

LUCIEN BÉNÉTEAU

**Ordre minimum des boucles de Moufang commutatives
de classe 2 (Resp. 3)**

Annales de la faculté des sciences de Toulouse 5^e série, tome 3, n° 1 (1981), p. 75-88

http://www.numdam.org/item?id=AFST_1981_5_3_1_75_0

© Université Paul Sabatier, 1981, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ORDRE MINIMUM DES BOUCLES DE MOUFANG COMMUTATIVES DE CLASSE 2 (RESP. 3)

Lucien Bénéteau ⁽¹⁾

(1) Université Paul Sabatier, 118 route de Narbonne, 31062 Toulouse Cédex - France.

Résumé : Disons «M-boucle» pour Boucle de Moufang commutative finie. Le but est ici de montrer que :

(i) toute M-boucle d'ordre non divisible par 81 (resp. 6561) est associative (resp. de classe ≤ 2), et que :

(ii) il y a exactement deux M-boucles non associatives d'ordre 81, l'une d'exposant 3, l'autre d'exposant 9. Ce dernier point doit être rapproché du fait bien connu que, pour tout premier p , l'ordre minimum des p -groupes non commutatifs est p^3 , et que si $p \geq 3$ il y a seulement deux groupes non commutatifs d'ordre p^3 , l'un d'exposant p , l'autre d'exposant p^2 . Mais nous verrons que l'ordre minimum des M-boucles de classe 3 n'est autre que $6561 = 3^8$, ce qui ne ressemble en rien aux propriétés correspondantes en théorie des groupes. Ce résultat est la clef des quelques théorèmes de classification des M-boucles de petite cardinalité dont nous disposons actuellement.

Summary : The aim of this paper is to show that

(i) any commutative Moufang loop (CML) whose order is not divisible by 81 (resp. 6561) is associative (resp. centrally nilpotent of class < 2), and that

(ii) there are exactly two non-associative CMLs of order 81, one being of exponent 3 and the other one of exponent 9. This last statement is to be compared with the well-known fact that for any prime p the minimum order of the non-commutative p -groups is p^3 , and that, if $p \neq 2$, there are only two non-commutative groups of order p^3 , one of exponent p , and the other one of exponent p^2 . But we shall prove that the minimum order of the CMLs of class 3 is accurately $6561 = 3^8$, a fact without any comparable group-theoretical analogous. Now this result is the key of the few classification theorems of small order CMLs that are now at our disposal.

I - INTRODUCTION ET CONVENTIONS

1.1. - Une *boucle commutative* sera ici un ensemble fini E muni d'une loi de composition interne commutative $x, y \mapsto x \cdot y$ qui possède une unité 1 (i.e. un élément vérifiant $1 \cdot x = x$ pour chaque x de E) et qui obéit à la «règle de simplification», en ce sens que $x \cdot y = x \cdot z$ entraîne $y = z$. Toute translation $y \mapsto x \cdot y$ est alors une permutation de E , d'où l'existence d'un inverse unique x^{-1} associé à chaque élément x . Une *sous-boucle* de (E, \cdot) peut se définir comme une partie stable non vide de E . Si x appartient à une sous-boucle H , la restriction à H de $y \mapsto x \cdot y$ est une permutation de H , de sorte que H contient 1 et x^{-1} . Une *boucle de Moufang commutative* (ou *M-boucle*) sera une boucle commutative où l'on a l'identité :

$$(x \cdot y) \cdot (x \cdot z) = x^2 \cdot (y \cdot z) \quad \text{avec} \quad x^2 = x \cdot x$$

C'est là une généralisation des groupes abéliens (finis). Les x_i étant des éléments d'une M-boucle, les produits $a = (x_0 \cdot x_1) \cdot x_2$ et $b = x_0 \cdot (x_1 \cdot x_2)$ ne sont en général pas égaux, mais il existe toujours un élément α_1 unique pour lequel $a \cdot \alpha_1 = b$; on définit les «associateurs» $\alpha_r = (x_0, x_1, x_2, \dots, x_{2r-1}, x_{2r})$ par récurrence sur $r \geq 1$ en posant que $\alpha_1 = (x_0, x_1, x_2)$ est l'élément $a^{-1} \cdot b$ précédemment défini et que $\alpha_{r+1} = (\alpha_r, x_{2r+1}, x_{2r+2})$.

THEOREME 1.2. *Soit E une M-boucle engendrée par d éléments. Si $d = 1$ ou 2 , alors E est un groupe abélien (théorème de MOUFANG [9]). Plus généralement pour $d \geq 2$ on a $\alpha_r = 1$ identiquement dès que $r \geq d - 1$ (théorème de BRUCK-SLABY [9]).*

Définition. Le plus petit entier k pour lequel $\alpha_k = 1$ identiquement se nomme la classe de nilpotence «centrale» (ou «associative») de la M-boucle E ; nous dirons simplement : *la classe de E* , et nous la noterons $k(E)$.

Retenons que $k(E) \leq \sup(d-1, 1)$ lorsque E admet un système générateur comprenant d éléments.

1.3. - Dans la suite E désigne une M-boucle. Pour toute sous-boucle H de E , l'ordre de H , soit $|H|$, divise $|E|$, et nous noterons $[E : H]$ l'indice de H dans E , i.e. le quotient $|E| / |H|$. L'ordre d'un élément x de E est classiquement défini comme l'ordre de la sous-boucle qu'il engendre. Nous appellerons *exposant de E* le plus petit commun multiple des ordres des éléments de E . Par définition une *M_3 -boucle* sera une M-boucle qui est soit d'exposant 3, soit réduite à $\{1\}$. Nous renvoyons le lecteur à la bibliographie pour des interprétations des M_3 -boucles en termes de «designs» (système triples de Steiner où tout plan est affine [3] [6] [14], matroïdes parfaits [6] [12] et schémas d'association [12]).

1.4. - Si x et y sont des éléments de la M -boucle E , alors l'application $z \rightarrow z \cdot (x,y,z)$ est un automorphisme de E , dit «automorphisme intérieur» (cf. [9]). Nous écrivons $H < E$ pour exprimer que H est une sous-boucle de E , et $H \triangleleft E$ pour « H sous-boucle normale de E », i.e. sous-boucle invariante par tout automorphisme intérieur. Si $H \triangleleft E$ et $K \triangleleft E$ alors $H.K \triangleleft E$. Le centre de E est l'ensemble $Z(E)$ des éléments invariants par tout automorphisme intérieur, autrement dit c'est l'ensemble des z vérifiant $(x,y,z) = 1$ pour tout couple x,y .

La sous-boucle dérivée de E , soit $E' = \mathcal{D}(E)$, est la sous-boucle engendrée par les associateurs. La sous-boucle de Frattini de E , soit $\Phi(E)$, est l'intersection des sous-boucles maximales de E . Notons en outre $\theta(E)$ l'ensemble des x^3 pour x parcourant E , et $G(E)$ (resp. $H(E)$) l'ensemble des éléments de E dont l'ordre est premier à 3 (resp. une puissance de 3). Par construction $Z(E)$, E' et $\Phi(E)$ sont des sous-boucles. Il en va de même de $\theta(E)$, $G(E)$ et $H(E)$ puisque l'on a $(x.y)^n = x^n.y^n$ identiquement pour tout entier n . En outre, chacune de ces six sous-boucles remarquables est normale, puisqu'invariante par tout automorphisme.

PROPOSITION 1.5. La boucle E est produit direct de $G(E)$ (qui est un groupe abélien) et de $H(E)$ (dont l'ordre est une puissance de 3). En outre $Z(E)$ contient $G(E) \cdot \theta(E)$ tandis que E' est contenu dans $H(E) \cap \Phi(E)$.

Preuve. Voir BRUCK [8], et pour $E' \subset \Phi(E)$, voir [3].

COROLLAIRE. La sous-boucle dérivée E' et le quotient central $E / Z(E)$ d'une M -boucle sont des M_3 -boucles. Lorsque E n'est pas un groupe abélien, $[E : Z(E)] \geq 27$.

Preuve. Soit $[E : Z(E)] = 3^c$. Si $c \leq 2$, $E/Z(E)$ est engendré par deux éléments, donc E est un groupe abélien d'après le théorème de MOUFANG (voir [3] pour plus de détails).

Définition. Pour tout $k > 1$, soit s_k l'ordre minimum des M -boucles de classe k .

Puisque $k(E) = k(H(E))$, on a :

COROLLAIRE 1.6. Pour tout $k > 1$, s_k est une puissance de 3, et toute M -boucle d'ordre non divisible par s_k est de classe $< k$.

Nous allons montrer en section 2 :

THEOREME 1.7. L'ordre minimum des M -boucles de classe 2 est $s_2 = 81$; en outre il y a exactement deux M -boucles non associatives d'ordre 81, l'une d'exposant 3, l'autre d'exposant 9.

Cet énoncé ne surprendra guère. S'agissant des p -groupes, p étant un premier, on sait que l'ordre minimum des non commutatifs n'est autres que p^3 , et si $p \neq 2$ il existe en tout et pour tout deux groupes non commutatifs d'ordre p^3 , l'un d'exposant p , l'autre d'exposant p^2 . Celui qui est d'exposant p n'est autre que le groupe des matrices de forme :

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \gamma & \beta & 1 \end{pmatrix}$$

où $\alpha, \beta, \gamma \in \mathbb{F}_p$.

Le léger décalage que nous avons pour les M -boucles ($81 = 3^4$, alors que l'ordre minimum est 3^3 pour les 3-groupes non commutatifs) provient de ce que le centre d'une M -boucle non associative est d'indice $\geq 3^3$, alors que le centre d'un p -groupe non commutatif est d'indice minoré seulement par p^2 ... Par ailleurs il a été maintes fois démontré que 81 est le plus petit ordre possible pour une M_3 -boucle non associative (Marshall HALL Jr. [13] , J.P. SOUBLIN [18]). Il est en outre bien connu que la M_3 -boucle libre en 3 générateurs, que l'on note L_3 , est la seule M_3 -boucle non associative d'ordre 81 (voir [18] par exemple) ; en fait L_3 n'est autre que la boucle décrite par ZASSENHAUS et BOL (cf. [7]), premier exemple connu de boucle de Moufang finie et non associative...

Concernant la classe 3, le résultat était peu prévisible, car il ne ressemble aucunement aux propriétés correspondantes dans les p -groupes :

THEOREME 1.8. *L'ordre minimum des M -boucles de classe 3 est $s_3 = 6561 = 81^2 = 3^8$; et les M -boucles de classe 3 et d'ordre 6561 sont soit d'exposant 3, soit d'exposant 9.*

Cet énoncé est essentiel, car il sert de soubassement aux quelques théorèmes de classification que nous avons pu énoncer concernant les M -boucles de petite cardinalité ; il conduit entre autres à la preuve du fait qu'il existe en tout et pour tout cinq M_3 -boucle non associatives d'ordre $\leq 3^6$ (voir [6]). Mais ce résultat ne sera pas établi ici, non plus que le fait que l'on a exactement trois M_3 -boucles d'ordre 6561 et de classe 3 (énoncé sans démonstration dans [4]). S. KLOSSEK avait construit une M_3 -boucle de classe 3 et d'ordre 6561 (voir [17]), mais c'est BRUCK qui a construit les premiers exemples de M -boucle de classe 3 (tous les exemples présentés par BOL étaient de classe 2) ; nous verrons que le procédé de construction présenté par BRUCK, appliqué au plus petit des groupes de BURNSIDE d'exposant 3 et de classe 3, à savoir $\mathbb{B}(3, 3)$, donne précisément une M_3 -boucle de classe 3 et d'ordre 6561.

Les égalités : $s_2 = 81$ et $s_3 = 81^2$ laisseraient penser que les s_k seraient des puissances de 81... Pourtant il semblerait raisonnable de conjecturer que $s_4 = 3^{22}$ (?), le nombre 22 correspondant à une certaine famille d'associateurs qui doivent être libres dans toute M-boucle de classe 4. Ce point ne sera pas détaillé ici.

Nous utiliserons fréquemment la :

PROPOSITION 1.9. (Voir [3]). *Si E est une M-boucle d'ordre une puissance de 3, $\Phi(E)$ est la plus petite sous-boucle normale par laquelle le quotient est un 3-groupe abélien élémentaire - autrement dit $\Phi(E) = E' \cdot \theta(E)$. Tous les systèmes générateurs minimaux de E ont même cardinal d avec $[E : \Phi(E)] = 3^d$. En outre $d \geq k(E) + 1$, d'après 1.2.*

2 - LES M-BOUCLES NON ASSOCIATIVE D'ORDRE MINIMUM

2.1. - Soit E une M-boucle non associative ; puisque $H = H(E)$ est également non associative, $[H : \Phi(H)] \geq 3^3$ car H ne saurait être engendré par deux éléments ; en outre $\Phi(H) \supset H'$, et H' est d'ordre au moins 3. Donc $|E| \geq |H| \geq 3^4 = 81$.

Si $|E| = 81$, alors $E = H$ et nécessairement $[E : \Phi(E)] = 3^3$, $\Phi(E) = E'$ et $|E'| = 3$. Comme nous savons que la M_3 -boucle libre en trois générateurs, notée L_3 , est la seule M_3 -boucle non associative d'ordre 81, il nous reste seulement à examiner le cas où E n'est pas d'exposant 3. Définissons N_3 comme la M-boucle en 3 générateurs u, v, w soumis aux seules relations :

$$u^3 = 1 = v^3 \quad \text{et} \quad (u,v,w) = w^3.$$

En reprenant les calculs de [8] p. 329, on montre que tout élément X de N_3 s'écrit sous la forme :

$$X = u^{x_1} \cdot v^{x_2} \cdot w^a \quad \text{avec} \quad x_i \in \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} \quad \text{et} \quad a \in \mathbb{Z}_9 = \mathbb{Z}/9\mathbb{Z},$$

le produit de deux tels éléments X et $Y = u^{y_1} \cdot v^{y_2} \cdot w^b$ étant

$$X \cdot Y = u^{z_1} \cdot v^{z_2} \cdot w^c$$

avec $z_1 = x_1 + y_1$, $z_2 = x_2 + y_2$ et $c = a + b + 3(y_1 - x_1)(x_2 b_3 - a_3 y_2)$. Or, une vérification directe montre que les trois formules ci-dessus donnent dans $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$ une loi de M-boucle engendrée par $U = (1,0,0)$, $V = (0,1,0)$ et $W = (0,0,1)$, lesquels vérifient les trois relations imposées

aux générateurs de N_3 . De ce fait, la boucle ainsi décrite est N_3 .

PROPOSITION 2.2. *Les boucles L_3 et N_3 sont, à un isomorphisme près, les seules M-boucles non associatives d'ordre 81. L'exposant de N_3 est 9.*

Preuve. Soit $\theta(E) = \{x^3 \mid x \in E\}$, où E est une M-boucle non associative d'ordre 81. Si $\theta(E) \neq \{1\}$, puisque $\theta(E) \subset \Phi(E) = E'$ qui est d'ordre 3, on a $|\theta(E)| = 3$. Cela signifie que l'endomorphisme de E défini par $x \mapsto x^3$ a pour noyau une sous-boucle K d'indice 3 dans E . Comme K est maximale, K contient $\Phi = \Phi(E)$. Nous avons déjà observé que $[E : \Phi] = 3^3$ nécessairement, donc $[K : \Phi] = 3^2$. Prenons deux éléments u et v de K tels que $u\Phi$ et $v\Phi$ engendrent K/Φ . Si $w \in E \setminus K$, alors u, v, w engendrent E , et donc $\alpha = (u, v, w)$ engendre E , donc $w^3 = \alpha^\epsilon$ avec $\epsilon = \pm 1$. On se ramène au cas $\epsilon = 1$ en remplaçant au besoin u par u^{-1} . Par ailleurs $u^3 = 1 = v^3$ puisque u et v sont dans K . Nous avons donc vu que, si E n'était pas d'exposant 3, E était représentation de N_3 ; en fait $|E| = |N_3|$, donc E est isomorphe à N_3 , q.e.d.

2.3. - Quelques remarques bibliographiques

A la connaissance de l'auteur, le théorème qui précède -ou du moins une assertion équivalente- a été démontré par KEPKA et NEMEC. Ces deux chercheurs tchèques m'ont envoyé un manuscrit («Commutative Moufang loops and distributive groupoids of small order», Université de Prague; reçu en Octobre 1979), dans lequel on peut voir entre autres une description relativement précise de toutes les M-boucles finies en trois générateurs, avec en outre l'énoncé d'un très beau théorème de classification des M-boucles non associatives d'ordre $243 = 3^5$: il en existe seulement six. On savait depuis [3] qu'il n'en existait qu'une d'exposant 3, à savoir $F_3 \times L_3$ (produit direct du 3-groupe élémentaire d'ordre 3 par L_3). Ce dernier résultat, présenté par l'auteur au 6th British Combinatorial Conference en 1977, a été démontré indépendamment par KEPKA en termes de «quasigroupes de Steiner distributifs» (cf. [15]). Il suffira de consulter [1] ou [18] pour se convaincre du fait que la classification des quasigroupes de Steiner distributifs en classes d'isomorphie se ramène à celle des M_3 -boucles. S'agissant des M_3 -boucles non associatives, l'on sait montrer à présent qu'il y en a exactement 3 d'ordre 3^6 et au moins 6 d'ordre 3^7 (voir [6]). Mais on ignore, à la connaissance de l'auteur, le nombre exact des M_3 -boucles d'ordre 3^7 et celui des M-boucles d'ordre 3^6 ... Les travaux de O. CHEIN ([10] et [11]) ne sont ici d'aucun secours car ils portent exclusivement sur les boucles de Moufang non commutatives d'ordre < 81 .

3 - LES p-GROUPES ET LES 3-M-BOUCLES

3.1. - Formellement, l'énoncé démontré dans la section précédente rappelle le résultat classique suivant :

PROPOSITION 3.1. *Si p est un nombre premier, il existe seulement deux groupes non abéliens d'ordre p^3 . Lorsque $p \neq 2$, ces groupes \mathcal{G}_p et \mathcal{H}_p sont d'exposant respectifs p et p^2 . On peut décrire \mathcal{G}_p comme l'objet libre en deux générateurs parmi les groupes d'exposant p et de classe ≤ 2 , tandis que \mathcal{H}_p n'est autre que le groupe en deux générateurs u et v soumis aux seules relations $u^p = 1 = v^{p^2}$ et $(u,v) = v^p$. (Voir par exemple H.J. ZASSENHAUSS, The theory of groups, Chelsea Publishing Company, 2nd édition 1958).*

3.2. - De fait, les boucles L_3 et N_3 peuvent se reconstruire en utilisant le :

THEOREME 3.2 (BRUCK). *Soit G un groupe tel que l'application $h : G \rightarrow G$ définie par $h(x) = x^3$ est un endomorphisme de G dans le centre de G. Alors :*

(i) *G est centralement nilpotent de classe $k \leq 3$*

(ii) *le produit cartésien $\mathbb{F}_3 \times G$, de terme générique (r,x) avec $r \in \mathbb{F}_3 = \{-1,0,1\}$ et $x \in G$, organisé par la loi binaire :*

$$(r,x) * (s,y) = \begin{cases} (r+s, xy) & \text{si } r-s = -1 \\ (r+s, x^{-1}yx^2) & \text{si } r-s = 0 \\ (r+s, yx) & \text{si } r-s = 1 \end{cases}$$

est une M-boucle de classe $k = k(G)$ pour la nilpotence centrale associative.

(iii) *sur chaque sous-groupe monogène, la loi de groupe canonique du produit cartésien $\mathbb{F}_3 \times G$ induit même structure que la M-boucle considérée.*

Preuve. Seul (iii) ne figure pas dans [8]. Mais si $y = x^n$ nous avons $xy = x^{n+1} = x^{-1}yx^2 = yx$, de sorte que

$$(r,x) * (nr,x^n) = ((n+1)r,x^{n+1}).$$

On en déduit que $(\mathbb{F}_3 \times G, *)$ admet pour neutre $(0,1_G)$, que tout (r,x) a pour inverse $(-r,x^{-1})$

et, par récurrence sur n , le fait que, pour tout entier relatif n , la puissance $n^{\text{ième}}$ de (r,x) au sens de $(*)$ n'est autre que (nr, x^n) , q.e.d.

COROLLAIRE 1. Si G est un 3-groupe fini «3-abélien» (en ce sens que $(xy)^3 = x^3y^3$ identiquement dans G), alors $(\mathbb{F}_3 \times G, *)$ est une 3-M-boucle ayant même exposant que G .

COROLLAIRE 2. Les boucles $(\mathbb{F}_3 \times \mathcal{G}_3, *)$ et $(\mathbb{F}_3 \times \mathcal{H}_3, *)$ sont très exactement les deux M-boucles non abéliennes d'ordre 81, i.e. L_3 et N_3 dans cet ordre.

Preuves. On notera que, dans l'énoncé du corollaire 1, il n'est pas imposé a priori que $h(x) = x^3$ aboutisse dans le centre. Mais ceci résulte en fait de l'identité $(xy)^3 = x^3y^3$. En effet si $|G| = 3^n$, pour tout $y \in G$ l'élément $a = y^{(1+3+3^2+\dots+3^{n-1})}$ vérifie $a^{-2} = y$. Comme par ailleurs $a^{-1}x^3a = (a^{-1}xa)^3 = a^{-3}x^3a^3$, il vient $x^3 = a^{-2}x^3a^2 = yx^3y^{-1}$ valable pour tout y , ce qui signifie que x^3 est un élément central. Ceci est du reste général : tout p -groupe p -abélien a un centre qui contient toutes les puissances $p^{\text{ièmes}}$. En outre, pour qu'un p -groupe soit p -abélien, il suffit qu'il soit de classe ≤ 2 et que son dérivé soit d'exposant p . Donc \mathcal{H}_3 est 3-abélien ($\mathcal{H}_3 = \langle (u,v) \rangle$) et l'on peut appliquer le théorème, q.e.d.

3.3. - Pour chaque entier $n \geq 1$, désignons par $\mathbb{B}(n,3)$ l'objet libre en n générateurs dans les groupes d'exposant 3. Naturellement $\mathbb{B}(1,3) \cong (\mathbb{F}_3, +)$. On montre en outre que $\mathbb{B}(2,3) \cong \mathcal{G}_3$, qui est de classe 2, et nous avons le :

THEOREME DE LEVI ET VAN DER WAERDEN. Le groupe $\mathbb{B}(n,3)$ est d'ordre $3^{f(n)}$ avec $f(n) = n + \binom{n}{2} + \binom{n}{3}$. Il est centralement nilpotent de classe 3 dès que $n \geq 3$ (voir LEVI, F. et

B.L. VAN DER WAERDEN : Über eine besondere Klasse von Gruppen, Abh. Math. Sem. Hansische Univ. 9, 154-158, 1933).

COROLLAIRE. La M-boucle $(\mathbb{F}_3 \times \mathbb{B}(3,3), *)$ est de classe 3 et d'ordre $3^8 = 6561$.

Historiquement, l'énoncé de BRUCK -que nous venons d'appliquer à $\mathbb{B}(3,3)$ - fut le premier mode de construction qui ait conduit à des M-boucles qui n'étaient pas de classe 2 (voir [9]) ; en effet tous les exemples de BOL se sont révélés être de classe 2.

4 - ORDRE MINIMUM DES M-BOUCLES DE CLASSE 3

4.1. - Nous venons de prouver l'existence d'une M-boucle de classe 3 et d'ordre $6561 = 3^8$. Il reste à démontrer que, si E est une M-boucle de classe exactement 3, son ordre est minoré par 3^8 . On peut sans perte de généralité supposer que l'ordre de E est une puissance de 3, soit 3^t . Tout système générateur de E doit contenir au moins 4 éléments -dans le cas contraire E serait de classe ≤ 2 - donc

$$[E : E'] \geq [E : \Phi(E)] \geq 3^4$$

Nous aurons donc prouvé que $t \geq 8$ si nous établissons que $|E'|$ est minoré par 3^4 , l'objet de l'énoncé qui suit :

THEOREME 4.2. *Pour qu'une M-boucle soit de classe > 2 , il faut et il suffit qu'il existe des éléments x, y, z, a pour lesquels*

$$(x, y, a, a, z) \neq 1,$$

auquel cas la sous-boucle engendrée par les 4 associateurs (x, y, a, a, z) , (x, y, a) , (y, z, a) , (z, x, a) est un 3-groupe abélien élémentaire d'ordre $81 = 3^4$.

Nous aurons besoin, pour la preuve, de la notion de «deuxième centre» $Z_2(F)$ d'une M-boucle F ; définissons-le comme l'ensemble des éléments z de la boucle pour lesquels (z, x, y, u, v) s'annule pour tout x, y, u, v dans F.

LEMME 4.3.

(i) *Pour tout quadruplet a, b, x, y d'éléments d'une M-boucle F, nous avons*

$$(a.b, x, y) = (a, x, y) \cdot (b, x, y) \cdot (a, x, y, a, b) \cdot (b, x, y, b, a).$$

(ii) *Si a (ou b) appartient à $Z_2(F)$, alors*

$$(a.b, x, y) = (a, x, y) \cdot (b, x, y)$$

(iii) *L'égalité ci-dessus est vérifiée pour tout quadruplet a, b, x, y d'éléments de F si et seulement si $Z_2(F) = F$, i.e. si F est de classe au plus 2.*

Preuve du lemme. Pour la formule de (i) se reporter en [9] p. 135. On en déduit (ii). L'égalité $(a.b, x, y) = (a, x, b).b, x, y)$ est donc vérifiée en classe 2 ; la réciproque est établie en [8] .

Preuve du théorème. Posons $\beta = (x, y, a, a, z) = f(x, y, z ; a)$. Nous avons aussi $\beta = (a, x, y, a, z)$ puisque $(a, x, y) = (x, y, a)$ (voir [9]). Donc si l'on suppose que f est identiquement nulle, la boucle considérée est de classe ≤ 2 d'après les parties (i) et (iii) du lemme précédent. Par conséquent toute M-boucle de classe > 2 contient des éléments x, y, z et a pour lesquels $\beta = (x, y, a, a, z) \neq 1$, et inversement par définition de la nilpotence.

Soit donc $\beta = (x, y, a, a, z) \neq 1$; considérons $\alpha_1 = (x, y, a)$, $\alpha_2 = (y, z, a)$ et $\alpha_3 = (z, x, a)$. La sous-boucle F engendrée par x, y, z et a est de classe ≤ 3 d'après le théorème de BRUCK-SLABY. Ceci entraîne d'abord que F' est un 3-groupe abélien élémentaire (voir [5] ou encore [9] 6.3 p. 146 ; il résulte de [9] (4.8) p. 140 que (F', F', F') est engendré par des associateurs de poids ≥ 4). Par ailleurs on peut traduire : $k(F) \leq 3$ par : $F' \subset Z_2(F)$ ou encore par : $(F', F, F) \subset Z(F)$ (voir [9]). Il résulte donc de la partie (ii) du lemme précédent que toute égalité de forme :

$$\beta^m \cdot \alpha_1^{n_1} \cdot \alpha_2^{n_2} \cdot \alpha_3^{n_3} = 1, \text{ avec } m, n_1, n_2, n_3 \in \mathbb{F}_3$$

va entraîner que :

$$\begin{aligned} (\alpha_1^{n_1}, a, z) &= (\alpha_2^{-n_2} \cdot \alpha_3^{-n_3} \cdot \beta^{-m}, a, z) \\ &= (\alpha_2^{-n_2}, a, z) \cdot (\alpha_3^{-n_3}, a, z) \cdot (\beta^{-m}, a, z) \end{aligned}$$

soit donc

$$\beta^{n_1} = (\alpha_1, a, z)^{n_1} = (\alpha_2, a, z)^{-n_2} \cdot (\alpha_3, a, z)^{-n_3}$$

puisque β^{-m} appartient à $Z(F)$. Mais :

$$(\alpha_2, a, z) = (y, z, a, a, z) = 1$$

car la sous-boucle engendrée par y, z et a est de classe au plus 2. De même $(\alpha_3, a, z) = 1$. Il reste donc $\beta^{n_1} = 1$, ce qui signifie que $n_1 = 0$ puisque $\beta \neq 1$. Nous avons montré que toute égalité de forme $\beta^m \alpha_1^{n_1} \alpha_2^{n_2} \alpha_3^{n_3} = 1$ entraînerait que n_1 était nul (modulo 3). Or les α_i sont interchangeables : il résulte de [9] p. 138, lemme 3.9, que

$$(x, y, a, a, z) = (y, z, a, a, x) = (z, x, a, a, y)$$

c'est-à-dire $\beta = (\alpha_1, a, z) = (\alpha_2, a, x) = (\alpha_3, a, y)$. Nous pouvons donc montrer en permutant circulairement les lettres x, y, z que, dans notre «combinaison linéaire» $\beta^m \cdot \alpha_1^{n_1} \cdot \alpha_2^{n_2} \cdot \alpha_3^{n_3}$, tous les n_i sont nuls. Il reste $\beta^m = 1$, qui entraîne $m = 0$ car $\beta \neq 1$. Ainsi $S = \beta, \alpha_1, \alpha_2, \alpha_3$ est bien un système libre dans F' , considéré ici comme espace vectoriel sur \mathbb{F}_3 . D'où $| \langle S \rangle | = 3^4$, q.e.d.

COROLLAIRE 4.4. *Soit G un groupe fini tel que $x \mapsto x^3$ soit un endomorphisme de G dans son centre. Si G est de classe de nilpotence centrale 2 (resp. 3) alors G est divisible par 3^3 (resp. 3^7).*

Preuve. Cet énoncé, qui est de pure théorie des groupes, peut s'établir par un calcul sur les commutateurs. Pour ce faire, on pourra se ramener au cas d'un 3-groupe puisque l'hypothèse entraîne que G est produit direct d'un 3-groupe de classe ≤ 3 et d'un groupe abélien d'ordre premier à 3... Mais il est plus simple ici de remarquer qu'un tel groupe G peut être utilisé pour produire une M-boucle d'ordre $3 \mid G$ et de classe $k = k(G)$. Les minoration de $|G|$ données dans l'énoncé se déduisent des énoncés correspondant dans les M-boucles. Soit dit en passant, ces minoration sont les meilleures possibles comme le montrent les exemples de $\mathbb{B}(2,3)$ et $\mathbb{B}(3,3)$ (voir (3.3)).

4.5. - Une conjecture sur s_4

Soit une M-boucle de classe k . On a toujours $[E : E'] \geq [E : \Phi(E)] \geq 3^{k+1}$ puisque E est engendré par au moins $k + 1$ éléments (théorème de BRUCK-SLABY). Par ailleurs il est clair que l'on a $k \geq 2$ si et seulement s'il existe un associateur (x, y, z) non nul. Nous avons montré que l'on avait $k > 3$ si et seulement s'il existe un «biassociateur» non nul de forme (x, y, a, a, z) . La propriété précédente se généralise. Par exemple l'inégalité $k \geq 4$ équivaut à la présence d'un triassociateur non nul de forme :

$$\gamma = (x, y, a, a, z, u, v)$$

Il suffit pour le voir d'exprimer que le quotient central $E/Z(E)$ est au moins de classe 3, de sorte qu'il existe dans E un biassociateur de forme $\beta = (x, y, a, a, z)$ qui n'appartient pas au centre. On montre de même par récurrence sur r que l'inégalité $k \geq r + 3$ se traduit par la présence d'un $(r + 2)$ -associateur non nul de forme :

$$\delta = (x, y, a, a, z, u_1, v_1, v_2, \dots, u_r, v_r).$$

D'un point de vue prospectif pour la détermination de s_4 , il importe de remarquer :

- d'une part, que la présence d'un associateur non nul de forme $\tau = (x, y, a, a, b, b, z)$ n'est aucunement nécessaire pour que l'on ait $k \geq 4$. Certes, nous avons montré en [5] que, lorsque E est engendré par 5 éléments, l'existence d'un τ non nul est nécessaire pour que l'on ait $k = 4$. Mais BRUCK ([9] pp. 131-132) fournit un exemple de M_3 -boucle en 6 générateurs de classe 4 où tous les τ sont nuls.

- d'autre part que si, dans une M -boucle, tous les associateurs de forme τ sont nuls, alors chaque associateur de forme $\gamma = (x, y, a, a, z, u, v)$ est antisymétrique par rapport aux cinq facteurs x, y, z, u et v .

Il semble conjecturable que, si $k \geq 4$, alors $|E'| \geq 3^{17}$ (?) et donc $|E| \geq 3^{22}$ (?)

REFERENCES

- [1] L. BENETEAU. «*Boucles de Moufang commutatives d'exposant 3 et quasigroupes de Steiner distributifs*». C.R. Acad. Sc. Paris t. 281, 1975.
- [2] L. BENETEAU. «*Les groupes de Fischer au sens restreint : (II) majorants de l'ordre et de la classe de nilpotence du dérivé en fonction de la dimension*». Note aux C.R. Acad. Sc. Paris, Série A, p. 735, 1977 ; Zbl. (1979), 389.20026.
- [3] L. BENETEAU. «*Topics about Moufang Loops and Hall triple Systems*». «Simon Stevin», vol. 54, n^o 2, pp. 107-124, avril 1980.
- [4] L. BENETEAU. «*Problèmes de majorations dans les quasigroupes distributifs et les groupes de Fischer*». Actes Colloque «Algèbre appliquée et combinatoire», pp. 22-34, Univ. Sc. et Méd. de Grenoble, juin 1978.
- [5] L. BENETEAU. «*Free commutative Moufang loops and anticommutative graded rings*». Journal of Algebra, vol. 67, n^o 1, pp. 1-35, 1980.
- [6] L. BENETEAU. «*Une classe particulière de matroïdes parfaits*». Proc. Colloque franco-canadien de Combinatoire, juin 1979, Annals of discrete Math, 8, pp. 229-232, 1980.
- [7] G. BOL. «*Gewebe und Gruppen*». Math. Ann. 114, 1937, pp. 414-431 ; Zbl. 16, 226.
- [8] R.H. BRUCK. «*Contribution to the theory of loops*». Bull. Amer. Math. Soc. 60, pp. 245-354, 1946 ; MR 8 # 134.
- [9] R.H. BRUCK. «*A survey of binary systems*». Springer, Berlin, Göttingen, Heidelberg, 1958 ; MR 20 # 76 ; 2nd printing 1968.
- [10] O. CHEIN. «*Moufang loops of small order*». Trans. Amer. Math. Soc. 188, 2, 1974.
- [11] O. CHEIN and H.O. PFLUFELDER. «*The smallest Moufang loop*». Archiv. der Math. 22, pp. 573-576, 1971.
- [12] M. DEZA. «*Finite commutative Moufang loops, related matroids, and association schemes*». A paraître in Proc. Conference on Combinatorics, 1979, Arcata, California, Humboldt State Univ., Utilitus Math.

