M2 AA – ALGÈBRE EFFECTIVE

Épreuve du 27 novembre 2023, 13h50 – *durée : 3 heures*

Les documents et ordinateurs sont autorisés, voire nécessaires. Écrivez lisiblement, numérotez vos pages. Les candidat·es peuvent rédiger en français ou en anglais. Les 3 exercices sont indépendants.

Exercice 1. Soit K un corps et soit I un idéal de $K[x_1,\dots,x_n]$. On dira qu'un sous-ensemble E de $K[x_1,\dots,x_n]$ est *stable par l'action d'une permutation* $\sigma \in \mathfrak{S}_n$ si $f\cdot\sigma \in E$ pour tout $f \in E$.

(1) Supposons qu'il existe un ensemble de générateurs F de I qui soit stable par l'action de toutes les permutations de $\mathfrak{S}_n$. Montrer que I est stable par l'action de toutes les permutations de $\mathfrak{S}_n$.

(2) On conserve les hypothèses de (1). Montrer que si G est une base de Gröbner marquée de I pour un ordre monomial $<$, alors pour tout $\sigma \in \mathfrak{S}_n$, il existe un ordre monomial pour lequel $G\cdot\sigma$ est la base de Gröbner marquée.

(3) Soit maintenant $\mathcal{P}_n$ le sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ des matrices de permutations. L'action de $\mathrm{GL}_n(\mathbb{R})$ sur $\mathbb{R}^n$ induit une action de $\mathcal{P}_n$ sur $\mathbb{R}^n_{\geq 0}$.

On conserve les hypothèses de (1). Soit $GF(I)$ l'éventail de Gröbner de I. Montrer que toute matrice $P \in \mathcal{P}_n$ envoie un cône maximal de $GF(I)$ sur un cône maximal de $GF(I)$. En particulier, $GF(I)$ est invariant par l'action de $\mathcal{P}_n$.

(4) Application : pour cette question, prenons $K = \mathbb{Q}$, $n = 3$ et $I = \langle x+y+z^2, x+y^2+z, x^2+y+z\rangle$. Dessinez son éventail de Gröbner, en précisant les bases de Gröbner marquées pour chaque cône maximal. (On pourra s'aider des questions précédentes pour simplifier les calculs et la description des bases de Gröbner ; il peut être utile de considérer l'action de $\mathcal{P}_3$ sur l'intersection de $\mathbb{R}^3_{\geq 0}$ avec le plan $x+y+z=1$.)

Il peut être utile de commencer par les ordres monomiaux suivants :

(a) lex, avec $x > y > z$.

(b) degrevlex, avec $x > y > z$.

(c) L'ordre donné par la matrice $\begin{bmatrix} 10 & 6 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, qu'on peut créer par la commande suivante :

```
R = PolynomialRing(QQ, 'x,y,z', order=TermOrder('wdeglex',(1,2,3))).
```

Exercice 2. Soient K et L deux corps, et soit $\alpha \in L \setminus \{0\}$ un élément *algébrique* sur K, c'est-à-dire qu'il existe un polynôme $f \in K[X]$ tel que $f(\alpha) = 0$. Soit $P_\alpha \in K[X]$ le *polynôme minimal* de α, c'est-à-dire le polynôme unitaire qui engendre l'idéal

$$I_\alpha = \{f \in K[X] \mid f(\alpha) = 0\}.$$

On considère le corps $K(\alpha)$; le morphisme $K[X] \to K(\alpha) : f(X) \mapsto f(\alpha)$ est surjectif de noyau $\langle P_\alpha\rangle$, de sorte que $K(\alpha) \cong K[X]/\langle P_\alpha\rangle$.

Soit maintenant $\beta \in K(\alpha)$. On peut écrire $\beta = B(\alpha)$, avec $B(X) \in K[X]$. On cherche le polynôme minimal P_β de β sur K.

(1) Considérons l'idéal $I = \langle Y - B(X), P_\alpha(X)\rangle$ de $K[X,Y]$. Montrer que $(Y - B(X), P_\alpha(X))$ est une base de Gröbner de I pour l'ordre lexicographique avec $Y > X$.

(2) Montrer que le morphisme $\varepsilon : K[X,Y] \to K(\alpha) : f(X,Y) \mapsto f(\alpha,\beta)$ a pour noyau I. (Pour l'inclusion de $\ker\varepsilon$ dans I, on pourra effectuer la division multivariée d'un élément $f \in \ker\varepsilon$ par la base de Gröbner trouvée en (1) et montrer que le reste est nul.)

(3) Montrer que l'idéal d'élimination $I \cap K[Y]$ est égal à $\langle P_\beta(Y)\rangle$. (On pourra voir que $\langle P_\beta(Y)\rangle$ est le noyau de l'application $f(Y) \mapsto f(\beta)$, et appliquer (2)).

(4) Utiliser ce qui précède pour calculer le polynôme minimal de $\sqrt[3]{5} - 2(\sqrt[3]{5})^2$ sur $\mathbb{Q}$. Expliquer quelles bases de Gröbner doivent être calculées pour obtenir ce résultat. (On pourra utiliser sans preuve que $X^3 - 5$ est le polynôme minimal de $\sqrt[3]{5}$ sur $\mathbb{Q}$.)

Exercice 3. On fixe un corps k.

Un *problème d'optimisation linéaire en entiers* est un problème où l'on cherche à minimiser une forme linéaire $\ell(Z_1, \ldots, Z_n) = c_1 Z_1 + \ldots c_1 Z_n$ soumise aux système (*) d'équations linéaires

$$\begin{array}{rcl} a_{1,1}Z_1 + \ldots + a_{1,n}Z_n &=& b_1 \\ &\vdots& \\ a_{m,1}Z_1 + \ldots + a_{m,n}Z_n &=& b_m \end{array}$$

où les $a_{i,j}$ et les b_j sont des entiers positifs, et où les Z_i cherchés sont des entiers positifs. Considérons le morphisme d'anneaux

$$\begin{array}{rcl} \phi : k[y_1, \ldots, y_n] & \longrightarrow & k[x_1, \ldots, x_m] \\ y_j & \longmapsto & f_j := x_1^{a_{1,j}} \cdots x_m^{a_{m,j}}. \end{array}$$

(1) Montrer que $(Z_1, \ldots, Z_n) \in \mathbb{N}^n$ est une solution du système (*) si et seulement si $\phi(y_1^{Z_1} \cdots y_n^{Z_n}) = x_1^{b_1} \cdots x_m^{b_m}$.

(2) Montrer qu'un monôme $x^d = x_1^{d_1} \cdots x_m^{d_m}$ est dans $k[f_1, \ldots, f_n]$ si et seulement s'il peut s'écrire comme un monôme en les $f_1, \ldots, f_n$. En déduire que le système (*) admet une solution dans $\mathbb{N}^n$ si et seulement si $x_1^{b_1} \cdots x_m^{b_m} \in k[f_1, \ldots, f_n]$.

(3) Soit $<$ un ordre monomial sur $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ tel que tout monôme faisant intervenir l'un des x_i est plus grand que tout monôme ne faisant intervenir que les y_j. L'ordre est dit *adapté* si, pour tous monômes y^Z et $y^{Z'}$ tels que $\phi(y^Z) = \phi(y^{Z'})$ et $\ell(Z_1, \ldots, Z_n) > \ell(Z'_1, \ldots, Z'_n)$, on a que $y^Z > y^{Z'}$.

Montrer qu'il existe un ordre adapté. (Indication : on pourra considérer un ordre matriciel dont les premières lignes donnent un ordre monomial sur les x_i, et les lignes suivantes font intervenir les $a_{i,j}$ et les c_i.)

(4) Soit F un ensemble fini de polynômes constitué uniquement de monômes ou de binômes. Montrer que pour tout polynôme f comportant d termes, le reste $\overline{f}^F$ comporte au plus d termes.

De façon similaire, montrer que si h_1 et h_2 sont des polynômes comportant au plus 2 termes, alors $S(h_1, h_2)$ comporte au plus 2 termes.

(5) Soit $J = \langle f_1 - y_1, \ldots, f_n - y_n \rangle$ en tant qu'idéal de $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$. Soit $<$ un ordre adapté comme à la question (3), et soit G une base de Gröbner réduite de J pour cet ordre.

   (a) Montrer que G ne contient que des monômes et des binômes (indication : utiliser (4)). En déduire que pour tout monôme m, le reste $\overline{m}^G$ est un monôme.

   (b) On étend ϕ à $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$ en posant $\phi(x_i) = x_i$ pour tout $i \in \{1, \ldots, m\}$. Montrer que le noyau de ϕ est J.

   (c) Soit $f = x_1^{b_1} \cdots x_m^{b_m}$. Montrer que si $f \in k[f_1, \ldots, f_n]$ et $\overline{f}^G = y_1^{Z_1} \cdots y_n^{Z_n}$, alors $(Z_1, \ldots, Z_n)$ est une solution de (*) qui minimise ℓ. (Indication : si Z' est une autre solution, considérer $y^Z - y^{Z'}$.)