SÉMINAIRE SCHÜTZENBERGER

PAUL M. COHN

L'algorithme inverse faible et quelques anneaux qui le possèdent

Séminaire Schützenberger, tome 1 (1969-1970), exp. n° 19, p. 1-6

<http://www.numdam.org/item?id=SMS_1969-1970__1__A11_0>

Séminaire SCHÜTZENBERGER-LENTIN-NIVAT
(Problèmes mathématiques
de la Théorie des automates)
Année 1969/70, n° 19, 6 p.

14 avril 1970

L'ALGORITHME INVERSE FAIBLE ET QUELQUES ANNEAUX QUI LE POSSÈDENT

par Paul M. COHN

1. - L'algorithme inverse faible est un moyen technique pour étudier les anneaux de séries formelles en des indéterminées non commutatives : $k\langle\langle X\rangle\rangle$. Jusqu'à présent c'était le seul exemple pour montrer l'utilité de cet algorithme ; aujourd'hui, je veux présenter une classe plus étendue d'exemples. Mais pour commencer, je dois rappeler la notion d'algorithme inverse faible.

2. - Tout le monde connaît l'algorithme de division (ou stathme de division) dû à EUCLIDE pour $\mathbb{Z}$ et à STEVIN pour $k[x]$. Il n'existe pas d'analogue raisonnable pour les polynômes à plusieurs variables $k[x_1, \dots, x_n] = k[X]$. Mais, si les variables ne commutent pas, il en existe ; je n'entrerai pas dans les détails (voir [4]), et me bornerai à rappeler qu'on peut l'utiliser comme l'algorithme habituel, pour :

(i) calculer les plus grands communs diviseurs (quand ils existent),

(ii) montrer que $k\langle X\rangle$ est un anneau à idéaux libres (au lieu d'être anneau principal),

(iii) montrer que toute matrice inversible est produit de matrices élémentaires (cf. [8]). En particulier, $k\langle X\rangle$ est un anneau factoriel dans un certain sens [6].

3. - Considérons maintenant l'anneau $R = k[[x]]$ de séries formelles dans une indéterminée x , sur un corps k . La divisibilité dans cet anneau est extrêmement simple : Etant donnés a , $b \in R$, on a : ou $a|b$ ou $b|a$, et on n'a pas besoin d'un algorithme pour le constater. Si on note $v(a)$ l'ordre de la série a , alors on a $a|b$ si, et seulement si, $v(a) \leqslant v(b)$.

L'anneau des séries formelles fait partie de la famille des anneaux filtrés. Si on pose $R_n = \{x \in R \mid v(x) \geqslant n\}$, alors on a la filtration

$$R = R_0 \supseteq R_1 \supseteq R_2 \supseteq \dots , \qquad \bigcap_{n \geqslant 0} R_n = 0 .$$

Pour tout anneau filtré, on peut définir la notion de v-dépendance :

1° $a_1, \dots, a_n$ sont v-dépendants à droite s'il existe $b_1, \dots, b_n \in R$ tels que

$$v(\Sigma\, a_i\, b_i) > \min_i \{v(a_i) + v(b_i)\} .$$

2° $a \in R$ est <u>v-dépendant à droite</u> de $a_1, \dots, a_n$ si $a = 0$, ou s'il existe $b_1, \dots, b_n \in R$ tels que

$$v(a - \sum a_i b_i) > v(a) \quad \text{et} \quad v(a_i) + v(b_i) \geq v(a) .$$

Ces définitions expriment précisément la dépendance linéaire ordinaire dans l'anneau gradué associé.

<u>Définition</u>. - Un anneau filtré R satisfait à l'algorithme inverse faible si, pour toute famille v-dépendante $a_1, \dots, a_m$ avec $v(a_1) \leq \dots \leq v(a_m)$, quelque a_i est v-dépendant à droite de $a_1, \dots, a_{i-1}$.

Prenons $R = k[[x]]$ comme exemple. Toute famille comprenant plus d'un élément est v-dépendante : $ab - ba = 0$. Donc, si $v(a) \leq v(b)$, alors il existe $c \in R$ avec $v(b - ac) > v(b)$. Par répétition, on trouve $g \in R$ tel que $b = ag$. Cet exemple montre en effet que tout anneau filtré complet à algorithme inverse faible, s'il est commutatif, n'est autre qu'un anneau de valuation discrète. Mais, dans le cas général, il existe d'autres exemples.

Un exemple intéressant est l'anneau $k\langle\langle X\rangle\rangle$ de séries de puissances formelles dans un ensemble X d'indéterminées non commutatives. Il n'est pas difficile de montrer (une fois qu'on est tombé sur la bonne définition) qu'ici encore on a l'algorithme inverse faible [5].

Voici les conséquences les plus importantes. Si R est un anneau filtré complet à algorithme inverse faible, alors :

1° Tout idéal (à gauche et à droite) de type fini est libre, comme module sur R, de rang bien déterminé (on dit que R est un <u>semi-fir</u> ; la même condition pour idéaux avec n générateurs au plus donne des <u>n-firs</u>).

2° On peut calculer les p. g. c. d. et p. p. c. m. de deux éléments (quand ils existent).

3° R est <u>anneau factoriel rigide</u> : Tout élément $c \neq 0$, ou bien est inversible, ou bien admet une factorisation complète $c = a_1 \dots a_r$, et si $c = b_1 \dots b_s$ en est une autre, alors $s = r$ et $b_i = u_{i-1} a_i u_i^{-1}$ (u_i est une unité, $u_0 = u_r = 1$). Remarquons qu'un anneau entier R est factoriel rigide si, et seulement si, R est un r-fir à factorisations complètes ("<u>r-fir atomique</u>") et anneau local.

4. - Comme je l'ai dit, mon but est de trouver d'autres exemples d'anneaux à algorithme inverse faible. Pour cela, prenons un anneau R avec filtration α-adique, où α est un idéal de R :

$$R \supseteq \alpha \supseteq \alpha^2 \supseteq \dots$$

Posons $K = gr_o R = R/\mathfrak{a}$, et pour $i \geqslant 1$, $M_i = gr_i R = \mathfrak{a}^i/\mathfrak{a}^{i+1}$. Alors K est un anneau, M_i est un K-bimodule, et la multiplication sur $gr\ R$ induit des épimorphismes

$$M_i \otimes_K M_j \longrightarrow M_{i+j} \quad (1)$$

Convenons d'appeler l'idéal $\mathfrak{a}$-tensoriel si les applications (1) sont des isomorphismes . Cela est le cas précisément si

$$M_i = M_1 \otimes \dots \otimes M_1 \quad (i \text{ facteurs}).$$

Donc on voit que R est tensoriel par rapport à $\mathfrak{a}$ si, et seulement si, $gr\ R$ est l'algèbre tensorielle de $M_1 = \mathfrak{a}/\mathfrak{a}^2$ sur $K = R/\mathfrak{a}$.

Voici une condition suffisante pour la tensorialité.

LEMME. - Soient R un anneau, $\mathfrak{a}$ un idéal bilatère de R qui est libre, comme R-module à droite (ou à gauche). Alors R est tensoriel par rapport à $\mathfrak{a}$.

Ce lemme se démontre en prenant une base $\{e_\lambda\}$ pour $\mathfrak{a}$, et en vérifiant que, pour chaque $n \geqslant 1$, les produits $e_{\lambda_1} \dots e_{\lambda_n}$ forment une base de $\mathfrak{a}^n$.

Par exemple, dans le cas commutatif, les conditions sont vérifiées précisément quand $\mathfrak{a}$ est principal : $\mathfrak{a} = tR$, et alors il est facile de trouver des conditions sous lesquelles la complétion $\mathfrak{a}$-adique de R est un anneau de valuation discrète. Le même raisonnement est encore valable dans le cas général et nous donne le théorème suivant :

THÉORÈME 1 - Soient R un anneau et $\mathfrak{a}$ un idéal bilatère de R . Si :

(i) $K = R/\mathfrak{a}$ est un corps (même gauche),
(ii) $\bigcap \mathfrak{a}^n = 0$,
(iii) $\mathfrak{a}$ est libre, comme R-module à droite,

alors R satisfait à l'algorithme inverse faible par rapport à la filtration $\mathfrak{a}$-adique.

Démonstration. - $gr\ R$ est une algèbre tensorielle sur le corps K , donc il satisfait à l'algorithme inverse faible, donc R aussi.

5. - Pour illustrer le théorème 1, nous avons besoin du théorème d'intersection pour les firs [10]. Rappelons-nous d'abord un résultat d'ALBRECHT [1] (généralisant un résultat antérieur de KAPLANSKY) :

Tout module projectif (à droite), sur un anneau semi-héréditaire à droite, est somme directe des modules de type fini.

Soient R héréditaire à droite, et M un module à droite avec un nombre fini de relations, c'est-à-dire $M = F/N$, où F est libre et N de type fini. Tout sous-module de M est de la forme P/N où $N \subseteq P \subseteq F$, et P est projectif, par hypothèse. Par le résultat d'ALBRECHT, P est somme directe des modules de type fini, donc il contient un composant P' de type fini et contenant N. Mettons $P = P' \oplus P''$, alors on a la suite exacte

$$0 \longrightarrow P'/N \longrightarrow P/N \longrightarrow P/P' \cong P'' \longrightarrow 0 ,$$

qui est scindée parce que P'' est projectif. Cela nous montre que tout sous-module de M est somme directe d'un module projectif (P'') et d'un module de présentation finie (P'/N).

Un module M sur un anneau R quelconque est dit <u>lié</u> si $\mathrm{Hom}_R(M , R) = 0$. Un tel module ne peut pas avoir de composants projectifs non nuls. Donc on obtient le lemme suivant (voir [9]) :

LEMME 2. - <u>Tout sous-module lié d'un module de présentation finie sur un anneau héréditaire est de présentation finie ; en particulier, les sous-modules liés d'un tel module satisfont à la condition maximale.</u>

Nous allons utiliser ce lemme pour un <u>fir</u>, c'est-à-dire un anneau où tout idéal à gauche ou à droite est libre, de rang bien déterminé.

THÉORÈME 2. - <u>Soit</u> $\mathfrak{a}$ <u>un idéal bilatère propre dans un fir</u> R ; <u>alors</u>

$$\bigcap \mathfrak{a}^n = 0 .$$

<u>Esquisse de démonstration.</u> - Supposons que $\mathfrak{a}^\omega = \mathfrak{a}^n \neq 0$. Etant donnés

$$a_1 , \dots , a_n \in \mathfrak{a}^\omega ,$$

si on remplace les a_i par une base d'idéal à droite $\sum a_i R$, on obtient une famille linéairement indépendante dans $\mathfrak{a}^\omega$. Prenons $a_1 , \dots , a_n \in \mathfrak{a}^\omega$ $(n \geqslant 1)$ linéairement indépendants à droite, et considérons $M = R/\sum a_i R$. On a : $\sum a_i R \neq 0$, donc $xa_i = 0$ $(i = 1 , \dots , n)$ implique $x = 0$, ce qui montre que M est lié. Soit $\{e_\lambda\}$ une base pour $\mathfrak{a}$ comme idéal à gauche. Si on écrit :

$$a_i = \sum b_{i\lambda} e_\lambda , \tag{2}$$

il est facile de voir que $b_{i\lambda} \in \mathfrak{a}^\omega$ (parce que $a_i \in \mathfrak{a}^\omega$ et les e_λ sont linéairement indépendants). Comme $\mathfrak{a}$ est propre dans R, il s'ensuit que :

$$\sum a_i R \subset \sum b_{i\lambda} R ,$$

donc M contient $\qquad M_1 = (\sum b_{i\lambda} R)/(\sum a_i R) \neq 0$.

M_1 est encore lié, car si $\lambda = 1, 2, \ldots, t$ sont les indices pour lesquels un $b_{i\lambda} \neq 0$ apparaît dans (2), alors une matrice de relations pour le module M_1 est donnée par

$$\begin{pmatrix} e & & 0 \\ & e & \\ & & \ddots \\ 0 & & e \end{pmatrix} \quad \text{où} \quad e = \begin{pmatrix} e_1 \\ \vdots \\ e_t \end{pmatrix}$$

Cela entraîne que M_1 est lié. Le quotient $M/M_1 = R/\sum b_{i\lambda} R$ est encore lié avec $b_{i\lambda} \in \alpha^{\omega}$, donc on peut recommencer. Ainsi on obtient une chaîne

$$M_1 \subset M_2 \subset \ldots \subset M$$

de modules avec quotients liés. Ici, tous les M_i sont liés, et comme tous sont de type fini (lemme 2), la chaîne doit se terminer, ce qui est une contradiction.

6. - Avec le théorème d'intersection (théorème 2), nous sommes en état d'utiliser le théorème 1 : Soit α un idéal bilatère propre dans un fir R. La condition (iii) du théorème 1 est automatique, et le théorème 2 nous montre que (ii) est valable. Il reste encore (i), et pour cela il nous faut postuler explicitement le résultat suivant :

THÉORÈME 3. - Soient R un fir, et α un idéal bilatère propre tel que R/α soit un corps. Alors R satisfait à l'algorithme inverse faible par rapport à la filtration α-adique de R.

Exemple. - Soit K un corps (même gauche) avec un sous-corps k. Formons le produit libre de deux copies de K :

$$R = K \star_k K .$$

C'est un fir (par les résultats de [7]), et on a une surjection $R \longrightarrow K$ consistant à identifier les deux facteurs. Donc R satisfait à l'algorithme inverse faible.

7. - Terminons par une question du plus grand intérêt : Est-ce qu'on peut plonger $K \star_k K$ dans un corps ? Si on savait que tout fir peut être plongé dans un corps cela donnerait la réponse. Les résultats précédents montrent qu'il suffit de plonger tout anneau factoriel rigide local dans un corps. Malheureusement, cela n'est pas vrai. La rigidite porte sur les relations de longueur 2, et cela ne suffit pas pour le plongement dans un corps (voir [3]). Il s'agit donc d'exploiter des conditions de longueur arbitraires, telles que la suivante (vraie dans tout anneau à algorithme inverse faible) due à BERGMAN [2] :

Soient R un anneau filtré complet à algorithme inverse faible, et n un entier donné. Alors toute suite de n éléments de R peut être réduite par une matrice de permutation suivie d'une matrice de la forme unitriangulaire à une suite de termes v-indépendants suivis de zéros.

Addendum (13 juin 1970)

Le problème, cité au n° 7, vient d'être résolu : Tout fir peut être plongé dans un corps. La démonstration, qui paraîtra dans [11], utilise un lemme tout à fait analogue au critère de rationalité pour les séries formelles dû à NIVAT ([12], Th. 5) dont il s'inspire.

BIBLIOGRAPHIE

[1] ALBRECHT (F.). - On projective modules over semihereditary rings, Proc. Amer. math. Soc., t. 12, 1961, p. 638-639.

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

[3] BOWTELL (A. J.). - On a question of Malcev, J. of Algebra, t. 7, 1967, p.126-139.

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

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

[6] COHN (P. M.). - Noncommutative unique factorization domains, Trans. Amer. math. Soc., t. 109, 1963, p. 313-331.

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

[8] COHN (P. M.). - Free associative algebras, Bull. London math. Soc., t. 1, 1969, p. 1-39.

[9] COHN (P. M.). - Bound modules over heredity rings (à paraître dans un volume dédié à la mémoire de A. I. Mal'cev).

[10] COHN (P. M.). - On a class of rings with inverse weak algorithm (à paraître).

[11] COHN (p. M.). - The embedding of firs in skew fields (à paraître).

[12] NIVAT (M.). - Séries rationnelles et algébriques en variables non commutatives Cours du DEA, 1969/70.

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

(Texte reçu le 3 juillet 1970)