168. Sur les Groupes Factorisables par Deux 2-Groupes Cycliques. I

(*Cas où leur groupe des commutateurs est cyclique*)

Par Noboru ITÔ et Akiko ÔHARA

(Comm. by K. SHODA, M.J.A., Dec. 13, 1956)

1. On dit qu'un groupe G est «factorisable» par deux sous-groupes A et B, si tout élément g de G peut se mettre sous la forme $g=ab$ avec a de A et b de B. Nous avons ainsi un groupe factorisable sous la forme $G=AB=BA$. Parmi les résultats récemment publiés sur ce sujet, les théorèmes suivants sont nécessaires pour l'étude qui va suivre: *soit G un groupe factorisable par deux sous-groupes arbitraires A, B et soit (A, B) le sous-groupe engendré par tous les commutateurs $(a, b)=aba^{-1}b^{-1}$ avec a de A et b de B. Alors (A, B) est toujours un sous-groupe distingué de G [4]; si G est un groupe factorisable par deux sous-groupes abéliens, le groupe des commutateurs G' de G est abélien [2, 4].* En particulier, le cas où G est un groupe factorisable par deux p-groupes cycliques, a été étudié par B. Huppert [1]: *on a $d(G')=1$ pour $p\neq 2$ et $d(G')\leqq 2$ pour $p=2$, où $d(G')$ désigne le nombre des générateurs indépendants de G'*; et de plus, *pour $p=2$, lorsque $A\frown B=1$ G' ne peut être un groupe abélien du type $(2^r, 2^r)$, où γ est un entier positif* [3]. Or, nous allons déterminer la structure du groupe factorisable par deux 2-groupes cycliques.

2. Nous considérons d'abord la structure d'un groupe factorisable par deux 2-groupes cycliques dont le groupe des commutateurs G' est cyclique.

Théorème 1. *Soit G un p-groupe, où $p\geqq 2$. Si son groupe des commutateurs G' est cyclique et s'il existe un sous-groupe cyclique N tel que $N\supsetneqq G'$, on peut trouver un sous-groupe cyclique L tel que l'on ait $L\supseteqq N$ et $L\subsetneqq \Phi(G)$, où $\Phi(G)$ est le groupe de Frattini de G.*

En effet, comme G/G' est abélien on peut trouver un groupe quotient cyclique L/G' tel que $L/G'\subsetneqq \Phi(G/G')$, où $L/G'\supseteqq N/G'$. Et de plus, on a $\Phi(G/G')=\Phi(G)G'/G'=\Phi(G)/G'$, car G est un p-groupe. D'où il existe un sous-groupe L tel que $L\supseteqq N$, $L\subsetneqq\Phi(G)$ et que L/G' est cyclique.

Ensuite, montrons que ce sous-groupe L est cyclique. Désignons par $\overline{H}$ le groupe quotient par G' d'un sous-groupe H contenant G'. Soient N, G', $\overline{L}$ engendrés par n, c, $\overline{l}$ respectivement. Soit l'indice $(\overline{L}:\overline{N})$=l'indice $(L:N)=p^m$ avec un entier $m\geqq 0$. On a alors $\overline{l}^{p^m}=\overline{n}^{\gamma}$ avec un certain entier γ, où $\overline{n}$ est la classe à laquelle n appartient.

On peut voir aisément que $(\gamma, p)=1$, c'est-à-dire que $\gamma=\delta p+q$ où $p>q>0$. Dès que $\bar{l}^{p^m}=\bar{n}^r$, on a $l^{p^m}=n^r c^\alpha$ où l est un représentant du générateur $\bar{l}$ et α est un certain entier. Comme c^α appartient à N, il existe un entier β tel que $c^\alpha=n^{p^\beta}$. On a alors $l^{p^m}=n^r c^\alpha=n^{\delta p+q}n^{p^\beta}=n^{\delta p+p^\beta+q}$. Donc, il s'en suit que $\{l^{p^m}\}=\{n^{\delta p+p^\beta+q}\}=\{n\}=N$. Cela signifie que l a l'ordre $p^m|N|$ où $|N|$ désigne l'ordre de N, c'est-à-dire que L est un groupe cyclique engendré par l, c.q.f.d.

Théorème 2. *Soit G un groupe factorisable par deux 2-groupes cycliques A, B. Si son groupe des commutateurs G' est cyclique et s'il existe un sous-groupe cyclique N tel que $N\supsetneqq G'$, il existe alors un sous-groupe cyclique L tel que $L\supsetneqq G'$ et que le groupe quotient G/L est cyclique.*

En effet, d'après le Théorème 1, il existe un sous-groupe cyclique L tel que $L\supseteqq N$ et $L\subsetneqq\Phi(G)$. D'autre part, il est bien connu que $G/\Phi(G)$ est un groupe abélien du type $(2, 2)$, ou un groupe cyclique d'ordre 2. Mais dans le dernier cas, G est cyclique. Ainsi $G/\Phi(G)$ a deux générateurs indépendants. Puisque le générateur l de L n'appartient pas à $\Phi(G)$, on peut choisir l, h comme représentants de deux générateurs de $G/\Phi(G)$: $l^2\in\Phi(G)$, $h^2\in\Phi(G)$, $G=\{l, h, \Phi(G)\}=\{l, h\}$. D'où on conclut qu'il existe un sous-groupe cyclique $\{l\}=L$ tel que $L\supsetneqq G'$ et que G/L est cyclique, c.q.f.d.

Théorème 3. *Soit G un groupe factorisable par deux 2-groupes cycliques A, B. Si son groupe des commutateurs G' est cyclique et s'il n'existe pas de sous-groupe cyclique N tel que $N\supsetneqq G'$, le groupe quotient G/G' est alors un groupe abélien du type $(2^r, 2)$. Et de plus, G peut être construit modulo $(G')^2$ par les relations $a^{2^r}=b^2=c^2=1$, $(a, b)=c$.*

On peut supposer que $G'\neq 1$. Car, si G est abélien il existe toujours un sous-groupe cyclique N tel que $N\supsetneqq 1=G'$, et alors G ne satisfait pas à la condition du théorème.

a) Cas où l'ordre $|G'|=2$.

Soient a, b, c les générateurs de A, B, G' respectivement et soient $2^\alpha, 2^\beta$ les ordres de a, b respectivement. Sans restreindre la généralité nous pouvons supposer que $\alpha\geqq\beta$. Comme G' est un sous-groupe distingué de G d'ordre 2, G' est contenu dans le centre de G. Dans ce cas, on a les relations bien connues: $(a^2, b)=(a, b^2)=1$. Cela signifie que le sous-groupe $\{a^2\}\{b^2\}$ est contenu dans le centre Z de G. Si $Z\supsetneqq\{a^2\}\{b^2\}$, le groupe G serait abélien. Donc on a $Z=\{a^2\}\{b^2\}$. Comme le générateur c de G' appartient au centre Z, c peut être représenté par une forme $c=a^{2l}b^{2m}$ avec certains entiers positifs l, m. En effet, si $2l\equiv 0\ (2^\alpha)$ ou $2m\equiv 0\ (2^\beta)$, G' serait contenu dans B ou dans A. On a

$$c^2=1=a^{4l}b^{4m},$$
$$a^{4l}=b^{-4m}\equiv 1\equiv b^{4m}\qquad (A\frown B).$$

Soient $2^{\alpha-t}$, $2^{\beta-t}$ les ordres de a, b modulo $A\cap B$ respectivement. Lorsque $A\cap B=1$, il est clair que l'on peut mettre $t=0$. Et de plus, on peut supposer que $\beta-t>1$. Car, si $\beta-t=1$, on a $b^2\in A\cap B\subsetneqq A$, A a l'indice 2 dans G et alors A serait un sous-groupe distingué de G. Comme G' est contenu dans A, G ne satisfait pas à la condition du théorème. On peut déduire des relations $a^{4l}\equiv b^{4m}\equiv 1$ $(A\cap B)$ le fait que $4l\equiv 0$ $(2^{\alpha-t})$, $4m\equiv 0$ $(2^{\beta-t})$, c'est-à-dire que $2l=h2^{\alpha-t-1}$, $2m=k2^{\beta-t-1}$ avec certains entiers positifs h, k. Si au moins un de ces entiers h, k est pair, par exemple, $h=2n$, on a

$$\begin{aligned} c=a^{2l}b^{2m}&=a^{2n2^{\alpha-t-1}}b^{k2^{\beta-t-1}}\\ &=a^{2^{\alpha-t}n}b^{k2^{\beta-t-1}}\\ &\equiv b^{k2^{\beta-t-1}} \qquad (A\cap B), \end{aligned}$$

c'est-à-dire $G'\subsetneqq B$, contrairement à l'hypothèse du théorème. Donc, h, k sont nécessairement impairs: $h=2h'+1$, $k=2k'+1$. On a alors

$$\begin{aligned} c&=a^{2l}b^{2m}\\ &=a^{(2h'+1)2^{\alpha-t-1}}b^{(2k'+1)2^{\beta-t-1}}\\ &=a^{2^{\alpha-t-1}}b^{2^{\beta-t-1}}a^{2^{\alpha-t}h'}b^{2^{\beta-t}k'}\\ &=a^{2^{\alpha-t-1}}b^{2^{\beta-t-1}}a^{2^{\alpha-t}n} \quad \text{pour un certain entier } n. \end{aligned}$$

Pour $\alpha>\beta$, on a $c=(a^{2^{\alpha-\beta}}b)^{2^{\beta-t-1}}a^{2^{\alpha-t}n}=\{(a^{2^{\alpha-\beta}}b)a^{2^{\alpha-\beta+1}n}\}^{2^{\beta-t-1}}$, où $\beta-t-1>0$. Ainsi il existe un sous-groupe cyclique $N=\{(a^{2^{\alpha-\beta}}b)a^{2^{\alpha-\beta+1}n}\}$ tel que $N\supsetneqq G'$. Pour $\alpha-t-1=\beta-t-1\geqq 2$, on a $(ab)^{2^{\beta-t-1}}=(b,a)^{\frac{1}{2}2^{\beta-t-1}(2^{\beta-t-1}-1)}a^{2^{\beta-t-1}}b^{2^{\beta-t-1}}=a^{2^{\beta-t-1}}b^{2^{\beta-t-1}}$. On en déduit que $c=(ab)^{2^{\beta-t-1}}a^{2^{\beta-t}n}=\{(ab)a^{2n}\}^{2^{\beta-t-1}}$. Comme $2^{\beta-t-1}\geqq 4$, il existe un sous-groupe cyclique $N=\{(ab)a^{2n}\}$ tel que $N\supsetneqq G'$. Donc, il nous reste à considérer le cas où $\alpha-t-1=\beta-t-1=1$. Dans ce cas on a $c=a^2b^2a^{2^{\alpha-t}n}$. Cela signifie que b^2 appartient à A modulo G' et alors que A est un sous-groupe ayant l'indice 2 modulo G' dans G. Lorsque G/G' est cyclique, G est abélien. D'où on conclut donc que G/G' est un groupe abélien du type $(2^r, 2)$.

b) Cas où l'ordre $|G'|>2$.

Soit g un générateur de G' et soit G_0 le sous-groupe cyclique engendré par l'élément g^2. Il est clair que G_0 est un sous-groupe distingué de G. On a $(G/G_0)'=G'G_0/G_0=G'/G_0$. Donc $(G/G_0)'$ a l'ordre 2. S'il existe un groupe cyclique L/G_0 tel que $L/G_0\supsetneqq(G/G_0)'$, on aurait $\{l\}G_0/G_0\supsetneqq G'/G_0$ et alors $\{l\}G_0\supsetneqq G'$, où l est un représentant du générateur de L/G_0. Donc on aurait $\{l\}\supsetneqq G'$, ce qui est contraire à l'hypothèse du théorème. D'où on résulte qu'il n'existe pas de groupe quotient L/G_0 tel que $L/G_0\supsetneqq(G/G_0)'$. D'après le cas démontré a), $G/G_0/(G/G_0)'$ est un groupe abélien du type $(2^r, 2)$. L'isomorphisme

$G/G_0/(G/G_0)'=G/G_0/G'/G_0\cong G/G'$ nous donne que G/G' est aussi un groupe abélien du type $(2^\gamma, 2)$.

c) Construction d'un groupe G modulo $(G')^2$.

Supposons que l'on peut construire G modulo $(G')^2$ dans le cas où l'ordre $|G'|=2$. Dans le cas où l'ordre $|G'|>2$, comme l'ordre $|(G/G_0)'|=2$, on peut construire G/G_0 modulo $\{(G/G_0)'\}^2=(G'/G_0)^2$. D'après que $G/G_0/(G'/G_0)^2\cong G/(G')^2$ on peut construire G modulo $(G')^2$. Donc, il est suffisant de montrer que l'on peut construire G modulo $(G')^2$ dans le cas où l'ordre $|G'|=2$.

Soit G/G' un groupe quotient abélien du type $(2^\gamma, 2)$. Soient a, b deux représentants des générateurs de G/G': $a^{2^\gamma}\in G'$, $b^2\in G'$. Si $a^{2^\gamma}=c$ ou $b^2=c$, où c est un générateur de G', on aurait alors $\{a\}\supsetneqq\{c\}$ ou $\{b\}\supsetneqq\{c\}$, ce qui est contraire à l'hypothèse du théorème. Donc on a $a^{2^\gamma}=1$, $b^2=1$. En conséquence on a $G=\{a\}\{b\}\{c\}=\{a\}\{b\}$ selon les relations $a^{2^\gamma}=b^2=c^2=1$, $c=(a, b)$, c.q.f.d.

3. a) On peut démontrer directement le Théorème 2 sans utiliser le Théorème 1. Car, G/G' est produit direct de deux groupes quotients cycliques. Soient f, g deux représentants des générateurs de G/G': $f^{2^\gamma}\in G'$, $g^{2^\delta}\in G'$, $G/G'=\{\bar{f}\}\times\{\bar{g}\}$. Alors il nous reste à examiner dans les quatres cas: $f^{2^\gamma}=c$, $g^{2^\delta}=c$; $f^{2^\gamma}=c$, $g^{2^\delta}=1$; $f^{2^\gamma}=1$, $g^{2^\delta}=c$; $f^{2^\gamma}=1$, $g^{2^\delta}=1$. Dans les trois premiers cas, le théorème est évidemment établi. Dans le dernier cas on peut voir par les calculs élémentaires le fait qu'il n'existe pas de sous-groupe cyclique N tel que $N\supsetneqq G'$, excepté le cas où $\gamma=\delta=1$. Mais pour $\gamma=\delta=1$, la structure du groupe est bien connue et ainsi le théorème est vrai.

b) Comme on a le cas trivial pour $\alpha=1$ ou $\beta=1$, on peut supposer que $\alpha>1$ et $\beta>1$. Dans le cas où $A\frown B=1$ et l'ordre $|G'|=2$, on peut choisir le sous-groupe L du Théorème 2 tel que $L=\{a^{2^{\alpha-\beta}}b\}$ pour $\alpha>\beta$ ou $\alpha=\beta>2$, et il n'existe pas de sous-groupe cyclique contenant proprement G' pour $\alpha=\beta=2$. En effet, par démonstration du Théorème 3 on peut voir facilement que $G=\{a\}\{b\}=\{a^{2^{\alpha-\beta}}b\}\{a\}$ et $\{a^{2^{\alpha-\beta}}b\}\supsetneqq G'$, excepté dans le cas où $\alpha=\beta=2$. La structure du groupe G est très simple dans le cas où l'ordre $|G'|=2$ et $\alpha=\beta=2$.

c) Lorsque b^2 appartient au centre de G, G' est un sous-groupe cyclique engendré par le commutateur (a, b) et l'ordre de G' est égal au nombre minimal n pour que a^n appartient au centre de G. En effet, pour le groupe $G=\{a\}\{b\}=\{a\}\{b^2\}\cdot\{b\}$ on a $G'=(\{a\}\{b^2\})'$ $(\{a\}\{b^2\}, \{b\})=(\{a\}, \{b^2\})(\{a\}\{b^2\}, \{b\})=(\{a\}\{b^2\}, \{b\})\subseteqq\{a\}\{b^2\}$ [4]. D'autre part G' est engendré par tous les commutateurs (a^i, b) où $0<i\leqq 2^\alpha$, car on a $(a^i, b^{2m})=1$, $(a^i, b^{2m+1})=(a^i, b)b(a^i, b^{2m})b^{-1}=(a^i, b)$. Comme il existe deux entiers l, m tels que $(a, b)=aba^{-1}b^{-1}=a^lb^{2m}$, on

a $(a^i, b)=a^iba^{-i}b^{-1}=a^{i-1}\cdot aba^{-1}b^{-1}\cdot ba^{-i+1}b^{-1}=a^{i-1}\cdot a^lb^{2m}\cdot ba^{-i+1}b^{-1}=a^lb^{2m}\cdot a^{i-1}ba^{-i+1}b^{-1}$. Donc on a des relations $(a^i, b)=(a, b)(a^{i-1}, b)$ et alors on a $(a^i, b)=(a, b)^i$. On en conclut que G' est engendré par un seul élément (a, b). Pour $(a, b)^n=1$ on a $(a^n, b)=1$, c'est-à-dire que a^n appartient au centre de G.

Références

[1] B. Huppert: Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, Math. Z., **58**, 243–264 (1953).

[2] N. Itô: Über das Produkt von zwei abelschen Gruppen, Math. Z., **63**, 400–401 (1955).

[3] N. Itô: Über das Produkt von zwei zyklischen 2-Gruppen, Pub. Math., **4**, 517–520 (1956).

[4] A. Ōhara: Note on commutator subgroups of factorisable groups, Proc. Japan Acad., **31**, 612–614 (1955).