Note di Matematica Vol. III, 45-53 (1983)

UNE CONJECTURE SUR LES SUITES CENTRALES D'UNE BOUCLE DE MOUFANG COMMUTATIVE LIBRE

Lucien BENETEAU (*)

The lower and upper central series $\{\mathscr{C}^i(E)\}$ *and* $\{Z_j(E)\}$ *of a CML (commutative Moufang loop)* E *are defined just as the central series of a goup, the associators* $(x,y,z) = (x(yz))^{-1}((xy)z)$ *playing the same role as the commutators for groups. As was skown recently, if* $E = \mathbb{L}_n$ *(resp.* L_n*) is the free CML (resp. exponent 3 CML) on* $n \geq 3$ *generators, the common length of the central series is exactly* $n-1$. *Besides* $Z_1(\mathbf{L}_n)$ *contains a torsion-free abelian group* A_n *of rank* n *such that* $\mathbb{L}_n = L_n/A_n$. *In view of WITT's result about the central series of "the free nilpotent groups of bounded class" we conjecture that the inclusion:* $\mathscr{C}^i \subset Z_{n-1-i}$ *is in fact an equality in* L_n. *In* $\mathbb{L}_n$, *this would imply that* Z_{n-1-i} *is the direct product of* $\mathscr{C}^i$ *by* A_n. *The required equalities will be actually checked when either* $i = 1$ *or* $n \leq 4$.

(*) Université Paul Sabatier, 118, route de Narbonne, U.E.R. de Mathématiques 31062 TOULOUSE CEDEX - FRANCE -

Les *boucles de Moufang commutatives* (ou M-*boucles*) sont des généralisations des groupes abéliens (voir [1]): la commutativité, l'existence d'une unité 1 et celle d'un inverse x^{-1} associé a chaque élément x sont conservés, mais l'associativité de la loi x,y est remplacée par les deux identités suivantes:

$$x^{-1}\cdot(x\cdot y) = y, \quad \text{et} \quad (x,y)\cdot(x,z) = x^{2}\cdot(y\cdot z)$$

avec $x^2 = x\cdot x$. Les M-boucles d'exposant 3 sont celles qui vérifient $x^3 = 1$ identiquement avec $x^3 = x^2\cdot x(=x\cdot x^2)$; nous les appellerons les M_3-*boucles*. Soit E une M-boucle . L'*associateur* de trois éléments x,y,z de E est le produit:

$$(x,y,z) = (x\cdot(y\cdot z))^{-1}\cdot((x\cdot y)\cdot z) \ .$$

Nous écrirons $H < E$ pour exprimer que H est une *sous-boucle* de E (i.e. une partie non vide stable pour $x,y \mapsto x^{-1}\cdot y$), et $H \triangleleft E$ pour "H *sous-boucle normale* de E" (i.e. sous-boucle contenant tout associateur de forme (x,y,h) pour x et y dans E et h dans H). *Si* $A \triangleleft E$ *et* $H < E$, *alors* $A.H < E$. La *sous-boucle dérivée* de E, soit $E' = \mathscr{D}(E)$, est la sous-boucle engendrée par les associateurs. Le *centre* (associatif) Z(E) est l'ensemble des éléments z de E pour lesquels $(x,y,z) = 1$ identiquement.

La *sous-boucle de Frattini* $\Phi(E)$ est formée des éléments de E qui appartiennent à toute sous-boucle maximale. Chacune des sous-boucles $\mathscr{D}(E)$, $Z(E)$, $\Phi(E)$ est normale. La *suite centrale montante* de E est la suite $(Z_i(E))_{i\in\mathbb{N}}$ formée des sous-boucles $Z_i(E)$ définies inductivement par $Z_o(E) = \{1\}$ et $Z_{i+1}(E) = \{z|z\in E, \forall x,y \in E,$

$(x,y,z) \in Z_i(E)\}$. En particulier $Z_1(E)$ n'est autre que le centre $Z(E)$ précédemment défini. La *suite centrale descendante* de E est la suite des $E_i = \mathscr{C}^i(E)$ définies inductivement par $\mathscr{C}^o(E) = E$ et par le fait que $\mathscr{C}^{i+1}(E)$ est la sous-boucle engendrée par les (α,x,y) pour $\alpha \in \mathscr{C}^i(E)$ et $x,y \in E$. En particulier $\mathscr{C}^1(E) = \mathscr{D}(E)$. Si n est un entier ≥ 3, désignons par $\mathbb{L}_n$ (resp. L_n) *la* M-*boucle libre (resp. la* M_3-*boucle libre) en* n *générateurs.*

PROPOSITION 1. *Si* $E = \mathbb{L}_n$ *ou* L_n *avec* $n \geq 3$, *alors* $\Phi(E) = \mathscr{D}(E)$ *et*

$$\begin{cases} \mathscr{C}^{n-2}(E) \underset{\neq}{\supset} \{1\} = \mathscr{C}^{n-1}(E), \\ Z_{n-2}(E) \underset{\neq}{\subset} E = Z_{n-1}(E), \\ \forall i,\ 2 \leq i \leq i \leq n-1,\ \ \mathscr{C}^{n-i}(E) \subset Z_{i-1}(E). \end{cases}$$

Preuve: L'égalité $\Phi(E) = \mathscr{D}(E)$ provient de [1] et de $\Phi(E/\mathscr{D}(E)) = \{1\}$. Les autres propriétés résultent d'une réécriture du théorème de BRUCK-SLABY [3] compte tenu des précisions apportées en [2] par exemple ... En somme, les deux suites centrales associées à $\mathbb{L}_n$ (resp. L_n) ont même longueur n-1, et si l'on range les termes intermédiaires par ordre croissant pour l'inclusion, soit:

$$\mathscr{C}^{n-2} \subset \mathscr{C}^{n-3} \subset \ldots \mathscr{C}^{n-1} \ldots \subset \mathscr{C}^2 \subset \mathscr{C}^1.$$

et

$$Z_1 \subset Z_2 \subset \ldots Z_{i-1} \ldots \subset Z_{n-3} \subset Z_{n-2}.$$

nous avons entre termes de même rang une relation d'inclusion en tout point analogue à celle que nous aurions dans un groupe nilpotent.

PROPOSITION 2. *Dans* L_n *avec* $n \geq 3$, *l'avant dernier terme autre que* L_n *de la suite centrale montante coïncide avec la sous-boucle dérivée, i.e.* $Z_{n-2}(L_n) = \mathcal{D}(L_n)$.

Preuve: S'il existe un élément z dans $Z_{n-2}(L_n) \setminus \Phi(L_n)$, alors il existe un système générateur S de L_n, formé de n éléments et contenant z. Soit B une "base libre" de L_n, i.e. un ensemble de n éléments tels que L_n puisse être considéré comme la M_3-boucle libre sur B. Il existe un endomorphisme (surjectif) f de L_n pour lequel f(B) = S. Comme L_n est fini (cf. [1] par exemple), f est en fait un isomorphisme de sorte que S est aussi une base libre. Mais alors toute permutation de S s'étend en un isomorphisme de L_n, de sorte que la présence d'un élément de S qui appartient à $Z_{n-2}(L_n)$ entraîne que $S \subset Z_{n-2}(L_n)$, et donc que $L_n = Z_{n-2}(L_n)$, contradictoire avec le théorème précédent. Par conséquent $Z_{n-2}(L_n)$ est nécessairement contenu dans $\Phi(L_n) = \mathcal{D}(L_n)$, q.e.d. . Du reste, nous venons de le voir, $Aut(L_n)$ opère transitivement sur $L_n \setminus \Phi(L_n)$, de sorte $\Phi(L_n)$ *est la plus grande sous-boucle caractéristique de* L_n.

COROLLAIRE. *Dans* $\mathbb{L}_n$, *avec* $n \geq 3$, *l'ensemble* $A = \theta(\mathbb{L}_n)$ *des* x^3 *pour* $x \in \mathbb{L}_n$ *est un groupe abélien libre de rang* n, *et* $Z_{n-2}(\mathbb{L}_n)$ *est produit direct de* A *et de la* M_3*-boucle* $\mathcal{D}(\mathbb{L}_n)$:

$$Z_{n-2}(\mathbb{L}_n) = A.\mathscr{D}(\mathbb{L}_n),\ A \cap \mathscr{D}(\mathbb{L}_n) = \{1\}.$$

Le "premier centre" $Z(\mathbb{L}_n)$ *est produit direct de* A *et du 3-groupe abélien élémentaire* $Z(\mathbb{L}_n) \cap \mathscr{D}(\mathbb{L}_n)$.

Entre autres conséquences, $L_n = \mathbb{L}_n/\theta(\mathbb{L}_n)$ possède "autant d'associateurs" que $\mathbb{L}_n$, en ce sens que $|\mathscr{D}(L_n)| = |\mathscr{D}(\mathbb{L}_n)|$.

Preuve: Nous savons que A est contenu dans $Z(\mathbb{L}_n)$. Si $B=\{e_1,e_2,\ldots,e_n\}$ est une base libre de $\mathbb{L}_n$, tout élément x de $\mathbb{L}_n$ s'écrit sous forme

$$x = (e_1^{x_1} \cdot e_2^{x_2}) \cdot e_3^{x_3}) \ldots e_n^{x_n}) \cdot \alpha$$

où les x_1 sont des entiers, avec $\alpha \in \mathscr{D}(\mathbb{L}_n)$. Comme $\alpha^3 = 1$, on voit que x^3 appartient au sous-groupe de $Z(\mathbb{L}_n)$ engendré par les e_i^3. Considérons le diagramme commutatif suivant:

$$\begin{array}{ccccccccc}
1 \to & \mathscr{D}(\mathbb{L}_n) & \to & \mathbb{L}_n & \overset{\phi}{\to} & \mathbb{L}_{n}/\mathscr{D}(\mathbb{L}_n) & \simeq & \mathbf{Z}^n & \to 1 \\
 & \downarrow & & \downarrow\tau & & \downarrow & & & \\
1 \to & \mathscr{D}(\mathbb{L}_n) & \to & \mathbb{L}_{n}/A \simeq \mathbb{L}_n & \to & L_{n}/\mathscr{D}(L_n) & \simeq & \mathbf{Z}_3^n & \to 1
\end{array}$$

Dans $Z(\mathbb{L}_n)$, le système $B^3 = \{e_i^3 | \ i = 1,2,\ldots n\}$ est libre puisque $\phi(B^3)$ est libre. Donc $A = \langle B^3\rangle$ est bien abélien de rang n. Si $z \in Z_{n-2}(\mathbb{L}_n)$, alors $\tau(z) \in Z_{n-2}(L_n) = \mathscr{D}(L_n) = \tau(\mathscr{D}(\mathbb{L}_n))$ donc

$z \in A.\mathscr{D}(\mathbb{L}_n)$. Comme nous savons déjà que $Z_{n-2}(L_n)$ contient $\mathscr{C}^1(\mathbb{L}_n) = \mathscr{D}(\mathbb{L}_n)$ et A (contenu dans $Z_1(\mathbb{L}_n)$), nous en déduisons que $Z_{n-2}(\mathbb{L}_n) = A.\mathscr{D}(\mathbb{L}_n)$. Puisque $\mathscr{D}(\mathbb{L}_n)$ ne contient que des éléments d'ordre 3 ou 1, nécessairement $A \cap \mathscr{D}(\mathbb{L}_n) = \{1\}$, de sorte que le produit $A.\mathscr{D}(\mathbb{L}_n)$ est direct. Comme

$$A \subset Z(\mathbb{L}_n) \subset Z_{n-2}(\mathbb{L}_n) = A.\mathscr{D}(\mathbb{L}_n),$$

il est clair que $Z(\mathbb{L}_n)$ est produit direct de A par $Z(\mathbb{L}_n) \cap \mathscr{D}(\mathbb{L}_n)$.

Le résultat de Witt concernant les objets libres de type fini dans l'espèce de structure des groupes nilpotents de classe $\leq k$ (voir : WITT, E., Treue Darstellung Liescher Ringe, J. Reine Angew. Math. 117, 1937, pp. 152-160) suggère la conjecture suivante. Soit $n \geq 3$. Dans L_n, *la suite centrale montante de E serait formée des mêmes termes que la suite centrale descendante (?) pris dans l'ordre inverse;* autrement dit nous aurions $Z_1(L_n) = \mathscr{C}^{n-2}(L_n), Z_2(L_n) = \mathscr{C}^{n-3}(L_n)$ et plus généralement $Z_{i-1}(L_n) = \mathscr{C}^{n-i}(L_n)$ pour chaque $i = 2,3,\ldots(n-1)$. Il en résulterait que l'on aurait dans $\mathbb{L}_n$ une situation analogue, les termes de la suite centrale montante se déduisant de ceux de la suite centrale descendante, d'une part en renversant l'ordre, d'autre part en faisant le produit (direct) par $A = \theta(\mathbb{L}_n$, e.g. $Z_1(\mathbb{L}_n) = A.\mathscr{C}^{n-2}(\mathbb{L}_n)$ et plus généralement $Z_{i-1}(\mathbb{L}_n) = A.\mathscr{C}^{n-i}(\mathbb{L}_n)$ pour $i = 2,3,\ldots(n-1)$.. Nous savons seulement que $Z_{i-1}(\mathbb{L}_n)$ contient le produit direct $A.\mathscr{C}^{n-i}(\mathbb{L}_n)$, et que l'on a égalité pour $i = n-1$, correspondant aux plus grands termes non triviaux de chaque suite. De ce fait, la conjecture est évidemment vérifiée pour n=3. Nous allons l'établir pour n=4.

PROPOSITION 3. *Nous avons:*

$Z_1(L_4) = \mathscr{C}^2(L_4)$ *et* $Z_2(L_4) = \mathscr{C}^1(L_4)(=\mathscr{D}(L_4) = \Phi(L_4)$ *et si* $A=\theta(\mathbb{L}_4)$, *alors*

$$Z_1(\mathbb{L}_4) = A.\mathscr{C}^2(\mathbb{L}_4) \quad et \quad Z_2(\mathbb{L}_4) = A.\mathscr{C}^1(\mathbb{L}_4),$$

les deux produits ci-dessus étant directs.

Preuve. Relativement au deuxième centre Z_2, les égalités découlent de ce qui précède. Nous reprendrons ici implicitement les notations mises en place en [2] 2.5 pour la description de $\mathscr{C}^1(L_4)$ et de $\mathscr{C}^1(\mathbb{L}_4)$. Soit donc $S = \{g_1,g_2,g_3,g_4\}$ une base libre de L_4; désignons par g_{ijk} (resp. $g_{ijk,\ell m}$) l'associateur (g_i,g_j,g_k) (resp. l'associateur $((g_i,g_j,g_k),g_\ell,g_m)$, et posons:

$$\alpha_1 = g_{234},\ \alpha_2 = g_{134},\ \alpha_3 = g_{124},\ \alpha_4 = g_{123}$$

$$\beta_1 = g_{231,14},\quad \beta_2 = g_{132,24}$$

$$\beta_3 = g_{123,34},\quad \beta_4 = g_{124,43}$$

Nous admettrons:

- que $\mathscr{C}^1(L_4)$ est un 3-groupe abélien élémentaire d'ordre 3^8 dont un système génerateur (libre) est constitué par les α_i et les β_j (voir [2]).

- que tout élément d du deuxième centre $Z_2(L_4)$ (ici égal à $\mathscr{C}^1(L_4)$) a un comportement "distributif" pour l'associateur, en ce sens que $(du,v,w) = (d,v,w)(u,v,w)$ identiquement (cf. [3]).

- que l'on a les identités suivantes (cf. [2]):

$$\begin{cases} (\alpha_1, g_i, g_j) = \beta_j^{(-1)^{i+j}} = (\alpha_i, g_j, g_i)^{-1} \text{ si } i \neq j. \\ \\ (\alpha_k, g_i, g_j) = 1 \quad \text{si} \quad k \neq i \quad \text{et} \quad k \neq j. \end{cases}$$

Soit z un élément de $Z_1(L_4) \subset Z_2(L_4) = \mathscr{C}^1(L_4)$. Comme z est un produit des α_i et des β_j, on peut le mettre sous la forme:

$$z = \alpha_1^{a_1}\ \alpha_2^{a_2}\ \alpha_3^{a_3}\ \alpha_4^{a_4}\ \gamma$$

avec $\gamma \in \mathscr{C}^2(L_4) \subset Z_1(L_4)$, les a_i étant dans $\mathbb{F}_3 = \mathbf{Z}/3\mathbf{Z}$. Chaque α_i étant "distributif" (voir plus haut) nous avons pour tout couple i, j avec $i \neq j$,

$$(z,g_i,g_j) = \Big(\prod_{\ell=1}^{\ell=4} \alpha_\ell^{a\ell},\ g_i, g_j\Big) = \prod_{\ell=1}^{\ell=4} (\alpha_\ell, g_i, g_j)^{a\ell}$$

$$= (\alpha_i, g_i, g_j)^{a_i}\ (\alpha_j, g_i, g_j)^{a_j}$$

$$= \beta_j^{(-1)^{i+j} a_i}\ \beta_i^{(-1)^{i+j+1} a_j}$$

En écrivant que chaque (z,g_i,g_j) s'annule (puisque $z \in Z_1(L_4)$) on en déduit que $a_i = 0$ pour tout i, les β_i formant un système libre dans la $\mathbb{F}_3$-espace vectoriel $\mathscr{C}^1(L_4)$. D'où $z = \gamma \in \mathscr{C}^2(L_4)$. Nous avons montré que $Z_1(L_4) = \mathscr{C}^2(L_4)$. On en déduit que, dans $\mathbb{L}_4$, tout élément de $Z_1(\mathbb{L}_4)$ est congru modulo A à un élément de $\mathscr{C}^2(\mathbb{L}_4)$ ce qui complète la preuve.

Note. Des calculs ultérieurs montrent que L_5 vérific également la conjecture et que $Z_{n-3}(L_n) = \mathscr{C}^2(L_n)$ pour tout $n \geq 4$.

BIBLIOGRAPHIE

[1] BENETEAU L. "*Le quotient de Frattini d'une boucle de Moufang commutative*", C.R. Acad. Sc. Paris, t. 290, Sér. A, pp.443-446, 1980.

[2] BENETEAU L. "*Free commutative Moufang loops and anticommutative graded rings*", Journal of Algebra, 67, n°I,pp.1-35, 1980.

[3] BRUCK R.H. "*A survey of binary systems*", Springer, Berlin, Göttingen, Heidelberg, 1958; MR 20 # 76; 2nd printing 1968.

[4] DEZA M. "*Finite commutative Moufang loops, related matroids and association schemes, à paraître in* Proc. Conference on Combinatorics, 1979, Arcata, California, Humboldt State Univ., Ultilitus Math.

Lavoro pervenuto alla Redazione il 3 Gennaio 1983
ed accettato per la pubblicazione il 14 Giugno 1983
su parere favorevole di M. Curzio e G. Zappa