JOURNAL OF NUMBER THEORY 2, 235–236 (1970)

Sur une question d'Olga Taussky

JEAN-PIERRE SERRE

Collège de France,
Paris 5, France

Communicated by H. Zassenhaus

Received October 13, 1969

Soit G un groupe. Sa suite dérivée $(D^n(G))$, $n = 0, 1,...,$ est définie par les formules:

$$D^0(G) = G, \quad D^{n+1}(G) = (D^n(G), D^n(G)) \quad \text{si} \quad n \geqslant 0.$$

On pose $G^{\mathrm{ab}} = G/D^1(G)$.

Supposons que G soit un p-groupe fini, p étant un nombre premier. Lorsque G^{ab} est cyclique, il est immédiat que $D^1(G) = \{1\}$; lorsque $p = 2$ et que G^{ab} est de type $(2, 2)$, on peut montrer (cf. [6]) que $D^1(G)$ est cyclique, donc que $D^2(G) = \{1\}$. Ces cas mis à part, la connaissance de G^{ab} ne permet d'affirmer la trivialité d'aucun des $D^n(G)$. Plus précisément:

THÉORÈME. *Soit n un entier $\geqslant 1$ et soit P un p-groupe abélien fini qui ne soit, ni cyclique, ni d'ordre 4. Il existe alors un p-groupe fini G tel que $D^n(G) \neq \{1\}$ et $G^{\mathrm{ab}} \simeq P$.*

(Ceci répond à la question posée dans [7], question qui avait d'ailleurs été résolue lorsque $p \neq 2$ ou lorsque P est "assez gros", cf. [1], [2].)

Démonstration. Puisque P n'est pas cyclique, on peut l'écrire comme produit $P = A \times B$, où A et B sont non triviaux. Notons a (resp. b) l'ordre de A (resp. B); on a

$$a \geqslant 2, \qquad b \geqslant 2, \qquad ab > 4.$$

Considérons le *produit libre* $A * B$ de A et de B ([4], p. 180) et soit $r : A * B \to A \times B$ l'homomorphisme canonique de ce groupe sur $A \times B$. Le noyau R de r est le groupe $D^1(A * B)$; de plus, on vérifie facilement (cf. par exemple [4], p. 196, exerc. 24) que R est un *groupe libre* de base la famille des commutateurs $x^{-1}y^{-1}xy$, avec $x \in A - \{1\}$, $y \in B - \{1\}$ (les commutateurs étant pris dans $A * B$). Le rang de R est $(a - 1)(b - 1)$; vu les inégalités ci-dessus, il est $\geqslant 2$, i.e. R est *non abélien*. Il en résulte que l'on a $D^m(R) \neq \{1\}$ pour tout $m \geqslant 0$. Choisissons alors un élément $z \neq 1$

de $D^{n-1}(R) = D^n(A * B)$. On sait, depuis Magnus, que tout groupe libre est *séparé* pour la p-topologie (celle définie par les sous-groupes distingués d'indice une puissance de p); cf., par exemple, [3], chap. I, n° 5 ou Bourbaki, *Gr. et Alg. de Lie*, chap. II, §5, n° 5. Il existe donc un sous-groupe distingué N de R, d'indice une puissance de p, ne contenant pas z. Quitte à remplacer N par l'intersection de ses conjugués dans $A * B$, on peut supposer que N est distingué dans $A * B$. Le groupe $G = (A * B)/N$ répond alors à la question. En effet, c'est une extension de $A \times B$ par R/N, donc un p-groupe; le groupe G^{ab} s'identifie à $A \times B = P$; enfin $D^n(G)$ contient l'image de z, qui n'est pas égale à 1 par construction.

Remarques

(1) On peut, si l'on veut, imposer à $D^n(G)$ de contenir un élément d'ordre p^m, avec m donné.

(2) L'argument utilisé plus haut montre en fait ceci: soient A et B deux p-groupes finis, et soit $A *_p B$ le *pro-p-groupe* (cf. [5], chap. I, n° 1.4) complété de $A * B$ pour la p-topologie; c'est le produit libre de A et B dans la catégorie des pro-p-groupes. On a alors une suite exacte

$$\{1\} \to R_p \to A *_p B \to A \times B \to \{1\},$$

où R_p est un pro-p-groupe libre (*loc. cit.*, n° 1.5) de base la famille des commutateurs $x^{-1}y^{-1}xy$ avec $x \in A - \{1\}$, $y \in B - \{1\}$.

(3) On peut également démontrer le théorème en construisant explicitement un groupe G ayant les propriétés voulues. Par exemple, lorsque P est de type (2, 2, 2) on peut prendre pour G le sous-groupe de $\mathbf{GL}(2, \mathbf{Z}/2^N\mathbf{Z})$, $N \geqslant 5.2^n$, engendré par les trois matrices d'ordre 2 que voici: $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & 4\\ 0 & -1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & 0\\ 4 & -1\end{smallmatrix}\right)$. C'est la méthode suivie dans [1].

Bibliographie

1. C. R. Hobby, The derived series of a finite p-group, *Illinois J. Math.* **5** (1961), 228–233.
2. N. Ito, Note on p-groups, *Nagoya Math. J.* **1** (1950), 113–116.
3. M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, *Ann. Sci. ENS* **71** (1954), 101–190.
4. W. Magnus, A. Karrass et D. Solitar, "Combinatorial Group Theory," Wiley (Interscience), New York, 1966.
5. J.-P. Serre, "Cohomologie Galoisienne," Lecture Notes in Mathematics, n° 5, Springer-Verlag, New York/Berlin, 1965.
6. O. Taussky, A remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.
7. O. Taussky, Research problem 9, *Bull. Amer. Math. Soc.* **64** (1958), 124.