Université Bordeaux 1 — **Algèbre et calcul formel – Master**
Mathématiques — Année 2018–2019

FEUILLE D'EXERCICES n° 13

Exercice 1 – 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 $k[x_1, \dots, x_n]$. Soit $a = (a_1, \dots, a_n) \in \mathbb{N}^n$, on note $x^a = x_1^{a_1} \dots x_n^{a_n}$ 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 $a_1 = b_1, \dots, a_{i-1} = b_{i-1}, a_i < b_i$.

```
A.<x,y,z>=PolynomialRing(QQ,order='lex')
x>y
x>y**2*z
```

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 $a_1 = b_1, \dots, a_{i-1} = b_{i-1}, a_i < b_i$.

```
B.<x,y,z>=PolynomialRing(QQ,order='deglex')
x>y
x>y**2*z
x*y**2*z**3 > x**3*y**2
x**2*y**3*z > x**3*y*z**2
```

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 $a_n = b_n, \dots, a_{i+1} = b_{i+1}, a_i > b_i$.

```
C.<x,y,z>=PolynomialRing(QQ,order='degrevlex')
x>y
x>y**2*z
x*y**2*z**3 > x**3*y**2
x**2*y**3*z > x**3*y*z**2
```

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

```
pr.<x,y,z>=PolynomialRing(QQ)
pr==A
pr==C
```

Exercice 2 – Reprenons l'exercice 2 de la feuille 12, avec $k = \mathbb{Q}$. On utilise donc $\prec = \prec_{\text{lex}}$ et on considère les polynômes $f = xy^2 - x$, $f_1 = xy + 1$ et $f_2 = y^2 - 1$. Soit $I = < f_1, f_2 >$.

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

```
pr.<x,y>=PolynomialRing(QQ,order='lex')
```

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

```
I=pr.ideal([f1,f2])
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 $\mathbb{Q}[x,y]/I$:

```
A.<a,b>=pr.quotient(I)
```

Alors, 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 alors écrire

```
f(a,b)
```

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

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

Ici, on ne voit pas bien ce qui ce passe. Essayer avec $g = x^2y - x$ à la place de f.

2) Le quotient $\mathbb{Q}[x,y]/I$ est un espace vectoriel sur $\mathbb{Q}$. En utilisant la base de Gröbner de I trouvée, donner une base de cet espace vectoriel. Quelle est sa dimension ?

Exercice 3 – Reprendre l'exercice 3 de la feuille 12 : calculer à la machine la base de Gröbner et effectuer un calcul qui permet de décider si le polynôme donné appartient ou non à l'idéal.

Exercice 4 – On reprend l'exercice 5 de la feuille 12, avec $K = \mathbb{Q}$. On utilise l'ordre lexicographique gradué, avec $\prec = \prec_{\text{deglex}}$, où $y \prec x$. Soient $g = x^3 - 2xy$, $h = x^2y - 2y^2 + x$, $G = \{g, h\}$ et $I =< G >$. Soit B la base de Gröbner réduite de I.

1) On a déjà calculé B. Vérifier le résultat en utilisant la machine.

2) Quels est l'ensemble S des monômes standards de $\mathbb{Q}[x,y]/I$ pour B ? Quelle est la dimension de $\mathbb{Q}[x,y]/I$ comme $\mathbb{Q}$-espace vectoriel ?

3) Écrire le produit dans $\mathbb{Q}[x,y]/I$ de chaque couple d'éléments de S en fonction des éléments de S.

4) Soit $f = x^5 + y^2 + xy \in \mathbb{Q}[x,y]$. Quelle est la forme normale $n(f)$ de f par rapport à B (c'est-à-dire le reste de la division de f par B) ? On pourra pour répondre exécuter les commandes suivantes.

```
A.<a,b>=pr.quotient(I)
f=x**5+y**2+x*y
(f(a,b)).lift()
```

5) Quelle est la base de Gröbner réduite de I pour l'ordre lexicographique, où $y \prec x$?

6) Donner l'ensemble $\mathcal{M}$ des monômes standards correspondant.

7) Établir la table de multiplication de ces monomes standards dans $\mathbb{Q}[x,y]/(f)$.

8) Écrire la matrice de la multiplication par x dans $\mathcal{M}$, puis celle de la multiplication par y.

Exercice 5 –

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

Exercice 6 – 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, Déterminer 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 7 – On considère $R = K[X_1, \ldots, X_n]$ muni de l'ordre lexicographique $\prec$ tel que

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

Soit I un idéal de R. Pour tout $l \in [1, n]$, on note $I_l = K[X_{l+1}, \ldots, X_n] \cap I$.

1) Montrer que I_l est un idéal de $K[X_{l+1}, \ldots, X_n]$

On veut démontrer le théorème suivant.

Théorème 1. *Soit G une base de Gröbner de I. Alors $G_l = K[X_{l+1}, \ldots, X_n] \cap G$ est une base de Gröbner de I_l.*

2) Soit $f \in I_l$. Montrer qu'il existe $g \in G$ tel que $\mathrm{lt}(g)$ divise $\mathrm{lt}(f)$. Montrer alors que $\mathrm{lt}(g) \in K[X_{l+1}, \ldots, X_n]$. Montrer enfin que $g \in G_l$.

3) En déduire que $< \mathrm{lt}(I_l) > \subset < \mathrm{lt}(G_l) >$.

4) Terminer la démonstration du théorème.

Exercice 8 – On cherche à résoudre dans $\mathbb{C}^2$ le système

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

où

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

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

Exercice 9 – Dans $\mathbb{R}^3$, on considère la courbe C d'équation paramétrée $x = t^2$, $y = t^3$, $z = t^4$.

1) Déterminer la base de Gröbner réduite de l'idéal de $\mathbb{R}[x, y, z]$ correspondant, où l'ordre utilisé est l'ordre lexicographique avec $x \prec y \prec z \prec t$.

2) Donner un système d'équations qui détermine C de façon implicite.

3) L'ensemble des solutions de ce système est-il égal à C ?

Exercice 10 –

1) Même exercice avec 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 11 – 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 $x > y > z$. Quels sont les monomes standards correspondants ?

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

Exercice 12 – 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.