MÉMOIRES DE LA S. M. F.

DANIEL LAZARD

# Équations linéaires dans les anneaux de polynômes

*Mémoires de la S. M. F.*, tome 49-50 (1977), p. 131-135

<http://www.numdam.org/item?id=MSMF_1977__49-50__131_0>

© Mémoires de la S. M. F., 1977, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (http://smf.emath.fr/Publications/Memoires/Presentation.html) 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/

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math France
Mémoire 49-50, 1977, p. 131-135



# EQUATIONS LINEAIRES DANS LES ANNEAUX DE POLYNOMES

par Daniel LAZARD

QUELQUES PROBLEMES FREQUENTS -

Soient $k$ un corps, $A = k[X_1, \ldots, X_n]$ ; on désigne par $a_i$, $b$, des éléments donnés de $A$.

(i) Déterminer si $b$ appartient à l'idéal $(a_1, \ldots, a_s)$; cela revient à résoudre l'équation : $\sum_{i=1}^{s} a_i z_i = b$.

(ii) Déterminer si les polynômes $a_1, \ldots, a_s$ ont un zéro commun dans une clôture algébrique de $k$. Cela revient à résoudre l'équation $\Sigma\, a_i z_i = 1$.

(iii) Déterminer la dimension de la variété définie par les équations $a_1, \ldots, a_s$. On peut montrer que cela se ramène à des problèmes du type (ii).

## I - UN EXEMPLE -

1. En 1955, J.P. Serre a posé la question suivante : Si $A$ est un anneau de polynômes à $n$ variables sur un corps $k$, tout $A$-module projectif est-il libre ? En 1973, Suslin et Vaserstein ont montré que cela est vrai, pour $n = 3$, pour $n = 4$ et $\mathrm{car}(k) \neq 2$, pour $n = 5$ et $k$ fini de caractéristique $\neq 2$. Ils ont montré également que, pour $n = 4$, un module projectif non libre est nécessairement de rang 2 et facteur direct de $A^3$; autrement dit un tel module est défini par trois éléments $p_1, p_2, p_3$, de $A$ tels qu'il existe $q_i \in A$ vérifiant $\sum_{i=1}^{3} p_i q_i = 1$.

Il semble tentant de chercher un tel exemple sur ordinateur quand $A = k[X_1, X_2, X_3, X_4]$ où $k$ est le corps à deux éléments. Examinons ce qu'il faut faire en se limitant aux $p_i$ de degré $\leq 2$.

2. Il y a $2^{45} \simeq 3.10^{13}$ tels systèmes de trois polynômes de degré 2. C'est beaucoup trop pour un examen systématique. Mais en faisant agir $SL_3(k)$ sur les $p_i$ et $A_4(k)$ sur les indéterminées, on ne change pas (à un isomorphisme près) le module défini par les $p_i$ et on peut réduire beaucoup le nombre de cas à examiner : on peut se ramener d'abord au cas où les parties de degré $\leq 1$ de $p_1, p_2, p_3$ sont de l'une des six formes $(1, 0, 0)$, $(1, X, 0)$, $(1, X, Y)$, $(1 + X, 0, 0)$, $(1 + X, Y, 0)$, $(1 + X, Y, Z)$, ce qui laisse encore $6.2^{30} \simeq 6.10^4$ cas à examiner. En poursuivant la réduction, on peut raisonnablement espérer se restreindre à un nombre de triplets assez petit pour que l'on puisse en faire une étude systématique.

3. Il faut ensuite éliminer ceux de ces triplets qui ne définissent pas de modules projectifs. Cela revient à déterminer si l'équation linéaire $\Sigma\ p_i\ q_i = 1$ admet une solution. Nous reviendrons ultérieurement sur ce problème.

4. Parmi les modules projectifs que l'on trouve ainsi, beaucoup, peut être tous, sont libres. Il s'agit donc d'éliminer ceux pour lequel c'est manifeste, par exemple ceux pour lesquels un des $p_i$ ou un des $q_i$ est constant et ceux pour lesquels une combinaison linéaire à coefficients constants des $p_i$ (resp. des $q_i$) est un polynôme constant. Quand deux systèmes définissent des modules isomorphes, on peut également éliminer l'un d'eux. On peut espérer ainsi ne retenir qu'un nombre de triplets $(p_1 , p_2 , p_3)$ assez petit pour être examinés individuellement à la main. Une nouvelle élimination, manuelle cette fois, devrait alors conduire à ne conserver sur quelques triplets candidats à être l'exemple cherché.

5. Soit $(p_1 , p_2 , p_3)$ l'un d'eux. Pour que le module projectif ainsi défini ne soit pas libre, il faut et il suffit que l'équation (à 6 inconnues polynômes)

$$\begin{vmatrix} p_1 & r_1 & s_1 \\ p_2 & r_2 & s_2 \\ p_3 & r_3 & s_3 \end{vmatrix} = 1$$

n'ait pas de solution. Si on se limite au cas où les $r_i$ et les $s_i$ sont de degré au plus 2, cela se ramène à savoir si un système de 210 équations quadratiques à 90 inconnues sur le corps à deux éléments possède ou non une solution dans une extension algébrique.

6. Quelles conclusions peut-on tirer de cette étude ?

6.1. Elle ne peut permettre de résoudre le problème de Serre pour $n = 4$ et $k$ corps à deux éléments : la limitation sur les degrés des $p_i$ empêche d'examiner tous les modules projectifs et donc d'affirmer qu'ils sont tous libres. La limitation sur les degrés des $r_i$ et des $s_i$ empêche de montrer qu'un triplet $(p_1 , p_2 , p_3)$ définit un module projectif qui n'est pas libre. On peut donc au mieux espérer trouver un module projectif qui a de bonnes chances de ne pas être libre.

6.2. Nous "espérons" beaucoup de choses. Cela est justifié par le fait que ces espérances ont été réalisées quand nous avons fait la même étude pour $n = 3$ avant la publication des résultats de Vaserstein [3].

6.3. En dehors de problèmes "ad hoc" que beaucoup de patience et de temps d'ordinateur permetrraient de résoudre, on est confronté à deux problèmes d'intérêt général.

a) Résoudre un système d'équations linéaires sur un anneau de polynômes

b) Déterminer si une famille d'hypersurfaces affines possède un point commun.

II - ALGORITHMIQUE -

1. Pour résoudre de tels problèmes il y a trois étapes à surmonter : Il faut d'abord montrer qu'il existe des algorithmes finis. Pour le problème a) cela a été fait en 1925 par G. Hermann [1] et pour le problème b) cela résulte de la théorie de l'élimination, dont c'est d'ailleurs le but, et cela a été résolu avant la fin du siècle dernier. Plus récemment Seidenberg a établi une liste importante de problèmes d'algèbre commutative qui possèdent des algorithmes [5].

2. Quand il existe un algorithme fini, il faut en trouver de suffisamment rapides pour pouvoir être exécutés sur ordinateurs. Ce problème apparaît clairement si on essaie d'appliquer le Théorème d'Hermann cité ci-dessus à la résolution de I.3. Le théorème affirme en effet que, si l'équation $\Sigma\, p_i\, q_i = 1$ admet une solution, elle en admet une où les $q_i$ sont de degré au plus 6650. Pour résoudre une telle équation la méthode des "coefficients indéterminés" conduit à un système linéaire d'environ $8.10^{13}$ équations et $2.10^{14}$ inconnues sur le corps de base $k$ !!

3. Quand on possède de bons algorithmes, il faut les réaliser en machine le mieux possible, ce qui pose de nouveaux problèmes, par exemple : comment gérer les polynômes de manière économique ?

III - RESOLUTION D'UN SYSTEME D'EQUATIONS LINEAIRES SUR $A = k[X_1, \ldots, X_n]$

Soit $\sum_{j=1}^{s} a_{ij}\, z_j = b_i$, $i = 1, \ldots, t$; un système d'équations linéaires qui sera dit sans second membre si tous les $b_i$ sont nuls. Résoudre un système avec second membre signifie déterminer s'il existe des solutions et, dans l'affirmative, en exhiber une; résoudre un système sans second membre signifie trouver un système de générateurs du module des solutions. Voici le meilleur algorithme que je connaisse.

1. Déterminer sur le corps des fractions $K = k(X_1, \ldots, X_n)$ de $A$ des équations principales au sens de la théorie de Cramer. Si le système a un second membre et n'a pas de solutions dans $K$, la résolution s'arrête là; dans tous les autres cas, on peut négliger les équations non principales et supposer que le rang du système est égal à $t$.

2. Si $k$ est fini, on remplace $k$ par une extension algébrique infinie sur laquelle on résoud le système (les solutions sur $k$ s'obtenant ensuite par descente fidèlement plate). On peut aussi utiliser une extension transcendante pure.

3. Si le système n'a pas de second membre, on le rend homogène à l'aide d'une indéterminée auxiliaire. J'entends par système homogène un système dont la matrice est la matrice d'un homomorphisme gradué de $A^s$ dans $A^t$, les éléments de base de $A^s$ (resp. $A^t$) étant homogènes de degrés non nécessairement égaux.

4. Soit I l'idéal homogène engendré :

- S'il n'y a pas de second membre, par les déterminants de rang maximal extraits de la matrice ainsi homogénéisée.
- S'il y a un second membre, par les parties de plus haut degré des déterminants de rang maximal extraits de la matrice des $(a_{ij})$.

Il faut déterminer une borne inférieure c de la codimension de I et un changement linéaire et homogène d'indéterminées tel que l'on ne change pas cette codimension en annulant les indéterminées d'indice supérieur à c. Cela revient à trouver une variété linéaire projective de dimension maximale ne rencontrant pas une variété donnée en aucun point (même irrationnel).

5. Supposons le changement d'indéterminées (ci-dessus) effectué. On dispose alors du résultat non trivial suivant :

$D_1$, $D_2$ ... étant les degrés des générateurs de I rangés par ordre décroissant, si le système avec second membre admet une solution, il en admet une dont le degré en $X_1, \ldots, X_c$ est inférieur ou égal à $D = \sum_{i=1}^{c} (D_i - 1)$. Le module des solutions du système sans second membre est engendré par les solutions "triviales" (solutions sur $k(X_1, \ldots, X_n)$ auxquelles on a chassé les dénominateurs) et par les solutions dont le degré en $X_1, \ldots, X_c$ est inférieur ou égal à $\sum_{i=1}^{c} (D_i - 1)$.

La "méthode des coefficients indéterminés" permet alors de se ramener à un système d'équations sur $k\left[X_{c+1}, \ldots, X_n\right]$. Une récurrence permet alors de terminer la résolution.

6. Le résultat suivant améliore beaucoup 5 quand c = 1 ou 2 et quand le système n'a pas de second membre :

Il existe un changement de variables, analogue à celui de 4., tel que, si $a_{ij}$ est homogène de degré $d_j - e_i$ avec $d_1 \geq d_2 \geq \ldots \geq d_s$, les solutions sont engendrées par les solutions triviales et les solutions telles que le degré de $z_k$ en $X_1$ et $X_2$ soit inférieur ou égal à

$$D_k = \sum_{j=1}^{t+2} d_j - \sum_{i=1}^{t} e_i - d_k - p - 2$$

où p est le degré du p. g. c. d. des déterminants de rang t extrait de la matrice des $(a_{ij})$.

Remarque -

1) Si les $d_j - e_i = d$ sont constants, et si $c = 2$, la majoration pour le degré en $X_1$ et $X_2$ des solutions du système sans second membre est $2\,dt - 2$ dans le cas de 5., et $dt + d - 2$ dans le cas de 6., ce qui montre que 6. est effectivement meilleur que 5.

2) Des contre-exemples montrent que la majoration de 6. est la meilleure possible dans le cas où $n = 2$ et où il n'y a pas de second membre.

3) On peut affiner les résultats en faisant intervenir, outre le degré global, les degrés partiels en une ou plusieurs parmi les indéterminées. Ces résultats sont trop compliqués à énoncer pour trouver leur place ici.

4) Depuis la rédaction de cet exposé, le problème de Serre a été complètement résolu [2].

5) Les résultats esquissés dans le paragraphe III sont démontrés et améliorés dans [4].

BIBLIOGRAPHIE

[1] G. HERMANN.- Die Frage der entlich vielen Schritte in der Theorie der Polynomideale.- Math. Annalen 95 (1926), p. 736-788.

[2] D. FERRAND.- Les modules projectifs de type fini sur un anneau de polynômes sur un corps sont libres.- Séminaire Bourbaki.- Juin 1976.

[3] D. LAZARD.- Calculs sur les modules projectifs.- Publ. Sém. Math. Univ. Rennes.- Colloque d'Algèbre commutative (1972).

[4] D. LAZARD.- Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination.- Soumis à Bull. S.M.F.

[5] A. SEIDENBERG.- Construction in Algebra.- Trans. Amer. Math. Soc. 197 (1974) p. 273-313.

D. LAZARD
Département de Mathématiques
Avenue du Recteur Pineau
86022 POITIERS - CEDEX