THE GENERATION OF THE LOWER CENTRAL SERIES

P. X. GALLAGHER

1. Introduction. Let G be a finite group with commutator subgroup G'. In an earlier paper **(4)** it was shown that each element of G' is a product of n commutators, if $4^n \geqslant |G'|$. The object of this paper is to improve this result in two directions:

THEOREM 1a. *If $(n + 2)!\,n! > 2|G'| - 2$, then each element of G' is a product of n commutators.*

THEOREM 1b. *If G is a p-group, with $|G'| = p^a$, and if $n(n + 1) > a$, then each element of G' is a product of n commutators.*

The rth member $G^{(r)}$ of the lower central series of G is the subgroup generated by the r-fold commutators

$$[\sigma_1, \ldots, \sigma_{r+1}] \qquad (\sigma_1, \ldots, \sigma_{r+1} \in G),$$

defined inductively by

$$[\sigma_1, \ldots, \sigma_{r+1}] = [[\sigma_1, \ldots, \sigma_r], \sigma_{r+1}] \qquad (r > 1),$$
$$[\sigma_1, \sigma_2] = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2, \quad \text{and} \quad [\sigma_1] = \sigma_1.$$

THEOREM 2. *If $n > \sqrt{2^{r-1}/3}\,\log(2|G^{(r)}| - 2)$, then each element of $G^{(r)}$ is a product of n r-fold commutators.*

Let W be a word in s variables $x_1, \ldots, x_s$ and let G_W be the normal subgroup of G generated by the set S_W of all elements of the form

$$W(\sigma_1, \ldots, \sigma_s) \qquad (\sigma_1, \ldots, \sigma_s \in G).$$

Up to a point, the same method which proves Theorem 2 applies to the problem of estimating the least integer n for which $(S_W)^n = G_W$. In §2 this problem is reduced to the estimation of the sums

$$d_\chi = |G|^{-s} \sum_{\sigma_1, \ldots, \sigma_s \in G} \bar{\chi}(W(\sigma_1, \ldots, \sigma_s)) \tag{1}$$

corresponding to the irreducible characters χ of G, and to an elementary extremal problem. In §3 sharp estimates of d_χ are obtained for the cases $W = [x_1, \ldots, x_{r+1}]$ $(r \geqslant 1)$ and in §4 the corresponding extremal problem is considered. In §5 Theorems 1 and 2 are proved and an example is given which shows that the condition on n in Theorem 1b is of the correct order of magnitude.

Received October 22, 1963.

2. Reduction of the problem. Given a finite group G and a word W in s variables, denote by $\phi_n(\sigma)$ the number of ns-tuples (σ_{ij}) of elements of G such that

$$\sigma = W(\sigma_{11}, \ldots, \sigma_{1s}) \ldots W(\sigma_{n1}, \ldots, \sigma_{ns}).$$

Since ϕ_1 is a class-function on G, we have

$$\phi_1 = \sum c_\chi \chi,$$

where χ ranges over the irreducible characters of G, and

$$c_\chi = |G|^{-1} \sum_\rho \phi_1(\rho)\bar{\chi}(\rho) = |G|^{-1} \sum_{\sigma_1, \ldots, \sigma_s} \bar{\chi}(W(\sigma_1, \ldots, \sigma_s)) = |G|^{s-1} d_\chi.$$

For $n > 1$,

$$\phi_n(\sigma) = \sum_\tau \phi_{n-1}(\sigma\tau^{-1})\phi_1(\tau).$$

Since for irreducible characters χ and χ'

$$\sum_\tau \chi(\sigma\tau^{-1})\chi'(\tau) = |G|f_\chi^{-1}\chi(\sigma) \quad \text{or} \quad 0$$

according as $\chi = \chi'$ or not, where f_χ is the degree of χ, it follows by induction on n that

$$\phi_n(\sigma) = |G|^{n-1+n(s-1)} \sum_\chi (d_\chi/f_\chi)^n f_\chi \chi(\sigma).$$

Now suppose that $\sigma \notin (S_W)^n$. Since

$$1 \in S_W \subset (S_W)^2 \subset \ldots \subset (S_W)^n,$$

we have $\phi_m(\sigma) = 0$ for $1 \leqslant m \leqslant n$, and also $\sum f_\chi \chi(\sigma) = 0$. This proves that

$$\sum_\chi (d_\chi/f_\chi)^m f_\chi \chi(\sigma) = 0 \text{ if } \sigma \notin (S_W)^n \qquad (0 \leqslant m \leqslant n). \tag{2}$$

For the case $W = [x_1, x_2]$, $d_\chi = f_\chi^{-1}$, this formula was given by Burnside (**2**, p. 319).

Since $\chi(\sigma) \leqslant f_\chi$ for all $\sigma \in G$, we have $|d_\chi| \leqslant f_\chi$; we have $|d_\chi| = f_\chi$

$$\Leftrightarrow \chi|S_W \text{ is constant}$$

$$\Leftrightarrow \chi \text{ is a character of } G/G_W$$

$$\Leftrightarrow d_\chi = f_\chi.$$

Therefore, for $\sigma \in G_W$,

$$\sum_{d_\chi = f_\chi} f_\chi \chi(\sigma) = \sum_{d_\chi = f_\chi} f_\chi^2 = (G : G_W),$$

and

$$\sum_{d_\chi \neq f_\chi} |f_\chi \chi(\sigma)| \leqslant \sum_{d_\chi \neq f_\chi} f_\chi^2 = |G| - (G : G_W),$$

and consequently

$$\sum_{d_\chi \neq f_\chi} |f_\chi \chi(\sigma)| \leqslant (|G_W| - 1) \sum_{d_\chi = f_\chi} f_\chi \chi(\sigma) \quad \text{if } \sigma \in G_W, \tag{3}$$

https://doi.org/10.4153/CJM-1965-041-5 Published online by Cambridge University Press

Denote by $\lambda_0, \lambda_1, \ldots$ the sequence of distinct values of d_χ/f_χ, arranged so that $1 = \lambda_0 > |\lambda_1| \geqslant |\lambda_2| \geqslant \ldots$. Denote by $a_i = a_i(\sigma)$ the coefficient of λ_i^m in (2). Then for $\sigma \in G_W - (S_W)^n$,

$$(2') \qquad \sum_{i\geqslant 0} a_i \lambda_i^m = 0 \qquad (0 \leqslant m \leqslant n),$$

$$(3') \qquad \sum_{i\geqslant 1} |a_i| \leqslant a_0(|G_W| - 1).$$

Denote by $A_n = A_n(\lambda_1, \lambda_2, \ldots)$ the greatest lower bound of $\sum_{i\geqslant 1} |a_i|$, where the a_i now are subject only to (2′) with the normalization $a_0 = 1$. Then

LEMMA 1. *If $A_n > |G_W| - 1$, then $(S_W)^n = G_W$.*

3. An upper bound for d_χ. In this section

$$d_{\chi,r} = |G|^{-(r+1)} \sum \bar{\chi}([\sigma_1, \ldots, \sigma_{r+1}])$$

is estimated for $r \geqslant 0$. Since $[\sigma_1] = \sigma_1$, $d_{\chi,0} = 1$ or 0 according as $\chi = 1$ or $\chi \neq 1$. Let $\chi\bar{\chi} = \sum b_{\chi\psi}\, \psi$. Using

$$\sum_\tau \chi(\sigma^{-1}\tau^{-1}\sigma\tau) = |G| f_\chi^{-1} \bar{\chi}(\sigma)\chi(\sigma),$$

we have, for $r \geqslant 0$,

$$(4) \qquad d_{\chi,r+1} = f_\chi^{-1} \sum b_{\chi\psi}\, d_{\psi,r}.$$

Since $b_{\chi 1} = 1$ and $b_{\chi\psi} \geqslant 0$ for all ψ, this shows that $d_{\chi,1} = f_\chi^{-1}$ and $d_{\chi,r} > 0$ for $r \geqslant 1$.

Denote by μ_r the maximum of $d_{\chi,r}/f_\chi$, where χ ranges over the characters for which $d_{\chi,r} \neq f_\chi$.

LEMMA 2. *If p is the smallest prime divisor of $|G|$, then*

$$\mu_r \leqslant 1 - \left(1 + \frac{1}{p}\right)\left(1 - \frac{1}{p}\right)^r \qquad (r \geqslant 1).$$

Proof. If ψ is not a character of $G/G^{(r)}$, then $d_{\psi,r} \leqslant \mu_r f_\psi$, while if ψ is a character of $G/G^{(r)}$, then $d_{\psi,r} = f_\psi$. Since $\sum b_{\chi\psi} f_\psi = f_\chi^2$, we have

$$(5) \qquad \begin{aligned} \sum b_{\chi\psi}\, d_{\psi,r} &\leqslant \sum{}' b_{\chi\psi} f_\psi + (f_\chi^2 - \sum{}' b_{\chi\psi} f_\psi)\mu_r \\ &= f_\chi^2 \mu_r + (1 - \mu_r) \sum{}' b_{\chi\psi} f_\psi, \end{aligned}$$

where the prime denotes that the sum is over the characters ψ of $G/G^{(r)}$. Since $(\psi, 1)_{G^{(r)}} = f_\psi$ or 0 according as ψ is a character of $G/G^{(r)}$ or not,

$$(6) \qquad \sum{}' b_{\chi\psi} f_\psi = (\chi\bar{\chi}, 1)_{G^{(r)}} = (\chi, \chi)_{G^{(r)}}.$$

A theorem of A. H. Clifford **(3)** shows that $\chi|G^{(r)} = a \sum \xi_i$, where a is a positive integer and the ξ_i range over the t distinct G-conjugates of a certain irreducible character ξ of $G^{(r)}$. If χ is not a character of $G/G^{(r+1)}$, then $\chi|G^{(r)}$ is not a multiple of a single linear character, so $tf_\xi^2 \geqslant p$, or using $f_\chi = atf_\xi$,

$$(7) \qquad (\chi, \chi)_{G^{(r)}} = a^2 t \leqslant f_\chi^2\, p^{-1}.$$

Combining (4), (5), (6), (7), if χ is not a character of $G/G^{(r+1)}$, then

$$d_{\chi,r+1} \leqslant f_\chi \mu_r + (1 - \mu_r) f_\chi p^{-1} = (p^{-1} + (1 - p^{-1})\mu_r) f_\chi,$$

showing that

$$\mu_{r+1} \leqslant \frac{1}{p} + \left(1 - \frac{1}{p}\right)\mu_r.$$

The statement of the lemma now follows by induction on r, starting with $\mu_1 \leqslant p^{-2}$.

For each r and p, Lemma 2 is "best possible." Let q be a prime such that p divides $q - 1$ and let ν be an integer of order p (mod q). Let G be the split extension of Z_q by Z_p, a generator of Z_p acting on Z_q by raising each element of Z_q to the νth power. Then $G^{(1)} = G^{(2)} = \ldots = Z_q$, and each character of G has degree 1 or p. Each of the characters χ of degree p is induced by a linear character of Z_q, so there is equality in (7). It is now easily shown by induction on r that $d_{\chi,r}/p = \mu_r$ for each character χ of degree p, and there is equality in the statement of Lemma 2.

4. A lower bound for A_n. Let $1 = \lambda_0 > \lambda_1 > \ldots$ be a finite sequence of positive numbers and let A_n be as defined at the end of §2.

LEMMA 3.

$$A_n \geqslant \prod_{i=1}^{n} (\lambda_i^{-1} - 1); \qquad A_n \geqslant \tfrac{1}{2}\exp(2n\sqrt{1 - \lambda_1}).$$

Proof. The conditions (2′) together with the normalization $a_0 = 1$ are equivalent to the condition that for each nth degree polynomial $p(x)$,

$$p(1) = -\sum_{j\geqslant 1} a_j p(\lambda_j). \tag{8}$$

To prove the first estimate, put

$$p(x) = \prod_{i=1}^{n} (x - \lambda_i).$$

We have $p(\lambda_j) = 0$ for $1 \leqslant j \leqslant n$ and $|p(\lambda_j)| \leqslant \lambda_1 \ldots \lambda_n$ for $j > n$, so by (8),

$$\prod_{i=1}^{n} (1 - \lambda_i) \leqslant \left(\sum_{j>n} |a_j|\right) \prod_{i=1}^{n} \lambda_i,$$

which implies the first estimate.

To prove the second estimate, consider the renormalized nth degree Tchebychev polynomial

$$Q_n(y) = \tfrac{1}{2}\{(y + \sqrt{y^2 - 1})^n + (y - \sqrt{y^2 - 1})^n\}.$$

It is known that $|Q_n(y)| \leqslant 1$ for $|y| \leqslant 1$ (**1**, p. 58). Therefore

$$p(x) = Q_n((2x/\lambda_1) - 1)$$

https://doi.org/10.4153/CJM-1965-041-5 Published online by Cambridge University Press

satisfies $|p(x)| \leqslant 1$ for $0 \leqslant x \leqslant \lambda_1$, so (8) implies that

$$A_n \geqslant Q_n((2/\lambda_1) - 1). \tag{9}$$

Substituting $y = (2/\lambda_1) - 1$,

$$y + \sqrt{y^2 - 1} = (1 + \sqrt{1 - \lambda_1})/(1 - \sqrt{1 - \lambda_1}) \geqslant \exp(2\sqrt{1 - \lambda_1}),$$

which proves the second estimate.

5. Proof of Theorems 1 and 2. An example. Denote by $f_0, f_1, \ldots$ the distinct degrees of the irreducible characters of G arranged in increasing order. For $W = [x_1, x_2]$, $\lambda_i = f_i^{-2}$ in the notation of §2, so using Lemma 3,

$$A_n \geqslant \prod_{i=1}^{n} (f_i^2 - 1) \geqslant \prod_{i=1}^{n} ((i + 1)^2 - 1) = \tfrac{1}{2}(n + 2)!\, n!.$$

If G is a p-group, the f_i are powers of p so

$$A_n \geqslant \prod_{i=1}^{n} (f_i^2 - 1) \geqslant \prod_{i=1}^{n} (p^{2i} - 1) > \tfrac{1}{2}p^{n(n+1)}.$$

If $|G'| = p^a$, then $\frac{1}{2}p^{n(n+1)} > |G'| - 1$ is equivalent with $n(n + 1) > a$. Considering Lemma 1, this completes the proof of Theorem 1.

For $W = [x_1, \ldots, x_{r+1}]$, $\lambda_1 = \mu_r$ in the notation of §2 and §3, so using Lemmas 3 and 2,

$$A_n \geqslant \tfrac{1}{2}\exp(2n\sqrt{1 - \mu_r}) \geqslant \tfrac{1}{2}\exp(2n\sqrt{3/2^{r+1}}).$$

Thus if

$$n > \sqrt{2^{r-1}/3}\,\log(2|G^{(r)}| - 2),$$

then $A_n > |G^{(r)}| - 1$, and by Lemma 1 each element of $G^{(r)}$ is a product of n r-fold commutators. This completes the proof of Theorem 2.

The following example, suggested by one of I. D. Macdonald (**5**, p. 139), shows that the bound in Theorem 1b is of the correct order of magnitude. Let p be a prime number and let N be a positive integer. Consider the group G with generators σ_i $(1 \leqslant i \leqslant N)$ and defining relations

$$\sigma_i^p = [\sigma_i, \sigma_j]^p = [\sigma_i, \sigma_j, \sigma_k] = 1 \qquad (1 \leqslant i, j, k \leqslant N).$$

Then $G' = Z(G)$ is an elementary abelian p-group with basis

$$[\sigma_i, \sigma_j] \ (1 \leqslant i < j \leqslant N),$$

and G/G' is an elementary abelian p-group with basis $\sigma_i G'$ $(1 \leqslant i \leqslant N)$. Since the commutator of two elements depends only on their cosets mod $Z(G)$, there are at most $(G{:}Z(G))^2$ distinct commutators. Therefore, if each element of G' is a product of n commutators, then $(G{:}Z(G))^{2n} \geqslant |G'|$, or since $(G{:}Z(G)) = p^N$ and $|G'| = p^{N(N-1)/2}$, we must have $n \geqslant (N - 1)/4$, and therefore $n(n + 1) > a/8$.

References

1. N. I. Achieser, *Theory of approximation* (New York, 1956).
2. W. Burnside, *Theory of groups of finite order* (Cambridge, 1911).
3. A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. *38* (1937), 533–50.
4. P. X. Gallagher, *Group characters and commutators*, Math. Z., *79* (1962), 122–6.
5. I. D. Macdonald, *On a set of normal subgroups*, Proc. Glasgow Math. Assoc., *5* (1962), 137–46.

Columbia University, New York