Séminaire Dubreil.
Algèbre et théorie
des nombres

Paul M. Cohn

Progrès récent dans l'étude des algèbres associatives libres

Séminaire Dubreil. Algèbre et théorie des nombres, tome 22, n° 2 (1968-1969), exp. n° 16, p. 1-7

<http://www.numdam.org/item?id=SD_1968-1969__22_2_A4_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
22e année, 1968/69, n° 16

28 avril 1969

PROGRÈS RÉCENT DANS L'ÉTUDE DES ALGÈBRES ASSOCIATIVES LIBRES

par Paul M. COHN

1. L'algèbre associative libre à d générateurs $X_1, \ldots, X_d$ sur un corps (commutatif) k, notée $A = k\langle X_1, \ldots, X_d\rangle$, se définit, soit comme solution d'un problème universel, soit comme anneau de polynômes en des variables non commutatives ; mais ce qui lui donne l'air "familière", c'est la forme normale de ses éléments, qui est très simple, plus simple même que pour les polynômes commutatifs. Les éléments de A s'écrivent tous d'une façon univoque :

$$(1) \qquad \sum \alpha_{i_1 \ldots i_r} X_{i_1} \ldots X_{i_r} \qquad (\alpha_{i_1 \ldots i_r} \in k) \ ,$$

et tous les $\alpha_{i_1 \ldots i_r}$, sauf un nombre fini, sont nuls. Sans cette dernière restriction, on obtient encore un anneau, noté $\hat{A} = k\langle\langle X_1, \ldots, X_d\rangle\rangle$, qui est analogue à l'anneau de séries de puissances formelles, auquel il se réduit pour $d = 1$.

Malgré la forme simple (1) de leurs éléments, on connait très peu de chose sur les anneaux A et $\hat{A}$. Jusqu'à présent, l'outil le plus pratique était l'algorithme faible pour A (voir [3], [5]), et l'algorithme inverse faible pour $\hat{A}$ (voir [4]). Mais il y avait beaucoup de problèmes qui résistaient encore. Depuis 1967, la situation s'est améliorée avec la parution de la thèse de G. M. BERGMAN [1], et je voudrais parler des quelques problèmes qu'il résout, et des progrès qu'on a fait depuis.

2. Par la définition même de A, il arrive rarement que deux éléments de A commutent. Toutefois, si $c \in A$, alors tous les polynômes en c (à coefficients dans k) commutent, et on s'est demandé si la réciproque est vraie, c'est-à-dire, étant donnés $a, b \in A$ tels que $ab = ba$, existe-t-il $c \in A$ tel que $a, b \in k[c]$? Plus généralement, on peut se poser la question suivante :

(A) Si C est le centralisateur d'un élément $a \in A$, $a \notin k$, est-ce que $C = k[c]$ pour un $c \in A$?

On savait que :

(α) C est toujours un anneau commutatif (voir [4]),

(β) C est de degré de transcendance 1 sur k (voir [5]),

mais on était très loin de répondre affirmativement à (A) ; or BERGMAN vient de démontrer le théorème suivant :

THÉORÈME 1 (voir [1], [2]). - Le centralisateur d'un élément non scalaire, dans une algèbre associative libre sur un corps k, est un anneau de polynômes de la forme $k[c]$.

La démonstration du théorème 1 se fait en deux étapes, ayant toutes les deux leur intérêt propre :

(γ) C est toujours intégralement clos (dans son corps de fractions) ;
(δ) C peut être plongé dans un anneau de polynômes $k[X]$.

Montrons d'abord comment le théorème 1 résulte de (γ), (δ). On sait (voir [6]), qu'une sous-algèbre de $k[X]$ est libre (donc anneau de polynômes en une variable sur k) si, et seulement si, elle est intégralement close. C'est le cas pour C (par (γ)), donc $C \simeq k[y]$.

Pour démontrer (γ), on utilise le fait que les idéaux de A (à deux générateurs, au moins) sont libres, et cela reste vrai quand on étend le corps de base. Je n'entrerai pas dans les détails, mais donnerai plutôt quelques précisions sur (δ), qui exige des idées non moins astucieuses, mais assez simples pour être indiquées ici.

L'algèbre A a une base assez naturelle, formée des monômes $u = x_{i_1} \dots x_{i_r}$. Il s'agit de trouver un préordre de ces monômes tel que toutes les puissances $u, u^2, \dots$ d'un monôme quelconque occupent la même place. Un tel préordre est donné si on associe à chaque monôme u sa puissance infinie : $u^\infty = uuu \dots$, et on ordonne ces suites infinies lexicographiquement.

Pour un monôme u quelconque, posons

$$A_u = \{\Sigma\, \alpha_v\, v \mid v \leqslant u\}, \qquad I_u = \{\Sigma\, \alpha_v\, v \mid v < u\},$$

où $\leqslant$ indique le préordre défini auparavant, et $v < u$ veut dire : $v \leqslant u$, mais non pas $u \leqslant v$.

On vérifie sans peine que A_u est une k-algèbre, et I_u un idéal bilatère dans A_u ; donc on peut former A_u/I_u. Ici, toutes les puissances de u doivent figurer tandis que le reste a été anéanti. On a donc un anneau de polynômes, c'est-à-dire

$$A_u/I_u \simeq k[x] \quad . \tag{2}$$

Retournons au centralisateur C d'un élément non scalaire de A. On sait ([1]) que C est engendré, en tant qu'anneau, par une famille finie d'éléments ; mais en

tout cas, on pourrait au besoin le remplacer par un sous-anneau. Si C est engendré par $z_1, \dots, z_r$, soit u le dernier monôme (dans notre préordre) qui apparaît dans les z_i. Alors $C \subseteq A_u$, tandis que $C \not\subseteq I_u + k$, de telle sorte que l'homomorphisme (2), restreint à C, l'applique sur une sous-algèbre $\neq k$. Il ne reste plus qu'à montrer que cet homomorphisme est injectif. Sinon, l'image serait de degré de transcendance zéro sur k, donc algébrique sur k, mais aussi intégralement close, donc égale à k, ce qui n'est pas le cas. Ceci termine l'esquisse de la démonstration du théorème 1.

Voici une hypothèse dont le cas le plus simple non trivial implique le théorème de Bergman :

(B) Soient A une algèbre associative libre, et B une sous-algèbre, engendrée par m éléments $y_1, \dots, y_m$. Alors, ou bien B est libre sur $y_1, \dots, y_m$, ou bien il y a une algèbre entre B et A, à moins de m générateurs.

Pour $m = 1$, c'est trivial. Le cas $m = 2$ se démontre par le théorème suivant, qui est une conséquence des résultats de [4] :

THÉORÈME 2. - Dans une algèbre associative libre, deux éléments a, b, qui ne sont pas libres, commutent.

Si B est engendré par y_1, y_2, ou bien y_1 et y_2 ne commutent pas, donc B est libre sur y_1, y_2, d'après le théorème 2, ou bien ils commutent, et alors $B \subseteq k[z]$, d'après le théorème 1.

Malheureusement, il ne semble pas que (B) soit vrai pour $m > 2$. Selon une communication de BERGMAN (légèrement simplifiée), si on prend dans $k\langle x, y, z\rangle$ des éléments $u = xyxz + xy$, $u' = zxyx + yx$, $v = xyx$, on a $uv = vu'$, mais il ne semble pas qu'il y ait une algèbre à deux générateurs, contenant u, u', v. J'ai quand-même l'impression que (B) doit subsister sous une forme modifiée, en faisant entrer le degré ou l'ordre. D'ailleurs (B), dans la forme ci-dessus, implique que tout objet projectif de type fini dans la catégorie des algèbres associatives soit libre ; c'est là un autre problème encore ouvert (qui est résolu pour le cas de 2 générateurs au plus, d'après ce qui vient d'être dit).

3. Passons à un autre problème qui concerne la relation entre A et $\hat{A}$. Si R est sous-anneau de S (même élément-unité bien-entendu), on dit que S est extension inerte de R si, pour tout $c \in R$ tel que

$$c = ab \qquad (a, b \in S),$$

il existe un élément inversible u de S tel que au , $u^{-1} b \in R$. On a maintenant le théorème suivant.

THÉORÈME 3 (BERGMAN-TARASOV ; voir [1], [8]). - Soient A une algèbre associative libre, et $\hat{A}$ sa complétée, alors $\hat{A}$ est extension inerte de A .

La démonstration de TARASOV est assez longue, et elle utilise l'algorithme faible, tandis que celle de BERGMAN, beaucoup plus courte, se sert de l'algorithme inverse faible, l'outil naturel pour $\hat{A}$, comme il a déjà été dit. D'ailleurs, tous les deux démontrent un peu plus. TARASOV montre, en même temps que le théorème 3, le théorème suivant.

THÉORÈME 4 (voir [8]). - Soient a , b , c , $d \in A$ tels que b , d soient inversibles dans $\hat{A}$, et, de plus, $ab^{-1} = cd^{-1}$ dans $\hat{A}$. Alors il existe

$$p , q , r , s \in A \quad \text{tels que} \quad a = pr , \ b = qr , \ c = ps , \ d = qs .$$

On aimerait avoir une démonstration du théorème 4 plus directe que celle de TARASOV. Pour cela, regardons ce que démontre BERGMAN. Dans l'anneau $\hat{A}$ de puissances formelles, considérons la relation entre éléments de $\hat{A}$: $pq \in A$. Cela définit une connexion de Galois sur $\hat{A} \times \hat{A}$. Pour tout sous-ensemble X de $\hat{A}$, on posera

$$X_s = \{p \in \hat{A} \mid pX \subseteq A\} , \qquad X_d = \{q \in \hat{A} \mid Xq \subseteq A\} .$$

Les ensembles de la forme X_s , X_d sont appelés fermés à gauche et à droite respectivement. Si P est fermé à gauche, et $Q = P_d$, alors $P = Q_s$, donc chacun des P , Q détermine l'autre. Nous convenons d'appeler de tels P , Q un couple d'ensembles fermés associés.

THÉORÈME 5 (BERGMAN [1]). - Soit P , Q un couple d'ensembles fermés associés dans l'anneau $\hat{A} = k\langle\langle x_1 , \dots , x_d \rangle\rangle$, et supposons P , $Q \neq (0)$. Alors il existe $u \in \hat{A}$ inversible tel que $P = Au$, $Q = u^{-1} A$.

La démonstration, assez directe, utilise l'algorithme inverse faible. Nous la supprimons, mais nous remarquons que la déduction du théorème 3 à partir du théorème 5 est tout-à-fait triviale et peut être laissée aux lecteurs. Par contre, on ne voit pas tout-de-suite comment déduire le théorème 4. Pour cela, il nous faut une généralisation légère du théorème 5.

Pour un anneau R quelconque, on note $R^{r\times s}$ l'ensemble des matrices $r \times s$ à éléments dans R . Il est alors évident qu'on peut définir une connexion de Galois

sur $\hat{A}^{r\times s} \times \hat{A}^{s\times t}$ par la condition $pq \in A^{r\times t}$. Et de façon analogue au théorème 5, on peut démontrer le théorème suivant :

THÉORÈME 6. - Soit P , Q un couple d'ensembles fermés, où $P \subseteq \hat{A}^{r\times s}$, $Q \subseteq \hat{A}^{s\times t}$, et P , $Q \neq (0)$. Alors il existe $u \in GL_s(\hat{A})$ (c'est-à-dire une matrice $s \times s$ inversible sur $\hat{A}$) tel que $P = A^{r\times s}\, u$, $Q = u^{-1} A^{s\times t}$.

Maintenant revenons au théorème 4 de TARASOV. On a $ab^{-1} = cd^{-1} = z \in \hat{A}$; alors $a = zb$, $c = zd$, et

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} zb & zd \\ b & d \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix} (b \quad d) \quad .$$

Soit P la fermeture à gauche de $(b \quad d)$, alors P contient $\begin{pmatrix} z \\ 1 \end{pmatrix}$, et sa fermeture à droite, Q , contient $(b \quad d)$. En appliquant le théorème 6, on trouve $q \in \hat{A}$, q inversible, tel que zq , $q \in A$ et $q^{-1} b$, $q^{-1} d \in A$. Si on pose $p = zq$, $r = q^{-1} b$, $s = q^{-1} d$, alors $b = qr$, $d = qs$, $a = zb = pr$, $c = zd = ps$, donc le théorème 4 est démontré.

Une fois le théorème 6 acquis, on se demande si on ne peut pas dépasser le théorème 4, et cela est le cas, en effet. Le théorème 4 montre que certaines relations multiplicatives dans $\hat{A}$ sont conséquences des relations multiplicatives dans A (ce qui n'est pas évident a priori). Notons $E(A)$ l'ensemble des éléments de A à terme constant non nul. Ce sont donc des éléments inversibles de $\hat{A}$, et, si on note par $\mathrm{alg}(A , E(A))$ la k-algèbre universelle engendrée par A , des éléments inverses formels pour les éléments de $E(A)$, on a ainsi un homomorphisme évident

$$\varphi : \mathrm{alg}(A , E(A)) \longrightarrow \hat{A} \quad . \tag{3}$$

Cet homomorphisme a déjà été considéré par MAGNUS [7], qui montre que les règles

$$s_i \longmapsto 1 - x_i \ , \qquad s_i^{-1} \longmapsto 1 + x_i + x_i^2 + \dots \ ,$$

définissent une immersion du groupe libre sur les s_i dans $\hat{A}$. Cela montre que l'application (3), restreinte au groupe engendré par les $1 - x_i$, est injective. En effet, nous pouvons montrer le théorème ci-dessous.

THÉORÈME 7. - L'application (3) est injective.

On démontre cette assertion en notant que la relation

$$a_1 b_1^{-1} a_2 b_2^{-1} \dots a_n b_n^{-1} = u_1^{-1} \ , \tag{4}$$

dans un anneau R quelconque (avec $b_1 , \dots , b_n , u_1 \in U(R)$), est équivalente à l'équation de matrices

$$(5)\quad \begin{pmatrix} a_1 & 0 & 0 & \dots & (-1)^n b_n \\ b_1 & a_2 & 0 & \dots & 0 \\ 0 & b_2 & a_3 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & b_{n-1} \quad a_n \end{pmatrix} = \begin{pmatrix} 1 & & & & 0 \\ & u_2 & & & \\ & & u_3 & & \\ & & & \ddots & \\ 0 & & & & u_n \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \dots & (-1)^n u_1 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} v_1 & & & & \\ & v_2 & & 0 & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & v_n \end{pmatrix},$$

où les u_i , v_i sont définis récursivement par

$$a_1 = v_1 , \qquad b_1 = u_2 v_1 ; \qquad a_i = u_i v_i , \qquad b_i = u_{i+1} v_i$$

(il se trouve alors que $b_n = u_1 v_n$, en vertu de (4)).

Si (4), avec $u_1 = 1$, est vrai dans $\hat{A}$, la matrice au milieu du deuxième membre de (5) a un rang $< n$, et on peut donc exprimer le premier membre comme produit d'une matrice $n \times (n - 1)$ et d'une matrice $(n - 1) \times n$. Cela est encore vrai dans A (par le théorème 6), et on en déduit que (4), avec $u_1 = 1$, est encore valable dans $\mathrm{alg}(A , E(A))$.

On pourrait tenter de généraliser même le théorème 7. Pour cela remarquons que les éléments de $\hat{A}$ à terme constant nul, soit $\hat{A}'$, forment une algèbre radicale, c'est-à-dire admettent une opération $x \longmapsto x'$ telle que

$$x + x' + xx' = x + x' + x'x = 0 \quad .$$

On peut également former l'algèbre radicale libre sur les x_i , et on a évidemment un homomorphisme de cette algèbre, R , sur $\hat{A}'$:

$$\Phi : \quad R \longrightarrow \hat{A}' \quad .$$

Maintenant, on peut se demander si Φ est injectif. C'est une question encore non résolue (pour autant que je sache). L'affirmation que Φ est injectif est plus forte que le théorème 7, dans le sens qu'on peut en déduire ce théorème, mais pas inversement.

BIBLIOGRAPHIE

[1] BERGMAN (G. M.). - Commuting elements in free algebras, and related topics in ring theory (Thesis, Harvard University, 1967).

[2] BERGMAN (G. M.). - Centralizers in free associative algebras, Trans. Amer. math. Soc. (à paraître).

[3] COHN (P. M.). - On a generalization of the Euclidean algorithm, Proc. Cambridge phil. Soc., t. 57, 1961, p. 18-30.

[4] COHN (P. M.). - Factorization in non-commutative power series rings, Proc. Cambridge phil. Soc., t. 58, 1962, p. 452-464.

[5] COHN (P. M.). - Rings with a weak algorithm, Trans. Amer. math. Soc., t. 109, 1963, p. 332-356.

[6] COHN (P. M.). - Subalgebras of free associative algebras, Proc. London math. Soc., Series 3, t. 14, 1964, p. 618-632.

[7] MAGNUS (W.). - Beziehungen zwischen höheren Kommutatoren, J. für reine und angew. Math., t. 177, 1937, p. 105-115.

[8] TARASOV (B. V.). - Sur les algèbres associatives libres [en russe], Algebra i Logika, t. 6, 1967, n° 4, p. 93-105.

(Texte reçu le 9 juin 1969)

Paul M. COHN
Bedford College
Regents Park
LONDON N. W. 1
(Grande-Bretagne)