J. Eur. Math. Soc. 16, 597–618 © European Mathematical Society 2014
DOI 10.4171/JEMS/441

Nikolay Nikolov · Dan Segal

On normal subgroups of compact groups

Received February 7, 2012 and in revised form August 16, 2012

Abstract. Among compact Hausdorff groups G whose maximal profinite quotient is finitely generated, we characterize those that possess a proper dense normal subgroup. We also prove that the abstract commutator subgroup $[H, G]$ is closed for every closed normal subgroup H of G.

Keywords. Compact groups, dense normal subgroups, closed normal subgroups, conjugacy width

0. Introduction

Let G be a compact Hausdorff topological group with identity component G^0, so G^0 is a connected compact group and G/G^0 is the maximal profinite quotient of G. We say that G is of *f.g. type* if G/G^0 is (topologically) finitely generated. In [NS2] we established a number of results about groups of this type, including

Theorem 0.1. *The* (*abstract*) *derived group* $G' = [G, G]$ *is closed in* G.

Theorem 0.2. *G has a virtually-dense normal subgroup of infinite index if and only if G has an open normal subgroup G_1 such that* either *G_1 has infinite abelianization* or *G_1 has a strictly infinite semisimple quotient.*

(A *strictly infinite semisimple group* is a Cartesian product of infinitely many finite simple groups or compact connected simple Lie groups). The purpose of this note is (1) to generalize Theorem 0.1, and (2) to characterize the compact groups of f.g. type that possess a *dense* proper normal subgroup (which must then have infinite index, by the main result of [NS1]); this analogue to Theorem 0.2 is a little technical to state: see Theorem 2.1 in Section 2 below.

Here and throughout, *simple* group is taken to mean *non-abelian* simple group.

1. Commutators

1.1. The main result

Theorem 1.1. *Let G be a compact Hausdorff group of f.g. type and H a closed normal subgroup of G. Then the* (*abstract*) *commutator subgroup* $[H, G]$ *is closed in* G.

N. Nikolov: Mathematical Institute, Oxford OX2 6GG, UK; e-mail: nikolov@maths.ox.ac.uk
D. Segal: All Souls College, Oxford OX1 4AL, UK; e-mail: dan.segal@all-souls.ox.ac.uk

Mathematics Subject Classification (2010): Primary 22C05; Secondary 20E18

When G is profinite, this is Theorem 1.4 of [NS1]; when G is connected, it may be deduced quite easily from known results (cf. [HM, Theorem 9.24]). The general case, however, seems harder: to prove it we have to beef up slightly the main technical result of [NS2]; the beefed-up version appears as Proposition 1.4 below.

Now let G and H be as in Theorem 1.1. For a subset $\mathcal{X}$ of G we let $\overline{\mathcal{X}}$ denote the closure of $\mathcal{X}$ in G, and for $f \in \mathbb{N}$ write

$$\mathcal{X}^{*f} = \{x_1 \dots x_f \mid x_1, \dots, x_f \in \mathcal{X}\}.$$

The minimal size of a finite topological generating set for G (if there is one) is denoted $\mathrm{d}(G)$.

First reduction. Let $\mathcal{N}$ denote the set of closed normal subgroups N of G such that G/N is a Lie group. Set

$$\mathcal{X} = \{[h, g] \mid h \in H,\ g \in G\}. \tag{1}$$

Then $\mathcal{X}$ is a compact set, so $\mathcal{X}^{*f}$ is closed for each finite f. Suppose that for some f we have

$$[H, G]N = \mathcal{X}^{*f} N \ \forall N \in \mathcal{N}.$$

Then

$$[H, G] \subseteq \bigcap_{N \in \mathcal{N}} \mathcal{X}^{*f} N = \overline{\mathcal{X}^{*f}} = \mathcal{X}^{*f} \subseteq [H, G]$$

(cf. [HM, Lemma 9.1]), so $[H, G]$ is closed.

Thus it will suffice to prove

Theorem 1.2. *Let G be a compact Lie group and H a closed normal subgroup of G. Then*

$$[H, G] = \mathcal{X}^{*f}$$

where $\mathcal{X}$ is given by (1) and f depends only on $\mathrm{d}(G/G^0)$.

Second reduction. We assume now that G is a compact Lie group, with $\mathrm{d}(G/G^0) = d$. Then G/G^0 is finite and $G = G^0\Gamma$ for some finite subgroup $\Gamma = \langle g_1, \dots, g_{2d}\rangle$ where $g_{2i} = g_{2i-1}^{-1}$ for each i; also $G^0 = ZS$ where $Z = \mathrm{Z}(G^0)$ and S is connected semisimple (cf. [HM, Theorems 6.36, 6.15, 6.18]).

Put $H_1 = HZ \cap S$, $H_2 = H_1^0$. Then H_2 is connected semisimple, so every element of H_2 is a commutator ([HM, Cor. 6.56]); it follows that $H_2 \subseteq \mathcal{X}$. So replacing G by G/H_2 we may suppose that H_1 is finite, which implies that $H_1 \leq Z$ since H_1 is normal in S and S is connected. Then $H_3 := H \cap G^0 \leq ZH_1 = Z$.

As H_3 is abelian we have

$$[H_3, G] = [H_3, \Gamma] = \prod_{i=1}^{d} [H_3, g_{2i}] \subseteq \mathcal{X}^{*d},$$

and $\mathcal{X}^{*d}$ is closed; so replacing G by $G/\overline{[H_3, G]}$ we may suppose that $H_3 \leq \mathrm{Z}(G)$.

Let $x \in H$ and $y \in G^0$. Then $x^n \in H_3$ where $n = |G : G^0|$, and there exists $v \in G^0$ such that $y = v^n$ (every element of G^0 is an nth power, because it lies in a torus: see [HM, Theorem 9.32]). Now

$$1 = [x^n, v] = [x, v]^n = [x, v^n] = [x, y].$$

Thus $G^0 \leq \mathrm{C}_G(H)$.

Put $D = H\Gamma \cap G^0$. Then $H\Gamma = D\Gamma$. Since $H\Gamma/H_3$ is finite, we have $H_3 \geq (H\Gamma)^0 = H^0 := H_4$. There exists a finite subgroup L of $H\Gamma$ such that $H\Gamma = H_4L$ ([HM, Theorem 6.74]). Then $L \lhd H\Gamma$ (since $H_4 \leq \mathrm{Z}(G)$) and $\Delta := L \cap H \lhd G^0\Gamma = G$ since $[H, G^0] = 1$. Moreover $H = H_4\Delta$; and $[H, G] = [\Delta, G]$.

Applying [HM, Theorem 6.74] to the group G/Δ, we find a finite subgroup Q/Δ of G/Δ such that $G = G^0Q$ and $Q/\Delta \cap (G/\Delta)^0 \leq \mathrm{Z}((G/\Delta)^0)$, hence $Q \cap G^0\Delta \lhd G$. Then $Q \cap G^0$ is central in G^0. Replacing each g_i by an element of $G^0g_i \cap Q$, we may suppose that $\Gamma \leq Q$. Now putting

$$E = \Delta\Gamma \leq Q \quad \text{and} \quad A = E \cap G^0 \leq \mathrm{Z}(G^0),$$

we have

$$E = \Delta\Gamma = A\Gamma, \quad [A, A\Delta] = [A \cap \Delta, E] = 1, \quad [H, G] = [\Delta, \Gamma] = [\Delta, E].$$

Conclusion of the proof. In the following subsection we establish

Theorem 1.3. *Let G be a finite group, H a normal subgroup of G and $\{y_1, \dots, y_r\}$ a symmetric subset of G. Suppose that $G = H\langle y_1, \dots, y_r\rangle = A\langle y_1, \dots, y_r\rangle$ where A is an abelian normal subgroup of G with $[A, H] = 1$. Then*

$$[H, G] = \Big(\prod_{i=1}^{r}[H, y_i]\Big)^{*f_1} \quad \textit{where } f_1 = f_1(r).$$

Applying this with E, Δ in place of G, H we obtain

$$[H, G] = [\Delta, E] = \Big(\prod_{i=1}^{2d}[\Delta, g_i]\Big)^{*f_1(2d)}.$$

Taking account of all the reductions, we see that Theorem 1.2 follows, with

$$f = 1 + d + 2df_1(2d).$$

1.2. A variant of the 'Key Theorem'

Theorem 1.3 depends on the following proposition. We recall some notation from [NS2]; throughout this subsection, G will be a finite group.

Notation. For $\mathbf{g}, \mathbf{v} \in G^{(m)}$ and $1 \leq j \leq m$,

$$\tau_j(\mathbf{g}, \mathbf{v}) = v_j[g_{j-1}, v_{j-1}]\dots[g_1, v_1], \quad \mathbf{v} \cdot \mathbf{g} = (v_1g_1, \dots, v_mg_m), \quad \mathbf{c}(\mathbf{v}, \mathbf{g}) = \prod_{j=1}^{m}[v_j, g_j].$$

Proposition 1.4. *There exists a function $k : \mathbb{N} \to \mathbb{N}$ with the following property. Let G be a finite group, $H = [H, G]$ a soluble normal subgroup of G, and $C \le \mathrm{C}_G(H)$ a normal subgroup of G. Suppose that $G = C\langle g_1, \ldots, g_r\rangle$. Put $m = r \cdot k(r)$, and for $1 \le j < k(r)$ and $1 \le i \le r$ set*

$$g_{i+jr} = g_i.$$

Then for each $h \in H$ there exist $\mathbf{v}(i) \in H^{(m)}$ $(i = 1, 2, 3)$ such that

$$h = \prod_{i=1}^{3} \mathbf{c}(\mathbf{v}(i), \mathbf{g}) \tag{2}$$

and

$$C\langle g_1^{\tau_1(\mathbf{g},\mathbf{v}(i))}, \ldots, g_m^{\tau_m(\mathbf{g},\mathbf{v}(i))}\rangle = G \quad \textit{for } i = 1, 2, 3. \tag{3}$$

In fact we can take

$$k(r) = 1 + 4(r + 1) \cdot \max\{r, 7\}. \tag{4}$$

This reduces to (a special case of) Theorem 3.10 of [NS2] when $C = 1$. The latter can be beefed up in a similar way in the general case where H is not necessarily soluble; as this will not be needed here, we leave it for the interested reader to fill in the details. The ingredients of the proof (in both cases) are all taken from [NS2, Section 3], though they need to be arranged in a different way.

A normal subgroup N of a group G is said to be *quasi-minimal normal* if N is minimal subject to

$$1 < N = [N, G].$$

Let $Z = Z_N$ be a normal subgroup of G maximal subject to $Z < N$. Then $[Z,_n G] = [[[Z, G], G], \ldots, G] = 1$ for some n, which implies that (i) $Z = N \cap \zeta_\omega(G)$ is uniquely determined, and (ii) $[Z, N] \le [Z, H] \le [Z, G_\omega] = 1$. (Here $\zeta_\omega(G)$ denotes the hypercentre and G_ω the nilpotent residual of G; if G is finite, G_ω is the last term of the lower central series of G and $[\zeta_\omega(G), G_\omega] = 1$.) An elementary argument (cf. [NS2, Lemma 3.4]) shows that Z is contained in the Frattini subgroup $\Phi(G)$ of G. If N is soluble then $\overline{N} = N/Z$ is an abelian chief factor of G.

We fix $k = k(r)$ as given by (4). Fix $h \in H$. For $S \lhd G$ let us say that $\mathbf{v} = (v(i)_j) \in H^{(3m)}$ satisfies E(S), resp. G(S) if (2), resp. (3) is true modulo S. By hypothesis, E(H) and G(H) are satisfied by $\mathbf{v} = (1, \ldots, 1)$.

Since $H = [H, G]$ there is a chain

$$H = H_0 > H_1 \ge \cdots \ge H_z = 1$$

such that H_{i-1}/H_i is a quasi-minimal normal subgroup of G/H_i for $i = 1, \ldots, z$. Fix $l < z$ and suppose that $\mathbf{u} \in H^{(3m)}$ satisfies E(H_l) and G(H_l). Our aim is to find elements $\mathbf{a}(i) \in {H_l}^{(m)}$ such that $\mathbf{v} = \mathbf{a} \cdot \mathbf{u}$ satisfies E(H_{l+1}) and G(H_{l+1}). If we can do this, the proposition will follow by induction.

To simplify notation we now replace G by G/H_{l+1}. Put $N = H_l$, now a soluble quasi-minimal normal subgroup of G, and set $Z = Z_N$.

The argument is done in three steps. Put $K_1 = N$, $K_2 = N'[Z, G]$, $K_3 = [Z, G]$, $K_4 = 1$. We assume that $\mathbf{u}$ satisfies E(N) and G(N). Fix $q \leq 3$ and suppose that $\mathbf{u}$ satisfies E(K_q) and G(K_q); we will find $\mathbf{a}(i) \in N^{(m)}$ such that $\mathbf{v} = \mathbf{a} \cdot \mathbf{u}$ satisfies E(K_{q+1}) and G(K_{q+1}). Again, to simplify notation we may replace G by G/K_{q+1} and so assume that $K_{q+1} = 1$, and set $K = K_q$. Thus we have to show that (2) and (3) hold.

Lemma 1.5.

$$\Big(\prod_{i=1}^{3} \mathbf{c}(\mathbf{a}(i)\cdot\mathbf{u}(i),\mathbf{g})\Big)\Big(\prod_{i=1}^{3}\mathbf{c}(\mathbf{u}(i),\mathbf{g})\Big)^{-1} = \prod_{i=1}^{3}\Big(\prod_{j=1}^{m}[a(i)_j, g_j]^{\tau_j(\mathbf{g},\mathbf{u}(i))}\Big)^{w(i)}$$

where $w(i) = \mathbf{c}(\mathbf{u}(i-1),\mathbf{g})^{-1}\ldots\mathbf{c}(\mathbf{u}(1),\mathbf{g})^{-1}$.

This is a direct calculation. The next lemma is easily verified by induction on m (see [NS1], Lemma 4.5):

Lemma 1.6.

$$\langle g_j^{\tau_j(\mathbf{g},\mathbf{u})} \mid j = 1,\ldots,m\rangle = \langle g_j^{u_j h_j} \mid j = 1,\ldots,m\rangle$$

where $h_j = g_{j-1}^{-1}\ldots g_1^{-1}$.

Now we are given $\mathbf{u}(i) \in H^{(m)}$ and $\kappa \in K$ such that

$$h = \kappa \prod_{i=1}^{3}\mathbf{c}(\mathbf{u}(i),\mathbf{g})$$

and

$$G = CK\langle g_j^{\tau_j(\mathbf{g},\mathbf{u}(i))} \mid j = 1,\ldots,m\rangle = CK\langle g_j^{u(i)_j h_j} \mid j = 1,\ldots,m\rangle \quad \text{for } i = 1,2,3, \tag{5}$$

the second equality thanks to Lemma 1.6.

Let $\mathbf{v} = \mathbf{a}\cdot\mathbf{u}$ with $\mathbf{a}(i) \in N^{(m)}$; the goal is to find a suitable $\mathbf{a}$. Lemma 1.5 shows that (2) is then equivalent to

$$\prod_{i=1}^{3}\Big(\prod_{j=1}^{m}[a(i)_j, g_j]^{\tau_j(\mathbf{g},\mathbf{u}(i))}\Big)^{w(i)} = \kappa. \tag{6}$$

This can be further simplified by setting

$$\begin{aligned} y(i)_j &= g_j^{\tau_j(\mathbf{g},\mathbf{u}(i))w(i)}, & t(i)_j &= g_j^{u(i)_j h_j},\\ b(i)_j &= a(i)_j^{\tau_j(\mathbf{g},\mathbf{u}(i))w(i)}, & c(i)_j &= a(i)_j^{u(i)_j h_j}. \end{aligned} \tag{7}$$

Define $\phi(i) : N^{(m)} \to N$ by

$$\mathbf{b}\phi(i) = \mathbf{c}(\mathbf{b},\mathbf{y}(i)), \quad \mathbf{b} \in N^{(m)}. \tag{8}$$

Then (6) becomes

$$\prod_{i=1}^{3}\mathbf{b}(i)\phi(i) = \kappa, \tag{9}$$

and (5) is equivalent to

$$G = CK\langle y(i)_1, \dots, y(i)_m\rangle = CK\langle t(i)_1, \dots, t(i)_m\rangle \quad \text{for } i = 1, 2, 3. \tag{10}$$

Similarly, by Lemma 1.5 again, (3) holds if and only if for $i = 1, 2, 3$ we have

$$G = CZ\langle t(i)_j^{c(i)_j} \mid j = 1, \dots, m\rangle \tag{11}$$

(where Z is added harmlessly since $Z \leq \Phi(G)$).

Let $\mathcal{X}(i)$ denote the set of all $\mathbf{c}(i) \in N^{(m)}$ such that (11) holds, and write $W(i)$ for the image of $\mathcal{X}(i)$ under the bijection $N^{(m)} \to N^{(m)}$ defined in (7) sending $\mathbf{c}(i) \mapsto \mathbf{b}(i)$.

To sum up: to establish the existence of $\mathbf{a}(1), \mathbf{a}(2), \mathbf{a}(3) \in N^{(m)}$ such that the $\mathbf{v}(i) = \mathbf{a}(i) \cdot \mathbf{u}(i)$ satisfy (2) and (3), it suffices to find $(\mathbf{b}(1), \mathbf{b}(2), \mathbf{b}(3)) \in W(1) \times W(2) \times W(3)$ such that (9) holds.

We set $\varepsilon = \min\{1/7, 1/r\}$, and will write $^{-} : G \to G/Z$ for the quotient map.

The case $q = 1$. In this case we have $K = N$ and we are assuming that $K_2 = N'[Z, G] = 1$. We use additive notation for N and consider it as a G-module. Note that $[CK, N] = 1$. Then (10) together with $N = [N, G]$ implies that

$$\phi(1) : \mathbf{b} \mapsto \sum_{j=1}^{m} b_j(y(1)_j - 1)$$

is a surjective ($\mathbb{Z}$-module) homomorphism $N^{(m)} \to N$. It follows that

$$|\phi(1)^{-1}(c)| = |\ker \phi(1)| = |N|^{m-1}$$

for each $c \in N$.

Now fix $i \in \{1, 2, 3\}$. According to Theorem 2.1 of [NS2], at least one of the elements g_j has the $\varepsilon/2$-fixed-point space property on $\overline{N}$ (see [NS2, Section 2.1]); therefore at least k of the elements $\overline{t(i)_j}$ have this property. Now we apply [NS2, Proposition 2.8(i)] to the group G/CZ: if $N \nleq CZ$ this shows that (11) holds for at least $|\overline{N}|^m(1-|\overline{N}|^{r-k\varepsilon/2})$ values of $\overline{\mathbf{c}(i)}$ in $|\overline{N}|^m$. If $N \leq CZ$ the same holds trivially for *all* $\overline{\mathbf{c}(i)}$ in $|\overline{N}|^m$. It follows in any case that

$$|W(i)| = |\mathcal{X}(i)| \geq |Z|^m \cdot |\overline{N}|^m(1 - |\overline{N}|^{r-k\varepsilon/2}) = |N|^m(1 - |\overline{N}|^{r-k\varepsilon/2}). \tag{12}$$

We need to compare $|\overline{N}|$ with $|N|$. Observe that $\mathbf{b} \mapsto \sum_{j=1}^{r} b_j(g_j - 1)$ induces an epimorphism from $\overline{N}^{(r)}$ onto N; consequently, $|N| \leq |\overline{N}|^r$. Thus since $k\varepsilon/2r > 1$ we have

$$|W(i)| \geq |N|^m(1 - |N|^{1-k\varepsilon/2r}) > 0,$$

so $W(i)$ is non-empty for each i. For $i = 2, 3$ choose $\mathbf{b}(i) \in W(i)$ and put

$$c = \kappa\Big(\prod_{i=2}^{3} \mathbf{b}(i)\phi(i)\Big)^{-1}.$$

Then

$$|\phi(1)^{-1}(c)| + |W(1)| \geq |N|^m(|N|^{-1} + 1 - |N|^{1-k\varepsilon/2r}) > |N|^m$$

since $k\varepsilon/2r > 2$. It follows that $\phi(1)^{-1}(c) \cap W(1)$ is non-empty. Thus we may choose $\mathbf{b}(1) \in \phi(1)^{-1}(c) \cap W(1)$ and ensure that (9) is satisfied.

The case $q = 2$. Now we take $K = N'$, assuming that $K_3 = [Z, G] = 1$. Since $N' \leq Z$, the argument above again gives (12).

The maps $\phi(i)$ are no longer homomorphisms, however. Below we establish

Proposition 1.7. *Let N be a soluble quasi-minimal normal subgroup and C a normal subgroup of the finite group G, with $[C, N] = 1$. Assume that $G = C\langle y(i)_1, \ldots, y(i)_m\rangle$ for $i = 1, 2, 3$. Then for each $c \in N'$ there exist $c_1, c_2, c_3 \in N$ such that $c = c_1c_2c_3$ and*

$$|\phi(i)^{-1}(c_i)| \geq |N|^m \cdot |\overline{N}|^{-r-2} \quad (i = 1, 2, 3), \tag{13}$$

where $\phi(i)$ is given by (8) and $r = \mathrm{d}(G/C)$.

Since now $K \leq Z$, the hypotheses of Proposition 1.7 follow from (10). Put $c = \kappa$ and choose c_1, c_2, c_3 as in the proposition. As $k\varepsilon > 4r + 4$, we see that (12) and (13) together imply that $\phi(i)^{-1}(c_i) \cap W(i)$ is non-empty for $i = 1, 2, 3$. Thus we can find $\mathbf{b}(i) \in \phi(i)^{-1}(c_i) \cap W(i)$ for $i = 1, 2, 3$ to obtain (9).

The case $q = 3$. Now we take $K = [Z, G]$. Since $G = C\langle g_1, \ldots, g_r\rangle$, we have $K = \prod_{j=1}^r [Z, g_j]$. Thus $\kappa = \prod_{j=1}^r [z_j, g_j]$ with $z_1, \ldots, z_r \in Z$. In this case, (9) is satisfied if we set

$$\begin{aligned} b(1)_j &= z_j \quad && (1 \leq j \leq r), \\ b(1)_j &= 1 && (r < j \leq m), \\ b(i)_j &= 1 && (i = 2, 3,\ 1 \leq j \leq m), \end{aligned}$$

because $y(i)_j$ is conjugate to g_j under the action of H and $[Z, H] = 1$.

For each i we have $W(i) \supseteq Z^{(m)}$, since in this case (10) implies (11) if $c(i)_j \in Z$ for all j. So $\mathbf{b}(i) \in W(i)$ for each i, as required.

This concludes the proof of Proposition 1.4, modulo

Proof of Proposition 1.7. Now N is a quasi-minimal normal subgroup of $G = C\langle g_1, \ldots, g_r\rangle$. Recall the definition of Z_N as a normal subgroup of G maximal subject to $Z < N$; we saw that Z_N is in fact uniquely determined. Put $\Gamma = N\langle g_1, \ldots, g_r\rangle$. Let $g_0 \in N \setminus Z_N$. Since $[C, N] = 1$ we have $N = \langle g_0^G\rangle = \langle g_0^{\langle g_1,\ldots,g_r\rangle}\rangle$ and so $\Gamma = \langle g_1, \ldots, g_r, g_0\rangle$; thus $d(\Gamma) \leq r + 1$. For each i and j we have $y(i)_j = c_{ij}x_{ij}$ with $c_{ij} \in C$ and $x_{ij} \in \Gamma$. Then for $i = 1, 2, 3$ we have

$$\Gamma = (\Gamma \cap C)\langle x_{i1}, \ldots, x_{im}\rangle = \langle x_{i1}, \ldots, x_{im}, x_{i,m+1}, \ldots, x_{im'}\rangle$$

where $m' = m + r + 1$ and $x_{ij} \in C$ for $m < j \leq m'$.

Define $\psi(i) : N^{(m')} \to N$ by

$$\mathbf{b}\psi(i) = \prod_{j=1}^{m'} [b_j, x_{ij}].$$

We apply Proposition 7.1 of [NS1] to the group Γ and its soluble quasi-minimal normal subgroup N. This shows that for each $c \in N'$ there exist $c_1, c_2, c_3 \in N$ such that $c = c_1c_2c_3$ and

$$|\psi(i)^{-1}(c_i)| \geq |N|^{m'} \cdot |\overline{N}|^{-r-2} \qquad (i = 1, 2, 3).$$

Now

$$(b_1, \ldots, b_{m'})\psi(i) = (b_1, \ldots, b_m)\phi(i)$$

for each $\mathbf{b} \in N^{(m')}$; so

$$\psi(i)^{-1}(c_i) = \phi(i)^{-1}(c_i) \times N^{(r+1)}$$

and it follows that

$$|\phi(i)^{-1}(c_i)| = |\psi(i)^{-1}(c_i)| \cdot |N|^{-(r+1)} \geq |N|^m \cdot |\overline{N}|^{-r-2}$$

as required.

This completes the proof.

Proof of Theorem 1.3. Now G is a finite group, H is a normal subgroup of G and $\{y_1, \ldots, y_r\}$ is a symmetric subset of G. We are given that $G = H\langle y_1, \ldots, y_r\rangle = A\langle y_1, \ldots, y_r\rangle$ where A is an abelian normal subgroup of G with $[A, H] = 1$. The claim is that

$$[H, G] = \Big(\prod_{i=1}^{r} [H, y_i]\Big)^{*f_1}$$

where $f_1 = f_1(r)$.

Put $\Gamma = \langle y_1, \ldots, y_r\rangle$, so $G = H\Gamma = A\Gamma$. Choose n so that $[H,_n G] = K$ satisfies $K = [K, G]$. By [S, Proposition 1.2.5] we have

$$[H, G] = \prod_{i=1}^{r} [H, y_i] \cdot K.$$

Put $G_1 = K\Gamma$ and $A_1 = A \cap G_1$. Then $G_1 = A_1\Gamma$ and $K = [K, \Gamma] = [K, G_1]$. So replacing H by K, G by G_1 and A by A_1 we reduce to the case where $H = [H, G]$. This implies in particular that

$$G = H\Gamma = G'\Gamma = G'\langle y_1, \ldots, y_r\rangle.$$

Now $AH \cap \Gamma$ is centralized by A and normalized by Γ, so $AH \cap \Gamma \lhd G$. But $AH = A(AH \cap \Gamma)$ so

$$H' = (AH)' = (AH \cap \Gamma)' \leq \Gamma.$$

Theorem 1.2 of [NS2] gives

$$[H', G] = [H', \Gamma] = \Big(\prod_{i=1}^{r}[H', y_i]\Big)^{*f_0(r)}$$

(where $f_0(r)$ depends only on r). Replacing G by $G/[H', G]$, we reduce to the case where $H' \leq \mathrm{Z}(G)$. Thus $H = [H, G]$ is nilpotent. It follows by Proposition 1.4 that

$$H = \Big(\prod_{i=1}^{r}[H, y_i]\Big)^{*3k(r)}.$$

Putting everything together we can take

$$f_1 = 1 + f_0(r) + 3k(r).$$

(The alert reader may wonder how we could establish the hard result Theorem 1.3 using only a version of the easier, 'soluble' case of the 'Key Theorem' from [NS2]; the answer is that the full strength of the latter is implicitly invoked at the point where we quote [NS2, Theorem 1.2].)

2. Dense normal subgroups

2.1. The main result

Definition. (a) Let S be a finite simple group. Then $Q(S)$ denotes the following subgroup of $\mathrm{Aut}(S)$:

$\mathrm{PGO}_{2n}^{+}(q)$	if $S = D_n(q),\ n \geq 5$,
$\mathrm{PGO}_{2n}^{-}(q)$	if $S = {}^2D_n(q)$,
$\mathrm{Inn}(S)$	if $S = C_n(q)$,
$\mathrm{InnDiag}(S)$	if S is of another Lie type,
$\mathrm{Aut}(S)$	in all other cases.

Note that when $S = D_n(q)$ then $Q(S) = \mathrm{PGO}_{2n}^{+}(q) = \mathrm{PSO}_{2n}^{+}(q)\langle\tau\rangle$ and when $S = {}^2D_n(q)$ then $Q(S) = \mathrm{PGO}_{2n}^{-}(q) = \mathrm{PSO}_{2n}^{-}(q)\langle[q]\rangle$, where τ is the non-trivial graph automorphism of $D_n(q)$ and $[q]$ denotes the field automorphism of order 2 of ${}^2D_n(q)$.

(b) Let S be a connected compact simple Lie group. Then

$$Q(S) = \begin{cases} \mathrm{Aut}(S) & \text{if } S = \mathrm{PSO}(2n),\ n \geq 3, \\ \mathrm{Inn}(S) & \text{else.} \end{cases}$$

(c) A compact topological group H is *Q-almost-simple* if $S \lhd H \leq Q(S)$ where S is a finite simple group or a compact connected simple Lie group with trivial centre (and S is identified with $\mathrm{Inn}(S)$). Note that if H is not finite, then H is Q-almost-simple if and only if it is either simple or else isomorphic to $\mathrm{Aut}(\mathrm{PSO}(2n))$ for some $n \geq 3$, because $|\mathrm{Aut}(S)/\mathrm{Inn}(S)| = 2$ for $S = \mathrm{PSO}(2n)$.

If H is Q-almost-simple as above, the *rank* of H is defined to be the (untwisted) Lie rank of S if S is of Lie type, n if $S \cong \mathrm{Alt}(n)$, and zero otherwise.

Theorem 2.1. *Let G be a compact Hausdorff group of f.g. type. Then G has a proper dense normal subgroup if and only if one of the following holds:*

- *G has an infinite abelian quotient,* or
- *G has a strictly infinite semisimple quotient,* or
- *G has Q-almost-simple quotients of unbounded ranks.*

(The quotients here refer to G as a *topological* group, i.e. they are continuous quotients—in the first case this makes no difference, in view of Theorem 0.1.)

2.2. The profinite case

Let G be an infinite finitely generated profinite group. It is clear that in each of the following cases, G has a *countable*, hence proper, dense normal subgroup:

- G is abelian (because G contains a dense (abstractly) finitely generated subgroup),
- G is semisimple (G is the Cartesian product of infinitely many finite simple groups, and the restricted direct product is a dense normal subgroup).

Let G_2 denote the intersection of all maximal open normal subgroups of G not containing G'; thus

$$G_{\text{ss}} := G/G_2$$

is the maximal semisimple quotient of G. The preceding observations imply:

- G has a proper dense normal subgroup if either $G^{\text{ab}} := G/G'$ or G_{ss} is infinite

(recall that G' is closed, so G/G' is again profinite, by Theorem 0.1).

We recall a definition and a result from [NS2, Section 1]:

Definition. G_0 denotes the intersection of the centralizers of all simple non-abelian chief factors of G (here by 'chief factor' of G we mean a chief factor of some G/K where K is an open normal subgroup of G).

Proposition 2.2 ([NS2, Corollary 1.8]). *Let N be a normal subgroup of* (*the underlying abstract group*) *G. If $NG' = NG_0 = G$ then $N = G$.*

Now let $\mathcal{X}$ denote the class of all finitely generated profinite groups H such that $H_0 = 1$ and both H^{ab} and H_{ss} are finite, and let $\mathcal{X}(\text{dns})$ denote the subclass consisting of those groups that contain a proper dense normal subgroup.

Lemma 2.3. *Let G be a finitely generated profinite group. Then G contains a proper dense normal subgroup if and only if at least one of the following holds:*

(a) *G^{ab} is infinite,*
(b) *G_{ss} is infinite,*
(c) $G/G_0 \in \mathcal{X}(\text{dns})$.

Proof. We have shown above that G contains a proper dense normal subgroup if either (a) or (b) holds, and the same clearly follows in case (c). Suppose conversely that none of (a), (b) or (c) holds. Then $G/G_0 \in \mathcal{X} \setminus \mathcal{X}(\mathrm{dns})$. Now let N be a dense normal subgroup of G. Since G^{ab} is finite, G' is open in G and so $NG' = G$. As G/G_0 has no proper dense normal subgroup, we also have $NG_0 = G$. Now Proposition 2.2 shows that $N = G$. □

Thus it remains to identify the groups in $\mathcal{X}(\mathrm{dns})$.

For any chief factor S of G let $\mathrm{Aut}_G(S)$ denote the image of G in $\mathrm{Aut}(S)$, where G acts by conjugation. Now we can state

Proposition 2.4. *Let $G \in \mathcal{X}$. Then $G \in \mathcal{X}(\mathrm{dns})$ if and only if the simple chief factors S of G such that*

$$\mathrm{Aut}_G(S) \leq Q(S) \tag{14}$$

have unbounded ranks.

Since $\mathrm{Aut}_G(S)$ is a Q-almost-simple image of G for such chief factor S, this will complete the proof of Theorem 2.1 in the case of a profinite group G.

Proposition 2.4 depends on the following four lemmas, which will be sketched in the next subsection:

Lemma 2.5. *There exists $\varepsilon_* > 0$ such that*

$$\log |[S, f]| \geq \varepsilon_* \log |S|$$

whenever S is a finite simple group and $f \in \mathrm{Aut}(S) \setminus Q(S)$.

Lemma 2.6. *If S is a finite simple group of rank at most r and $1 \neq f \in \mathrm{Aut}(S)$ then*

$$\log |[S, f]| \geq \varepsilon(r) \log |S|,$$

where $\varepsilon(r) > 0$ depends only on r.

Lemma 2.7. *Given $\varepsilon > 0$, there exists $k(\varepsilon) \in \mathbb{N}$ with the following property: if S is a finite simple group and $f \in \mathrm{Aut}(S)$ satisfies $\log |[S, f]| \geq \varepsilon \log |S|$ then*

$$S = ([S, f][S, f^{-1}])^{*k(\varepsilon)}.$$

Lemma 2.8. *For every $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that if S is a finite simple group of rank at least n and $f \in Q(S)$, then there exists $s \in S$ such that*

$$\log |[S, sf]| < \varepsilon \log |S|.$$

Proof of Proposition 2.4. Now G^{ab} and G_{ss} are finite, and $G_0 = 1$. This implies that G has a semisimple closed normal subgroup $T = \overline{G^{(3)}}$, and the simple factors of T are precisely the simple chief factors of G (here $\overline{G^{(3)}}$ denotes the closure of the third term of the derived series of G; see [NS2, Section 1.1]). Thus $T = T_0 \times T_1 \times T_2$ where T_0 is the product of those simple factors S such that $G = S\mathrm{C}_G(S)$, T_1 is the product of those

$S \not\leq T_0$ for which (14) holds, and T_2 is the product of the rest. Note that T_0 is finite, because $T_0 \cong G_{\mathrm{ss}}$. We fix a finite set $\{a_1, \ldots, a_d\}$ of (topological) generators for G.

Suppose that T_1 contains factors of unbounded ranks. Pick a sequence (S_j) of simple factors of T_1 such that $\mathrm{rank}(S_j) \to \infty$ and let $T_3 = \prod_{j\in\mathbb{N}} S_j$. Then $T = T_3 \times T_4$ for a suitable complement T_4. If G/T_4 has a proper dense normal subgroup then so does G; so replacing G by G/T_4 we may assume that $T = T_3$.

In view of Lemma 2.8, we can find $s_{ij} \in S_j$ such that

$$\frac{\log |[S_j, s_{ij}a_i]|}{\log |S_j|} < \varepsilon_j$$

for all i and j, where $\varepsilon_j \to 0$ as $j \to \infty$. For each i put

$$b_i = (s_{ij}) \cdot a_i \in T a_i,$$

and note that $[S_j, s_{ij}a_i] = [S_j, b_i]$. Let $N = \langle b_1^G, \ldots, b_d^G\rangle$ be the normal subgroup of G generated (algebraically) by $b_1, \ldots, b_d$.

Since $\mathrm{Aut}_G(S_j) \neq \mathrm{Inn}(S_j)$, for each j there exists i such that $[S_j, b_i] \neq 1$, and so $1 \neq [S_j, N] \leq S_j \cap N$. As each S_j is simple it follows that N contains the (restricted) direct product $P = \langle S_j \mid j \in \mathbb{N}\rangle$. Therefore $\overline{N} \geq \overline{P} = T$, and as $a_i \in TN$ for each i it follows that N is dense in G.

On the other hand, $N \neq G$. To see this, fix i and j, set $b = b_i$, $S = S_j$, and write $\dagger = \dagger_j : G \to \mathrm{Aut}_G(S)$ for the natural map. Then $|G^\dagger| \leq |\mathrm{Aut}(S)| \leq |S|^{1+\eta_j}$ where $\eta_j \to 0$ as $j \to \infty$, because $\mathrm{rank}(S_j) \to \infty$ (see [GLS, Section 2.5]). So

$$|(b^G)^\dagger| = |[G^\dagger, b^\dagger]| \leq |G^\dagger : S^\dagger|\, |[S^\dagger, b^\dagger]| \leq |S|^{\eta_j} \cdot |[S, b]| \leq |S|^{\eta_j+\varepsilon_j}.$$

Now for $n \in \mathbb{N}$ set $X_n = (b_1^G \cup (b_1^{-1})^G \cup \cdots \cup b_d^G \cup (b_d^{-1})^G)^{*n}$. Then

$$|X_n^\dagger| \leq (2d|S|^{\eta_j+\varepsilon_j})^n < |S_j| = |S_j^\dagger|$$

if $|S_j| > (2d)^{2n}$ and $\eta_j + \varepsilon_j < (2n)^{-1}$. This holds for all sufficiently large values of j; thus we may choose a strictly increasing sequence $(j(n))$ and for each n an element $x_{j(n)} \in S_{j(n)}$ such that

$$x_{j(n)}^{\dagger_{j(n)}} \notin X_n^{\dagger_{j(n)}}.$$

Let $t \in T_1$ have $x_{j(n)}$ as its $S_{j(n)}$-component for each n. Then $t^{\dagger_{j(n)}} = x_{j(n)}^{\dagger_{j(n)}} \notin X_n^{\dagger_{j(n)}}$ for every n, and so

$$t \notin \bigcup_{n=1}^{\infty} X_n = N;$$

hence $N \neq G$ as claimed.

For the converse, suppose that every simple factor of T_1 has rank at most r. Let N be a dense normal subgroup of G. Then $NT = G$ by Lemma 2.3, since $(G/T)_0 = G/T$.

Let $a_1, \ldots, a_d$ be as above and choose $c_i \in a_i T \cap N$. For each simple factor S of T_2, there exists i such that conjugation by c_i induces on S an automorphism not in $Q(S)$. Then Lemmas 2.7 and 2.5 show that

$$S = ([S, c_i][S, c_i^{-1}])^{*k(\varepsilon_*)}.$$

It follows that

$$T_2 = \Big(\prod_{i=1}^{d}[T, c_i][T, c_i^{-1}]\Big)^{*k(\varepsilon_*)} \subseteq N.$$

For each simple factor S of T_1, there exists i such that conjugation by c_i does not centralize S. Since each such S has rank at most r, we see in the same way, now using Lemmas 2.7 and 2.6, that

$$T_1 = \Big(\prod_{i=1}^{d}[T, c_i][T, c_i^{-1}]\Big)^{*k(\varepsilon(r))} \subseteq N.$$

We conclude that

$$|G : N| = |T : T \cap N| \leq |T : T_1 T_2| = |T_0| < \infty.$$

Therefore N is open in G by [NS1, Theorem 1.1] (= [NS2, Theorem 5.1]), and so $N = G$.

2.3. Some lemmas

Proof of Lemma 2.7. S is a simple group and $f \in \mathrm{Aut}(S)$ satisfies $\log|[S, f]| \geq \varepsilon \log|S|$. Put $Y = [S, f]^S$ and $X = [S, f][S, f^{-1}]$. Then $Y^{*k(\varepsilon)} = S$ by [LS2, Proposition 1.23], where $k(\varepsilon) = \lceil c'/\varepsilon \rceil$; and $X \supseteq Y$ by [NS2, Lemma 3.5].

Proof of Lemma 2.6. S is a simple group of rank at most r and $1 \neq f \in \mathrm{Aut}(S)$. Then $C = \mathrm{C}_S(f)$ is a proper subgroup of S, and the main result of [BCP] implies that $|S : C| \geq |S|^{\varepsilon(r)}$ where $\varepsilon(r) > 0$ depends only on r. It follows that $|[S, f]| = |S : C| \geq |S|^{\varepsilon(r)}$.

Proof of Lemma 2.8. We are given a simple group S and $f \in Q(S)$. We have to show that if $\mathrm{rank}(S)$ is large enough then there exists $s \in S$ such that $\log|[S, sf]| < \varepsilon \log|S|$ (we will not distinguish between s and the inner automorphism it induces).

If S is a large alternating group, we can choose s so that sf is either 1 or (conjugation by) a transposition, and the claim is clear.

Otherwise, we may assume that S is a classical group of dimension n over a field of size q. Note that when S is an orthogonal group then $\mathrm{PGO}_n^{\epsilon}(q)/\mathrm{PSO}_n^{\epsilon}(q)$ is generated by a single reflection if q is odd and is trivial if q is even (or n is odd). At the same time $\mathrm{PSO}_n^{\epsilon}(q)/\mathrm{Inn}(S)$ is generated by a product of two reflections if q is odd and is generated by a transvection if q is even (see [GLS, Section 2.7]; $\epsilon \in \{\pm 1\}$). In all cases, there exists $s \in S$ such that $sf = h$, where h is an automorphism of S such that h is a product of at most three reflections/transvections in case when S is an orthogonal group or else h is a diagonal element with $n-1$ eigenvalues equal to 1 in case S is $\mathrm{PSU}_n(q)$ or $\mathrm{PSL}_n(q)$. In each case, $\log|C_S(h)|/\log|S| \to 1$ as $\mathrm{rank}(S) \to \infty$ uniformly in q. Lemma 2.8 follows.

Proof of Lemma 2.5. Now S is a simple group and $f \in \mathrm{Aut}(S) \smallsetminus Q(S)$. This implies that S is of Lie type, and in view of Lemma 2.6 we may assume that S is a classical group of large rank. We have to show that $\log |\mathrm{C}_S(f)|/\log |S| \leq 1 - \varepsilon_*$ where $\varepsilon_* > 0$.

Case I: $f \in \mathrm{InnDiag}(S)$. This can only happen when S is an orthogonal group in even dimension or a symplectic group and q is odd. In both cases the description of $\mathrm{Inndiag}(S)$ of [GLS, Section 2.7] for the classical groups and the definition of $Q(S)$ show that f is a similarity, i.e. there is some $\lambda \in \mathbb{F}_q^*$ with $(f(v), f(v)) = \lambda(v, v)$ for all $v \in V$, the natural module for S. Here $(\cdot, \cdot)$ is the natural bilinear form on V. Moreover λ is not a square in $\mathbb{F}_q^*$, for if $\lambda = \mu^2$ then $\mu^{-1} f = f \in \mathrm{PGO}_{2n}^{\pm}(q) = Q(S)$, a contradiction. We shall call f a *proper* similarity if $\lambda \notin (\mathbb{F}_q^*)^2$. By considering an appropriate odd power of f we may assume that f is a semisimple element of $\mathrm{GL}(V)$. Let t be the maximal multiplicity of some eigenvalue of f over the algebraic closure of V. We claim that $t \leq (\dim V)/2$. For if $t > (\dim V)/2$ then t belongs to some rational eigenvalue $\mu \in \mathbb{F}_q^*$ and there is some element v of the μ-eigenspace of f with $(v, v) \neq 0$ (because the maximal dimension of totally isotropic subspaces of V is $(\dim V)/2$). But then $\lambda(v, v) = (f(v), f(v)) = \mu^2(v, v)$, a contradiction since λ is non-square. This establishes the claim. Now Lemma 3.4(ii) of [LS1] shows that

$$|f^S| > c' q^{(\dim V - t)(\dim V)/2} > c' q^{(\dim V)^2/4}$$

for some constant $c' > 0$. This means that $\log |\mathrm{C}_S(f)|/ \log |S|$ is bounded away from 1.

Case II: $f \notin \mathrm{InnDiag}(S)$.

(a) Assume first that either

- S is untwisted and f does not involve a graph automorphism, or else
- S is twisted and f has order at least 3 modulo $\mathrm{InnDiag}(S)$.

We follow the methods of [NS2, Subsection 4.1.5]. Let L be the adjoint simple algebraic group with a Steinberg morphism F such that S is the socle of L_F. Then $L_F = \mathrm{InnDiag}(S)$ by [GLS, Lemma 2.5.8(a) and Theorem 2.2.6(e)]. We may write f as $f = \phi g$ where $g \in \mathrm{InnDiag}(S)$ and ϕ is a field automorphism of order $m \geq 2$ ($m \geq 3$ if S is twisted). We have $F = \phi^m$ if S is untwisted, $F^2 = \phi^m$ if S is twisted. Since L is connected, Lang's theorem implies that there is some $g_0 \in L$ such that $g = g_0^{\phi} g_0^{-1}$. Let $x \in L$. The following conditions on x are equivalent:

(i) $x \in S$ and x is fixed by ϕg,
(ii) $y := x^{g_0}$ is fixed by ϕ and $x = y^{g_0^{-1}}$ is fixed by F.

Ignoring the second part of (ii) we see that $|C_S(f)| \leq |L_\phi|$. Now $\log |L_\phi| \sim \dim L \log |K_\phi|$ where K_ϕ is the fixed field of ϕ. On the other hand if $S = L_F$ is untwisted then $\log |S| \sim \dim L \log |K_F|$ where K_F is the fixed field of $F = \phi^m$, while if S is twisted then $\log |S| \sim \dim L \log |K_{F^2}|/2$, where K_{F^2} is the fixed field of $F^2 = \phi^m$. We conclude that $\log |L_\phi| \sim (a/m) \log |S|$ where $a = 1$ if S is untwisted and $a = 2$ otherwise. In both cases $|C_S(F)| \leq |S|^{2/3}$.

The remaining cases are:

(b) $S = A_n(q)$ and $f = g\phi\tau$ for an element $g \in \mathrm{GL}_{n+1}(q)$, a field automorphism ϕ and a graph automorphism τ.
(c) $S = {}^2A_n(q)$ and $f = g[q]$ for $g \in \mathrm{U}_{n+1}(q)$. Here $[q]$ denotes the automorphism of U_{n+1} induced by the field automorphism $x \mapsto x^q$.
(d) $S = D_n(q)$ and $f = g\phi\tau$ with $g \in \mathrm{InnDiag}(S)$, where either the field automorphism ϕ is non-trivial or $g \in \mathrm{InnDiag}(S) \setminus \mathrm{PSO}_n(q)$ is a proper similarity.
(e) $S = {}^2D_n(q)$ with $f = g[q]$ where $g \in \mathrm{InnDiag}(S) \setminus \mathrm{PSO}_n(q)$ is a proper similarity.

We consider these in turn.

Case (b). Here τ is conjugate to the involution $x \mapsto (x^T)^{-1}$ in GL_{n+1}. Thus we may assume that $f(x) = g^{-1}(x^T)^{-\phi}g$ for a matrix $g \in \mathrm{GL}_{n+1}$. Put $V = \mathbb{F}_q^{n+1}$, the natural module for S of column vectors. The condition $f(x) = x$ is equivalent to $(x^\phi)^T gx = g$, which is equivalent to the requirement that x preserve the non-degenerate form $B : V \times V \to \mathbb{F}_q$ defined by $B(v, w) = (v^\phi)^T gw$. Now the result will follow from

Lemma 2.9. *Let V be an m-dimensional vector space over a finite field F, let ϕ be an automorphism of F, and let B be a form on V which is non-degenerate and such that $B(\alpha v, \beta w) = \alpha^\phi \beta B(v, w)$ for any $\alpha, \beta \in F$. Then the subgroup G_B of elements $x \in \mathrm{GL}(V)$ that preserve B has size at most $|F|^{m(m+1)/2}$.*

We omit the proof, an exercise in linear algebra. Note that Lemma 2.9 estimates the fixed points of f in $\mathrm{SL}_{n+1}(q)$ which is the universal cover $\tilde{S}$ of S. The trivial bound $|[S, f]| \geq |[\tilde{S}, f]|\,|\mathrm{Z}(\tilde{S})|^{-1}$ together with $\log |\mathrm{Z}(\tilde{S})|/\log |S| \to 0$ as $\mathrm{rank}(S) \to \infty$ then completes the proof of case (b).

Case (c). The argument here also follows the idea in [NS2, Subsection 4.1.5]. Let X be the algebraic group GL_{n+1}. Let $[q]$ be the morphism $x \mapsto x^{[q]}$ of X and let F be the Frobenius morphism $x \mapsto x^{\tau[q]}$ whose fixed point set on SL_{n+1} is the universal cover $\tilde{S} = \mathrm{SU}_{n+1}(q)$ of S. By Lang's theorem we can write $g = g_0^{[q]} g_0^{-1}$ for some $g_0 \in X$. Since g is fixed by F, the element $h := g_0^{-F} g_0$ is fixed by $[q]$, i.e. $h \in \mathrm{GL}_{n+1}(q)$. Let $x \in \mathrm{SL}_{n+1}$. The following two conditions on x are equivalent:

(i) $x \in \tilde{S}$ and x is fixed by $[q]g$,
(ii) $y := x^{g_0} \in \mathrm{SL}_{n+1}$ is fixed by $[q]$ and $x = y^{g_0^{-1}}$ is fixed by F.

Therefore the number of fixed points of $[q]g$ on $\tilde{S}$ is equal to the number of elements $y \in \mathrm{SL}_{n+1}(q)$ such that

$$(y^{g_0^{-1}})^F = x^F = x = (y^F)^{g_0^{-F}} = y^{g_0^{-1}},$$

equivalently

$$(y^F)^{(g_0^{-F} g_0)} = y.$$

Observing that for $y \in \mathrm{SL}_{n+1}(q)$ we have $y^F = y^\tau$, the last condition becomes $y^{\tau h} = y$. By Case (a) the number of such y is at most $q^{(n+1)n/2}$, which is about $|\tilde{S}|^{1/2}$. We have proved that $|[\tilde{S}, f]| \geq |\tilde{S}|^{1/2-o(1)}$; the corresponding result for $|[S, f]|$ follows just as in case (b).

Case (d). Let U be the fixed point subgroup of the graph automorphism τ in $S = D_n(q)$. Then $U = B_{n-1}(q)$ and $\log|U|/\log|S| \to 1$ as $n \to \infty$. Hence it is enough to prove that $\log|\mathrm{C}_S(f) \cap U|/\log|S| \leq 1 - \varepsilon$ for some fixed $\varepsilon > 0$. Now $\mathrm{C}_S(f) \cap U$ is contained in the fixed point set of $g\phi$ on S, which has size at most $|S|^{1-\epsilon}$ by Case II (a) if $\phi \neq 1$ and by Case I otherwise.

Case (e). This is similar to Case (d) on putting $U = \mathrm{C}_S([q]) \cong B_{n-1}(q)$, noting that $\log|U|/\log|S| \to 1$ as $n \to \infty$, and applying Case I to $\mathrm{C}_S(g)$.

2.4. *The general case*

Assume now that G is a compact group with G/G^0 finitely generated. We will show that G has a proper dense normal subgroup—say G has DNS—if and only if one of the following holds:

(a) G^{ab} is infinite,
(b) G has a strictly infinite semisimple quotient,
(c) G has Q-almost-simple quotients of unbounded ranks.

Suppose that G is infinite and abelian. Then either G maps onto an infinite finitely generated abelian profinite group, or G^0 has finite index in G. In the first case, G has DNS by a remark in Subsection 2.2; in the second case, G maps onto a non-trivial torus ([HM, Proposition 8.15]), hence onto $\mathbb{R}/\mathbb{Z}$: then the inverse image of $\mathbb{Q}/\mathbb{Z}$ is a dense proper subgroup of G. Thus in general, if (a) holds then G has DNS. If (b) holds, a dense normal subgroup is provided by the inverse image in G of the restricted direct product of simple factors in a strictly infinite semisimple quotient of G.

Suppose that (c) holds but neither (a) nor (b) does. If G has Q-almost-simple *finite* quotients of unbounded ranks then so does G/G^0, and then G has DNS by Subsection 2.2. Otherwise, there exists a strictly increasing sequence (n_i) (with $n_1 \geq 3$) such that G maps onto each $\mathrm{Aut}(S_i)$ where $S_i \cong \mathrm{PSO}(2n_i)$ for each i. Then for each i, the inverse image D_i in G of $\mathrm{Inn}(S_i)$ has index 2. Since G has only finitely many open subgroups of index 2, we can replace (n_i) with an infinite subsequence and reduce to the case where $D_i = D$ is constant. Then G has closed normal subgroups $N_i < D$ such that $D/N_i \cong S_i$ and G/N_i induces $\mathrm{Aut}(D/N_i)$ on D/N_i; replacing G by a quotient we may assume that $\bigcap_{i=1}^{\infty} N_i = 1$.

Then $D = \prod_i S_i$ where $S_i = \bigcap_{j \neq i} N_j \cong \mathrm{PSO}(2n_i)$. Also $G = D\langle y \rangle$ where $y^2 \in D$ and y acts on S_i like $s_i\tau_i$, where $s_i \in S_i = \mathrm{Inn}(S_i)$ and τ_i is the non-trivial graph automorphism of S_i given by conjugation by the diagonal matrix $\mathrm{diag}(1, 1, \ldots, 1, -1) \in \mathrm{O}(2n)$.

Let $\tau = (s_i^{-1})_{i \in \mathbb{N}} \cdot y \in Dy$. Then τ induces τ_i on each S_i and $\tau^2 \in \mathrm{C}_G(D) = 1$. Put $N = \langle \tau^G \rangle$. Then for each i we have $S_i \cap N \supseteq [S_i, \tau] \neq 1$, so $S_i \cap \overline{N}$ is a non-trivial closed normal subgroup of S_i and hence $S_i \leq \overline{N}$. Therefore $D \leq \overline{N}$ and it follows that $\overline{N} = G$.

We claim that $N \neq G$. To see this, observe that $\dim(S_i) = 2n^2 - n$ while $\dim(\mathrm{C}_{S_i}(\tau_i)) = \dim(\mathrm{O}(2n-1)) = 2(n-1)^2 - n + 1$; therefore

$$\frac{\dim [S_i, \tau_i]}{\dim(S_i)} \to 0 \quad \text{as } i \to \infty.$$

This implies that for each m there exist $i(m) \in \mathbb{N}$ and $s_{i(m)} \in S_{i(m)} \setminus [S_{i(m)}, \tau]^{*m}$, and we may choose $i(m) > i(m-1)$ for each $m > 1$. Now let $h \in D$ be such that $h_{i(m)} = s_{i(m)}$ for all m. We claim that $h \notin N$.

Indeed, suppose that

$$w = \prod_{j=1}^{m} \tau^{g_j} \in D,$$

where without loss of generality $g_j = (g_{j,i})_i \in D$. Then m is even and

$$w_i = [x_1, \tau][x_2^\tau, \tau] \ldots [x_{m-1}, \tau][x_m^\tau, \tau] \in [S_i, \tau]^{*m}$$

where $x_j = g_{j,i}$. Therefore $w_{i(m)} \neq h_{i(m)}$, so $h \neq w$.

Thus N is a proper dense normal subgroup of G.

For the converse, let N be a proper dense normal subgroup of G, and assume that neither (a) nor (b) holds; we will show that (c) must hold.

1. If $G^0 N < G$ we are done by the profinite case. So we may assume that $G^0 N = G$.

2. Let $Z = \mathrm{Z}(G^0)$. Suppose that $NZ = G$. Then $G' \leq N$; but we have assumed that G^{ab} is finite, so N has finite index in G, hence contains G^0, whence $N = G$, a contradiction. Therefore $NZ < G$, and replacing N by NZ we may assume that $Z \leq N$. Now replacing G by G/Z we may suppose that $Z = 1$. In this case we have

$$G^0 = \prod_{i \in I} S_i$$

where each S_i is a compact connected simple (and centreless) Lie group.

3. Put $D = G^0 \cap N$. Then $[G^0, N] \leq D < G^0$. It follows that

$$G^0 = G^{0\prime} \leq [G^0, G] = [G^0, \overline{N}] \leq \overline{D},$$

so D is dense in G^0. Suppose that $S_i \nleq D$ for some i. As S_i is abstractly simple, we have $S_i \cap D = 1$, whence $D \leq \mathrm{C}_{G^0}(S_i)$, a proper closed subgroup of G^0. It follows that $S_i \leq D$ for every i. Since $D < \overline{D}$ this implies that the index set I must be infinite.

Since G/G^0 is finitely generated, we have $G = G^0 \overline{\langle y_1, \ldots, y_d \rangle}$ for some $y_l \in N$. Then $[G^0, y_l] \subseteq D$ for each l. Applying [NS2, Proposition 5.18] we deduce that there exists an infinite subset J of I such that each y_l normalizes S_i for every $i \in J$. As $\mathrm{N}_G(S_i)$ is closed and contains G^0, it follows that S_i is normal in G for every $i \in J$. We may take $J = \{i \in I \mid S_i \lhd G\}$.

Put $P = \prod_{i \in J} S_i$ and $C = \mathrm{C}_G(P)$. Suppose that $CN = G$. Then

$$P = P' \leq [P, G] = [P, N] \leq N.$$

Now apply the preceding argument to G/P: since $(G/P)^0 = (\prod_{i \in I \setminus J} S_i)P/P$, this implies that G normalizes S_j for infinitely many $j \in I \setminus J$, which contradicts the definition of J.

It follows that $CN < G$. So replacing N by CN and then replacing G by G/C, we may assume that $C = 1$. As $C \cap G^0 = \prod_{i \in I \setminus J} S_i$, this means in particular that $S_i \lhd G$ for all $i \in I$ (renaming J to I), and that $\mathrm{C}_G(G^0) = 1$.

Now $\mathrm{Out}(S_i)$ embeds in Sym(3) for each i. As G/G^0 is a finitely generated profinite group, it admits only finitely many continuous homomorphisms to Sym(3), so G has an open normal subgroup $H \geq G^0$ such that H induces inner automorphisms on each S_i. Then $H = \mathrm{C}_H(G^0)G^0 = G^0$; thus G/G^0 is finite. Hence there exists a finite subset Y of N such that $G = G^0 Y$.

4. Put $C_i = \mathrm{C}_G(S_i)$ and now set $J = \{i \in I \mid C_i S_i = G\}$. For $i \in J$ put $K_i = \bigcap_{i \neq j \in J} C_j$ and $X = \bigcap_{i \in J} C_i$. Then for $i \in J$ we have

$$S_i \cong XS_i/X \lhd K_i/X \cong G/C_i \cong S_i,$$

so $K_i = X \times S_i$. Hence the image of G/X in the product $\prod_{i \in J} G/C_i \cong \prod_{i \in J} S_i$ contains the restricted direct product, and it follows that $G/X \cong \prod_{i \in J} S_i$. Since we have assumed that G has no strictly infinite semisimple quotient, it follows that J is finite.

As $S_i \leq D$ for each i, we may now replace G by $G/\prod_{i \in J} S_i$, and so assume that J is empty. Then for each i there exists $y(i) \in Y$ such that $y(i)$ induces an outer automorphism on S_i.

5. In the next subsection we will prove

Proposition 2.10. *Let S be a compact connected simple and centreless Lie group and y an outer automorphism of S. Then*

$$S = ([S, y] \cdot [S, y^{-1}])^{*k}$$

where

$$k = k_0 \quad \text{if } S \ncong \mathrm{PSO}(2n)\ \forall n,$$
$$k \leq k(n) \quad \text{if } S \cong \mathrm{PSO}(2n),$$

$k_0 \in \mathbb{N}$ is an absolute constant and $k(n) \in \mathbb{N}$ depends on n.

Now let $t \geq 3$ and let

$$J(t) = \{i \in I \mid S_i \ncong \mathrm{PSO}(2n)\ \forall n > t\}.$$

Put $k(t) = \max\{k_0,\ k(n)\ (n \leq t)\}$. Then for each $i \in J(t)$ we have

$$S_i = \prod_{y \in Y} ([S_i, y] \cdot [S_i, y^{-1}])^{*k(t)}.$$

Therefore

$$\prod_{i \in J(t)} S_i = \prod_{y \in Y} \Big(\Big[\prod_{i \in J(t)} S_i, y \Big] \cdot \Big[\prod_{i \in J(t)} S_i, y^{-1} \Big] \Big)^{*k(t)} \subseteq N,$$

since the product in the middle is a closed set. As $N < G = G^0 N$ it follows that $\prod_{i \in J(t)} S_i < G^0$; thus $J(t) \neq I$.

Thus for every t there exist $n > t$ and $i \in I$ such that $S_i \cong \mathrm{PSO}(2n)$, and then G has the Q-almost-simple quotient $G/C_i \cong \mathrm{Aut}(\mathrm{PSO}(2n))$. Thus (c) holds.

2.5. More lemmas

Throughout this section, we take S to be a compact connected simple Lie group (see for example [H, Table IV, p. 516]). We assume that S has an outer automorphism. Such an automorphism is the product of an inner automorphism and a non-trivial graph automorphism; this only exists when S has type A_n, D_n, or E_6. We choose and fix a maximal torus T of S, a root system Φ of characters of T, and a set of fundamental roots $\{\alpha_1, \ldots, \alpha_r\}$. Throughout, $r = r(S)$ will denote the rank of S, and W the Weyl group.

We need not assume that $\mathrm{Z}(S) = 1$, but will sometimes for brevity identify elements of S with the corresponding inner automorphisms.

The function $\lambda : T \to [0, 1]$ was defined in [NS2, Subsection 5.5.4]:

$$\lambda(t) = (\pi r)^{-1} \sum_{i=1}^{r} |l(\alpha_i(t))|$$

where $l(e^{i\theta}) = \theta$ for $\theta \in (-\pi, \pi]$.

Proposition 2.10 depends on Lemma 5.19 of [NS2] which we restate here in the following form:

Proposition 2.11. *For each $\epsilon > 0$ there is an integer $k = k'(\epsilon)$ such that if $g \in T$ satisfies $\lambda(g) > \epsilon$ then $S = (g^S \cup g^{-S})^{*k}$.*

We shall prove

Lemma 2.12. (i) *There exists $\epsilon = \epsilon(S) > 0$ such that for each $f \in \mathrm{Aut}(S) \setminus \mathrm{Inn}(S)$ there exist an element $g \in [S, f]$ and a conjugate g_1 of g with $g_1 \in T$ and $\lambda(g_1) > \epsilon$.*
(ii) *If $S = \mathrm{(P)SU}(n)$ where $n > 30$, we can take $\epsilon(S) = (200\pi)^{-1}$.*

A simple calculation shows that if $g \in [S, f]$ then $g^S \subseteq [S, f][S, f^{-1}]$ and $g^{-S} \subseteq [S, f^{-1}][S, f]$, and so

$$(g^S \cup g^{-S})^{*k} \subseteq ([S, f][S, f^{-1}][S, f][S, f^{-1}])^{*k} = ([S, f][S, f^{-1}])^{*2k}.$$

Now if $r > 6$, then S has type D_r or A_r. Among centreless compact simple groups, the one of type D_r is $\mathrm{PSO}(2r)$ and the one of type A_r is $\mathrm{PSU}(r+1)$. So Proposition 2.10 will follow from these results on setting

$$k_1 = \max\{k'(\epsilon(S)) \mid r(S) \leq 30\},$$
$$k_0 = 2\max\{k_1,\ k'((200\pi)^{-1})\}, \qquad k(n) = 2k'(\epsilon(\mathrm{PSO}(2n)))$$

(this makes sense because only finitely many groups S have rank at most 30).

Proof of Lemma 2.12(i). For $g \in S$, choose an S-conjugate g' of g inside T and set

$$\eta(g) = \max\{l(\alpha(g')) \mid \alpha \in \Phi\};$$

as different choices for g' lie in the same orbit of W on T, this definition is independent of the choice of g'. It is clear that $\eta(g) = 0$ is equivalent to $g \in \mathrm{Z}(S)$.

Now given $g \in S \setminus \mathrm{Z}(S)$, we have $\eta(g) = l(\alpha(g')) > 0$ for some root $\alpha \in \Phi$, and there exists $w \in W$ with $\alpha^w = \alpha_j$ for some j. Setting $g_1 = g'^w$ we see that

$$\lambda(g_1) \geq (\pi r)^{-1} l(\alpha_j(g_1)) = (\pi r)^{-1} l(\alpha(g')) = (\pi r)^{-1}\eta(g).$$

Suppose now that the statement (i) is false. Then we can find a sequence $f_i = g_i s_i \in \mathrm{Aut}(S)$, with $g_i \in S$ and s_i a non-trivial graph automorphism, such that

$$\sup\{\eta(g) \mid g \in [S, f_i]\} \to 0 \quad \text{as } i \to \infty. \tag{15}$$

Since S is a compact group and $\mathrm{Out}(S)$ is finite we can find a subsequence $f_{i(j)} = g_{i(j)}s_{i(j)}$ with $s_{i(j)} = s$ the same non-trivial graph automorphism for all $j \geq 1$ and $(g_{i(j)})_j$ converging to an element $g \in S$. Thus the subsequence $f_{i(j)}$ converges to the automorphism $f_\infty = gs$ in $\mathrm{Aut}(S)$. Now (15) implies that $[S, f_\infty] \subseteq \mathrm{Z}(S)$ and hence that $f_\infty = 1$ since $S = [S, S]$, a contradiction since $s = g^{-1} f_\infty$ is not inner.

For Lemma 2.12(ii), we fix $S = \mathrm{SU}(n)$ with $n > 30$ and choose T to be the group of diagonal matrices $A = \mathrm{diag}(x_1, \ldots, x_n)$ in S; then Φ consists of all characters $\alpha_{i,j}$ defined by $\alpha_{i,j}(A) = x_i x_j^{-1}$. The Weyl group W of S is $\mathrm{Sym}(n)$ acting on T by permuting the eigenvalues. The function $\lambda : T \to [0, 1]$ is given by

$$\lambda(A) = (\pi(n-1))^{-1} \sum_{i=1}^{n-1} |l(x_i x_{i+1}^{-1})|.$$

The only non-trivial graph automorphism of $\mathrm{SU}(n)$ is induced by complex conjugation of the matrix entries.

Lemma 2.13. *Suppose that $A \in T$ satisfies $\lambda(A^w) \leq \epsilon$ for every $w \in W$. Let $x_1, \ldots, x_n$ be all the eigenvalues of A listed with multiplicities. Then there exists an eigenvalue x of A such that $|l(xx_i^{-1})| < 20\pi\epsilon$ for at least $9n/10$ values of $i \in \{1, \ldots, n\}$.*

Proof. Suppose the claim is false. Then for any eigenvalue x of A, at least one tenth of the other eigenvalues x_i satisfy $|l(xx_i^{-1})| \geq 20\pi\epsilon$. Hence we can reorder $x_1, \ldots, x_n$ as $y_1, \ldots, y_n$ so that $|l(y_i y_{i+1}^{-1})| \geq 20\pi\epsilon$ for each $i = 1, \ldots, [n/10]$. This means that

$$\lambda(\mathrm{diag}(y_1, \ldots, y_n)) \geq (\pi(n-1))^{-1} \times 20\pi\epsilon \times [n/10] > \epsilon,$$

contradicting the hypothesis. □

Proof of Lemma 2.12(ii). Consider an element $a \in \mathrm{SU}(n)$ which has eigenvalues $1, \omega := \exp(\pi i/3)$ and -1, each with multiplicity $m := [(n-1)/3]$. Then a^f has eigenvalues 1, ω^{-1} and -1 with the same multiplicity m.

We claim that the element $b := a^{-1}a^f$ has an S-conjugate $b_1 \in T$ with $\lambda(b_1) > (200\pi)^{-1}$. Suppose this is not true. Then by Lemma 2.13 there exist a b-invariant subspace V_1 of $\mathbb{C}^n$ with $\dim V_1 \geq 9n/10$ and a complex number σ such that all eigenvalues of b on V_1 are of the form $\sigma \exp(it)$ with $|t| < 1/10$. As a consequence, for any unit vector $v \in V_1$ we have $|b \cdot v - \sigma v| < |1 - \exp(i/10)| < 1/10$ (because all eigenvalues of $b - \sigma\mathrm{Id}$ on V_1 have norm at most $|1 - \exp(i/10)|$).

Whatever the complex number σ, there is some $\mu \in \{1, \omega, -1\}$ such that $l(\mu\sigma) \in [\pi/6, 5\pi/6] \cup [-\pi/2, -5\pi/6]$. This means that $l(\sigma\mu x^{-1}) \geq \pi/6$ for each $x = 1, -1, \omega^{-1}$. Therefore $|\sigma\mu - x| > 1/2$ for each such x.

Let V_2 be the μ-eigenspace of a and let V_3 be the sum of the 1,-1 and ω^{-1}-eigenspaces of a^f. We have $\dim V_3 = 3m$, $\dim V_2 = m$, while $n \leq 3m + 3$ and $\dim V_1 \geq 9n/10$. As $n > 30$ we have

$$\dim V_1 + \dim V_2 + \dim V_3 > 2n,$$

which implies that $V_1 \cap V_2 \cap V_3$ is non-empty. Pick a unit vector $v \in V_1 \cap V_2 \cap V_3$. Since $b = a^{-1}a^f$ we have $ab \cdot v = a^f \cdot v$. We can write $bv = \sigma v + u$ where u is a vector of norm less than 1/10. Since v and σv belong to V_2 we have $ab \cdot v = \mu\sigma v + u_1$ where $u_1 = au$ has norm less than 1/10. On the other hand $v \in V_3$ and so we may write $v = w_1 + w_2 + w_3$ where w_1, w_2, w_3 are x_i-eigenvectors of a^f where $(x_1, x_2, x_3) = (1, \omega^{-1}, -1)$. But distinct eigenspaces of a unitary operator are mutually orthogonal, hence $|w_1|^2 + |w_2|^2 + |w_3|^2 = |v|^2 = 1$. Now

$$\mu\sigma(w_1 + w_2 + w_3) + u_1 = \mu\sigma v + u_1 = ab \cdot v = a^f \cdot v = x_1 w_1 + x_2 w_2 + x_3 w_3,$$

giving

$$\sum_{i=1}^{3} (\mu\sigma - x_i) w_i = -u_1,$$

and since $|\mu\sigma - x_i| \geq 1/2$ for each $i = 1, 2, 3$ by the choice of μ, this implies that

$$10^{-2} > |u_1|^2 = \sum_{i=1}^{3} |\mu\sigma - x_i|^2 |w_i|^2 \geq \frac{1}{4} \sum_{i=1}^{3} |w_i|^2 = 1/4.$$

This contradiction completes the proof.

References

[BCP] Babai, L., Cameron, P. J., Pálfy, P.: On the orders of primitive groups with restricted non-abelian composition factors. J. Algebra **79**, 161–168 (1982) Zbl 0493.20001 MR 0679977

[GLS] Gorenstein, D., Lyons, R., Solomon, R.: The Classification of the Finite Simple Groups. No. 3. Amer. Math. Soc., Providence (1998) Zbl 0890.20012 MR 1490581

[H] Helgason, H.: Differential Geometry, Lie Groups and Symmetric Spaces. Grad. Stud. Math. 34, Amer. Math. Soc., Providence (2001) Zbl 0993.53002 MR 1834454

[HM] Hofmann, K. H., Morris, S. A.: The Structure of Compact Groups. 2nd ed., de Gruyter Stud. Math. 25, de Gruyter, Berlin (2006) Zbl 06182019 MR 1646190

[LS1] Liebeck, M. W., Shalev, A.: Simple groups, permutation groups and probability. J. Amer. Math. Soc. **12**, 497–520 (1999) Zbl 0916.20003 MR 1639620

[LS2] Liebeck, M. W., Shalev, A.: Diameters of finite simple groups: sharp bounds and applications. Ann. of Math. **154**, 383–406 (2001) Zbl 1003.20014 MR 1865975

[NS1] Nikolov, N., Segal, D.: On finitely generated profinite groups, I: strong completeness and uniform bounds. Ann. of Math. **165**, 171–238 (2007) Zbl 1126.20018 MR 2276769

[NS2] Nikolov, N., Segal, D.: Generators and commutators in finite groups; abstract quotients of compact groups. Invent. Math. **190**, 513–602 (2012) Zbl 1268.20031 MR 2995181

[S] Segal, D.: Words: Notes on Verbal Width in Groups. London Math. Soc. Lecture Note Ser. 361, Cambridge Univ. Press, Cambridge (2009) Zbl 1198.20001 MR 2547644