Université de Lille

Master Mathématiques, 2020-21

Feuille d'exercices 2

§1. Bases de Gröbner / ordres monomiaux

1. Exercice
1.1) Montrer que les ordres lexicographique pure, lexicographique gradué et lexicographique gradué inverse sont bien des ordres monomiaux comme affirmé dans le cours.
1.2) La relation définie en oubliant la comparaison des degrés dans la définition de l'ordre lexicographique gradué inverse définit-elle une relation d'ordre monomial?

2. Exercice
Prendre un polynôme au hasard et ordonner ses termes par rapport à l'ordre lexicographique pure, à l'ordre lexicographique gradué et à l'ordre lexicographique gradué inverse.

3. Exercice
Soit $\underline{w} = (w_1, \dots, w_r) \in \mathbb{R}^r_+$ un vecteur de *poids*. On note $\underline{x} \cdot \underline{w} = x_1 w_1 + \cdots + x_r w_r$ le produit scalaire d'un vecteur $\underline{x} = (x_1, \dots, x_r) \in \mathbb{R}^r$ avec $\underline{w} \in \mathbb{R}^r_+$. On considère la relation sur les monômes telle que $x^{\underline{m}} \leq x^{\underline{n}}$ si $\underline{w} \cdot \underline{m} \leq \underline{w} \cdot \underline{m}$. Montrer que cette relation définit un ordre monomial lorsque les nombres $w_1, \dots, w_n$ sont $\mathbb{Q}$-linéairement indépendants.

§2. Bases de Gröbner / réduction et calcul de bases de Gröbner

1. Exercice
Prendre une famille de polynômes au hasard $(g_1, \dots, g_k)$ avec $k = 1, 2$ ou 3. Prendre des polynômes f au hasard et calculer leur division par rapport à la famille $(g_1, \dots, g_k)$. Expliciter des exemples de polynômes tels que $f \to^* r_1$ et $f \to^* r_2$ pour des polynômes réduits tels que $r_1 \neq r_2$.

2. Problème
On détermine complètement les écritures standards $f = q_1 g_1 + \cdots + q_k g_k + r$ que l'algorithme de division peut produire, pour une famille de polynômes donnée $g_1, \dots, g_k$, en supposant que dans l'algorithme de division, lorsque l'on a $\mathrm{lm}(g_i) | w_t$ pour plusieurs polynômes $\mathrm{lm}(g_i)$ on choisit toujours d'effectuer la réduction

$$f_{t-1} \to f_t = f_{t-1} - \frac{c_t w_t}{\mathrm{lt}(g_{i_t})} g_{i_t}$$

pour le premier polynôme g_{i_t} tel que $\mathrm{lm}(g_{i_t}) | w_t$ qui vient dans l'ordre de la famille $(g_1, \dots, g_k)$.
On écrit $\mathrm{lm}(g_i) = x^{\underline{m}(i)}$ le monôme dominant de chaque polynôme g_i. On pose

$$\Delta_1 := \underline{m}(1) + \mathbb{N}^r, \quad \Delta_2 := (\underline{m}(2) + \mathbb{N}^r) \setminus \Delta_1, \quad \dots, \quad \Delta_k = (\underline{m}(k) + \mathbb{N}^r) \setminus \bigcup_{i=1}^{k-1} \Delta_i$$

$$\text{et} \quad \overline{\Delta} = \mathbb{N}^r \setminus \bigcup_{i=1}^{k} \Delta_i.$$

(On notera que ces ensembles Δ_i, $i = 1, \dots, k$, et $\overline{\Delta}$ forment une partition de $\mathbb{N}^r$.)

BF, Courriel: `Benoit.Fresse@univ-lille.fr`

2.1) Montrer que $\underline{n} = (n_1, \ldots, n_r)$ vérifie $\underline{n} \in \Delta_i$ si $x^{\underline{m}(i)}$ divise $x^{\underline{n}}$ et $x^{\underline{m}(j)}$ ne divise pas $x^{\underline{n}}$ pour $j < i$. Montrer que $\underline{n} = (n_1, \ldots, n_r)$ vérifie $\underline{n} \in \overline{\Delta}$ si aucun monôme $x^{\underline{m}(i)}$ ne divise $x^{\underline{n}}$.
2.2) Montrer que dans une expression $f = q_1 g_1 + \cdots + q_k g_k + r$ retournée par un algorithme de division, on a $x^{\underline{n}} \in \mathrm{supp}(q_i) \Rightarrow \underline{n} + \underline{m(i)} \in \Delta_i$ et $x^{\underline{n}} \in \mathrm{supp}(r) \Rightarrow \underline{n} \in \overline{\Delta}$.
2.3) Montrer que, pour un polynôme f donné, on a une unique décomposition $f = q_1 g_1 + \cdots + q_k g_k + r$ qui satisfait les conditions de la question précédente. L'écriture standard de f qui résulte de l'algorithme de division est donc caractérisée par ces conditions.

Référence: voir [3, §2.3, exercice 11].

3. Exercice
Les polynômes $(x^2 - y, x^3 - z)$ forment-ils une base de Gröbner dans l'ordre lexicographique gradué? Dans l'ordre lexicographique pure lorsque l'on prend $x < y < z$? Lorsque l'on prend $x > y > z$?

4. Exercice
Construire une base de Gröbner de l'idéal $I = (x^2 - 2yz, xy^2 + z^2, yz + z)$ pour l'ordre lexicographique gradué et pour l'ordre lexicographique gradué inverse.

5. Exercice
Soient $G = (g_1, \ldots, g_m)$ et $H = (h_1, \ldots, h_n)$ des bases de Gröbner associé à des idéaux $I = (g_1, \ldots, g_m)$ et $J = (h_1, \ldots, h_n)$. On suppose que l'on a $pgcd(\mathrm{lm}(g_i), \mathrm{lm}(h_j)) = 1$ $(\forall i, j)$. Montrer que la famille $G \cup H = (g_1, \ldots, g_m, h_1, \ldots, h_n)$ forme alors une base de Gröbner de l'idéal $I + J$.

§3. Idéaux monomiaux et applications

1. Exercice
Soient I et J des idéaux d'un anneau de polynômes $\mathbb{K}[x_1, \ldots, x_r]$ tels que $I \subset J$. Montrer que si on a $\mathrm{lm}(I) = \mathrm{lm}(J)$ pour un ordre monomial donné, alors on a $I = J$.

2. Exercice
Soit I un idéal de $\mathbb{K}[x_1, \ldots, x_r]$ muni d'une base de Gröbner $G = (g_1, \ldots, g_k)$. Pour $f \in \mathbb{K}[x_1, \ldots, x_r]$, on note $\overline{f}^G$ le résultat du processus de division de f par les polynômes $G = (g_1, \ldots, g_k)$, de sorte que $f \to^* \overline{f}^G$ et $\overline{f}^G$ donne l'expression de f dans la base de $\mathbb{K}[x_1, \ldots, x_r]/I$ consistuée des classes des monômes tels que $w \notin \mathrm{lm}(I)$ (voir cours). Prouver que l'on a les relations

$$\overline{f_1 + f_2}^G = \overline{f_1}^G + \overline{f_2}^G \quad \text{et} \quad \overline{f_1 f_2}^G = \overline{\overline{f_1}^G \cdot \overline{f_2}^G}^G.$$

§4. Anneaux noethériens

1. Problème
Le but de ce problème est de démontrer le théorème de la base de Hilbert laissé en exercice dans le cours: "Si un anneau R est noethérien, alors l'anneau des polynômes $R[x]$ est noethérien.".

Partie 1.
Pour un idéal I de $R[x]$, on note $d_n(I)$ le sous ensemble de R tel que:

$$d_n(I) := \{0\} \cup \{a \neq 0 \,|\, \exists p(x) \in I \text{ avec } p(x) = ax^n + a_{n-1}x^{n-1} + \ldots + a_0\}.$$

1.1) Prouver que $d_n(I)$ forme un idéal de R. Observer que l'on a $d_n(I) \subset d_{n+1}(I)$ pour tout $n \in \mathbb{N}$.

1.2) Soient I et J des idéaux de $R[x]$ tels que $I \subset J$. On note que l'on a clairement $d_n(I) \subset d_n(J)$, pour tout $n \in \mathbb{N}$. Prouver que pour de tels idéaux I et J tels que $I \subset J$, on a $d_n(I) = d_n(J)$ $(\forall n \in \mathbb{N}) \Leftarrow I = J$. *Indication:* Considérer un polynôme de degré minimal dans $J \setminus I$, soit $q(x) \in J \setminus I$, et un polynôme $p(x) \in I$ de même coefficient dominant que $p(x)$ via $d_n(I) = d_n(J)$ pour $n = \deg q(x)$. Que peut-on dire du polynôme $q(x) - p(x)$?

Partie 2.

Soit $I_0 \subset I_1 \subset \cdots \subset I_k \subset \cdots$ une suite croissante d'idéaux de $R[x]$. On forme la double famille d'idéaux $d_n(I_k)$, $(n,k) \in \mathbb{N}^2$, qui forme une double suite d'inclusion:

$$\begin{tikzcd}
d_0(I_0) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_0(I_1) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \arrow[r, dash, "\subset"] & d_0(I_k) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_0(I_{k+1}) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \\
d_1(I_0) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_1(I_1) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \arrow[r, dash, "\subset"] & d_1(I_k) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_1(I_{k+1}) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \\
\vdots \arrow[d, dash, "\cap"] & \vdots \arrow[d, dash, "\cap"] & & \vdots \arrow[d, dash, "\cap"] & \vdots \arrow[d, dash, "\cap"] & \\
d_n(I_0) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_n(I_1) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \arrow[r, dash, "\subset"] & d_n(I_k) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_n(I_{k+1}) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \\
d_{n+1}(I_0) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_{n+1}(I_1) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \arrow[r, dash, "\subset"] & d_{n+1}(I_k) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & d_{n+1}(I_{k+1}) \arrow[r, dash, "\subset"] \arrow[d, dash, "\cap"] & \cdots \\
\vdots & \vdots & & \vdots & \vdots &
\end{tikzcd}$$

d'après les observations de la partie précédente.

1.3) Prouver que $d_n(I_k)$, $(n,k) \in \mathbb{N}^2$, possède un élément maximal ou, de façon équivalente, qu'il existe un couple (m,l) tel que $n \geq m$ et $k \geq l \Rightarrow d_n(I_k) = d_m(I_l)$. *Indication:* On pourra considérer la famille diagonale $d_n(I_n)$.

1.4) Pour $n < m$ fixé, on considère la suite $d_n(I_k)$, $k \in \mathbb{N}$, et l'indice k_n tel que $k \geq k_n \Rightarrow d_n(I_k) = d_k(I_{k_n})$, en utilisant l'hypothèse que R est noethérien. Puis on pose $K = \max(l, k_0, \dots, k_{m-1})$. Prouver que pour $k \geq K$, on a $d_n(I_k) = d_n(I_K)$ quel que soit $n \in \mathbb{N}$. *Indication:* On distinguera les cas $n \geq m$ et $n < m$.

1.5) Conclure que l'on a $k \geq K \Rightarrow I_k = I_K$ en utilisant les résultats de la partie précédente.

2. Exercice

2.1) Soit

$$A_0 \xrightarrow{\phi_1} A_0 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_r} A_r \xrightarrow{\phi_{r+1}} \cdots$$

une suite de morphismes de $\mathbb{K}$-algèbres $\phi_r : A_{r-1} \to A_r$. On définit la *colimite* de cette suite comme l'ensemble A_∞ constitué des couples (a_r, r) tels que $r \in \mathbb{N}$, $a_r \in A_r$, quotienté par la relation d'équivalence telle que $(a_r, r) \equiv (\phi_{r+1}(a_r), r+1)$. On note $i_r : A_r \to A_\infty$ l'application canonique qui envoie $a_r \in A_r$ sur la classe de (a_r, r) dans A_∞.

Montrer que A_∞ hérite d'une structure de $\mathbb{K}$-algèbre telle que chaque application $i_r : A_r \to A_\infty$ définit un morphisme de $\mathbb{K}$-algèbres. Montrer que A_∞ peut-être caractérisé (à isomorphisme de $\mathbb{K}$-algèbre près) par la propriété universelle suivante: "Pour toute $\mathbb{K}$-algèbre B munie de morphismes

$f_r : A_r \to B$ tels que $f_{r+1}\phi_{r+1} = f_r$ $(\forall r)$, il existe un unique morphisme $f_\infty : A_\infty \to B$ tel que $f_\infty i_r = f_r$ $(\forall r)$.”. On matérialise la construction de ce morphisme dans un diagramme:

$$\begin{tikzcd}
A_0 \arrow[r, "\phi_1"] \arrow[drrrrr, bend right=10, "f_0"'] & \cdots \arrow[r, "\phi_r"] & A_r \arrow[r, "\phi_{r+1}"] \arrow[drrr, "f_r"'] & A_{r+1} \arrow[r, "\phi_{r+2}"] \arrow[drr, "f_{r+1}"'] & \cdots \arrow[r] & A_\infty \arrow[d, dotted, "\exists! f_\infty"] \\
 & & & & & B
\end{tikzcd} .$$

2.2) On pose $A_r = \mathbb{K}[x_r]$ pour une indéterminée x_r et on considère la suite de morphisme de $\mathbb{K}$-algèbres $\phi_r : \mathbb{K}[x_{r-1}] \to \mathbb{K}[x_r]$ tels que $\phi_r(x_{r-1}) = x_r^r$, pour $r = 1, 2, \ldots$. On note par abus de notation x_r l'image de la variable $x_r \in A_r$ dans A_∞ et on pose $x = x_0$. Soit B un anneau. Montrer que se donner un morphisme de $\mathbb{K}$-algèbres $f_\infty : A_\infty \to B$ revient à fixer un élément $b \in B$ tel que $b = f_\infty(x)$ et un système de racine de b, c'est à dire une collection d'éléments b_n, $n \in \mathbb{N}^*$, tels que $b_n^n = b$ et qui satisfait la relation de cohérence $b_n^d = b_{n/d}$ lorsque $d|n$. (*Indication:* Quelle relation lie x_r et $x = x_0$ dans A_∞?) On interprète donc A_∞ comme un anneau universel $\mathbb{K}[x^{1/n}, n \in \mathbb{N}^*]$ que l'obtient en ajoutant formellement des racines de la variable $x^{1/n}$, $n \in \mathbb{N}^*$, dans l'anneau des polynômes $\mathbb{K}[x]$.

2.3) Prouver que cet anneau $A = \mathbb{K}[x^{1/n}, n \in \mathbb{N}^*]$ n'est pas noethérien en exhibant une suite strictement croissante infinie d'idéaux $I_0 \subset I_1 \subset \cdots \subset I_r \subset I_{r+1} \subset \cdots$ dans A.

§5. Bibliographie

Certains exercices sur les bases de Gröbner, quand ils ne sont pas classiques, sont tirés ou inspirés des références ci-dessous auxquelles on renvoie pour des études exhaustives du sujet.

1. William W. Adams, Philippe Loustaunau. An introduction to Gröbner bases. Graduate Studies in Mathematics 3, American Mathematical Society, 1994.
2. Thomas Becker, Volker Weispfenning, in cooperation with Heinz Kredel. Gröbner bases. A computational approach to commutative algebra. Graduate Texts in Mathematics 141, Springer-Verlag, 1993.
3. David Cox, John Little, Donal O'Shea. Ideals, varieties and algorithms. An introduction to computational algebraic geometry and commutative algebra. Undergraduate Texts in Mathematics, Springer-Verlag, 1992.
4. Viviane Ene, Jürgen Herzog. Gröbner bases in commutative algebra. Graduate Studies in Mathematics 130, American Mathematical Society, 2012.
5. Raf Fröberg. An introduction to Gröbner bases. Pure and Applied Mathematics. John Wiley & Sons, 1997.