Powers in finite groups and a criterion for solubility

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2AZ, UK
m.liebeck@imperial.ac.uk

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904, Israel
shalev@math.huji.ac.il

Abstract

We study the set $G^{[k]}$ of k^{th} powers in finite groups G. We prove that if $G^{[12]}$ is a subgroup then G must be soluble; moreover, 12 is the minimal number with this property. The proof relies on results of independent interest, classifying almost simple groups G and positive integers k for which $G^{[k]}$ contains the socle of G.

1 Introduction

Powers in groups have been extensively studied in connection with the Burnside problems, powerful p-groups and p-adic analytic groups, and other areas. For a group G and a positive integer k, denote by $G^{[k]}$ the set $\{x^k : x \in G\}$ of k^{th} powers in G. It is known [6] that if G is a powerful p-group, then $G^{[p]}$ is a subgroup of G; Malcev[8] showed that if G is finitely generated nilpotent, then $G^{[k]}$ always contains a subgroup of finite index in G; see also [3], where $G^{[k]}$ is studied for finitely generated linear groups.

In this paper we study the power subsets $G^{[k]}$ in finite groups in general, and in almost simple groups in particular. One of our main results is the following somewhat surprising solubility criterion.

Theorem 1 *Let G be a finite group, and suppose that $G^{[12]}$ is a subgroup of G. Then G is soluble.*

Some remarks about this result are in order. First, 12 is the minimal number with this property: we shall see below (Proposition 6) that for every $k < 12$ there is an almost simple group G such that $G^{[k]} = \mathrm{soc}(G)$, the socle of G. Secondly, the proof of the theorem shows that the same conclusion holds with 12 replaced by any integer 2^a3^b with $a \geq 2, b \geq 1$, and there are other numbers which also work (see Section 5). Thirdly, the proof relies on the classification of finite simple groups, and requires a detailed study of power subsets in almost simple groups, which is of some independent interest (see Theorem 7 below). A further consequence of this is the following.

The authors are grateful for the support of an EPSRC grant. The second author acknowledges the support of grants from the Israel Science Foundation and ERC.

2010 Mathematics Subject Classification: 20D10, 20E07, 20D06

Theorem 2 *Let G be a finite group, and suppose that $G^{[3]}$ and $G^{[4]}$ are both subgroups of G. Then G is soluble.*

The next result concerns the set of squares in a finite group. Of course if $G^{[2]} = G$, then G has odd order and hence is soluble by the Feit-Thompson theorem. It turns out that finite groups in which the set of squares is a subgroup need not be soluble; however, their non-abelian composition factors are rather restricted:

Theorem 3 *Let G be a finite group such that $G^{[2]}$ is a subgroup. Then the non-abelian composition factors of G are among the groups $L_2(q)$ (q odd), $L_2(q^2)$ (q even) and $L_3(4)$.*

It is easy to see that if $G^{[k]}$ is a subgroup for all values of k, then G must be nilpotent: indeed, if p is a prime divisor of $|G|$ and k is the p'-part of $|G|$, then $G^{[k]}$ must be the unique Sylow p-subgroup of G.

The next result connects general finite groups and non-abelian composition factors as far as power subsets are concerned.

Theorem 4 *Let G be a finite group and k a positive integer such that $G^{[k]}$ is a subgroup of G. Then for every non-abelian composition factor T of G, either $T \subseteq \mathrm{Aut}(T)^{[k]}$ or the exponent of T divides k. In particular, if k is odd or has at most two prime divisors, then $T \subseteq \mathrm{Aut}(T)^{[k]}$ for all non-abelian composition factors T.*

We now discuss our results on almost simple groups – that is, groups whose socle is a non-abelian simple group. Clearly not all elements of a (non-abelian) simple group are squares. Somewhat surprisingly, it turns out that there are simple groups T in which every element is a square in the automorphism group of T:

Proposition 5 *Let T be one of the simple groups $L_2(q)$ (q odd), $L_2(q^2)$ (q even) or $L_3(4)$. Then every element of T has a square root in $\mathrm{Aut}(T)$. Moreover, there is a group G of the form $T.2$ such that $G^{[2]} = T$.*

The group G in the conclusion is, in the respective cases, $PGL_2(q)$ (q odd), $L_2(q^2)\langle\sigma\rangle$ (q even, σ a field automorphism of order 2), or $L_3(4)\langle\sigma\rangle$ (σ a graph-field automorphism). Other results on squares in finite simple groups and their proportion can be found in [7].

Our next result gives further examples for simple groups.

Proposition 6 (i) *Let $k = p^r > 2$ with p prime, and let $T = L_2(p^{kl})$ for some $l \geq 1$. Then every element of T has a k^{th} root in $\mathrm{Aut}(T)$. Moreover, if $G = T\langle\sigma\rangle$, where σ is a field automorphism of order k, then $G^{[k]} = T$.*

(ii) *Let $k = 2p^r$ with p an odd prime, and let $T = L_2(p^{kl/2})$ for some $l \geq 1$. Then every element of T has a k^{th} root in $\mathrm{Aut}(T)$. Moreover, if $G = PGL_2(p^{kl/2})\langle\sigma\rangle$, where σ is a field automorphism of order $k/2$, then $G^{[k]} = T$.*

Our next theorem shows that there are no further examples of this phenomenon.

Theorem 7 *Let T be a finite simple group, and let $k > 1$ be a positive integer dividing $|T|$. Suppose $\mathrm{Aut}(T)^{[k]}$ contains T. Then $k = p^r$ or $2p^r$ for some prime p. Further, if $k = 2$ then $T = L_2(q)$ or $L_3(4)$ is as in Proposition 5; and if $k = p^r > 2$ or $k = 2p^r$ (p odd), then $T = L_2(p^{kl})$ or $L_2(p^{kl/2})$ is as in Proposition 6.*

Note that the assumption that k divides $|T|$ can be made without loss of generality, since if $k = ab$ where a divides $|T|$ and $(|T|, b) = 1$, then $\mathrm{Aut}(T)^{[k]}$ contains T if and only if $\mathrm{Aut}(T)^{[a]}$ contains T.

The next result is immediate from Theorem 7.

Corollary 8 (i) *If T is a finite simple group with $T \neq L_2(q)$, $L_3(4)$, and k is a positive integer such that* $\mathrm{Aut}(T)^{[k]}$ *contains T, then k is coprime to* $|T|$.

(ii) *If G is a finite almost simple group, then $G^{[p]}$ is a subgroup of G for at most one odd prime p dividing* $|\mathrm{soc}(G)|$.

The layout of the paper is as follows. Section 2 is devoted to our examples of almost simple groups G with the property that $G^{[k]}$ contains $\mathrm{soc}(G)$ given in Propositions 5 and 6. In Section 3 we show that these are the only such examples, thereby proving Theorem 7, and also deduce Corollary 8. Section 4 is devoted to general finite groups. We start it with the proof of Theorem 4, and use this to deduce Theorems 1, 2 and 3. Finally in Section 5 we investigate the set of numbers k for which the assumption that $G^{[k]}$ is a subgroup implies that G is soluble.

2 Almost simple groups: examples

First we prove Proposition 5. Let T be one of the simple groups in the statement of the proposition. Elements of odd order in T are squares, so we need only handle elements of even order.

First consider $T = L_2(q)$ with q odd. Let $G = PGL_2(q)$. If $x \in T$ is an element of even order, then its order divides $\frac{1}{2}(q + \epsilon)$ for some $\epsilon \in \{\pm 1\}$, and there is an element $y \in G$ of order $q + \epsilon$ such that $x \in \langle y^2 \rangle$. Hence $G^{[2]} = T$.

Now let $T = L_2(q^2)$ with q even, and $G = T\langle\sigma\rangle$ where σ is an involutory field automorphism. For $\alpha \in \mathbb{F}_{q^2}$, set

$$u(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

It is well known that every element of even order in T is conjugate to $u(1)$. For $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ we have $(u(\alpha)\sigma)^2 = u(\alpha + \alpha^\sigma)$. It follows that $u(1)$, and hence all elements of even order, are squares in G, and so $G^{[2]} = T$.

Finally, for $T = L_3(4)$ and $G = T\langle\sigma\rangle$ with σ a graph-field automorphism, the conclusion can be checked using [1]. This completes the proof of Proposition 5.

Now we prove Proposition 6. First consider part (i). Let $k = p^r$, $T = L_2(p^{kl})$ and $G = T\langle\sigma\rangle$ as in the statement. Define $u(\alpha)$ as above, for $\alpha \in F := \mathbb{F}_{p^{kl}}$. First assume p is odd. Then every element in T of order divisible by p is conjugate to $u(1)$ or $u(\beta)$ with $\beta \in F$ non-square. We have $(u(\alpha)\sigma)^k = u(Tr(\alpha))$, where Tr is the trace map $F \mapsto F_{p^l}$. Since Tr is surjective, this shows that $u(1)$ and $u(\beta)$ are both k^{th} powers in G, as required. Finally, for $p = 2$, every element of even order in T is conjugate to $u(1)$, and the same proof applies.

Now consider part (ii). Let $k = 2p^r$ with p an odd prime, and let $G = PGL_2(p^{kl/2})\langle\sigma\rangle$ be as in the proposition. For $x \in T = \mathrm{soc}(G)$, Proposition 5 shows that $x = y^2$ for some $y \in PGL_2(p^{kl/2})$. If y has order divisible by p, then y is in

T and has order p, and as in (i), there exists $z \in G$ such that $y = z^{p^r}$; the same holds trivially if y has order coprime to p. Hence $x = z^{2p^r} = z^k$, and the proof is complete.

3 Almost simple groups: Proof of Theorem 7

We begin with a preliminary result for general finite groups which will be used frequently in the proof.

Lemma 3.1 *Let G be a finite group with a normal subgroup T such that G/T is cyclic of order k. Write $G = T\langle\sigma\rangle$ where $\sigma^k \in T$. Suppose $y \in G^{[k]} \setminus T^{[k]}$. Then there exists i with $1 \leq i \leq k-1$ such that y^{σ^i} is T-conjugate to y. In particular, if k is prime then y^σ is T-conjugate to y.*

Proof. Write $y = x^k$. There exist $t \in T$ and $1 \leq i \leq k-1$ such that $x = t\sigma^{-i}$. Observe that

$$y^{\sigma^i} = ((t\sigma^{-i})^k)^{\sigma^i} = ((t\sigma^{-i})^k)^t = y^t.$$

The first assertion follows. For the second assertion, choose j such that $\sigma^{ij} \equiv \sigma \bmod T$, and observe that y^σ is T-conjugate to $y^{(\sigma^i)^j}$, which is T-conjugate to y. ∎

Now we embark on the proof of Theorem 7. Suppose T is a finite simple group and $k > 1$ is an integer dividing $|T|$ such that $\mathrm{Aut}(T)^{[k]}$ contains T.

Lemma 3.2 *If T is alternating or sporadic, then $T = A_5$ or A_6 and $k = 2$.*

Proof. Since $\mathrm{Out}(T)$ is 2 or 2^2 for these groups, k must be 2. Note that $A_5 \cong L_2(5)$ and $A_6 \cong L_2(9)$ appear in the conclusion by Theorem 5. For $n \geq 7$, $T = A_n$ does not occur, since for example permutations of cycle shape $(4,2)$ are not squares in S_n. And for T sporadic, one checks using the character tables in [1] that for those groups T which possess outer automorphisms, there are elements in T which have no square root in $\mathrm{Aut}(T)$. ∎

Lemma 3.3 *The conclusion of Theorem 7 holds if $T = L_2(q)$ or $L_3(4)$.*

Proof. For $L_3(4)$ the result can be checked using [1]. So suppose that $T = L_2(q)$ and that $T \subseteq \mathrm{Aut}(T)^{[k]}$ for some $k > 1$ dividing $|T|$. Let p be a prime dividing k, and let p^r be the p-part of k.

Assume first that p is odd and does not divide q. Then p divides $q - \epsilon$ with $\epsilon = \pm 1$. Let $x \in T$ be an element of order $(q-\epsilon)/(2, q-\epsilon)$. Clearly $x \notin T^{[p]}$. Hence $x \in (T\langle\sigma\rangle)^{[p]}$ where σ is a field automorphism of order p. By Lemma 3.1 this implies that x is T-conjugate to x^σ. But this is a contradiction as the only elements of $\langle x \rangle$ which are T-conjugate to x are $x^{\pm 1}$.

If p is odd and divides q, then since $T \subseteq \mathrm{Aut}(T)^{[p]}$, there must be an element of order p^r in $\mathrm{Out}(T)$, and hence $q = p^{p^r l}$ for some $l \geq 1$.

Now suppose $p = 2$ and $p^r = 2^r \geq 4$. If q is odd then 4 divides $q - \epsilon$ with $\epsilon = \pm 1$ and we let x be an element of order $(q-\epsilon)/2$. Then $x \notin T^{[2]}$, and so $x \in (T\langle\sigma\rangle)^{[4]}$

where σ induces an outer automorphism of order 4; but x is not T-conjugate to x^σ for such an automorphism, so this contradicts Lemma 3.1. If q is even then T has an outer automorphism of order 2^r, so $q = 2^{2^r l}$ for some l.

Next assume that $p = p^r = 2$. Then either q is odd, or q is even and T has an outer automorphism of order 2 so that $q = 2^{2l}$ for some l.

From the above, we conclude that one of the following holds:

$$k = p^r,\ q = p^{p^r l}$$
$$k = 2,\ q \text{ odd}$$
$$k = 2p^r,\ q = p^{p^r l}, p \text{ odd}$$

These are precisely the possibilities on the conclusion of Theorem 7. ∎

We assume from now on that $T \neq L_2(q)$ or $L_3(4)$. Let p be a prime divisor of k, so that $\mathrm{Aut}(T)^{[p]}$ contains T.

Lemma 3.4 *The group T is not $L_n(q)$.*

Proof. Suppose $T = L_n(q)$. By assumption $n \geq 3$ and $(n,q) \neq (3,2),(3,4)$.

Assume first that $p|q-1$ and $p \geq 3$. Let $\lambda \in \mathbb{F}_q^*$ have order $q-1$ and define $x = \mathrm{diag}(a(\lambda,1), \lambda^{-2}, 1, \ldots, 1)Z \in T$, where Z is the group of scalars and

$$a(\lambda,\beta) = \begin{pmatrix} \lambda & \beta \\ 0 & \lambda \end{pmatrix}. \tag{1}$$

For $q > 4$, the centralizer of x in $PGL_n(q)$ consists of elements of the form $\mathrm{diag}(a(\alpha,\beta),\gamma,A)Z$, and x cannot be the p^{th} power of one of these as λ is not a p^{th} power in $\mathbb{F}_q^*$. Hence x is not a p^{th} power in $PGL_n(q)$; a similar argument gives the same conclusion when $q = 4$. It follows that x must be a p^{th} power in a group $T\langle\sigma\rangle$, where σ involves a field automorphism of order p (i.e. σ is a product of a (possibly trivial) diagonal automorphism and such a field automorphism). Then x is T-conjugate to x^σ, by Lemma 3.1. But this is not the case, as can be seen by consideration of the eigenvalues of x and x^σ.

Now assume that $p = 2$ and q is odd. Let $A \in GL_2(q)$ be an element of order q^2-1 with eigenvalues λ, λ^q over $\mathbb{F}_{q^2}$, and define $x = \mathrm{diag}(A, \lambda^{-q-1}, 1, \ldots, 1)Z \in T$. By considering the centralizer of x as above, we see that it is not a square in $PGL_n(q)$. Therefore x must be a square in a group $T\langle\sigma\rangle$ where σ involves an involutory field, graph or graph-field automorphism of T. A graph automorphism inverts the eigenvalues of x, while an involutory field automorphism sends the eigenvalue $,\lambda^{-q-1}$ to $,\lambda^{-qq_0-q_0}$ where $q = q_0^2$. Hence we see that x cannot be T-conjugate to x^σ, contradicting Lemma 3.1.

This deals with the case where $p|q-1$, so assume from now on that p does not divide $q-1$. If $p > 2$ the outer automorphisms of T of order p are field automorphisms, while if $p = 2$ they are field, graph or graph-field automorphisms.

Assume $p > 2$. If $p|q$, take $x = \mathrm{diag}(a(\lambda,1), \lambda^{-2}, 1, \ldots, 1)Z \in T$ with $|\lambda| = q-1$ as before. Then x is not a p^{th} power in T, and also is not conjugate to x^σ if σ is a field automorphism of order p. And if p does not divide q, choose e minimal such that $p|q^e-1$ and let

$$x(\lambda) = \mathrm{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{e-1}}) \in GL_1(q^e) \leq GL_e(q)$$

for $\lambda \in \mathbb{F}_{q^e}$. For λ of order $\frac{q^e-1}{q-1}$, let $x = \mathrm{diag}(x(\lambda), I_{n-e})Z \in T$. The we see as usual that x is not a p^{th} power in T and is not conjugate to x^σ if σ is a field automorphism of order p. This handles the case $p > 2$.

Finally, let $p = 2$. As p does not divide $q-1$ by assumption, q is even. If $q > 4$ let $x = \mathrm{diag}(a(\lambda, 1), \lambda^{-2}, 1, \ldots, 1)Z \in T$ with $|\lambda| = q-1$ and argue as above. If $q = 2$ or 4 and $n \geq 5$, let $x(\lambda) \in SL_3(q)$ be as above with $e = 3$ and $\lambda \in \mathbb{F}_{q^3}$ of order q^2+q+1, and define $x = \mathrm{diag}(x(\lambda), J_{n-3})$ where J_{n-3} is a unipotent Jordan block of size $n-3$. Then x is not a square in T (as J_{n-3} is not a square in $SL_{n-3}(q)$), and x is not conjugate to x^σ for σ an involutory field, graph or graph-field automorphism of T.

This leaves the cases $T = L_4(2)$ and $L_4(4)$ (since $(n,q) \neq (3,2), (3,4)$ by assumption). The first of these is the alternating group A_8 which has already been handled. And $L_4(4)$ has an element x of order 30 of the form $\mathrm{diag}(a(\lambda, 1), M)$ where λ has order 3 and $M \in GL_2(4)$ has order 15 and determinant λ; we argue in the usual way that x is not a square in $\mathrm{Aut}(T)$. ∎

Lemma 3.5 *T is not $U_n(q)$.*

Proof. Suppose $T = U_n(q)$. Then $n \geq 3$ and $(n,q) \neq (3,2)$.

The proof is quite similar to the previous lemma. Assume first that $p|q+1$ and $n \geq 4$. Let $x = \mathrm{diag}(a(\lambda, \beta), \lambda^{-2}, 1, \ldots, 1)Z \in T$ for $\lambda \in \mathbb{F}_{q^2}$ of order $q+1$ and suitable $\beta \in \mathbb{F}_{q^2}$ (where $a(\lambda, \beta)$ is as in (1) and matrices are taken relative to a basis with first three vectors e, f, d where e, f are singular, $(e,f) = 1$ and d is nonsingular and perpendicular to e, f). If $q > 2$ we can argue as in the previous lemma that x is not a p^{th} power in $PGU_n(q)$ and is not conjugate to x^σ for any further outer automorphism σ of T of order p. And if $q = 2$ then $p = 3$ and we take $x = \mathrm{diag}(a(\lambda, \beta), \lambda^{-1}, \lambda^{-1}, 1, \ldots, 1)Z \in T$ with $|\lambda| = 3$ and argue similarly.

Now assume $p|q+1$ and $n = 3$ (so $q > 2$). Again take $x = \mathrm{diag}(a(\lambda, \beta), \lambda^{-2})Z \in T$, with λ of order $q+1$. As usual, x is not a p^{th} power in $PGU_3(q)$, and is not conjugate to x^σ for σ a field automorphism unless $p = 2$ and $q = 5$. So it remains to handle $T = U_3(5)$ with $p = 2$; this can be done using [1].

Next assume that $p|q$. If $q > 2$, take $x = \mathrm{diag}(a(\lambda, \beta), \lambda^{-2}, 1, \ldots, 1)Z \in T$ with λ of order $q+1$ again and argue as before. And in the case where $q = 2$, take $x = \mathrm{diag}(a(\lambda, \beta), \lambda^{-1}, \lambda^{-1}, 1, \ldots, 1)Z \in T$ with $|\lambda| = 3$.

It remains to deal with the case where p divides neither $q+1$ nor q. Then $p > 2$, and any outer automorphism of T of order p is a field automorphism. Choose the first factor in the product $(q^2-1)(q^3+1)(q^4-1)\cdots(q^n-(-1)^n)$ that p divides. If it is q^i+1, take x to be a generator of a cyclic torus of T of type $GU_1(q^i) < GU_i(q) \leq GU_n(q)$ (we must intersect this with $SU_n(q)$ and factor out Z); and if it is $q^{2i}-1$, take x to be a generator of a cyclic torus of type $GL_1(q^{2i}) < GL_i(q^2) < GU_n(q)$. Now argue that x is not a p^{th} power in T and is not conjugate to x^σ for σ a field automorphism of order p. ∎

Lemma 3.6 *T is not $PSp_{2n}(q)$.*

Proof. Suppose $T = PSp_{2n}(q)$. Then $n \geq 2$ and $(n,q) \neq (2,2)$.

Assume $p > 2$. Then any outer automorphism of T of order p is a field automorphism.

If $p|q$, let $A \in Sp_2(q)$ be an element of order $q+1$, and define $x = \mathrm{diag}(A, J_{2n-2})Z \in T$, where as before J_{2n-2} is a unipotent Jordan block of size $2n-2$. Then $C_T(x) \leq (Sp_2(q) \times Sp_{2n-2}(q))/Z$, and since J_{2n-2} is not a p^{th} power in $Sp_{2n-2}(q)$, x is not a p^{th} power in T. Also for a field automorphism σ of order p, x^σ is not conjugate to x.

If p does not divide q, let e be minimal such that $p|q^e - \delta$ for some $\delta = \pm 1$. If $\delta = -1$, let x be a generator of a cyclic torus of T of order $q^e + 1$ (or $(q^e+1)/2$) in a subgroup of type $Sp_2(q^e) \leq Sp_{2e}(q)$; and if $\delta = +1$, then e is odd and we let x generate a torus of order $q^e - 1$ (or $(q^e - 1)/2$) in a subgroup of type $GL_1(q^e) \leq GL_e(q) \leq Sp_{2e}(q)$. Then x is not a p^{th} power in T and x^σ is not conjugate to x for a field automorphism σ of order p.

Now assume $p = 2$. Then a non-diagonal involutory outer automophism of T involves a field automorphism or, if $n = 2$ and $q = 2^{2k+1}$, a graph automorphism. Let $x = \mathrm{diag}(A, J_{2n-2})Z \in T$ again, and argue as before that x is not a square in T and x^σ is not conjugate to x for a field automorphism σ of order 2. Finally, in the case where $n = 2$ and $q = 2^{2k+1}$ we need also to observe that x^σ is not conjugate to x for σ an involutory graph automorphism; this follows as $x = su$ with $s = \mathrm{diag}(A, I_2)$ and $u = \mathrm{diag}(I_2, J_2)$ a long root element of T, so $x^\sigma = s^\sigma u^\sigma$ with u^σ a short root element, hence is not conjugate to x. ■

Lemma 3.7 *T is not an orthogonal group.*

Proof. Suppose T is orthogonal, so $T = P\Omega(V) = P\Omega_{2n+1}(q)$ (q odd, $n \geq 3$) or $P\Omega^\epsilon_{2n}(q)$ ($n \geq 4$, $\epsilon = \pm$).

First assume that $p = 2$ and q is odd. Let A be a matrix in $GL_2(q)$ of order $q^2 - 1$ with eigenvalues λ, λ^q over $\mathbb{F}_{q^2}$. With respect to a suitable basis, there is an element $x = \mathrm{diag}(A, A^{-T}, \lambda^{q+1}, \lambda^{-q-1}, I)$ which lies in a subgroup $GL_3^*(q)$ of T (the subgroup of matrices of square determinant in $GL_3(q)$). We argue in the usual way that x is not a square in $P\Delta(V)$ (notation of [5]) and is not conjugate to x^σ if σ involves an involutory field automorphism.

Now suppose $p = 2$ and q is even. In this case we let A be an element of order $q+1$ in $\Omega_2^-(q)$ and argue in the usual way with an element $x = \mathrm{diag}(A, J_{2n-4}, J_2)$ in a subgroup $\Omega_2^-(q) \times \Omega_{2n-2}^{-\epsilon}(q)$ of T.

Now let $p > 2$. If $p|q$, let A be an element of order $q+1$ in $\Omega_2^-(q)$ and let $x = \mathrm{diag}(A, J_{2n-3}, J_1)$ in a subgroup $\Omega_2^-(q) \times \Omega_{2n-2}^{-\epsilon}(q)$. And if p does not divide q, choose e minimal such that $p|q^e - \delta$ for some $\delta = \pm 1$. If $\delta = -1$, let x be a generator of a cyclic torus of type $\Omega_2^-(q^e) < \Omega_{2e}^-(q)$, and if $\delta = +1$ (so e is odd), let x generate a cyclic torus of type $GL_1(q^e) < GL_e(q) < \Omega_{2e}^+(q)$.

With x as in the previous paragraph, we argue in the usual way that x is not a p^{th} power in T and that x is not conjugate to x^σ when $\sigma \in P\Gamma(V)$ (notation of [5]) involves a field automorphism of order p. This completes the proof except in the case where $p = 3$ and $T = P\Omega_8^+(q)$, in which case σ could involve a triality automorphism of T.

So assume finally that $T = P\Omega_8^+(q)$ and $p = 3$.

If $q = 3^a$, let $x = \mathrm{diag}(J_5, \lambda, \lambda^{-1}, 1)$ lying in a subgroup of type $\Omega_5(q) \times \Omega_3(q)$, where $\lambda \in \mathbb{F}_q$ has order $(q-1)/2$. Write $x = us$ with $u = J_5 \in \Omega_5(q)$ and $s = (\lambda, \lambda^{-1}, 1) \in \Omega_3(q)$. Then $x \notin T^{[3]}$ as u is not a cube in T. If σ is an outer automorphism of order 3 involving a triality, then x is not T-conjugate to x^σ since

u is not conjugate to u^σ (as $u^\sigma = J_4^2$ in a subgroup of type $Sp_4(q)$); and if σ is a field automorphism then the same conclusion holds since s is not conjugate to s^σ.

If q is not a power of 3, let 3 divide $q-\epsilon$ ($\epsilon = \pm 1$), let A be an element of order $(q-\epsilon)/(2, q-1)$ in $\Omega_2^\epsilon(q)$, and let $x = \mathrm{diag}(A, J_4, J_2)$ (q even) or $\mathrm{diag}(A, J_5, J_1)$ (q odd) lying in a subgroup of type $\Omega_2^\epsilon(q) \times \Omega_6^\epsilon(q)$. Now argue as in the previous paragraph. ■

Lemma 3.8 *T is not an exceptional group of Lie type.*

Proof. Suppose T is an exceptional simple group of Lie type over $\mathbb{F}_q$. Exclude $G_2(2)' = U_3(3)$ and ${}^2G_2(3)' = L_2(8)$.

Assume first that $p > 2$. Then the only outer automorphisms of T of order p are field automorphisms, together with diagonal (and field-diagonal) automorphisms when $p = 3$, $T = E_6^\epsilon(q)$ and $3|q-\epsilon$.

If $p|q$, then except for $T = {}^2G_2(q)$, there is a fundamental $A = SL_2(q)$ in T, with centralizer D (where $D = E_7(q)$, $D_6(q)$, $A_5^\epsilon(q)$, $C_3(q)$, $A_1(q)$ or $A_1(q^3)$, according as $T = E_8(q)$, $E_7(q)$, $E_6^\epsilon(q)$, $F_4(q)$, $G_2(q)$ or ${}^3D_4(q)$ respectively). Let $s \in A$ be an element of order $q+1$, and let $u \in D$ be a regular unipotent element. Define $x = su$. Then $C_T(x) \le AD$, and so x is not a p^{th} power in T (as u is not a p^{th} power in D). Also x is not conjugate to x^σ for σ a field automorphism of order p, so this completes the proof in this case, except for $T = {}^2G_2(q)$.

For $T = {}^2G_2(q)$, $p = 3$, $q = 3^{2k+1} > 3$, we require a more detailed argument. Adopting the notation of [2, Table 2.4], T has a Sylow 3-subgroup $P = \{x(t,u,v) : t,u,v \in \mathbb{F}_q\}$ of order q^3 and exponent 9, where

$$x(t,u,v) \cdot x(t',u',v') = x(t+t', u+u'+t't^{3\theta}, v+v'-t'u+(t')^2t^{3\theta}),$$

θ being the map $t \to t^{3^k}$. Then $Z(P) = \{x(0,0,v) : v \in \mathbb{F}_q\}$. If $y = x(1,0,0)$ then y has order 9 (so is not a cube in T), $y^3 \in Z(P)$ and $C_T(y) = \langle y \rangle Z(P)$ (see [9]). If σ is an outer automorphism of T of order 3, then it is a field automorphism and we can take it to act on P as $x(t,u,v) \to x(t^\sigma, u^\sigma, v^\sigma)$. Suppose y is a cube in $T\langle\sigma\rangle$, say $y = (x\sigma)^3$ with $x \in T$. Then $x\sigma \in C_{T\langle\sigma\rangle}(y) = \langle y \rangle Z(P)\langle\sigma\rangle$, so $x = y^k x(0,0,v)$ for some integer k and $v \in \mathbb{F}_q$. But then since y centralizes $x(0,0,v)$ we have $(x\sigma)^3 = y^{3k}x(0,0,v^{1+\sigma+\sigma^2})$ which has order dividing 3, so cannot equal y. Hence y is not a cube in $T\langle\sigma\rangle$, completing the proof in this case.

Now assume p does not divide q (still with $p > 2$). Postpone the case where $p = 3$, $T = E_6^\epsilon(q)$ and $3|q-\epsilon$. From [4, Section 2], we check that with a few exceptions (listed below), there is a cyclic maximal torus of T of order divisible by p. If we take x to be a generator of this torus, then x is not a p^{th} power in T, and is not conjugate to x^σ if σ is a field automorphism of order p. The exceptions are as follows:

T	$E_7(q)$	$E_6(q)$	${}^2E_6(q)$	$F_4(q)$	${}^2G_2(q)$
p	q_4, q_8	q_6	q_3	q_4	q_2

Here q_i denotes a primitive prime divisor of $q^i - 1$. For the $T = E_7(q)$ case, take x to be an element of order $\frac{q^4-1}{q-1}$ or $\frac{q^4+1}{2,q-1)}$ in a subsystem subgroup $A_3(q)$ or $D_4(q)$ in the respective cases $p = q_4, q_8$. If $x = y^p$ for some $y \in T$ then y lies in a maximal torus; but we see from [4] that there is no maximal torus in which x is a p^{th} power. Hence x is not a p^{th} power in T. And if σ is a field automorphism of order p, then from the action of σ on $A_3(q)$ or $D_4(q)$, we see that x is not conjugate to x^σ. The cases $T = E_6^\epsilon(q)$ are handled similarly by taking x to be an element of order $\frac{q^6-1}{q-\epsilon}$ in a subgroup $A_5^\epsilon(q)$. Finally, in the $F_4(q)$ and ${}^2G_2(q)$ cases we take x of order $\frac{q^4-1}{(2,q-1)}$ or $\frac{q+1}{2}$ in a maximal torus of the form $\langle x\rangle \times (2, q-1)$.

Now consider the postponed case where $p = 3$, $T = E_6^\epsilon(q)$ and $3|q-\epsilon$. In a subsystem subgroup $A_1(q)A_5^\epsilon(q)$, take an element $x = yz$, where $y \in A_1(q)$ has order $q-\epsilon$ and z is a regular unipotent element in $A_5^\epsilon(q)$. If $T.3$ denotes the group generated by inner and diagonal automorphisms of T, then $C_{T.3}(x) = \langle y\rangle U$ where U is a unipotent group, so x is not a cube in $T.3$. Also x is not conjugate to x^σ when σ involves a field automorphism of order 3.

This completes the case where $p > 2$. Now suppose $p = 2$. Note that $T \neq {}^2B_2(q)$, ${}^2G_2(q)$ or ${}^2F_4(q)$ $(q > 2)$ as these have no outer automorphisms of order 2.

Assume q is odd. For $T = E_8(q)$, $F_4(q)$, ${}^3D_4(q)$ or $G_2(q)$ $(q \neq 3^k)$, take x to be a generator of a cyclic maximal torus of even order (which exists by [4]), and argue as usual that x is not a square in T and is not conjugate to x^σ for σ an involutory field automorphism. The other groups $E_7(q)$, $E_6^\epsilon(q)$, $G_2(q)$ $(q = 3^k)$ possess diagonal or graph automorphisms of order 2, so require a little more care.

For $T = E_7(q)$ we work in a subsystem subgroup $A_2(q)A_5(q)$. This has normalizer $N = A_2(q)A_5(q).2$ in the inner-diagonal group $T.2$. The outer involution acts diagonally on the $A_5(q)$ factor and as an inner automorphism on $A_2(q)$. Take an element x in the factor $A_2(q) \cong SL_3(q)$ of order q^2-1. Then $C_{T.2}(x) \leq N$, so we see that x is not a square in $T.2$. Also x is not conjugate to x^σ when σ involves an involutory field automorphism, so this case is done.

For $T = E_6^\epsilon(q)$, take x to be an element of order q^4-1 in a subsystem subgroup $A_4^\epsilon(q) \cong SL_5^\epsilon(q)$. No torus in T has an element of order $2(q^4-1)$ (see [4]), so x is not a square in T. If σ is a graph automorphism of T, it acts as a graph automorphism on a suitable subgroup $A_4^\epsilon(q)$, and hence we see that x is not conjugate to x^σ. Also x is not conjugate to x^σ when σ involves an involutory field automorphism.

Now consider $T = G_2(q)$ with $q = 3^k$. Let $q \equiv \epsilon \bmod 4$ with $\epsilon = \pm 1$. There is a subgroup $A_1\tilde{A}_1$ in T, a commuting product of two $SL_2(q)$'s where A_1 is generated by long root groups and $\tilde{A}_1$ by short root groups. Let $x = us$ with $u \in A_1$ of order 3 and $s \in \tilde{A}_1$ of order $q-\epsilon$. Then $C_T(x) \leq A_1\tilde{A}_1$, and hence we see that $x \notin T^{[2]}$. If σ is an involutory outer automorphism of T involving a graph automorphism, then x^σ is not T-conjugate to x (since the long root element u is not conjugate to the short root element u^σ); and if σ is a field automorphism then the same conclusion holds as s^σ is not conjugate to s.

Now assume that q is even (still with $p = 2$). Use [1] for the case where $T = {}^2F_4(2)'$. Since we have ruled out T of type ${}^2B_2$ or ${}^2F_4$, this leaves T of type $E_8, E_7, E_6^\epsilon, F_4, G_2$ or ${}^3D_4$. For all but the E_6^ϵ and F_4 cases we can argue exactly as for the $p|q$ case done above for $p > 2$. For E_6^ϵ and F_4 there are graph automorphisms to take into account.

In the case where $T = E_6^\epsilon(q)$, in a subsystem subgroup $A_1(q)A_5^\epsilon(q)$ take $x = us$ where $u \in A_1(q)$ is an involution and $s \in A_5^\epsilon(q)$ an element of order $\frac{q^6-1}{q-\epsilon}$. Then $C_T(x) = C_{A_1(q)}(u)\langle s\rangle$, so x is not a square in T. Also a graph automorphism σ normalizing $A_1(q)A_5^\epsilon(q)$ acts as a graph automorphism on $A_5^\epsilon(q)$, hence inverts x, so x is not T-conjugate to x^σ. And x is not conjugate to x^σ when σ involves an involutory field or graph-field automorphism.

Finally, consider $T = F_4(q)$. In a subsystem subgroup $A_2(q)A_2(q)$ take $x = us$, where u is a regular unipotent element of the first factor, and s an element of order $q^2 + q + 1$ in the second. Since $C_T(s) = A_2(q)\langle s\rangle$, x is not a square in T. For σ a graph automorphism, $x^\sigma = u^\sigma s^\sigma$ is not conjugate to x, as u and u^σ are not conjugate, one being regular in a long root A_2, the other in a short root A_2. And as usual, x is not conjugate to x^σ when σ is an involutory field automorphism. This completes the proof. ∎

4 General finite groups

First we prove Theorem 4. Let G be a finite group and suppose $G^{[k]}$ is a subgroup of G. The proof is by induction on $|G|$. Let N be a minimal normal subgroup of G. Then $(G/N)^{[k]}$ is a subgroup, hence by induction its non-abelian composition factors satisfy the conclusion of the theorem. If N is abelian then the theorem follows. So we may assume that $N = T^r$ for some non-abelian simple group T. It suffices to show that either $T \subseteq \mathrm{Aut}(T)^{[k]}$ or the exponent of T divides k. Assume the contrary, and let $t \in T \setminus \mathrm{Aut}(T)^{[k]}$.

Let $\bar{G} = G/C_G(N)$. Then $\bar{G}$ embeds in $\mathrm{Aut}(N) = \mathrm{Aut}(T) \wr S_r$. We identify N with its image in $\bar{G}$.

We claim that the element $n = (t, 1, \dots, 1) \in T^r = N$ is not a k^{th} power in $\bar{G}$. To see this, suppose $n = x^k$ where $x = (x_1, \dots, x_r)\sigma$ with each $x_i \in \mathrm{Aut}(T)$ and $\sigma \in S_r$. Then $\sigma^k = 1$. If $\sigma(1) = 1$ then $t = x_1^k$, contradicting the fact that t is not a k^{th} power in $\mathrm{Aut}(T)$. So σ has a cycle $(1\, i_2 \cdots i_s)$ with $s \geq 1$. Calculating the coordinates of x^k in positions 1 and i_s, we get $t = x_1 x_{i_2} \cdots x_{i_s}$ and $1 = x_{i_s} x_1 \cdots x_{i_{s-1}}$, a contradiction.

It follows that $G^{[k]}$ is a normal subgroup of G which does not contain N. Hence $G^{[k]} \cap N = 1$. Therefore all k^{th} powers in N are trivial, which means that k is divisible by the exponent of T. This contradicts our assumption on T, and completes the proof of the first assertion of Theorem 4. The last assertion follows using Burnside's $p^a q^b$ theorem.

Finally we deduce Theorems 1, 2 and 3. Suppose G is a finite group such that $G^{[k]}$ is a subgroup, where k divides 12. Then Theorem 4 shows that $T \subseteq \mathrm{Aut}(T)^{[k]}$ for every composition factor T of G.

If $k = 2$ then Theorem 7 shows that the non-abelian composition factors of G are among the groups $L_2(q)$ (q odd), $L_2(q^2)$ (q even) and $L_3(4)$, proving Theorem 3.

Now assume that both $G^{[3]}$ and $G^{[4]}$ are subgroups of G. Suppose G is not soluble, and let T be a non-abelian composition factor. Since all non-abelian simple groups have order divisible by 4, Theorem 7 shows that $T = L_2(q)$ with q even. Then T has order divisible by 3, so Theorem 7 now gives a contradiction. Hence G is soluble, proving Theorem 2.

Finally, assume that $G^{[12]}$ is a subgroup of G. If T is a non-abelian composition factor, then $T \subseteq \mathrm{Aut}(T)^{[12]} \subseteq \mathrm{Aut}(T)^{[4]}$, so again Theorem 7 gives $T = L_2(q)$ with q even. But then 12 divides $|T|$, so Theorem 7 gives a contradiction. Hence G is soluble, and Theorem 1 is proved.

5 Good and bad numbers

Define a positive integer k to be *good* if the assumption that $G^{[k]}$ is a subgroup implies that G is soluble, and *bad* otherwise. We observed in the Introduction that 12 is the minimal good number.

Proposition 5.1 *The following numbers are good:*

(i) $2^a p^b$ *with* $a \geq 2$, $b \geq 1$ *and* $p \in \{3, 5, 17\}$*;*

(ii) 105.

Proof. We copy the proof of Theorem 1. Let k one of the numbers in (i) or (ii) and suppose $G^{[k]}$ is a subgroup of G. Assume G has a non-abelian composition factor T. Then $T \subseteq \mathrm{Aut}(T)^{[k]}$ by Theorem 4. For k as in (i), Theorem 7 implies that $T = L_2(2^{4r})$ for some r; but then $|T|$ is divisible by the primes $p \in \{3, 5, 17\}$, so Theorem 7 gives a contradiction. Finally, assume $k = 105$. If $|T|$ is divisible by 3, then Theorem 7 implies that $T = L_2(3^{3r})$; but then $|T|$ is divisible by 7 and Theorem 7 gives a contradiction. And if $|T|$ is coprime to 3, then T is a Suzuki group; then 5 divides $|T|$ and once again Theorem 7 gives a contradiction. ∎

Proposition 5.2 *The following numbers are bad:*

(i) p^a *and* $2p^a$ *with* p *prime;*

(ii) *numbers coprime to* 6*;*

(iii) $3^a p^b$ *with* $p > 3$ *prime and* $a, b \geq 1$*.*

Proof. (i) This is clear from Proposition 6.

(ii) Let k be coprime to 6. Using Dirichlet's theorem on primes in arithmetic progression, one can see that there is a prime $p > 3$ such that $T = L_2(p)$ has order coprime to k. Then $T^{[k]} = T$, which shows that k is bad.

(iii) Let $k = 3^a p^b$ as in (iii). If $p \neq 5$ then k is coprime to the order of one of the Suzuki groups $Sz(8)$ or $Sz(32)$, so k is bad. And if $p = 5$ then p does not divide the order of $T = L_2(3^{3^a})$, so Proposition 6 shows that there is a group G with socle T such that $G^{[k]} = T$. ∎

It follows quickly that 20 is the smallest even good number greater than 12, and 105 is the smallest odd good number.

References

[1] J.H.Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[2] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups.* Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[3] E. Hrushovski, P.H. Kropholler, A. Lubotzky and A. Shalev, Powers in finitely generated groups, *Trans. Amer. Math. Soc.* **348** (1996), 291–304.

[4] W.M. Kantor and A. Seress, Prime power graphs for groups of Lie type, *J. Algebra* **247** (2002), 370–434.

[5] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. no. 129, Cambridge University Press, 1990.

[6] A. Lubotzky and A. Mann, Powerful p-groups, I: Finite groups, *J. Algebra* **105** (1987), 484–505.

[7] M.S. Lucido and M.R. Pournaki, Elements with square roots in finite groups, *Algebra Colloq.* **12** (2005), 677–690.

[8] A.I. Malcev, Homomorphisms onto finite groups, *Ivanov Gos. Ped. Inst. Uchen. Zap. Fiz. Mat. Nauki* **8** (1958), 49–60.

[9] H.N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.