Université de Bordeaux
Mathématiques

Algèbre et calcul formel – Master
2025–2026

FEUILLE D'EXERCICES n° 12

Bases de Gröbner

Commençons par rappeler la définition de quelques ordres monomiaux fréquemment utilisés, et voyons comment faire appel à eux sur sage. On travaille sur l'anneau $k[x_1, \ldots, x_n]$. Soit $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$, on note $x^a = x_1^{a_1} \ldots x_n^{a_n}$ et

$$\deg x^a = \sum_{i=1}^{n} a_i.$$

Ordre Lexicographique : $x^a < x^b$ si et seulement s'il existe $1 \leqslant i \leqslant n$ tel que $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i < b_i$.

```
sage: A.<x,y,z>=PolynomialRing(QQ,order='lex')
sage: A
Multivariate Polynomial Ring in x, y, z over Rational Field
sage: A.term_order()
Lexicographic term order
sage: x>y
True
sage: x>y^2*z
True
```

Ordre lexicographique gradué : $x^a < x^b$ si $\deg x^a < \deg x^b$ ou si $\deg x^a = \deg x^b$ et s'il existe $1 \leqslant i \leqslant n$ tel que $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}, a_i < b_i$.

```
sage: B.<x, y, z> = PolynomialRing(QQ, order='deglex')
sage: B
Multivariate Polynomial Ring in x, y, z over Rational Field
sage: B.term_order()
Degree lexicographic term order
sage: x>y
True
sage: x>y^2*z
False
sage: x*y^2*z^3 > x^3*y^2
True
sage: x^2*y^3*z > x^3*y*z^2
False
```

Ordre lexicographique gradué inverse : $x^a < x^b$ si $\deg x^a < \deg x^b$ ou si $\deg x^a = \deg x^b$ et s'il existe $1 \leqslant i \leqslant n$ tel que $a_n = b_n, \ldots, a_{i+1} = b_{i+1}, a_i > b_i$.

```
sage: C.<x, y, z> = PolynomialRing(QQ, order='degrevlex')
sage: C
Multivariate Polynomial Ring in x, y, z over Rational Field
sage: C.term_order()
Degree reverse lexicographic term order
sage: x>y
True
sage: x>y^2*z
False
sage: x*y^2*z^3 > x^3*y^2
True
sage: x^2*y^3*z > x^3*y*z^2
True
```

Si l'on n'indique pas l'ordre, l'ordre par défaut est l'ordre lexicographique gradué inverse.

```
sage: D.<x, y, z> = PolynomialRing(QQ)
sage: D.term_order()
Degree reverse lexicographic term order
sage: D == C
True
```

Exercice 1 – On utilise l'ordre lexicographique et on considère les polynômes $f = xy^2 - x$, $f_1 = xy + 1$ et $f_2 = y^2 - 1$. Soit $I =< f_1, f_2 >$.

Pour définir $\mathbb{Q}[x, y]$, on écrit comme indiqué ci-dessus :

```
sage: Qxy.<x,y>=PolynomialRing(QQ,order='lex')
```

Pour définir I et trouver une base de Gröbner de I :

```
sage: I=Qxy.ideal([f1,f2])
sage: I.groebner_basis()
```

Pour savoir si f appartient à I, on peut définir l'anneau quotient $\mathbb{Q}[x, y]/I$, et on calcule l'image $\bar{f}$ de f dans ce quotient. Alors $f \in I$ si et seulement si $\bar{f} = 0$. Pour calculer $\bar{f}$, on définit d'abord $\mathbb{Q}[x, y]/I$:

```
sage: A.<a,b>=Qxy.quotient(I)
```

Ainsi, A désigne l'anneau quotient $\mathbb{Q}[x, y]/I$ et a, b sont les images respectives de x et y dans ce quotient. Pour calculer $\bar{f}$, on peut écrire

```
sage: f(a,b)
```

Si on veut le reste de la division de f par une base de Gröbner de I :

```
sage: lift(f(a,b))
```

1) Essayer avec $g = x^2y - x$ à la place de f.

2) Vous pouvez tester si la famille génératrice fournie est une base de Gröbner avec la commande

```
sage: I.basis_is_grobner()
```

$[f_1, f_2]$ est-elle une base de Gröbner ?

On peut aussi effectuer la division multivariée grâce à la commande

```
sage: f.reduce(L)
```

où L peut contenir soit une liste de polynômes, soit directement un idéal. Dans ce dernier cas, la réduction est faite selon une base de Gröbner.

3) Vérifiez que

```
sage: lift(g(a, b))
```

et

```
sage: g.reduce(I)
```

donnent bien la même chose.

4) Remontrez que $[f_1, f_2]$ n'est pas une base de Gröbner en obtenant un autre reste pour g.

5) Déterminez une base de Gröbner de I à l'aide de sage.

Exercice 2 –

Soit g, h deux polynômes multivariés non nuls. Soit $\alpha = (\alpha_1, \ldots, \alpha_n)$ le degré du terme dominant de g et soit $\beta = (\beta_1, \ldots, \beta_n)$ le degré du terme dominant de h. On rappelle que leur S-polynôme est défini par la relation

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

où $\gamma = (\max(\alpha_1, \beta_1), \ldots, \max(\alpha_1, \beta_1))$.

On rappelle également le critère de Buchberger :

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

1) Implémentez une fonction `S_poly(g, h)` qui calcule le S-polynôme de deux polynômes en argument.

2) Implémentez une fonction `is_grobner(L)` qui teste si une liste L de polynômes multivariés vérifie le critère de Buchberger.

3) Implémentez l'algorithme de Buchberger pour calculer une base de Gröbner.

4) Vérifiez que votre implémentation est correcte en la comparant avec ce que vous renvoie la commande native de sage.

Exercice 3 – On cherche à résoudre dans $\mathbb{R}$ le système

$$(\mathcal{S}) \ : \ \begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

Soient $f_1 = x^2 + y + z - 1$, $f_2 = x + y^2 + z - 1$ et $f_3 = x + y + z^2 - 1$. Soit $I = < f_1, f_2, f_3 >$.

1) En utilisant un ordre monomial judicieusement choisi, déterminez par un système de générateurs les idéaux $I \cap \mathbb{Q}[z]$ et $I \cap \mathbb{Q}[y, z]$.

2) Résoudre le système $(\mathcal{S})$.

Exercice 4 – On cherche à résoudre dans $\mathbb{Q}^2$ le système

$$f(x, y) = g(x, y) = 0, \tag{1}$$

où

$$f(x, y) = (y^2 + 6)(x - 1) - y(x^2 + 1),$$
$$g(x, y) = (x^2 + 6)(y - 1) - x(y^2 + 1).$$

1) Déterminer la base de Gröbner réduite de l'idéal $I = < f, g >$ de $\mathbb{Q}[x, y]$, correspondant à l'ordre lexicographique avec $x \succ y$, puis résoudre le système (1).

2) Vous pouvez aussi obtenir directement la solution à l'aide de la commande `I.variety()`

3) Faire un graphe. Pour cela, on peut utiliser les commandes suivantes.

```
sage: A=implicit_plot(f,(x,0,6),(y,0,6),color='red')
sage: B=implicit_plot(g,(x,0,6),(y,0,6),color='green')
sage: C=points([[2,2],[2,3],[3,2],[3,3]],pointsize=20)
sage: A+B+C
```

Exercice 5 – [Monômes Standards]

Soit K un corps et $R = K[X_1, \ldots, X_n]$ muni d'un ordre monomial. Soit I un idéal de R et G une base de Gröbner de I.

Définition 2. Soit $\alpha \in \mathbb{N}^n$. Le monôme X^α est dit **standard** par rapport à G si pour tout $g \in G$, le terme $lt(g)$ ne divise pas X^α.

1) Calculer la base de Gröbner réduite pour l'ordre lexicographique avec $x > y$ de l'idéal de $\mathbb{Q}[x, y]$:

$$I = < x^2 + y - 1, xy - x > .$$

2) Les polynômes suivants appartiennent-ils à I ?

$$f_1 = x^2 + y^2 - y \ , \ f_2 = 3xy^2 - 4xy + x + 1$$

3) Montrez que l'ensemble des monômes standards relativement à G forme une base du K-espace vectoriel R/I.

4) Donner une base de $\mathbb{Q}[x, y]/I$.

Exercice 6 – Dans $\mathbb{R}^3$, on considère la courbe $\mathcal{C}$ d'équation paramétrée

$$\begin{cases} x = t^2 \\ y = t^3 \\ z = t^4 \end{cases}$$

Soient $f_1 = x - t^2$, $f_2 = y - t^3$ et $f_3 = z - t^4 \in \mathbb{Q}[t, x, y, z]$ et $I =< f_1, f_2, f_3 >$.

1) Déterminer $J = I \cap \mathbb{Q}[x, y, z]$.

2) On note $V(J) = \{A = (a_0, a_1, a_2) \in \mathbb{R}^3 \ : \ f(A) = 0 \ \forall f \in J\}$. Montrer que $C = V(J)$.

Exercice 7 –

1) Que constate-t-on si l'on cherche à refaire l'exercice 6 sur la courbe de $\mathbb{R}^2$ d'équation paramétrée

$$x = \frac{1 - t^2}{1 + t^2} \ , \ y = \frac{2t}{1 + t^2}$$

2) Même exercice avec la courbe paramétrée

$$x = \frac{3t}{1 + t^3} \ , \ y = \frac{3t^2}{1 + t^3}$$

Exercice 8 – Dans $k[x, y, z]$, soient $f_1 = x - z^4$, $f_2 = y - z^5$ et $I =< f_1, f_2 >$.

1) Calculer la base de Gröbner réduite de I pour l'ordre lexicographique avec $x \succ y \succ z$. Quels sont les monomes standards correspondants ?

2) Calculer la base de Gröbner réduite de I pour l'ordre lexicographique gradué avec $x \succ y \succ z$. Quels sont les monomes standards correspondants ?

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 $\mathbb{C}$. En utilisant la question précédente, et avec l'aide de sage, calculer le polynôme minimal m de $a^2 + a + 1$?

3) En utilisant sage, vérifier que $m(a^2 + a + 1)$ est bien égal à 0.

4) Dans le système sage, il existe une commande pour calculer un polynôme minimal : la commande `minpoly`. Retrouver m en utilisant cette commande.