

**FEUILLE D'EXERCICES n° 11**  
Polynômes à plusieurs variables

Dans ce travail, on utilisera l'ordre lexicographique  $\prec_{\text{lex}}$  sur les monômes et aussi parfois l'ordre lexicographique gradué  $\prec_{\text{grlex}}$ .

Soit  $k$  un corps, et soit  $A = k[x_1, x_2, \dots, x_n]$ . On rappelle la définition des  $S$ -polynômes. Soit  $a = (a_1, \dots, a_n) \in \mathbb{N}^n$ . On note  $x^a = x_1^{a_1} \dots x_n^{a_n}$ . Soient  $g$  et  $h$  non nuls dans  $A$ . Soit  $\alpha = (\alpha_1, \dots, \alpha_n)$  le degré du terme dominant de  $g$  et soit  $\beta = (\beta_1, \dots, \beta_n)$  le degré du terme dominant de  $h$ . On note  $\gamma = (\max(\alpha_1, \beta_1), \dots, \max(\alpha_n, \beta_n))$ . Alors on définit

$$S(g, h) = \frac{x^\gamma}{\text{lt}(g)}g - \frac{x^\gamma}{\text{lt}(h)}h.$$

Le théorème suivant fournit un critère pratique pour reconnaître ou pour construire une base de Gröbner.

**Théorème 1.** *Un ensemble fini  $G = \{g_1, \dots, g_s\} \subset A$  est une base de Gröbner (de l'idéal de  $A$  engendré par  $G$ ) si et seulement si pour tout couple  $(i, j)$ , où  $1 \leq i \leq j \leq s$ , le reste de la division de  $S(g_i, g_j)$  par  $(g_1, \dots, g_s)$  est nul.*

Le premier exercice est un exercice de révision sur les groupes et les idéaux. Les suivants portent sur la division multivariée et les bases de Gröbner.

**Exercice 1** – [GROUPE, IDÉAUX]

Soient  $(A, +, \times)$  un anneau commutatif unitaire et  $\mathcal{P}$  une partie de  $A$ . On note

$$\langle \mathcal{P} \rangle = \left\{ \sum_{p \in \mathcal{F}} f_p p : \mathcal{F} \subset \mathcal{P} \text{ est fini et } f_p \in A \forall p \in \mathcal{F} \right\}$$

- 1) Montrer que  $\mathcal{P}$  est le plus petit idéal de  $A$  contenant  $\mathcal{P}$ .
- 2) Le sous-groupe de  $(A, +)$  engendré par  $\mathcal{P}$  est-il un idéal de  $A$ ?

**Exercice 2** – On utilise  $\prec = \prec_{\text{lex}}$ . Soient  $f = xy^2 - x$ ,  $f_1 = xy + 1$  et  $f_2 = y^2 - 1$ .

- 1) Diviser  $f$  par  $f_1$ , puis diviser le reste obtenu par  $f_2$ .
- 2) Le polynôme  $f$  appartient-il à  $\langle f_1, f_2 \rangle$ ?

**Exercice 3** – On utilise  $\prec = \prec_{\text{lex}}$ . Soient  $f = x^2y - xy^2 + y^2$ ,  $f_1 = xy - 1$  et  $f_2 = y^2 - 1$ .

- 1) Écrire de deux façons différentes  $f = g + r$ , où  $g \in \langle f_1, f_2 \rangle$  et où aucun terme de  $r$  n'est divisible par le terme dominant de  $f_1$  ni de  $f_2$ .
- 2) Le polynôme  $f$  appartient-il à  $I$ ?
- 3) Calculer  $f_3 = S(f_1, f_2)$ . Peut-on diviser ce polynôme par  $f_1$  ou  $f_2$ ?

- 4) Montrer que  $(f_1, f_2, f_3)$  est une base de Gröbner de  $I = \langle f_1, f_2 \rangle$ .
- 5) En déduire une autre méthode pour décider si  $f$  appartient ou pas à  $I$ .
- 6) On demande à sage une base de Gröbner de  $\langle f_1, f_2 \rangle$ . Il rend  $[y^2 - 1, x - y]$ . Commenter.

**Exercice 4** – On utilise  $\prec = \prec_{\text{lex}}$ . Soient  $f = xy^2 + 1$ ,  $f_1 = xy + 1$  et  $f_2 = y + 1$ .

- 1) En divisant  $f$  par  $f_1$ , puis par  $f_2$ , décomposer  $f = g + r$ , où  $g \in \langle f_1, f_2 \rangle$  et où aucun terme de  $r$  n'est divisible par le terme dominant de  $f_1$  ni de  $f_2$ .
- 2) Faire de même en divisant d'abord par  $f_2$ , puis par  $f_1$ .
- 3) Le polynôme  $f$  appartient-il à l'idéal engendré par  $f_1$  et  $f_2$  ?
- 4) Déterminer une base de Gröbner de l'idéal de  $\mathbb{Q}[x, y]$  engendré par  $f_1$  et  $f_2$ .

**Exercice 5** – On utilise  $\prec = \prec_{\text{grlex}}$ . Soient  $g = x^3 - 2xy$ ,  $h = x^2y - 2y^2 + x$ ,  $G = \{g, h\}$  et  $I = \langle G \rangle$ .

- 1) Montrer que  $x^2 \in I$ , que  $x^2 \in \langle \text{lt}(I) \rangle$ , mais que  $x^2 \notin \langle \text{lt}(G) \rangle$ .
- 2) Trouver une base de Gröbner de  $I$ .
- 3) Trouver la base de Gröbner réduite de  $I$ .

**Exercice 6** – Dans  $k[x, y, z]$ , soient  $f_1 = x - z^4$ ,  $f_2 = y - z^5$  et  $I = \langle f_1, f_2 \rangle$ .

- 1) Trouver une base de Gröbner de  $I$  pour l'ordre lexicographique (où  $x \succ y \succ z$ ). Soit  $B$  cette base.
- 2) Montrer que  $B$  n'est pas une base de Gröbner de  $I$  pour l'ordre lexicographique gradué.

**Exercice 7** – Soit  $k$  un corps. Montrer que les idéaux  $I = \langle x + xy, y + xy, x^2, y^2 \rangle$  et  $J = \langle x, y \rangle$  de  $k[x, y]$  sont égaux.

**Exercice 8** – [SYSTÈMES LINÉAIRES ET BASES DE GRÖBNER]

Soient  $k$  un corps,  $n$  un entier naturel non nul et  $A = (a_{i,j})_{i,j}$  une matrice de  $M_n(k)$ . Soient  $R = k[x_1, \dots, x_n]$  et

$$G_A = \left\{ \sum_{j=1}^n a_{i,j} x_j \in R : 1 \leq i \leq n \right\}$$

l'ensemble des polynômes linéaires correspondant aux lignes de la matrice  $A$ . On note  $I_A = \langle G_A \rangle$  l'idéal de  $R$  engendré par les éléments de  $G_A$ . Soit  $V(G_A) = V(I_A) = \text{Ker } A$  l'ensemble des solutions du système  $Ax = 0$ .

- 1) Montrer que si  $L \in \text{GL}_n(k)$ , alors  $I_{LA} = I_A$ .

2) On suppose qu'il existe  $L \in \text{GL}_n(k)$  telle que

$$U = LA = \begin{pmatrix} I_r & V \\ 0 & 0 \end{pmatrix},$$

où  $V \in M_{r, n-r}(k)$ . Montrer que  $G_U$  est la base de Gröbner réduite de  $I_A$  pour tout ordre  $\prec$  sur les monômes tel que  $x_1 \succ x_2 \succ \cdots \succ x_n$ .

3) Quelle est la base de Gröbner réduite de  $I_A$  dans le cas où  $A$  est inversible ?

**Exercice 9** – Soit  $K$  un corps. Soit  $a$  un élément algébrique sur  $K$ . On rappelle que le polynôme minimal  $m$  de  $a$  sur  $K$  est le polynôme unitaire de plus petit degré de  $K[x]$  tel que  $m(a) = 0$ . De plus, si  $P \in K[x]$ , alors  $P(a) = 0$  si et seulement si  $m$  divise  $P$ .

1) Soit  $f$  un polynôme irréductible de  $K[x]$ . Soit  $g \in K[x]$ , et soit  $m$  le polynôme minimal de l'image de  $g$  dans  $K[x]/(f)$ . Soit  $I$  l'idéal de  $K[x, y]$  engendré par  $g(x) - y$  et  $f(x)$ . Montrer que  $I \cap K[y] = m(y)K[y]$ .

2) Soit  $f = x^3 + x + 1 \in \mathbb{Q}[x]$ . Vérifier que  $f$  est irréductible dans  $\mathbb{Q}[x]$ . Soit  $a$  une racine de  $f$  dans  $\mathbb{C}$ . Comment peut-on calculer le polynôme minimal de  $a^2 + a + 1$  en utilisant une base de Gröbner ?