Generating finite soluble groups

by L.G. Kovács and Hyo-Seob Sim

Australian National University, GPO Box 4, Canberra 2601, Australia

ABSTRACT

We prove that if a finite soluble group $G$ can be generated by $s$ subgroups with pairwise coprime orders, each of these subgroups being generatable by $r$ elements, then $G$ itself can be generated by $r+s-1$ elements. No stronger conclusion can hold in general: we construct such groups, even with $s-1$ of the relevant subgroups actually cyclic, which cannot be generated by fewer than $r+s-1$ elements. We also show that if a finite soluble group $G$ has a family of $d$-generator subgroups whose indices have no common divisor, then $G$ can be generated by $d+1$ elements.

Let $d$ be a positive integer, $G$ a finite soluble group, $U$ a simple $G$-module, $C_G(U)$ the kernel of the action of $G$ on $U$, and $D_G(U)$ the intersection of the normal subgroups $N$ of $G$ such that $C_G(U)/N$ is $G$-isomorphic to $U$. The quotient $C_G(U)/D_G(U)$ is known as the crown of $G$ corresponding to (the isomorphism type of) $U$; as $G$-module, this crown is a direct sum of isomorphic copies of $U$, with the number of summands called the $U$-rank of $G$. Of course $U$ is finite and its ring of $G$-endomorphisms is a finite field: call the dimension of $U$ over that field the absolute dimension of $U$. It is an immediate consequence of two theorems of Gaschütz (Satz 4.1 of [2] and Satz 4 of [1]) that $G$ can be generated by $d+1$ elements if and only if the $U$-rank of $G$ is at most $d+1$ whenever $G$ acts trivially on $U$ and at most $d$ times the absolute dimension of $U$ when the action on $U$ is nontrivial. Since the absolute dimension of $U$ is also the multiplicity of $U$ as direct summand in the largest semisimple quotient of the regular $G$-module over the relevant prime field, this conclusion may also be phrased as follows.
LEMMA. \textit{A finite soluble group} \( G \) \textit{can be generated by} \( d + 1 \) \textit{elements if and only if} \( G/G' \) \textit{can be so generated and each crown of} \( G \) \textit{on which} \( G \) \textit{acts non-trivially can be generated (as} \( G \)-\textit{module}) \textit{by} \( d \) \textit{elements.}

Our aim here is to draw attention to another consequence of these ideas of Gaschütz. It answers a question which had been put to us by Professor Luis Ribes, and shows that the Grushko-Neumann Theorem has no simple analogue in the context of pro-(finite soluble) groups; for a discussion of the relevant issues, see Ribes and Wong \cite{6}.

**Theorem 1.** \textit{If a finite soluble group} \( G \) \textit{is generated by} \( s \) \textit{subgroups of pairwise coprime orders, and if each of these subgroups can be generated by} \( r \) \textit{elements, then} \( G \) \textit{can be generated by} \( r + s - 1 \) \textit{elements.}

**Proof.** If \( G \) \textit{satisfies the hypotheses, so does every homomorphic image of} \( G \). The claim is obvious when \( r = 1 \) or \( s = 1 \), and also when \( G \) \textit{is abelian}. In view of the Lemma, it suffices therefore to show that the crown of \( G \) corresponding to an arbitrarily chosen nontrivial \( U \) \textit{can be generated (as module) by} \( r + s - 2 \) \textit{elements}. In doing so, we may replace \( G \) \textit{by its quotient modulo} \( D_G(U) \) \textit{or, more conveniently, assume that} \( D_G(U) = 1 \). Write \( C \) for \( C_G(U) \). By Satz 5.1 of Gaschütz \cite{2}, \( C \) \textit{is then complemented in} \( G \); let \( K \) \textit{denote one of its complements, and} \( p \) \textit{the unique prime divisor of the order of} \( C \). Let \( H_1, \ldots, H_s \) \textit{be the subgroups provided by the hypothesis; arrange the listing of these subgroups so that} \( H_2, \ldots, H_s \) \textit{are all} \( p' \)-\textit{groups. If} \( H \) \textit{is a Hall} \( p' \)-	extit{subgroup of} \( K \), \textit{it is also a Hall subgroup of} \( G \), \textit{so each of} \( H_2, \ldots, H_s \) \textit{has} \( G \)-\textit{conjugates contained in} \( H \); \textit{therefore they have} \( C \)-\textit{conjugates contained in} \( K \). On replacing \( K \) \textit{by a conjugate if necessary, one can arrange that one of these subgroups,} \( H_2 \) \textit{say, is actually contained in} \( K \). That done, for \( i = 3, \ldots, s \) \textit{choose elements} \( c_i \) \textit{in} \( C \) \textit{so that} \( H_i^{c_i} \leq K \). Finally, \textit{choose a family of} \( r \) \textit{elements to generate} \( H_1 \), and \textit{write these elements as} \( x_1 y_1, \ldots, x_r y_r \) \textit{with} \( x_j \in K, y_j \in C \). Then \( G \) \textit{is clearly generated by} \( H_1, H_2, H_3^{c_1}, \ldots, H_s^{c_{s-1}}, c_3, \ldots, c_s \), \textit{and hence also by} \( K \) \textit{and} \( y_1, \ldots, y_r, c_3, \ldots, c_s \). \textit{It follows that} \( G \) \textit{is the product of} \( K \) \textit{with the} \( G \)-\textit{submodule of} \( C \) \textit{generated by the} \( r + s - 2 \) \textit{elements last listed. As} \( K \) \textit{and} \( C \) \textit{intersect trivially, that submodule must therefore be} \( C \) \textit{itself, and so we see that} \( C \) \textit{can be generated by the required number of elements.}

Given positive integers \( r \) and \( s \), it is not hard to construct examples, even with \( H_1, \ldots, H_{s-1} \) cyclic, such that \( G \) \textit{cannot be generated by fewer than} \( r + s - 1 \) \textit{elements}. When \( s = 1 \) \textit{there is nothing to do, and the case of} \( r = 1 \) \textit{will be left to the reader. In the remaining case, let} \( p_1, \ldots, p_s \) \textit{be distinct primes, and} \( q \) \textit{a prime which is congruent to} \( 1 \) \textit{modulo} \( p_1 \cdots p_{s-1} p_s^2 \). \textit{Further, let} \( E \) \textit{be an extraspecial group of order} \( p_s^{r+1} \) \textit{when} \( r \) \textit{is even, or the central product of a cyclic group of order} \( p_s^2 \) \textit{with an extraspecial group of order} \( p_s^r \) \textit{when} \( r \) \textit{is odd. For} \( i = 1, \ldots, s-1 \), \textit{let} \( H_i \) \textit{be a group of order} \( p_i \) \textit{generated, say, by} \( h_i \). \textit{The direct product} \( H_1 \times \cdots \times H_{s-1} \times E \) \textit{then has a faithful simple module} \( U \) \textit{of order}
Any such \( U \) is absolutely simple even as \( E \)-module; the \( h_i \) and the central elements of \( E \) act on it as scalars or, in multiplicative terminology, as powering automorphisms. Let \( W \) be the direct product of \((r + s - 2)[r/2]\) copies of such a \( U \), and \( \{w_1, \ldots, w_{r+s-2}\} \) an \( E \)-module generating set for it. Form \( G \) as the semidirect product of \( W \) with the direct product acting on it, and let \( H_s \) be the subgroup generated by \( E \) and \( w_s, \ldots, w_{r+s-2} \). Using the Lemma, it is easy to see that \( H_s \) can be generated by \( r \) elements, and that \( G \) cannot be generated by fewer than \( r + s + 1 \) elements: so we shall be done if we show that \( H_s, H_{s+1}, H_s \) together generate \( G \). Let \( h_s \) be a nontrivial element in the centre of \( E \); for \( i = 1, \ldots, s \), let \( k_i \) be an integer such that the action of \( h_i \) on \( U \) is given by \( h_i: u \mapsto u^{k_i} \); note that \( k_i \not\equiv 1 \pmod{q} \). The outstanding claim now follows from

\[
[h_i^{w_i}, h_s] = [h_i, [h_i, w_i], h_s] = [w_i^{1-k_i}, h_s] = w_i^{(1-k_i)(k_i-1)}.
\]

The hypothesis of Theorem 1 may be seen as a weakening of the hypothesis of Theorem 2 in [4], which asserts that if each Sylow subgroup of a finite soluble group can be generated by \( d \) elements then the group itself can be generated by \( d + 1 \) elements. The examples just constructed show that Theorem 1 cannot be strengthened to provide a generalization of that result. Instead, one can readily establish the following.

**THEOREM 2.** If a finite soluble group \( G \) has a family of \( d \)-generator subgroups whose indices have no common divisor, then \( G \) can be generated by \( d + 1 \) elements.

The proof begins like that of Theorem 1, with a reduction to the consideration of \( C = C_1(U) \) for some \( U \) such that \( D(U) = 1 \), and of a complement \( K \) of \( C \) in \( G \). The coprimality assumption then ensures that one of the \( d \)-generator subgroups, \( H \) say, contains \( C \). In view of the Lemma, it will suffice to prove that \( C \) can be generated by \( d \) elements as \( H \)-module. By Nakayama's Lemma, this will follow if we show it for the largest semisimple quotient of \( C \) instead. Given a simple \( H \)-module \( V \), let \( M \) denote the intersection of those normal subgroups \( N \) of \( H \) which are contained in \( C \) and such that \( C/N \) is \( H \)-isomorphic to \( V \). The proof will be completed by showing that, for every choice of \( V \), the \( H \)-module \( C/M \) can be generated by \( d \) elements. To this end, note first that \( H \cap K \) complements \( C \) in \( H \), and that \( C_{H \cap K}(V) \) is normal in \( H \cap K \): thus \( C_{H \cap K}(V)N/N \) is normalized by \( (H \cap K)N/N \). Of course it is also centralized by \( C/N \), so it is normal in \( H/N \). Thus \( C_{H \cap K}(V)N \) is normal in \( H \), and by an isomorphism theorem \( C_H(V)/C_{H \cap K}(V)N \) is \( H \)-isomorphic to \( C/N \) and hence to \( V \). It follows first that \( C_{H \cap K}(V)N \subseteq D_H(V) \), and then that \( M \subseteq C \cap D_H(V) \). Another appeal to an isomorphism theorem now yields that \( C/M \) is \( H \)-isomorphic to a section of the crown of \( H \) corresponding to \( V \). By our Lemma, that crown can be generated by \( d \) elements; hence so can \( C/M \), and we are done.

In conclusion, we note that recently the solubility hypothesis has been re-
moved from Theorem 2 of [4] by Lucchini [5] and Guralnick [3]. One is therefore encouraged to ask: can it also be removed from our theorems? Further, using that a nontrivial simple module can never have order 2, it is easy to see that Theorem 2 of [4] remains valid even if the Sylow 2-subgroup is allowed \( d + 1 \) generators; does that slight generalization also survive the omission of the solubility hypothesis?

REFERENCES