Lemme 2.

$$L_{n+k} + (-1)^k L_{n-k} = L_n L_k.$$

Preuve : (16) s'écrit

$$L_{n+k} = L_n L_{k+1} - 5F_k F_{n-1}.$$

Changeons k en $-k$ et utilisons (4) :

$$F_{-n} = (-1)^{n+1} F_n \; ; \; L_{-n} = (-1)^n L_n.$$

On obtient :

$$L_{n-k} = (-1)^{k-1} L_n L_{k-1} + 5(-1)^k F_k F_{n-1}$$

d'où :

$$L_{n+k} + (-1)^k L_{n-k} = L_n(L_{k+1} - L_{k-1}) = L_n L_k.$$

2° Preuve de la proposition 1.

Montrons que :

$$S_n = \sum_{k=1}^{n} \frac{1}{F(2^k)} = \frac{L(2^n - 1)}{F(2^n)}.$$

(On a noté $F(n)$, $L(n)$ au lieu de F_n, L_n.)

C'est évident pour $n = 1$. Si la formule est vraie à l'ordre n on peut écrire :

$$\begin{aligned} S_{n+1} &= \frac{L(2^n - 1)}{F(2^n)} + \frac{1}{F(2^{n+1})} \\ &= \frac{L(2^n)L(2^n - 1)}{L(2^n)F(2^n)} + \frac{1}{F(2^{n+1})} \\ &= \frac{L(2^n)L(2^n - 1) + 1}{F(2^{n+1})} \text{ (d'après (25)).} \end{aligned}$$

Dans la formule du lemme 2, remplaçons n par 2^n et k par $2^n - 1$:

$$L(2^{n+1} - 1) - 1 = L(2^n)L(2^n - 1)$$

d'où :

$$S_{n+1} = \frac{L(2^{n+1} - 1)}{F(2^{n+1})}.$$

D'après les formules (3) de Binet, on a au voisinage de l'infini :

$$F_n \sim \frac{\alpha^n}{\sqrt{5}}, \qquad L_n \sim \alpha^n \qquad \text{avec} \qquad \alpha = \frac{1 + \sqrt{5}}{2}.$$

Un calcul immédiat montre alors que :

$$\lim_{n \to \infty} S_n = \frac{\sqrt{5}}{\alpha} = \frac{5 - \sqrt{5}}{2}$$

3° Preuve de la proposition 2.

Montrons d'abord que L_{2n} n'est jamais un carré. En effet (28) s'écrit :

$$L_{2n} - L_n^2 = 2(-1)^{n+1}.$$

Or il est immédiat que l'équation diophantienne $x^2 - y^2 = \pm 2$ n'a pas de solutions, d'où le résultat.

Supposons n impair ($n \geqslant 5$). *Dans la formule du lemme 2 remplaçons n* par $n + k$ avec k pair :

$$L_{n+2k} + L_n = L_{n+k} L_k$$

d'où

$$L_{n+2k} \equiv -L_n \pmod{L_k}$$

et par suite pour t entier naturel

$$L_{n+2kt} \equiv (-1)^t L_n \pmod{L_k}$$

n étant impair s'écrit :

$$n = c + 2.3^r k, \; k \neq 0$$

avec $c \in \{1, 3\}$, k pair non divisible par 3 (ce qui équivaut à $k \equiv \pm 2 \pmod 6$).

Donc :

$$L_n = L_{c+2k3^r} \equiv (-1)^{3^r} L_c = -L_c \pmod{L_k}.$$

Comme $L_1 = 1$, $L_3 = 4$, on a :

$$L_n \equiv -1 \pmod{L_k} \quad \text{ou} \quad L_n \equiv -4 \pmod{L_k}$$

$k \equiv \pm 2 \pmod 6$ et le lemme 1 entraînent que $L_k \equiv 3 \pmod 4$.

L_k admet donc au moins un diviseur premier $p \equiv 3 \pmod 4$.

Le critère d'Euler sur les résidus quadratiques ([4]) montre que -1 et -4 ne peuvent être des carrés modulo p, ce qui achève la démonstration.

Remarque. — On connaît aussi les carrés de la suite F_n

$$(F_0, F_1, F_2, F_{12})$$

les cubes dans les suites de Lucas (L_1) et de Fibonacci

$$(F_0, F_1, F_2, F_6).$$

Références.

[1] *R.M.S.*, novembre 1979.
[2] *R.M.S.*, février 1982.
[3] E. Ehrhart, *Articles de Maths.* (Cedic 1985), p. 144.
[4] Lelong Ferrand Arnaudies (*Algèbre*, p. 146).

Le lecteur trouvera dans [2] d'autres propriétés arithmétiques de la suite p_n. On peut aussi consulter Hardy-Wright (Theory of numbers) et la revue « Fibonacci Quartely » entièrement consacrée à ce sujet. [3] donne une autre méthode générale pour obtenir les identités fibonacciennes.

Sur la factorisation de Thompson

P. Lescot.

I. — Introduction.

Un théorème bien connu de J. G. Thompson ([2], Proposition 4.162), affirme que, si G est un groupe fini résoluble sans section isomorphe à S_3, alors on a :

$$(1) \qquad G = N_G(J_e(S))C_G(Z(S))O_{2'}(G),$$

où $J_e(S)$, $Z(S)$ et $O_{2'}(G)$ désignent respectivement le sous-groupe de S engendré par ses sous-groupes abéliens élémentaires d'ordre maximal, le centre de S et le plus grand sous-groupe distingué d'ordre impair de G. Le but de cette note est de démontrer un résultat plus fin dans le cas d'un groupe G pour lequel S est supposé de classe de nilpotence au plus 2 :

Théorème. — Soit G un groupe fini résoluble n'ayant pas de section isomorphe à S_4, et possédant un 2-sous-groupe de Sylow S de classe de nilpotence au plus 2 ; alors

$$G = N_G(J_e(S))O_{2'}(G).$$

Remarque 1. — Il est bien connu que, si S est abélien, on a même $G = N_G(S)O_{2'}(G)$ dès que G est seulement supposé résoluble.

Remarque 2. — Ce résultat est le meilleur possible ; en effet, considérons $G = S_4$. G est résoluble ; en outre, on a $O_{2'}(G) = 1$, et S est un groupe diédral d'ordre 8, donc S est de classe de nilpotence 2 et $J_e(S) = S$. Or S n'est pas distingué dans G, donc G ne vérifie pas la conclusion du théorème.

Les notations et la terminologie que nous employons sont maintenant traditionnelles en théorie des groupes finis, et coïncident avec celles de [1], à une exception près : $\subset$ désignera pour nous l'inclusion au sens large.

II. — Démonstration du théorème.

Nous aurons besoin du lemme suivant, dû à Hayashi ([3], Lemma 3.9) :

Lemme. — Soit G un {2, 3}-groupe fini résoluble ne possédant aucune section isomorphe à S_4 ; alors $G = O_{3,2,3}(G)$.

Remarque. — En fait, d'après le théorème de Burnside, l'hypothèse de résolubilité de G est superflue.

Démonstration du lemme. — Supposons le lemme faux, et soit G un groupe d'ordre minimal parmi ceux qui satisfont à ses hypothèses et non à sa conclusion ; il est clair que $O_3(G) = 1$, que G possède un unique sous-groupe distingué non-trivial minimal X, et que $N_0 = O_{2,3}(G) \subsetneq G$ est l'unique sous-groupe distingué propre maximal de G. Ceci entraîne (car $O_3(G/N_0) = 1$), que G/N_0 est d'ordre 2 ; on ne peut donc pas avoir $O_3(G) \subset N_0$, donc on a $G = O_3(G)$. Soit maintenant Q un 3-sous-groupe de Sylow de G ; d'après la minimalité de $|G|$, G/X satisfait la conclusion du lemme, soit $G/X = O_{3,2,3}(G/X)$. Mais $O_3(G) = G$ entraîne

$$O_3(G/X) = O_3(G)X/X = G/X,$$

d'où

$$G/X = O_{3,2}(G/X), \qquad \text{soit} \qquad QX \lhd G ;$$

l'argument de Frattini nous donne alors :

$$(2) \qquad G = XN_G(Q)$$

X est un 2-groupe abélien élémentaire, donc $C_X(Q) \lhd X$; (2) implique alors que $C_X(Q) \lhd G$. Par définition de X, on a $C_X(Q) = X$ ou $C_X(Q) = 1$. Dans le premier cas, une nouvelle application de (2) permet de conclure que Q est distingué dans G : absurde ! Donc $C_X(Q) = 1$; Q, agissant sans point fixe sur le 2-groupe abélien élémentaire X, est donc cyclique. Soit Q_0 l'unique sous-groupe d'ordre 3 de Q ; si l'on avait $Q_0 \neq Q$, on verrait, en appelant z un 2-élément appartenant à $N_G(Q) \backslash X$ (il en existe d'après (1)), que $H = X\langle z \rangle Q_0$ serait un contre-exemple au lemme d'ordre $|H| < |G|$: absurde ! Donc Q est d'ordre 3, donc (car $C_G(Q) = Q$) $N_G(Q)$ est isomorphe à S_3. X est alors un 2-groupe abélien élémentaire sur lequel S_3 agit irréductiblement et fidèlement, d'où $X \simeq (\mathbb{Z}/2\mathbb{Z})^2$; or

$$X \cap N_G(Q) = X \cap C_G(Q) = C_X(Q) = 1.$$

En conclusion,

$$G = XN_G(Q) = X \rtimes N_G(Q) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_3 \simeq S_4.$$

contradiction ! Le lemme est ainsi établi.

Démonstration du théorème. — Supposons le théorème faux, et soit G un groupe d'ordre minimal parmi ceux qui en vérifient l'hypothèse et non la conclusion ; il est clair que $O_{2'}(G) = 1$, d'où, d'après le lemme de Hall-Higman ([1],

p. 228, Theorem 3.2) $C_G(O_2(G)) \subset O_2(G)$. Posons $M = N_G(J_e(S))$; M est alors un sous-groupe propre de G.

1° M est l'unique sous-groupe maximal de G contenant S.

En effet, soit H un sous-groupe propre de G contenant S ; on a

$$O_2(G) \subset H, \quad \text{d'où} \quad O_2(G) \subset O_2(H)$$

et

$$O_{2'}(H) \subset C_G(O_2(G)) \subset O_2(G).$$

On en déduit $O_{2'}(H) = 1$; la minimalité de l'ordre de G entraîne alors que $H = N_H(J_e(S))$, soit $H \subset M$.

2° $\langle S^G \rangle = G$.

Dans le cas contraire, (1) entraîne $\langle S^G \rangle \subset M$. Soit alors g un élément de $G \setminus M$; on a $S^g \subset M$, d'où l'existence d'un élément m de M tel que $S^g = S^m$. On en tire $gm^{-1} \in N_G(S) \subset M$, d'où $g \in M$: absurde !

3° Il existe un nombre premier impair p tel que G soit un $\{2, p\}$-groupe.

Si tel n'était pas le cas, on pourrait trouver deux diviseurs premiers impairs q et r de $|G|$, S serait alors contenu dans un q'-sous-groupe de Hall H_1 de G, et dans un r'-sous-groupe de Hall H_2 de G. H_1 et H_2 seraient alors deux sous-groupes propres de G contenant S et tels que $\langle H_1, H_2 \rangle = G$, ce qui contredirait **1°**.

4° $p \neq 3$.

Si l'on avait $p = 3$, on aurait $G = O_{3,2,3}(G)$ d'après l'hypothèse et le lemme, c'est-à-dire $G = O_{2,3}(G)$, d'où $S \lhd G$ et $J_e(S) \lhd G$: absurde !

5° G n'a pas de section isomorphe à S_3.

Ceci est une conséquence immédiate de **3°** et de **4°**.

6° Z(S) = Z(G).

On a $O_{2'}(G) = 1$, donc Z(G) est un 2-groupe, d'où $Z(G) \subset O_2(G) \subset S$, d'où $Z(G) \subset Z(S)$. En outre, si $C_G(Z(S))$ était distinct de G, on aurait $C_G(Z(S)) \subset M$ d'après **1°**, d'où $G = M$ d'après (1) : absurde ! On a donc $C_G(Z(S)) = G$, d'où $Z(S) \subset Z(G)$.

7° $G = C_G(O_2(G)/Z(G))$.

En effet, soit $C = C_G(O_2(G)/Z(G)) \lhd G$; on a, d'après **3°** :

$$[S, O_2(G)] \subset [S, S] \subset Z(S) = Z(G),$$

d'où $S \subset C$ et $G = \langle S^G \rangle \subset C$ d'après **2°**.

8° La contradiction finale.

Soit P un p-sous-groupe de Sylow de G ; **7°** nous donne $[O_2(G), P] \subset Z(G)$, d'où

$$[O_2(G), P] = [O_2(G), P, P] = 1.$$

P centralise donc $O_2(G)$, donc

$$P \subset C_G(O_2(G)) \subset O_2(G),$$

d'où $P = 1$: absurde ! D'où le résultat.

Remerciements.

Je tiens à exprimer ma gratitude à George Glauberman et à Peter Sin pour de nombreuses discussions relatives à des sujets voisins de celui de cette note, et à Michel Enguehard pour m'avoir aidé à mettre au point la démonstration du lemme.

Bibliographie.

[1] D. Gorenstein, *« Finite groups »*, Chelsea, New York, 1980.

[2] D. Gorenstein, *« Finite simple groups »*, Academic Press, New York, 1982.

[3] M. Hayashi, 2-factorization in finite groups, *Pacific J. Math.*, **84** (1979), 97-142.

École normale supérieure de Lyon

Option mathématique
Première composition

6489. **Étude de l'image de $M_n(\mathbb{C})$ et de $M_n(\mathbb{R})$ par l'application exponentielle.**

(Voir l'énoncé complet dans la Revue n° 1, page 33.)

Partie I

1° Puisque $\exp(u).\exp(-u) = \mathrm{Id}$, on voit que $\exp(u)$ est inversible et

$$(\exp(u))^{-1} = \exp(-u).$$

2° *a)* L'application $(f, g) \mapsto fg$ de $(L_C(E))^2$ dans $L_C(E)$ est continue (bilinéaire en dimension finie). Par conséquent, par passage à la limite dans l'égalité

$$\forall n \in \mathbb{N}, \quad v\left(\sum_0^n \frac{u^k}{k!}\right)v^{-1} = \sum_0^n \frac{(vuv^{-1})^k}{k!}$$

on obtient

$$v \exp(u) v^{-1} = \exp(vuv^{-1}).$$

Choisissons une base de E, soit A la matrice de u dans cette base. On sait qu'il existe $P \in GL_n(\mathbb{C})$ et $T \in M_n(\mathbb{C})$ triangulaire supérieure telles que $A = PTP^{-1}$. Il est immédiat que si la diagonale principale de T est $(\lambda_1, \ldots, \lambda_n)$, celle de e^T est $(e^{\lambda_1}, \ldots, e^{\lambda_n})$. Il résulte alors de $\exp(A) = P \exp(T) P^{-1}$ que les valeurs propres de $\exp(A)$ sont $(e^{\lambda_1}, \ldots, e^{\lambda_n})$. Donc

$$\chi_u(X) = \prod_{i=1}^{n} (\lambda_i - X) \Rightarrow \chi_{\exp(u)}(X) = \prod_{i=1}^{n} (e^{\lambda_i} - X)$$

(en désignant par χ_v le polynôme caractéristique de l'endomorphisme v).

b) On a donc $\det \exp(u) = \prod_{i=1}^{n} e^{\lambda_i} = e^{\sum_{i=1}^{n} \lambda_i} = e^{tr(u)}$.

En particulier, si $A \in M_n(\mathbb{R})$, on a $\det \exp(A) = e^{tr(A)} > 0$ donc $\exp(A) \in GL_n^+(\mathbb{R})$.

3° Par un calcul facile, en posant $A = aI + \mu J$,

$$\forall k \in \mathbb{N}, \quad A^k = a^k I + k a^{k-1} \mu J \quad \text{puis} \quad \exp(A) = e^a I + e^a \mu J$$

$$\exp(A) = e^a \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}.$$

De même

$$\exp(B) = e^b \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}.$$

Pour calculer $\exp(A + B)$, lorsque

$$A + B = (a + b)I + \mu K$$

où $K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, on peut diagonaliser $A + B$ ou noter que

$$K^{2q} = I, \qquad K^{2q+1} = K,$$

d'où

$$\forall k \in \mathbb{N}, \quad (A + B)^k = \sum_{p=0}^{k} C_k^p (a + b)^{k-p} \mu^p K^p$$

$$= \left(\sum_{q=0}^{\left[\frac{k}{2}\right]} C_k^{2q} (a + b)^{k-2q} \mu^{2q} \right) I + \left(\sum_{q=0}^{\left[\frac{k-1}{2}\right]} C_k^{2q+1} (a + b)^{k-2q-1} \mu^{2q+1} \right) K$$

$$= \frac{1}{2}[(a + b + \mu)^k + (a + b - \mu)^k] I + \frac{1}{2}[(a + b + \mu)^k - (a + b - \mu)^k] K.$$