COURS 13

Bases standard

Résumé

Dans ce chapitre, nous allons généraliser à plusieurs variables à la fois l'algorithme d'Euclide et l'algorithme de Gauss.

Lien PGCD/Euclide/Gauss/Résultant. Géométrie et idéaux. Bases standard. Divisions à plusieurs variables. Historique. Bornes de complexité.

Exemple introductif : essayons de faire prouver à une machine le simplissime théorème d'Appollonius, qui affirme que les milieux des côtés d'un triangle rectangle, le sommet de l'angle droit et le pied de la hauteur relative à l'hypothénuse sont sur un même cercle. Ce n'est qu'une version simplifiée du cercle des 9 points d'un triangle.

Soit donc OAB un triangle rectangle de sommet O. Nous pouvons toujours choisir un système de coordonnées tel que l'origine soit en O, et les deux autres sommets les points respectivement $(2a, 0)$ et $(0, 2b)$. Le cercle passant par le sommet et les milieux $(a, 0)$ et $(0, b)$ des côtés a pour équation $X^2 + Y^2 - aX - bY = 0$. Vérifier que le milieu (a, b) de l'hypothénuse est sur ce cercle n'est qu'une évalution du polynôme équation. Le pied de la hauteur $M = (x, y)$ est définie par les relations linéaires de son appartenance à AB et l'orthogonalité entre OM et AB, soit le système linéaire $ay + bx - 2ab = by - ax = 0$. Résolution immédiate :

$$y = \frac{a}{b}x \; x = \frac{2ab^2}{a^2 + b^2} \; y = \frac{2a^2b}{a^2 + b^2}$$

Polynômes hypothèses (ici linéaires) $\Rightarrow$ polynôme conclusion, modulo une petite non-dégénérescence.

Exemple à 1 variable / PGCD / Euclide. Exemple de générateurs, Gauss.

Interprétation en termes de monômes privilégiés, réécriture, idéal, appartenance à l'idéal, anneau quotient.

Calcul dans $k(a, b)[x, y]$. On essaie d'écrire le polynôme conclusion (l'équation du cercle) comme « conséquence du système d'équations hypothèses », c'est-à-dire combinaison linéaire à coefficients polynomiaux des polynômes hypothèses.

Notion d'idéal engendré.

Monde du calcul (réécriture) vs. monde de la géométrie.

1. Introduction

Rappelons la notion d'anneau (resp. de corps) effectif. Tout d'abord que tout élément possède une représentation en machine via une **structure de données**. Puis les opérations de base : addition, opposé, multiplication, (resp. plus l'inversion d'un élément non nul) sont réalisables par un algorithme. Enfin, il ne faut pas

oublier le test d'égalité (qui se réduit au test à zéro) qui doit être algorithmique (cf. *** CEX Richardson cours 1 ***).

EXERCICE 1. L'anneau des entiers $\mathbb{Z}$ et le corps $\mathbb{Q}$ des rationnels sont effectifs. Imaginer une représentation et décrire les algorithmes.

EXERCICE 2. Un anneau de polynômes sur un corps effectif est effectif. Une extension algébrique ou transcendante de $\mathbb{Q}$ est un corps effectif.

EXERCICE 3. Un anneau quotient d'un anneau de polynômes sur un corps effectif par un idéal est effectif est-il effectif ?

Relation d'équivalence associée.

L'introduction nous suggère l'importance d'un ordre sur les monômes permettant de privilégier l'un d'entre eux.

Cas linéaire, cas à une variable.

2. Ordres totaux admissibles sur le monoïde des monômes

À un élément $a = (a_1, \dots, a_n)$ de $\mathbb{N}$ est associé le monôme ou produit de puissances $X = ({X_1}^{a_1} \cdots {X_n}^{a_n})$. Ainsi les monômes de l'anneau R forment un monoïde multiplicatif $\mathcal{M}_n$ isomorphe au monoïde additif $\mathbb{N}^n$ (l'élément neutre 1 correspond au point de coordonnées toutes nulles). Nous nous autoriserons à utiliser indifféremment la notation additive ou multiplicative.

DÉFINITION 1. *Un ordre total $<$ sur les monômes est dit* compatible *s'il est compatible avec la structure de monoïde. Tous les éléments distincts de l'élément neutre sont d'un même côté que celui-ci, et la multiplication par un monôme est croissante.*

Il est dit de plus admissible *si l'élément neutre est plus petit que tous les autres :*

(i) $1 < m$ *si* m *n'est pas l'élément neutre ;*

(ii) $m' < m''$ *implique pour tout* m $mm' < mm''$.

EXEMPLE 1. L'ordre lexicographique : pour ordonner deux points différents de $\mathbb{N}^n$, on regarde la première coordonnée où elles diffèrent. En fait, on devrait plutôt parler de l'ordre lexicographique *induit* par un ordre total sur les variables. C'est ainsi que l'ordre des lettres de l'alphabet induit un ordre sur les mots du dictionnaire.

EXEMPLE 2. Il existe aussi pour les rimailleurs des dictionnaires de rimes : les mots sont ordonnés d'après les dernières lettres ; et pour les amateurs de *Scrabble*, des listes de mots rangés par longueur croissante. *** ordres lexicographique inverse ; ordres diagonaux

EXEMPLE 3. *** Matrice à coefficients entiers/réels ; irrationnels.

THÉORÈME 1. **** th. de structure de Robbiano pour mention (référence ? Hahn–Banach ?)*

LEMME 1. *Tout ordre total admissible est un* bon *ordre, cést-à-dire que toute chaîne descendante (c'cest-à-dire une suite décroissante) stationne.*

DÉMONSTRATION. Exemple du dictionnaire (même infini) : si on l'ouvre au milieu et qu'on pique un mot, il n'y a qu'un nombre fini de pages précédentes. Par le théorème de Robbiano, nous pouvons nous ramener au cas particulier de l'ordre lexicographique. Celui-ci se traite par récurrence sur le nombre de lettres. □

Remarquons que la propiété est triviale pour les ordres diagonaux (finitude à degré constant).

3. Exposants privilégiés et escaliers

DÉFINITION 2. *En présence d'un ordre total admissible sur les monômes, nous appelerons* exposant privilégié *d'un polynôme* non nul *le plus grand de ses monômes.*

Notons bien que cette notion n'est pas définie pour le polynôme nul. On peut la voir comme l'analogue d'une linéarisation. ***

DÉFINITION 3. *Un* idéal de monômes *est une partie de $\mathcal{M}_n$ stable par multiplication externe : tout multiple d'un élément de cet idéal appartient encore à cet idéal. De manière isomorphe, une* partie stable *de $\mathbb{N}^n$ est stable par addition de quadrant : tout translaté d'un point de cette partie stable par un élément de $\mathbb{N}^n$ est encore dans cette partie stable.*

On parle de manière imagée d'un *escalier* (dessin).

$E(0) =$ DOUTEUX ; néanmoins cela a plus de sens que pour un seul polynôme, tant qu'on ne parle pas de générateurs. $E(A) = \mathbb{N}^n$

4. noethérianité du monoïde des monômes

[Lemme de Dickson]

1. Tout ensemble stable de $\mathbb{N}^n$ est engendré par un nombre fini d'éléments, c'est-à-dire :

$$E = \bigcup_{i=1}^{q} (a_i + \mathbb{N}^n)$$

2. Toute suite croissante de parties stables stationne.

Ces deux propriétés sont équivalentes.

1. implique 2. Soit E_i $i = 1, ldots$ une suite croissante de parties stables. Leur réunion E est encore stable, donc finiment engendré. Chacun des générateurs appartient à un membre de la suite, on prend le dernier qui contient tous les autres précedents et la suite s'arrête dessus.

2. implique 1. Soit donc une partie stable E non finiment engendrée, et a_1 un de ses éléments, qui ne peut donc pas l'engendrer. C'est donc qu'il existe un autre élément a_2 dans E, etc ...

DÉFINITION 4. *Une* base standard *d'un idéal de l'anneau de polynômes est un ensemble de polynômes de l'idéal dont les exposants privilégiés engendrent l'escalier de l'idéal.*

Notons bien que les éléments doivent appartenir à l'idéal mais que rien pour l'instant hormis la terminologie ne prouve qu'ils l'engendrent. C'est le paragraphe suivant qui va nous le démontrer, grâce à une généralisation à plusieurs variables de la notion de division.

5. Divisions

Pour ce faire, commençons par définir une *division élémentaire faible* (resp. *forte* d'un polynôme dividende par un seul diviseur. Ce diviseur s'écrit $exp(f) - reste(f)$, et nous lui associons la règle de réécriture $exp(f) \to reste(f)$. Elle consiste

à remplacer une occurence éventuelle de $exp(f)$ comme facteur du monôme privilégié (resp. de tout monôme) du dividende par le polynôme $reste(f)$.

L'itération du processus de division faible (resp. forte) s'arrête (noethérianité) sur un reste dont l'exposant privégié n'est plus divisible par $exp(f)$ (resp. dont aucun monôme n'est divisible par $exp(f)$).

Définition 5 (Divisions).

Division faible et forte par une famille (processus non déterministe).

Si un reste d'une division faible d'un dividende par une BS est nul, tout autre reste aussi. Sinon, l'exposant privilégié du reste est unique.

Le reste d'une division forte d'un dividende par une BS est unique. En particulier, la division réalise la projection canonique de l'anneau de polynômes sur son anneau quotient par l'idéal (opération k-linéaire.

Unicité des quotients. Décomposition en somme directe de l'anneau ambiant comme EV en un idéal et l'anneau quotient.

Noethérianité de l'anneau des polynômes (Théorème de Hilbert).

Notes

Historique rapide BS/GB, Macaulay/Hironaka/Groebner/Buchberger. Majorant doublement exponentiel du degré d'une BS. Mention et comparaison Hermann/Moreno. Borne inférieure de Mayr-Meyer. Annonce du cas général.