THÉORIE DES NOMBRES. — *Ordre maximal d'un élément d'un groupe de permutations.* Note (*) de M. **Jean-Louis Nicolas**, présentée par M. Paul Montel.

Soit S_n le groupe des permutations de n éléments. On définit avec Landau [*voir* (1), § 61] :

$$g(n) = \max_{\sigma \in S_n} [\text{ordre de } \sigma].$$

L'objet de cet article est de démontrer :

$$\lim_{n \to \infty} \frac{g(n+1)}{g(n)} = 1. \tag{1}$$

On sait déjà que pour tout n, on a $1 \leq g(n+1)/g(n) \leq 2$ [*voir* (2), p. 319]. Soit k un nombre entier, nous allons montrer que

$$\overline{\lim} \frac{g(n+1)}{g(n)} \leq \frac{k+1}{k}, \tag{2}$$

ce qui démontrera (1).

Rappelons que l'on désigne par $l(n)$ la fonction arithmétique additive dont la restriction aux puissances de nombres premiers est l'application identique. On a ainsi $l\left(\prod_i p_i^{\alpha_i}\right) = \sum_i p_i^{\alpha_i}$, avec p_i premier et $\alpha_i \geq 1$. On démontre que [*voir* (3), chap. 2] :

$$g(n) = \max_{l(j) \leq n} j. \tag{3}$$

Rappelons également que l'on sait définir une partie privilégiée G de $g(\mathbf{N})$. On dit que $N \in G$, s'il existe $\rho > 0$ tel que pour tout entier N′ différent de N, on ait $l(N') - l(N) \geq \rho \log(N'/N)$, et l'on connaît exactement la décomposition en facteurs premiers de $N \in G$ [*voir* (3), chap. 3].

Soit $M = g(n+1)$. On va construire un nombre A tel que

$$\frac{M}{A} \sim \frac{k+1}{k} \tag{4}$$

et que

$$l(A) < l(M). \tag{5}$$

Comme $l(M) = l(g(n+1)) \leq n+1$ d'après (3), on aura donc $l(A) \leq n$ et également

$$A \leq g(l(A)) \leq g(n) \leq g(n+1),$$

car g est croissante, et cela démontrera (2).

Soit $N \leq M$ le nombre de l'ensemble G immédiatement inférieur ou égal à M. Il lui est associé un nombre réel ρ qui tend vers l'infini avec N. On définit x, y, z par

$$\frac{z^{k+1}-z^k}{\log z} = \frac{y^k - y^{k-1}}{\log y} = \frac{x}{\log x} = \rho. \tag{6}$$

On en déduit :

$$z \sim \left(\frac{x}{k+1}\right)^{\frac{1}{k+1}} \quad \text{et} \quad y \sim \left(\frac{x}{k}\right)^{\frac{1}{k}}. \tag{7}$$

On sait que, dans la décomposition en facteurs premiers de N, les nombres premiers compris entre z et y ont pour exposant k.

LEMME. — *Soit* $(r_i)_{1 \leq i \leq u}$ *les nombres premiers supérieurs à* z *tels que* $(r_i)^{k+1}$ *divise* M. *On a* $u = O(\sqrt{z})$.

Soit $(Q_j)_{1 \leq j \leq v}$ *les nombres premiers compris entre* $y/2$ *et* y *tels que* Q_j^k *ne divise pas* M, *on a* $v = O(\sqrt{y})$.

Démonstration. — D'après la proposition 1 du chapitre 2 de ([3]), on a

$$l(M) - l(N) \geq \sum_{1 \leq i \leq u} \left(\frac{r_i^{k+1} - r_i^k}{\log r_i} - \rho \right) \log r_i. \tag{8}$$

Or $\rho = (z^{k+1} - z^k)/\log z$, la fonction $t \mapsto (t^{k+1} - t^k)/\log t$ a une dérivée croissante et équivalente à $(k+1)t^k/\log t$ et l'on a $r_1 \geq z$, $r_2 \geq z+2$, ..., $r_i \geq z + 2(i-1)$. La relation (8) devient

$$\begin{aligned} l(M) - l(N) &\geq \sum_{1 \leq i \leq u} (r_i - z)(1-\varepsilon) \frac{(k+1)z^k}{\log z} \log r_i \\ &\geq (1-\varepsilon)(k+1)z^k \sum_{1 \leq i \leq u} 2(i-1) \geq (1-\varepsilon)(k+1)z^k u^2. \end{aligned}$$

Comme le nombre N′ suivant N dans G est tel que $l(N') \leq l(N) + P$ où P est le plus petit nombre premier ne divisant pas N, et que l'on sait que $\rho \sim P/\log P \sim x/\log x$, ce qui donne $P \sim x$, on a $P \geq l(M) - l(N)$, d'où

$$x \geq (1-\varepsilon)(k+1)z^k u^2. \tag{9}$$

Or, d'après (7), $(k+1)z^{k+1} \sim x$; (9) devient donc :

$$(1-\varepsilon)u^2 \leq z \qquad \text{soit} \quad u = O(\sqrt{z}).$$

La deuxième partie du lemme se démontre de façon analogue.

Construction de A. — Soit $\tau = 5/8$. D'après un résultat de Ingham, on sait que le nombre de nombres premiers compris entre z et $z_1 = z + z^\tau$ est équivalent à $z^\tau/\log z$. On peut donc choisir $(k+1)$ nombres premiers : $(R_i)_{1\leq i\leq k+1}$ compris entre z et z_1 et qui divisent M avec un exposant $(\alpha_i)_{1\leq i\leq k+1}$ tel que $\alpha_i \leq k$ pour tout i, à cause du lemme précédent. On peut également choisir, entre $y - y^\tau = y_1$ et y, k nombres premiers $(q_j)_{1\leq j\leq k}$ qui divisent M avec un exposant $(\beta_j)_{1\leq j\leq k}$ tel que $\beta_j \geq k$ pour tout j. On pose alors :

$$A = M \frac{R_1 R_2 \dots R_{k+1}}{q_1 q_2 \dots q_k}.$$

Il reste à vérifier les relations (4) et (5). On a, à cause de (7) :

$$\frac{A}{M} \sim \frac{z^{k+1}}{y^k} \sim \frac{\frac{x}{k+1}}{\frac{x}{k}} \sim \frac{k}{k+1}, \tag{10}$$

ce qui démontre (4) et :

$$\begin{aligned} l(M) - l(A) &= \sum_{j=1} q_j^{\beta_j} - q_j^{\beta_j - 1} - \sum_{i=1}^{k+1} R_i^{k+1} - R_i \\ &\geq \sum_{j=1}^{k} q_j^k - q_j^{k-1} - \sum_{i=1}^{k+1} R_i^{k+1} - R_i^k \\ &\geq k(y_1^k - y_1^{k-1}) - (k+1)(z_1^{k+1} - z_1^k) = \varphi(k, y_1, z_1). \end{aligned} \tag{11}$$

On écrit

$$\varphi(k, y_1, z_1) = \varphi(k, y, z) - \Delta(y, y_1, k) - \Delta(z_1, z, k+1),$$

avec

$$\varphi(k, y, z) = k(y^k - y^{k-1}) - (k+1)(z^{k+1} - z^k) = \frac{x}{\log x} \log \frac{y^k}{z^{k+1}} \sim \frac{x}{\log x} \log \frac{k+1}{k},$$

d'après (6) et (10); et avec

$$\begin{aligned} \Delta(y, y_1, k) &= k(y^k - y^{k-1} - y_1^k + y_1^{k-1}) \\ &\leq k(y - y_1)(k y^{k-1}) = k^2 y^{\tau+k-1} = O\left(\frac{kx}{y^{1-\tau}}\right) = o\left(\frac{x}{\log x}\right) \end{aligned}$$

et de même :

$$\Delta(z_1, z, k) \leq (k+1)^2 z_1^{\tau+k} = O\left(\frac{(k+1)x}{z^{1-\tau}}\right) = o\left(\frac{x}{\log x}\right).$$

On a donc $\varphi(k, y_1, z_1) \sim (x/\log x) \log[(k+1)/k]$ et (11) nous permet de vérifier (5).

On pourrait adapter le calcul précédent en prenant k comme fonction de x dans (6). On arriverait à montrer que pour n assez grand,

$$\frac{g(n+1)}{g(n)} \leq 1 + \frac{(\log\log n)^8}{\log n}.$$

La majoration n'est pas très bonne. Il est vraisemblable que l'on a $g(n+1)/g(n) \leqq 1 + 1/n^{\alpha}$ pour un α assez petit. En effet, on sait que $g(n+1)/g(n) \geqq 1 + c\sqrt{\log n}/n^{1/4}$ pour une infinité de n [*voir* (3), chap. 2, théorème 6].

(*) Séance du 1er juin 1970.

(1) E. LANDAU, *Handbuch der Lehre von der Verteilung der Primzahlem*, B. G. Teubner, Leipzig und Berlin, 1909.

(2) J. L. NICOLAS, *Acta Arithmetica*, 14, 1968, p. 315-332.

(3) J. L. NICOLAS, *Ordre maximal d'un élément du groupe des permutations et highly composite numbers* (à paraître dans le *Bulletin de la Société mathématique de France*, 1969).

(*Département de Mathématiques,*
Université de Sherbrooke,
Québec, Canada.)

181981. — Imp. GAUTHIER-VILLARS. — 55, Quai des Grands-Augustins, Paris (6e).
Imprimé en France.