*Acta Mathematica Academiae Scientiarum Hungaricae*
*Tomus 19 (3—4), (1968), pp. 413—435.*

# ON SOME PROBLEMS OF A STATISTICAL GROUP-THEORY. IV

By

P. ERDŐS and P. TURÁN (Budapest), members of the Academy

**1.** In this paper we shall continue the statistical investigation of $S_n$, the symmetric group of $n$ letters. Let $P$ be a generic element of $S_n$, and $\mathbf{O}(P)$ its order. In the first paper of this series (see [1]) we proved that the relation*

$$\log \mathbf{O}(P) = \left(\frac{1}{2} + o(1)\right) \log^2 n \tag{1.1}$$

holds in $S_n$, apart from $o(n!)$ $P$'s. This was refined in [2] to a „logarithmic-Gaussian" distribution. The interest of these results is clearly shown by the theorem of E. LANDAU (see [3]) according to which

$$\lim_{n\to\infty} \frac{\max_{P\in S_n} \log \mathbf{O}(P)}{\sqrt{n \log n}} = 1. \tag{1.2}$$

These theorems can obviously be reformulated in terms of the orders of all cyclic subgroups of $S_n$. In this setting it is natural to raise the same question for the *pairwise nonisomorphic* cyclic subgroups of $S_n$. So we have two problems.

I. What is the maximum number of the pairwise nonisomorphic cyclic subgroups of $S_n$?

II. Does there exist a „sharp almost all theorem" for their order too?

These problems are in turn equivalent to the problems, how many *different* values can $\mathbf{O}(P)$ assume and whether or not these values show a behaviour analogous to (1.1). We shall answer these problems by the following two theorems.

THEOREM I. *The number $W(n)$ of different values of $\mathbf{O}(P)$ in $S_n$ is*

$$\exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}. \tag{1.3}$$

THEOREM II. *„Almost all" of the possible different $\mathbf{O}(P)$-values (with $o(W(n))$ exceptions at most) are of the form*

$$\exp\left\{(1+o(1))\frac{\sqrt{6}\log 2}{\pi}\sqrt{n\log n}\right\}. \tag{1.4}$$

* Here and in what follows the $o$ and $O$-signs refer to $n \to +\infty$.

These theorems seem to us of interest for more than one reason. Comparing (1. 3) with the „exact" interval for $\mathbf{O}(P)$ furnished by (1. 2) it turned out that $W(n)$ is very small* and hence there must be „very big" intervals within

$$I: 1 \leqq x \leqq \exp\left\{(1+o(1))\sqrt{n \log n}\right\} \stackrel{\text{def}}{=} M, \tag{1. 5}$$

containing no $\mathbf{O}(P)$-values; this means the nonexistence of certain cyclic subgroups in $S_n$. The *explicit* determination of such intervals seems to us to be of interest. Since $\frac{\sqrt{6}}{\pi} \log 2 \sim 0{,}5404$ the value in (1. 4) is „essentially"

$$M^{0,5404}$$

which is very large compared to the value (1. 1) which is „essentially" only

$$\exp\{2(\log\log M)^2\}.$$

This fact gives obviously an interest to the problem for which $m$ is the number of $P$'s with $\mathbf{O}(P)=m$ maximal and what is the value of this maximum.

For the study of the distribution of the $\mathbf{O}(P)$-values it is of interest to study mean-values of $\mathbf{O}(P)$. We have found that

$$M_1(n) \stackrel{\text{def}}{=} \frac{1}{n!} \sum_{P \in S_n} \mathbf{O}(P) < \exp\left\{c_1 \sqrt{\frac{n}{\log n}}\right\} \tag{1. 6}$$

where $c_1$ — and later $c_2, c_3, \ldots$ — stand for positive numerical, explicitely calculable constants.** Owing to (1. 2) and the quick increase of the function $\exp(\sqrt{x \log x})$ one had the guess for a much larger $M_1(n)$-value. Since we do not have at present an *asymptotically exact* formula for $M_1(n)$ we shall postpone the treatment of this problem to another occasion.

**2.** The statistical point of view leads to transparent laws in different sort of questions too. Such questions are e.g. the study of conjugacy-classes and commutability of elements of $S_n$. So — denoting the total number of conjugacy classes of $S_n$ by $V(n)$ — we assert the

THEOREM III. *The elements $P$ of $S_n$ — with exception of the elements of $o(V(n))$ conjugacy-classes — are commutable exactly with*

$$\exp\left\{(1+o(1))\frac{\sqrt{6}}{4\pi}\sqrt{n}\log^2 n\right\} \tag{2. 1}$$

*$P$'s.*

As an application of this theorem DR. J. DÉNES has communicated us orally the following remarkable theorem.

* A trivial upper bound for $W(n)$ is the number of divisors of $n!$. But this is $> \prod_{\frac{n}{2} < p \leqq n} 2 = 2^{\pi(n)-\pi\left(\frac{n}{2}\right)}$ which is much bigger than the expression in (1.3).

** If some constant depends on certain parameters, this will be always explicitely stated.

For all $P$'s — with exception of the elements of $o(V(n))$ conjugacy classes — the „general commutator-equation"

$$XYX^{-1}Y^{-1}=P \quad (X,\ Y\in S_n) \tag{2.2}$$

has

$$\exp\left\{(1+o(1))\frac{\sqrt{6}}{2\pi}\sqrt{n}\log^2 n\right\} \tag{2.3}$$

solutions.

Dr. Dénes intends to publish his proof elsewhere.

For the „special commutator equation"

$$XYX^{-1}Y^{-1}=E \quad (E \text{ unitelement}) \tag{2.4}$$

the number of solutions* is the number of commutable pairs in $S_n$. As to this we found with Vera T. Sós that this number is

$$n!p(n), \tag{2.5}$$

$p(n)$ being the number of partitions of $n$. More generally we assert the

Theorem IV. *The number of commutable $(a, b)$ pairs (with the convention of the footnote) from an arbitrary group $G$ of order $N$ is $Nk$ where $k$ stands for the number of conjugacy classes in $G$.*

We shall deduce two corollaries from it.

Corollary I. *In an arbitrary group of order $N$ the number of commutable pairs (with the above convention) is at least** $N\log\log N$. By other words a finite group cannot be „too non-commutative".*

Taking into account the Hardy—Ramanujan asymptotical formula

$$p(n)\sim\frac{1}{4n\sqrt{3}}\exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right) \tag{2.6}$$

for the number of partition of $n$ one can see from (2. 5) at once that Corollary I will no more be true if $N\log\log N$ is replaced by

$$N\exp\left(A\sqrt{\frac{\log N}{\log\log N}}\right), \qquad A>\frac{2\pi}{\sqrt{6}}.$$

Nevertheless it would be of interest to improve the lower bound in Corollary I or even determine the minimum number of conjugacy classes in groups of order $N$. The second corollary which is an immediate consequence of (2. 6) (and (2. 5)) is the

Corollary II. *The probability that a random pair $(P_1, P_2)$ of $S_n$ commute tends with $1/n$ rapidly to 0.*

* $(X, Y)$ and $(Y, X)$ are counted as different solutions if $X\neq Y$.

** The logarithm is meant here with the base 2.

Since Theorem IV and its Corollary I are not of statistical nature we postpone their proofs to Appendix I. For the same reason we postpone the solution of the following group theoretical extremal problem to Appendix II:

Determine all „least commutable" $P$'s, i.e. the $P$'s which commute with the minimal number of $P$'s of $S_n$.

The solution is given by the

THEOREM V. *The $P$'s with the required minimum property are exactly those whose canonical cycle-decomposition consists of two cycles with the length* 1 *and* $(n-1)$ *respectively, if only* $n \geqq 6$.

**3.** We shall also deal statistically with a different sort of questions. All groups $G$ of order $\leqq n$ can be embedded into $S_n$; but it is an important longstanding question to determine for each $G$ the minimal $g$ such that $G$ can be embedded into $S_g$. Here one can hope a simple law for $g$ in a statistical sense only. What we can do at present is to present such a law for commutative groups with order $\leqq n$. Denoting the total number of such groups by $G(n)$ this is given by

THEOREM VI. *If* $\psi(n) \nearrow \infty$ *so that*

$$\lim_{x \to \infty} \frac{\log \psi(x)}{\log x} = 0 \tag{3.1}$$

*then all commutative groups of order* $\leqq n$, *with the exception of* $o(G(n))$ *such groups at most, can be embedded into* $S_l$ *with*

$$l = \left[ \frac{n}{\psi(n)} \right]. \tag{3.2}$$

We shall also show that the theorem is best-possible in the sense that choosing

$$L \overset{\text{def}}{=} [n^{1-\delta}]$$

with an arbitrary small $\delta > 0$, we show that more than $c_2(\delta) G(n)$ Abelian groups of order $\leqq n$ are not embeddable into $S_L$.

The theorems as well as the proofs of this paper are directly or indirectly connected with partition-problems, even with some which would be considered by nonarithmeticians in themselves rather weird and artificial. By this connection the partition-problems cannot be considered anymore to be an isolated playground for arithmeticians, since the search of analogous statistical laws for other „big" groups will *systematically* lead to such problems. Part of the partition problems revelant here are of the type that for what kind of partitions is it true that „almost all" of them consist of $\Phi(n)(1+o(1))$ summands, $\Phi(n)$ depending on the type of partitions under consideration. Such results for some special kind of partitions has been found by ERDŐS and LEHNER (see [4]); the method used here for another special type of partitions seems to be extendable to a *general* class of partition-problems. However, in this paper we shall confine ourselves to the case we actually need here.

**4.** Now we turn to the proofs of our assertions. For the proof of Theorem I we shall need some lemmata.

LEMMA I. *If for* $x>0$

$$f(x)=\prod_{q \text{ prime}}(1+e^{-qx})$$

*then we have* for* $x\to+0$

$$\log f(x)=\frac{\pi^2}{12x\log\frac{1}{x}}+O\left(\frac{1}{x}\frac{\log\log\frac{1}{x}}{\log^2\frac{1}{x}}\right).$$

For the proof we write

$$\log f(x)=\int_0^\infty \log(1+e^{-xr})\,d\pi(r)=x\int_0^\infty \frac{\pi(r)}{1+e^{-xr}}\,dr$$

where $\pi(r)$ denotes the number of primes not exceeding $r$. Hence

$$\log f(x)=x\int_2^\infty \frac{\operatorname{Li} r}{1+e^{-xr}}\,dr+O(1)\int_2^\infty x\frac{re^{-\sqrt{\log r}}}{1+e^{-xr}}\,dr+O(1). \tag{4.1}$$

Splitting the second integral into

$$\int_2^{x^{-\frac{1}{2}}}+\int_{x^{-\frac{1}{2}}}^{x^{-1}\log^2 x^{-1}}+\int_{x^{-1}\log^2 x^{-1}}^{\infty}$$

one can easily see that this is

$$O\left(\frac{1}{x}\right)\exp\left(-\frac{1}{2}\sqrt{\log\frac{1}{x}}\right)$$

and also

$$\log f(x)=\int_2^\infty \frac{\log(1+e^{-xr})}{\log r}\,dr+O\left(\frac{1}{x}\right)\exp\left(-\frac{1}{2}\sqrt{\log\frac{1}{x}}\right). \tag{4.2}$$

Splitting the remaining integral into

$$\int_2^{x^{-1}\log^{-10}x^{-1}}+\int_{x^{-1}\log^{-10}x^{-1}}^{10x^{-1}\log x^{-1}}+\int_{10x^{-1}\log x^{-1}}^{\infty} \tag{4.3}$$

the first and third integrals in (4. 3) are evidently

$$O\left(\frac{1}{x\log^{10}\frac{1}{x}}\right);$$

* The asymptotic part of this lemma is implicitely contained in the paper of HARDY and RAMANUJAN [5], p. 130. For our aims however the remainder term is quite essential, whereas the paper of Hardy and Ramanujan contains no remainder term at all.

replacing in the second $\log r$ by $\log \frac{1}{x}$ the error is

$$O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right).$$

Hence

$$\log f(x) = \frac{1}{\log\frac{1}{x}}\int_0^\infty \log(1+e^{-xr})\,dr + O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right),$$

from which Lemma I follows at once.

**5.** Further we shall need the

LEMMA II. *If for* $x>0$

$$F(x) = \prod_{q\,\text{prime}} (1+e^{-qx}+e^{-q^2x}+e^{-q^3x}+\ldots)$$

*then we for* $x\to+0$

$$\log F(x) = \frac{\pi^2}{12x\log\frac{1}{x}} + O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right).$$

For the proof we write

$$\log F(x) = \log f(x) + \sum_q \log\left\{\frac{e^{-q^2x}+e^{-q^3x}+\ldots}{1+e^{-qx}}+1\right\}.$$

Hence

$$|\log F(x)-\log f(x)| \leqq \sum_q \log\{1+e^{-q^2x}+e^{-q^3x}+\ldots\} \leqq$$

$$\leqq \sum_q \sum_{\nu=2}^\infty \exp(-q^\nu x) = (1-e^{-x})\sum_{n=0}^\infty e^{-nx}\left(\sum_{\substack{q,\nu\\ q^\nu\leqq n,\ \nu\geqq 2}} 1\right) =$$

$$= O(x)\sum_{n=0}^\infty \sqrt{n}\,e^{-nx} = O\left(\frac{1}{\sqrt{x}}\right)$$

which, together with Lemma I proves Lemma II.

**6.** The proof of Theorem I will easily be completed connecting Lemma II with the

LEMMA III. *Let for* $x>0$ *be*

$$h(x) = \sum_{n=0}^\infty a_n e^{-nx}, \qquad a_n \geqq 0$$

*and for* $x \to +0$ *with numerical positive* $A$

$$\log h(x) = \frac{A}{x \log \frac{1}{x}} \left\{ 1 + O\left( \frac{\log\log \frac{1}{x}}{\log \frac{1}{x}} \right) \right\}. \tag{6.1}$$

*Then**

$$S_N = \sum_{n \leqq N} a_n = \exp\left\{ 2 \sqrt{2A \frac{N}{\log N}} + O\left( \frac{\sqrt{N} \log\log N}{\log N} \right) \right\}.$$

For the proof let

$$x_0 = \frac{\lambda}{\sqrt{N \log N}} \tag{6.2}$$

$\lambda$ positive constant, to be determined. Then

$$\log h(x_0) = \frac{2A}{\lambda} \sqrt{\frac{N}{\log N}} \left\{ 1 + O\left( \frac{\log\log N}{\log N} \right) \right\}. \tag{6.3}$$

Hence

$$\exp\left( -\lambda \sqrt{\frac{N}{\log N}} \right) S_N \leqq \sum_{n \leqq N} a_n e^{-n x_0} \leqq h(x_0) =$$

$$= \exp\left\{ \frac{2A}{\lambda} \sqrt{\frac{N}{\log N}} \left( 1 + O\left( \frac{\log\log N}{\log N} \right) \right) \right\}$$

i. e.

$$S_N \leqq \exp\left\{ \left( \lambda + \frac{2A}{\lambda} \right) \sqrt{\frac{N}{\log N}} + O\left( \frac{\sqrt{N} \log\log N}{\log^{3/2} N} \right) \right\}.$$

Choosing

$$\lambda = \sqrt{2A} \tag{6.4}$$

we got already

$$S_N \leqq \exp\left\{ 2 \sqrt{2A \frac{N}{\log N}} + O\left( \frac{\sqrt{N} \log\log N}{\log^{3/2} N} \right) \right\} \tag{6.5}$$

which is the second part of Lemma III (slightly stronger). Further if $\delta = \delta(N) \to 0$ will be determined later, we write

$$\exp\left\{ \sqrt{2A \frac{N}{\log N}} \left( 1 + O\left( \frac{\log\log N}{\log N} \right) \right) \right\} = h(x_0) = \tag{6.6}$$

$$= \sum_{n \leqq (1-\delta)N} + \sum_{(1-\delta)N \leqq n \leqq (1+\delta)N} + \sum_{(1+\delta)N < n \leqq 100N} +$$

$$+ \sum_{n > 100N} a_n e^{-n x_0} \overset{\text{def}}{=} S_1 + S_2 + S_3 + S_4.$$

* The Tauberian theorem differs again from that of HARDY—RAMANUJAN (l.c. [5]) containing in hypothesis as well as in assertion remainder terms, which is quite essential for our later aims. Besides in formula (5.281) 1. c. the factor $\frac{2\pi}{\sqrt{3}}$ seems to be replaced by $\frac{2\pi}{\sqrt{6}}$.

As to $S_4$ (6. 5) gives easily

$$(6.7)\quad S_4 < \int_{100N}^{\infty} \exp\left\{\sqrt{2A}\left(2\sqrt{\frac{y}{\log y}}-\frac{y}{\sqrt{N\log N}}\right)+c_2\frac{\sqrt{y}\log\log y}{\log^{3/2} y}\right\}dy = o(1).$$

For $S_3$ we get

$$(6.8)\quad S_3 \leqq 100N\exp\left\{c_3\frac{\sqrt{N}\log\log N}{\log^{3/2} N}\right\}\exp\left\{\sqrt{\frac{2A}{\log N}}\max_{y\leqq(1+\delta)N}\left(2\sqrt{y}-\frac{y}{\sqrt{N}}\right)\right\}.$$

Since for all sufficiently large $N$'s

$$\max_{y\leqq(1+\delta)N}\left(2\sqrt{y}-\frac{y}{\sqrt{N}}\right) = \sqrt{N}\left\{2\sqrt{1+\delta}-(1+\delta)\right\} =$$

$$= \sqrt{N}\left\{1-\frac{\delta^2}{4}+O(\delta^3)\right\} < \sqrt{N}\left(1-\frac{\delta^2}{5}\right)$$

(6. 8) gives

$$(6.9)\quad S_3 < \exp\left\{\sqrt{2A\frac{N}{\log N}}\left(1-\frac{\delta^2}{5}\right)+O\left(\frac{\sqrt{N}\log\log N}{\log^{3/2} N}\right)\right\}.$$

As to $S_1$ (6. 5) gives

$$S_1 < N\exp\left\{c_3\frac{\sqrt{N}\log\log N}{\log^{3/2} N}\right\}\exp\left\{\sqrt{2A}\max_{y\leqq(1-\delta)N}\left(2\sqrt{\frac{y}{\log y}}-\frac{y}{\sqrt{N\log N}}\right)\right\}.$$

One can easily see that the last maximum is

$$(6.10)\quad \sqrt{\frac{N}{\log N}}\left\{2\sqrt{1-\delta}-(1-\delta)\right\}+O\left(\frac{\sqrt{N}}{\log^{3/2} N}\right) =$$

$$= \sqrt{\frac{N}{\log N}}\left\{1-\frac{\delta^2}{4}+O(\delta^3)\right\}+O\left(\frac{\sqrt{N}}{\log^{3/2} N}\right) < \left(1-\frac{\delta^2}{5}\right)\sqrt{\frac{N}{\log N}}+c_4\frac{\sqrt{N}}{\log^{3/2} N}.$$

Hence choosing

$$(6.11)\quad \delta = \sqrt{\frac{\log\log N}{\log N}}$$

(6. 6), (6. 7), (6. 9), (6. 10) and (6. 11) give for all sufficiently large $N$'s

$$S_2 > \exp\left\{\sqrt{2A\frac{N}{\log N}}\left(1-c_5\frac{\log\log N}{\log N}\right)\right\}$$

and a fortiori

$$\exp\left\{-\sqrt{2A\frac{(1-\delta)N}{\log N}}\right\}\left(\sum_{(1-\delta)N<m\leqq(1+\delta)N} a_n\right) >$$

$$> \exp\left\{\sqrt{2A\frac{N}{\log N}} - c_6\frac{\sqrt{N}\log\log N}{\log^{3/2} N}\right\}$$

and — replacing $N$ by $\frac{N}{1+\delta}$ —

$$S_N > \exp\left\{2\sqrt{2A\frac{N}{\log N}} - c_7\sqrt{\frac{N}{\log N}}\,\delta - c_6\frac{\sqrt{N}\log\log N}{\log^{3/2} N}\right\}$$

which completes the proof of Lemma III.

**7.** Now we can turn to the proof of Theorem I. Let

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \qquad 2 \leqq p_1 < p_2 < \dots < p_r \tag{7.1}$$

be an $\mathbf{O}(P)$-value; the canonical cycle-decomposition of this $P$ should consist of $m_\nu$ cycles of length $n_\nu$ ($\nu = 1, 2, \dots, k$) i.e.

$$1 \leqq n_1 < n_2 \dots < n_k, \tag{7.2}$$

$$m_\nu \geqq 1, \qquad \nu = 1, 2, \dots, k, \tag{7.3}$$

$$\sum_{\nu=1}^{k} m_\nu n_\nu = n \tag{7.4}$$

so that

$$\mathbf{O}(P) = [n_1, n_2, \dots, n_k] = N. \tag{7.5}$$

Since each $p_\nu^{\alpha_\nu}$ is a factor of some $n_j$ and

$$n_1 + n_2 \leqq n_1 n_2 \quad \text{for integer} \quad n_1 \geqq 2,\ n_2 \geqq 2 \tag{7.6}$$

we have

$$p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_r^{\alpha_r} \leqq n_1 + n_2 + \dots + n_k \leqq \sum_{j=1}^{k} m_j n_j = n, \tag{7.7}$$

$$p_1 < p_2 < \dots < p_r.$$

Hence to each such $\mathbf{O}(P)$-value we make correspond uniquely a set of powers of distinct primes with the sum $\leqq n$.

But conversely, having any sum of prime-powers

$$q_1^{\beta_1} + q_2^{\beta_2} + \dots + q_l^{\beta_l} \leqq n \tag{7.8}$$

with

$$2 \leqq q_1 < q_2 < \dots < q_l,\ q_l \text{ primes} \tag{7.9}$$

the number $q_1^{\beta_1}q_2^{\beta_2}\dots q_l^{\beta_l}$ is the order of a $P_1$; such a $P_1$ is furnished by any permutations of $S_n$ consisting of $l$ cycles with cycle-lengths $q_1^{\beta_1}$, $q_2^{\beta_2}$, ..., $q_l^{\beta_l}$ respectively and

$$n-\sum_{j=1}^{l} q_j^{\beta_j}$$

further cycles of length 1. Hence the different $\mathbf{O}(P)$-values are the $q_1^{\beta_1}q_2^{\beta_2}\dots q_l^{\beta_l}$-numbers extended to all systems satisfying (7. 8)—(7. 9). Hence $W(n)$ is identical with the number of solutions of (7. 8)—(7. 9).

Now the number of solutions of (7. 8)—(7. 9) is evidently $\sum_{\nu\leqq n} a_\nu$ where for $x>0$

$$\sum_{\nu=0}^{\infty} a_\nu e^{-\nu x} = F(x) = \prod_{q\,\text{prime}} (1+e^{-qx}+e^{-q^2x}+e^{-q^3x}+\dots).$$

Application of Lemma II and III completes the proof of Theorem I.

Owing to the grouptheoretical connection it would be desirable to obtain better approximations to $W(n)$ than the one given by our Theorem I. The Tauberian theorems of Ingham (see INGHAM [6]) would certainly lead to a better result but the verification of its assumptions would be much more laborious than the way we have chosen. The same holds on the saddle point technique of ROTH—SZEKERES (see [7]).

**8.** For the proof of Theorem II we shall need two further lemmata.

LEMMA IV. *For* $x\to+0$ *we have*

$$\sum_{q\,\text{prime}} \frac{1}{e^{qx}+1} = \frac{\log 2}{x\log\frac{1}{x}} + O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right).$$

For the proof we write

$$\sum_{q} \frac{1}{e^{qx}+1} = \int_0^\infty \frac{d\pi(r)}{e^{xr}+1}.$$

Analogously as in Lemma I this is

$$\frac{1}{\log\frac{1}{x}}\int_0^\infty \frac{dr}{e^{xr}+1} + O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right) = \frac{\log 2}{x\log\frac{1}{x}} + O\left(\frac{\log\log\frac{1}{x}}{x\log^2\frac{1}{x}}\right)$$

indeed.

**9.** The next lemma is the crucial one. Let us consider all solutions of the system (7. 8)—(7. 9). Then we assert that the number of summands follows a rather strong statistical law. More exactly we assert the

LEMMA V. *For almost all* solutions of the system* (7. 8)—(7. 9) *the inequality*

$$l = \frac{2\sqrt{6}}{\pi} \log 2 \sqrt{\frac{n}{\log n}} + O\left(\sqrt{n} \log^{-0,73} n\right) \tag{9. 1}$$

*holds.*

For the proof we define

$$H_{mn} = \sum_{\substack{p_1^{\alpha_1} + p_2^{\alpha_2} + \ldots + p_m^{\alpha_m} \leqq n \\ p_1 < p_2 < \ldots < p_m}} 1 \tag{9. 2}$$

Then we have for $x > 0$, $y$ real

$$G(y, x) \overset{\text{def}}{=} \sum_{\mu, \nu} A_{\mu\nu} e^{-\mu y - \nu x} = \prod_{q \text{ prime}} \{1 + e^{-y-qx} + e^{-y-q^2x} + \ldots\} \tag{9. 3}$$

and we have to investigate

$$S_{mn} = \sum_{\substack{\mu \leqq m \\ \nu \leqq n}} A_{\mu\nu} = \sum_{\mu \leqq m} H_{\mu n} \tag{9. 4}$$

where $m = m(n)$ will be determined later. Writing $G(y, x)$ in the form

$$G(y, x) = F(x) \prod_{q \text{ prime}} \left\{1 + \frac{(e^{-y} - 1)(e^{-qx} + e^{-q^2x} + \ldots)}{1 + e^{-qx} + e^{-q^2x} + \ldots)}\right\} \overset{\text{def}}{=} F(x) G_0(y, x); \tag{9. 5}$$

putting

$$x_1 = \frac{\pi}{\sqrt{6n \log n}}, \qquad y_1 = y_1(n) \to 0 \tag{9. 6}$$

to be determined, we get

$$S_{mn} \leqq \left(F(x_1) e^{nx_1}\right) \left(G_0(y_1, x_1) e^{my_1}\right). \tag{9. 7}$$

For the first factor on the right Lemma II gives the upper bound

$$\exp\left\{\frac{2\pi}{\sqrt{6}} \sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n} \log\log n}{\log^{3/2} n}\right)\right\}. \tag{9. 8}$$

The second factor in (9. 7) is owing to (9. 5)

$$\leqq \exp\left\{my_1 - \sum_{q \text{ prime}} \frac{(1 - e^{-y_1}) e^{-qx_1}}{1 + e^{-qx_1} + e^{-q^2x_1} + \ldots}\right\} = \exp y_1 \left\{m - \left(1 - \frac{y_1}{2}\right) \sum_{q \text{ prime}} \frac{1}{e^{qx_1} + 1} + \right.$$

$$\left. + \left(1 - \frac{y_1}{2}\right) \sum_{q \text{ prime}} \left(\frac{1}{e^{qx_1} + 1} - \frac{1}{e^{qx_1} + 1 + e^{(q-q^2)x_1} + e^{(q-q^3)x_1} + \ldots}\right)\right\}.$$

* i.e. with $o(W(n))$ exceptions at most, with the notation of Theorem I.

The last sum being

$$< \sum_{q \text{ prime}} \frac{e^{(q-q^2)x_1} + e^{(q-q^3)x_1} + \dots}{(e^{qx_1}+1)^2} < \sum_{q \text{ prime}} \sum_{\nu=2}^{\infty} \exp\left(-q^\nu \frac{x_1}{2}\right) = O\left(\frac{1}{\sqrt{x_1}}\right) = O(n \log n)^{1/4}$$

the last factor in (9. 7) has the upper bound

$$\exp y_1 \left\{ m - \left(1 - \frac{y_1}{2}\right) \sum_{q \text{ prime}} \frac{1}{e^{qx_1}+1} + O(n \log n)^{1/4} \right\}.$$

Using Lemma IV this is in turn

$$\text{(9. 9)} \qquad \leqq \exp y_1 \left\{ m - \left(1 - \frac{y_1}{2}\right) \frac{2\sqrt{6}\,\log 2}{\pi} \sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\,\log\log n}{\log^{3/2} n}\right) \right\}.$$

This together with (9. 7) and (9. 8) gives

$$S_{mn} \leqq \exp\left\{ \frac{2\pi}{\sqrt{6}} \sqrt{\frac{n}{\log n}} + c_7 \frac{\sqrt{n}\,\log\log n}{\log^{3/2} n} + \right.$$

$$\left. + y_1 \left( m - \frac{2\sqrt{6}\log 2}{\pi} \sqrt{\frac{n}{\log n}} \right) + \frac{y_1^2}{2} \frac{2\sqrt{6}\log 2}{\pi} \sqrt{\frac{n}{\log n}} \right\}.$$

Now choosing

$$\text{(9. 10)} \qquad m = \frac{2\sqrt{6}\log 2}{\pi} \sqrt{\frac{n}{\log n}} - \frac{\sqrt{n}}{\log^{0,73} n}, \qquad y_1 = \log^{-0,26} n$$

this gives for all sufficiently large $n$'s

$$\text{(9. 11)} \qquad S_{mn} \leqq \exp\left\{ \frac{2\pi}{\sqrt{6}} \sqrt{\frac{n}{\log n}} - \frac{1}{2} \frac{\sqrt{n}}{\log^{0,99} n} \right\}.$$

**10.** We shall need also an upper bound for

$$\text{(10. 1)} \qquad S^*_{M,n} \overset{\text{def}}{=} \sum_{\substack{\mu \leqq M \\ \nu \leqq n}} A_{\mu\nu} = \sum_{\mu \leqq M} H_{\mu n}$$

$M = M(n)$ to be determined later. First let us observe that for $\nu \leqq n$ and $\mu > 3\sqrt{n}$

$$p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_\mu^{\alpha_\mu} > \sum_{1 \leqq l \leqq 3\sqrt{n}} l > n$$

i. e.

$$\text{(10. 2)} \qquad S^*_{M,n} = \sum_{\substack{M \leqq \mu \leqq 3\sqrt{n} \\ \nu \leqq n}} A_{\mu\nu}.$$

We apply Cauchy's coefficient-estimation with

$$x = x_1 = \frac{\pi}{\sqrt{6n \log n}}, \qquad y = y_1 = -|y_1| \to 0$$

to be determined for $A_{\nu\mu}$; this gives, using (9. 5), (9. 7) and (9. 8) again

$$A_{\mu\nu} \leqq \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}}+O\left(\frac{\sqrt{n}\log\log n}{\log^{3/2} n}\right)\right\}\cdot \tag{10.3}$$

$$\cdot\exp\left\{-\mu|y_1|+(e^{|y_1|}-1)\frac{e^{-qx_1}+e^{-q^2x_1}+\ldots}{1+e^{-qx_1}}\right\}.$$

The second factor in (10.3) cannot exceed

$$\exp|y_1|\left\{-\mu+(1+|y_1|)\sum_{q\,\text{prime}}\frac{1}{e^{qx_1}+1}+O(n\log n)^{1/4}\right\}.$$

Using again Lemma IV this is

$$\leqq \exp\left\{|y_1|\left(-\mu+\frac{2\sqrt{6}\log 2}{\pi}\sqrt{\frac{n}{\log n}}\right)+c_8 y_1^2\sqrt{\frac{n}{\log n}}\right\}$$

and thus from (10. 2) and (10. 3)

$$S^*_{M,n} \leqq \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}}+c_9\frac{\sqrt{n}\log\log n}{\log^{3/2} n}+\right. \tag{10.4}$$

$$\left.+|y_1|\left(-M+\frac{2\sqrt{6}\log 2}{\pi}\sqrt{\frac{n}{\log n}}\right)+c_8 y_1^2\sqrt{\frac{n}{\log n}}\right\}.$$

Choosing now

$$M=\frac{2\sqrt{6}\log 2}{\pi}\sqrt{\frac{n}{\log n}}+\frac{\sqrt{n}}{\log^{0,73} n}, \tag{10.5}$$

$$y_1=-\log^{-0,26} n \tag{10.6}$$

we get

$$S^*_{M,n} \leqq \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}}-\frac{1}{2}\sqrt{n}\log^{-0,99} n\right\}. \tag{10.7}$$

Since from Theorem I we have

$$W(n)=\sum_{\substack{\mu,\nu\\ \nu\leqq n}} A_{\mu\nu} > \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}}-c_{10}\frac{\sqrt{n}\log\log n}{\log n}\right\}$$

this, (9. 11) and (10. 7) prove Lemma V.

**11.** Now we can turn to the proof of Theorem II.
As told all $\mathbf{O}(P)$-values are the numbers

$$q_1^{\beta_1} q_2^{\beta_2}\ldots q_l^{\beta_l} \tag{11.1}$$

satisfying (7. 8)—(7. 9). Owing to Lemma V with $o(W(n))$ exceptions also*

$$l = \frac{2\sqrt{6}\log 2}{\pi}\sqrt{\frac{n}{\log n}} + O\left(\sqrt{n}\log^{-0,73} n\right) \tag{11.2}$$

is satisfied. But we have always

$$l! \leqq q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l} < \left(\frac{q_1^{\beta_1} + \dots + q_l^{\beta_l}}{l}\right)^l \leqq \left(\frac{n}{l}\right)^l. \tag{11.3}$$

Now using (11. 2) we have on one hand

$$l! > \exp(l\log l - l) \geqq \exp\left\{\frac{\sqrt{6}\log 2}{\pi}(1-o(1))\sqrt{n\log n}\right\} \tag{11.4}$$

and on the other hand

$$\left(\frac{n}{l}\right)^l = \exp\left(l\log\frac{n}{l}\right) \leqq \exp\left\{\frac{\sqrt{6}\log 2}{\pi}(1+o(1))\sqrt{n\log n}\right\}$$

which prove Theorem II.

**12.** Next we turn to Theorem III. Let — as in Theorem IV — $p(n)$ stand for the number of the partitions of $n$; we characterise the partitions with the numbers $m_\nu$, $n_\nu$ in section 7. According to the classical asymptotic formula of HARDY and RAMANUJAN (see [5]) we have

$$p(n) = (1+o(1))\frac{1}{4n\sqrt{3}}\exp\left(\frac{2\pi}{\sqrt{6}}\sqrt{n}\right). \tag{12.1}$$

Let us denote by

$$\pi_1, \pi_2, \dots, \pi_{p(n)} \tag{12.2}$$

the partitions of $n$ and define the „partition-function" $h(\pi_\nu)$ by

$$h(\pi_\nu) = \frac{m_1^2 n_1 + \dots + m_k^2 n_k}{m_1 + \dots + m_k}. \tag{12.3}$$

Then we need the

LEMMA VI. *For almost all partitions, i.e. with $o(p(n))$ exceptions at most, for $n > n_0$ the inequality*

$$h(\pi_\nu) \leqq \sqrt{n}\log^2 n \tag{12.4}$$

*holds (the right side could be replaced by $c_{11}\sqrt{n}\log n$).*

For the proof of this lemma we consider first the set $\Pi$ of the $\pi_\nu$-partitions with

$$\max_{j=1,2,\dots,k} m_j n_j > \sqrt{n}\log^2 n. \tag{12.5}$$

* The remainder term was of course only for Lemma V of vital importance.

Fixing $m_j$ and $n_j$ let $\Pi^{(m_j, n_j)}$ be the corresponding subset of $\Pi$ and $|\Pi|$ the cardinality of $\Pi$. Then

$$|\Pi^{(m_j, n_j)}| \leqq p(n - m_j n_j) \leqq p\left(n - \sqrt{n}\log^2 n\right)$$

and from (12. 1)

$$< (1+o(1))\frac{1}{4\left(n-\sqrt{n}\log^2 n\right)\sqrt{3}} \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{n-\sqrt{n}\log^2 n}\right\} <$$

$$< (1+o(1))\frac{1}{4n\sqrt{3}} \exp\left\{\frac{2\pi}{\sqrt{6}}\sqrt{n}\left(1-\frac{\log^2 n}{2\sqrt{n}}\right)\right\} = p(n)\,(1+o(1)) \exp\left\{-\frac{\pi}{\sqrt{6}}\log^2 n\right\}.$$

Since $\Pi = \bigcup_{m_j,\, n_j} \Pi^{(m_j, n_j)}$ and $m_j, n_j$ has at most $n$ values, we get

$$|\Pi| < p(n) 2n^3 \exp\left\{-\frac{\pi}{\sqrt{6}}\log^2 n\right\} = o\left(p(n)\right).$$

Hence with exception of $o\left(p(n)\right)$ $\pi_\nu$'s at most the inequality

$$\max_j m_j n_j \leqq \sqrt{n}\log^2 n \tag{12.6}$$

holds. For these partitions we have

$$h(\pi_\nu) \leqq \max_j m_j n_j \frac{\sum_j m_j}{\sum_j m_j} \leqq \sqrt{n}\log^2 n$$

indeed.

We shall need also the following theorem of ERDŐS—LEHNER (see [4]).

With the notation of section 7 for all but $o\left(p(n)\right)$ partitions the inequality

$$\left|(m_1 + \ldots + m_k) - \frac{\sqrt{6}}{2\pi}\sqrt{n}\log n\right| \leqq \omega(n)\sqrt{n} \tag{12.7}$$

holds, if only $\omega(x) \nearrow \infty$ for $x \to \infty$.

I.e. almost all partitions consist of $(1+o(1))\dfrac{\sqrt{6}}{2\pi}\sqrt{n}\log n$ summands.

**13.** Now we can prove Theorem III as follows. Let us consider the conjugacy-classes of $S_n$; as well known $P_1$ and $P_2$ belong to the same class if and only if the cycles of their canonical cycle decomposition are pairwise identical in their number as well to their respective length. Hence a conjugacy-class $\mathfrak{A}$ is determined by the common

$$(n_1, n_2, \ldots, n_k;\ m_1, m_2, \ldots, m_k) \tag{13.1}$$

numbers of their P's. Thus first of all

$$V(n) = p(n). \tag{13.2}$$

i.e. the number of the conjugacy-classes of $S_n$ equals to the number of partitions of $n$. Secondly the number of $P$'s in the class $\mathfrak{A}$ is

$$\frac{n!}{m_1!\, m_2! \dots m_k!\, n_1^{m_1}\, n_2^{m_2} \dots n_k^{m_k}}, \tag{13.3}$$

owing to Cauchy's formula (see e.g. RIORDAN [8]). Fixing $P_0$ in the class $\mathfrak{A}$ let the centraliser of $P_0$ be $C(P_0)$. As well-known there is a one-to-one correspondence between the conjugates of $P_0$ and the cosets of $C(P_0)$ in $S_n$. Hence, with the notation of section 12 we have

$$|\mathfrak{A}| = \frac{|S_n|}{|C(P_0)|} \tag{13.4}$$

and thus the number of $P$'s commutable with $P_0$ is owing to (13. 3)

$$|C(P_0)| = m_1!\, m_2! \dots m_k!\, n_1^{m_1}\, n_2^{m_2} \dots n_k^{m_k} \tag{13.5}$$

for all $P_0$'s of the class $\mathfrak{A}$.

Now we remark that

$$\frac{(m_1+m_2+\dots+m_k)!}{|C(P_0)|} = \frac{(m_1+m_2+\dots+m_k)!}{m_1!\, m_2! \dots m_k!}\left(\frac{1}{n_1}\right)^{m_1}\left(\frac{1}{n_2}\right)^{m_2}\dots\left(\frac{1}{n_k}\right)^{m_k} < \tag{13.6}$$

$$< \left(\frac{1}{n_1}+\frac{1}{n_2}+\dots+\frac{1}{n_k}\right)^{m_1+\dots+m_k} \leqq \left(\sum_{\nu=1}^{k}\frac{1}{\nu}\right)^{m_1+\dots+m_k} < (1+\log k)^{m_1+\dots+m_k}.$$

Hence

$$|C(P_0)| > \frac{(m_1+\dots+m_k)!}{(1+\log n)^{m_1+\dots+m_k}} > \left(\frac{m_1+\dots+m_k}{2e\log n}\right)^{m_1+\dots+m_k}. \tag{13.7}$$

So far we made no restrictions on the conjugacy class $\mathfrak{A}$. Now we take into consideration Lemma VI, (12. 7) and (13. 2); these give that with exception of the $P$'s of

$$o(V(n)) = o(p(n))$$

conjugacy-classes in the remaining set $\Pi_1$ of conjugacy-classes, both inequalities (12. 4) and (12. 7) hold. Hence for $P_0 \in \Pi_1$ (12. 7) and (13. 7) give (using also the inequality $l! > \left(\frac{l}{e}\right)^l$)

$$|C(P_0)| > \left(\frac{\sqrt{n}}{50}\right)^{(1-o(1))\frac{\sqrt{6}}{2\pi}\sqrt{n}\log n} > \exp\left\{(1-o(1))\frac{\sqrt{6}}{4\pi}\sqrt{n}\log^2 n\right\},$$

which gives the first half of Theorem III.

On the other hand (13. 5) gives (using the inequality $l! \leqq l^l$ for all $P_0$'s)

$$|C(P_0)| \leqq (m_1 n_1)^{m_1}(m_2 n_2)^{m_2} \dots (m_k n_k)^{m_k} \leqq \left(\frac{m_1^2 n_1 + \dots + m_k^2 n_k}{m_1+\dots+m_k}\right)^{m_1+\dots+m_k}.$$

Now restricting $P_0$ to $\Pi_1$ we may apply (12. 4) and (12. 7); thus

$$|C(P_0)| \leqq \left(\sqrt{n}\log^2 n\right)^{(1+o(1))\frac{\sqrt{6}}{2\pi}\sqrt{n}\log n} = \exp\left\{(1+o(1))\frac{\sqrt{6}}{4\pi}\sqrt{n}\log^2 n\right\},$$

which completes the proof of Theorem III.

As a by-product we notice the following

COROLLARY. *All conjugacy-classes of* $S_n$, *with* $o(p(n))$ *exceptions at most, contain*

$$n!\exp\left\{-(1+o(1))\frac{\sqrt{6}}{4\pi}\sqrt{n}\log^2 n\right\}$$

*P's.*

**14.** Next we turn to theorem VI. We shall need the well-known theorem of ERDŐS—SZEKERES* (see [9]).

Denoting the number of pairwise nonisomorphic Abelian groups of order $m$ by $k(m)$ we have

$$\sum_{m\leqq n} k(m) = A_0 n(1+o(1)), \qquad A_0 = \zeta(2)\zeta(3)\ldots, \tag{14.1}$$

$\zeta(s)$ is the Riemann zeta function.

Taking this in account we have only to prove that (3. 2) is satisfied for all but $o(n)$ Abelian groups of order $\leqq n$.

We shall need the remark (which follows at once from the fundamental theorem of finite Abelian groups) that

$$k(m_1 m_2) = k(m_1)k(m_2) \quad \text{if} \quad (m_1, m_2) = 1. \tag{14.2}$$

We shall denote by $z(m)$ the maximal prime-power divisor of $m$ and let us fix a $\psi(n)$ with property (3. 1). Let $M$ be the set of integers $m$ not exceeding $n$ with the property

$$z(m) > \frac{n}{2\psi(n)}. \tag{14.3}$$

We shall need the

LEMMA VIII. *The inequality*

$$U = \sum_{m\in M} k(m) = o(n)$$

*holds.*

Let

$$z(m) = q^{\alpha} > \frac{n}{2\psi(n)}.$$

Then we have

$$m = q^{\alpha} m_1, \qquad (q^{\alpha}, m_1) = 1$$

* Their theorem furnishes also a remainder-term. However here — in contrary to the previous discussions — it is immaterial. Even $> O(n)$ is enough.

and hence — using also that $k(q^\alpha)=p(\alpha)$ and (14. 1) —

$$U=\sum_{\frac{n}{2\psi(n)}\leqq q^\alpha\leqq n}k(q^\alpha)\sum_{\substack{m_1\leqq\frac{n}{q^\alpha},\,(m_1,\,q)=1\\ z(m_1)<q^\alpha}}k(m_1)\leqq\sum_{\frac{n}{2\psi(n)}\leqq q^\alpha\leqq n}p(\alpha)\sum_{m_1\leqq\frac{n}{q^\alpha}}k(m_1)=O(n)\sum_{\frac{n}{2\psi(n)}\leqq q^\alpha\leqq n}\frac{p(\alpha)}{q^\alpha}.$$

(14. 4)

The contribution of $\alpha=1$ is $o(n)$ owing to

$$\sum_{\frac{n}{2\psi(n)}\leqq q\leqq n}\frac{1}{q}=o(1). \tag{14. 5}$$

Since roughly

$$\alpha<2\log n$$

and

$$p(\alpha)<ce^{2\sqrt{\alpha}}<ce^{4\sqrt{\log n}},$$

the contribution of $\alpha\geqq 2$ is

$$<O\left(ne^{4\sqrt{\log n}}\right)\sum_{2\leqq\alpha\leqq 2\log n}\sum_{m>\left(\frac{n}{2\psi(n)}\right)^{1/\alpha}}m^{-\alpha}< \tag{14. 6}$$

$$<O\left(ne^{4\sqrt{\log n}}\right)\left(\frac{n}{\psi(n)}\right)^{-\frac{1}{2}}\log n=o(n),$$

which completes the proof of lemma VIII.

Owing to this lemma it is enough to restrict ourselves to Abelian groups of order $m\leqq n$ with the property

$$z(m)\leqq\frac{n}{2\psi(n)}. \tag{14. 7}$$

**15.** Let $m$ be such an integer and let

$$m=a_1a_2\ldots a_k\qquad(=q_1^{\beta_1}q_2^{\beta_2}\ldots q_s^{\beta_s}) \tag{15. 1}$$

be any decomposition of $m$ into prime-powers. Let us consider

$$D(m)=a_1+a_2+\ldots+a_k. \tag{15. 2}$$

Since an easy induction gives for integers $b_j\geqq 2$

$$b_1+b_2+\ldots+b_l\leqq b_1b_2\ldots b_l,$$

we get

$$D(m)\leqq q_1^{\beta_1}+q_2^{\beta_2}+\ldots+q_s^{\beta_s}. \tag{15. 3}$$

Since only at most one of the $q_j^{\beta_j}$ can exceed $\sqrt{n}$, we get from (14. 7)

$$D(m)\leqq\frac{n}{2\psi(n)}+s\sqrt{n}\leqq\frac{n}{2\psi(n)}+\sqrt{n}\log n\leqq\left[\frac{n}{\psi(n)}\right]=l. \tag{15. 4}$$

Now take for $n > c_{12}$ any commutative group $G$ of order $m \leqq n$ with (14. 7) of type $(a_1, a_2, \ldots, a_k)$. But then forming the permutations of $a_1 + \ldots + a_k \leqq l$ elements

$$(12\ldots a_1)^{v_1}(a_1+1, a_1+2, \ldots, a_1+a_2)^{v_2}\ldots(a_1+\ldots+a_{k-1}+1, \ldots, a_1+a_2+\ldots+a_k)^{v_k}$$

$$1 \leqq v_1 \leqq a_1,\ 1 \leqq v_2 \leqq a_2, \ldots, 1 \leqq v_k \leqq a_k$$

these form a group $G^*$ isomorphic to $G$ which is a subgroup of $S_l$ indeed.

In order to prove that the theorem is no more true for $S_{[n^{1-\delta}]}$ with an arbitrarily small numerical positive $\delta$ we have only to remark that for a prime $q$ the group $G$, the order of which is divisible by $q$, cannot be embedded into $S_d$ with $d < q$ further that the number of integers $\leqq n$ divisible by a $q > n^{1-\delta}$ is

$$\sum_{n^{1-\delta} \leqq q \leqq n} \left[\frac{n}{q}\right] > n \log \frac{1}{1-\delta} - o(n)$$

and finally (14. 1).

## APPENDIX I

As told we are going to give the proof of Theorem IV and its corollaries in this Appendix. Let us consider a fixed conjugacy-class $Q_j$ of $G$ containing $|Q_j|$ elements; let $\alpha$ be one of its elements and $C(\alpha)$ its centraliser, containing $|C(\alpha)|$ elements. Hence $\alpha$ commutes in $G$ with $\left(\frac{N}{|Q_j|} - 1\right)$ elements, different from $\alpha$. Since the same holds for all elements of $Q_j$, the total number of commutable $(\alpha, \beta)$ pairs with $\alpha \in Q_j$, $\alpha \neq \beta$ is

$$|Q_j|\left(\frac{N}{|Q_j|} - 1\right) = N - |Q_j|.$$

Summation for $j = 1, 2, \ldots, k$ gives

$$kN - \sum_{j=1}^{k} |Q_j| = kN - N.$$

This gives the total number of commutable $(\alpha, \beta)$-pairs with $\alpha \neq \beta$; since we have $N$ further commutable pairs $(\alpha, \alpha)$, the proof of Theorem IV is finished.

In order to prove Corollary I we appeal to the following well-known theorem (see [10]).

Let $2 = \alpha_1 < \alpha_2 < \ldots$ be defined by the recursion

$$\alpha_{v+1} = \alpha_1 \alpha_2 \ldots \alpha_v + 1. \tag{I. 1}$$

If for a fixed $v$ and positive integers $x_1, x_2, \ldots, x_v$

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_v} < 1 \tag{I. 2}$$

then

$$\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_v} \leqq 1 - \frac{1}{\alpha_{v+1} - 1}. \tag{I. 3}$$

Next we apply the following reasoning of LANDAU (see [11]). With the above $Q_j$'s we have

$$|Q_1| = 1 \quad \text{and for} \quad 2 \leqq j \leqq k \qquad |Q_j| = \frac{N}{y_{j-1}}, \qquad (y_l \text{ positive integers})$$

and hence

$$\frac{1}{y_1} + \frac{1}{y_2} + \ldots + \frac{1}{y_{k-1}} = 1 - \frac{1}{N}.$$

But then (I. 2) is fulfilled and (I. 3) is applicable with $v = k-1$. This gives

$$1 - \frac{1}{N} \leqq 1 - \frac{1}{\alpha_k - 1}, \quad \text{i. e.} \quad \alpha_k \geqq N+1. \tag{I. 4}$$

Now from (I. 1)

$$\frac{\alpha_{v+1} - 1}{\alpha_v - 1} = \alpha_v, \qquad \alpha_{v+1} = \alpha_v^2 - \alpha_v + 1 < \alpha_v^2$$

i. e.

$$\alpha_k \leqq 2^{2^k}.$$

Hence (I. 4) gives

$$2^{2^k} > N \quad \text{or} \quad k > \log\log N$$

which together with Theorem IV proves Corollary I indeed.

## APPENDIX II

**1.** Now we prove Theorem V. According to (13. 5) the number of elements with which a fixed $P_0 \in S_n$ is commutable depends only upon the conjugacy class to which $P_0$ belongs; the extremal class is a class $Q = Q(n_1, n_2, \ldots, n_k; m_1, m_2, \ldots, m_k)$ for which

$$f(Q) \overset{\text{def}}{=} m_1!\, m_2! \ldots m_k!\, n_1^{m_1}\, n_2^{m_2} \ldots n_k^{m_k} \tag{II. 1}$$

is minimal under the restrictions (7. 2)—(7. 3)—(7. 4). Hence we have to show that the minimum is $(n-1)$ and the only extremal class $Q_0$ corresponds to

$$k = 2, \quad m_1 = m_2 = 1, \quad n_1 = 1, \quad n_2 = (n-1). \tag{II. 2}$$

First we remark that for

$$k \geqq 4, \qquad 1 \leqq a_1 < a_2 < \ldots < a_k \tag{II. 3}$$

the inequality

$$a_1 a_2 a_3 \ldots a_k \geqq a_1 + a_2 + \ldots + a_k + 14 \tag{II. 4}$$

holds. Namely the expression

$$\frac{1}{a_1 a_2 a_3} + \frac{1}{a_1 a_2 a_4} + \frac{1}{a_1 a_3 a_4} + \frac{1}{a_2 a_3 a_4}$$

attains its maximum for $a_1=1, a_2=2, a_3=3, a_4=4$, which is 5/12. Hence

$$1 \geqq \frac{1}{a_1 a_2 a_3} + \ldots + \frac{1}{a_2 a_3 a_4} + \frac{7}{12}.$$

Thus

$$a_1 a_2 a_3 a_4 \geqq a_1 + a_2 + a_3 + a_4 + 14\left(\frac{a_1}{1}\right)\left(\frac{a_2}{2}\right)\left(\frac{a_3}{3}\right)\left(\frac{a_4}{4}\right) \geqq a_1 + a_2 + a_3 + a_4 + 14$$

i.e. (II. 4) holds for $k=4$. If it holds for $k \leqq k_0$

$$a_1 a_2 \ldots a_{k_0} \geqq a_1 + a_2 + \ldots + a_{k_0} + 14$$

then multiplying by $a_{k_0+1}(>2)$

$$a_1 a_2 \ldots a_{k_0+1} \geqq a_1 + \ldots + a_{k_0} + 14 a_{k_0+1} =$$

$$= (a_1 + a_2 + \ldots + a_{k_0+1}) + 13 a_{k_0+1} > a_1 + a_2 + \ldots + a_{k_0+1} + 14$$

which proves (II. 4). One can see quite analogously that for

(II. 5) $$k \geqq 3, \quad 2 \leqq a_1 < a_2 < \ldots < a_k$$

the inequality

(II. 6) $$a_1 a_2 \ldots a_k \geqq a_1 + a_2 + \ldots + a_k + 14$$

holds.

For $k=1$ we have

$$f(Q) = n > n-1 = f(Q_0)$$

i.e. this class cannot be extremal. Putting aside temporarily the case $k=2$ we suppose

(II. 7) $$k \geqq 3$$

and hence

(II. 8) $$n_k \geqq 3.$$

Let now $Q^*(n_1^*, \ldots, n_k^*;\ m_1^*, \ldots, m_k^*)$ be an extremal-class. We assert that

(II. 9) $$n_v^* \geqq 3 \to m_v^* = 1,$$

i.e. a cycle-length $\geqq 3$ can occur at most once in an extremal-class. For if not, let $n_j^*$ the longest cycle-length with $m_j^* \geqq 2$. This implies that if the cycle-length $m_j^* n_j^*$ occurs at all in $Q^*$ and $= n_l^*$ then

(II. 10) $$m_l^* = 1.$$

Then we consider the class $Q_1$ which comes from $Q^*$ contracting all cycles with length $n_j^*$ into a single cycle (of length $m_j^* n_j^*$). In the case (II. 10)

(II. 11) $$\frac{f(Q_1)}{f(Q^*)} = \frac{2!(m_j^* n_j^*)^2}{1!(m_j^* n_j^*) m_j^*! (n_j^*)^{m_j^*}} = \frac{2}{(m_j^*-1)!(n_j^*)^{m_j^*-1}} < 1$$

and in the case when the cycle-length $m_j^* n_j^*$ does not occur in $Q^*$

$$\frac{f(Q_1)}{f(Q^*)} = \frac{1!(m_j^* n_j^*)}{m_j^*!(n_j^*)^{m_j^*}} = \frac{1}{(m_j^*-1)!(n_j^*)^{m_j^*-1}} < 1 \tag{II. 12}$$

i.e. $Q^*$ could not be an extremal class. Hence (II. 9) is proved.

Next we assert that

$$n_j^* = 1 \to m_v^* = 1 \tag{II. 13}$$

i.e. the cycle-length $n_1 = 1$ can occur in an extremal-class at most once. Obviously we may suppose

$$(3 \leqq) n_k^* \leqq n-1. \tag{II. 14}$$

Supposing

$$m_1^* \geqq 2$$

we consider the class $Q_2$ which arises from $Q^*$ taking away one cycle of length 1 and replacing the cycle with length $n_k^*$ by one of length $(n_k^*+1)$. Then owing to (II. 14) and (II. 9) we have

$$\frac{f(Q_2)}{f(Q^*)} = \frac{(m_1^*-1)!\,1^{m_1^*-1}1!(n_k^*+1)}{m_1^*!\,1^{m_1^*}\cdot 1!\,n_k^*} = \frac{n_k^*+1}{n_k^*\cdot m_1^*} \leqq \frac{4}{3}\cdot\frac{1}{2} < 1$$

and thus $Q^*$ could be an extremal-class. Hence (II. 13) is proved.

(II. 11) and (II. 13) give at the same time that the cycle-length 2 can occur at most twice in an extremal-class and it could occur twice *only* if $Q^*$ has (exactly) one cycle of length 4. If $Q^*$ has no cycle with length 8, then replacing $Q^*$ by $Q_3$ which contains a cycle of length 8, taking off the two cycles of length 2 and the one with length 4 we get

$$\frac{f(Q_3)}{f(Q^*)} = \frac{1!\,8^1}{2!\,2^2\cdot 1!\,4^1} < 1; \tag{II. 15}$$

if $Q^*$ has (exactly) one cycle of length 8 then

$$\frac{f(Q_3)}{f(Q^*)} = \frac{2!\,8^2}{2!\,2^2\cdot 1!\,4^1\cdot 1!\,8^1} < 1. \tag{II. 16}$$

Thus the cycle-length 2 can occur at most once too, i.e.

$$m_1^* = m_2^* = \ldots = m_k^* = 1$$

and

$$f(Q^*) = n_1^* n_2^* \ldots n_k^* \tag{II. 17}$$

with

$$n_1^* + n_2^* + \ldots + n_k^* = n, \qquad k \geqq 3$$

$$1 \leqq n_1^* < n_2^* < \ldots < n_k^*. \tag{II. 18}$$

If $k \geqq 4$ then (II. 4), (II. 17) and (II. 18) give

$$f(Q^*) \geqq n+14 > f(Q_0)$$

i.e. we may suppose

(II. 19) $$k=3.$$

(II. 5) gives at once that in this case

$$n_1=1$$

and hence

$$f(Q^*)=n_2n_3$$

$$2\leqq n_2<n_3,\quad n_2+n_3=n-1$$

for which for $n\geqq 6$

$$f(Q^*)\geqq 2(n-3)>(n-1),$$

i.e. $Q^*$ cannot be extremal.

For the case $k=2$ the above reasoning can be repeated and gives that for $Q^*\neq Q_0$ $f(Q^*)>f(Q_0)$ which completes the proof.

*(Received 11 September 1967)*

## References


[1] P. ERDŐS and P. TURÁN, On some problems of a statistical group theory, I, *Zeitschr. für Wahrscheinlichkeitstheorie und verw. Gebiete*, **4** (1965) pp. 175—186.

[2] P. ERDŐS and P. TURÁN, On some problems of a statistical group theory. III, *Acta Math. Acad. Sci. Hung.*, **18** (1967), pp. 309—320.

[3] E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlen*, I. (1909), p. 222.

[4] P. ERDŐS and J. LEHNER, The distribution of the number of summands in the partitions of a positive integer, *Duke Math. Journ.*, **8** (2) (1941), pp. 335—345.

[5] G. H. HARDY and S. RAMANUJAN, Asymptotic formulae for the distribution of integers of various types, *Proc. of Lond. Math. Soc.* (2) **16** (1917), pp. 117—132.

[6] A. E. INGHAM, A Tauberian theorem for partitions, *Annals of Math.*, **42** (1941), pp. 1075—1090.

[7] K. F. ROTH and G. SZEKERES, Some asymptotic formulae in the theory of partitions, *The Quart. Journ. of Math.*, Oxford Second Series, **5** (1954), pp. 241—259.

[8] J. RIORDAN, *An introduction to combinatorial analysis* (New York, 1958).

[9] P. ERDŐS and G. SZEKERES, Über die Anzahl der Abelschen Gruppen gegebener Ordnung, *Acta Litt. ac. Scient. Szeged*, **7** (1934), pp. 95—102.

[10] The series $\sum\frac{1}{\alpha_\nu}$ is ussually called Engel-series of second kind; for its properties and for a proof of (I. 2)—(I. 3) see e.g. P. ERDŐS, On the integer solutions of the equation $\frac{1}{x_1}+\ldots+\frac{1}{x_n}=\frac{a}{b}$ (in Hungarian), *Matematikai Lapok*, **I. 3** (1950), pp. 192—210.

[11] E. LANDAU, *Math. Annalen*, **56** (1903), pp. 674—678.