

Algèbre effective - TD2

Ordres monomiaux, bases de Gröbner

Exercice 1. 1. (1.7.3) Montrer qu'en deux variables, les ordres *deglex* et *degrevlex* sont égaux.

2. Construire un exemple de $f, g, h \in k[x, y, z]$ tels que $\bar{f}^{g, h}$ soit différent pour les ordres *deglex* et *degrevlex*.

Exercice 2. (1.7.5) Soit $<$ un ordre total sur l'ensemble des monômes de $k[x_1, \dots, x_n]$ tel que pour tous $\alpha, \beta, \gamma \in \mathbb{N}^n$,

$$x^\alpha \leq x^\beta \implies x^{\alpha+\gamma} \leq x^{\beta+\gamma}.$$

On définit sa version graduée $<^{\deg}$ par

$$\alpha <^{\deg} \beta \iff |\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } \alpha < \beta).$$

Montrer que $<^{\deg}$ est un ordre monomial.

Exercice 3. (1.7.6) Montrer que dans un anneau de polynômes à une variable, l'algorithme de division multivariée coïncide avec l'algorithme de division euclidienne.

Exercice 4. (1.7.9) Soit $g \in k[x_1, \dots, x_n] - \{0\}$. Montrer que pour tout ordre monomial, $\{g\}$ est une base de Gröbner de l'idéal $\langle g \rangle$.

Exercice 5. (1.7.11) Soit I un idéal de $k[x_1, \dots, x_n]$. Soit G une partie finie de I . On fixe un ordre monomial sur $k[x_1, \dots, x_n]$. Montrer que les propositions suivantes sont équivalentes:

- (1) $\langle G \rangle = I$ et pour tout $f \in I$, $\bar{f}^G = 0$;
- (2) $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$.

Exercice 6. (1.7.13) Soient G et G' deux bases de Gröbner d'un même idéal de $k[x_1, \dots, x_n]$ pour le même ordre monomial, et soit $f \in k[x_1, \dots, x_n]$. Montrer que les restes $\bar{f}^G$ et $\bar{f}^{G'}$ sont égaux. (Indication : considérer la différence $\bar{f}^G - \bar{f}^{G'}$ et son reste pour la division par G .)

Exercice 7. (1.7.21) Soit k un corps. Soit I un idéal de $R = k[x_1, \dots, x_n]$, et soit $f \in R$. L'objectif de l'exercice est de montrer que $f \in \sqrt{I}$ si et seulement si $\langle I, tf - 1 \rangle = \langle 1 \rangle$ dans $k[x_1, \dots, x_n, t]$.

1. Supposons d'abord que $f \in \sqrt{I}$. Montrer, en calculant $t^m f^m - 1$ pour un m bien choisi, que $1 \in \langle I, tf - 1 \rangle$.

2. Supposons désormais que $f \notin \sqrt{I}$.

(a) Soit $\bar{k}$ une clôture algébrique de k . Montrer qu'il existe $p \in \mathbb{A}^n(\bar{k})$ tel que $f(p) \neq 0$ et tel que pour tout $g \in I$, $g(p) = 0$.

(b) On considère le morphisme de k -algèbres :

$$\begin{aligned} \varepsilon: k[x_1, \dots, x_n, t] &\longrightarrow \bar{k} \\ x_i &\longmapsto p_i \\ t &\longmapsto \frac{1}{f(p)}. \end{aligned}$$

Montrer que $\langle I, tf - 1 \rangle \subseteq \ker(\varepsilon) \subsetneq k[x_1, \dots, x_n, t]$. En déduire que $1 \notin \langle I, tf - 1 \rangle$.

3. Déduire de ce résultat une façon de répondre à la question suivante : étant donné deux systèmes d'équations polynomiales $f_1 = \dots = f_r = 0$ et $g_1 = \dots = g_s = 0$, est-ce que leurs ensembles de solutions dans $\bar{k}^n$ sont les mêmes ?

4. Implémenter cette méthode.

Polytope de Newton et monômes dominants

Définition 1. L'enveloppe convexe d'une partie $S \subset \mathbb{R}^n$ est la plus petite partie convexe de $\mathbb{R}^n$ contenant S . On la note $\text{Conv}(S)$.

Définition 2. Un polytope dans $\mathbb{R}^n$ est l'enveloppe convexe d'un nombre fini de vecteurs.

Définition 3. Un point v d'un polytope $P \subset \mathbb{R}^n$ est appelé sommet de P si $v \notin \text{Conv}(P - \{v\})$. On notera $\text{Vert}(P)$ l'ensemble des sommets de P .

Théorème 1 (de l'hyperplan séparant). Soient U, V deux parties convexes disjointes de $\mathbb{R}^n$. Supposons U fermée et V compacte. Il existe un vecteur $x \in \mathbb{R}^n$ non nul et un réel c tels que :

- (1) pour tout $u \in U$, $\langle x | u \rangle \geq c$;
- (2) pour tout $v \in V$, $\langle x | v \rangle < c$.

Théorème 2 (Minkowski-Weyl). Les polytopes sont exactement les intersections bornées de familles finies de demi-espaces délimités par des hyperplans affines.

Exercice 8 (Quels termes d'un polynôme peuvent être dominants ?). Dans cet exercice, on considère un polytope $P = \text{Conv}(S)$ où $S = \{v_1, \dots, v_r\} \subseteq \mathbb{Q}^n$. En particulier,

$$P = \left\{ \sum_{i=1}^r \lambda_i v_i \mid \lambda_i \in [0, 1], \sum_{i=1}^r \lambda_i = 1 \right\}.$$

Dans une telle combinaison linéaire, on peut toujours supposer que les v_i tels que $\lambda_i \neq 0$ sont affinement indépendants. On en déduit que comme les v_i sont à coordonnées rationnelles,

$$P \cap \mathbb{Q}^n = \left\{ \sum_{i=1}^r \lambda_i v_i \mid \lambda_i \in \mathbb{Q} \cap [0, 1], \sum_{i=1}^r \lambda_i = 1 \right\}.$$

1. Montrer les propriétés suivantes des polytopes.

- (a) Les sommets de P appartiennent à S .
- (b) L'enveloppe convexe de $\text{Vert}(P)$ est P .
- (c) Pour tout vecteur $v \in \mathbb{R}^n$, $\text{Conv}(P \cup \{v\}) = \bigcup_{p \in P} [pv]$.

2. On considère désormais que $v_1, \dots, v_r$ sont les vecteurs d'exposants des monômes d'un polynôme $f \in k[x_1, \dots, x_n]$. Le polytope P est alors appelé polytope de Newton de f . Montrer que si $v_i \notin \text{Vert}(P)$ alors le monôme correspondant n'est dominant pour aucun ordre monomial.

3. Prenons $f = x^4 y^2 + x^3 y^5 + x^3 y^3 + xy \in k[x, y]$. Dessiner son polygone de Newton. Montrer que les monômes $x^3 y^3$ et xy ne sont dominants pour aucun ordre monomial. Donner des ordres monomiaux pour lesquels $x^4 y^2$ et $x^3 y^5$ sont dominants.

4. D'après la question précédente, conjecturer une condition suffisante sur un monôme pour qu'il existe un ordre monomial tel que ce monôme soit dominant.

5. Soit $Q \subseteq \mathbb{R}^n$ un polytope tel que $Q \cap (\mathbb{R}_+)^n = \emptyset$. Montrer qu'il existe un vecteur $x \in (\mathbb{R}_+)^n$ tel que pour tout $q \in Q$, $\langle x | q \rangle < 0$.

6. Étant donné une forme linéaire à coefficients positifs ou nuls, construire un ordre monomial compatible.

7. Supposons qu'un sommet v de P satisfasse la condition suffisante précédemment conjecturée. Montrer que quitte à translater P , on peut supposer que $P \cap (\mathbb{R}_+)^n = \{0\}$. En déduire un ordre monomial pour lequel v est le monôme dominant de P .