $A(G)$ of a simple Chevalley group G has a normal series

$$G \cong A_0(G) \leqslant A_1(G) \leqslant A_2(G) \leqslant A_3(G) = A(G)\,,$$

where $A_0(G)$ is the group of inner automorphisms, and $A_i(G)$ is the group obtained from $A_{i-1}(G)$ by adjoining certain automorphisms, namely diagonal automorphisms when $i=1$, field automorphisms when $i=2$, and graph automorphisms when $i=3$. The labeling of automorphisms as diagonal, field, or graph automorphisms depends on the choice of a Tits system for G which we assume fixed.

Case 1: τ in $A_1(G)$

If G is of type (2.1a), then τ is induced by some element x in a corresponding linear group. Using the work [11] of G.E. Wall, we obtain an exponent which works for these groups when n is sufficiently large, say $n \geqslant n_0$. The remaining groups are of type (2.1a) with $n < n_0$, or of type (2.1b), and hence belong to a finite number of families, where each family is parameterized by q. The argument given for a similar situation in [1] in the proof of Theorem 2 applies.

Case 2: τ in $A_2(G) - A_1(G)$

Theorems of Lang [5] and Steinberg [8], Theorem 10.1, can be used to identify $C_G(\tau)$, from which the theorem follows, except in the cases $p=2$ and G is any group other than ${}^3D_4(q^3)$ in (2.2b), or $p=3$ and $G={}^3D_4(q^3)$. We shall return to these exceptions after discussing the next case.

Case 3: τ in $A_3(G) - A_2(G)$

The automorphisms in this case exist only if $p=2$ or 3, G is one of the groups

(2.3a) $A_n(q)$, $D_n(q)$, $E_6(q)$

(2.3b) $C_2(q)$, $F_4(q)$, $G_2(q)$,

and q is a power of 2 or 3 in the case (2.3b). The proof of the previous case can be used unless G is of type (2.3a) and $\tau=\beta\alpha$, where β is a graph automorphism and $\alpha\in A_1(G)$. Suppose we have one of these cases. If p does not divide q, we proceed as follows: The cases $p=2$ and $G=A_n(q)$, $p=3$ and $G=D_4(q)$ follow by results of Steinberg [7], page 169, and Tits [10], §§8.2.8, 9.1.2, 9.2.1, and the remark following 9.2.1. If $p=2$ and $G=D_n(q)$ or $E_6(q)$, we view $A_1(G)$ as the fixed-point set of an algebraic endomorphism σ of a corresponding algebraic group $\bar{G}$, and extend τ to an algebraic automorphism $\bar{\tau}$ of order p of $\bar{G}$ such that $\sigma\bar{\tau}=\bar{\tau}\sigma$. In particular, $C_G(\tau)$ is related to the fixed-point set of σ on $C_{\bar{G}}(\bar{\tau})$, which can be studied by choosing an appropriate Tits system of $\bar{G}$. If p divides q, then τ fixes a Sylow p-subgroup U of G, and in fact centralizes a suitably large subgroup of U. In every case, the existence of the exponent can be shown.

Finally, we return to the exceptions noted in case 2, which were in fact the twisted forms of the groups in (2.3). As before, we can view $A_1(G)$ as the fixed-points of an algebraic endomorphism σ of a corresponding algebraic group $\bar{G}$, and extend τ to an algebraic endomorphism $\bar{\tau}$ of $\bar{G}$ such that σ induces an automorphism of $C_{\bar{G}}(\bar{\tau})$. The proof is then completed by appealing to the previous two cases.

University of Illinois

References

[1] R. Brauer and P. Fong: *On the centralizers of p-elements in finite groups*, Bull. London Math. Soc. **6** (1974), 319–324.

[2] R. Brauer and K. Fowler: *On groups of even order*, Ann. of Math. **62** (1955), 565–583.

[3] D. Gorenstein and J. Walter: *The π-layer of a finite group*, Illinois J. Math. **15** (1971), 555–564.

[4] J.A. Green: *On the number of automorphisms of a finite group*, Proc. Royal Soc. **237** (1956), 574–581.

[5] S. Lang: *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[6] T. Springer and R. Steinberg: *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Math., No. 131 Springer-Verlag, 1970.

[7] R. Steinberg: Lectures on Chevalley groups, Yale University, 1967.

[8] R. Steinberg: *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. **80** (1968), 1–108.

[9] J. Thompson: *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci. **45** (1959), 578–581.

[10] J. Tits: *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Études Sci. Publ. Math. **2** (1959), 37–84.

[11] G.E. Wall: *On the conjugacy classes in the unitary, symplectic, and orthogonal groups*, J. Australian Math. Soc. **3** (1963), 1–62.