

Bases de Gröbner

TD 3

1 Idéaux monomiaux

Fonctions utiles : `LeadingCoefficient`, `LeadingMonomial`, `LeadingTerm`.

Exercice 1. Soit $I = \langle x^\alpha, \alpha \in A \rangle$ un idéal monomial et S l'ensemble des exposants qui apparaissent dans I . On considère un ordre monomial. Montrer que le plus petit élément de S appartient à A .

Exercice 2. Dans l'anneau $k[x_1, \dots, x_n, y_1, \dots, y_m]$ on considère l'ordre défini par l'ordre lexicographique sur les x_i et par l'ordre tdeg sur les y_j :

$$x^\alpha y^\beta > x^\gamma y^\delta \iff x^\alpha >_{lex} x^\gamma \text{ ou } x^\alpha = x^\gamma \text{ et } y^\beta >_{tdeg} y^\delta$$

Montrer que $>$ est un ordre monomial.

Exercice 3.

1. Écrire une fonction qui teste si un monôme m_1 est plus petit qu'un monôme m_2 pour l'ordre lexicographique.
2. Écrire une fonction qui, étant donnée une séquence de monômes, renvoie son plus petit élément m .
3. Écrire une fonction qui énumère les monômes dans l'ordre croissant pour l'ordre lexicographique.

2 Calcul de bases de Gröbner

Fonctions utiles : `gbasis`.

Exercice 4. Soit l'idéal $I = \langle x^2 - 2xz + 5, xy^2 + yz^3, 3y^2 - 8z^3 \rangle$ de $\mathbb{Q}[x, y, z]$.

1. Donner une base de Gröbner de I pour l'ordre lexicographique.
2. Donner une base de Gröbner de I pour l'ordre total.

Exercice 5. Soit l'idéal I de $\mathbb{Q}[x, y]$ défini par

$$I = \langle x^2 y^2 - x, xy^3 + y \rangle.$$

1. Donner une base de Gröbner de I pour l'ordre lexicographique.
2. Vérifier que les éléments obtenus appartiennent effectivement à I .
3. Soit $P = x^3 y^2 + 2xy^4$. Calculer $\overline{P}^G$.

Exercice 6. Dans $k[X_1, X_2, X_3]$, on choisit l'ordre lexicographique inverse. Calculer une base de Gröbner de l'idéal $I = (X_1 X_2 X_3 + X_3^3, X_2^2)$.

Exercice 7. Soit G une base de Gröbner pour l'idéal $I \subset k[x_1, \dots, x_n]$ (avec l'ordre lexicographique) et supposons qu'il existe $p \neq q \in G$ tels que $LT(p)$ divise $LT(q)$. Montrer que $G \setminus \{q\}$ est encore une base de Gröbner pour I .

Exercice 8. Le polynôme $x^3 + 1$ est-il combinaison linéaire (sur $\mathbb{Q}[x, y, z]$) de $x + y + z, xy + yz + zx$ et $xyz + 1$?

Exercice 9. Soit $I \in k[x_1, \dots, x_n]$ un idéal principal. Montrer que tout sous-ensemble fini contenant un générateur de I est une base de Gröbner pour I .

Exercice 10. Soit l'idéal

$$I = \langle c^5 - b^3d^2, a^2d - bc^2, a^2c^3 - b^4d, a^4c - b^5 \rangle$$

de $k[a, b, c, d]$.

1. Montrer que le système générateur de I est une base de Gröbner pour l'ordre lexicographique avec $a > b > c > d$.
2. Trouver un ordre sur les variables tel que $\langle c^{11}, bc^2, b^3d^2, b^4d, b^5, a^2b^2d^3, a^4bd^4 \rangle$ soit $\langle LT(I) \rangle$.

Exercice 11. On se place dans un anneau $R = k[X_1, \dots, X_n]$ où k est un corps commutatif. Soit I un idéal de R non nul. Une base de Gröbner universelle est un ensemble qui est une base de Gröbner de I pour tous les ordres admissibles de R . Calculer une base de Gröbner universelle de l'idéal de $\mathbb{Q}[X, Y]$ engendré par $X - Y^2$ et $XY - X$.

Exercice 12. Soit l'anneau A des polynômes à $2m$ indéterminées $(x_{ij})_{1 \leq i \leq 2, 1 \leq j \leq n}$, à coefficients dans k . Soit I l'idéal de A engendré par les $\binom{m}{2}$ polynômes $D_{k,\ell} = x_{1k}x_{2\ell} - x_{1\ell}x_{2k}$.

1. Pour $m = 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I .
2. Pour $m \geq 3$, montrer que les $D_{k,\ell}$ forment une base de Gröbner universelle de I .

Exercice 13. Soit V un sous-espace vectoriel de k^n de dimension $n - d < n$. Soit I son idéal annulateur dans $k[x]$: l'idéal I est engendré par d formes linéaires indépendantes

$$I = \left\langle \sum_{j=1}^n a_{ij}x_j, 1 \leq i \leq d \right\rangle.$$

On dit qu'une forme linéaire non nulle de I est un circuit si son ensemble de variables est minimal pour l'inclusion. On dit qu'un d -sous-ensemble $J = \{j_1, \dots, j_d\} \subset \{1, \dots, n\}$ est une base, si le déterminant D_J de la matrice $(a_{ij})_{i,j \in \{j_1, \dots, j_d\}}$ associée est non nul.

1. Montrer que les circuits sont précisément les formes linéaires non nulles

$$D_{k_1, \dots, k_{d-1}, 1}x_1 + D_{k_1, \dots, k_{d-1}, 2}x_2 + \dots + D_{k_1, \dots, n}x_n$$

où $1 \leq k_1 < \dots < k_{d-1} \leq n$.

2. En déduire qu'il y a au plus $\binom{n}{d-1}$ circuits.
3. Soit I' un idéal engendré par des formes linéaires. Montrer que l'ensemble des circuits dans I est une base de Gröbner universelle de I .

3 Critère de Buchberger

Fonction utile : `SPolynomial`.

Exercice 14. Soient les polynômes $P_1 = x^3y - 2x^2y^2 + x$ et $P_2 = 3x^4 - y$ de $\mathbb{Q}[x, y]$ avec l'ordre lexicographique.

1. Calculer $P = S(P_1, P_2)$.
2. Soit $I = \langle P_1, P_2 \rangle$. La base (P_1, P_2) est-elle de Gröbner ?

Exercice 15. Déterminer si les ensembles suivants sont des bases de Gröbner des idéaux qu'ils engendrent.

1. $\{x^2 - y, x^3 - z\}$ pour l'ordre lexicographique gradué.
2. $\{x^2 - y, x^3 - z\}$ pour l'ordre lexicographique avec $x < y < z$ puis $x > y > z$.
3. $\{xy^2 - xz + y, xy - z^2, x - yz^4\}$ avec l'ordre lexicographique.

Exercice 16. La fonction $S(f, g)$ dépend-elle du choix de l'ordre monomial ?

Exercice 17. Soit $I \subset k[x_1, \dots, x_n]$ un idéal et G une base de Gröbner de I .

1. Montrer que $\overline{f}^G = \overline{g}^G$ si et seulement si $f - g \in I$.
2. En déduire que $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.
3. En déduire que $\overline{fg}^G = \overline{f}^G \overline{g}^G$.

4 Algorithme de Buchberger, Bases de Gröbner réduite

Exercice 18. Déterminer une base de Gröbner des idéaux suivants :

1. $I = \langle x^2, xy + y^2 \rangle$ de $k[x, y]$ avec l'ordre lexicographique.
2. $I = \langle y^2, xyz + z^3 \rangle$ de $\mathbb{Q}[x, y, z]$ avec l'ordre lexicographique inverse gradué.
3. $I = \langle x^2y - 1, xy^2 - x \rangle$ de $\mathbb{Q}[x, y]$ avec les ordres lexicographique et lexicographique gradué.
4. $I = \langle x - z^3, y - z^5 \rangle$ de $\mathbb{Q}[x, y, z]$ avec les ordres lexicographique et lexicographique inverse gradué.

Exercice 19. Montrer que pour tout $m \geq 1$, la base réduite de Gröbner de

$$I_m = \langle x^{m+1} - yz^{m-1}t, xy^{m-1} - z^m, x^mz - y^mt \rangle \subset k[x, y, z, t]$$

avec l'ordre lexicographique inverse gradué contient $f_m = z^{m^2+1} - y^{m^2}t$. En déduire la base réduite de Gröbner de I_m .

Exercice 20. Soit $2 \leq n' \leq n$.

1. Soient $r \geq 1$ un entier et $J = (m_1, \dots, m_r)$ un idéal monomial de $k[X_1, \dots, X_n]$. Soit I l'idéal engendré par les m_i . Donner des générateurs de l'idéal $J \cap (X_{n'}, \dots, X_n)$. Dans la suite on fixe sur $k[X_1, \dots, X_n]$ l'ordre lexicographique inverse, on désigne par I un idéal homogène non nul et par I' l'intersection $I' = I \cap (X_{n'}, \dots, X_n)$.
2. Montrer que $LT(I') = LT(I) \cap (X_{n'}, \dots, X_n)$.

3. Soit $f_1, \dots, f_s$ une base de Gröbner de I formée de polynômes homogènes. Dédurre des questions précédentes des générateurs de $LT(I')$. En déduire une base de Gröbner de I' .
4. Soit $f_1, \dots, f_s$ une base de Gröbner réduite de I formée de polynômes homogènes. Donner une condition nécessaire et suffisante pour qu'on ait $I \cap (X_n) = X_n I$.

Exercice 21. Soit l'idéal $I = \langle y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2 \rangle$.

1. Montrer que $I \cap \mathbb{Q}[x] = \langle x^3 - x^2 \rangle$. (On pourra utiliser l'exercice 20).
2. Montrer que $I \cap \mathbb{Q}[y] = \langle y^5 - 2y^4 \rangle$.

Exercice 22. Soient f et g deux polynômes non nuls sans facteur commun et I l'idéal qu'ils engendrent. On suppose que (f, g) est une base de Gröbner de I .

1. On pose : $LT(f) = \lambda mm'$, $LT(g) = \mu mm''$, où m est un monôme, m' et m'' sont deux monômes premiers entre eux, λ et μ sont deux scalaires. En utilisant la division du S -polynôme $S(f, g)$ par la suite f, g , montrer qu'il existe un polynôme g_1 dont $LT(g_1)$ n'est pas divisible par $LT(f)$ et tel que f divise $g_1 + \lambda m'$.
2. En déduire que $m = 1$.
3. En déduire que (f, g) est une base de Gröbner de I si et seulement si $LT(f)$ et $LT(g)$ sont premiers entre eux.
4. On pose $f = hf'$, $g = hg'$, où f' et g' n'ont pas de facteur commun. Montrer que (f, g) est une base de Gröbner de I si et seulement si (f', g') est une base de Gröbner de l'idéal I' engendré par f' et g' .
5. Donner une condition nécessaire et suffisante pour que (f, g) soit une base de Gröbner de I .