Annals of Mathematics, **165** (2007), 239–273

On finitely generated profinite groups, II: products in quasisimple groups

By Nikolay Nikolov* and Dan Segal

Abstract

We prove two results. (1) There is an absolute constant D such that for any finite quasisimple group S, given $2D$ arbitrary automorphisms of S, every element of S is equal to a product of D 'twisted commutators' defined by the given automorphisms.

(2) Given a natural number q, there exist $C = C(q)$ and $M = M(q)$ such that: if S is a finite quasisimple group with $|S/\mathrm{Z}(S)| > C$, β_j $(j = 1, \dots, M)$ are any automorphisms of S, and q_j $(j = 1, \dots, M)$ are any divisors of q, then there exist inner automorphisms α_j of S such that $S = \prod_1^M [S, (\alpha_j\beta_j)^{q_j}]$.

These results, which rely on the classification of finite simple groups, are needed to complete the proofs of the main theorems of Part I.

1. Introduction

The main theorems of Part I [NS] were reduced to two results about finite quasisimple groups. These will be proved here.

A group S is said to be *quasisimple* if $S = [S, S]$ and $S/\mathrm{Z}(S)$ is simple, where $\mathrm{Z}(S)$ denotes the centre of S. For automorphisms α and β of S we write

$$T_{\alpha,\beta}(x, y) = x^{-1}y^{-1}x^{\alpha}y^{\beta}.$$

Theorem 1.1. *There is an absolute constant $D \in \mathbb{N}$ such that if S is a finite quasisimple group and $\alpha_1, \beta_1, \dots, \alpha_D, \beta_D$ are any automorphisms of S then*

$$S = T_{\alpha_1,\beta_1}(S, S) \cdot \dots \cdot T_{\alpha_D,\beta_D}(S, S).$$

Theorem 1.2. *Let q be a natural number. There exist natural numbers $C = C(q)$ and $M = M(q)$ such that if S is a finite quasisimple group with $|S/\mathrm{Z}(S)| > C$, $\beta_1, \dots, \beta_M$ are any automorphisms of S, and $q_1, \dots, q_M$ are*

*Work done while the first author held a Golda-Meir Fellowship at the Hebrew University of Jerusalem.

any divisors of q, then there exist inner automorphisms $\alpha_1, \dots, \alpha_M$ of S such that

$$S = [S, (\alpha_1\beta_1)^{q_1}] \cdot \dots \cdot [S, (\alpha_M\beta_M)^{q_M}].$$

These results are stated as Theorems 1.9 and 1.10 in the introduction of [NS]. Both may be seen as generalizations of Wilson's theorem [W] that every element of any finite simple group is equal to the product of a bounded number of commutators: indeed, we shall show that in Theorem 1.2, $C(1)$ may be taken equal to 1. The latter theorem also generalizes the theorem of Martinez, Zelmanov, Saxl and Wilson ([MZ], [SW]) that in any finite simple group S with $S^q \neq 1$, every element is equal to a product of boundedly many q^{th} powers, the bound depending only on q.

The proofs depend very much on the classification of finite simple groups, and in Section 2 we give a brief résumé on groups of Lie type, its main purpose being to fix a standard notation for these groups, their subgroups and automorphisms. Section 3 collects some combinatorial results that will be used throughout the proof, and in Section 4 we show that Theorem 1.1 is a corollary of Theorem 1.2 (it only needs the special case where $q = 1$).

The rest of the paper is devoted to the proof of Theorem 1.2. This falls into two parts. The first, given in Section 5, concerns the case where $S/\mathrm{Z}(S)$ is either an alternating group or a group of Lie type over a 'small' field; this case is deduced from known results by combinatorial arguments. The second part, in Sections 6–10, deals with groups of Lie type over 'large' fields: this depends on a detailed examination of the action of automorphisms of S on the root subgroups. The theorem follows, since according to the classification all but finitely many of the finite simple groups are either alternating or of Lie type.

Notation. For a group S and $x, y \in S$, $x^y = y^{-1}xy$. If $y \in S$ or $y \in \mathrm{Aut}(S)$,

$$[x, y] = x^{-1}x^y, \ [S, y] = \{[x, y] \mid x \in S\}.$$

We will write $\overline{S} = S/\mathrm{Z}(S)$, and identify this with the group $\mathrm{Inn}(S)$ of inner automorphisms of S. Similarly for $g \in S$ we denote by $\bar{g} \in \mathrm{Inn}(S)$ the automorphism induced by conjugation by g. The Schur multiplier of S is denoted $M(S)$, and $\mathrm{Out}(S)$ denotes the outer automorphism group of S. For a subset $X \subseteq S$, the subgroup generated by X is denoted $\langle X \rangle$, and for $n \in \mathbb{N}$

$$X^{*n} = \{x_1 \dots x_n \mid x_1, \dots, x_n \in X\}.$$

We use the usual notation F^* for the multiplicative group $F \setminus \{0\}$ of a field F (this should cause no confusion). The symbol log means logarithm to base 2.

2. Groups of Lie type: a résumé

Apart from the alternating groups $\mathrm{Alt}(k)$ ($k \geq 5$) and finitely many sporadic groups, every finite simple group is a *group of Lie type*, that is, an untwisted or twisted Chevalley group over a finite field. We briefly recall some features of these groups, and fix some notation. Suitable references are Carter's book [C], Steinberg's lectures [St] and [GLS]. For a useful summary (without proofs) see also Chapter 3 of [At].

Untwisted Chevalley groups. Let $\mathcal{X}$ be one of the Dynkin diagrams A_r ($r \geq 1$), B_r ($r \geq 2$), C_r ($r \geq 3$), D_r ($r \geq 4$), E_6, E_7, E_8, F_4 or G_2; let Σ be an irreducible root system of type $\mathcal{X}$ and let Π be a fixed base of fundamental roots for Σ. This determines Σ_+: the positive roots of Σ.

The number $r := |\Pi|$ of fundamental roots is the *Lie rank*. If $w \in \Sigma_+$ is a positive root then we can write w uniquely as a sum of fundamental roots (maybe with repetitions). The number of summands, denoted $\mathrm{ht}(w)$, is called the *height* of w. Thus Π is exactly the set of roots of height 1.

Let $\mathcal{X}(F)$ denote the F-rational points of a split simple algebraic group of type $\mathcal{X}$ over the field F. To each $w \in \Sigma$ is associated a one-parameter subgroup of $\mathcal{X}(F)$,

$$X_w = \{X_w(t) \mid t \in F\},$$

called the *root subgroup* corresponding to w.

The associated *Chevalley group* of type $\mathcal{X}$ over F is defined to be the subgroup S of $\mathcal{X}(F)$ generated by all the root subgroups X_w for $w \in \Sigma$. It is *adjoint* (resp *universal*) if the algebraic group is adjoint (resp. simply connected). With finitely many exceptions S is a quasisimple group.

Let $U = U_+ := \prod_{w \in \Sigma_+} X_w$ and $U_- := \prod_{w \in \Sigma_-} X_w$, the products being ordered so that $\mathrm{ht}(|w|)$ is nondecreasing. Then U_+ and U_- are subgroups of S (the positive, negative, unipotent subgroups).

For each multiplicative character $\chi : \mathbb{Z}\Sigma \to F^*$ of the lattice spanned by Σ, we define an automorphism $h(\chi)$ of S by

$$X_w(t)^{h(\chi)} = X_w(\chi(w) \cdot t).$$

The set of all such $h(\chi)$ forms a subgroup $\mathcal{D}$ of $\mathrm{Aut}(S)$, called the group of *diagonal automorphisms*.

The group H of *diagonal elements* of S is the subgroup generated by certain semisimple elements $h_v(\lambda)$ ($v \in \Pi$, $\lambda \in F^*$); the group H normalizes each root subgroup, and we have

$$X_w(t)^{h_v(\lambda)} = X_w(\lambda^{\langle w,v \rangle} t)$$

where $\langle w, v \rangle = 2(w, v)/|v|^2$. In particular $X_w(t)^{h_w(\lambda)} = X_w(\lambda^2 t)$. The inner automorphisms of S induced by H are precisely the inner automorphisms lying in $\mathcal{D}$, and $\mathcal{D}$ acts trivially on H.

For each power p^f of $\mathrm{char}(F)$ there is a *field automorphism* $\phi = \phi(p^f)$ of S defined by

$$X_w(t)^\phi = X_w(t^{p^f}).$$

The set Φ of field automorphisms is a group isomorphic to $\mathrm{Aut}(F)$.

The groups $\mathcal{D}$ and Φ stabilize each root subgroup and each of the *diagonal subgroups* $H_v = \{h_v(\lambda) \mid \lambda \in F^*\}$.

We write $\mathrm{Sym}(\mathcal{X})$ for the group of (root-length preserving) symmetries of the root system Σ. This is a group of order at most 2 except for $\mathcal{X} = D_4$, in which case $\mathrm{Sym}(\mathcal{X}) \cong \mathrm{Sym}(3)$. Let $\tau \in \mathrm{Sym}(\mathcal{X})$ be a symmetry that preserves the weight lattice of the algebraic group $\mathcal{X}(-)$ (e.g. if the isogeny type of $\mathcal{X}(-)$ is simply connected or adjoint). Then (cf. Theorem 1.15.2(a) of [GLS]) there exists an automorphism of S, denoted by the same symbol τ, which permutes the root subgroups in the same way as τ acts on Σ; in fact:

$$(X_w(t))^\tau = X_{w^\tau}(\epsilon_w t), \quad \epsilon_w \in \{\pm 1\} \text{ with } \epsilon_w = 1 \text{ if } w \in \Pi.$$

This is called an *ordinary graph automorphism*.

In case $\mathcal{X} = B_2, G_2, F_4$ and $p = 2, 3, 2$ respectively, such an automorphism of S exists also when τ corresponds to the (obvious) symmetry of order 2 of the Dynkin diagram, which does *not* preserve root lengths. It is defined by

$$X_w(t)^{\tau_0} = X_{w^\tau}(t^r), \quad r = 1 \text{ if } w \text{ is long}, \ \ r = p \text{ if } w \text{ is short}\ .$$

In this case τ_0 is called an *extraordinary graph automorphism*, and we set $\Gamma = \{1, \tau_0\}$. In all other cases, we define Γ to be the set of all ordinary graph automorphisms.

Observe that $\Gamma \neq \{1\}$ only when the rank is small (≤ 6) or when $\mathcal{X}$ is A_r or D_r. The set Γ is a group unless S is one of $B_2(2^n), G_2(3^n)$ and $F_4(2^n)$, when $|\Gamma| = 2$ and the extraordinary element of Γ squares to the generating field automorphism of Φ. In all cases, Γ is a set of coset representatives for $\mathrm{Inn}(S)\mathcal{D}\Phi$ in $\mathrm{Aut}(S)$.

Twisted Chevalley groups. These are of types ${}^2A_r, {}^2B_2, {}^2D_r, {}^2E_6, {}^2F_4, {}^2G_2$, and ${}^3D_4$.

The *twisted group* S^* of type ${}^n\mathcal{X}$ is associated to a certain graph automorphism of an untwisted Chevalley group S of type $\mathcal{X}$. The structure of S^* is related to that of S, the most notable difference being that root subgroups may be no longer one-parameter. Another difference is that S^* does not have graph automorphisms.

Let $\tau \in \Gamma \backslash \{1\}$ be a graph automorphism of S as defined above, and let $n \in \{2, 3\}$ be the order of the symmetry τ on Σ. The group S^* is the fixed-point set in S of the so-called *Steinberg automorphism* $\sigma = \phi\tau$, where ϕ is the nontrivial field automorphism chosen so that σ has order n.

We define $F_0 \subseteq F$ to be the fixed field of ϕ if $\mathcal{X}$ has roots of only one length; otherwise set $F_0 = F$. In all cases, $(F : F_0) \leq 3$.

The (*untwisted*) *rank* of S^* is defined to be the Lie rank r of the (original) root system Σ.

The root subgroups of S^* now correspond to equivalence classes ω under the equivalence relation on Σ defined as follows.

Let Σ be realized as a set of roots in some Euclidean vector space V. The symmetry τ extends to a linear orthogonal map of V and by v^* we denote the orthogonal projection of $v \in \Sigma$ on $C_V(\tau)$, the subspace fixed by τ. Now, for $u, v \in \Sigma$ define

$$u \sim v \text{ if } u^* = qv^* \text{ for some positive } q \in \mathbb{Q}.$$

Each equivalence class ω of $\Sigma/\sim$ is the positive integral span of a certain orbit $\overline{\omega}$ of τ on the root system Σ.

The root subgroups are the fixed points of σ acting on

$$W_\omega := \langle X_v | \quad v \in \omega \rangle \leq S.$$

In order to distinguish them from the root subgroups of the corresponding untwisted group we denote them by Y_ω. For later use we list their structure and multiplication rules below (cf. Table 2.4 of [GLS]).

Let $p = \mathrm{char}(F)$ and suppose that $\phi(t) = t^{p^f}$. The automorphism $t \mapsto t^p$ of F is denoted by $[p]$.

Case A_1^d. ω is one of $\{v\}$, $\{v, v^\tau\}$, $\{v, v^\tau, v^{\tau^2}\}$ and consists of pairwise orthogonal roots; here $|\omega| = d$. When $d = 2$ and there are two root lenghts, v is a long root. Then

$$Y_\omega = \{Y_\omega(t) := \prod_{i=0}^{d-1} X_{v^{\tau^i}}(t^{\phi^i}) \mid t \in \widetilde{F}\}$$

is a one-parameter group; here $\widetilde{F} = F$ except when $d = 1$ when $\widetilde{F} = F_0$.

Case A_2. $\omega = \{w, v, w + v\}$ is of type A_2 with symmetry τ swapping v and w. Here $|F| = p^{2f}$, $|F_0| = p^f$, $\phi^2 = 1$. Elements of Y_ω take the form

$$Y_\omega(t, u) = X_v(t)X_w(t^\phi)X_{v+w}(u) \quad (t, u \in F)$$

with $t^{1+\phi} = u + u^\phi$, and the multiplication is given by

$$Y_\omega(t, u)Y_\omega(t', u') = Y_\omega(t + t', u + u' + t^\phi t').$$

Case B_2. In this case $p = 2$, $[2]\phi^2 = 1$. The set ω has type B_2 with base $\{v, w\}$ where $\langle v, w \rangle = -2$. Elements of Y_ω take the form

$$Y_\omega(t, u) = X_v(t)X_w(t^\phi)X_{v+2w}(u)X_{v+w}(t^{1+\phi} + u^\phi) \quad (t, u \in F)$$

with multiplication $Y_\omega(t, u)Y_\omega(t', u') = Y_\omega(t + t', u + u' + t^{2\phi}t')$.

Case G_2. Here $p = 3$, $[3]\phi^2 = 1$ and $|F| = 3p^{2f}$. The set ω has type G_2 with base $\{v, w\}$ where $\langle v, w\rangle = -3$. Elements of Y_ω take the form

$$Y_\omega(t,u,z) = X_v(t)X_w(t^\phi)X_{v+3w}(u)X_{v+w}(u^\phi - t^{1+\phi})X_{2v+3w}(z)X_{v+2w}(z^\phi - t^{1+2\phi})$$

where t, u, $z \in F$. The multiplication rule is

$$Y_\omega(t,u,z)Y_\omega(t',u',z') = Y_\omega(t+t', u+u'+t't^{3\phi}, z+z'-t'u+(t')^2t^{3\phi}).$$

The root system Σ^* of S^* is defined as the set of orthogonal projections ω^* of the equivalence classes ω of the untwisted root system Σ under $\sim$. See Definition 2.3.1 of [GLS] for full details.

The twisted root system Σ^* may not be reduced (i.e. it may contain several positive scalar multiples of the same root). However in the case of classical groups Σ^* is reduced with the following exception: in type ${}^2A_{2m}$ the class $\omega = \{u, v = u^\tau, u+v\}$ of roots in Σ spanning a root subsystem of type A_2 gives rise to a pair of 'doubled' roots $\omega^* = \{u+v, (u+v)/2\}$ in Σ^*. In this case Σ^* is of type BC_m, see [GLS, Prop. 2.3.2]. Note that the doubled roots ω^* above correspond to *one* root subgroup in S^*, namely Y_ω.

The groups H, U_+, $U_- \le S^*$ are the fixed points of σ on the corresponding groups in the untwisted S. The group of field automorphisms Φ is defined as before; the group of diagonal automorphisms $\mathcal{D}$ corresponds to the diagonal automorphisms of S that commute with σ; there are no graph automorphisms, and we set $\Gamma = 1$.[1]

The group $\mathcal{D}_0$. In the case when S is a classical group of Lie rank at least 5 we shall define a certain subgroup $\mathcal{D}_0 \subseteq \mathcal{D}$ to be used in Section 5 below.

Suppose first that S is *untwisted* with a root system Σ of classical type (A_r, B_r, C_r or D_r, $r \ge 5$) and a set Π of fundamental roots.

If the type is D_r define $\Delta = \{w_1, w_2\}$ where $w_1, w_2 \in \Pi$ are the two roots swapped by the symmetry τ of Π. If the type is A_r then let $\Delta := \{w_1, w_2\}$ where $w_1, w_2 \in \Pi$ are the roots at both ends of the Dynkin diagram (so again we have $w_1^\tau = w_2$).

If the type is B_r or C_r set $\Delta = \{w\}$ where $w \in \Pi$ is the *long* root at one end of the Dynkin diagram defined by Π. Recall that in this case $\Gamma = 1$.

Let $\Pi_0 = \Pi \setminus \Delta$ and observe that in all cases $\Pi_0^\Gamma = \Pi_0$. Now define

$$\mathcal{D}_0 = \left\langle h(\chi) \mid \chi_{|\Pi_0} = 1 \right\rangle.$$

When S^* is *twisted* with a root system Σ^* define $\mathcal{D}_0^* \subseteq S^*$ to be the group of fixed points of $\mathcal{D}_0$ under σ, where $\mathcal{D}_0$ is the corresponding subgroup defined for the untwisted version S of S^*. For future reference, in this case we also

[1] Note that our definition of graph automorphisms differs from the one in [GLS].

consider the set of roots $\Pi_0 \subseteq \Sigma$ as defined above for the untwisted root system Σ of S.

When using the notation S for a twisted group, we will write $\mathcal{D}_0$ for the group here denoted $\mathcal{D}_0^*$.

Clearly $|\mathcal{D}_0| \leq |F^*|^2$, and we have

LEMMA 2.1. *If $\overline{H}$ is the image of the group H of diagonal elements in* $\mathrm{Inn}(S)$ *then $\mathcal{D} = \overline{H}\mathcal{D}_0$.*

Moreover, provided the type of S is not A_r or ${}^2A_r$ then there is a subset $A = \{h(\chi_i) \mid 1 \leq i \leq 4\} \subseteq \mathcal{D}_0$ of at most 4 elements of $\mathcal{D}_0$ such that $\mathcal{D} = A \cdot \overline{H}$.

Proof. We only give the proof for the untwisted case which easily generalizes to the twisted case by consideration of equivalence classes of roots under $\sim$.

From the definition of Δ one sees that Π_0 can be ordered as $\nu_1, \nu_2, \ldots, \nu_k$ so that for some root $w \in \Delta$,

$$\langle \nu_i, \nu_{i+1} \rangle = \langle \nu_k, w \rangle = -1, \quad i = 1, 2, \ldots, k-1,$$

and all other possible pairs of roots in $\Pi_0 \cup \{w\}$ are orthogonal.

Now, given $h = h(\chi) \in \mathcal{D}$ where χ is a multiplicative character of the root lattice $\mathbb{Z}\Sigma$, we may recursively define a sequence $h_i = h_i(\chi_i) \in \mathcal{D}$ ($i = 1, 2, \ldots, k$) so that $h_0 = h$, $h_{i+1}h_i^{-1} \in \overline{H}$ and χ_i is trivial on $\nu_1, \ldots, \nu_i$. Indeed, suppose h_i is already defined for some $i < k$ and $\chi_i(\nu_{i+1}) = \lambda \in F^*$, say. Put $h_{i+1} = h_i h_{\nu_{i+2}}(\lambda)$ (where by convention $\nu_{k+1} = w$). Then χ_{i+1} and χ_i agree on $\nu_1, \ldots, \nu_i$, while

$$\chi_{i+1}(\nu_{i+1}) = \chi_i(\nu_{i+1})\lambda^{\langle \nu_{i+1}, \nu_{i+2} \rangle} = 1.$$

Clearly we have $h_k \in \mathcal{D}_0$ while $h \cdot h_k^{-1} \in \overline{H}$. This proves the first statement of the lemma.

The second statement is now obvious since the group $\mathcal{D}/\overline{H}$ has order at most 4 in that case. □

Thus $\mathcal{D}_0$ allows us to choose a representative for a given element in $\mathcal{D}/\overline{H}$ which centralizes many root subgroups (i.e. those corresponding to Π_0).

Automorphisms and Schur multipliers. Let S be a Chevalley group as above, untwisted or twisted. We identify $\overline{S} = S/\mathrm{Z}(S)$ with the group of inner automorphisms $\mathrm{Inn}(S)$.

- $\mathrm{Aut}(S) = \overline{S}\mathcal{D}\Phi\Gamma$ ([GLS, Th. 2.5.1]).
- $\mathcal{D}\Phi\Gamma$ is a subgroup of $\mathrm{Aut}(S)$ and $\mathcal{D}\Phi\Gamma \cap \overline{S} = \overline{H}$.

- When Γ is nontrivial it is either of size 2 or it is Sym(3); the latter only occurs in the case $\mathcal{X} = D_4$. The set

$$\overline{S}\mathcal{D}\Phi$$

  is a normal subgroup of index at most 6 in $\mathrm{Aut}(S)$.

- The *universal cover* of S is the largest perfect central extension $\widetilde{S}$ of S. Apart from a finite number of exceptions $\widetilde{S}$ is the universal Chevalley group of the same type as S. The exceptions arise only over small fields ($|F| \leq 9$).

- The kernel $M(S)$ of the projection $\widetilde{S} \to S$ is the *Schur multiplier* of S. We have $|M(S)| \leq 48$ unless S is of type A_r or ${}^2A_r$, in which case (apart from a few small exceptions) $M(S)$ is cyclic of order dividing $\gcd(r+1, |F_0| \pm 1)$. We also have the crude bound $|M(S)| \leq |S|$.

- $\big|\mathcal{D} : \overline{H}\big| \leq \big|M(\overline{S})\big|$.

- $|\mathrm{Out}(S)| \leq 2f|M(\overline{S})|$ where $|F| = p^f$ unless S is of type D_4.

Suppose that T is a quasisimple group of Lie type, with $T/\mathrm{Z}(T) = S$. Then $T = \widetilde{S}/K$ for some $K \leq \mathrm{Z}(\widetilde{S})$. An automorphism γ of $\widetilde{S}$ that stabilizes K induces an automorphism $\overline{\gamma}$ of T. The map $\gamma \mapsto \overline{\gamma}$ is an isomorphism between $N_{\mathrm{Aut}(\widetilde{S})}(K)$ and $\mathrm{Aut}(T)$; see [A, §33]. Thus every automorphism of T lifts to an automorphism of $\widetilde{S}$.

3. Combinatorial lemmas

The first three lemmas are elementary, and we record them here for convenience. G denotes an arbitrary finite group.

LEMMA 3.1. *Suppose that* $|G| \leq m$.

(i) *If* $f_1, \ldots, f_m \in G$ *then* $\prod_{l=i}^{j} f_l = 1$ *for some* $i \leq j$.

(ii) *If* $G = \langle X \rangle$ *and* $1 \in X$ *then* $G = X^{*m}$.

LEMMA 3.2. *Let* M *be a* G*-module and suppose that* $\sum_{i=1}^{L} M(g_i^{e_i} - 1) = M$ *for some* $g_i \in G$ *and* $e_i \in \mathbb{N}$. *Then*

$$M = \sum_{i=1}^{L} M(g_i - 1).$$

LEMMA 3.3. *Let* $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathrm{Aut}(G)$. *Then*

$$[G, \alpha_1\alpha_2 \ldots \alpha_m] \subseteq [G, \alpha_1] \cdot \ldots \cdot [G, \alpha_m].$$

We shall also need the following useful result, due to Hamidoune:

LEMMA 3.4 ([H]). *Let X be a subset of G such that X generates G and $1 \in X$. If $|G| \leq m\,|X|$ then $G = X^{*2m}$.*

We conclude with some remarks about quasisimple groups. Let S be a finite quasisimple group. Then $\mathrm{Aut}(S)$ maps injectively into $\mathrm{Aut}(\overline{S})$ and $\mathrm{Out}(S)$ maps injectively into $\mathrm{Out}(\overline{S})$. Since every finite simple group can be generated by 2 elements [AG], it follows that

$$|\mathrm{Aut}(S)| \leq |\mathrm{Aut}(\overline{S})| \leq \left|\overline{S}\right|^2.$$

Also S can be generated by two elements, since if $S = \langle X\rangle\, \mathrm{Z}(S)$ then $S = [S,S] \subseteq \langle X\rangle$.

Since $\left|M(\overline{S})\right| < \left|\overline{S}\right|$ ([G, Table 4.1]) and $|\mathrm{Z}(S)| \leq \left|M(\overline{S})\right|$ we have $|S| \leq \left|\overline{S}\right|^2$.

If $g \in S \setminus \mathrm{Z}(S)$ then $[S,g]\cdot[S,g]^{-1}$ contains (many) noncentral conjugacy classes of S; it follows that S is generated by the set $[S,g]$.

4. Deduction of Theorem 1.1

This depends on the special case of Theorem 1.2 where $q = 1$. Assuming that this case has been proved, we begin by showing that the constant $C(1)$ may be reduced to 1, provided the constant $M(1)$ is suitably enlarged.

Let $\mathcal{S}$ denote the finite set of quasisimple groups S such that $|S/\mathrm{Z}(S)| \leq C = C(1)$, and put $M' = C^4$. We claim that if $S \in \mathcal{S}$ and $\beta_1, \ldots, \beta_{M'}$ are any automorphisms of S then there exist $g_1, \ldots, g_{M'} \in S$ such that

$$S = \prod_{j=1}^{M'} [S, \overline{g}_j \beta_j]. \tag{1}$$

Thus in Theorem 1.2 we may replace $C(1)$ by 1 provided we replace $M(1)$ by $\max\{M(1),\, M'\}$.

Since $|\mathrm{Aut}(S)| \leq \left|\overline{S}\right|^2 \leq C^2$, Lemma 3.1(i) implies that the sequence $(\beta_1, \ldots, \beta_{M'})$ contains subsequences $(\beta_1(i), \ldots, \beta_{j(i)}(i))$, $i = 1, \ldots, C^2$, such that (a) $\prod_{l=1}^{j(i)} \beta_l(i) = 1$ for each i, and (b) for each $i < C^2$, $\beta_{j(i)}(i)$ precedes $\beta_1(i+1)$; we will call such subsequences 'strictly disjoint'.

Fix a noncentral element $g \in S$ and put

$$g_1(i) = g$$
$$g_2(i) = \cdots = g_{j(i)}(i) = 1$$

for $i = 1, \ldots, C^2$. Then Lemma 3.3 gives

$$\prod_{l=1}^{j(i)} [S, \overline{g_l(i)}\beta_l(i)] \supseteq [S, \overline{g} \prod_{l=1}^{j(i)} \beta_l(i)] = [S,g]$$

for each i. As $[S,g]$ generates S and $|S| < \left|\overline{S}\right|^2 \leq C^2$ it now follows by Lemma 3.1(ii) that

$$S = [S,g]^{*C^2} \subseteq \prod_{i=1}^{C^2} \prod_{l=1}^{j(i)} [S, \overline{g_l(i)}\beta_l(i)].$$

This gives (1) for a suitable choice of the g_j, each equal to either g or 1.

Let us re-define $M(1)$ now so that the statement of Theorem 1.2 holds with $C(1) = 1$, and set $D = M(1)$. Then Theorem 1.1 follows on taking $S = G$ and $k = D$ in the next lemma:

LEMMA 4.1. *Let G be a group and let $\beta_1, \dots, \beta_k \in \mathrm{Aut}(G)$. Suppose that there exist $g_1, \dots, g_k \in G$ such that*

$$G = \prod_{i=1}^{k} [G, \overline{g}_i\beta_i].$$

Then for any $\alpha_1, \dots, \alpha_k \in \mathrm{Aut}(G)$,

$$G = \prod_{i=1}^{k} T_{\alpha_i,\beta_i}(G,G).$$

Proof. Note the identities

$$T_{\alpha,\beta}(h^{-\alpha^{-1}}, z^h) = [h^{-1}, \alpha^{-1}]^{-1} \cdot [z, \overline{h}\beta],$$
$$a[xa, \beta] = [x, \beta]a^{\beta};$$

the second one implies that

$$a[G, \beta] = [G, \beta]a^{\beta}$$

for any $a \in G$ and $\beta \in \mathrm{Aut}(G)$.

Now let $g_1, \dots, g_k$ be the given elements of G and put $a_i = [g_i^{-1}, \alpha_i^{-1}]^{-1}$ for each i. Then

$$\prod_{i=1}^{k} T_{\alpha_i,\beta_i}(G,G) \supseteq a_1[G, \overline{g}_1\beta_1]a_2[G, \overline{g}_2\beta_2] \dots a_k[G, \overline{g}_k\beta_k]$$
$$= [G, \overline{g}_1\beta_1][G, \overline{g}_2\beta_2] \dots [G, \overline{g}_k\beta_k] \cdot b = G$$

where

$$b = \prod_{i=1}^{k} a_i^{\overline{g}_i\beta_i \dots \overline{g}_k\beta_k}.$$

This completes the proof. □

5. Alternating groups and groups of Lie type over small fields

Given $q \in \mathbb{N}$ we fix a large integer $K = K(q)$ (greater than 100, say); how large K has to be will appear in due course. Let $\mathcal{S}_{\mathbf{1a}}$ denote the family of all quasisimple groups S such that $\overline{S} = \mathrm{Alt}(k)$ for some $k > K$, and let $\mathcal{S}_{\mathbf{1b}}$ denote the family of all quasisimple groups of Lie type of Lie rank greater than K over fields F with $|F| \leq K$. Let $\mathcal{S}_1 = \mathcal{S}_{\mathbf{1a}} \cup \mathcal{S}_{\mathbf{1b}}$.

For $S \in \mathcal{S}_1$ we define a subgroup S_0 of S as follows:

(a) If $\overline{S} = \mathrm{Alt}(k)$, let S_0 be the inverse image in S of $\mathrm{Alt}(\{3, \dots, k\}) \cong \mathrm{Alt}(k-2)$, the pointwise stabilizer of $\{1, 2\}$;

(b) If S is of Lie type, first recall the definition of $\mathcal{D}_0 \subseteq \mathcal{D}$ and $\Pi_0 \subseteq \Sigma$ from Section 2.

In case $\Sigma = A_r, D_r$ (i.e. S has type $A_r, D_r, {}^2A_r$ or ${}^2D_r$) there is a graph automorphism $\tau \neq 1$ of the untwisted version of S. Define S_0 to be the group of fixed points under τ of the group

$$R := \langle X_v(\lambda) \mid v \in \pm\Pi_0,\ \lambda \in \mathbb{F}_p \rangle .$$

Here $\mathbb{F}_p$ is the prime field of F.

In the remaining cases (i.e. Σ of type B_r, C_r and S is untwisted) define $S_0 := R$.

It is easy to see that in all cases from (b) we have $S_0 \leq S$ and S_0 is centralized by $\mathcal{D}_0\Phi\Gamma$.

In case (a), let τ denote the lift to $\mathrm{Aut}(S)$ of the automorphism of $\overline{S}$ given by conjugation by (12). Then $\mathrm{Aut}(S) = \mathrm{Inn}(S)\langle\tau\rangle$ and τ acts trivially on S_0. Also $\log|S|/\log|S_0| \leq 2$ and $|\mathrm{Z}(S)| \leq 2$.

In case (b), S_0 is again a quasisimple group of Lie type, and of Lie rank at least $K/2 - 1$ ([GLS, §2.3]). It is fixed elementwise by automorphisms of S lying in the set $\mathcal{D}_0\Phi\Gamma$, and we have

$$\log|S|/\log|S_0| \leq 2(F : \mathbb{F}_p) + A \leq 3\log K, \tag{2}$$

say, where A is some constant. Also $|\mathrm{Z}(S)| \leq K$.

From Section 2 we have $|\mathcal{D}_0| \leq |F^*|^2$ and $\mathrm{Aut}(S) = \mathrm{Inn}(S)\mathcal{D}_0\Phi\Gamma$. Note that $\mathcal{D}_0\Phi\Gamma$ is a subgroup of $\mathrm{Aut}(S)$ and $|\mathcal{D}_0\Phi\Gamma| \leq 2K^2\log K$.

Now let $S \in \mathcal{S}_1$. To prove Theorem 1.2 for S, we have to show that given automorphisms $\beta_1, \dots, \beta_M$ of S, where M is sufficiently large, and given divisors $q_1, \dots, q_M$ of q, we can find inner automorphisms $\alpha_1, \dots, \alpha_M$ of S such that

$$S = [S, (\alpha_1\beta_1)^{q_1}] \cdot \ldots \cdot [S, (\alpha_M\beta_M)^{q_M}]. \tag{3}$$

We may freely adjust each of the automorphisms β_i by an inner automorphism, and so without loss of generality we assume that each $\beta_i \in \{1, \tau\}$ if $\overline{S}$ is alternating, and that each $\beta_i \in \mathcal{D}_0\Phi\Gamma$ if S is of Lie type.

LEMMA 5.1. *Provided $K = K(q)$ is sufficiently large, there exists a q^{th} power h in S_0 such that*

$$\log |\overline{h}^{\overline{S}}| \geq \frac{\log |S|}{36 \log K}.$$

Proof. By examining the proofs of Lemmas 1 – 4 of [SW], one finds that provided the degree (resp the Lie rank) of $\overline{S_0}$ is large enough, $\overline{S_0}$ is a product of six conjugacy classes of q^{th} powers (even stronger results may be deduced from [LS2].) It follows that S_0 contains a q^{th} power h such that the conjugacy class of $\overline{h}$ in $\overline{S_0}$ has size at least $|\overline{S_0}|^{1/6}$. The result now follows from (2) since $|S_0| \leq |\overline{S_0}|^2$. □

Next, we quote a related result of Liebeck and Shalev:

THEOREM 5.2 ([LS2, Th. 1.1]). *There is an absolute constant C_0 such that for every simple group T and conjugacy class X of T,*

$$T = X^{*t},$$

where $t = \lfloor C_0 \log |T| / \log |X| \rfloor$.

Now take $T = S/\mathrm{Z}(S)$ and $X = \overline{h}^T$ where $h \in S_0$ is given by Lemma 5.1. Since $[S, h] = (h^{-1})^S \cdot h$, the above theorem gives

$$S = [S, h]^{*\lceil 36 C_0 \log K \rceil} \cdot \mathrm{Z}(S).$$

Applying Lemma 3.4 we deduce that

$$S = [S, h]^{*M'} \tag{4}$$

where $M' = \lceil 72 K C_0 \log K \rceil$.

Suppose now that $M \geq 2K^2 \log K \cdot M'$. Then the group generated by $\beta_1, \ldots, \beta_M$ has order at most M/M', and we may use Lemma 3.1, as in the preceding section, to find strictly disjoint subsequences $(\beta_1(i)^{q_{1,i}}, \ldots, \beta_{j(i)}(i)^{q_{j(i),i}})$ of $(\beta_1^{q_1}, \ldots, \beta_M^{q_M})$, $i = 1, \ldots, M'$, such that $\prod_{l=1}^{j(i)} \beta_l(i)^{q_{l,i}} = 1$ for each i.

Since h is is a q^{th} power in S_0, for each i there exists $h_i \in S_0$ such that $h_i^{q_{1,i}} = h$. Then each $\overline{h_i}$ commutes with each β_j; now, putting

$$\begin{aligned} \alpha_1(i) &= \overline{h_i}, \\ \alpha_j(i) &= 1 \qquad (j \geq 2), \end{aligned}$$

we have

$$\prod_{l=1}^{j(i)} (\alpha_l(i)\beta_l(i))^{q_{l,i}} = \overline{h}.$$

Hence

$$[S,h]=[S,\prod_{l=1}^{j(i)}(\alpha_l(i)\beta_l(i))^{q_{l,i}}]\subseteq\prod_{l=1}^{j(i)}[S,(\alpha_l(i)\beta_l(i))^{q_{l,i}}],$$

by Lemma 3.3, and (3) follows from (4).

Thus Theorem 1.2 holds for groups $S\in\mathcal{S}_1$ provided $K=K(q)$ and $M=M(q)$ are sufficiently large.

6. Groups of Lie type over large fields: reductions

As before, we fix a positive integer q and denote by $K=K(q)$ some large positive integer, to be specified later. Let $\mathcal{S}_2$ (resp. $\mathcal{S}_3$) denote the family of all quasisimple groups of Lie type of Lie rank at most 8 (resp. at least 9) over fields F with $|F|>K$. According to the classification, all but finitely many finite quasisimple groups lie in $\mathcal{S}_1\cup\mathcal{S}_2\cup\mathcal{S}_3$, and so it remains only to prove Theorem 1.2 for groups in $\mathcal{S}_2\cup\mathcal{S}_3$.

The validity of this theorem for groups of Lie type over large fields depends on there being 'enough room' for certain equations to be solvable. In order to exploit this, we need to restrict the action of the relevant automorphisms to some very small subgroups; this is made possible (as in the preceding section) by choosing a suitable representative for each outer automorphism. The desired 'global' conclusion will then be derived with the help of the following result of Liebeck and Pyber:

THEOREM 6.1 ([LP, Th. D]). *Let S be a quasisimple group of Lie type. Then $S=(U_+U_-)^{*12}\cdot U_+$.*

For the rest of this section, S denotes a group in $\mathcal{S}_2\cup\mathcal{S}_3$, and we use the notation of Section 2 for root subgroups etc. Our aim is to prove

PROPOSITION 6.2. *There is a constant $M_1=M_1(q)$ such that if $\gamma_1,\dots,\gamma_{M_1}$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and $q_1,\dots,q_{M_1}$ are divisors of q then there exist elements $h_1,\dots,h_{M_1}\in H$ and $u_1,\dots,u_{M_1}\in U$ such that*

$$U\subseteq\prod_{i=1}^{M_1}[U,(\overline{u_ih_i}\gamma_i)^{q_i}].$$

By symmetry, the same result will then hold with U_- in place of $U=U_+$. Since $\mathrm{Aut}(S)=\mathrm{Inn}(S)\mathcal{D}\Phi\Gamma$, this together with the above theorem shows that Theorem 1.2 holds for S as long as $M(q)\geq 25M_1(q)$.

To establish Proposition 6.2, we shall express U as a product of certain special subgroups, each of which itself satisfies a similar property. There are several different cases to consider, and we apologise for the complexity of the

argument. The basic idea in all cases is the same: the required result is reduced to showing that certain equations are solvable over a suitable finite field, and then applying a general result about such equations, namely Lemma 7.1 below.

The first class of special subgroups is defined as follows:

Definition 6.3. Let S be a quasisimple group of Lie type.

Case 1: *when S is untwisted.* Let ω be an equivalence class of roots from $\Sigma/\sim$ as defined in Section 2. The corresponding *orbital subgroup* is then defined to be

$$O(\omega) = W_\omega := \langle X_v \mid v \in \omega \rangle = \prod_{v \in \omega} X_v$$

(product ordered by increasing height of roots)

Case 2: *when $S = S^*$ is twisted.* Define

$$O(\omega) := Y_\omega$$

to be the root subgroup of S corresponding to the equivalence class ω of the untwisted root system Σ under $\sim$ described in Section 2.

Note (i). The orbital subgroups are invariant under $\mathcal{D}\Phi\Gamma$.

(ii). In case 2, Y_ω is in fact a subgroup of the orbital subgroup W_ω defined in Case 1 for the untwisted version of S^*.

In Section 8 we prove

PROPOSITION 6.4. *There is a positive integer $L = L(q)$ such that if $\gamma_1, \ldots, \gamma_L$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$, $q_1, \ldots, q_L$ are divisors of q and $O = O(\omega)$ is an orbital subgroup of S then there exist elements $h_1, \ldots, h_L \in H$ such that*

$$O \subseteq \prod_{i=1}^{L} [O, (\overline{h_i}\gamma_i)^{q_i}].$$

Now suppose that $S \in \mathcal{S}_2$. Then U is equal to the product of at most 120 root subgroups, each of which is contained in an orbital subgroup. So in this case Proposition 6.2 follows as long as we take $M_1(q) \geq 120L$.

For arbitrary groups $S \in \mathcal{S}_3$ we can't write U as a bounded product of orbital subgroups. However, S is then a classical group, and contains a relatively large subgroup of type SL. For the group SL itself we prove

PROPOSITION 6.5. *Let $S = \mathrm{SL}_{r+1}(F)$, where $|F| > K$ and $r \geq 3$. There is a constant $M_2 = M_2(q)$ such that if $\gamma_1, \ldots, \gamma_{M_2}$ are automorphisms of S*

lying in $\mathcal{D}\Phi\Gamma$ *and* $q_1, \ldots, q_{M_2}$ *are divisors of* q *then there exist automorphisms* $\eta_1, \ldots, \eta_{M_2} \in \mathcal{D}$ *and elements* $u_1, \ldots, u_{M_2} \in U$ *such that*

$$U \subseteq \prod_{i=1}^{M_2} [U, (\overline{u_i}\eta_i\gamma_i)^{q_i}].$$

Note that this differs from Proposition 6.2 in that the elements η_i are allowed to vary over *all diagonal automorphisms* of S, not just the inner ones.

We also need to consider the following special subgroups V_{s+1} and V^*_{s+1} of the full unitriangular group:

Definition 6.6. (i) In $\mathrm{SL}_{s+1}(F)$ define

$$V_{s+1} = \begin{pmatrix} 1 & * & \cdots & * & * \\ & 1 & \mathbf{0} & 0 & * \\ & & \ddots & \mathbf{0} & \vdots \\ & & & 1 & * \\ & & & & 1 \end{pmatrix} < \mathrm{SL}_{s+1}(F)$$

as the group of unitriangular matrices differing from the identity only in the first row and last column.

(ii) Consider $\mathrm{SU}_{s+1}(F)$ as the set of fixed points of the Steinberg automorphism σ of $\mathrm{SL}_{s+1}(F)$. Then

$$V^*_{s+1} = V_{s+1} \cap \mathrm{SU}_{s+1}(F),$$

the set of fixed points of σ on V_{s+1}.

Note that V_{s+1} and V^*_{s+1} are stabilized by automorphisms of $\mathrm{SL}_{s+1}(F)$, resp. $\mathrm{SU}_{s+1}(F)$, lying in $\mathcal{D}\Phi\Gamma$.

Proposition 6.7. *Let* $S = \mathrm{SL}_{s+1}(F)$ *or* $\mathrm{SU}_{s+1}(F)$ *where* $s \geq 5$ *and* $|F| > K$. *Put* $V = V_{s+1}$ *in the first case,* $V = V^*_{s+1}$ *in the second case. There is a positive integer* $L_1 = L_1(q)$ *such that if* $\gamma_1, \ldots, \gamma_{L_1}$ *are automorphisms of* S *lying in* $\mathcal{D}\Phi\Gamma$ *and* $q_1, \ldots, q_{L_1}$ *are divisors of* q *then there exist elements* $h_1, \ldots, h_{L_1} \in H$ *such that*

$$V = \prod_{i=1}^{L_1} [V, (\overline{h_i}\gamma_i)^{q_i}].$$

Of course, the point here is that L_1 is independent of s.

The last two propositions will be proved in Section 9. We need one more kind of special subgroup, denoted P. This is defined for groups S of type

$$\mathcal{X} \in \{{}^2A_r,\ B_r,\ C_r,\ D_r,\ {}^2D_r\},\ r \geq 4.$$

Recall that Σ is the root system of $\mathcal{X}$ (twisted or untwisted). In each of these five cases, there exist fundamental roots δ, $\delta' \in \Sigma$ (equal unless $\mathcal{X} = D_r$, see below) such that the other fundamental roots $\Pi' = \Pi - \{\delta, \delta'\}$ generate a root system Σ' of type A_s, for the appropriate $s\,(= \lceil \frac{r}{2} \rceil - 1,\ \ r-1$ or $r-2)$: in types ${}^2A_r, B_r, C_r$ and ${}^2D_r$ we take $\delta = \delta'$ to be the fundamental root of length distinct from the others; in type D_r, $\{\delta, \delta'\}$ is the pair of fundamental roots swapped by the symmetry τ of D_r (see [GLS, Prop. 2.3.2]).

If S is untwisted, put $S_1 = \langle X_w \mid w \in \Sigma' \rangle$ and $U_1 = \prod_{w \in \Sigma'_+} X_w$. If S is twisted, define S_1 and U_1 similarly by replacing the root subgroups X_w with the corresponding root subgroup Y_ω, $\omega^* \in \Sigma'$.

Then S_1 is a quasisimple group of type A_s (a Levi subgroup of S), it is fixed pointwise by Γ, and U_1 is its positive unipotent subgroup.

Definition 6.8. If S is *untwisted*, set

$$P = \prod_{w \in \Sigma_+ \setminus \Sigma'_+} X_w.$$

If S is *twisted*, set

$$P = \prod_{\omega^* \in \Sigma_+ \setminus \Sigma'_+} Y_\omega.$$

Note that P is a subgroup of U stabilized by $\mathcal{D}\Phi\Gamma$ and that

$$U = U_1 P.$$

In the final section we prove

Proposition 6.9. *Assume that $|F| > K$ and that S is of type B_r, C_r, D_r or ${}^2D_r$, where $r \geq 4$. There is a constant $N_1 = N_1(q)$ such that if $\gamma_1, \dots, \gamma_{N_1}$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and $q_1, \dots, q_{N_1}$ are divisors of q then there exist elements $h_1, \dots, h_{N_1} \in H$ such that*

$$P \subseteq \prod_{i=1}^{N_1} [P, (\overline{h_i}\gamma_i)^{q_i}].$$

Proposition 6.10. *Assume that $|F| > K$ and that S is of type ${}^2A_r$, where $r \geq 4$. There is a constant $N_1' = N_1'(q)$ such that if $\gamma_1, \dots, \gamma_{N_1'}$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and $q_1, \dots, q_{N_1'}$ are divisors of q then there exist automorphisms $\eta_1, \dots, \eta_{N_1'} \in \mathcal{D}$ such that*

$$P \subseteq \prod_{i=1}^{N_1'} [P, (\eta_i\gamma_i)^{q_i}].$$

Assuming the last five propositions, we may now complete the

Proof of Proposition 6.2. We take S to be a quasisimple group in $\mathcal{S}_3$, and deal with each type in turn.

Case 1: *Type* A_s, *where* $s \geq 5$. (For $S \in \mathcal{S}_3$ we only need $s \geq 9$; the more general result is needed for later applications.)

Assume to begin with that $S = \mathrm{SL}_{s+1}(F)$; here $|F| > K$ and $s \geq 5$. Let S^1 be the copy of $\mathrm{SL}_{s-1}(F)$ sitting in the middle $(s-1) \times (s-1)$ square of S, and let U^1 denote the upper unitriangular subgroup of S^1.

Now U^1 is the positive unipotent subgroup of S^1, and the diagonal subgroup H of S induces by conjugation on S^1 its full group of diagonal automorphisms. Also, diagonal, field and graph automorphisms of S restrict to automorphisms of the same type on S^1. Thus given M_2 automorphisms γ_i of S lying in $\mathcal{D}\Phi\Gamma$ and M_2 divisors q_i of q, Proposition 6.5 applied to S^1 shows that there exist elements $h_i \in H$ and $u_i \in U^1$ such that

$$U^1 \subseteq \prod_{i=1}^{M_2} [U^1, (\overline{u_i h_i}\gamma_i)^{q_i}].$$

On the other hand, we have $U = U^1 V_{s+1}$. With Proposition 6.7 this shows that Proposition 6.2 holds for $S = \mathrm{SL}_{s+1}(F)$ provided we take $M_1 \geq M_2 + L_1$.

The validity of Proposition 6.2 then follows for every quasisimple group S of type A_s ($s \geq 5$), since automorphisms of S in $\mathcal{D}\Phi\Gamma$ lift to automorphisms of the same type of its universal covering group $\mathrm{SL}_{s+1}(F)$.

Case 2: *Type* ${}^2A_s$, *where* $s \geq 9$. As above, we may assume that in fact $S = \mathrm{SU}_{s+1}(F)$. Considering the fixed points of the Steinberg automorphism in $\mathrm{SL}_{s+1}(F)$, we see that

$$U = U^1 V^*_{s+1}$$

where U^1 is the positive unipotent subgroup of S^1 and S^1 is a copy of $\mathrm{SU}_{s-1}(F)$ sitting 'in the middle' of S. Again, the diagonal subgroup H of S induces by conjugation on S^1 its full group of diagonal automorphisms.

Now we apply Definition 6.8 and the discussion preceding it to the group S^1; this gives a subgroup S_2 of S^1 of type A_t where $t = \left\lceil \frac{s-2}{2} \right\rceil - 1 \geq 3$, and the subgroup P, and we have

$$U^1 = U_2 P$$

where U_2 denotes the positive unipotent subgroup of S_2.

Proposition 6.2 now follows for S on combining Propositions 6.5 (for U_2), 6.10 (for P), and 6.7 (for V^*_{s+1}), and taking $M_1 = M_2 + L_1 + N'_1$.

Case 3: *Type* B_r, C_r, D_r *or* ${}^2D_r$, *where* $r \geq 9$. Again we apply Definition 6.8 and the discussion preceding it. This gives a subgroup S_1 of S of type A_s,

where $s \geq 7$, and the corresponding subgroup P, and $U = U_1 P$ where U_1 is the positive unipotent subgroup of S_1. In this case, Proposition 6.2 follows from Case 1, done above, and Proposition 6.9, on taking $M_1 = M_2 + L_1 + N_1$.

This completes the proof, modulo Propositions 6.4–6.10.

The proofs of Propositions 6.9 and 6.10, given in Section 10, are similar to that of Proposition 6.4, but even more complicated. An alternative approach is available if we are prepared to quote the following general result, which is established in [N]:

THEOREM 6.11. *Let S be a quasisimple group of classical type over a finite field F. Then S contains a subgroup S_1 such that*

(i) *S_1 is quasisimple of type A_n over F or F_0, for some n,*

(ii) *S_1 is invariant under $\mathcal{D}\Phi\Gamma$,*

(iii) *there exist $g_1, \ldots, g_h \in S$ such that $S = \prod_{i=1}^{h} g_i^{-1} S_1 g_i$, where h is an absolute constant.*

(The constant h is probably rather less than 600.)

Suppose we have established Proposition 6.2 for groups of type A_n. Then Theorem 1.2 holds for such groups, with a constant $M(q)$ say. Now let $S \in \mathcal{S}_3$, not of type A_n, and let β_{ij} $(1 \leq i \leq h,\ 1 \leq j \leq M(q))$ be given automorphisms of S. Let $x_{ij} \in S$ be such that $\gamma_{ij} := \overline{x_{ij}}\beta_{ij} \in \mathcal{D}\Phi\Gamma$. Applying Theorem 1.2 to S_1 we find elements $y_{ij} \in S_1$ such that for each i,

$$S_1 = \prod_{j=1}^{M(q)} [S_1,\ (\overline{y_{ij}}\gamma_{ij})^{q_{ij}}].$$

With (iii) this gives

$$S = \prod_{i=1}^{h} \prod_{j=1}^{M(q)} [S_1^{g_i},\ (\overline{u_{ij}}\beta_{ij})^{q_{ij}}]$$

where

$$u_{ij} = g_i^{-1} y_{ij} x_{ij} g_i^{\beta_{ij}^{-1}} \in S.$$

Thus Theorem 1.2 holds for S on replacing $M(q)$ by $hM(q)$. In this approach, it suffices to prove only Case 1 of Proposition 6.2, and Definition 6.8 and Propositions 6.9, 6.10 may be omitted (as may the part of Proposition 6.7 dealing with the group SU).

7. Surjective maps

The following lemma lies at the heart of the proof; here q and M denote positive integers:

LEMMA 7.1. *Let F be a finite field and let $\phi_1, \dots, \phi_M$ be automorphisms of F. Let $\mu_1, \mu_2, \dots, \mu_M$ be nonzero elements of F, let $q_1, \dots, q_M$ be divisors of q and let $c_1, \dots, c_M$ be positive integers. For $\lambda, t \in F$ put*

$$f_{i,\lambda}(t) = \mu_i \lambda^{c_i(1+\phi_i+\cdots+\phi_i^{q_i-1})} t^{\phi_i^{q_i}} - t$$

and for $\underline{\lambda}, \mathbf{t} \in F^{(M)}$ define

$$f_{\underline{\lambda}}(\mathbf{t}) = \sum_{i=1}^{M} f_{i,\lambda_i}(t_i). \tag{5}$$

(a) *Assume that $M > q(cq+1)$ and $|F| > c(cq+1)^q$ where $c = \max\{c_1, \dots, c_M\}$. Then there exist $\lambda_1, \dots, \lambda_M \in F^*$ such that the map $f_{\underline{\lambda}} : F^{(M)} \to F$ is surjective.*

(b) *Let $\overline{F} \subseteq F$ be a subfield such that $(F : \overline{F}) = 2$. Assume that $M > 2q(2cq+1)$ and that $|F| > c^2(2cq+1)^{2q}$. Then the conclusion of part* (a) *holds for some $\lambda_1, \dots, \lambda_M \in \overline{F}^*$.*

Proof. We shall give the proof of part (a) first and afterwards indicate the modifications necessary to deduce part (b).

It will clearly suffice to show that for some subset $J \subseteq \{1, \dots, M\}$ and some $\lambda_j \in F^*$ $(j \in J)$ the map $F^{(|J|)} \to F$ given by

$$(t_i)_{i \in J} \mapsto \sum_{i \in J} f_{i,\lambda_i}(t_i)$$

is surjective. When $|J| = 1$, this is equivalent to showing that it has zero kernel (as it is linear over the prime field). Letting F_i denote the fixed field of ϕ_i in F, we consider three cases.

Case 1. Suppose that for some i we have $\mu_i \notin [F^*, \phi_i^{q_i}]$. Then for $t \in F^*$ we have

$$f_{i,1}(t) = \mu_i t^{\phi_i^{q_i}} - t = \left(\mu_i - [t^{-1}, \phi_i^{q_i}]\right) t^{\phi_i^{q_i}} \neq 0,$$

so the kernel of $f_{i,1} : F \to F$ is zero; we take $J = \{i\}$, $\lambda_i = 1$.

Henceforth, we may assume that for each i there exists $b_i \in F^*$ such that

$$\mu_i = b_i b_i^{-\phi_i^{q_i}}.$$

Case 2. Suppose that $|F_i| > cq+1$ for some i. Let λ be a generator for the cyclic group F^*. We claim that the map $f_{i,\lambda} : F \to F$ has zero kernel. Indeed, suppose not. Then there exists $t \in F^*$ such that

$$\mu_i \lambda^{c_i(1+\phi_i+\cdots+\phi_i^{q_i-1})} t^{\phi_i^{q_i}} = t,$$

so that writing $B = [F^*, \phi_i]$ we have

$$\lambda^{c_i(1+\phi_i+\cdots+\phi_i^{q_i-1})} = b_i^{-1} t \cdot (b_i^{-1}t)^{-\phi_i^{q_i}} \in B.$$

As $\lambda^{c_i(1+\phi_i+\cdots+\phi_i^{q_i-1})} \equiv \lambda^{c_i q_i}$ modulo B it follows that the cyclic group F^*/B has order dividing $c_i q_i$. But $|F^*|/|B| = |F_i^*| > cq \geq c_i q_i$, a contradiction. Thus we may take $J = \{i\}$, $\lambda_i = \lambda$ in this case.

Case 3. Suppose that $|F_i| \leq cq+1$ for all i. Then there are at most $cq+1$ possibilities for the size of each F_i, and also at most q possibilities for each q_i. As $M > q(cq+1)$ there exist $i < j \in \{1, \ldots, M\}$ such that $|F_i| = |F_j|$ and $q_i = q_j$. Say $i = 1$ and $j = 2$. We claim that in this case, there exists $\lambda \in F^*$ such that the map

$$(t_1, t_2) \mapsto f_{1,\lambda}(t_1) + f_{2,1}(t_2)$$

from $F^{(2)}$ to F is surjective.

It will suffice to show that for a suitable λ,

$$(t_1, t_2) \mapsto b\left(\lambda^{c_1(1+\phi_1+\cdots+\phi_1^{q_1-1})} t_1^{\phi_1^{q_1}} - t_1\right) - \left(t_2^{\phi_2^{q_2}} - t_2\right) = g_\lambda(t_1, t_2),$$

say, is surjective, where $b = -b_1 b_2^{-1}$: replace t_i by $b_i^{-1} t_i$ and divide by $-b_2$.

Since ϕ_1 and ϕ_2 have the same fixed field, they generate the same subgroup of $\mathrm{Aut}(F)$. So $\phi_1 = \phi_2^l$ for some l. Writing

$$t^* = t + t^{\phi_2^{q_2}} + \cdots + t^{\phi_2^{(l-1)q_2}}$$

and recalling that $q_1 = q_2$ we have

$$\begin{aligned} g_\lambda(t, (bt)^*) &= b\left(\lambda^{c_1(1+\phi_1+\cdots+\phi_1^{q_1-1})} t^{\phi_1^{q_1}} - t\right) - \left((bt)^{\phi_1^{q_1}} - bt\right) \\ &= \left(b\lambda^{c_1(1+\phi_1+\cdots+\phi_1^{q_1-1})} - b^{\phi_1^{q_1}}\right) t^{\phi_1^{q_1}}. \end{aligned}$$

It follows that g_λ is surjective unless the bracketed factor is zero.

Suppose that this factor is zero for every $\lambda \in F^*$. Taking $\lambda = 1$ gives $b^{-1} b^{\phi_1^{q_1}} = 1$, which then implies that $\lambda^{c_1(1+\phi_1+\cdots+\phi_1^{q_1-1})} = 1$ for every $\lambda \in F^*$. Then $\lambda^{c_1 \phi_1^{q_1}} = \lambda^{c_1}$, hence λ^{c_1} is in the fixed field E of $\phi_1^{q_1}$ for every λ, and it follows that $|F^*| \leq c_1 |E^*|$. On the other hand, the degree of the extension E/F_1 divides q_1; as $|F_1| \leq cq+1$ this implies $|E| \leq (cq+1)^q$. Thus

$$|F| \leq 1 + c_1((cq+1)^q - 1) \leq c(cq+1)^q,$$

contradicting the hypothesis.

This completes the proof of part (a). For part (b) we need some additional notation:

Let $\overline{F}_i = \overline{F} \cap F_i$ be the fixed field of ϕ_i in $\overline{F}$ and let $\bar{\phi}_i$ be the generator of $\mathrm{Gal}(F/\overline{F}_i)$. If θ is the nontrivial automorphism of $F/\overline{F}$ then $\langle \bar{\phi}_i \rangle = \langle \phi_i, \theta \rangle$.

The proof proceeds on the same lines as Part (a) with the following modifications:

Case 1 is the same.

In Case 2 we assume $|\overline{F}_i| > 2cq + 1$ and take $\lambda := \mu^{1+\theta} \in \overline{F}^*$, where μ is a generator of F^*. Suppose that the kernel of $f_{i,\lambda}$ is nonzero. Define $B := [F^*, \bar{\phi}_i]$. By considering $\lambda^{c_i(1+\phi_i+\cdots+\phi_i^{q_i-1})}$ modulo B we deduce that the cyclic group F^*/B has order $|\overline{F}_i^*|$ dividing $2c_iq_i$, a contradiction.

In Case 3 we assume that $|\overline{F}_i| \leq 2cq + 1$ for all i. As $F_i/\overline{F}_i$ has degree 1 or 2 this leaves at most $2(2cq + 1)$ possibilities for F_i and hence there is a pair $1 \leq i < j \leq M$ such that $F_i = F_j$ and $q_i = q_j$. We proceed as in Part (a) except that at the end we reach the conclusion that for each $\lambda \in \overline{F}^*$ the element λ^{c_1} is in the fixed field $\overline{E} \subseteq \overline{F}_1$ of $\phi_1^{q_1}\,|_{\overline{F}_1}$. This gives $|\overline{F}^*| \leq c_1|\overline{E}^*|$ and as before $|\overline{E}| \leq |\overline{F}_1|^{q_1}$. Therefore

$$|F| = |\overline{F}|^2 \leq (c|\overline{F}_1|^q)^2 \leq c^2(2cq + 1)^{2q},$$

contradicting the hypothesis of Part (b). □

8. Orbital subgroups

We can now give the

Proof of Proposition 6.4. Recall that S is a quasisimple group of Lie type over a field F of size at least $K = K(q)$, and that the equivalence class $\omega \subseteq \Sigma_+$ is spanned by some orbit $\overline{\omega}$ of positive roots from the untwisted system Σ. Thus ω is the positive part of some (possibly orthogonally decomposable) root system of dimension at most 3. In fact the type of ω is one of $A_1, A_1 \times A_1, A_1 \times A_1 \times A_1, A_2, B_2$ or G_2. Therefore ω has a height function with respect to its fundamental roots. Let $\omega(i)$ be the set of (untwisted) roots of height at least i in ω.

The chief obstacle to applying Lemma 7.1 to $O = O(\omega)$ is that O may not be abelian. However it is a nilpotent p-group and our strategy is to find a filtration $O = O(1) \geq O(2) \geq \ldots \geq 1$ of normal subgroups such that each quotient $O(i)/O(i+1)$ is abelian and is even a vector space over F_0 or F. This filtration is in fact provided by the sets $\omega(i)$ above.

For clarity we shall divide the proof in two parts, dealing first with the case when S is of untwisted type and second with the case when S has twisted type.

The untwisted case. Recall that in this case we have $O(\omega) = W_\omega = \prod_{w\in\omega} X_w$. Define

$$W^i = \prod_{v\in\omega(i)} X_v.$$

This provides a natural filtration of subgroups

$$O = W_\omega = W^1 \geq W^2 \geq W^3 \geq W^4 = \{0\} \tag{6}$$

of length at most 3. The factors W^i/W^{i+1} are abelian and are modules for the group $\mathcal{D}\Phi\Gamma$.

The automorphisms $\gamma_i^{q_i}$ may involve a graph automorphism and thus may not stabilize the root subgroups.

We shall show that, provided L_0 and $|F|$ are sufficiently large, given $i \in \{1,2,3\}$ and $\gamma_1,\dots,\gamma_{L_0} \in \mathcal{D}\Phi\Gamma$, we can find elements $h_j \in H$ such that

$$W^i/W^{i+1} = \prod_{j=1}^{L_0} [W^i/W^{i+1}, \beta_j], \tag{7}$$

where $\beta_j = (\overline{h_j}\gamma_j)^{e_j q_j}$ for some $e_i \in \{1,2,3\}$ to be chosen below. Then Lemma 3.2 implies that the same will hold when each exponent $e_j q_j$ is replaced by q_j, and Proposition 6.4 will follow, in view of (6), if we take $L \geq 3L_0$.

To establish (7), fix a root $w \in \omega$ and define $e_j = e_j(w)$ to be the size of the orbit of w under the graph component of γ_j. Then $e_j \in \{1,2,3\}$ and $\gamma_j^{e_j}$ stabilizes the root subgroup X_w. Set

$$\alpha_j = (\overline{h_j}\gamma_j)^{e_j} = \overline{h_j}^{1+\gamma_j^{-1}+\cdots+\gamma_j^{1-e_j}} \gamma_j^{e_j},$$

where the $h_j \in H$ remain to be determined. We shall show that for a suitable L_1 it is possible to choose elements $h_j \in H$ so that

$$X_w \subseteq \prod_{j=1}^{L_1} [X_w, \alpha_j^{q_j}]. \tag{8}$$

Since ω contains at most six roots, this will give (7) with $L_0 = 6L_1$ (on relabelling γ_j and e_j, ($j = 1,\dots,L_0$) as $\gamma_l(w)$ and $e_l(w)$ with $w \in \omega$, $l = 1,\dots,L_1$).

If $e_j = 1$ we simply choose $h_j = h_w(\lambda_j)$ which acts on X_w as $t \mapsto \lambda_j^2 t$.

If $e_j = 2$ then the graph component τ of γ_j^{-1} sends w to another root $v \in \omega$. Let

$$h_j = h_w(\lambda_j^2) h_v(\lambda_j^{-\langle v,w\rangle}).$$

Then h_j acts trivially on X_v, and on X_w it acts as $t \mapsto \lambda_j^{4-\langle\tau,v\rangle\langle v,w\rangle} t$. Notice that $\langle w,v\rangle\langle v,w\rangle \in \{0,1,2,3\}$. Also $h_j^{\gamma_j^{-1}}$ acts trivially on X_w. It follows that $h_j h_j^{\gamma_j^{-1}}$ acts on X_w as multiplication by $\lambda_j^{c_j}$, where $c_j \in \{1,2,3,4\}$.

If $e_j = 3$, set $h_j = h_w(\lambda_j)$. The roots w, w^τ, w^{τ^2} are pairwise orthogonal; hence h_j acts trivially on X_{w^τ} and $X_{w^{\tau^2}}$; i.e. h_j^τ and $h_j^{\tau^2}$ act trivially on X_w. Therefore $h_j^{1+\gamma_j^{-1}+\gamma_j^{-2}}$ acts on X_w as multiplication by λ_j^2.

Suppose $\gamma_j^{e_j} \in \mathcal{D}\Phi\Gamma$ acts on $X_w(t)$ as $t \mapsto \nu_j t^{\phi_j}$ with $\nu_j \in F^*$ and $\phi_j \in \mathrm{Aut}(F)$. Then an easy computation shows that $\alpha_j^{q_j} = \left(\overline{h_j}^{1+\cdots+\gamma_j^{1-e_j}} \gamma_j^{e_j}\right)^{q_j}$ acts on $X_w(t)$ as

$$t \mapsto \mu_j \lambda_j^{c_j \phi_j (1+\phi_j+\cdots+\phi_j^{q_j-1})} t^{\phi_j^{q_j}}, \tag{9}$$

where $c_j \in \{1,2,3,4\}$ and μ_j is a constant which depends on ν_j, ϕ_j. In each case, therefore, (8) follows from Lemma 7.1, with $\lambda_j^{\phi_j}$ in place of λ_j, as long as we take $L_1 > q(4q+1)$ and $K > 4(4q+1)^q$.

The twisted case. Suppose now that $S = S^*$ is twisted with root system Σ^* coming from the corresponding untwisted root sytem Σ. The complication here is that the root subgroups are not necessarily 1-parameter. They are parametrized by the same equivalence classes ω of roots under the equivalence relation $\sim$ of Σ considered above. Recall the definition of the root subgroups Y_ω and their description in Section 2.

Notice that Y_ω can be considered as a subgroup of W_ω in the untwisted group above defined for Σ; in fact it is the subgroup of W_ω fixed by the Steinberg automorphism σ and inherits a filtration $Y_\omega = Y^1 \geq Y^2 \geq Y^3 \geq Y^4 = \{0\}$ from W. We shall therefore take $L > 3L_2$ and show that for large enough L_2 it is always possible to choose $\beta_j = (\overline{h_j}\gamma_j)^{q_j}$ with $h_j \in H$ so that

$$Y^i/Y^{i+1} = \prod_{j=1}^{L_2} [Y^i/Y^{i+1}, \beta_j]. \tag{10}$$

It is straightforward to adapt the strategy from the previous section since the parametrization of Y_ω is coming ready from the ambient untwisted group. However we keep in mind that we don't have all the diagonal elements at our disposal: only those fixed by σ.

In all cases Y^i/Y^{i+1} is a one-parameter group, parametrized by either F_0 or F. Also now $\Gamma = 1$, and we shall apply the argument from the previous subsection with each $e_j = 1$.

The case of F_0. When $\omega = A_1$ and $i = 1$, or $\omega = A_2$ and $i = 2$, the set $\omega(i) \setminus \omega(i+1)$ contains a single root v. Then

$$Y^i = X_v(aF_0) \cdot Y^{i+1},$$

where $a = 1$ for type A_1, and $a \in F$ is any solution of $a + a^\phi = 0$ for type A_2.

In this case, we set $h_j = h_v(\lambda_j) \in H$ where the $\lambda_j \in F_0$ are chosen so that the map $f_{\underline{\lambda}}$ defined by (5), with $c_i = 2$ for each i, is surjective. This is possible

by Lemma 7.1 (applied to F_0) provided $|F_0| > 2(2q+1)^q$ and $L_2 > q(2q+1)$ Then (10) follows as in the preceding subsection.

The case of F. In all other cases except for $\omega = (A_1)^3$, the set $\omega(i) \setminus \omega(i+1) = \{v, w\}$ consists of a pair of roots, swapped by τ. Say v is the longer root. Then

$$Y^i = \Big\{ X_v(\xi) X_w(\xi^\phi) \mid \xi \in F \Big\} \cdot Y^{i+1}.$$

Again we argue as in the preceding subsection (with $e_j = 1$), but this time we set

$$h_j = h_v(\rho_j) h_w(\rho_j^\phi),$$

for suitably chosen $\rho_j \in F$. Then h_j acts on Y^i/Y^{i+1} via $\xi \mapsto \rho_j^{2+\langle v,w\rangle\phi}\xi$. Notice that $|\langle v, w\rangle| \in \{0, 1, 2, 3\}$, and that if $\langle v, w\rangle \neq 0$ then $[|\langle v, w\rangle|]\phi^2$ is the indentity automorphism of F. Consequently

$$t^{4-(\langle v,w\rangle\phi)^2} = t^{4-|\langle v,w\rangle|} \quad \forall\, t \in F.$$

Taking $\rho_j = \lambda_j^{2-\langle v,w\rangle\phi}$ makes h_j act on Y^i/Y^{i+1} via

$$\xi \mapsto \lambda_j^{4-|\langle v,w\rangle|} \cdot \xi.$$

So again we can apply Lemma 7.1 with $c_i = c = 4-|\langle v, w\rangle|$ for each i, provided we assume that $L_2 > q(4q+1)$ and $|F| > 4(4q+1)^q$; and (10) follows as above.

Finally, when $\omega = \{v, v^\tau, v^{\tau^2}\}$ is of type $(A_1)^3$ we use

$$h_j = h_v(\lambda_j) h_{v^\tau}(\lambda_j^{\phi_j}) h_{v^{\tau^2}}(\lambda_j^{(\phi_j)^2}),$$

($\lambda_j \in F$). This acts on $Y_\omega(t)$ as $t \mapsto \lambda_j^2 t$, and we apply Lemma 7.1 with all $c_i = 2$.

9. The unitriangular group

Here we establish Propositions 6.5 and 6.7. We begin with the latter which concerns the group $V = V_{s+1}$ of unitriangular matrices in $S = \mathrm{SL}_{s+1}(F)$ or $\mathrm{SU}_{s+1}(F)$ that differ from the identity only in the first row and last column; here $s \geq 5$ and $|F| > K = K(q)$.

We shall consider only the unwisted case $S = \mathrm{SL}_{s+1}(F)$. If $S = \mathrm{SU}_{s+1}(F)$ the proof proceeds in exactly the same way by consideration of the fixed points of σ on the groups V^i (and there is no need to square $(\overline{h}_j\gamma_j)^{q_j}$).

Now, the group V has a filtration

$$V = V^1 > V^2 > V^3 > 1$$

where $V^2 = \{g \in V \mid g_{12} = g_{s,s+1} = 0\}$ and $V^3 = \{g \in V \mid g_{1j} = g_{i,s+1} = 0 \text{ for } 1 < j < s,\ 2 < i < s+1\}$. Write

$$W_i = \langle \mathbf{1} + e_{1,i+1}F,\ \mathbf{1} + e_{s+1-i,s+1}F \rangle$$

where e_{ij} denotes the matrix with 1 in the (i,j) entry and 0 elsewhere. Each W_i is an orbital subgroup of S and we have

$$V = W_1 \cdot V^2,\ V^2 = W_2 W_3 \dots W_{s-2} \cdot V^3,\ \ V^3 = W_{s-1}.$$

Now let $\gamma_1, \gamma_2, \dots$ be automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and let $q_1, q_2, \dots$ be divisors of q. We have to find elements $h_1, h_2, \dots \in H$ such that

$$V = \prod_{i=1}^{L_1} [V, (\overline{h_i}\gamma_i)^{q_i}].$$

Let $L = L(q)$ be the integer given in Proposition 6.4, and take $L_1 = 2L + L_3$. Applying that proposition to W_1 and to W_{s-1}, and relabelling the γ_i and q_i, we are reduced to showing that there exist $h_1, \dots, h_{L_3} \in H$ such that

$$V^2/V^3 = \prod_{i=1}^{L_3} [V^2/V^3, (\overline{h_i}\gamma_i)^{q_i}]; \tag{11}$$

note that $V^2/V^3 \cong F^{(2(s-3))}$ is a module for $\mathcal{D}\Phi\Gamma$.

Now for any $\lambda_i \in F^*$ we may choose $h_i \in H$ so that the diagonal component of $\overline{h_i}\gamma_i$ is of the form $\mathrm{diag}(\lambda_i^{-1}, *, 1, \dots, 1, *, \lambda_i)$; this acts on V^2/V^3 as multiplication by λ_i. Let ϕ_i denote the field component of γ_i. Provided $L_3 > 2q(2q+1)$, Lemma 7.1 gives elements $\lambda_1, \dots, \lambda_{L_3} \in F^*$ such that the map $f : F^{(L_3)} \to F$ defined by

$$(t_1, t_2, \dots, t_{L_3}) \mapsto \sum_{i=1}^{L_3} (\lambda_i^{\phi_i(1+\phi_i+\dots+\phi_i^{2q_i-1})} t_i^{\phi_i^{2q_i}} - t_i)$$

is surjective. Formula (9), from the previous section, shows that the action of $\sum_i ((\overline{h_i}\gamma_i)^{2q_i} - 1)$ on each root of V^2/V^3 is in fact given by f. Therefore

$$V^2/V^3 = \prod_{i=1}^{L_3} [V^2/V^3, (\overline{h_i}\gamma_i)^{2q_i}],$$

and (11) follows by Lemma 3.2.

This completes the proof of Proposition 6.7, with

$$L_1(q) = 2L(q) + 2q(2q+1) + 1. \qquad \square$$

It remains to prove Proposition 6.5. Let $S = \mathrm{SL}_{r+1}(F)$, where $|F| > K$ and $r \geq 3$, and put $M_2 = 4L(q) + 1$. We are given automorphisms $\gamma_1, \dots, \gamma_{M_2} \in \mathcal{D}\Phi\Gamma$ and divisors $q_1, \dots, q_{M_2}$ of q, and have to find automorphisms $\eta_1, \dots, \eta_{M_2} \in \mathcal{D}$ and elements $u_1, \dots, u_{M_2} \in U$ such that

$$U \subseteq \prod_{i=1}^{M_2} [U, (\overline{u_i}\eta_i\gamma_i)^{q_i}] \tag{12}$$

(here U is the full upper unitriangular group in S). Since we are allowed to adjust γ_i by any element of $\mathcal{D}$, we may without loss of generality assume from now on that each $\gamma_i \in \Phi\Gamma$.

A matrix $g \in U$ will be called *proper* if $g_{i,i+1} \neq 0$ for $1 \leq i \leq r$. Let U_k be the product of all positive root groups of height $\geq k$ (so $u \in U_k$ precisely if $u_{ij} = 0$ for $0 < j - i < k$). It is well known that $U_1 > U_2 > \dots$ is the lower central series of U and that for each $k \leq r-1$ and each proper matrix g the map $x \mapsto [x, g]$ induces a surjective linear map of $\mathbb{F}_p$-vector spaces

$$[-, g] : U_k/U_{k+1} \to U_{k+1}/U_{k+2}. \tag{13}$$

We call the section U_k/U_{k+1} the k^{th} *layer of* U. By a slight abuse of notation, we shall identify $\mathcal{D}$ with the group of diagonal matrices in $\mathrm{GL}_{r+1}(F)$ modulo scalars.

LEMMA 9.1. *Let $q_0 \in \mathbb{N}$ and suppose that $|F| > (q_0+1)^{q_0}$. Then for any $\gamma \in \Phi\Gamma$, there exist $u \in U$ and $\eta \in \mathcal{D}$ such that the matrix*

$$g = (u\eta\gamma)^{q_0}(\eta\gamma)^{-q_0}$$

is proper.

Proof. Let $\gamma \in \Phi\Gamma$ act on the root subgroup $X_r(t)$ of height one as $X_r(t)^\gamma = X_{r^\tau}(t^\psi)$ (here ψ is a field automorphism of F, and τ may be 1).

Case 1: *When $\psi^{q_0} \neq 1$.* Then we can find $\lambda \in F^*$ such that $\lambda \neq \lambda^{\psi^{q_0}}$, and so

$$\mu = \lambda^{1+\psi^{-1}+\dots+\psi^{1-q_0}} \neq 1.$$

Let $h(\lambda)$ be the diagonal automorphism $\mathrm{diag}(1, \lambda^{-1}, \lambda^{-2}, \dots)$, acting on each fundamental root group X_r ($r \in \Pi$) by $t \mapsto \lambda t$. Then $h(\lambda)$ commutes with τ and we have $h(\mu)\gamma^{q_0} = (h(\lambda)\gamma)^{q_0}$.

Now let $v = \prod_{r\in\Pi} X_r(1)$ be the unitriangular matrix with 1's just off the diagonal. Then v is centralized by γ modulo U_2 and $[v, h(\mu)^{-1}]$ is proper. Putting

$$u = [v, h(\lambda)^{-1}],\ \eta = h(\lambda)$$

we have, modulo U_2,

$$(u\eta\gamma)^{q_0} \equiv (h(\lambda)^v\gamma^v)^{q_0} \equiv ((h(\lambda)\gamma)^{q_0})^v \equiv (h(\mu)\gamma^{q_0})^v \equiv [v, h(\mu)^{-1}](\eta\gamma)^{q_0},$$

so that $g \equiv [v, h(\mu)^{-1}]$ is proper as required.

Case 2: *When $\psi^{q_0} = 1$.* Let F_1 be the fixed field of ψ. Then $[F : F_1] \leq q_0$, and so if $|F| > (q_0+1)^{q_0}$ it follows that $|F_1| > q_0 + 1$. Therefore we can choose $\lambda \in F_1$ such that

$$\lambda^{q_0} = \lambda^{1+\psi^{-1}+\dots+\psi^{1-q_0}} \neq 1,$$

and the rest of the proof is as in Case 1. □

To establish (12), we begin by showing that we can obtain the slightly smaller group U_3 as a product of $2L+1$ sets $[U_3, (\overline{u_i}\eta_i\gamma_i)^{q_i}]$.

LEMMA 9.2. *Let $\gamma_0, \gamma_1, \dots, \gamma_{2L} \in \Phi\Gamma$ and let $q_0, \dots, q_{2L}$ be divisors of q. Then there exist $\eta_i \in \mathcal{D}$ $(i = 0, \dots, 2L)$ and $u \in U$ such that*

$$U_3 = \prod_{i=1}^{2L} [U_3, (\eta_i\gamma_i)^{q_i}] \cdot [U_3, (\overline{u}\eta_0\gamma_0)^{q_0}].$$

(So here we have $u_i = 1$ for $i = 1, \dots, 2L$ and $u_0 = u$.)

Proof. First, note that if $\alpha \in \mathrm{Aut}(U)$ and $x, y \in U_k$ then

$$[xy, \alpha] = [x, \alpha][x, \alpha, y][y, \alpha] \equiv [x, \alpha][y, \alpha] \pmod{U_{2k}}. \tag{14}$$

Say $\gamma_i = \phi_i$ or $\phi_i\tau$ where $\phi_i \in \Phi$. Then, by a double application of Lemma 7.1, we can find $\lambda_i \in F^*$, $i = 1, 2, \dots, 2L$, such that *both* of the maps f_+, $f_- : F^{(2L)} \to F$ defined by

$$f_+(\mathbf{t}) = \sum_{i=1}^{2L} \lambda_i^{\phi_i + \phi_i^2 + \cdots + \phi_i^{2q_i}} t_i^{\phi_i^{2q_i}} - t_i,$$

$$f_-(\mathbf{t}) = \sum_{i=1}^{2L} \lambda_i^{-(\phi_i + \phi_i^2 + \cdots + \phi_i^{2q_i})} t_i^{\phi_i^{2q_i}} - t_i$$

are surjective. Indeed, it suffices to ensure that each of the maps

$$\mathbf{t} \mapsto \sum_{i=1}^{L} \lambda_i^{\phi_i + \phi_i^2 + \cdots + \phi_i^{2q_i}} t_i^{\phi_i^{2q_i}} - t_i$$

and

$$\mathbf{t} \mapsto \sum_{i=L+1}^{2L} \lambda_i^{-(\phi_i + \phi_i^2 + \cdots + \phi_i^{2q_i})} t_i^{\phi_i^{2q_i}} - t_i$$

is surjective.

We now take

$$\eta_i = \begin{cases} \mathrm{diag}(\lambda_i, 1, \lambda_i, 1, \dots, \lambda_i, 1) & (s \text{ odd}) \\ \\ \mathrm{diag}(\dots, 1, \lambda_i, 1, \lambda_i, \underline{1}, \lambda_i^{-1}, 1, \lambda_i^{-1}, 1, \dots) & (s \text{ even}), \end{cases}$$

where in the even rank case the underlined unit $\underline{1}$ has the central position $1 + \frac{s}{2}$ on the diagonal of SL_{s+1}.

It is easy to see that if w is a root of *odd* height, then either $X_w(t)^{\eta_i} = X_w(\lambda_i t)$ for all i, or else $X_w(t)^{\eta_i} = X_w(\lambda_i^{-1} t)$ for all i. Moreover, it follows from the definition that $\eta_i^\tau = \eta_i$. Then the surjectivity of f_+ and f_- together

imply that $X_w = \prod_{i=1}^{2L}[X_w, (\eta_i\gamma_i)^{2q_i}]$ for all roots w of odd height. (Note that $\gamma_i^{2q_i}$ stabilizes every root of Σ). Hence when $k \geq 3$ is *odd* we have

$$U_k/U_{k+1} = \prod_{i=1}^{2L}[U_k/U_{k+1}, (\eta_i\gamma_i)^{2q_i}].$$

It follows from Lemma 3.2 that the product $\prod_{i=1}^{2L}[U_3, (\eta_i\gamma_i)^{q_i}]$ covers each odd layer of U_3.

To deal with the even layers we use the map (13). Put $\beta_i = (\eta_i\gamma_i)^{q_i} \in \mathcal{D}\Phi\Gamma$ for each i. Now take $b \in U_3$ and let $k \geq 3$ be odd. Suppose that we have already found $x_i, y \in U_3$ such that

$$b \equiv \prod_{i=1}^{2L}[x_i, \beta_i] \cdot [y, \overline{g}\beta_0] \pmod{U_k},$$

where $g = (u\eta_0\gamma_0)^{q_0}(\eta_0\gamma_0)^{-q_0}$ is the proper matrix provided by Lemma 9.1.

We claim that there exist $x_1', x_2', \ldots, x_{2L}',\ y' \in U_k$ such that

$$b \equiv \prod_{i=1}^{2L}[x_i x_i', \beta_i] \cdot [yy', \overline{g}\beta_0] \pmod{U_{k+2}}. \tag{15}$$

By (14) this is equivalent to

$$\prod_{i=1}^{2L}[x_i', \bar{\beta}_i] \cdot [y', \overline{g}\beta_0] \equiv b' \pmod{U_{k+2}} \tag{16}$$

where $b' = b \cdot (\prod[x_i, \beta_i] \cdot [y, \overline{g}\beta_0])^{-1} \in U_k$. Also,

$$[y', \overline{g}\beta_0] = [y', \beta_0] \cdot [y', g]^{\beta_0}.$$

Let

$$V_1 = \left(U_{k+2} \prod_{\mathrm{ht}(w)=k} X_w\right)/U_{k+2}, \qquad V_2 = \left(U_{k+2} \prod_{\mathrm{ht}(w)=k+1} X_w\right)/U_{k+2}.$$

We identify U_k/U_{k+2} with $V_1 \oplus V_2$. The elementary abelian p-group V_1 corresponds to the (odd) k^{th} layer of U, while V_2 is the (even) $(k+1)^{\text{th}}$ layer.

Now, on the one hand the map $y' \mapsto [y', g]U_{k+2}$ $(y' \in V_1)$ is a surjective linear map from V_1 onto V_2. On the other hand, the argument above shows that the map $\mathbf{x}' \mapsto \prod_{i=1}^{2L}[x_i', \beta_i]U_{k+2}$ $(\mathbf{x}' \in V_1^{(2L)})$ is a surjective linear map from $V_1^{(2L)}$ onto V_1.

We can therefore solve the equation (16) in U_k/U_{k+2} in the following way. Suppose $b' = b_1 + b_2$ with $b_i \in V_i$. First choose $y' \in V_1$ so that $[y', g] = b_2^{\beta_0^{-1}}$ and

observe that $[y', \beta_0] \in V_1$. Consider this y' fixed and then choose appropriate $x_i' \in V_1$ so that

$$\prod_{i=1}^{2L} [x_i', \beta_i] = b_1 - [y', \beta_0].$$

It follows by induction on the odd k, starting with $k = 3$, that we can solve (15) with $k = r + 1$, and as $U_{r+1} = 1$ this establishes the lemma. □

What remains to be done is to obtain the first two layers U_1/U_2 and U_2/U_3. We shall need $2L$ more automorphisms $(\eta_i\gamma_i)^{q_i}$.

The set of roots of height 1 is Π, and we denote by Ξ the set of roots of height 2. We show first how to obtain $\prod_{w\in\Pi} X_w$.

For a choice of $\lambda_i \in F^*$, $i = 1, 2, \dots, L$, put

$$\eta_i = \operatorname{diag}(1, \lambda_i, \lambda_i^2, \lambda_i^3, \dots).$$

For each fundamental root w we then have

$$X_w(t)^{\eta_i} = X_w(\lambda_i t).$$

In particular the restrictions of η_i and η_i^τ to U_1/U_2 are the same. As in the proof of Proposition 6.7, above, we may apply Lemma 7.1 to find $\lambda_i \in F^*$ such that

$$U_1/U_2 \subseteq \prod_{i=1}^{L} [U_1/U_2, (\eta_i\gamma_i)^{2q_i}] \subseteq \prod_{i=1}^{L} [U_1/U_2, (\eta_i\gamma_i)^{q_i}].$$

The analogous result for $\prod_{w\in\Xi} X_w$ is obtained similarly using the diagonal automorphisms

$$\eta_i = \operatorname{diag}(1, 1, \lambda_i, \lambda_i, \lambda_i^2, \lambda_i^2, \dots).$$

As $U = (\prod_{w\in\Pi} X_w) \cdot (\prod_{w\in\Xi} X_w) \cdot U_3$, the last two observations together with Lemma 9.2 complete the proof of Proposition 6.5, with $M_2 = 4L + 1$.

10. The group P

Here we prove Propositions 6.9 and 6.10. Let us recall the setup. S is a quasisimple group of type

$$\mathcal{X} \in \{{}^2A_r,\ B_r,\ C_r,\ D_r,\ {}^2D_r\},$$

with root system Σ (twisted or untwisted). Here r can be any integer greater than 3. There exist fundamental roots $\delta, \delta' \in \Sigma$ (equal unless $\mathcal{X} = D_r$) such that the other fundamental roots $\Pi' = \Pi - \{\delta, \delta'\}$ generate a root system Σ' of type A_s, for the appropriate s: in types ${}^2A_r, B_r, C_r$ and ${}^2D_r$ we take $\delta = \delta'$ to

be the fundamental root of length distinct from the others; in type D_r, $\{\delta, \delta'\}$ is the pair of fundamental roots swapped by the symmetry τ of D_r.

If S is untwisted, set

$$P = \prod_{w \in \Sigma_+ \setminus \Sigma'_+} X_w.$$

If S is twisted, set

$$P = \prod_{\omega^* \in \Sigma_+ \setminus \Sigma'_+} Y_\omega.$$

PROPOSITION 6.9. *Assume that $|F| > K$ and that S is of type B_r, C_r, D_r or ${}^2D_r$. There is a constant $N_1 = N_1(q)$ such that if $\gamma_1, \dots, \gamma_{N_1}$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and $q_1, \dots, q_{N_1}$ are divisors of q then there exist elements $h_1, \dots, h_{N_1} \in H$ such that*

$$P \subseteq \prod_{i=1}^{N_1} [P, (\overline{h_i}\gamma_i)^{q_i}].$$

We consider first the *untwisted* case, where S has type B_r, C_r or D_r. By inspection of the root systems we see that every positive root $w \in \Sigma_+$ can be written as $w = e\delta + w_1 + e'\delta' + w_2$ with some $e, e' \in \{0, 1\}$ and $w_1, w_2 \in \Sigma'_+ \cup \{0\}$. In the last expression we include the possibility $\delta = \delta'$.

For $w = (e\delta + w_1) + (e'\delta' + w_2)$ as above we set $t(w) := e + e'$.

For $i = 1, 2$ let $P(i)$ be the product of roots subgroups X_w with $t(w) \geq i$ in any order; this is in fact a normal subgroup of P. Then $P = P(1)$, and both $P(1)/P(2)$ and $P(2)$ are abelian. Each of $P(1)$ and $P(2)$ is a product of orbital subgroups and so invariant under $\mathcal{D}\Phi\Gamma$.

Recall Lemma 2.1. The type of S is here different from A_n and ${}^2A_n$ and therefore there are characters $\chi_i : \Sigma \to F^*$ $(i = 1, \dots, 4)$ of the root lattice such that (i)

$$\mathcal{D} = \bigcup_{i=1}^{4} h(\chi_i)\overline{H}$$

and (ii)

$$\chi_i(w) = 1 \ \forall w \in \Pi \setminus \Delta$$

where Δ is a fixed set of fundamental roots of size at most 2; if $X = D_r$ then $\Delta = \{\delta, \delta'\}$; otherwise Δ consists of a single root at one end of the Dynkin diagram.

In view of (i), we may assume that the diagonal component d_j of each γ_j is one of the four $h(\chi_i)$ above. Setting $N_1 > 4N_2$ and relabelling the γ_j if necessary we may further suppose that

$$1 \leq j \leq N_2 \Longrightarrow d_j = h(\chi_1) = h_0, \text{ say.}$$

Observe that for any root $w \in \Sigma_+$ the multiplicity of each of $v \in \Delta$ in w is 0, 1 or 2, and the last case occurs only when Δ has size 1. Therefore h_0 can act in only 4 possible different ways on X_w as w ranges over Σ_+. We deduce that a given $\gamma_j^{2q_j}$ can act in at most four different ways on the various root subgroups. (The possible presence of a graph automorphism component of γ_j in case of D_r requires additional attention.) We make this more precise:

Given γ_j for $j = 1, 2, \dots, N_2$, each with diagonal component h_0, for each j there are elements $c_j(i) \in F^*$ $(i = 1, \dots, 4)$ with the following property:

For each root $w \in \Sigma_+$ there exists $i = i(w) \in \{1, 2, 3, 4\}$ such that $\gamma_j^{2q_j}$ acts on X_w as

$$X_w(t) \mapsto X_w(c_j(i)t^{\phi_j^{2q_j}}).$$

Here ϕ_j is the field automorphism component of γ_j.

For any $\lambda \in F^*$ let χ_λ denote the character of Σ which takes value λ^4 on $\{\delta, \delta'\}$ and is 1 on all the other fundamental roots. The automorphism $h_\lambda := h(\chi_\lambda)$ is a fourth power in $\mathcal{D}$ and therefore inner. Observe that if $v \in \Sigma_+ \backslash \Sigma'_+$ then

$$X_v(t)^{h_\lambda} = X_v(\lambda^{4 \cdot t(v)}t),$$

where $t(v) \in \{1, 2\}$ is as defined above.

Let ϕ_j be the field automorphism component of γ_j. The automorphisms $(h_{\lambda_j}\gamma_j)^{2q_j}$ stabilize each root subgroup $X_w \leq P$ and act on $X_w(t)$ as

$$t \mapsto c_j(i)\lambda_j^{4t(w)\cdot(\phi_j + \phi_j^2 + \cdots + \phi_j^{2q_j})} \cdot t^{\phi_j^{2q_j}},$$

where $i = i(w) \in \{1, 2, 3, 4\}$ as above, $t(w) = 2$ if $X_w \leq P(2)$ and $t(w) = 1$ otherwise.

We set $N_2 = N_3 + N_4$. Let $\{1, 2, \dots, N_2\} = J_3 \cup J_4$ where J_3 and J_4 have sizes N_3 and N_4 respectively. set $N_3 = 4M$ and let J_3 be a union of four subsets $J_3(i)$, $i = 1, \dots, 4$ each of size M.

Using Lemma 7.1 with all $c_i = 4$, provided $|F|$ is large compared to q and $M > 2q(8q + 1)$, we may find $\underline{\lambda} \in F^{(J_3)}$ such that the maps

$$\mathbf{t} \in F^{(J_3(i))} \mapsto \sum_{j \in J_3(i)} \left(c_j(i)\lambda_j^{4(\phi_j + \phi_j^2 + \cdots + \phi_j^{2q_j})} \cdot t_j^{\phi_j^{2q_j}} - t_j \right) \tag{17}$$

are surjective for each $i = 1, 2, 3, 4$.

This gives

$$P/P(2) \subseteq \prod_{j \in J_3} [P/P(2), (h_{\lambda_j}\gamma_j)^{2q_j}] \subseteq \prod_{j \in J_3} [P/P(2), (h_{\lambda_j}\gamma_j)^{q_j}]. \tag{18}$$

Similarly, another four-fold application of Lemma 7.1 with $c_i = 8$ gives that for $N_4 > 4 \times 2q(16q+1)$ there exist $\lambda_j \in F^*$ for $j \in J_4$ such that the analogue of (17) holds and hence

$$P(2) \subseteq \prod_{j\in J_4} [P(2), (h_{\lambda_j}\gamma_j)^{2q_j}] \subseteq \prod_{j\in J_4} [P(2), (h_{\lambda_j}\gamma_j)^{q_j}]. \tag{19}$$

This concludes the proof in the untwisted case.

It remains to establish the *twisted* case, where S has type ${}^2D_r$. We will denote by Σ^0 the untwisted root system corresponding to Σ.

The group $P = P^*$ inherits a filtration $P = P^*(1) > P^*(2)$ from the associated untwisted root system D_r: each $P^*(i)$ is the fixed point set of σ on the corresponding group $P(i)$ defined as above for the untwisted version of S; the subgroup $P^*(i)$ is the product of all root subgroups Y_ω with equivalence class ω consisting of untwisted roots w with $t(w) \le i$. Recall that in type ${}^2D_r$ the root subgroups Y_ω are all one-parameter.

The group $P^*(2)$ is the product of the root subgroups Y_ω defined by a singleton $\omega = \{w\}$ where the positive root $w \in \Sigma^0$ is fixed by τ. Then $Y_\omega = \{X_w(t) \mid t \in F_0\}$.

On the other hand the group $P^*/P^*(2)$ is the product of $Y_\omega P^*(2)$ where $\omega = \{u, v\} \subseteq \Sigma^0_+$ has type $A_1 \times A_1$ and $Y_\omega(t) = X_u(t)X_v(t^\phi)$ is parametrized by $t \in F$.

We now proceed as in the previous case:

By Lemma 2.1 we may take $N_1 > 4N_2$ and may assume that the automorphisms γ_j all have the same diagonal component h_0 for $j = 1, 2, \dots, N_2$.

There are elements $c_j(i) \in F^*$, $(1 \le j \le N_2,\ i = 1, 2, 3, 4)$, depending on h_0, such that the automorphism $\gamma_j^{q_j}$ acts on a root element $Y_\omega(t)$ as $t \mapsto c_j(i)t^{\phi_j^{q_j}}$, where $i = i(\omega) \in \{1, 2, 3, 4\}$ depends only on ω.

Let $\{a, b\}$ be the pair of fundamental roots in Σ^0 corresponding to the short root $\delta \in \Sigma$. For $\lambda \in F^*$ let χ_λ be the character of the untwisted root system Σ^0 defined by $\chi(a) = \lambda^4$, $\chi(b) = \lambda^{4\phi}$ and χ is 1 on the rest of the fundamental roots of Σ^0.

Define $h_\lambda := h(\chi)$. Then h_λ is an inner diagonal automorphism and is fixed by σ; therefore $h_\lambda \in \overline{H}$. If ϕ_j is the field component of γ_j then $(h_{\lambda_j}\gamma_j)^{q_j}$ acts on $Y_\omega(t)$ as

$$t \mapsto c_j(i)\lambda_j^{c_\omega(\phi_j + \cdots + \phi_j^{q_j})} t^{\phi_j^{q_j}},$$

where $c_j(i)$ and $i = i(\omega)$ are as above, and

- $c_\omega = 4 + 4\phi$ if ω has type A_1 (when t ranges over F_0),
- $c_\omega = 4$ if ω has type $A_1 \times A_1$ (when t ranges over F).

We set $N_2 = N_3 + N_4$. In the same way as in the previous case, provided N_3, N_4 and $|F_0|$ are sufficiently large compared to q, it is possible to choose $\lambda_j \in F^*$ for $j = 1, 2, \dots, N_3$ and $\lambda_j \in F_0^*$ for $N_3 < j \leq N_4$ so that the appropriate equivalents of (17) hold. This gives (18) and (19) and concludes the proof in the case of type ${}^2D_r$.

PROPOSITION 6.10. *Assume that $|F| > K$ and that S is of type ${}^2A_r$. There is a constant $N_1' = N_1'(q)$ such that if $\gamma_1, \dots, \gamma_{N_1'}$ are automorphisms of S lying in $\mathcal{D}\Phi\Gamma$ and $q_1, \dots, q_{N_1'}$ are divisors of q then there exist automorphisms $\eta_1, \dots, \eta_{N_1'} \in \mathcal{D}$ such that*

$$P \subseteq \prod_{i=1}^{N_1'} [P, (\eta_i \gamma_i)^{q_i}].$$

The proof is along lines similar to the above; as we are aiming for a slightly weaker conclusion, we may assume from the start that each $\gamma_j \in \Phi$.

If r is odd then all the root subgroups Y_ω of P are one-parameter, P is abelian and we set $P(2) = P$.

If r is even then define $P(2)$ to be the product of all the *one parameter* root subgroups Y_ω of P together with the $r/2$ groups

$$B_\omega := \{X_w(a \cdot t_0) \mid \quad t_0 \in F_0\},$$

where w is the root fixed by τ in an equivalence class $\omega \subseteq \Sigma_+^0$ of type A_2 and a is a fixed solution to $a + a^\phi = 0$.

Both $P(2)$ and $P/P(2)$ are abelian groups and modules for $\mathcal{D}\Phi$.

We first deal with the group $P/P(2)$. It is nontrivial only if r is even. Then $P/P(2)$ is a product of its subgroups of the form

$$\{A_\omega(t) := X_v(t) \cdot X_u(t^\phi) P(2)/P(2) \mid \quad t \in F\},$$

where the untwisted roots v and $u = v^\tau$ span a root system $\omega = \{u, v, u + v\}$ of type A_2 in Σ_+^0.

For $\lambda \in F_0^*$ let η_λ be the inner diagonal automorphism of S induced by $\mathrm{diag}(\lambda^{-1}, \dots, \lambda^{-1}, 1, \lambda, \dots, \lambda)$. (The unit coefficient is in the middle position $r/2 + 1$ on the diagonal.) Then $(\eta_\lambda \gamma_j)^{q_j}$ acts on each $A_\omega(t) \leq P/P(2)$ by

$$t \mapsto \lambda^{\gamma_j + \dots + \gamma_j^{q_j}} \cdot t^{\gamma_j^{q_j}}.$$

Lemma 7.1, part (b), gives that there is a choice of $(\lambda_1, \dots, \lambda_{N_2'}) \in F_0^{(N_2')}$, provided $N_2' > 2q(2q+1)$, such that the map

$$\mathbf{t} \in F^{(N_2')} \mapsto \sum_{j=1}^{N_2'} \left(\lambda_j^{\gamma_j + \dots + \gamma_j^{q_j}} \cdot t_j^{\gamma_j^{q_j}} - t_j \right)$$

is surjective onto F. This gives (in case r is even)

$$P/P(2) = \prod_{j=1}^{N_2'} [P/P(2), (\eta_{\lambda_j}\gamma_j)^{q_j}]. \tag{20}$$

The abelian group $P(2)$ requires a little more attention since the range of the parameter is sometimes F and sometimes F_0. More precisely $P(2)$ is a product of groups of the following three types:

Type 1: $Y_\omega(t_0) = X_w(t_0)$ where $\omega = \{w\}$ is a singleton equivalence class of untwisted roots and t_0 ranges over F_0 (this type occurs only in case r is odd).

Type 2: $B_\omega = \{X_w(a \cdot t) \mid t \in F_0\}$, $w = v + u = w^\tau$ and v, u span a root system ω of type A_2 (which happens only for r even).

Type 3: $Y_\omega(t) = X_v(t)X_u(t^\phi)$ where $\{u, v\}$ is an equivalence class of untwisted roots ω of type $A_1 \times A_1$ and t ranges over F.

Now, for $\lambda_j \in F_0$ let η_{λ_j} be the diagonal automorphism of S defined above (with the unit coefficient omitted when r is odd). Thus η_{λ_j} acts on the parameter t (or t_0) above as multiplication by λ_j^2.

For $N_3', N_4' \in \mathbb{N}$ let J_i, $i = 3, 4$ denote two consecutive intervals of integers of lengths N_i' each.

Provided N_i' is sufficiently big compared to q, then according to Lemma 7.1 it is possible to find $\lambda_j \in F_0^{J_i}$ such that the following two maps are surjective:

$$f_3 : F_0^{J_3} \longrightarrow F_0 \quad \mathbf{t} \mapsto \sum_{j \in J_1} \left(\lambda_j^{2(\gamma_j + \cdots + \gamma_j^{q_j})} \cdot t_j^{\gamma_j^{q_j}} - t_j \right)$$

$$f_4 : F^{J_4} \longrightarrow F \quad \mathbf{t} \mapsto \sum_{j \in J_4} \left(\lambda_j^{2(\gamma_j + \cdots + \gamma_j^{q_j})} \cdot t_j^{\gamma_j^{q_j}} - t_j \right)$$

(Note that we need part (b) of Lemma 7.1 for f_4.)

This implies that for $J = J_3 \cup J_4$ we have

$$P(2) = \prod_{j \in J} [P(2), (\eta_{\lambda_j}\gamma_j)^{q_j}].$$

Together with (20) this gives the result if we take $N_1' > N_2' + N_3' + N_4'$.

New College, Oxford OX1 3BN, United Kingdom
E-mail address: nikolay.nikolov@new.ox.ac.uk

All Souls College, Oxford OX1 4AL, United Kingdom
E-mail address: dan.segal@all-souls.ox.ac.uk

References

[A] M. Aschbacher, *Finite Group Theory*, *Cambridge Studies Adv. Math.* **10**, Cambridge Univ. Press, Cambridge, 1986.

[AG] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.

[C] R. W. Carter, *Simple groups of Lie Type*, *Pure Appl. Math.* **28**, John Wiley and Sons, New York, 1972.

[At] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, U.K., 1985.

[G] D. Gorenstein, *Finite Simple Groups*, Plenum Press, New York, 1982.

[GLS] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups* 3, AMS *Mathematical Surveys and Monographs* **40**, A.M.S., Providence, RI, 1998.

[H] Y. O. Hamidoune, An application of connectivity theory in graphs to factorization of elements in groups, *European J. Combin.* **2** (1981), 349–355.

[LP] M. W. Liebeck and L. Pyber, Finite linear groups and bounded generation, *Duke Math. J.* **107** (2001), 159–171.

[LS1] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.***12** (1999), 497–520.

[LS2] ———, Diameters of finite simple groups: sharp bounds and applications, *Ann. of Math.* **154** (2001), 383–406.

[MZ] C. Martinez and E. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469–479.

[N] N. Nikolov, A product decomposition for the classical quasisimple groups, *J. Group Theory*, to appear.

[NS] N. Nikolov and D. Segal, On finitely generated profinite groups, I: Strong completeness and uniform bounds, *Ann. of Math.* **165** (2007), 171–238.

[SW] J. Saxl and J. S. Wilson, A note on powers in simple groups, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 91–94.

[St] R. Steinberg, Lectures on Chevalley groups, Yale University Mathematics Dept., 1968.

[W] J. S Wilson, On simple pseudofinite groups. *J. London Math. Soc.* **51** (1995), 471–490.

(Received August 28, 2003)