

Les bases de Gröbner

Sommaire

1.	Les idéaux monomiaux	75
2.	Le théorème de la base de Hilbert	77
3.	Les bases de Gröbner	81
4.	Premières propriétés des bases de Gröbner	83

§ 1 Les idéaux monomiaux

V.1.1. Définition.— Un idéal I de $\mathbb{K}[x_1, \dots, x_n]$ est dit *monomial*, s'il existe une partie A de \mathbb{N}^n , éventuellement infinie, telle que I soit constitué de tous les polynômes s'exprimant comme somme finie de la forme

$$\sum_{\alpha \in A} h_{\alpha} x^{\alpha},$$

où les h_{α} sont des polynômes de $\mathbb{K}[x_1, \dots, x_n]$.

Autrement dit, un idéal I est monomial s'il est engendré par des monômes, *i.e.* s'il existe une partie A de \mathbb{N}^n , telle que

$$I = \langle x^{\alpha} \mid \alpha \in A \rangle.$$

V.1.2. Exemples.— L'idéal $I = \langle x^4 y^2, x^3 y^4, x^2 y^5 \rangle$ est un idéal monomial de $\mathbb{K}[x, y]$. L'idéal $I = \langle x - y \rangle$ n'est pas monomial.

V.1 Proposition. — Soit $I = \langle x^\alpha \mid \alpha \in A \rangle$ un idéal monomial. Un monôme x^β est dans I si, et seulement si, x^β est divisible par x^α , pour un $\alpha \in A$.

Preuve. Si x^β est divisible par un monôme x^α , $\alpha \in A$, alors, il existe un polynôme h de $\mathbb{K}[x_1, \dots, x_n]$, tel que $x^\beta = hx^\alpha$, d'où $x^\beta \in I$.

Supposons que x^β soit un monôme de I . Il existe alors une décomposition

$$x^\beta = h_{\alpha(1)}x^{\alpha(1)} + \dots + h_{\alpha(s)}x^{\alpha(s)},$$

où $h_{\alpha(i)} \in \mathbb{K}[x_1, \dots, x_n]$ et $\alpha(i) \in A$. En développant chaque polynôme $h_{\alpha(i)}$, le terme de droite se décompose en une combinaison linéaire de monômes, et chaque monôme est divisible par un $x^{\alpha(i)}$. Par suite, x^β est divisible par un $x^{\alpha(i)}$. \square

V.2 Proposition. — Soit I un idéal monomial et soit f un polynôme de $\mathbb{K}[x_1, \dots, x_n]$. Les assertions suivantes sont équivalentes

- i) $f \in I$,
- ii) tout terme de f est dans I ,
- iii) f est une combinaison linéaire de monômes de I .

Preuve. Supposons que $I = \langle x^\alpha \mid \alpha \in A \rangle$. Les implications **iii**) \Rightarrow **ii**) \Rightarrow **i**) sont immédiates. Si $f \in I$, alors

$$f = h_{\alpha(1)}x^{\alpha(1)} + \dots + h_{\alpha(s)}x^{\alpha(s)},$$

où les $h_{\alpha(i)} \in \mathbb{K}[x_1, \dots, x_n]$ et $\alpha(i) \in A$. En décomposant chaque polynôme $h_{\alpha(i)}$ en combinaison linéaire de monômes, on obtient **iii**). \square

On en déduit que deux idéaux monomiaux sont égaux, si et seulement si, ils contiennent les mêmes monômes.

V.1.3. Le lemme de Dickson.— Le résultat suivant est important dans la suite, car il nous permettra de montrer que tout idéal de $\mathbb{K}[x_1, \dots, x_n]$ possède une base finie.

V.3 Théorème (lemme de Dickson). — Soit $I = \langle x^\alpha \mid \alpha \in A \rangle$ un idéal monomial de $\mathbb{K}[x_1, \dots, x_n]$. Alors, il existe $\alpha(1), \dots, \alpha(s) \in A$ tels que

$$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle.$$

En d'autres termes, tout idéal monomial possède une base finie.

Exercice 1. — Montrer le lemme de Dickson V.3 pour les idéaux monomiaux de $\mathbb{K}[x]$.

Preuve. (Idée !) On procède par récurrence sur n . Pour le cas $n = 1$, voir l'exercice précédent. On suppose le théorème vrai au rang $n - 1$. On considère alors l'anneau des polynômes à n indéterminées, que l'on notera $\mathbb{K}[x_1, \dots, x_{n-1}, y]$. Les monômes en les indéterminées x_1, \dots, x_{n-1}, y , s'écrivent sous la forme $x^\alpha y^m$, avec $\alpha = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$ et $m \in \mathbb{N}$.

Supposons que I soit un idéal monomial de $\mathbb{K}[x_1, \dots, x_{n-1}, y]$. Considérons l'idéal J de $\mathbb{K}[x_1, \dots, x_{n-1}]$ engendré par les monômes x^α , pour lesquels $x^\alpha y^m \in I$, pour $m \geq 0$. Comme J est un idéal monomial de $\mathbb{K}[x_1, \dots, x_{n-1}]$, d'après l'hypothèse de récurrence, il existe $\alpha(1), \dots, \alpha(s) \in \mathbb{N}$, tels que

$$J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle.$$

Par construction de J , pour tout $i \in \llbracket 1, s \rrbracket$, il existe $m_i \in \mathbb{N}$ tel que $x^{\alpha(i)} y^{m_i} \in I$. Soit $m = \max\{m_i \mid i \in \llbracket 1, s \rrbracket\}$. Pour tout entier $k \in \llbracket 0, m-1 \rrbracket$, on définit l'idéal J_k de $\mathbb{K}[x_1, \dots, x_{n-1}]$ engendré par les monômes x^β , tels que $x^\beta y^k \in I$. D'après l'hypothèse de récurrence, J_k admet une base finie :

$$J_k = \langle x^{\alpha_k(1)}, \dots, x^{\alpha_k(s_k)} \rangle.$$

On montre alors (exercice !) que l'idéal I est engendré par les monômes suivants

$$\begin{aligned} x^{\alpha(1)} y^m, \dots, x^{\alpha(s)} y^m &\in J \\ x^{\alpha_0(1)}, \dots, x^{\alpha_0(s_0)} &\in J_0 \\ x^{\alpha_1(1)} y, \dots, x^{\alpha_1(s_1)} y &\in J_1 \\ &\vdots \\ x^{\alpha_{m-1}(1)} y^{m-1}, \dots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1} &\in J_{m-1} \end{aligned}$$

Reste à montrer que cet ensemble fini de générateurs peut être choisi à partir d'un ensemble de générateurs de l'idéal. Ceci est une conséquence de la proposition V.1 (exercice !). \square

§ 2 Le théorème de la base de Hilbert

V.2.1. L'idéal des termes dominants.— Soit I un idéal non nul de $\mathbb{K}[x_1, \dots, x_n]$. On note $\text{lt}(I)$ l'ensemble des termes dominants des éléments de I :

$$\text{lt}(I) = \{\text{lt}(f) \mid f \in I\}.$$

On note $\langle \text{lt}(I) \rangle$ l'idéal engendré par les éléments de $\text{lt}(I)$, on l'appelle l'*idéal des termes dominants* de I .

V.2.2. Remarque.— Supposons que $I = \langle f_1, \dots, f_s \rangle$, pour tout $i \in \llbracket 1, s \rrbracket$, on a

$$\text{lt}(f_i) \in \text{lt}(I) \subset \langle \text{lt}(I) \rangle,$$

par suite

$$\langle \text{lt}(f_1), \dots, \text{lt}(f_s) \rangle \subset \langle \text{lt}(I) \rangle.$$

Il est cependant possible que cette inclusion soit stricte, comme l'illustre l'exemple suivant.

V.2.3. Exemple.— On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$, avec $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$. Considérons le polynôme $f = xy^2 - x$, on a

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y),$$

et

$$xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0.$$

La seconde équation montre que $f \in I$ et d'après la première équation, on a

$$-x - y = f - yf_1 \in I.$$

Ainsi $x + y \in I$ et $\text{lt}(x + y) = x \in \langle \text{lt}(I) \rangle$. Or

$$x \notin \langle \text{lt}(f_1), \text{lt}(f_2) \rangle = \langle xy, y^2 \rangle,$$

car x n'est pas divisible par xy ou y^2 . L'inclusion

$$\langle \text{lt}(f_1), \text{lt}(f_2) \rangle \subset \langle \text{lt}(I) \rangle,$$

est ainsi stricte.

V.4 Proposition.— Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$. Alors

- i) l'idéal $\langle \text{lt}(I) \rangle$ est monomial,
- ii) il existe des polynômes $g_1, \dots, g_t \in I$, tels que $\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle$.

Preuve. Montrons **i)**. Considérons l'idéal engendré par les monômes dominants des polynômes non nul de I ,

$$\langle \text{lm}(g) \mid g \in I - \{0\} \rangle.$$

On a $\text{lt}(g) = \text{lc}(g)\text{lm}(g)$, ainsi $\text{lm}(g)$ et $\text{lt}(g)$ ne diffèrent que d'un facteur multiplicatif près de \mathbb{K} , par suite

$$\langle \text{lm}(g) \mid g \in I - \{0\} \rangle = \langle \text{lt}(g) \mid g \in I - \{0\} \rangle,$$

Or $\langle \text{lt}(I) \rangle = \langle \text{lt}(g) \mid g \in I - \{0\} \rangle$, d'où

$$\langle \text{lt}(I) \rangle = \langle \text{lm}(g) \mid g \in I - \{0\} \rangle$$

et $\langle \text{lt}(I) \rangle$ est un idéal monomial.

Montrons **ii**). Comme $\langle \text{lt}(I) \rangle = \langle \text{lm}(g) \mid g \in I - \{0\} \rangle$, d'après le lemme de Dickson, théorème V.3, il existe des polynômes g_1, \dots, g_t tels que

$$\langle \text{lt}(I) \rangle = \langle \text{lm}(g_1), \dots, \text{lm}(g_t) \rangle$$

comme, pour tout i , $\text{lm}(g_i)$ et $\text{lt}(g_i)$ ne diffèrent que d'un facteur multiplicatif près de \mathbb{K} , par suite

$$\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle.$$

□

Exercice 2. — Soit I l'idéal de $\mathbb{R}[x, y, z]$ engendré par les trois polynômes

$$g_1 = xy^2 - xz + y, \quad g_2 = xy - z^2, \quad g_3 = x - yz^4.$$

En utilisant l'ordre lexicographique, donner un polynôme g de I tel que

$$\text{lt}(g) \notin \langle \text{lt}(g_1), \text{lt}(g_2), \text{lt}(g_3) \rangle.$$

Exercice 3. — On considère les idéaux étudiés dans les exercices 16 et 17 du chapitre précédent :

1. $I = \langle f_1, f_2 \rangle \subset \mathbb{R}[x, y, z]$ avec $f_1 = x^2y - z$ et $f_2 = xy - 1$.
2. $I = \langle f_1, f_2 \rangle \subset \mathbb{R}[x, y]$ avec $f_1 = 2xy^2 - x$, $f_2 = 3x^2y - y - 1$.
3. $I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{R}[x, y, z]$ avec $f_1 = x^4y^2 - z$, $f_2 = x^3y^2 - z$, $f_3 = x^3y^3 - 1$, $f_4 = x^2y^4 - 2z$.

En utilisant l'ordre lexicographique gradué, dans chaque cas, montrer que l'idéal $\langle \text{lt}(I) \rangle$ est strictement plus grand que l'idéal engendré par les termes $\text{lt}(f_i)$.

V.2.4. Le théorème de la base de Hilbert.— De la proposition V.4 et de l'algorithme de division, nous montrons que tout idéal de $\mathbb{K}[x_1, \dots, x_n]$ est engendré par un nombre fini de polynômes.

V.5 Théorème (Théorème de la base de Hilbert).— Tout idéal I de $\mathbb{K}[x_1, \dots, x_n]$ possède un nombre fini de générateurs, *i.e.*, il existe des polynômes g_1, \dots, g_t de I , tels que $I = \langle g_1, \dots, g_t \rangle$.

Autrement dit, tout idéal de $\mathbb{K}[x_1, \dots, x_n]$ possède une base finie.

Preuve. Fixons un ordre monomial sur $\mathcal{M}(x_1, \dots, x_n)$. Si I est l'idéal nul, on peut prendre 0 comme générateur : $I = \{0\} = \langle 0 \rangle$. Supposons I non nul, alors il contient au moins un

polynôme non nul. D'après la proposition V.4 ii), il existe des polynômes g_1, \dots, g_t de I tels que

$$\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle.$$

Montrons que $I = \langle g_1, \dots, g_t \rangle$. Comme $g_1, \dots, g_t \in I$, l'inclusion $\langle g_1, \dots, g_t \rangle \subset I$ est immédiate. Inversement, soit f un polynôme de I . Faisons la division de f par les polynômes g_1, \dots, g_t , il en résulte une décomposition

$$f = u_1 g_1 + \dots + u_t g_t + r,$$

où u_1, \dots, u_t, r sont des polynômes de $\mathbb{K}[x_1, \dots, x_n]$, tels que $r = 0$ ou r est une somme de termes non divisibles par $\text{lt}(g_1), \dots, \text{lt}(g_t)$. Montrons que $r = 0$. On a

$$r = f - u_1 g_1 - \dots - u_t g_t \in I.$$

Si $r \neq 0$, alors

$$\text{lt}(r) \in \langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle.$$

D'après la proposition V.1, $\text{lt}(r)$ est alors divisible par un $\text{lt}(g_i)$, ce qui contredit la propriété de r . Par suite, $r = 0$ et on a

$$f = u_1 g_1 + \dots + u_t g_t \in \langle g_1, \dots, g_t \rangle.$$

Ainsi $I \subset \langle g_1, \dots, g_t \rangle$, qui termine la preuve. \square

V.2.5. Suites croissantes d'idéaux.— Voici une première application du théorème de la base de Hilbert.

V.6 Théorème (Propriété des suites croissantes d'idéaux).— Si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_k \subseteq \dots$$

est une suite croissante d'idéaux de $\mathbb{K}[x_1, \dots, x_n]$, alors il existe un rang $N \geq 1$ tel que

$$I_N = I_{N+1} = I_{N+2} = \dots$$

Exercice 4 (preuve du théorème V.6).— Considérons une suite croissante d'idéaux de $\mathbb{K}[x_1, \dots, x_n]$:

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

1. Montrer que $I = \bigcup_{i=1}^{\infty} I_i$ est un idéal de $\mathbb{K}[x_1, \dots, x_n]$.
2. En déduire le théorème V.6.

V.2.6. Ensemble algébrique affine d'un idéal.— Voici une autre application, de nature géométrique, du théorème de la base de Hilbert.

Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$. On note $\mathbf{V}(I)$ le sous-ensemble de \mathbb{K}^n défini par

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in \mathbb{K}^n \mid f(a_1, \dots, a_n) = 0, \text{ pour tout } f \in I\}.$$

Du théorème de la base de Hilbert, on déduit

V.7 Proposition. — Pour tout idéal I de $\mathbb{K}[x_1, \dots, x_n]$, $\mathbf{V}(I)$ est un ensemble algébrique affine. En particulier, si $I = \langle f_1, \dots, f_s \rangle$, alors $\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_s)$.

Exercice 5. — Montrer la proposition V.7.

§ 3 Les bases de Gröbner

La base $\{g_1, \dots, g_t\}$ obtenue dans le théorème de la base de Hilbert, théorème V.5 vérifie $\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle$. Comme nous avons vu avec l'exemple V.2.3, toutes les bases ne satisfont pas à cette propriété.

V.3.1. Définition. — Un ordre monomial étant fixé, un sous-ensemble fini $G = \{g_1, \dots, g_t\}$ d'un idéal I est appelé *base de Gröbner* (ou *base standard*) si

$$\langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle = \langle \text{lt}(I) \rangle.$$

Exercice 6. — Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$. Montrer qu'un sous-ensemble $G = \{g_1, \dots, g_t\}$ de I est une base de Gröbner de I si, et seulement si, le terme dominant de tout élément de I est divisible par un des $\text{lt}(g_i)$.

V.3.2. Exemple. — On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$ avec l'ordre alphabétique $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$. On a vu dans l'exemple V.2.3 que l'inclusion

$$\langle \text{lt}(f_1), \text{lt}(f_2) \rangle \subset \langle \text{lt}(I) \rangle,$$

est stricte, par suite $\{f_1, f_2\}$ n'est pas une base de Gröbner de I .

V.3.3. Exemple. — On fixe l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$ avec l'ordre alphabétique $y < x$. Soient $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y + 1$. Montrons que $\{f_1, f_2\}$ n'est pas une base de Gröbner de I . Le polynôme $f = xy^2 - 1$ a deux décompositions

$$\begin{aligned} f &= 0(xy + 1) + (xy - x)(y + 1) + (x - 1) \\ f &= (y)(xy + 1) + (-1)(y + 1) + 0. \end{aligned}$$

D'après la deuxième équation, $f \in I$, d'où d'après la première équation $x - 1 \in I$ et $x = \text{lt}(x - 1) \in \text{lt}(I)$. Or $x \notin \langle xy, y \rangle$, car ni xy , ni y ne divisent x . On en déduit que l'inclusion

$$\langle \text{lt}(f_1), \text{lt}(f_2) \rangle \subset \langle \text{lt}(I) \rangle,$$

est stricte, $\{f_1, f_2\}$ n'est donc pas une base de Gröbner de I .

V.3.4. Exemple.— Considérons les polynômes $g_1 = z + x$ et $g_2 = y - x$ de $\mathbb{Q}[x, y, z]$. On utilise l'ordre lexicographique sur $\mathbb{Q}[x, y, z]$ avec $x < y < z$. Montrons que $G = \{g_1, g_2\}$ est une base de Gröbner de l'idéal $I = \langle g_1, g_2 \rangle$. Supposons le contraire, c'est-à-dire qu'il existe $f \in I$, tel que

$$\text{lt}(f) \notin \langle \text{lt}(g_1), \text{lt}(g_2) \rangle = \langle z, y \rangle.$$

Alors z ne divise pas $\text{lt}(f)$ et y ne divise pas $\text{lt}(f)$. En raison de l'ordre lexicographique, z et y n'apparaissent pas non plus dans les autres termes de f . Par suite, f est un polynôme en la seule indéterminée x . Par ailleurs, on a

$$f = h_1(z + x) + h_2(y - x),$$

avec $h_1, h_2 \in \mathbb{Q}[x, y, z]$. On a alors pour tous $a, c \in \mathbb{Q}$,

$$f(a, a, c) = h_1(a, a, c)(a + c).$$

Comme \mathbb{Q} est infini et y n'apparaît pas dans les termes de f , on en déduit que $f = h_1(x, x, z)(x + z)$. Par suite $z + x$ divise f , qui est contradictoire avec le fait que f est d'une seule indéterminée x . Ainsi, G est une base de Gröbner de I .

V.3.5. Exemple.— Considérons les polynômes $g_1 = x - y^2w$, $g_2 = y - zw$, $g_3 = z - w^3$ et $g_4 = w^3 - w$ de $\mathbb{Q}[x, y, z, w]$. On considère l'ordre lexicographique avec l'ordre alphabétique $w < z < y < x$. Montrons que $G = \{g_1, g_2, g_3, g_4\}$ est une base de Gröbner de l'idéal $I = \langle g_1, g_2, g_3, g_4 \rangle$. On procède comme dans l'exemple précédent. Supposons le contraire, soit qu'il existe un polynôme $f \in I$ tel que

$$\text{lt}(f) \notin \langle \text{lt}(g_1), \text{lt}(g_2), \text{lt}(g_3), \text{lt}(g_4) \rangle = \langle x, y, z, w^3 \rangle.$$

Par suite, f est un polynôme d'une seule indéterminée w tel que $\text{lt}(f)$ n'est pas divisible par w^3 . Comme $f \in I$, on a une décomposition

$$f = h_1(x - y^2w) + h_2(y - zw) + h_3(z - w^3) + h_4(w^3 - w).$$

Alors pour tout $a \in \mathbb{Q}$, on a

$$f(a^9, a^4, a^3, a) = h_4(a^9, a^4, a^3, a)(a^3 - a).$$

Comme x , y et z n'apparaissent pas dans f et comme \mathbb{Q} est infini, on obtient $f = h_4(w^9, w^4, w^3, w)(w^3 - w)$. Par suite, $w^3 - w$ divise f , ce qui est contradictoire avec le fait que w^3 ne divise pas $\text{lt}(f)$. Ainsi G est une base de Gröbner de I .

V.8 Proposition. — Un ordre monomial étant fixé, tout idéal non nul de $\mathbb{K}[x_1, \dots, x_n]$ possède une base de Gröbner. De plus, toute base de Gröbner d'un idéal forme une base de cet idéal.

Preuve. Soit I un idéal non nul de $\mathbb{K}[x_1, \dots, x_n]$. Soit $G = \{g_1, \dots, g_t\}$ un ensemble de polynômes comme construit dans la preuve du théorème de la base de Hilbert, théorème V.5. Par construction, c'est une base de Gröbner.

Pour la seconde assertion, si g_1, \dots, g_s sont des polynômes de I vérifiant $\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle$, toujours d'après la preuve du théorème V.5, $I = \langle g_1, \dots, g_t \rangle$. C'est donc une base de I . \square

Exercice 7. — D'après la proposition V.8, si $G = \{g_1, \dots, g_t\}$ est un sous-ensemble d'un idéal I vérifiant $\langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle$, alors $I = \langle g_1, \dots, g_t \rangle$. L'objectif de cet exercice est de construire une autre preuve de ce résultat.

1. Supposons que $f \in I$. Montrer qu'à chaque étape de la division de f par $\{g_1, \dots, g_t\}$, le terme dominant du « polynôme sous le radical » est dans $\langle \text{lt}(I) \rangle$.
2. En déduire que si l'algorithme de division termine, alors $f \in \langle g_1, \dots, g_t \rangle$.
3. Conclure.

Exercice 8. — On utilise l'ordre lexicographique gradué avec l'ordre alphabétique $z < y < x$. Soit $I = \langle f_1, f_2, f_3 \rangle$ l'idéal de $\mathbb{R}[x, y, z]$ engendré par les polynômes

$$f_1 = x^4y^2 - z^5, \quad f_2 = x^3y^3 - 1, \quad f_3 = x^2y^4 - 2z.$$

L'ensemble $\{f_1, f_2, f_3\}$ forme-t-il une base de Gröbner pour I ?

Exercice 9. — On utilise l'ordre lexicographique avec l'ordre alphabétique $z < y < x$. Soit $I = \langle f_1, f_2 \rangle$ l'idéal de $\mathbb{R}[x, y, z]$ engendré par les polynômes

$$f_1 = x - z^2, \quad f_2 = y - z^3.$$

L'ensemble $\{f_1, f_2\}$ forme-t-il une base de Gröbner pour I ?

§ 4 Premières propriétés des bases de Gröbner

V.9 Proposition. — Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$ et soit $G = \{g_1, \dots, g_t\}$ une base de Gröbner de I . Soit f un polynôme de $\mathbb{K}[x_1, \dots, x_n]$. Il existe un unique $r \in \mathbb{K}[x_1, \dots, x_n]$ qui satisfait aux deux assertions suivantes :

- i) les termes de r ne sont pas divisibles par $\text{lt}(g_1), \dots, \text{lt}(g_t)$.

ii) il existe $g \in I$, tel que $f = g + r$.

En particulier, r est le reste de la division de f par G , peu importe l'ordre utilisé sur les éléments de G pendant la division.

Preuve. Divisons le polynôme f par $\{g_1, \dots, g_t\}$, d'après le théorème IV.11, il existe des polynômes u_1, \dots, u_t et r , tels que

$$f = u_1 g_1 + \dots + u_t g_t + r,$$

où r satisfait à l'assertion i). En posant, $g = u_1 g_1 + \dots + u_t g_t$, le polynôme r satisfait aussi à l'assertion ii).

Montrons l'unicité de r . Supposons qu'il existe r et r' satisfaisant les deux assertions :

$$f = g + r = g' + r'.$$

Alors

$$r - r' = g' - g \in I.$$

Ainsi, si $r \neq r'$, on a

$$\text{lt}(r - r') \in \langle \text{lt}(I) \rangle = \langle \text{lt}(g_1), \dots, \text{lt}(g_s) \rangle.$$

Par suite, $\text{lt}(r - r')$ est divisible par un $\text{lt}(g_i)$. Or, ceci est impossible puisque aucun terme de r et r' n'est divisible par $\text{lt}(g_1), \dots, \text{lt}(g_t)$. Par suite, $r - r'$ doit être nul, ce qui montre l'unicité.

La dernière assertion de la proposition est une conséquence de l'unicité du reste. \square

Attention, même si le reste est unique, les quotients u_1, \dots, u_s peuvent être différents d'une décomposition à l'autre.

V.4.1. Forme normale.— Le reste défini par la proposition V.9 est appelé la *forme normale* du polynôme f par la division par G . On note

$$f \xrightarrow{G} r.$$

V.10 Proposition. — Soit I un idéal de $\mathbb{K}[x_1, \dots, x_n]$ et soit $G = \{f_1, \dots, f_t\}$ une base de Gröbner de I . Un polynôme f de $\mathbb{K}[x_1, \dots, x_n]$ est un élément de I , si et seulement si, le reste de la division de f par G est égal à 0.

Autrement dit,

$$f \in I, \quad \text{si, et seulement si,} \quad f \xrightarrow{G} 0.$$

Preuve. Si le reste est nul, alors $f \in I$. Inversement, étant donné $f \in I$, alors, on a une décomposition $f = f + 0$ satisfaisant les deux assertions de proposition V.9. Par suite, 0 est le reste de la division de f par G . \square