Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Louis Nicolas

Statistiques sur le groupe symétrique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 13, n° 2 (1971-1972), exp. n° G2, p. G 1-G 6.

<http://www.numdam.org/item?id=SDPP_1971-1972__13_2_A12_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
13e année, 1971/72, n° G2, 6 p.

29 novembre 1971

STATISTIQUES SUR LE GROUPE SYMÉTRIQUE

par Jean-Louis NICOLAS

L'objet de cet exposé est de résumer les travaux de P. ERDÖS et P. TURÁN : "On some problems of a statistical group theory". Déjà 4 articles ont paru sous ce titre ([2], [3], [4], [5]) et 3 autres au moins sont en préparation.

1. Introduction.

Soit S_n le groupe des permutations de n objets, et notons $O(P)$ l'ordre de la permutation P dans le groupe S_n. E. LANDAU (cf. [8], § 61 et [10], chap. 2) a défini

$$g(n) = \max_{P \in S_n} O(P) ,$$

et montré que $\log g(n) \sim \sqrt{x \log n}$. D'autre part, il y a beaucoup de permutations d'ordre n (ce qui est très petit devant $g(n)$), il y a au moins les $(n-1)!$ permutations circulaires. Il semble donc difficile de trouver une loi de distribution pour $O(P)$ quand $P \in S_n$. Et pourtant on a le résultat suivant.

THÉORÈME 1([2]). - *L'ordre prépondérant de P dans S_n est* $\exp(\frac{1}{2} + o(1))\log^2 n$ *et, plus précisément :*

Pour tout ε, $\delta > 0$, il existe $n_0(\varepsilon, \delta)$ tel que, pour $n \geq n_0$ tous les $P \in S_n$, sauf au plus $\delta n!$, vérifient

$$\exp((1/2) - \varepsilon) \log^2 n \leq O(P) \leq \exp((1/2) + \varepsilon) \log^2 n .$$

THÉORÈME 2 ([4]). - *Soit $K(n, x)$ le nombre de $P \in S_n$ satisfaisant à*

$$\log O(P) \leq (1/2) \log^2 n + x \log^{3/2} n .$$

On a

$$\lim_{n \to \infty} \frac{K(n, x)}{n!} = \sqrt{\frac{3}{2\pi}} \int_{-\infty}^{x} \exp(-(3/2)\lambda^2) d\lambda ,$$

uniformément pour $-x_0 \leq x \leq x_0$, x_0 étant aussi grand que l'on veut.

2. Etude du groupe symétrique S_n.

1° Un élément P du groupe S_n se décompose en cycles de façon unique (cf. [10], p. 137). Par exemple, pour $n = 9$,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1\ 9\ 5)(2\ 8\ 4\ 6)(3\ 7) .$$

Les longueurs des cycles forment une partition de n. On désigne par

$$1 \leq n_1 < n_2 < \ldots < n_k \leq n ,$$

les différentes longueurs de cycles de P, et par m_v le nombre de cycles de longueur n_v. On a

$$\sum_v m_v n_v = n , \quad 1 \leqslant v \leqslant k ,$$

et

$$O(P) = \text{p. p. c. m. } (n_1 , n_2 , \dots , n_k) .$$

2° A chaque élément $P \in S_n$, on peut donc associer une partition

$$\underbrace{n_1 + n_1 + \dots + n_1}_{m_1 \text{ fois}} + \dots + \underbrace{n_k + \dots + n_k}_{m_k \text{ fois}} = n$$

de l'entier n. Réciproquement, une partition étant donnée, le nombre de $P \in S_n$ qui lui sont associés est

$$(1) \qquad \frac{n!}{m_1! \dots m_k! \, n_1^{m_1} \dots n_k^{m_k}} ,$$

d'après une formule due à CAUCHY ([11], p. 67).

A chaque $\lambda \in S_n$, on associe l'automorphisme intérieur σ_λ, défini par $\sigma_\lambda(P) = \lambda P \lambda^{-1}$. Si la décomposition en cycles de P est

$$P = (a_1 , a_2 , \dots , a_i)(b_1 , b_2 , \dots , b_j)(\dots) .$$

On voit que $\sigma_\lambda(P)$ transforme λa_1 en λa_2 et qu'on peut écrire :

$$\sigma_\lambda(P) = (\lambda a_1 , \lambda a_2 , \dots , \lambda a_i)(\lambda b_1 , \dots , \lambda b_j)(\dots) .$$

Ainsi P et $\sigma_\lambda(P)$ sont associés à la même partition. Réciproquement, si P et Q sont associés à la même partition, il est facile de trouver λ tel que $Q = \sigma_\lambda(P)$. La classe de conjugaison de P, c'est-à-dire l'ensemble des $\sigma_\lambda(P)$, quand $\lambda \in S_n$, coïncide donc avec l'ensemble des permutations associées à la partition de P, et son cardinal est donné par (1).

3° Soit P une permutation associée à la partition $\sum_v m_v n_v$, $1 \leqslant v \leqslant k$. Parmi les $\lambda \in S_n$, il y a ceux tels que $\sigma_\lambda(P) = P$, c'est-à-dire ceux qui commutent avec P et qui forment le normalisateur $C(P)$ de P. Il y a les autres λ pour lesquels $\sigma_\lambda(P)$ appartient à la classe de conjugaison $Q(P)$ de P. Mais si $P' \in Q(P)$, il existe une bijection entre $C(P)$ et $H(P') = \{\lambda \in S_n \mid \sigma_\lambda(P) = P'\}$. Si λ_0 est un élément fixé de $H(P')$, l'application qui à $\lambda \in C(P)$ fait correspondre $\lambda_0 \lambda \in H(P')$ est une telle bijection : Lorsque P' parcourt $Q(P)$, les $H(P')$ ont tous le même cardinal que $C(P)$, et l'on a

$$\text{card } C(P) \times \text{card } Q(P) = n! ,$$

soit

$$(2) \qquad \text{card } C(P) = m_1! \, m_2! \dots m_k! \, n_1^{m_1} \, n_2^{m_2} \dots n_k^{m_k} .$$

4° Soit G un groupe fini d'ordre N ayant pour classes de conjugaison $Q_1 = \{e\}$, Q_2, $\dots$, Q_k avec $q_i = \text{card } Q_i$. Les résultats du paragraphe précédent

s'appliquent, et l'on a, pour $a \in Q_i$:

$$\text{card}\{x \in G \mid ax = xa\} = N/q_i$$
$$\text{card}\{(a , x) \in Q_i \times G \mid ax = xa\} = q_i(N/q_i) = N$$
$$\text{card}\{(a , x) \in G \times G \mid ax = xa\} = kN .$$

Le nombre de couples (a , b) qui commutent dans G est donc égal à kN , où k est le nombre de classes de conjugaison de G .

5° Dans un groupe G fini d'ordre N , il ne peut pas y avoir trop peu de couples (a , b) qui **commutent**, autrement dit le nombre k de classes de conjugaison de G ne peut pas être trop petit. Plus précisément, on doit avoir $k \geq \log \log N$.

Avec les mêmes notations qu'au 4°, les q_i doivent vérifier : $q_1 = 1$, q_i divise N pour tout i , et $\sum_i q_i = N$, $1 \leq i \leq k$. Si l'on pose $x_i = N/q_i$, on doit avoir :

$$(3) \qquad \frac{1}{x_2} + \frac{1}{x_3} + \ldots + \frac{1}{x_k} = 1 - \frac{1}{N} .$$

LEMME ([5], appendice 1, et [6]). - Soit α_ν la suite définie par

$$\alpha_1 = 2 , \alpha_2 = 3 , \alpha_3 = 7 , \alpha_4 = 43 , \ldots , \alpha_{\nu+1} = \alpha_1 \alpha_2 \ldots \alpha_\nu + 1 .$$

Si, pour ν fixé et pour des entiers positifs $x_1 , x_2 , \ldots , x_\nu$, on a : $\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_\nu} < 1$, alors on a : $\frac{1}{x_1} + \ldots + \frac{1}{x_\nu} \leq 1 - \frac{1}{\alpha_{\nu+1} - 1}$.

A l'aide de ce lemme, d'une estimation de la suite α_ν et de (3), on déduit que $k \geq \log \log N$.

6° Tout groupe fini G d'ordre n se plonge dans S_n ; En désignant par $1 , 2 , \ldots , n$, les éléments du groupe, on fait correspondre à $a \in G$ la permutation

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a.1 & a.2 & \ldots & a.n \end{pmatrix} ,$$

et on constate que c'est un homomorphisme.

Un groupe G d'ordre n étant donné, un problème classique et irrésolu est de trouver $f(n)$ minimum tel que G se plonge dans $S_{f(n)}$. On a ici une réponse partielle à ce problème dans le cas des groupes commutatifs. On désigne par $G(n)$ le nombre de groupes commutatifs d'ordre $\leq n$. On a : $G(n) \sim An$ (cf. [7]).

THÉORÈME 3 ([5], théorème 6). - Si $\psi(n) \longrightarrow \infty$ avec n , et si $\frac{\log \psi(n)}{\log n} \longrightarrow 0$, alors tous les groupes commutatifs d'ordre $\leq n$, sauf $o(G(n))$ d'entre eux, sont plongeables dans $S_{f(n)}$ avec $f(n) = [n/(\psi(n))]$.

Mais si $f(n) = [n^{1-\delta}]$, il y a plus de $c\,G(n)$ groupes commutatifs d'ordre $\leq n$ qui ne sont pas plongeables dans $S_{f(n)}$.

3. Résultat statistiques.

1° Tableau récapitulatif.

	S_n Groupe symétrique	$P(n)$ Ensemble des partitions de n	$\mathfrak{W}(n) \in N$ Ensemble des ordres de P, quand $P \in S_n$
	P	$\sum_v m_v n_v$, $1 \leqslant v \leqslant k$	p. p. c. m. $[n_1, \ldots, n_k]$
Cardinaux	card $S_n = n!$	card $P(n) = p(n)$ $p(n) \sim \frac{1}{4n\sqrt{3}} \exp(\frac{2\pi}{\sqrt{6}}\sqrt{n})$ (HARDY et RAMANUJAN)	card $\mathfrak{W}(n) = W(n)$ $W(n) = \exp(\frac{2\pi}{\sqrt{6}}\sqrt{\frac{n}{\log n}} + O(\frac{\sqrt{n}\log\log n}{\log n})$ ([5], Théorème 1)
Ordre prépondérant	$\exp(\frac{1}{2}+o(1))\log^2 n$ (cf. [2])	$\exp(A + o(1))\sqrt{n}$ (ERDOS et TURAN, à paraître)	$\exp(1+o(1))\frac{\sqrt{6}\log 2}{\pi}\sqrt{n \log n}$ ([5], Théorème 2)
Nombre de cycles prépondérant	$g(P) = \sum_v m_v$, $1 \leqslant v \leqslant k$ $\log n \pm \omega(n)\sqrt{\log n}$ (cf. [2])	$\frac{\sqrt{6}}{2\pi}\sqrt{n}\log n \pm \omega(n)\sqrt{n}$ (cf. [5], § 12)	

2° Résultats sur les classes de conjugaison :

(a) Mises à part $o(p(n))$ classes, toutes les autres ont comme cardinal ([5], § 13) :

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

(b) Le cardinal maximal d'une classe de conjugaison est $n!/(n-1)$ et est obtenu lorsque la permutation P a deux cycles, l'un de longueur $n-1$, l'autre de longueur 1. Une telle permutation ne commute qu'avec $(n-1)$ éléments de S_n.

3° Résultats sur la divisibilité de $O(P)$ ([3]).

Soit $\omega(n) \longrightarrow \infty$, on pose :

$$A = \frac{\log n}{\log_2 n}\{1 + 3\frac{\log_3 n}{\log_2 n} - \frac{\omega(n)}{\log_2 n}\}$$

$$B = \frac{\log n}{\log_2 n}\{1 + 3\frac{\log_3 n}{\log_2 n} + \frac{\omega(n)}{\log_2 n}\}.$$

Alors, pour presque tous les $P \in S_n$, $O(P)$ est divisible par tous les nombres $\leqslant A$, et n'est pas divisible par un nombre premier $\leqslant B$.

Enfin, pour presque tous les $P \in S_n$, le plus grand facteur premier de $O(P)$ est compris entre

$$n \exp(-\omega(n)\sqrt{\log n}) \quad \text{et} \quad n \exp(-\frac{1}{\omega(n)}\sqrt{\log n}).$$

4. Questions ouvertes.

1° Transformer les résultats du § 3 en résultats plus précis à l'aide de fonctions de distribution.

2° Trouver $f(n)$ tel que presque tous les $P \in S_n$ commutent avec $(1 + o(1))f(n)$ éléments de S_n.

3° Soit $h(m) = \text{card}\{P \in S_n \mid O(P) = m\}$. Trouver m tel que $h(m)$ soit maximal.

4° Calculer les moyennes :

$$\frac{1}{n!}\sum_{P \in S_n} O(P) \quad \text{et} \quad \frac{1}{p(n)}\sum_{\mathcal{P} \in \mathcal{C}(n)} O(\mathcal{P}).$$

5° Quels sont les groupes d'ordre n avec un nombre de classes de conjugaison minimal ?

6° L'ordre des sous-groupes de S_n est-il presque toujours pair ?

7° Nous avons étudié, dans les § 2, 4 et 5, le nombre de paires qui commutent dans un groupe G. Etudier le nombre de triplets g_1, g_2, g_3 tels que $g_i g_j = g_j g_i$ pour $i, j = 1, 2, 3$.

8° D'après un résultat de J. J. DIXON, la commutativité de $5/8n^2$ paires parmi les n^2 paires possibles assure la commutativité du groupe. Trouver un résultat analogue, pour assurer que le groupe soit résoluble.

BIBLIOGRAPHIE

[1] BEST (M. R.). - The distribution of some variables on symetric groups, Koninkl. nederl. Akad. Wetensch., Proc., Series A, t. 73, 1970, p. 385-402 (Indag. Math., t. 32, 1970, n° 5).

[2] ERDÖS (P.) and TURÁN (P.). - On some problems of a statistical group theory, I., Z. für Wahrscheinlichkeitstheorie, t. 4, 1965, p. 175-186.

[3] ERDÖS (P.) and TURÁN (P.). - On some problems of a statistical group theory, II., Acta Math. Acad. Scient. Hung., t. 18, 1967, p. 151-163.

[4] ERDÖS (P.) and TURÁN (P.). - On some problems of a statistical group theory, III., Acta Math. Acad. Scient. Hung., t. 18, 1967, p. 309-320.

[5] ERDÖS (P.) and TURÁN (P.). - On some problems of a statistical group theory, IV., Acta Math. Acad. Scient. Hung., t. 19, 1968, p. 413-435.

[6] ERDÖS (P.). - On the integer solutions of the equation $1/x_1 + \ldots + 1/x_n = a/b$ [en hongrois], Matematikai Lapok, t. 1, 1950, p. 192-210.

[7] ERDÖS (P.) und SZEKERES (G.). - Über die Anzahl der Abelschen Gruppen gegebener Ordnung, Acta. Scient. Math., Szeged, t. 7, 1934, p. 95-102.

[8] LANDAU (E.). - Handbuch der Lehre von der Verteilung der Primzahlen. - Leipzig und Berlin, B. G. Teubner, 1909.

[9] LANG (S.). - Algebra, - Reading, Addison-Wesley, 1965.

[10] NICOLAS (J.-L.). - Ordre maximal d'un élément du groupe des permutations, Bull. Soc. math. France, t. 97, 1969, p. 129-191 (Thèse Sc. math., Paris, 1968).

[11] RIORDAN (J.). - An introduction to combinatorial analysis. - New York, J. Wiley and Sons, 1958.

(Texte reçu le 13 décembre 1971)

Jean-Louis NICOLAS
65 rue du Javelot
75013 PARIS