COURS DE L'INSTITUT FOURIER

MONIQUE LEJEUNE-JALABERT

Introduction

Cours de l'institut Fourier, tome 19 (1984-1985), p. 7-14

<http://www.numdam.org/item?id=CIF_1984-1985__19__7_0>

INTRODUCTION

Depuis quelques années, l'apparition de systèmes, permettant d'effectuer sur ordinateur des calculs algébriques sur des polynômes, a suscité un renouveau d'intérêt pour la détermination d'algorithmes permettant de calculer effectivement certains invariants attachés à un système d'équations polynomiales ainsi que pour l'étude du nombre de pas de calculs à effectuer en fonction des données, par exemple le nombre de variables, le degré des équations.

Cette préoccupation, présente chez les mathématiciens à la fin du XIXème et au début de ce siècle, comme en témoignent par exemple "*Über die vollen Invariantensysteme*" de D. Hilbert (1893) [Hil 2], la préface de "*Algebraic theory of modular systems*" de F.S. Macaulay (1916) [Ma 1], "*Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*" de G. Hermann (1926) [He], s'était peu à peu estompée. A cette époque, d'une part les calculs qu'on avait reconnus comme pouvant être effectués en un nombre fini de pas, étaient le plus souvent trop longs pour être menés à bien à la main, d'autre part, bien qu'ayant permis de dégager de nombreux phénomènes, souvent, ils ne permettaient pas de fonder de façon satisfaisante les concepts de la théorie. (C'est le cas, par exemple, pour la définition de la dimension à partir de la théorie de l'élimination). Une longue et fructueuse période d'analyse plus abstraite commença alors. Le souci d'accompagner les nouveaux concepts introduits de méthodes de calcul passa le plus souvent au second plan. Certains se réjouirent de ne plus manipuler d'équations. On se souvient de cette célèbre boutade d'André Weil prétendant avoir éliminé la théorie de l'élimination.

Une fois mis au point, de tels algorithmes peuvent bien sûr être utilisés pour tester des conjectures ou trouver des contre-exemples en géométrie algébrique. Mais aussi leur construction et l'étude de leur complexité (nous ne donnons ici qu'un sens intuitif à ce terme), par le changement de point de vue opéré, amènent naturellement à la formulation de problèmes nouveaux en algèbre commutative (par exemple, que peut-on dire de l'entier à partir duquel, la fonction de Hilbert d'une k-algèbre graduée de type fini coïncide avec le polynôme de Hilbert en fonction de données sur cette k-algèbre?). Enfin, l'implémentation sur ordinateur de tels algorithmes, vu la richesse de leur structure, conduit à la mise en place de nouveaux concepts en informatique théorique.

Les notes qui suivent sont la rédaction d'un cours de D.E.A. fait à l'Université de Grenoble en 1984-1985. Elles sont largement "*self-contained* ". Les étudiants

ne possédant aucune connaissance préalable en algèbre commutative, seuls sont supposés connus quelques éléments de théorie des corps commutatifs ainsi que les notions courantes d'algèbre linéaire à coefficients dans de tels corps. –En particulier, il n'est volontairement pas fait usage de la notion de module plat, ce qui alourdit parfois certaines démonstrations comme celle du théorème de Bezout–.

Le chapitre 0 est consacré à des rappels, essentiellement l'algorithme permettant de déterminer le PGCD de 2 polynômes à une variable à coefficients dans un corps, l'algorithme de Gauss permettant de mettre sous forme triangulaire un système linéaire.

Au chapitre I, nous présentons les 2 algorithmes principaux : l'algorithme de division d'un polynôme à n variables par une suite de polynômes, qui généralise l'algorithme de division euclidienne pour les polynômes à une variable et est dû essentiellement à Hironaka [A.H.V]. Pour ce faire, nous introduisons différents ordres totaux sur $\mathbf{N}^n$, dans le but de mettre un ordre sur les monômes, généralisant à la fois la notion de degré pour un polynôme à une variable et celle de première variable figurant effectivement dans une forme linéaire, qui nous avaient permis de construire les algorithmes rappelés au chapitre 0. Un tel ordre étant choisi (nous verrons plus tard que ce choix dépend largement de la nature géométrique de l'information qu'on cherche à obtenir) tout polynôme $f \neq 0$ possède un plus grand monôme non trivial in f et à tout idéal $I \neq 0$ est associé un idéal de monômes in I, celui engendré par tous les "*plus grands monômes*" des $f \neq 0$ de I , invariant de nature essentiellement combinatoire puisqu'équivalent à la donnée des exposants $A_1, \ldots, A_s$ d'un système minimal de générateurs $X^{A_1}, \ldots, X^{A_s}$ de in I. $(A_1, \ldots, A_s$ est appelé l'escalier de $I)$. Cette construction est en fait assez ancienne puisqu'elle apparaît pour la première fois en 1927 dans "*Some properties of enumeration in the theory of modular systems*" de F.S. Macaulay [Ma 2] où il en montre la pertinence malgré son manque d'invariance par changement de variables. Elle est reprise par Hironaka en 1964 dans "*Resolution of singularities of an algebraic variety over a field of characteristic 0* " chap.III.§7 [Hir]. Il est alors facile de montrer que si in $f_i = X^{A_i}$, $i = 1, \ldots, s$, alors $f_1, \ldots, f_s$ est un système de générateurs de I . C'est une base standard de I .

Le deuxième algorithme (dû à B. Buchberger en 1970 [Bu]) permet d'obtenir, à partir d'une base quelconque d'un idéal I d'un anneau de polynômes à n variables sur un corps k , une base standard. Une telle base dépend bien entendu en général de l'ordre total choisi sur $\mathbf{N}^n$. Par exemple, l'ordre lexicographique (cf. définition I.1.1.2.1) convient aux problèmes d'élimination; si $1 \leq t \leq n$, $I \cap k[X_t, \ldots, X_n]$ est engendré par ceux des éléments d'une base standard de I ne dépendant que de $X_t, \ldots, X_n$. L'ordre lexicographique inverse (définition I.1.1.2.2) est adapté à des problèmes de section –on annule certaines variables–.

Nous revenons ici, d'une certaine façon, au point de vue : systèmes d'équations algébriques, puisque cet algorithme permet d'obtenir, à partir d'un

système donné, d'autres systèmes équivalents, en ce sens qu'ils engendrent le même idéal, sur lesquels on lit immédiatement l'information cherchée. Evidemment, en général, l'application d'une seule transformation ne suffit pas comme au chapitre 0 pour obtenir tous les types d'information. C'est un peu comme si, on devait regarder le système sous différents angles.

Le chapitre II est consacré à l'étude des solutions des systèmes algébriques, ce qu'on appelle classiquement les espaces algébriques affines. Nous rappelons brièvement la terminologie classique et l'existence d'une décomposition irrédondante d'un espace algébrique affine en composantes irréductibles par la méthode non effective, maintenant classique introduite par E. Noether en 1921 dans "*Idealtheorie in Ringbereichen*" [N] . Ceci nous permet de définir la dimension d'un tel espace, comme le sup des dimensions de ses composantes irréductibles, la k-dimension d'un espace affine Y irréductible sur k étant le degré de transcendance du corps des fractions de l'anneau quotient de $k[X_1, \ldots, X_n]$ par l'idéal de tous les polynômes (à coefficients dans k) nuls sur Y (cet anneau est justement intègre) sur k .

Introduisant ensuite la notion d'élément entier, nous obtenons le théorème des zéros de Hilbert : pour que le système $f_1, \ldots, f_s$ de polynômes de $k[X_1 \ldots, X_n]$ ait une solution au moins dans $\overline{k}^n$, $\overline{k}$ étant une clôture algébrique de k , il faut et il suffit que 1 n'appartienne pas à l'idéal I engendré par $f_1, \ldots, f_s$. C'est la démonstration de Samuel et Zariski [S.Z] que nous exposons ici.

Or la connaissance d'une base standard $g_1, \ldots, g_t$ de I , pour un des ordres quelconques que nous avons introduit, permet de répondre immédiatement à cette question. Il en est ainsi, si et seulement si, pour tout $i = 1, \ldots, t$, $\mathrm{in}\, g_i$ n'est pas réduit à un scalaire. En fait, la dimension d de l'espace des solutions dans $\overline{k}^n$ se lit immédiatement sur $\mathrm{in}\, I = (\mathrm{in}\, g_1, \ldots, \mathrm{in}\, g_t)$ calculé pour l'ordre diagonal. Les solutions de $\mathrm{in}\, I$ sont une réunion d'un nombre fini d'espaces vectoriels F_i d'équations $X_{i_1} = \cdots = X_{i_k} = 0$. d est le maximum des rangs de ces espaces vectoriels.

Si $d = 0$, autrement dit si le système possède un nombre fini de solutions dans $\overline{k}^n$, la détermination d'une base standard pour l'ordre lexicographique permet de "*résoudre*" le système. L'algorithme que nous présentons au §1 reste un peu théorique puisqu'il suppose la possibilité de "*déterminer* " les solutions dans $\overline{k}$ de polynômes de $k[X]$. Pour une analyse plus effective, on se reportera à "*Algebraic computation on algebraic numbers* " de C. Di Crescenzo et D. Duval (1985) [D.D].

Si $d \neq 0$, nous introduisons, en vue de la détermination des solutions, la notion de variables commodes. (La terminologie est inspirée par celle de Kouchnirenko dans [K]). Si les variables $X_1, \ldots, X_n$ sont commodes, pour tout $(x_{n-d+1}, \ldots, x_n) \in \overline{k}^d$ le système possède un nombre fini de solutions de la forme $(x_1, \ldots, x_{n-d}\ ;\ x_{n-d+1}, \ldots, x_n)$ que la méthode précédente permet de déterminer. (Sans condition sur les variables, ceci est faux en général; il suffit de considérer

l'équation $X_1X_2 - 1 = 0$, si $x_2 \neq 0$, la solution est $(\frac{1}{x_2}, x_2)$, si $x_2 = 0$, l'équation se réduit à -1 et n'a pas de solutions).

Nous fournissons un algorithme pour déterminer de tels variables. Cet algorithme est basé sur la détermination de bases standard pour l'ordre diagonal pour différents idéaux ainsi que sur le choix de points de $\overline{k}^n$ non solution de certains systèmes homogènes. Il permet également de déterminer d .

Dans le cas particulier où le système est formé de polynômes homogènes, le rang sur k de l'espace vectoriel I_s des polynômes de degré s appartenant à l'idéal qu'il engendre peut se lire directement connaissant une base standard de I . Nous utilisons ce fait pour en déduire le résultat classique de D. Hilbert (1890) [Hil 1] : si d est la dimension de son espace de solutions, il existe un entier N et un polynôme $P(T) \in \mathbf{Q}[T]$ de degré $d-1$ (si $d = 0$, $P(T) \equiv 0$) tel que si $s \geq N$,

$$H(s) = rg_k k[X_1, \ldots, X_n]_s / I_s = P(s)$$

c'est le polynôme de Hilbert de $k[X_1, \ldots, X_n]/I$. L'indice de régularité de $k[X_1, \ldots, X_n]/I$ est défini alors comme le plus petit entier n tel que $H(s) = P(s)$ si $s \geq n$.

Au chapitre III, nous abordons des questions liées à la complexité de l'algorithme de calcul d'une base standard. Nous nous limitons ici au cas des systèmes et idéaux homogènes. Nous discutons seulement dans des cas particuliers le problème de trouver une borne supérieure pour les degrés d'une base standard d'un idéal I ainsi que pour l'indice de régularité de $k[X]/I$ en fonction du nombre de variables et du maximum des degrés d'un système de générateurs de cet idéal. Utilisant dans l'étude qui suit, l'existence d'une décomposition primaire d'un idéal d'un anneau de polynômes, par souci d'être self-contained, nous rappelons brièvement ce résultat pour tout anneau noethérien. (Nous n'étudions pas ici de méthode de calcul effectif pour la détermination d'une telle décomposition).

La 1ère classe de systèmes ou idéaux que nous étudions est celle des intersections complètes. On dit que $I = (f_1, \ldots, f_r)$ est une intersection complète si $f_1, \ldots, f_r$ est une suite régulière de $k[X_1, \ldots, X_n]$ c'est-à-dire si f_i est non diviseur de zéro dans $k[X_1, \ldots, X_n]/f_1, \ldots, f_{i-1}$, $i = 1, \ldots, r$. Si la dimension de l'ensemble des solutions de $I = (f_1, \ldots, f_r)$ dans $\overline{k}^n$ est $n - r$, alors I est une intersection complète et c'est ce qui se passe en général.

La démonstration que nous donnons est essentiellement (à quelques retouches de vocabulaire près et des précisions sur les notions de généricité employées) la très belle démonstration originale de F.S. Macaulay "*The algebraic theory of modular systems*" §48 (1916) [Ma 1] . Le début du "*complexe de Koszul*" associé à

$$f_1, \ldots, f_r : \Lambda^2 k[X_1, \ldots, X_n]^r \xrightarrow{\phi_1} k[X_1, \ldots, X_n]^r \xrightarrow{\phi_0} k[K_1, \ldots, X_n]$$

$\phi_0(e_i) = f_i$, $i = 1, \ldots, r$; $\phi_1(e_i \wedge e_j) = f_j e_i - f_i e_j$, y est fortement suggéré.

Il en résulte alors assez facilement que si f_i est homogène de degré d_i , $i = 1, \ldots, r$, la série de Poincaré

$$F(t) = \sum_{s \geq 0} H(s) t^s$$

de $k[X_1, \ldots, X_n]/(f_1, \ldots, f_r)$ est $(1 - t^{d_1}) \cdots (1 - t^{d_r})/(1 - t)^n$, calcul également dû à F.S. Macaulay [Ma 1] (théorème 58). Dans ce cas $H(s)$ ne dépend que de $d_1, \ldots, d_r$ et n pour tout $s \in N$, l'indice de régularité est $d_1 + \cdots + d_r - n + 1$. En particulier, pour $r = n$, ceci implique que si le système homogène $f_1, \ldots, f_n$ ne possède que la solution triviale $(0, \ldots, 0)$, alors tout monôme de degré $\delta \geq d_1 + \cdots + d_n - n + 1$ appartient à l'idéal engendré par $f_1, \ldots f_n$, un des résultats classiques de la théorie de l'élimination. Et dans ce cas, $rg_k k[X_1, \ldots, X_n]/f_1, \ldots, f_n = d_1 \cdots d_n$.

Enfin, si les variables $X_1, \ldots, X_n$ sont commodes, une borne supérieure des degrés des éléments d'une base standard pour l'ordre lexicographique inverse est donnée par $d_1 + \cdots + d_r - r + 1$.

La 2ème classe que nous étudions est celle des Cohen-Macaulay. Cette notion a été introduite par F.S. Macaulay [Ma 1] chap.IV et il en également fourni les premiers exemples, les intersections complètes, certains idéaux engendrés par les mineurs d'une matrice à coefficients polynomiaux suffisamment générale. De nombreux autres exemples sont maintenant fournis par la théorie des invariants. Dans ce cas, si la dimension des solutions de $I = (f_1, \ldots, f_s)$ est $n - r$ et si f_i est homogène de degré d_i , $i = 1, \ldots, s$, avec $d_1 \geq d_2 \geq \cdots \geq d_s$, l'indice de régularité de $k[X_1, \ldots, X_n]/I$ est au plus $d_1 + \cdots + d_r - n + 1$ et si les variables $X_1, \ldots, X_n$ sont commodes pour I , $d_1 + \cdots + d_r - r + 1$ est encore une borne supérieure des degrés des éléments d'une base standard de cardinal minimal pour l'ordre lexicographique inverse. Enfin, lorsque $r = n$ (condition qui suffit à entraîner la propriété Cohen-Macaulay), $rg_k k[X_1, \ldots, X_n]/I \leq d_1 \cdots d_n$. Dans ces deux cas, l'algorithme de calcul d'une base standard pour l'ordre lexicographique inverse apparaît donc comme raisonnable.

Pour finir, un appendice est consacré à l'étude des relations entre systèmes homogènes et non homogènes, en particulier aux procédés d'homogénéisation et de déshomogénéisation. A cette occasion, quelques notions de géométrie projective sont introduites. Une deuxième appendice est consacré à la démonstration du théorème de Bezout classique.

Pour que les algorithmes que nous avons construits puissent être effectivement mis en oeuvre, il faut bien entendu que dans le corps k des coefficients des polynômes avec lesquels nous travaillons le calcul de la somme, de la différence, du produit, du quotient de deux éléments de k puisse être fait de façon effective. Il faut également (condition qui n'est pas forcément la plus facile à satisfaire) qu'on puisse décider si deux éléments de k sont égaux ou non. Ceci exclut par exemple de travailler avec $\mathbf{R}$ ou $\mathbf{C}$ qui ne sont susceptibles que de représentations approchées. J. Davenport [Da] appelle effectif tout corps possédant ces propriétés. Par exemple, si k est un corps effectif, $k(X)$ le corps des fonctions rationnelles est également effectif. Plus généralement $\mathbf{Q}(x_1, \ldots, x_n)$ ou $\mathbf{F}_p(x_1, \ldots, x_n)$ est effectif

si x_i est ou bien transcendant sur $\mathbf{Q}(x_1,\ldots,x_{i-1})$ (resp. $\mathbf{F}_p(x_1,\ldots,x_{i-1})$ ou bien algébrique sur $\mathbf{Q}(x_1,\ldots,x_{i-1})$ (resp $\mathbf{F}_p(x_1,\ldots,x_{i-1})$) , son polynôme minimal étant explicitement donné; $i = 1,\ldots,n$.

Citons enfin une liste de questions que nous n'avons pas abordées dans ces notes :

- l'effet des changements de variables sur l'escalier d'un idéal toujours pour un ordre fixé. (cf. [Ga 1] 1973). On peut montrer que pour presque tout changement de variables linéaire, l'escalier garde une valeur constante. C'est l'escalier générique.

- la généralisation à un sous-module de $k[X_1,\ldots,X_n]^p$ de la notion de base standard (cf. [Ga 2]).

- les questions d'écriture de syzygies ou résolutions libres. On peut, à partir d'une base standard de I pour un ordre quelconque, déterminer un système de générateurs pour le module des relations entre les éléments de cette base.

- le calcul d'une borne pour l'indice de régularité de $k[X_1,\ldots,X_n]/f_1,\ldots,f_s$, f_i étant homogène de degré d_i , $i = 1,\ldots,s$, en fonction de n , $d_1,\ldots,d_s$ dans le cas général. Un exemple dû à E.W. Mayr et A.R. Meyer [M.M] (1982) montre que, contrairement à ce qui se passe dans les cas que nous avons étudiés, l'indice de régularité peut être de l'ordre de $C(n)(\sup d_i)^{\alpha(n)}$, $\alpha(n)$ ayant une croissance exponentielle en n . M. Demazure fait une analyse détaillée de cet exemple dans [De] III.IV (1985).

Note : Les indications entre crochets dans le texte reportent à la bibliographie.