PUBLICATIONS MATHÉMATIQUES ET INFORMATIQUES DE RENNES

MARC GIUSTI

Théorie combinatoire de la dimension d'une variété algébrique

Publications de l'Institut de recherche mathématiques de Rennes, 1985, fascicule 4
« Séminaires de mathématiques - science, histoire et société », , p. 163-172

<http://www.numdam.org/item?id=PSMIR_1985___4_163_0>

THEORIE COMBINATOIRE DE LA DIMENSION D'UNE VARIETE ALGEBRIQUE

Marc GIUSTI

Centre de Mathématiques
Ecole Polytechnique
91128 PALAISEAU CEDEX
Laboratoire associé au CNRS No. 169

ABSTRACT

There are different definitions of the dimension of an algebraic projective variety, coming from geometry or algebra. We prove the classical equalities between them through new combinatorial definitions.

INTRODUCTION

Comment calculer la dimension d'un sous-ensemble algébrique projectif à partir d'un système donné d'équations? Il existe différentes définitions, dont l'équivalence constitue la théorie classique de la dimension en géométrie algébrique. La règle du jeu est alors la suivante: rendre une définition constructive pour lui associer un algorithme de calcul.

Une première méthode consiste à utiliser la fonction de Hilbert de l'anneau quotient. On accède facilement à cette fonction si on connaît un système particulier de générateurs, dit **base standard**, de l'idéal définissant. Pour conclure il faut maintenant savoir construire une telle base standard à partir de générateurs donnés, et enfin déterminer le polynôme de Hilbert pour en tirer son degré. On donnera ci-dessous les rappels et ingrédients nécessaires à l'élaboration d'un calcul de la dimension.

Malheureusement cette méthode souffre à l'évidence de défauts qui grèvent lourdement la complexité des calculs: on cherche un objet bien trop compliqué dont on ne retire qu'une très partielle information. Ces craintes sont fondées puisqu'il existe des exemples explicites d'idéaux, dûs à MAYR-MEYER [M-M], [D], pour lesquels le problème d'appartenance a une complexité exponentielle en espace. Comme la connaissance d'une base standard permet de résoudre aisément le problème d'appartenance, sa détermination requiert également un espace exponentiel...

Une deuxième approche emploie des sections par des sous-

variétés linéaires: c'est ce qui est pròposé par LAZARD [LA*].

On donne ici de nouvelles caractérisations de la dimension qui s'intercalent remarquablement bien entre les approches ci-dessus, puisqu'elles permettent de donner une nouvelle démonstration du théorème de la dimension, via leurs relations avec les définitions classiques.

1. ORDRES TOTAUX SUR LES MONOMES.

Soit k un corps. L'idée essentielle consiste à ordonner totalement les monômes de l'anneau de polynômes $R = k[x_0,x_1,\ldots,x_n]$, en bijection avec les points de $\mathbb{N}^{n+1}$, mais de manière compatible avec la multiplication de R. Les deux ordres principalement utilisés par la suite sont les suivants:

1.1. Définition: ordre lexicographique supérieur (resp. inférieur).

Un point a de $\mathbb{N}^{n+1}$ est supérieur (resp. inférieur) à un point b si et seulement s'il existe un indice i ($0 \leq i \leq n$) tel que:

$$a_n = b_n, \ \ldots, \ a_{i+1} = b_{i+1}, \ a_i > b_i$$

(resp.

$$a_0 = b_0, \ \ldots, \ a_{i-1} = b_{i-1}, \ a_i < b_i).$$

1.2. Définitions:

On associe alors à tout polynôme homogène non nul $f = \sum_{a \in \mathbb{N}^{n+1}} f_a x^a$ son support dans $\mathbb{N}^{n+1}$:

$$\mathrm{Supp}(f) = \{a \in \mathbb{N}^{n+1} \, ; \, f_a \neq 0\}.$$

Le plus grand (resp. petit) élément pour l'ordre lexicographique supérieur (resp. inférieur) du support de f est appelé son **exposant privilégié** exp(f). La **forme initiale** in(f) est le terme:

$$f_{\exp(f)} \, x^{\exp(f)}.$$

1.3. Définition et exemple.

Etant donné un idéal homogène I (non réduit à (0)), l'ensemble des exposants privilégiés de ses éléments non nuls constitue ce qu'on appelle une **partie stable** E(I) de $\mathbb{N}^{n+1}$, c'est-à-dire que:

$$a \in E(I) \Longrightarrow a + \mathbb{N}^{n+1} \subset E(I).$$

1.4. Lemme:

Toute partie stable E de $\mathbb{N}^{n+1}$ est engendrée par une famille finie $a^{(1)},\ldots,a^{(p)}$ de ses éléments, c'est-à-dire:

$$E = \bigcup_{i=1}^{p} (a^{(i)} + \mathbb{N}^{n+1}).$$

1.5. Démonstration:

Par récurrence sur n. L'assertion est immédiate pour $n = 0$. Ensuite soit $\pi:\mathbb{N}^{n+1} \to \mathbb{N}^n$ la projection canonique de $\mathbb{N}^{n+1}$ sur $\mathbb{N}^n \times (0)$ (identifié à $\mathbb{N}^n$). $\pi(E)$ est alors une partie stable de $\mathbb{N}^n$, engendrée par hypothèse de récurrence par une famille finie $a^{(1)},\ldots,a^{(p)}$.

Pour tout i $(1 \leqslant i \leqslant p)$ il existe donc un entier $a_n^{(i)}$ tel que $(a_0^{(i)},\ldots,a_{n-1}^{(i)},a_n^{(i)})$ appartienne à E. Soit $m = \operatorname{Sup}_{1 \leqslant i \leqslant p} (a_n^{(i)})$.

Maintenant chacune des sections E_j de E par l'hyperplan de coordonnées $x_n = j$ s'identifie par π à une partie stable de $\mathbb{N}^n$, engendrée par une famille finie. Les $\pi(E_j)$ forment une suite croissante de parties stables qui stationnent, égales à $\pi(E)$, pour j assez grand (en fait pour $j \geqslant m$). On en déduit l'existence d'une famille finie de générateurs de E.

1.6. Notation:

Si E est une partie stable de $\mathbb{N}^{n+1}$, on note D(E) le degré maximum des éléments du sous-ensemble générateur de E minimal pour l'inclusion.

2. BASES STANDARD.

2.1. Le théorème de division d'Hironaka:

Soit I un idéal homogène de R. Tout polynôme de R est congru modulo I à un polynôme (appelé reste de la division par I), soit nul, soit d'exposant privilégié en dehors de E(I).

2.2. Démonstration:

En effet si le polynôme f à diviser est non nul, il possède un exposant privilégié. Si ce dernier appartient à E(I), il est divisible par l'exposant privilégié d'un certain élément de I: appellons le g. Le polynôme initial f est congru à

$f_1 = f-(in(f)/in(g))g$, qui s'il n'est pas nul, a un exposant strictement plus petit que celui de f. On divise maintenant f_1; ce processus s'arrête puisque les monômes de degré donné sont en nombre fini.

2.3. Définition:

Soit I un idéal de R. D'après 1.4 E(I) est engendré par un sous-ensemble fini minimal $a_1,\dots,a_p$. **Une base standard** de I est une famille de polynômes $f_1,\dots,f_p$ de I dont les exposants privilégiés constituent cet ensemble générateur de E(I).

2.4. Corollaire:

Toute base standard d'un idéal engendre cet idéal.

En effet si on divise un polynôme de l'idéal par $f_1,\dots,f_p$, le reste doit être nul, puisque sinon son exposant devrait être simultanément dans E(I) et dans son complémentaire.

2.5. Corollaire (Théorème de la base finie de Hilbert ou nœtherianité de l'anneau de polynômes R):

Tout idéal de R admet un nombre fini de générateurs, et donc toute chaîne croissante d'idéaux est stationnaire.

2.6. Corollaire:

En tant que k-espace vectoriel, le quotient R/I est isomorphe à la somme directe des k-sous-espaces vectoriels de dimension un engendrés par les monômes du complémentaire de E(I):

$$R/I = \bigoplus_{a\notin E(I)} kx^a.$$

3. FONCTION ET POLYNOME DE HILBERT.

3.1. Définition:

Le **degré** d'un point $a = (a_0,\dots,a_n)$ de $\mathbb{N}^{n+1}$ est l'entier $|a| = a_0+\dots+a_n$.

Soit E une partie stable de $\mathbb{N}^{n+1}$; la fonction HF_E, qui associe à tout entier s le nombre d'éléments de degré s n'appartenant pas à E, est appelée la **fonction de Hilbert** du complémentaire de E:

$$HF(s) = \#(a\in\mathbb{N}^{n+1} \mid a\notin E\ ,\ |a| = s)$$

3.2. Lemme et définition:

Pour s assez grand, la fonction de Hilbert HF_E est égale à un polynôme HP_E (dit également de Hilbert). De plus il existe des entiers $c_o,\ldots,c_d$ tels que

$$HP_E(s) = \sum_{i=0}^{d} c_i \binom{s}{d-i}$$

où $\binom{s}{r} = \frac{1}{r!}s(s-1)(\ldots)(s-r+1)$ est la fonction coefficient du binôme.

Par définition, d est la **dimension** du complémentaire de E, c_o son **degré**.

On attribuera par convention le degré -1 au polynôme nul.

3.3. Définition:

Le lemme précédent permet de définir la **régularité** H(E) de la fonction de Hilbert, comme le plus petit entier à partir duquel elle devient égale au polynôme de Hilbert de E.

3.4. Proposition:

$H(E) \leqslant nD(E)$.

3.5. Démonstration de 3.2 et 3.4:

Par récurrence sur n. Les deux assertions sont immédiates pour $n = 1$.

Puis, reprenant les notations de 1.5, on considère le développement suivant de la fonction de Hilbert:

$$HF_E(s) = \sum_{i=0}^{s} HF_{E_i}(s-i).$$

que l'on brise en trois morceaux dès que s est assez grand:

$$HF_E(s) = \sum_{0\leqslant i\leqslant m-1} HF_{E_i}(s-i) + \sum_{m\leqslant i\leqslant s-H(E_m)} HF_{E_m}(s-i) + \sum_{s-H(E_m)+1\leqslant i\leqslant s} HF_m(s-i)$$

$$= \sum_{0\leqslant i\leqslant m-1} HF_{E_i}(s-i) + \sum_{H(E_m)\leqslant i\leqslant s-m} HF_{E_m}(i) + \sum_{0\leqslant i\leqslant H(E_m)-1} HF_m(i)$$

en tenant compte du fait que la section E_i est constante égale à E_m dès que i est plus grand que m.

En utilisant l'hypothèse de récurrence, et toujours pour s suffisamment grand, cette fonction devient:

$$HF_E(s) = \sum_{0\leqslant i\leqslant m-1} HP_{E_i}(s-i) + \sum_{H(E_m)\leqslant i\leqslant s-m} HP_{E_m}(i) + \sum_{0\leqslant i\leqslant H(E_m)-1} HF_m(i)$$

et cette expression est valable plus précisément dès que s dépasse $\sup_{0\leqslant i\leqslant m}(i+H(E_i))$, ce qui est assuré, toujours via l'hypothèse de récurrence, si s est plus grand que nD(E).

Il ne reste plus qu'à montrer que $\sum_{H(E_m)\leqslant i\leqslant s-m} HP_{E_m}(i)$ est bien un polynôme en s, à coefficients entiers sur la base binomiale, pour affirmer que cette dernière expression est le polynôme de Hilbert $HP_E(s)$. Cela résultera du lemme suivant.

3.6. Lemme:

Soit P un polynôme de $\mathbb{Q}[s]$ de degré d. Si r et s sont deux entiers, $\sum_{r\leqslant i\leqslant s} P(i)$ est un polynôme en s à coefficients rationnels, de degré d+1, à composantes entières sur la base binomiale si P l'était.

3.7. Démonstration:

Les fonctions coefficients du binôme $\binom{s}{0},\ldots,\binom{s}{d}$ forment une base sur $\mathbb{Q}$ de l'espace vectoriel des polynômes de degré inférieur ou égal à d. Il suffit donc de vérifier la première assertion sur ces polynômes particuliers, pour lesquels elle devient triviale.

4. THEORIE DE LA DIMENSION.

Dorénavant k est supposé algébriquement clos. Soit I un idéal homogène de R donné par un système fini de générateurs, et Z(I) l'ensemble algébrique projectif défini dans $\mathbb{P}^n_k$.

4.1. Définition (dimension de Hilbert):

C'est le degré d du polynôme de Hilbert du sous-ensemble stable E(I) de $\mathbb{N}^{n+1}$, relativement à un ordre total compatible.

4.2. Remarque: calculabilité de la dimension de Hilbert.

On sait construire une base standard de I à partir de générateurs donnés: les premiers algorithmes écrits sont dûs à BUCHBERGER [BU*], voir aussi [GA2], [GI], [LA4]. Le principe du calcul de la fonction de Hilbert découle facilement de 2.6, et remonte sans doute au moins à HIRONAKA [HI] ou GRAUERT [GR]. On en trouvera par exemple une exposition par GALLIGO [GA1]. Reste à déterminer le polynôme de Hilbert, grâce à la majoration de la régularité par le degré maximum des éléments d'une base standard

(3.4); en effet on connait des majorants de D(E(I)) en fonction des données [GI]. Cependant cette méthode peut se révéler impraticable comme on l'a relevé dans l'introduction.

4.3. Définition (dimensions géométriques):

La **dimension de section** est le plus petit entier s tel qu'il existe une sous-variété linéaire de codimension s+1 ne coupant pas Z(I).

La **dimension de projection** est le plus grand entier p tel qu'il existe une sous-variété linéaire de dimension p sur laquelle Z(I) se projette surjectivement.

4.4. Définition (dimension lexicographique inférieure et supérieure):

Soit x un système de coordonnées de $\mathbb{P}^n$. On note linf_x (resp. lsup_x) le plus petit (resp. grand) des entiers e tels que, relativement à l'ordre lexicographique inférieur (resp. supérieur) $E_x(I)$ coupe les n-e derniers axes de $\mathbb{N}^{n+1}$ (resp ne coupe pas le plan des e+1 premières coordonnées de $\mathbb{N}^{n+1}$). On appelle **dimension lexicographique inférieure** (resp. **supérieure**) le minimum linf des linf_x (resp. le maximum lsup des lsup_x) quand x parcourt tous les systèmes de coordonnées de $\mathbb{P}^n$.

4.5. Théorème de la dimension:

Les cinq notions de dimension coïncident, et la valeur commune est appelée la **dimension** de Z(I).

4.6. Démonstration:

4.6.1. $d \geq \mathrm{lsup}$.

Supposons qu'il existe des coordonnées de $\mathbb{P}^n$ telles que, relativement à un ordre compatible quelconque, par exemple l'ordre lexicographique supérieur, E(I) ne coupe pas le plan de $\mathbb{N}^{n+1}$ engendré par les e+1 premières coordonnées. Alors HF(s) est minorée par le nombre de monômes de degré s sur e+1 lettres, qui est $O(s^e)$; donc d est minoré par lsup.

4.6.2. $\mathrm{lsup} \geq p$.

Supposons que Z(I) se projette surjectivement sur un plan P de dimension p. Choisissons des coordonnées telles que ce plan soit défini par les équations $x_{p+1} = \ldots = x_n = 0$. Alors l'idéal $I \cap k[x_0,\ldots,x_p]$ se réduit à (0).

En effet, supposons que I contienne un polynôme $f(x_0,\ldots,x_p)$ non nul, donc ne s'annulant pas sur tout P. L'ensemble algébrique Z(I), qui est contenu dans le cylindre d'équation f=0, ne peut donc pas se projeter sur tout P. Dans de telles coordonnées, examinons E(I) relativement à l'ordre lexicographique supérieur. Si un polynôme possède une forme initiale ne dépendant que des p+1 premières variables, il jouit de la même propriété; donc E(I) ne coupe pas le plan des p+1 premières variables.

4.6.3. $p \geqslant s$.

D'après la définition de s, il existe une sous-variété linéaire L de codimension s+1 évitant Z(I). On peut d'autre part choisir une sous-variété linéaire B de dimension s évitant L. La projection de centre L envoie surjectivement Z(I) sur B, puisque s est minimal; en effet si M est un point de B, la sous-variété linéaire qu'il engendre avec L est de codimension s, donc coupe Z(I) en au moins un point dont l'image est M.

4.6.4. $s \geqslant linf$.

D'après la définition de s, il existe une sous-variété linéaire L de codimension s+1 évitant Z(I). On choisit des coordonnées telles que L soit définie par les équations $x_0 = \ldots = x_s$. L'idéal $J = I+(x_0+\ldots+x_s)$ définit la sous-variété vide, donc contient une puissance de l'idéal $(x_0,\ldots,x_n)$ d'après le Nullstellensatz. Quelque soit l'ordre choisi, E(J) coupe tous les axes de coordonnées. Dorénavant ne considérons que l'ordre lexicographique inférieur. Examinons un polynôme f de J, dont l'exposant soit sur un des axes $x_{s+1},\ldots,x_n$. Il est donc congru à un polynôme g de I modulo $(x_0,\ldots,x_s)$, qui ne peut pas être nul, et dont l'exposant privilégié est égal à celui de f. Donc la section de E(I) par le plan des n-s dernières coordonnées a des points sur tous les axes.

4.6.5. $linf \geqslant d$.

Supposons qu'il existe des coordonnées de P^n telles que, relativement à un ordre compatible quelconque, par exemple l'ordre lexicographique inférieur, E(I) coupe les n-linf derniers axes. En degré u suffisamment grand, le complémentaire de E(I) ne contient donc que des monômes sur au plus linf+1 lettres, et HF(u) est majoré par un $O(u^{linf})$.

REFERENCES

[BU1] B. BUCHBERGER, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Ph. D. Dissertation, U. Innsbruck, Austria, (1965).

[BU2] B. BUCHBERGER, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraisches Gleichungssystems, Aequationes Math. 4 (1970), 374-383.

[BU3] B. BUCHBERGER, A theoretical basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bull., 39 (1976), 19-29.

[D] M. DEMAZURE, Notes informelles de calcul formel, prépublications Centre de Mathématiques de l'Ecole Polytechnique (1984).
3. Le monoïde de Mayr-Meyer.
4. Le théorème de complexité de Mayr-Meyer.

[GA1] A. GALLIGO, A propos du théorème de préparation de Weierstrass, Lect. Notes in Math. 409 (1973), 543-579.

[GA2] A. GALLIGO, Algorithmes de construction de bases standard, preprint Université de Nice (1983).

[GI] M. GIUSTI, Some effectivity problems in polynomial ideal theory, in Eurosam 84, Lecture Notes in Computer Science 174, Springer (1984), 159-171.

[GR] H. GRAUERT, Über die Deformationen isolierter Singularitäten analytischer Mengen, Inventiones Math. 15 3 (1972)

[HI] H. HIRONAKA, Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. Math. 79, (1964) 109-326.

[LA1] D. LAZARD, Algèbre linéaire sur $K[x_1,...,x_n]$ et élimination, Bull. Soc. Math. France, 105 (1977), 165-190.

[LA2] D. LAZARD, Résolution des systèmes d'équations algébriques, Theoretical Computer Science 15 (1981), 77-110.

[LA3] D. LAZARD, Commutative algebra and computer algebra, Lect. Notes in Comp. Sciences 144 (1982), 40-48.

[LA4] D. LAZARD, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, in Eurocal 83, Lecture Notes in Computer Science 162, Springer (1983).

[M-M] E. MAYR, A. MEYER, The complexity of the word problems for commutative semi-groups and polynomial ideals, Adv. in Maths. 46 (1982), 305-329.