Can. J. Math., Vol. XXIII, No. 3, 1971, pp. 426–438

MAXIMAL ABELIAN SUBGROUPS OF THE SYMMETRIC GROUPS

JOHN D. DIXON

0. Introduction. Our aim is to present some global results about the set of maximal abelian subgroups of the symmetric group S_n. We shall show that certain properties are true for "almost all" subgroups of this set in the sense that the proportion of subgroups which have these properties tends to 1 as $n \to \infty$. In this context we consider the order and the number of orbits of a maximal abelian subgroup and the number of generators which the group requires.

Earlier results of this kind may be found in the papers [**1**; **2**; **3**; **4**; **5**]; the papers of Erdös and Turán deal with properties of the set of elements of S_n. The present work arose out of a conversation with Professor Turán who posed the general problem: given a specific class of subgroups (e.g., the abelian subgroups or the solvable subgroups) of S_n, what kind of properties hold for almost all subgroups of the class? It turns out that the class of maximal abelian subgroups is one of the easiest to deal with because of the simple structure of these groups (Lemma 6).

Our main results are given in Theorems 1 to 4 in Sections 1 and 2, although some of the subsidiary results of Section 1 throw interesting light on the structure of transitive abelian groups. Some of our results are rather surprising in view of the work of Erdös and Turán. For example, almost all maximal abelian subgroups of S_n have their orders "close" to $n - 1$ which is the smallest possible value (see Theorem 3 and the remark following Lemma 6), whilst according to [**3**], almost all elements of S_n have order "close" to $\exp\{\frac{1}{2}(\log n)^2\}$ which grows much faster than n. We also show that maximal abelian subgroups usually have few orbits and require few generators (Theorem 4), and show that the average number of generators required for a transitive abelian subgroup of S_n is bounded independently of n (Theorem 1); and we give estimates for the numbers of transitive abelian subgroups and maximal abelian subgroups of S_n (Theorems 1 and 2).

Notation. We use the notation $u_n \ll v_n$ to imply that there exists an absolute constant $c > 0$ such that $u_n \leqq cv_n$ for all values of n considered. Similarly, all the implied constants in O- and o- notation will be absolute constants.

1. Transitive abelian subgroups. Let t_n denote the number of transitive abelian subgroups of S_n. It is well known that a transitive abelian subgroup

Received July 23, 1970. This research was partially supported by the National Research Council of Canada Grant A7171.

of S_n is regular and hence of order n, and that it is its own centralizer and hence a maximal abelian subgroup (see [**8**, § 10.3]). Let $\mathscr{G}_n$ be a set of groups consisting of exactly one isomorphic copy of each abelian group of order n.

LEMMA 1. $t_n = (n-1)! \sum |\mathrm{Aut}\, A|^{-1}$, *where the sum is over all* $A \in \mathscr{G}_n$ *and* $|\mathrm{Aut}\, A|$ *denotes the order of the automorphism group of* A.

Proof. It is enough to show that if t_A is the number of transitive subgroups of S_n isomorphic to A, then

$$t_A = (n-1)!\, |\mathrm{Aut}\, A|^{-1} \text{ for all } A \in \mathscr{G}_n.$$

We shall first show that any two regular subgroups H, G of S_n which are isomorphic are conjugate in S_n. Let $x \mapsto x'$ denote the isomorphism $H \to G$. Since H and G are regular, the images 1^x $(x \in H)$ and $1^{x'}$ $(x' \in G)$ of the symbol 1 both run over the whole set $\{1, 2, \ldots, n\}$ exactly once. (S_n is taken to consist of all permutations of $\{1, 2, \ldots, n\}$). Thus we can define $w \in S_n$ by $1^{xw} = 1^{x'}$ $(x \in H)$. We now claim that $w^{-1}xw = x'$ for all $x \in H$. Indeed, for each symbol i we can choose $u' \in G$ such that $i = 1^{u'}$. Then $i^{w^{-1}xw} = (1^{u'w^{-1}})^{xw} = 1^{(ux)w} = 1^{u'x'} = i^{x'}$, since $(ux)' = u'x'$ by the isomorphism property. Since this holds for all i, $1 \leqq i \leqq n$, we have $w^{-1}xw = x'$. This is true for all $x \in$ H and so $w^{-1}Hw = G$ as asserted.

Now without loss in generality we may suppose that $A \in \mathscr{G}_n$ is a transitive abelian subgroup of S_n. As we noted at the beginning of this section, such a subgroup is regular. Thus, all the transitive abelian subgroups of S_n isomorphic to A are conjugate to A in S_n by what we just proved. Therefore t_A equals the index $|S_n{:}N(A)|$ of the normalizer of A in S_n. Moreover, as we noted above, A is its own centralizer in S_n, and so $N(A)/A \simeq \mathrm{Aut}\, A$ (see [**7**, § 13]). Thus $t_A = |S_n|/|N(A)| = n!/n|\mathrm{Aut}\, A| = (n-1)!\, |\mathrm{Aut}\, A|^{-1}$.

We define $f(n) = n^2 t_n/n! = n \sum |\mathrm{Aut}\, A|^{-1}$, summed over $A \in \mathscr{G}_n$. If $n = p_1^{k_1} \ldots p_s^{k_s}$ is the canonical prime factorization of n, then

$$|\mathrm{Aut}\, A| = |\mathrm{Aut}\, A_1| \ldots |\mathrm{Aut}\, A_s|$$

where A_i is the Sylow p_i-group of A, since the A_i are characteristic subgroups of A. Moreover, as the A_i range over $\mathscr{G}_{p_i^{k_i}}$ $(i = 1, \ldots, s)$, the direct product $A_1 \times \ldots \times A_s$ ranges over a complete set of non-isomorphic abelian groups of order n. Hence we conclude that

$$(1) \qquad f(n) = \prod_{i=1}^{s} f(p_i^{k_i}) \quad \text{when } n = p_1^{k_1} \ldots p_s^{k_s};$$

that is, f is multiplicative.

We now consider the value of $f(p^k)$ for a prime p.

LEMMA 2. *Let* A *be an abelian* p*-group of type* $(m_1, \ldots, m_r)$. *This means that* A *is a direct product of cyclic groups of orders* $p^{m_1}, \ldots, p^{m_r}$, *respectively.*

(*A requires r generators and we say A is of rank r*). *Then*

$$|\mathrm{Aut}\, A| = p^{n_A} \prod_{i=1}^{r} (1 - p^{-i}) \quad \text{where}$$

$$n_A = \sum_{i,j=1}^{r} \min(m_i, m_j).$$

Proof. Let H_{ij} denote the additive group of all homomorphisms of a cyclic group of order p^{m_i} into a cyclic group of order p^{m_j}; it is easily seen that $|H_{ij}| = p^{\min(m_i, m_j)}$. It is known (see [**7**, § 21]) that the ring E of endomorphisms of A is isomorphic to the ring of $r \times r$ matrices with (i, j)th entry from $H_{ij} (i, j = 1, \ldots, r)$; we can define a natural matrix sum and product in E because we can define addition in H_{ij} and composition between elements of H_{ij} and elements of H_{jk}. Note that $\mathrm{Aut}\, A$ is the group of units of E. Consider the ideal $J = pE$ of E. Clearly J is nilpotent since $p^h E = 0$ when

$$h = \max(m_1, \ldots, m_r).$$

Moreover E/J is isomorphic to the ring of all $r \times r$ matrices whose (i, j)th entry lies in H_{ij}/pH_{ij}, and this ring is isomorphic to the ring $\mathrm{M}(r, p)$ of all $r \times r$ matrices over a field with p elements. Since J is nilpotent, α is a unit in E if and only if $\alpha + J$ is a unit in E/J. But the group of units of $\mathrm{M}(r, p)$ is the general linear group $\mathrm{GL}(r, p)$ of order $\prod_{i=0}^{r-1} (p^r - p^i)$. Hence the group of units of E/J has this order, and so we conclude that the order of the group of units $\mathrm{Aut}\, A$ of E is

$$\begin{aligned} |\mathrm{Aut}\, A| &= |J| \prod_{i=0}^{r-1} (p^r - p^i) \\ &= \prod_{i,j} |H_{ij}| p^{-r^2} \cdot \prod_{i=0}^{r-1} (p^r - p^i) \\ &= p^{n_A} \prod_{i=1}^{r} (1 - p^{-i}) \end{aligned}$$

since $|H_{ij}| = p^{\min(m_i, m_j)}$.

Remark. This proof also includes some detailed information about the structure of $\mathrm{Aut}\, A$.

LEMMA 3. $f(p^k) < C_p (1 + p^{-4})/(1 - p^{-2})$ *where* $C_p = \prod_{i=1}^{\infty} (1 - p^{-i})^{-1}$.

Proof. Define $h(k, r) = \sum |\mathrm{Aut}\, A|^{-1}$ where the sum is over all $A \in \mathscr{G}_{p^k}$ of rank r. If we go from a group of type $(m_1, \ldots, m_s, 1, \ldots, 1)$ of rank r with all $m_i > 1$ to one of type $(m_1 - 1, \ldots, m_s - 1)$ of rank s, then the corresponding value of n_A in Lemma 2 is decreased by r^2. Thus Lemma 2 implies that

$$h(k, r) \leqq \begin{cases} \sum_{s=1}^{r} h(k - r, s) p^{-r^2} & \text{if } r < k \\ C_p p^{-k^2} & \text{if } r = k \end{cases} \tag{2}$$

Now from Lemma 2, $h(k, 1) < C_p p^{-k}$ and

$$h(k, 2) = \{(1 - p^{-1})(1 - p^{-2})\}^{-1} \sum_{1 \leqq j \leqq \frac{1}{2}k} p^{-(k-j)-3j} < C_p p^{-k-2}(1 - p^{-2})^{-1}.$$

We shall use (2), and induction on $k (k \geqq r)$ to prove that

$$(3) \qquad h(k, r) \leqq C_p p^{-k-2r+2} \text{ for } r \geqq 3.$$

In fact (3) is valid for $k = r$ by (2). On the other hand, if $l > r$ and (3) holds for all $k < l$, then (2) implies that

$$\begin{aligned} h(l, r) &\leqq \sum_{s=1}^{r} h(l - r, s) p^{-r^2} \\ &\leqq C_p p^{-r^2} \left\{ p^{-l+r} + p^{-l+r-2}(1 - p^{-2})^{-1} + \sum_{s=3}^{r} p^{-l+r-2s+2} \right\} \\ &< C_p p^{-l-2r+2} \quad \text{for } r \geqq 3. \end{aligned}$$

This proves the induction step, and so (3) is proved. Finally from these estimates of $h(k, r)$, we have

$$\begin{aligned} f(p^k) &= p^k \sum_{r=1}^{k} h(k, r) \\ &\leqq p^k \left\{ C_p p^{-k} + C_p p^{-k-2}(1 - p^{-2})^{-1} + \sum_{r=3}^{k} C_p p^{-k-2r+2} \right\} \\ &< C_p \frac{1 + p^{-4}}{1 - p^{-2}} \text{ as asserted.} \end{aligned}$$

Remark. It follows directly from this proof that $f(p^k) \geqq f(p) = p/(p - 1)$, for all $k \geqq 1$.

LEMMA 4. *For all $n \geqq 1$, $1 \leqq f(n)\varphi(n)/n < C_0$ where $\varphi(n)$ is the Euler φ-function and C_0 is a constant.* (*We may take*

$$C_0 = \Pi_p\{(1 - p^{-2})^{-2}(1 + p^{-4}) \Pi_{i=3}^{\infty}(1 - p^{-i})^{-1}\}$$

taken over all primes p).

Proof. From (1) and Lemma 3 we have

$$\begin{aligned} f(n) &< \prod_{p|n} C_p \left(\frac{1 + p^{-4}}{1 - p^{-2}} \right) < C_0 \prod_{p|n} (1 - p^{-1})^{-1} \\ &= C_0 n/\varphi(n). \end{aligned}$$

On the other hand, from the remark following Lemma 3, we have

$$f(n) \geqq \prod_{p|n} f(p) = n/\varphi(n).$$

https://doi.org/10.4153/CJM-1971-045-7 Published online by Cambridge University Press

LEMMA 5. *For all n, $f(n) \geqq 1$, and $f(n) = O$ (log log n) as $n \to \infty$. If we define $F(n) = \sum_{k=1}^{n} f(k)$, then $F(n) - F(m) \ll n - m + (\log n)^2$ for all $n \geqq m \geqq 1$.*

Proof. Since $n/\varphi(n) = O(\log \log n)$ (see [**6**, p. 267]), the estimates for $f(n)$ follow from Lemma 4. To prove the second part we note that

$$6\pi^{-2} < n^{-2}\sigma(n)\varphi(n) < 1$$

for all $n \geqq 1$, where $\sigma(n)$ is the sum of the divisors of n (see [**6**, p. 267]). Thus

$$F(n) - F(m) = \sum_{k=m+1}^{n} f(k) < C_0 \sum_{k=m+1}^{n} n/\varphi(n) < \frac{C_0\pi^2}{6} \sum_{k=m+1}^{n} \frac{\sigma(k)}{k}.$$

Now if we define $G(n) = \sum_{k=1}^{n} \sigma(k)$, then $G(n) = \pi^2 n^2/12 + O(n \log n)$ (see [**6**, p. 266]). Therefore

$$\begin{aligned} \sum_{k=m+1}^{n} \frac{\sigma(k)}{k} &= \sum_{k=m+1}^{n} G(k) \left\{\frac{1}{k} - \frac{1}{k+1}\right\} + \frac{G(n)}{n} - \frac{G(m)}{m+1} \\ &= \frac{\pi^2}{12} \left\{\sum_{k=m+1}^{n} \frac{k}{k+1} + n - \frac{m^2}{m+1}\right\} + O\left\{\sum_{k=m+1}^{n} \frac{\log k}{k} + \log n\right\} \\ &= \frac{\pi^2}{6}(n - m) + O(\log n)^2. \end{aligned}$$

Hence we conclude that $F(n) - F(m) \ll n - m + (\log n)^2$ as asserted.

We can now state our first theorem giving global information about the set of transitive abelian subgroups of S_n.

THEOREM 1. *The number t_n of transitive abelian subgroups of S_n lies in the range*

$$\frac{(n-1)!}{\varphi(n)} \leqq t_n < C_0 \frac{(n-1)!}{\varphi(n)}$$

(where C_0 is given in Lemma 4).

The proportion of these subgroups which require more than d generators is $O(4^{-d})$ independently of n; and indeed there exists a constant K_1 such that for all n the average number of generators of a transitive abelian subgroup of S_n is at most K_1.

Proof. The first part of the Theorem follows from Lemma 4 and the definition of $f(n)$. So we consider the second part.

It follows from Lemma 1 and the proof of Lemma 3 that the proportion q_d of transitive abelian subgroups of S_{p^k} which require d generators (that is, have rank d) is $p^k h(k, d)/f(p^k)$. Since $C_2 \geqq C_p$ for all p (see Lemma 3), it follows from the estimates for $h(k, d)$ in Lemma 3 that $q_d < (4/3)\, C_2 p^{-2d+2}$; hence the proportion of transitive abelian subgroups of S_{p^k} requiring more than d generators is $\ll p^{-2d}$ (uniformly in p, k and d). In general, an abelian group requires d generators if and only if at least one Sylow p-group requires d generators. But if A is a transitive abelian subgroup of S_n, and A_1 is a Sylow p-group of order p^k, then A_1 has a faithful (transitive) representation on each of its orbits (of length p^k). Thus the proportion of transitive abelian subgroups of S_n which require more than d generators is $\ll \sum_{p|n} p^{-2d} \ll 2^{-2d} = 4^{-d}$ as asserted.

The last assertion of the Theorem follows immediately, since $\sum_{d=1}^{\infty} 4^{-d}$ is finite.

2. Maximal abelian subgroups. We begin by characterizing the maximal abelian subgroups of S_n. It turns out that these subgroups have an especially simple structure (part (b) of Lemma 6), and it is this that makes our subsequent analysis relatively easy.

We shall need the following notation. If A is a subgroup of S_n and $\Omega_i \subseteq \{1, 2, \ldots, n\}$ is an orbit of A, then $A|\Omega_i$ will denote the group of restrictions $a|\Omega_i$ of a to Ω_i ($a \in A$). Note that $A|\Omega_i$ is embedded in a natural way in S_n as a subgroup fixing all symbols not in Ω_i.

LEMMA 6. *Let A be an abelian subgroup of S_n and let $\Omega_1, \ldots, \Omega_k$ be the orbits of A with lengths $n_1, \ldots, n_k$, respectively. Then A is a maximal abelian subgroup of S_n if and only if*

(a) *at most one $n_i = 1$; and*

(b) *$A = A|\Omega_1 \times \ldots \times A|\Omega_k$ (direct product), and so*

$$|A| = |A|\Omega_i| \ldots |A|\Omega_k| = n_1 \ldots n_k.$$

Proof. First, suppose that (a) did not hold. Then $n_i = n_j = 1$, say, and the transposition interchanging the symbols in Ω_i and Ω_j centralizes A. Hence A could not be maximal. Similarly, $A|\Omega_i \times \ldots \times A|\Omega_k$ is an abelian subgroup of S_n, and it contains A, so if (b) did not hold A could not be maximal. Thus (a) and (b) are necessary if A is a maximal abelian subgroup.

Conversely, suppose that (a) and (b) hold. To prove A is maximal it is enough to show that A equals its centralizer $C(A)$ in S_n. Let $u \in C(A)$. Then $u \in C(A|\Omega_i)$ by (b), and we claim that when $n_i \neq 1$, this implies that $\Omega_i^u = \Omega_i$. Indeed, let $l \in \Omega_i$ and $1 \neq a \in A|\Omega_i$. Then $l^a = m \neq l$ because $A|\Omega_i$ is regular, and so $l^{ua} = l^{au} = m^u \neq l^u$. Thus l^u is moved by $a \in A|\Omega_i$, and so $l^u \in \Omega_i$. This holds for all $l \in \Omega_i$, and so $\Omega_i^u = \Omega_i$ as claimed. But in the symmetric group on Ω_i, the transitive abelian subgroup $A|\Omega_i$ is maximal and hence its own centralizer, and so $n_i \neq 1$ implies that $u|\Omega_i \in A|\Omega_i$. Since by (a) there is at most one exceptional n_i, we can conclude that $u|\Omega_i \in A|\Omega_i$ for all i. Hence $u \in A$ by (b). Therefore we have shown that $C(A) \subseteq A$, and so A is maximal.

Remark. It is a simple exercise to deduce from this Lemma that for $n \geqq 3$, the smallest order of a maximal abelian subgroup of S_n is $n - 1$, and the largest order is $3^{[n/3]}$, $(4/3)3^{[n/3]}$, or $2.3^{[n/3]}$, depending on whether $n \equiv 0, 1, 2 \pmod 3$.

Let $\mathscr{A}_n$ denote the set of all maximal abelian subgroups of S_n and let $\mathscr{B}_n$ consist of those subgroups in $\mathscr{A}_n$ which have no orbit of length 1. We write a_n and b_n, respectively, to denote the orders of these sets. Clearly $a_n = b_n + nb_{n-1}$ by Lemma 6.

LEMMA 7. *We have the following generating functions.*

$$\sum_{n=0}^{\infty} \frac{b_n}{n!} z^n = \exp\left(\sum_{m=2}^{\infty} \frac{f(m)}{m^2} z^m\right) \tag{3}$$

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n = (1+z) \exp\left(\sum_{m=2}^{\infty} \frac{f(m)}{m^2} z^m\right). \tag{4}$$

Proof. (4) follows immediately from (3) and the relation $a_n = b_n + nb_{n-1}$; so consider (3).

The number of subgroups in $\mathscr{B}_n$ for which a fixed symbol 1 lies in an orbit of length k is clearly

$$\binom{n-1}{k-1} t_k b_{n-k} \qquad (k = 2, \ldots, n)$$

by Lemma 6, since there are $\binom{n-1}{k-1}$ possible orbits. Thus

$$b_n = \sum_{k=2}^{n} \binom{n-1}{k-1} t_k b_{n-k},$$

and so

$$\frac{nb_n}{n!} = \sum_{k=2}^{n} \frac{t_k}{(k-1)!} \frac{b_{n-k}}{(n-k)!} = \sum_{k=2}^{n} \frac{f(k)}{k} \frac{b_{n-k}}{(n-k)!}. \tag{5}$$

But if we write

$$\exp\left(\sum_{m=2}^{\infty} \frac{f(m)}{m^2} z^m\right) = \sum_{n=0}^{\infty} \frac{b'_n}{n!} z^n,$$

then upon differentiating and comparing coefficients of z^{n-1} we obtain (5), with b_m' in place of b_m $(m = 0, 1, \ldots, n)$. Since $b_0 = b_0' = 1$, the recursion formula (5) shows that $b_n = b_n'$ for all n. This proves (3).

We now define

$$p_k(n) = \binom{n-1}{k-1} t_k b_{n-k} \Big/ \sum_{j=2}^{n} \binom{n-1}{j-1} t_j b_{n-j}$$

(the "probability" that for a subgroup in $\mathscr{B}_n$ a specified symbol should lie in an orbit of length k). From the proof of Lemma 7 we see that

$$p_k(n) = \frac{f(k)}{k} \frac{b_{n-k}}{(n-k)!} \Big/ \frac{nb_n}{n!} \qquad (k = 2, \ldots, n)$$

and that

$$\sum_{k=2}^{n} p_k(n) = 1.$$

LEMMA 8.

$$\sum_{k=2}^{n} kp_k(n) = \sum_{k=2}^{n} f(k) \frac{b_{n-k}}{(n-k)!} \Big/ \frac{nb_n}{n!}$$
$$= n + O\{\log n \cdot (\log \log n)^2\},$$

and for each n_0, $1 \leqq n_0 \leqq n-2$,

$$\sum_{k=2}^{n-n_0} p_k(n) \ll \frac{1}{n_0} (\log n)(\log \log n)^2.$$

Proof. If we differentiate (3), multiply by z, and differentiate again, we get

$$\sum_{n=1}^{\infty} \frac{n^2 b_n}{n!} z^{n-1} = \left\{\sum_{m=2}^{\infty} f(m) z^{m-1} + z \left(\sum_{m=2}^{\infty} \frac{f(m)}{m} z^{m-1}\right)^2\right\} \exp\left(\sum_{m=2}^{\infty} \frac{f(m)}{m^2} z^m\right).$$

If we substitute (3) into this expression and compare coefficients of z^{n-1} we get

$$\frac{n^2 b_n}{n!} = \sum_{m=2}^{n} f(m) \frac{b_{n-m}}{(n-m)!} + \sum_{m=4}^{n} \sum_{l=2}^{m-2} \frac{f(l)}{l} \frac{f(m-l)}{m-l} \frac{b_{n-m}}{(n-m)!}. \tag{6}$$

Now

$$\sum_{l=2}^{m-2} \frac{f(l)}{l} \frac{f(m-l)}{m-l} \ll (\log \log m)^2 \sum_{l=2}^{m-2} \frac{1}{m} \left(\frac{1}{l} + \frac{1}{m-l}\right)$$
$$\ll \frac{1}{m} (\log \log m)^2 \log m, \text{ using Lemma 5.}$$

Therefore

$$\sum_{m=4}^{n} \sum_{l=2}^{m-2} \frac{f(l)}{l} \frac{f(m-l)}{m-l} \frac{b_{n-m}}{(n-m)!} \ll \log n \cdot (\log \log n)^2 \sum_{m=4}^{n} \frac{1}{m} \frac{b_{n-m}}{(n-m)!}$$
$$\ll \log n \cdot (\log \log n)^2 \frac{nb_n}{n!}$$

for all $n \geqq 4$ by (5), because $f(m) \geqq 1$. Hence we can conclude from (6) that

$$\sum_{m=2}^{n} f(m) \frac{b_{n-m}}{(n-m)!} = \frac{n^2 b_n}{n!} + O\left\{\log n \cdot (\log \log n)^2 \frac{nb_n}{n!}\right\}$$
$$= \frac{nb_n}{n!} \{n + O(\log n \cdot (\log \log n)^2)\}.$$

This proves the first part of the Lemma.

https://doi.org/10.4153/CJM-1971-045-7 Published online by Cambridge University Press

The second part of the Lemma follows from

$$\begin{aligned}\sum_{k=2}^{n-n_0} p_k(n) &\leqq \frac{1}{n_0}\sum_{k=2}^{n-n_0} (n-k)p_k(n) \leqq \frac{1}{n_0}\sum_{k=2}^{n} (n-k)p_k(n) \\ &= \frac{1}{n_0}\left\{n - \sum_{k=2}^{n} p_k(n)\right\} \\ &\ll \frac{1}{n_0}\log n \cdot (\log\log n)^2, \quad \text{for all } n \geqq 3,\end{aligned}$$

from above.

THEOREM 2. *The number a_n of maximal abelian subgroups of S_n lies in the range*

$$\frac{(n-1)!}{\varphi(n)} + \frac{n(n-2)!}{\varphi(n-1)} \leqq a_n \ll (\log\log n)\frac{n!}{n^2}$$

*for all $n \geqq 3$. (Note that the lower bound is always greater than $2n!/n^2$, and is $\gg$ $(\log\log n)n!/n^2$, for infinitely many n (see [**6**, p. 267])).*

Proof. We first claim that $b_n \ll (n+1)^{-3/2}n!$. If this were not so, there would be an increasing sequence of indices $n_k \to \infty$ for which

(7) $$b_{n_k}(n_k+1)^{3/2}/n_k! \geqq b_m(m+1)^{3/2}m!, \text{ for all } m \leqq n_k.$$

But by Lemma 8

$$\frac{n_k^2 b_{n_k}}{n_k!}(1+o(1)) = \sum_{m=0}^{n_k-2} f(n_k - m)\frac{b_m}{m!},$$

and substituting in the inequalities (7) and the estimate $f(l) \ll \log\log l$ of Lemma 5, we get the contradiction

$$n_k^{\frac{1}{2}} \ll \log\log n_k \text{ as } k \to \infty.$$

Thus $b_n \ll (n+1)^{-3/2}n!$. Applying Lemma 8 again we obtain

$$\begin{aligned}\frac{n^2 b_n}{n!}(1+o(1)) &= \sum_{m=2}^{n} f(m)\frac{b_{n-m}}{(n-m)!} \\ &\ll \sum_{m=2}^{n} (\log\log n)(n-m+1)^{-3/2} \\ &\ll \log\log n, \quad \text{for all } n \geqq 3.\end{aligned}$$

This combined with Theorem 1, and the observation that $b_n \geqq t_n$ for all $n \geqq 2$, shows that

(8) $$\frac{(n-1)!}{\varphi(n)} \leqq b_n \ll (\log\log n)\frac{n!}{n^2}.$$

Now the required estimate for a_n comes from the identity $a_n = b_n + nb_{n-1}$.

THEOREM 3. *Let μ_n denote the average of the logarithms of the orders of the maximal abelian subgroups of S_n. Then for each $\epsilon > 0$*

$$\mu_n = \log n + O(\log n)^\epsilon.$$

Moreover, almost all maximal abelian subgroups A of S_n satisfy

$$|\log n - \log|A|| < (\log n)^{\frac{1}{2}+\epsilon}$$

and the proportion of exceptions is $O(\log n)^{-\epsilon}$.

Proof. Let λ_n be the average corresponding to μ_n, but taken over the subgroups in $\mathscr{B}_n$. Clearly

$$\lambda_n = \sum_{k=2}^{n} p_k(n)(\log k + \lambda_{n-k}),$$

and so using Lemma 8, we get

$$\begin{aligned} (9) \qquad \lambda_n &= \sum_{k=n-n_0+1}^{n} p_k(n)(\log k + \lambda_{n-k}) + \sum_{k=2}^{n-n_0} p_k(n)(\log k + \lambda_{n-k}) \\ &\leqq \log n + \sup_{m<n_0} \lambda_m + O\left(\frac{1}{n_0}\log n(\log\log n)^2 \sup_{m<n} \lambda_m\right). \end{aligned}$$

We now claim that $\lambda_n \ll \log n$ for all $n \geqq 2$. If this were not so then there would exist an increasing sequence of indices $n_k \to \infty$ such that

$$\lambda_{n_k}/\log n_k \geqq \lambda_m/\log m, \text{ for } m = 2, \ldots, n_k,$$

and $\lambda_{n_k}/\log n_k \to \infty$.
Then taking $n_0 = [\log n_k]^2$, (9) yields

$$\lambda_{n_k} \leqq \log n_k + \frac{\log\log n_k}{\log n_k}\lambda_{n_k} + O\left\{\frac{(\log\log n_k)^2}{\log n_k}\lambda_{n_k}\right\}.$$

But this implies that $\lambda_{n_k} \ll \log n_k$ as $k \to \infty$, contrary to the choice of n_k. Thus $\lambda_n \ll \log n$ for all $n \geqq 2$. Applying (9) again, with $n_0 = [\exp(\log n)^\epsilon]$, we get

$$\lambda_n \leqq \log n + O(\log n)^\epsilon.$$

Now every subgroup in $\mathscr{A}_n$ is either in $\mathscr{B}_n$ or (discarding the orbit of length 1) corresponds to a subgroup in $\mathscr{B}_{n-1}$. Hence it is clear that μ_n is a weighted average of λ_n and λ_{n-1}; in view of our bound on λ_n, this means that

$$\mu_n \leqq \log n + O(\log n)^\epsilon.$$

Since every maximal subgroup of S_n has order $\geqq n - 1$ (see the remark after Lemma 6), $\mu_n \geqq \log(n - 1) = \log n + O(\log n)^\epsilon$, and so the first part of the Theorem is proved.

https://doi.org/10.4153/CJM-1971-045-7 Published online by Cambridge University Press

To prove the second part we introduce θ_n as the average of $(\log|A|)^2$, taken over all $A \in \mathscr{B}_n$. Again it is clear that

$$\theta_n = \sum_{k=2}^{n} p_k(n)\{(\log k)^2 + 2\lambda_{n-k}\log k + \theta_{n-k}\}.$$

Therefore, using our previous estimate for λ_m and using Lemma 8, we obtain

$$(10)\quad \theta_n \leqq (\log n)^2 + \sup_{m<n_0}\theta_m + O\{\log n\cdot\log n_0 + n_0^{-1}(\log n)^3(\log\log n)^3 + n_0^{-1}\log n\cdot(\log\log n)^2\sup_{m<n}\theta_m\}.$$

By an analysis analogous to that of (9), we can show that $\theta_n \ll (\log n)^2$ for all $n \geqq 2$, and so taking $n_0 = [\log n]^3$ in (10), we get

$$\theta_n \leqq (\log n)^2 + O(\log n\cdot\log\log n).$$

But this together with our estimate $\lambda_n \leqq \log n + O(\log n)^\epsilon$ yields

$$\frac{1}{b_n}\sum(\lambda_n - \log|A|)^2 = \theta_n - \lambda_n^2 \ll (\log n)^{1+\epsilon},$$

where the sum is over all $A \in \mathscr{B}_n$. As before, it may be seen that we can extend the average over $\mathscr{A}_n$ to obtain

$$\frac{1}{a_n}\sum(\lambda_n - \log|A|)^2 \ll (\log n)^{1+\epsilon},$$

where the sum if over all $A \in \mathscr{A}_n$. This in turn implies that the proportion of $A \in \mathscr{A}_n$ which fail to satisfy

$$|\lambda_n - \log|A|| < \tfrac{1}{2}(\log n)^{\frac{1}{2}+\epsilon}$$

is $O(\log n)^{-\epsilon}$. Since $\lambda_n = \log n + O(\log n)^\epsilon$, the second part of the Theorem now follows.

We define the function $\mathrm{L}(n)$ to be the integer $s \geqq 1$ such that $\log_s n \leqq 0 < \log_{s-1} n$ (here, $\log_s$ is the sth iterated logarithm). Note that $\mathrm{L}(n)$ grows very slowly; for example $\mathrm{L}(10^6) = 3$ and $\mathrm{L}(10^{10^6}) = 4$.

LEMMA 9. *Let $\beta > 0$, and let $\alpha_n \geqq 0$ $(n = 1, 2, \ldots)$. If*

$$\alpha_n \leqq \textstyle\sum_{k=2}^{n} p_k(n)(\beta + \alpha_{n-k})$$

for $n = 2, 3, \ldots$, then $\alpha_n \ll \mathrm{L}(n)$ for all n. On the other hand, if

$$\alpha_n \geqq \textstyle\sum_{k=2}^{n} p_k(n)(\beta + \alpha_{n-k})$$

for $n = 2, 3, \ldots$, then $\alpha_n \to \infty$ as $n \to \infty$.

Proof. Suppose that the first series of inequalities holds. Then applying

Lemma 8, with $n_0 = [\log n]^2$, we obtain

$$\alpha_n \leqq \beta + \sum_{k=n-n_0+1}^{n} p_k(n)\alpha_{n-k} + O\{n_0^{-1} \log n \cdot (\log \log n)^2\}$$
$$\leqq \beta' + \sup_{m<(\log n)^2} \alpha_m$$

for all $n \geqq 2$ if we choose β' large enough. Applying this inequality twice we get

$$\alpha_n \leqq 2\beta' + \sup_{m<(2\log \log n)^2} \alpha_m, \quad \text{for all } n \geqq 3. \tag{11}$$

Now $\mathrm{L}([(2 \log \log n)^2]) \leqq \mathrm{L}(n) - 1$, whenever $\log n \geqq (2 \log \log n)^2$, so if we choose $\beta'' > 0$ such that $\beta'' \geqq 2\beta'$, and $\alpha_n \leqq \beta''\mathrm{L}(n)$ for all n with $\log n < (2\log \log n)^2$, then induction with (11) shows that

$$\alpha_n \leqq \beta''\mathrm{L}(n) \text{ for all } n.$$

This proves the first part of the Lemma.

Now suppose that the second series of inequalities holds. Then observing that $p_k(n) \to 0$ as $n \to \infty$ for each fixed k, we conclude that

$$\liminf \alpha_n \geqq \liminf (\beta + \alpha_n)$$

which implies that $\liminf \alpha_n = \infty$; hence $\alpha_n \to \infty$.

THEOREM 4. *Let ω_n and γ_n denote, respectively, the average number of orbits and the average number of generators required by the maximal abelian subgroups of S_n. Then*

(a) $\omega_n \to \infty$ *but* $\omega_n \ll \mathrm{L}(n)$ *for all n;*

(b) $\gamma_n \ll \mathrm{L}(n)$ *for all n.*

Remark. In particular, it follows immediately that for each $\epsilon > 0$ almost all maximal abelian subgroups have fewer than $\mathrm{L}(n)^{1+\epsilon}$ orbits and require fewer than $\mathrm{L}(n)^{1+\epsilon}$ generators.

Proof. It is readily seen that it is enough to prove the corresponding assertions for the averages ω_n' and γ_n' taken over the subgroups in $\mathscr{B}_n$. But clearly $\omega_n' = \sum_{k=2}^{u} p_k(n)(1 + \omega_{n-k}')$, and so (a) follows from Lemma 9. On the other hand, if A and B are groups which require d_A and d_B generators, respectively, then $A \times B$ requires at most $d_A + d_B$ generators. Thus we find that

$$\gamma'_n \leqq \sum_{k=2}^{n} p_k(n)(K_1 + \gamma'_{n-k}),$$

by Theorem 1, and so (b) follows from Lemma 9.

REFERENCES

1. J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. *110* (1969), 199–205.

2. P. Erdös and P. Turán, *On some problems of a statistical group-theory.* II, Acta Math. Acad. Sci. Hun. *18* (1967), 151–163.
3. ——— *On some problems of a statistical group-theory.* III, Acta Math. Acad. Sci. Hung. *18* (1967), 309–320.
4. ——— *On some problems of a statistical group-theory.* IV, Acta Math. Acad. Sci. Hung. *19* (1968) 413–435.
5. ——— *On some problems of a statistical group-theory.* V (to appear).
6. G. H. Hardy and E. Wright, *Introduction to the theory of numbers* (Clarendon Press, Oxford, 1954).
7. A. G. Kurosh, *Theory of Groups*, Vol. 1 (Chelsea, N.Y., 1955).
8. W. Scott, *Group Theory* (Prentice-Hall, N.J., 1964).

Carleton University,
Ottawa, Ontario