Astérisque

DANIEL LAZARD

Algorithmes fondamentaux en algèbre commutative

Astérisque, tome 38-39 (1976), p. 131-138

<http://www.numdam.org/item?id=AST_1976__38-39__131_0>

Société Mathématique de France
Astérisque 38-39 (1976) p.131-138

ALGORITHMES FONDAMENTAUX EN ALGÈBRE COMMUTATIVE

par

Daniel LAZARD

1.- INTRODUCTION

Lorsque l'on cherche à effectuer des calculs explicites en algèbre commutative ou en géométrie algébrique, on rencontre fréquemment un certain nombre de problèmes généraux tels que :

- Comparaison, intersection de sous-modules ;
- Image réciproque d'un élément, d'un sous-module par une application linéaire ;
- Résolution d'un système d'équations linéaires avec ou sans second membre ;
- Recherche de décomposition primaire ;
- Recherche de résolution projective ;
- Calcul du P.G.C.D. dans les anneaux factoriels ;
- Dimension d'une variété définie par ses équations ;
- Existence de points sur une clôture algébrique, pour une variété algébrique ...

Ces problèmes peuvent se résoudre en un nombre fini d'opérations pour une grande classe d'anneaux ; il est naturel de considérer que les méthodes de résolution de ces problèmes sont les algorithmes fondamentaux de l'algèbre commutative et de la géométrie algébrique.

Malheureusement, les algorithmes connus sont, en général, extrêmement

mauvais, au point d'être totalement inutilisables sur ordinateurs, même dans des cas très simples. Cela tient certes à la complexité naturelle de ces problèmes, mais peu de recherches ont été effectuées pour optimiser les algorithmes.

Cette situation se comprend mieux quand on examine l'histoire de l'algèbre commutative et de la géométrie algébrique.

Jusqu'en 1920 environ, les géomètres se préoccupaient beaucoup de calculs explicites. Cela les a amenés à développer un certain nombre de méthodes algorithmiques, dont l'une des plus perfectionnées est la théorie de l'élimination. Mais, malgré leur grand entraînement au calcul manuel, les mathématiciens de cette époque sont arrivés aux limites de leurs possibilités.

Il a donc fallu mettre au point des méthodes abstraites, plus puissantes, mais non constructives. La mise au point de ces méthodes en algèbre commutative et en géométrie algébrique a pleinement occupé les algébristes jusqu'aux années 60.

Depuis l'apparition de la théorie des schémas de Grothendieck, on peut considérer que la géométrie algébrique possède une théorie suffisamment élaborée, et de nombreux géomètres reviennent à des problèmes qui avaient été abandonnés faute de moyens permettant de les résoudre. Simultanément, quelques mathématiciens, notamment Seidenberg, s'efforcent de développer la géométrie algébrique moderne sur une base constructive et sont amenés ainsi à démontrer l'existence d'algorithmes finis.

Très peu de géomètres utilisent cependant cet outil merveilleux qu'est l'ordinateur : cela tient pour une part à leur ignorance de l'informatique, mais surtout au fait que les algorithmes fondamentaux n'ont pas été, en général, suffisamment développés pour être facilement implantés en machine.

Cette situation historique explique que les résultats que nous allons

citer sont, soit très anciens ($\leqslant$ 1925), soit très récents ($\geqslant$ 1974).

2.- EXISTENCE DES ALGORITHMES FONDAMENTAUX

Définition.- Appelons anneau calculable un anneau commutatif unitaire noethérien A muni d'une application surjective $f : I \to A$, où I est une partie du monoïde J des mots sur un alphabet fini, cette situation étant telle que l'on possède des algorithmes pour :

1) si $m \in J$, tester $m \in I$

2) si $m \in I$ et $n \in I$, tester $f(m) = f(n)$

3) si $m \in I$ et $n \in I$, trouver $p \in I$ tel que :

$$f(p) = f(m) + f(n) \quad (\text{resp. } f(p) = f(m) - f(n),\ f(p) = f(m)f(n))$$

4) trouver (par leur représentant dans I) un système de générateurs du module des solutions du système d'équations :

$$\sum_{j=1}^{s} a_{ij} z_j = 0 \quad (i = 1,\ldots,t)$$

où les éléments a_{ij} sont de la forme f(m).

5) tester si le système $\sum_{j=1}^{s} a_{ij} z_j = b_i$ $(i = 1,\ldots,t)$ possède une solution, et dans l'affirmative, en exhiber une.

Remarque.- 1) Si $s = t = 1$, l'algorithme 5 permet de faire les divisions.

2) Si A est un corps, notre définition est équivalente à celle de "corps explicitement défini" de Van der Waerden [VW].

L'intérêt des anneaux calculables est que ce sont les anneaux pour lesquels il existe des algorithmes finis pour toutes les opérations fondamentales de l'algèbre linéaire ; plus précisément, on a le résultat suivant :

THÉORÈME 1.- Soient A un anneau calculable, M et N des A-modules de type fini donnés par générateurs et relations (i.e. définis comme conoyaux de

l'application linéaire définie par une matrice), E et F des sous-modules de M, G un sous-module de N, tous définis par leurs générateurs et $f : M \to N$ une application linéaire définie par sa matrice. On possède des algorithmes pour :

a) calculer des systèmes de générateurs pour les modules $E \cap F$,

$$E : F = \{a \in A ; \quad aF \subset E\}, \quad \operatorname{ann} E, \ f^{-1}(G), \ f^{-1}(O).$$

b) tester $x \in E$, $E \subset F$, $E = F$, $y \in f(E)$, $y \in \operatorname{im}(f)$.

La démonstration est facile, et se trouve essentiellement dans [H].

Il y a beaucoup d'anneaux calculables comme en témoignent les théorèmes de transfert suivant .

THÉORÈME 2.-

a) L'anneau des entiers $\mathbb{Z}$ est calculable.

b) Si A est calculable, il en est de même de $A[X]$.

c) Si A est calculable, et $x_1, \ldots, x_n$ appartiennent à A, il en est de même de $A/Ax_1 + \ldots + Ax_n$.

d) Si A est calculable, il en est de même de $S^{-1}A$ quand S est, soit l'ensemble de tous les éléments qui ne divisent pas O, soit une partie multiplicative de type fini (i.e. l'ensemble des éléments de la forme $s_1^{n_1} \ldots s_k^{n_k}$, $n_1, \ldots, n_k \in N$).

Les assertions a) et c) sont faciles, b) est due à Richmann [R] ; la seule difficulté de d) consiste à montrer qu'il existe $s = s_1^{n_1} \ldots s_k^{n_k} \in S$ tel que $\operatorname{ann}(s) = \operatorname{ann}(s_i s)$ pour tout i ; ceci entraîne que $\operatorname{ann}(st) = \operatorname{ann}(s)$ pour tout $t \in S$ et que $\operatorname{ann}(s) = \ker(A \to S^{-1}A)$.

Corollaire.-

a) Les anneaux suivants sont calculables :

$$\mathbb{Z}, \ \mathbb{Q}, \ \mathbb{F}_q, \quad \mathbb{Z}[X_1, \ldots, X_n], \quad K[X_1, \ldots, X_n], \quad (K \text{ corps calculable}).$$

b) Une extension algébrique finie d'une extension transcendante pure dénombrable d'un corps premier est calculable si l'extension algébrique est définie par générateurs et relations.

Problème ouvert.- Caractériser les corps calculables.

Dans le cas où $A = K[X_1,\ldots,X_n]$ est un anneau de polynôme sur un corps calculable, beaucoup d'autres calculs peuvent être menés à bien en un nombre fini d'opérations :

- Déterminer si une famille de polynômes possède un zéro commun sur une clôture algébrique de K.
- Même problème pour les polynômes homogènes.
- Dimension de la variété affine (resp. projective) définie par une famille de polynômes.
- Calcul du P.G.C.D.
- Décomposition d'un polynôme en facteurs irréductibles.
- Calcul de la décomposition primaire d'un idéal.
- Calcul des idéaux premiers associés à un idéal...

Les quatre premiers problèmes ont été résolus avant 1900 (théorie de l'élimination pour les trois premiers). Les cinquième et sixième problèmes nécessitent que l'on sache résoudre le cinquième sur $K[X]$. Le dernier problème nécessite encore une hypothèse supplémentaire sur K. On trouvera des détails et de nombreux autres problèmes pour lesquels il existe des algorithmes finis dans [S].

3.- OPTIMISATION DES ALGORITHMES FONDAMENTAUX

Au stade actuel de la théorie, par optimisation, il faut entendre le plus souvent : écriture d'algorithmes suffisamment économiques en temps de machine et en place mémoire pour pouvoir mener les calculs à bien dans des cas relativement simples. La plupart des algorithmes cités dans le paragra-

phe précédent sont en effet tellement mauvais qu'ils ne sont absolument pas utilisables. Quelques uns le sont pourtant, notamment :

* Résolution des systèmes d'équations linéaires sur $\mathbb{Z}$ ou $K[X]$ (K corps) [MC]

* Calcul du P.G.C.D. et décomposition en facteurs irréductibles dans $\mathbb{Z}$ $\mathbb{Z}[X_1,\ldots,X_n]$, $K[X_1,\ldots,X_n]$ (cf. [MC] et [C]). Pour le P.G.C.D. dans $K[X_1,\ldots,X_n]$, il faut, avant d'appliquer l'algorithme d'Euclide, faire un changement d'indéterminées de manière à rendre les polynômes qui apparaissent unitaires par rapport à la première variable ; ce changement de variable est rapide à déterminer et permet d'éviter l'introduction de fractions rationnelles ; si K est fini, il est parfois nécessaire de l'agrandir pour pouvoir faire ce changement de variables.

* Résultant de k polynômes homogènes à n variables.

Soient $f_1,\ldots,f_k$ ces polynômes, de degré $d_1,\ldots,d_k$, la numérotation étant telle que $d_1 \geqslant d_2 \geqslant \ldots \geqslant d_k \geqslant 1$. Supposons $k \geqslant n$ et posons $d = d_1 + \ldots + d_n - n + 1$. Considérons des polynômes homogènes variables g_i $(i = 1,\ldots,k)$, de degré $d - d_i$. L'application $(g_1,\ldots,g_n) \to \Sigma f_i g_i$ est une application linéaire d'espaces vectoriels de dimension finie sur K : l'espace de départ est de dimension $\sum_{i=1}^{k} \binom{d-d_i+n-1}{n-1}$ et l'espace d'arrivée est de dimension $\binom{d+n-1}{n-1} = \binom{d+n-1}{d}$.

Appelons M la matrice de cette application linéaire ; le théorème fondamental de la théorie de l'élimination est le suivant :

THÉORÈME 3.- Pour que les f_i aient un zéro non trivial commun, dans une clôture algébrique de K, il faut et il suffit que $k < n$ ou que $\operatorname{rang}(M) < \binom{d+n-1}{d}$.

Le théorème est facile à mettre en œuvre, car il se ramène à calculer le rang d'une matrice sur un corps. La valeur de d remarquablement petite

qui intervient rend ce théorème extrêmement précieux pour le maniement sur ordinateur des polynômes à plusieurs variables.

* Dimension d'une variété définie par des polynômes (que l'on peut supposer homogènes) $f_1,\ldots,f_k$.

On considère n polynômes du premier degré homogènes, à coefficients indéterminés $f_{k+i} = u_{i,1} X_1 + \ldots + u_{i,n} X_n$. La dimension cherchée est le plus grand ℓ tel que $f_1,\ldots,f_{k+\ell}$ aient un zéro commun sur une clôture algébrique de $K(u_{ij})$. On applique le théorème 3 à $f_1,\ldots,f_{k+n}$ et on calcule le rang de la matrice qui intervient par la méthode du pivot, en prenant chaque pivot dans la colonne la plus à gauche possible. Si le dernier pivot correspond à un coefficient de f_{i+k}, la dimension est i.

* Systèmes d'équations linéaires sur $K[X_1,\ldots,X_n]$. La méthode générale consiste à montrer qu'il suffit de chercher les solutions de degré inférieur à une certaine borne par rapport à certaines variables ; la "méthode des coefficients indéterminés" permet alors de se ramener à un nouveau système sur l'anneau des polynômes en les autres indéterminées ; une itération permet alors de se ramener à un système d'équations linéaires sur K. Cette méthode a été appliquée par G. Hermann en 1925 [H] pour éliminer les indéterminées une à une. Des résultats fins sur les matrices de polynômes permettent d'éliminer les variables au moins 2 par 2. Montrons par des exemples que ceci optimise beaucoup l'algorithme de Hermann (cf [L] et articles à paraître de l'auteur).

1) Pour résoudre sur $K[X_1,\ldots,X_n]$ le système :

$$a_{i1} z_1 + \ldots + a_{is} z_s = 0 \quad i = 1,\ldots,t$$

il suffit de chercher les solutions telles que le degré de z_j soit inférieur à D(t,n,d) pour tout j. La méthode de Hermann donne une valeur de D(t,n,d) de l'ordre de $(t\,d)^{2^{n-1}}$ alors que la valeur actuelle est de l'ordre de $(t\,d)^{\sqrt{3}^{n-1}}$.

2) Si $t = 1$, $d = 2$, $n = 3$, Hermann donne $D = 88$ alors que la valeur actuelle est $D = 6$. Rappelons que le nombre de coefficients à déterminer par polynôme inconnu est ici $\frac{1}{6}(D+3)(D+2)(D+1)$. En fait, en suivant de près la démonstration, on peut borner aussi certains degrés partiels, et limiter encore plus le nombre de scalaires à déterminer.

***

BIBLIOGRAPHIE

[C] G.E. COLLINS : The SAC-1 polynomial greatest common divisor and resultant system Computer. Sci. Dep. Tech. Rep. 145, U of Winconsin(72)

[H] G. HERMANN : Die Frage der endlich vielen Schritte in der theorie der Polynomideale, Math. Ann 95 (1926), 736-788.

[L] D. LAZARD : Algèbre linéaire sur les anneaux de polynômes. Cahiers de Math. N°3 (1974) Univ. de Montpellier.

D. LAZARD : Equations linéaires sur les anneaux de polynômes. Comptes-Rendus du colloque de Limoges (1975). A paraître.

[MC] M.T. Mc CLELLAN : The exact solution of systems of linear equations with polynomial coefficients. J. of A.C.M. 20 (1973) 563-588.

[MU] D.R. MUSSER : Multivariate polynomial factorisation. J. of A.C.M. 22 (1975) 291-308.

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

[V d W] B.L. Van der WAERDEN : Moderne Algebra, vol. 1, 2ème ed. Springer, Berlin 1937 ; ou trad. Angl. Ungar, New-York (1949).

Daniel LAZARD
Département de Mathématiques
Université de Poitiers
40 avenue du Recteur Pineau
86022 POITIERS