Feuille d'exercices n°6

Bases de Gröbner

Dans cette feuille, K désigne un corps (commutatif).

Exercice 1 (Divisions)**.** 1) Posons $g = XY^2 - X$, $f_1 = XY + 1$, $f_2 = Y^2 - 1$ dans $K[X, Y]$. Effectuer la division de g par (f_1, f_2) avec l'ordre lexicographique. Même question pour la division de g par (f_2, f_1). Comparer les résultats obtenus.

2) Posons $g = Z^3 - Y^2$, $f_1 = Y^2 - 1$, $f_2 = XY - Z^3$ dans $K[X, Y, Z]$. Effectuer la division de g par (f_1, f_2) avec l'ordre lexicographique. Même question avec l'ordre lexicographique gradué. Comparer les résultats obtenus.

Exercice 2 (Critère de base de Gröbner)**.** En utilisant le critère des S-polynômes, dire si les familles suivantes sont des bases de Gröbner de l'idéal qu'elles engendrent.

1) $(X + Z, Y - Z)$ pour l'ordre lexicographique ;
2) $(Y - X^2, Z - X^3)$ pour l'ordre lexicographique avec $X > Y > Z$; même question pour l'ordre lexicographique avec $Y > Z > X$.
3) $(X^3 - 2XY, X^2Y - 2Y^2 + X)$ pour l'ordre lexicographique gradué.

Exercice 3 (Critère d'appartenance à un idéal)**.** Soit I l'idéal $(X + Z, Y - Z)$ de $K[X, Y, Z]$.

1) Déterminer si le polynôme $X^2 + Y^2 + Z^2$ appartient à I.
2) Même question avec le polynôme $X^2 + 2XY - Y^2 + 2YZ$.

(On pourra utiliser le fait que $(X + Z, Y - Z)$ est une base de Gröbner de I pour l'ordre lexicographique, d'après l'exercice 2).

Exercice 4 (Construction d'un base de Gröbner)**.** En utilisant l'algorithme vu en cours, déterminer une base de Gröbner de l'idéal $I = (X^2Y - 1, X^2Y - X)$ de $K[X, Y]$ pour l'ordre lexicographique.

Solutions :
Exercice 1 : 1) Pour (f_1, f_2) : $g = Yf_1 + (-X - Y)$. Pour (f_2, f_1) : $g = Xf_2 + 0$. 2) Pour lex : $g = -f_1 + 0 \cdot f_2 + (Z^3 - 1)$. Pour grlex : $g = -f_1 - f_2 + (XY - 1)$.
Exercice 2 : 1) $S = XZ + YZ$ a un reste nul dans la division par $(X + Z, Y - Z)$ donc on a une base de Gröbner. 2) Pour lex avec $X > Y > Z$ on a $S = -XY + Z$; le reste dans sa division par $(Y - X^2, Z - X^3)$ est S, non nul, donc on n'a pas une base de Gröbner. Pour lex avec $Y > Z > X$, on a $S = -ZX^2 + YX^3$; le reste dans sa division par $(Y - X^2, Z - X^3)$ est nul donc on a une base de Gröbner. 3) On a $S = -X^2$; le reste dans sa division par $(X^3 - 2XY, X^2Y - 2Y^2 + X)$ est $-X^2$, non nul, donc on n'a pas une base de Gröbner.
Exercice 3 : 1) La division du polynôme f par $(g_1 = X+Z, g_2 = Y-Z)$ est $(X-Z)g_1 + (Y+Z)g_2 + 3Z^2$. Le reste est non nul donc le polynôme n'appartient pas à I. 2) La division du polynôme par (g_1, g_2) a un reste nul, le polynôme appartient à I.
Exercice 4 : Posons $g_1 = X^2Y - 1$, $g_2 = X^2Y - X$. On a $S(g_1, g_2) = X - 1$; son reste dans la division par (g_1, g_2) est $X - 1$, non nul. On pose $g_3 = X - 1$. On a $S(g_1, g_3) = XY - 1$, son reste dans la division par (g_1, g_2, g_3) est $Y - 1$, non nul. On pose $g_4 = Y - 1$. On calcule $S(g_1, g_2)$, $S(g_1, g_3)$, $S(g_1, g_4)$, $S(g_2, g_3)$, $S(g_2, g_4)$ et $S(g_3, g_4)$ et on vérifie que leurs restes dans la division par (g_1, g_2, g_3, g_4) sont tous nuls. Donc (g_1, g_2, g_3, g_4) est une base de Gröbner de I.

Quelques applications des bases de Gröbner à l'élimination

Résolution de systèmes polynomiaux. L'ensemble des solutions complexes du système

$$\begin{aligned} x^2 + y^2 + z^2 &= 1 \\ x^2 + z^2 &= y \\ x &= z \end{aligned}$$

correspond à $Z(I)$ où I est l'idéal de $\mathbb{C}[X, Y, Z]$ engendré par les polynômes $X^2 + Y^2 + Z^2 - 1, X^2 + Z^2 - Y, X - Z$. À l'aide d'un ordinateur on calcule une base de Gröbner de I pour l'ordre lexicographique $(X > Y > Z)$ et on obtient la famille

$$X^2 + Y^2 + Z^2 - 1, X^2 + Z^2 - Y, X - Z, Y^2 + Y - 1, Z^2 - \frac{1}{2}Y.$$

Le système est donc équivalent à

$$\begin{aligned} x^2 + y^2 + z^2 &= 1 \\ x^2 + z^2 &= y \\ x &= z \\ y^2 + y - 1 &= 0 \\ z^2 - \frac{1}{2}y &= 0. \end{aligned}$$

On remarque que l'avant-dernière équation ne dépend que de y (on a éliminé les autres variables) et ses racines sont $\frac{-1\pm\sqrt{5}}{2}$. En reportant dans la dernière équation, on trouve quatre valeurs possibles pour z. On explicite ainsi toutes les solutions (x, y, z) (il y en a quatre).

Mise sous forme implicite. Considérons la courbe paramétrée de $\mathbb{R}^3$ donnée par $x(t) = t^4$, $y(t) = t^3$, $z(t) = t^2$. Elle correspond à $V(I)$ où I est l'idéal $(X - T^4, Y - T^3, Z - T^2)$ de $\mathbb{R}[X, Y, Z, T]$ (à condition d'oublier la composante en t). À l'aide d'un ordinateur on calcule une base de Gröbner simplifiée de I pour l'ordre lexicographique avec $T > X > Y > Z$ et on obtient la famille

$$Z - T^2, TY - Z^2, TZ - Y, X - Z^2, Y^2 - Z^3.$$

Par ce procédé d'élimination, on a obtenu deux polynômes ne dépendant pas de T : $X - Z^2$ et $Y^2 - Z^3$. Cela montre que la courbe est contenue dans $Z(X - Z^2, Y^2 - Z^3)$ c'est-à-dire dans la courbe d'équation cartésienne $(x = z^2, y^2 = z^3)$. L'inclusion peut être stricte a priori.