

A GENERAL BRAUER-FOWLER THEOREM AND CENTRALIZERS IN LOCALLY FINITE GROUPS

BRIAN HARTLEY

A classical theorem of Brauer and Fowler, proved by quite elementary arguments, states that the order of a finite non-abelian simple group G is bounded in terms of the order of the centralizer of any involution in G . Here we use the classification of finite simple groups to show that the order of such a G is bounded in terms of the order of any automorphism α and the number of fixed points of α . It follows easily that if a locally finite group contains an element with finite centralizer, then it has a locally solvable subgroup of finite index.

1. Introduction. The main result of this paper is the following.

THEOREM A. *There exists an integer-valued function $f(n, k)$ such that if G is a finite group containing an element x of order n such that $|C_G(x)| \leq k$, then G has a soluble normal subgroup of index dividing $f(n, k)$.*

It will be useful to say that a quantity is a, b, \dots -bounded, if it is bounded above by some function of a, b, \dots . We shall see that Theorem A follows rather easily from the next result, the proof of which occupies the bulk of the paper.

THEOREM A'. *Let G be a finite non-abelian simple group admitting an automorphism of order n with at most k fixed points. Then $|G|$ is n, k -bounded.*

This is the general Brauer-Fowler Theorem referred to in the title. In sharp contrast to the real Brauer-Fowler Theorem [5], its proof depends on the classification of finite simple groups. The case of inner automorphisms was dealt with in [14, Theorem A1]. It is unclear whether there is more to be said about the structure of the soluble normal subgroup in Theorem A. Conceivably it should have a subgroup of n, k -bounded index and n -bounded Fitting height. This is the case when n is a prime power (see Theorem B below). See also [13] for further discussion of this.

A standard inverse limit argument, given in §2, establishes the following consequence of Theorem A.

COROLLARY A1. *If G is a locally finite group containing an element with finite centralizer, then G has a locally soluble normal subgroup of finite index.*

For elements of prime power order, one can say rather more than Theorem A. Taking into account [12], the following may either be deduced from Theorem A, or deduced from Theorem A' by an argument analogous to Brauer-Fong [4]. We leave the details to the reader.

THEOREM B. *If G is a finite group containing an element x of prime power order p^n with $|C_G(x)| \leq k$, then $|G : F_n O_{p',p}(G)|$ is p^n , k -bounded, where $F_n(G)$ is the n -th term of the Fitting series of G .*

COROLLARY B1. *If p is a prime and G is a locally finite group containing an element of prime power order p^n with finite centralizer, then G contains a normal subgroup H of finite index such that $H = O_{p',p}(H) = F_n(H)$.*

Here, $F_n(H)$ is defined inductively by putting $F_0(H) = 1$ and taking $F_{i+1}(H)/F_i(H)$ to be the Hirsch-Plotkin radical of $H/F_i(H)$. Corollary B1 is deduced in a similar way to Corollary A1.

The methods used to prove Theorem A' enable us to improve [11] Theorem 2 by removing some exceptions which we were not able to deal with before.

THEOREM C. *Let G be an infinite simple group of Lie type over a locally finite field K of characteristic p , and let α be an automorphism of finite order n of G . Suppose that p does not divide n . Then there exist infinitely many primes q such that α fixes an element of order q of G .*

This was proved in [11] provided that if G has type ${}^2B_2, {}^2F_4$, or 2G_2 , or if n is even and G has type G_2 , then n is a prime power. However, we will give a new and simpler proof of the general case here.

An important ingredient in the proof of Theorem A' is the knowledge of centralizers in G of elements in $\text{Aut } G \setminus \text{Inndiag } G$, where G is a group of Lie type and $\text{Inndiag } G$ the subgroup of $\text{Aut } G$ generated by the inner and diagonal automorphisms. Most of these centralizers

are given in [9], except for involutory “graph automorphisms” in their sense, and most of these have been worked out elsewhere. The case of the even-dimensional orthogonal groups in odd characteristic does not seem to be in the literature in a fully convenient form, though much of it is in Dieudonné [8]. We give a brief discussion of this in §3.

The work for this paper was carried out at the University of Oregon. The author is grateful to the SERC of the United Kingdom for financial assistance. He also warmly thanks Gary Seitz for much hospitality and kindness, as well as numerous conversations which were essential to the development of the proof.

2. Deductions from Theorem A'.

Deduction of Theorem A. It is more convenient (but equivalent) to think of x as an automorphism of G and work in the semidirect product $H = G\langle x \rangle$.

Suppose first that $G = G_1 \times \cdots \times G_s$ is a direct product of non-abelian simple groups G_i . Then x permutes the direct factors in orbits of lengths dividing n . If G_{i_1}, \dots, G_{i_t} is such an orbit and $K = G_{i_1} \times \cdots \times G_{i_t}$, then $C_K(x) \cong C_{G_{i_1}}(x^t)$. It is a well known consequence of the classification of finite non-abelian simple groups that no such group can admit a fixed-point-free automorphism (see [11] Lemma 4.1 for example). Consequently, $C_K(x) \neq 1$. Therefore the number of orbits is at most k . Since $|C_{G_{i_1}}(x^t)| \leq k$ we have a bound on $|G_{i_1}|$ from Theorem A', and hence on $|K|$. Consequently, $|G|$ is n, k -bounded.

In general, we form part of a chief series of H passing through G and consider a non-abelian chief factor U/V . We have $|C_{U/V}(x)| \leq k$ [2, VIII.10.14], so by what has just been said, $|U/V|$ is n, k -bounded. Let $N = \bigcap C_G(U/V)$ over all non-abelian chief factors U/V in our fixed chief series. Then N is soluble. As $G/C_G(U/V)$ is embedded in $\text{Aut } U/V$, its order is n, k -bounded.

Passing to G/N , we may assume that $N = 1$, and so G has a family Λ of x -invariant normal subgroups L such that $\bigcap_{L \in \Lambda} L = 1$ and $|G/L|$ is n, k -bounded for each $L \in \Lambda$. Now we use induction on k . If $k = 1$, then G is soluble as we have remarked. Otherwise we can choose $L \in \Lambda$ such that $C_G(x) \not\leq L$. Then by induction, L has a soluble normal subgroup S of $n, k/2$ -bounded index, and since $|G/L|$ is n, k -bounded, so is $|G:S|$.

Deduction of Corollary A1. Let G be a locally finite group containing an element x , of order n say, with finite centralizer of order k .

By Theorem A, we have a number f such that if F is any finite subgroup of G containing x , then F contains a soluble normal subgroup of index at most f . Let $\Sigma(F)$ be the set of all such subgroups of F and Φ the set of all finite subgroups of G containing x . If $F_i \in \Phi$ ($i = 1, 2$), $F_1 \geq F_2$, and $S \in \Sigma(F_1)$, then $S \cap F_2 \in \Sigma(F_2)$. Thus $\pi_{F_1 F_2} : S \mapsto S \cap F_2$ maps $\Sigma(F_1)$ into $\Sigma(F_2)$. We have an inverse system $\Sigma(F)_{F \in \Phi}$ of finite non-empty sets. The inverse limit is non-empty [15], and so we can choose $S_F \in \Sigma(F)$, one for each $F \in \Phi$, such that $S_{F_1} \cap F_2 = S_{F_2}$ whenever $F_1 \geq F_2$. Let $S = \bigcup_{F \in \Phi} S_F$. It is easy to see that this is a locally soluble normal subgroup of G of index at most f .

3. Some background results. Because of the classification of finite simple groups, which tells us among other things that there are only finitely many sporadic groups, the latter can be ignored in proving Theorem A'. This leaves us with alternating groups and groups of Lie type. The alternating groups are easy to handle and will be left to the reader. We now set up terminology for groups of Lie type and assemble some basic facts, many of which will be well known. For general background in this area, see [3, 7, 17].

Notation. \overline{G} denotes a connected reductive algebraic group over an algebraically closed field K of characteristic $p > 0$. Let σ be a Frobenius map on \overline{G} in the sense of [7, p. 31]. When \overline{G} is semisimple, this means precisely that σ is a surjective algebraic endomorphism of \overline{G} with finite fixed point group \overline{G}_σ . Sometimes we denote the fixed point group by $C_{\overline{G}}(\sigma)$. Let $G = O^{p'}(\overline{G}_\sigma)$. It is well known that σ fixes a Borel subgroup B of \overline{G} and a maximal torus T of \overline{G} contained in B . Let $N = N_{\overline{G}}(T)$ and $W = N/T$ be the Weyl group. Let σ^* be the map induced by σ on the character group $X = X(T)$ and on its real extension $X_R = X \otimes R$. There is a unique smallest integer $\delta \geq 1$ such that $\sigma^{*\delta}$ is a positive integral multiple of the identity, and we can write then $\sigma^* = q\sigma_0$, where $q = q(\sigma)$ is a positive real number and $\sigma_0^\delta = 1$. See [7], also [14, Section 3].

Suppose now that \overline{G} is simple as algebraic group. In this case, σ_0 is an isometry of X_R [17, p. E21]. The number q is an integral power of p except in types ${}^2B_2, {}^2F_4, {}^2G_2$, when q^2 is an odd power of 2, 2 or 3 respectively, and G is considered as defined over F_q except in the three cases just mentioned, when it is considered as defined over F_{q^2} (see [7, p. 36]). We often think of G as a Chevalley group constructed from a complex simple Lie algebra. Let **Chev** denote the

collection of all such groups G . If \overline{G} is also of adjoint type, then G is simple except in a few small cases, and all finite simple groups of Lie type arise in this way.

Our notation and terminology for automorphisms of G is sometimes consistent with [6], [19] and sometimes with [9, p. 78 *et seq.*]. This is unfortunate since their terminologies are sometimes in conflict, especially as regards graph automorphisms, but seems inescapable. When we use the undecorated terms “graph automorphism” and “field automorphism”, we do so in the sense of [6], [19]. In particular, we have in mind a fixed parametrization of G as a Chevalley group. We write “GL-graph automorphism” (for Gorenstein-Lyons), when we wish to speak of a graph automorphism in the sense of [9]. We have (see [9])

$$(3.1) \quad A = \text{Aut } G = \overline{G}_\sigma \Phi_G \Gamma_G,$$

where we have identified \overline{G}_σ with the group $\text{Inndiag } G$ it induces on G by conjugation, Φ_G is the group of field automorphisms of G , and Γ_G is a canonical set of graph automorphisms constructed as in [19, p. 157] or [6], together with, and perhaps consisting only of, the identity map. There is uniqueness of expression in the above.

We do not need to explain fully the terminology of [9], except to clarify the term “GL-graph automorphism”. An element α is a GL-graph automorphism if and only if either (i) G is untwisted and not of type B_2 , F_4 , or G_2 , and $\alpha \in \overline{G}_\sigma \Gamma_G \setminus \overline{G}_\sigma$, or (ii) G is twisted, the associated twist, or symmetry of the Dynkin diagram, has order d , and α is an element of $A \setminus \overline{G}_\sigma$ of order divisible by d . This is not quite what is said, but appears to be what is intended, in [9]. In particular, the groups B_2 , F_4 and G_2 have no GL-graph automorphisms. We need the following, which in most cases is well known.

LEMMA 3.1. *Suppose that \overline{G} is simple of adjoint type. Let α be an element of prime order r in $A \setminus \overline{G}_\sigma$. Then $C_G(\alpha)$ involves a finite non-abelian simple group H such that $|G|$ is $|H|$, r -bounded.*

Proof. This follows from [9, (9.1)] except in the case when $r = 2$ and α is a GL-graph automorphism. When G is untwisted this means that $\alpha \in \overline{G}_\sigma \gamma \setminus \overline{G}_\sigma$, where γ is an element of order 2 in Γ_G , and G has type A_l , D_l or E_6 . In characteristic 2 these cases are covered in [1]. Recalling that the graph automorphism of $P\Omega^+(2l, q)$ is induced by conjugation with an involution in $O^+(2l, q)$ [6, p. 272], we find the case D_l in [1, (8.7), (8.10)]. Types A_l and E_6 are in [1, (19.8),

see also §13]. For types A_l and E_6 in odd characteristic, see [10, Lemmas 4.25 and 4.27 and Remark 4.28]. The orthogonal groups D_l in odd characteristic do not appear to be covered in the literature and we deal with them in Lemma 3.2 below.

When G is twisted, the statement that α is a GL-graph automorphism of order 2 means that $\alpha \in \overline{G}_\sigma \gamma \setminus \overline{G}_\sigma$, where γ is the element of order 2 in Φ_G , and G has type ${}^2A_l, {}^2D_l, {}^2E_6$. In characteristic 2 we consult [1, (8.7), (19.8)]. In odd characteristic, types 2A_l and 2E_6 are dealt with in [10], see Lemmas 4.26 and 4.29 and Remark 4.30. This leaves the orthogonal groups 2D_l in odd characteristic, and they are also dealt with in Lemma 3.2 below.

We now set up some background on the orthogonal groups, in preparation for Lemma 3.2.

For some of what follows, and general background, see [8]. Let $S = \mathrm{SO}(2l, K)$, where K is an algebraically closed field of odd characteristic $p > 0$. Then S is a group of invertible linear transformations of a $2l$ -dimensional vector space V over K , preserving a non-degenerate symmetric bilinear form f on V . Since all such forms are equivalent, we may take f to have matrix

$$E_{2l} = \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix}.$$

with respect to a suitable basis $x_1, \dots, x_l, x_{-1}, \dots, x_{-l}$ of V . Let γ be given by

$$\gamma(x_{\pm l}) = x_{\mp l}; \quad \gamma(x_j) = x_j \quad (j \neq l).$$

Then γ preserves f , and so $\gamma \in O(2l, K)$. From [6, p. 272], we have that conjugation with γ induces on $SO(2l, K)$ its canonical graph automorphism (there is a natural root structure in this situation). We have

$$O = O(2l, K) = SO(2l, K) \rtimes \langle \gamma \rangle.$$

Let q be a power of p , think of G as a matrix group with respect to the above choice of basis, and let σ be the q -th power map on S . Then σ and $\sigma\gamma$ are Frobenius maps on S and induce Frobenius maps on $\overline{G} = \mathrm{PSO}(2l, K)$. The group \overline{G} is the adjoint group of type D_l , and

$$O^{p'}(\overline{G}_\tau) \cong P\Omega^\pm(2l, q),$$

where the plus sign is taken if $\tau = \sigma$ and the minus sign if $\tau = \sigma\gamma$. We are interested in the centralizers in $O^{p'}(\overline{G}_\tau)$ of involutions in $\overline{G}_\tau \langle \gamma \rangle$, and in particular in the non-abelian composition factors of these centralizers.

LEMMA 3.2. Let \overline{G} be as above, with $l > 1$, let w be any involution in $\overline{G}_\tau \langle \gamma \rangle$, and let $G = O^{p'}(\overline{G}_\tau)$. Then $C_G(w)$ involves at least one (and at most two) of the groups

$$P\Omega^\pm(l, q^2), \text{PSL}(l, q), \text{PSU}(l, q), P\Omega^\pm(2l-1, q), \\ P\Omega^{\varepsilon_1}(d, q) \times P\Omega^{\varepsilon_2}(2l-d, q) \quad (\varepsilon_i \in \{\pm 1\}, 1 < d < l).$$

More detail can be extracted from the proof, but we have no need of it.

Proof. Since \overline{G}_τ/G is of order dividing 4 [6, p. 99], it suffices to show that $C_{\overline{G}_\tau}(w)$ involves one of the above groups. Let Z be the centre of S . Then $Z = \langle -1 \rangle$. For any element $x \in O$, let

$$C^*(x) = \{g \in S : x^g = \pm x\}.$$

Then $C^*(x)/Z = C_{\overline{G}_\tau}(xZ)$. We calculate $C^*(w)$ for each element $w \in O$ such that wZ has order 2. If wZ is τ -invariant and $C = C^*(w)/Z$, then

$$C_{\overline{G}_\tau}(wZ) = C_\tau$$

and our results will follow from standard facts about Frobenius maps.

Now wZ is an involution if and only if w is either an involution different from -1 , or an element of order 4 whose square is -1 .

Suppose first that u is an involution, $u \neq -1$. Then we have

$$V = V_- \oplus V_+,$$

where V_- and V_+ are respectively the -1 and $+1$ -eigenspaces of u . These eigenspaces are orthogonal, and so the restriction of f to them is non-degenerate. Let $d = \dim V_-$, and $C^* = C^*(u)$. Then C^* leaves V_- and V_+ invariant if $d \neq l$, and permutes them if $d = l$. We clearly have

$$C^*(u) = (O(d, K) \times O(2l-d, K)) \cap S \quad (d \neq l),$$

and

$$C^*(u) = (O(l, K) \wr C_2) \cap S \quad (d = l).$$

Some abuse of notation is involved on the right hand side, but it should be clear what is intended.

Now let v be an element of order 4 in O such that $v^2 = -1$. Let ζ be a primitive 4-th root of 1 in K . Then

$$V = V_\zeta \oplus V_{-\zeta}$$

is the direct sum of the ζ - and $-\zeta$ -eigenspaces of v . These are easily seen to be totally isotropic, and hence by Witt's Theorem they have dimension at most l . Therefore $\dim V_\zeta = \dim V_{-\zeta} = l$. Each of these spaces induces the full dual of the other with respect to f . An element of $C^*(v)$ either fixes both V_ζ and $V_{-\zeta}$ or interchanges them, and in the former case, its actions on these two spaces must be mutually dual. We see that

$$C^*(v) = (\mathrm{GL}(l, K)\langle t \rangle) \cap S,$$

where t is an element of order 2 interchanging V_ζ and $V_{-\zeta}$ and inducing the inverse transpose map on $\mathrm{GL}(l, K)$.

It follows that the semisimple part of $C^*(u)/Z$ is either a central product (possibly direct) of two special orthogonal groups whose degrees sum to $2l$, or $\mathrm{SO}(2l-1, K)$ in case $d = 1$ or $2l-1$, and that of $C^*(v)/Z$ is a central extension of $\mathrm{PSL}(l, K)$.

Now if w is any involution in $\overline{G}_\tau\langle\gamma\rangle$, then w has the form u or v above, and wZ is τ -invariant. Hence $C = C^*(w)/Z$ is τ -invariant, and τ induces a Frobenius map on it.

By standard facts, the perfect radical of C_τ will be a central product of one or two central extensions of finite versions (possibly twisted) of the simple components of C^*/Z , defined over the field of q or q^2 elements. See [14], Lemma 3.3 and proof of Theorem C: finite case. The result follows.

The next result can be found for maximal tori of semisimple groups in [16, (2.4)], but the present case needs a little work and seems worth spelling out. Note that the possibility $S = \overline{G}$ is allowed.

LEMMA 3.3. *Let \overline{G} be connected reductive, and S be an arbitrary non-trivial σ -invariant torus of \overline{G} . Let S have rank r . Then $|S_\sigma| = |f(q)|$, where $f(X)$ is a real monic polynomial of degree r whose roots are roots of 1 of degree at most r^2 over the rationals. If \overline{G} is simple, then r^2 can be replaced by $2r$. Hence*

$$(q-1)^r \leq |S_\sigma| \leq (q+1)^r.$$

Proof. The map σ induces a Frobenius map on $C_{\overline{G}}(S)/S$ and fixes a maximal torus U/S of this group [8, p. 33]. Then U is a σ -invariant maximal torus of \overline{G} . Let W be the character group of U , and

$$S^\perp = \{\chi \in W : \chi(s) = 1 \text{ for all } s \in S\}.$$

Then $\overline{W} = W/S^\perp$ is naturally isomorphic to the character group $X(S)$ of S [8, p. 26]. Let σ^* be the map induced on the character group

of W by σ , so that

$$\sigma^* \chi(u) = \chi(\sigma(u)) \quad \text{for } \chi \in W, u \in U.$$

Then S^\perp is σ^* -invariant, and S_σ is in duality with, and hence isomorphic to, $\overline{W}/(\sigma^* - 1)\overline{W}$. By standard facts, the order of this group is $|\det(\sigma^* - 1)_{\overline{W}}|$, where $(\sigma^* - 1)_{\overline{W}}$ is the endomorphism induced on \overline{W} by $\sigma^* - 1$. In calculating this determinant, we can replace \overline{W} by its real extension \overline{W}_R . Then σ^* takes the form $q\sigma_0$, where σ_0 has finite order. For this is true of a maximally split torus, as is well known, and in general we twist by an element of the Weyl group, which just modifies σ_0 by an isometry of finite order. Thus, if $\overline{\sigma}_0$ is the map induced on \overline{W}_R by σ_0 , then

$$\begin{aligned} |S_\sigma| &= |\det(q\overline{\sigma}_0 - 1)| = |\det(q - \overline{\sigma}_0^{-1})| \cdot |\det \overline{\sigma}_0| \\ &= |\det(\overline{\sigma}_0^{-1} - q)| = |f(q)|, \end{aligned}$$

where f is the characteristic polynomial of $\overline{\sigma}_0^{-1}$. Since $\overline{\sigma}_0^{-1}$ has finite order, the roots of f are roots of 1. We have $f(X) = \prod_{i=1}^r (X - \zeta_i)$, where the ζ_i are roots of 1, hence $(q - 1)^r \leq |f(q)| \leq (q + 1)^r$, by the triangle inequality.

It remains only to give a (probably rather crude) estimate for the degrees over Q of the eigenvalues of σ_0 . If ζ is such an eigenvalue, then $q\zeta$ is an eigenvalue of σ^* , so $q\zeta$ is an algebraic integer of degree at most r over Q . Taking the absolute value of its norm, we find that $q^t \in \mathbb{Z}$ for some $t \leq r$, whence ζ^t has degree at most r over Q . Hence ζ has degree at most r^2 over Q . If \overline{G} is simple, then q^2 is an integer, and the above argument yields $2r$ instead of r^2 .

Much, if not all, of the next result is well known.

LEMMA 3.4. *Let \overline{G} be simple of adjoint type and let s be a semisimple element of order n in \overline{G}_σ . Then $C_G(s)$ contains a product $Y_1 \cdots Y_t$ of pairwise commuting groups in **Chev**, defined over extension fields of that over which G is defined. If \overline{G} is of classical type and has rank l , and*

$$r(n) = n + \left\lceil \frac{4}{n} \right\rceil,$$

then for some i , the overlying algebraic group of Y_i has rank at least $(l - n)/r(n)$. Further, $t \geq 1$ unless $C_{\overline{G}}(s)^0$ is abelian, in which case $C_{\overline{G}}(s)$ contains no element of order p .

Proof. Let \overline{G}_{sc} be the universal cover of \overline{G} and $\pi : \overline{G}_{sc} \rightarrow \overline{G}$ the canonical projection. Then s is the image of a semisimple element

$s' \in \overline{G}_{sc}$, and π maps $C_{\overline{G}_{sc}}(s')$ onto $C_{\overline{G}}(s)^o$. The structure of $C_{\overline{G}_{sc}}(s')$ is given by [14, Theorem 4.2], and then applying [14, Lemma 3.3] to $(C_{\overline{G}}(s)^o)_\sigma$ gives the result.

See also [16, (2.9)].

4. Generalities on fixed points of automorphisms of finite groups of Lie type. We continue with the notation of §3, and assume throughout that \overline{G} is simple (but not necessarily of adjoint type). We think of \overline{G} as realized in some explicit way as a Chevalley group over K . Let Φ be the group of field automorphisms of \overline{G} and Γ the set of graph automorphisms constructed as in [6, §12.2–12.4], together with the identity.

The first two results are very similar, but it seems better to deal with the cases of B_2 , F_4 and G_2 separately.

PROPOSITION 4.1. *Suppose that \overline{G} is not of type B_2 , F_4 or G_2 . Let $\sigma = \nu\gamma$, where ν is a Frobenius map in Φ and $\gamma \in \Gamma$, and let $G = O^{p'}(\overline{G}_\sigma)$. Let $\alpha = g\phi\delta \in A = \text{Aut } G$, with $g \in \overline{G}_\sigma$, $\phi \in \Phi_G$, and $\delta \in \Gamma_G$. Let ϕ have order r , let α have order n , and let $q = q(\sigma)$. Then one of the following occurs.*

(I) $C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(g_1)_\mu$, where $g_1 = \alpha^r \in \overline{G}_\sigma\Gamma_G$, and μ is a Frobenius map on \overline{G} such that $\mu(g_1) = g_1$ and $q(\mu)^r = q$. Further, g_1 has order n/r .

(II) $\gamma \neq 1$, $\delta = 1$, and the order m of γ divides r . Let $r = ms$, let $\alpha^s = g_2\phi^s$, where $g_2 \in \overline{G}_\sigma$, and let γ' be the element of Γ which agrees with ϕ^s on G . Then there is a Frobenius map μ on \overline{G} such that $\mu(g_2\gamma') = g_2\gamma'$, $q(\mu)^s = q$, and $C_{\overline{G}_\sigma}(\alpha) = C_G(g_2\gamma')_\mu$. Here, the order of $g_2\gamma'$ is n/s .

Further, if $r = n$ and n is coprime to the order of γ (the latter happens in particular if $\gamma = 1$), then α is conjugate under \overline{G}_σ to an element of $\Phi_G\Gamma_G$.

In case (II), of course, $\gamma' = \gamma$ unless \overline{G} has type D_4 , in which case $\gamma' = \gamma^{\pm 1}$.

The analogous result for types B_2 , F_4 and G_2 is as follows.

PROPOSITION 4.2. *Suppose that \overline{G} is of type B_2 , F_4 or G_2 . Let $\sigma = \nu\gamma$, where ν is a Frobenius map in Φ and $\gamma \in \Gamma$, and let $G = O^{p'}(\overline{G}_\sigma)$. Let $\alpha = g\phi \in A = \text{Aut } G$, with $g \in \overline{G}_\sigma$ and $\phi \in \Phi_G\Gamma_G$. Let ϕ have order r and α have order n , and let $g_1 = \alpha^r \in \overline{G}_\sigma$. Then*

$$C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(g_1)_\theta,$$

where θ is a Frobenius map on \overline{G} such that $\theta(g_1) = g_1$ and $q(\theta)^r = q$. Further, g_1 has order n/r , and if $r = n$, then α is conjugate under \overline{G}_σ to an element of $\Phi_G \Gamma_G$.

Special cases of the above results, at least, are certainly known, see [9] for example. Lang's Theorem is the main ingredient in their proof. It is useful to separate out part of the argument as follows.

LEMMA 4.3. Let $\alpha = g\theta \in A$, with $g \in \overline{G}_\sigma$ and $\theta \in \Phi_G \Gamma_G$. Let θ have order r and $\alpha^r = (g\theta)^r = g_1 \in \overline{G}_\sigma$. Suppose there is a Frobenius map τ on \overline{G} that induces θ on \overline{G}_σ and satisfies $\tau^r = \sigma$. Then

$$C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(g_1)_\psi,$$

where ψ is a Frobenius map on \overline{G} such that $\psi(g_1) = g_1$ and ψ is \overline{G} -conjugate to τ .

If, further, $r = n$, then α is conjugate to θ under \overline{G}_σ .

Proof. We have

$$C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(\langle \sigma, g\tau \rangle) = C_{\overline{G}}(\langle \tau^r, g\tau \rangle).$$

Now

$$(4.1) \quad (g\tau)^r = g \cdot g^{\tau^{-1}} \cdots g^{\tau^{-(r-1)}} \tau^r = g \cdot g^{\theta^{-1}} \cdots g^{\theta^{-(r-1)}} \tau^r = g_1 \tau^r,$$

whence $\tau^r = g_1^{-1}(g\tau)^r$. So

$$C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(\langle g_1^{-1}(g\tau)^r, g\tau \rangle) = C_{\overline{G}}(\langle g_1, g\tau \rangle).$$

By Lang's Theorem, working in the split extension $\overline{G}\Phi\Gamma$, we have that $g\tau$ is \overline{G} -conjugate to τ . Also, $g\tau$ acts as α on \overline{G}_σ and so commutes with $\alpha^r = g_1$. Letting ψ be the Frobenius map induced by conjugation with $g\tau$, we deduce that

$$C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(g_1)_\psi.$$

Now suppose that $r = n$. Choose $h \in \overline{G}$ such that

$$(4.2) \quad (g\tau)^h = \tau.$$

Raising (4.2) to the r -th power and using (4.1) shows that h commutes with $\tau^r = \sigma$, that is, $h \in \overline{G}_\sigma$. Then we find that

$$\alpha^h = (g\theta)^h = g^h[h, \theta^{-1}]\theta = g^h[h, \tau^{-1}]\theta = \theta$$

from (4.2).

Proof of Proposition 4.1. We consider various cases.

Case 1. $\gamma = 1, o(\delta)|r$. Let τ_0 be the element of Φ such that $\tau_0^r = \sigma$. Then τ_0 induces an element ϕ_0 of Φ_G of order r . Hence $\langle \phi_0 \rangle = \langle \phi \rangle$, and $\phi_0 = \phi^s$ with $(r, s) = 1$. Write $\alpha = \alpha_1 \alpha_2$ where α_1 is an r -element, α_2 is an r' -element, and $\alpha_1 \alpha_2 = \alpha_2 \alpha_1$. We have $\langle \alpha_1^s, \alpha_2 \rangle = \langle \alpha \rangle$ and so if $\beta = \alpha_1^s \alpha_2$, then $C_{\overline{G}_\sigma}(\beta) = C_{\overline{G}_\sigma}(\alpha)$. We have $\beta = g^* \phi^s \delta^s$ with $g^* \in \overline{G}_\sigma$. Let $\tau = \tau_0 \delta^s$. Since $\delta^r = 1$, we have $\tau^r = \sigma$, and τ induces $\phi^s \delta^s$. Clearly $\langle \beta^r \rangle = \langle \alpha^r \rangle$. By Lemma 4.3,

$$C_{\overline{G}_\sigma}(\beta) = C_{\overline{G}}(\beta^r)_\mu = C_{\overline{G}}(g_1)_\mu,$$

where μ is a Frobenius map \overline{G} -conjugate to τ and g_1 is μ -invariant. Thus, $q(\mu)^r = q$. Lemma 4.3 also yields that if $r = n$ in this case, then β , and hence α , is \overline{G}_σ -conjugate to an element of $\Phi_G \Gamma_G$.

Case 2. $\gamma = 1, \delta \neq 1$, and $(o(\delta), r) = 1$. Note that in this case, $r \neq n$. Let $\tau \in \Phi$ be such that $\tau^r = \sigma$. Then τ induces an element of order r of Φ_G , and by modifying the r -part of α as in Case 1, we may assume that this is ϕ . Let $m = o(\delta)$. We can write $\langle \alpha \rangle = \langle \alpha_1 \rangle \times \langle \alpha_2 \rangle$, where α_1 is an m' -element, α_2 is an m -element, and $\alpha_1 = x\phi$, $\alpha_2 = y\delta$ with $x, y \in \overline{G}_\sigma$. Then

$$(4.3) \quad \langle \alpha^r \rangle = \langle \alpha_1^r, \alpha_2 \rangle.$$

Let $x_1 = \alpha_1^r \in \overline{G}_\sigma$. Then $(x\tau)^r = x_1 \tau^r$ as in Case 1, so $\tau^r = x_1^{-1}(x\tau)^r$. We have

$$\begin{aligned} C_{\overline{G}_\sigma}(\alpha) &= C_{\overline{G}}(\langle \tau^r, x\tau, y\delta \rangle) = C_{\overline{G}}(\langle x_1^{-1}(x\tau)^r, x\tau, y\delta \rangle) \\ &= C_{\overline{G}}(\langle x_1, x\tau, y\delta \rangle) = C_{\overline{G}}(\langle \alpha_1^r, \alpha_2, x\tau \rangle) = C_{\overline{G}}(g_1)_\mu, \end{aligned}$$

from (4.3), where $\mu = x\tau$ which, by Lang's Theorem, is \overline{G} -conjugate to τ . Since $x\tau = \mu$ acts on g_1 as $x\phi = \alpha_1$, certainly g_1 is μ -invariant, and $q(\mu)^r = q$.

Case 3. $\gamma \neq 1, (r, m) = 1$, where $m = o(\gamma) \in \{2, 3\}$. In this case $\delta = 1$. We wish to invoke Lemma 4.3. Let $\tau \in \Phi$ be such that $\tau^r = \nu$, and let ν induce $\nu_1 \in \Phi_G$, so that ν_1 has order 2 or 3. First suppose that γ has order 2. Then ν_1 has order 2. Consider the effect of $\tau\gamma$ on \overline{G}_σ . Now τ^r induces ν_1 on \overline{G}_σ , and since $\nu\gamma$ is trivial on \overline{G}_σ , γ induces ν_1 also. So $\tau\gamma$ induces a field automorphism of order r on \overline{G}_σ , and by adjusting the r -part of α , we may assume that $\tau\gamma$ induces ϕ . Now everything, including the final conjugacy statement if $r = n$, follows from Lemma 4.3.

When γ has order 3 the situation is broadly similar. Arguing as above, we find that $(\tau\gamma)^r$ induces ν_1^{1-r} on \overline{G}_σ . If $r \equiv 1 \pmod{3}$, then

we find that $\tau\gamma$ induces a field automorphism of order r on \overline{G}_σ , and everything is identical. If $r \equiv -1 \pmod{3}$, we consider $\tau\gamma^2$ instead.

Case 4. $\gamma \neq 1$, $m = o(\gamma)|r$. Again $\delta = 1$. Verification of the final conjugacy statement does not arise here. Set $r = ms$, and let τ be the element of Φ such that $\tau^s = \nu$. Then τ induces on \overline{G}_σ a field automorphism of order $ms = r$, which is the order of ϕ . Now the natural map $\overline{G}_\sigma\Phi\Gamma \rightarrow \overline{G}_\sigma\Phi_G$ is monomorphic on the normal subgroup $\overline{G}_\sigma\Gamma$, and the element $g_2\gamma'$ occurring in (II) is the unique element of $\overline{G}_\sigma\Gamma$ mapping to α^s under it. Thus, replacing α by another generator of $\langle\alpha\rangle$ does not change $\langle g_2\gamma\rangle$. This allows us to make such a replacement and assume that τ induces ϕ on \overline{G}_σ . Now we have $\gamma' = \gamma^{-1}$, since $\tau^s = \nu$, τ^s induces ϕ^s , and $\nu\gamma$ induces the identity on \overline{G}_σ . We have

$$(g\tau)^s = g \cdot g^{\tau^{-1}} \cdots g^{\tau^{-(s-1)}} \tau^s = g \cdot g^{\phi^{-1}} \cdots g^{\phi^{-(s-1)}} \tau^s = g_2\tau^s,$$

since $(g\phi)^s = g_2\phi^s$. Hence $\nu = \tau^s = g_2^{-1}(g\tau)^s$ and

$$\begin{aligned} C_{\overline{G}_\sigma}(\alpha) &= C_{\overline{G}}(\langle \gamma g_2^{-1}(g\tau)^s, g\tau \rangle) \\ &= C_{\overline{G}}(\langle g_2\gamma^{-1}, g\tau \rangle) = C_{\overline{G}}(\langle g_2\gamma', g\tau \rangle). \end{aligned}$$

Now $g_2\gamma'$ has order n/s and commutes with $g\tau$, since these statements become true after applying the natural map $\overline{G}_\sigma\Phi\Gamma \rightarrow \overline{G}_\sigma\Phi_G$, and by Lang's Theorem, $g\tau$ induces on \overline{G} a Frobenius map μ conjugate to τ under \overline{G} . Therefore $q(\mu)^s = q(\tau^s) = q(\nu) = q(\sigma)$, and $C_{\overline{G}_\sigma}(\alpha) = C_{\overline{G}}(g_2\gamma')_\mu$.

Proof of Proposition 4.2. This follows directly from Lemma 4.3, since every element of $\Phi_G\Gamma_G$ is induced in the appropriate way by a Frobenius map on \overline{G} , when \overline{G} has type B_2 , F_4 or G_2 .

Now we extract from the above results the information that we need for the proofs of Theorems A' and C.

THEOREM 4.4. *Let \overline{G} have rank l , let α be an automorphism of order n of G , and suppose that p does not divide n . Then*

(i) $C_{\overline{G}_\sigma}(\alpha) = H_\psi$, where H is an infinite reductive group and ψ is a Frobenius map on \overline{G} such that H is ψ -invariant and $q(\psi)^m = q$ for some m dividing n .

(ii) $|C_{\overline{G}_\sigma}(\alpha)| \geq q^{1/m} - 1$ for some divisor m of n . Further, either $q^{1/m}$ is an integral power of p , or \overline{G} has type B_2 , F_4 or G_2 , $p = 2, 2, 3$ respectively, and $q^{2/m}$ is an odd power of p .

(iii) *There is a polynomial f with real coefficients and a positive integer m dividing n such that $|f(q^{1/m})|$ is an integer dividing $|C_{\overline{G}_\sigma}(\alpha)|$. The degree of f is at most l and its roots are roots of 1 of degree at most $2l$ over \mathbb{Q} .*

Proof. (i) From Propositions 4.1 and 4.2, we see that $C_{\overline{G}_\sigma}(\alpha)$ has the form $C_{\overline{G}}(\beta)_\psi$, where β is a semisimple algebraic automorphism of \overline{G} and ψ is a Frobenius map on \overline{G} commuting with β and so leaving $H = C_{\overline{G}}(\beta)$ invariant. Further, $q(\psi)^m = q$, where $m|n$. By a well known theorem of Steinberg [18, (8.1), (9.2)], H is an infinite reductive algebraic group.

(ii), (iii) By another theorem of Steinberg [18, (10.1)], ψ leaves invariant some maximal torus S of H . The rank of S is at most l . We obtain (ii) and (iii) by applying Lemma 3.3 to S_ψ . Since $q^{1/m} = q(\psi)$, it or its square is a power of p as stated.

5. Proofs of Theorems A' and C.

Proof of Theorem A'. We prove the theorem by induction on n . The case $n = 1$ is trivial. Note that when Theorem A' has been proved for all divisors of a given integer n , then Theorem A follows for all divisors of n , by the proof of that theorem. When we say that a given quantity is *bounded* during the course of this proof, we mean that it is bounded in terms of n and k .

The classification of finite simple groups tells us that our simple group G is either sporadic, alternating, or of Lie type. As there are only finitely many sporadic groups, they can be ignored. The alternating groups will be left as a simple exercise for the reader, and so we now assume that G is of Lie type and use the notation of §3.

It is sufficient to bound the rank l of \overline{G} and the field parameter q of G . Let α be the given automorphism. Write $n = p_1^{r_1} \cdots p_t^{r_t}$, where the p_i are distinct primes, and let $\alpha = \alpha_1 \cdots \alpha_t$, where α_i has order $p_i^{r_i}$ and the α_i commute. Let β_i be an element of order p_i in $\langle \alpha_i \rangle$.

Suppose first that $t = 1$, $p_1 = p$, and $n = p^r$. Then α leaves invariant some Sylow p -subgroup P of G . Let $\Phi(P)$ be the Frattini subgroup of P and \overline{P} be the elementary abelian group $P/\Phi(P)$. Then $|\overline{P}|$ is divisible by q^l (see [6, 5.3, 13.6]). Also $|C_{\overline{P}}(\alpha)| \leq k$ ([2, VIII.10.14]). We have $(\alpha - 1)^{p^r} = 0$ on \overline{P} , and it follows by well known arguments using Jordan blocks or the like that $|\overline{P}|$ divides $|C_{\overline{P}}(\alpha)|^{p^r} \leq k^{p^r}$. Hence q^l is bounded, as required.

Now we may assume without loss of generality that

$$p_1 \neq p.$$

We may further assume that

$$\beta_i \in \overline{G}_\sigma \quad \text{for } 1 \leq i \leq t.$$

For if some β_i is not in \overline{G}_σ , then Lemma 3.1 tells us that $C_G(\beta_i)$ involves a non-abelian simple group H such that $|G|$ is bounded in terms of $|H|$. But applying induction to the action of α on $C_G(\beta_i)$ gives us a bound on $|H|$ and hence on $|G|$.

Now we show that

$$\overline{G} \text{ has bounded rank.}$$

This is because, if \overline{G} has rank l and classical type, then by Lemma 3.4, $C_G(\beta_1)$ involves a group of Lie type of the form $H = O^{p'}(\overline{H}_\tau)$, where \overline{H} is a simple algebraic group of rank at least $(l - n)/r(n) \geq (l - n)/2n$, τ is a Frobenius map on \overline{H} , and H is defined over an extension of the field over which G is defined. By induction, we have a bound on $|H|$, and this gives us one on l . The ranks of the exceptional groups are of course bounded in any case.

Since $|C_{\overline{G}_\sigma}(\alpha)/G|$ is bounded in terms of l (in fact it is at most $l + 1$, see [6, pp. 98–99] for example), we have

$$|C_{\overline{G}_\sigma}(\alpha)| \text{ is bounded.}$$

It remains to bound q . Now if $C_{\overline{G}}(\beta_i)^0$ is non-abelian for some i such that $p_i \neq p$, then again we find that $C_G(\beta_i)$ involves a group in **Chev** over some extension field of F_q (F_{q^2} if G is a Suzuki or Ree group). This group will be simple unless q is already very small, and we obtain our bound on q by induction. If $p_i = p$ for some i , then as $\beta_i \in C_{\overline{G}}(\beta_1)^0$, we have that $C_{\overline{G}}(\beta_1)^0$ is non-abelian (see [14, Theorem C], for example, for this well known fact). We conclude that we may assume that

$$p_i \neq p \quad \text{for } 1 \leq i \leq t.$$

By Theorem 4.4, $|C_{\overline{G}_\sigma}(\alpha)| \geq q^{1/n} - 1$. This bounds q and concludes the proof.

Proof of Theorem C. This is now rather straightforward. Most cases were covered in [11], but we will give here a proof covering all cases. For our simple group G we have, by [14, Lemma 4.3], a simple

Chevalley group \overline{G} over K , a Frobenius map σ on \overline{G} , and a sequence of integers $n(1)|n(2)|\dots$ such that

$$G = \bigcup_{i=1}^{\infty} G_i, \quad \text{where } G_i = O^{p'}(\overline{G})_{\sigma^{n(i)}}.$$

Let Φ and Γ be the field and graph automorphisms of \overline{G} as at the beginning of §4. Let $H_i = \overline{G}^{\sigma^{n(i)}}$ and $H = \bigcup_{i=1}^{\infty} H_i$. Then we can take $\sigma \in \Phi\Gamma$ and α to be induced on G by an element $\beta\theta$, where β is conjugation by some element h of H and $\theta \in \Phi\Gamma$ [19, p. 195]. Further, θ commutes with σ . In fact, one of θ and σ will be in Φ , which commutes elementwise with $\Phi\Gamma$. Let $h \in H_i$. Then $\beta\theta$ leaves H_j invariant if $j \geq i$, and so we may assume that $\beta\theta$ leaves all H_i invariant. Further, $(\beta\theta)^n$ is trivial on each H_i . This is because $C_{H_i}(G_i) = 1$ and so every non-trivial automorphism of H_i restricts non-trivially to G_i .

Thus, we can think of α as an automorphism of order n of H leaving all H_i invariant. Since the groups H_i/G_i have order bounded independently of i (in fact by $l+1$, where l is the rank of \overline{G}), it will suffice to show that the numbers $|C_{H_i}(\alpha)|$ have infinitely many prime divisors between them.

Let $q = q(\sigma)$ and l be the rank of \overline{G} . By Theorem 4.4, $|C_{H_i}(\alpha)|$ is divisible by $|f_i(q^{n(i)/m(i)})|$, where f_i is some real monic polynomial whose degree is at most l and whose roots are roots of 1 of degree at most $2l$ over the rationals. The roots of f_i are drawn from a finite set, so only finitely many polynomials occur as f_i . There are clearly only finitely many possibilities for the $m(i)$. Thus, there is an infinite sequence i_1, i_2, \dots a polynomial f and a divisor m of n such that $f_{i_r} = f$ and $m_{i_r} = m$ for all r . By [11, Lemma 2.3], with $s = q^{1/m}$, the numbers $f(q^{n(i)/m})$ have infinitely many prime divisors between them. This concludes the proof.

REFERENCES

- [1] M. Aschbacher and G. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya J. Math., **63** (1976), 1–91.
- [2] N. Blackburn and B. Huppert, *Finite Groups I, II*, Springer-Verlag, Berlin, 1982.
- [3] A. Borel, *Linear Algebraic Groups*, Benjamin, New York, 1969.
- [4] R. Brauer and P. Fong, *On the centralizers of p -elements in finite groups*, Bull. London Math. Soc., **6** (1974), 319–324.
- [5] R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math., (2) **62** (1955), 565–583.

- [6] R. W. Carter, *Simple Groups of Lie Type*, Wiley-Interscience, London, 1972.
- [7] ———, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley-Interscience, Chichester, 1985.
- [8] J. Dieudonné, *La géométrie des Groupes Classiques*, Springer-Verlag, Berlin, 1955.
- [9] D. Gorenstein and R. Lyons, *The local structure of finite groups of characteristic 2 type*, *Memoirs Amer. Math. Soc.*, **42** No. 276 (1983).
- [10] Morton E. Harris, *Finite groups containing an intrinsic 2-component of Chevalley type over a field of odd order*, *Trans. Amer. Math. Soc.*, **272** (1982), 1–65.
- [11] B. Hartley, *Fixed points of automorphisms of certain locally finite groups and Chevalley groups*, *J. London Math. Soc.*, (2) **37** (1988), 421–436.
- [12] Brian Hartley and Volker Turau, *Finite groups admitting an automorphism of prime power order with few fixed points*, *Math. Proc. Cambridge Philos. Soc.*, **102** (1987), 431–441.
- [13] B. Hartley and I. M. Isaacs, *On characters and fixed points of coprime operator groups*, *J. Algebra*, **131** (1990), 342–358.
- [14] B. Hartley and M. Kuzucuoğlu, *Centralizers of elements in locally finite simple groups*, *Proc. London Math. Soc.*, (3) **62** (1991), 301–324.
- [15] O. H. Kegel and B. A. F. Wehrfritz, *Locally Finite Groups*, North-Holland, Amsterdam, 1973.
- [16] G. Seitz, *The root subgroups for maximal tori in finite groups of Lie type*, *Pacific J. Math.*, **106** (1983), 153–244.
- [17] T. A. Springer and R. Steinberg, *Conjugacy classes*, in *Seminar on Finite Groups and Related Algebraic Groups*, *Lecture Notes in Math.* Vol. 131, Springer-Verlag, Berlin, 1970, reprinted 1986.
- [18] R. Steinberg, *Endomorphisms of algebraic groups*, *Memoirs Amer. Math. Soc.*, **80** (1968).
- [19] ———, *Lectures on Chevalley groups*, Mimeographed notes, Yale University, 1967.

Received August 30, 1990 and in revised form March 6, 1991.

UNIVERSITY OF MANCHESTER
OXFORD ROAD
MANCHESTER M13 9PL, ENGLAND

