CHAPITRE
IV

Les bases de Gröbner

Sommaire

Dans ce chapitre, on considère un anneau de polynômes $\mathbb{K}[x_1,\dots,x_n]$ et on munit $\mathscr{M}[x_1,\dots,x_n]$ d'un ordre monomial.

§ 1 Les idéaux monomiaux

IV.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

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

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

IV.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 $x^{\alpha(i)}$. □

IV.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)** ⇒ **ii)** ⇒ **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)**. □

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

IV.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.

IV.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

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

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

Exercice 81. — Montrer le lemme de Dickson IV.3 pour les idéaux monomiaux de $\mathbb{K}[x]$.

Preuve. **(Idée !)** On procède par récurrence sur n. Pour le cas $n=1$, voir III.3.1. 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 il existe m (dépendant de α) tel que $x^\alpha y^m\in I$.

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

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

Par construction de J, pour tout $i\in[\![1,s]\!]$, il existe $m_i\in\mathbb{N}$ tel que $x^{\alpha(i)}y^{m_i}\in I$. Soit $m=\max\{m_i \mid i\in[\![1,s]\!]\}$. Pour tout entier $k\in[\![0,m-1]\!]$, 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 :

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

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

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

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 IV.1 (exercice !). □

§ 2 Le théorème de la base de Hilbert

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

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

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

IV.2.2. Remarque.— Supposons que $I=\langle f_1,\dots,f_s\rangle$, pour tout $i\in[\![1,s]\!]$, on a

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

par suite

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

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

IV.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 $\mathrm{lt}(x+y)=x\in\langle\mathrm{lt}(I)\rangle$. Or

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

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

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

est ainsi stricte.

IV.4 Proposition. — Soit I un idéal de $\mathbb{K}[x_1,\dots,x_n]$ différent de l'idéal $\{0\}$. Alors

i) l'idéal $\langle\mathrm{lt}(I)\rangle$ est monomial,

ii) il existe des polynômes $g_1,\dots,g_t\in I$, tels que $\langle\mathrm{lt}(I)\rangle=\langle\mathrm{lt}(g_1),\dots,\mathrm{lt}(g_t)\rangle$.

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

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

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

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

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

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

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

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

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

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

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

□

Exercice 82. — 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

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

Exercice 83. — On considère les idéaux étudiés dans les exercices 76 et 77 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 $\langle \mathrm{lt}(I) \rangle$ est strictement plus grand que l'idéal engendré par les termes $\mathrm{lt}(f_i)$.

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

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

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

Preuve. Fixons un ordre monomial sur $\mathscr{M}(x_1, \ldots, x_n)$. 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 IV.4 **ii)**, il existe des polynômes $g_1, \ldots, g_t$ de I tels que

$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle .$$

Montrons que $I = \langle g_1, \ldots, g_t \rangle$. Comme $g_1, \ldots, g_t \in I$, l'inclusion $\langle g_1, \ldots, g_t \rangle \subset I$ est immédiate. Inversement, soit f un polynôme de I et $G = \{g_1, \ldots, g_t\}$. L'algorithme de division par $g_1, \ldots, g_t$ donne une réduction $f \xrightarrow{G} r$ de f modulo G sous forme normale, c'est-à-dire une décomposition

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

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

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

Si $r \neq 0$, alors

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

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

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

Ainsi $I \subset \langle g_1, \ldots, g_t \rangle$, qui termine la preuve. □

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

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

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_k \subseteq \ldots$$

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

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

Exercice 84 (preuve du théorème IV.6). — Considérons une suite croissante d'idéaux de $\mathbb{K}[x_1, \ldots, x_n]$:

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

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

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

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

Du théorème de la base de Hilbert, on déduit

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

Exercice 85. — Montrer la proposition IV.7.

§ 3 Les bases de Gröbner

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

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

$$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle = \langle \mathrm{lt}(I) \rangle .$$

IV.3.2. Remarque.— Un sous-ensemble fini $G = \{g_1, \ldots, g_t\}$ d'un idéal I est une base de Gröbner si, et seulement si, le terme dominant de tout élément de I est divisible par un des $\mathrm{lt}(g_i)$.

Exercice 86. — Vérifier la remarque IV.3.2.

IV.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 $f_2 = y^2 - 1$. On a vu dans l'exemple IV.2.3 que l'inclusion

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

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

IV.3.4. 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

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

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

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

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

IV.3.5. 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

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

Alors z ne divise pas $\mathrm{lt}(f)$ et y ne divise pas $\mathrm{lt}(f)$. 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.

IV.3.6. 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

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

Par suite, f est un polynôme d'une seule indéterminée w tel que $\mathrm{lt}(f)$ 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 par $\mathrm{lt}(f)$. Ainsi G est une base de Gröbner de I.

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

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

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

Exercice 87. — 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 88. — 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

IV.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) aucun des termes de r n'est divisible par l'un des $\mathrm{lt}(g_1),\dots,\mathrm{lt}(g_t)$,

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. De plus, le polynôme r est l'unique réduction sous forme normale du polynôme f modulo G, on l'appelle également *la forme normale* de f modulo G.

Preuve. Le théorème III.11, qui s'obtient par division de f par $g_1,...,g_t$, montre l'existence d'un tel polynôme r sous forme normale par rapport à G.

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

$$\mathrm{lt}\left(r-r'\right)\in\langle\mathrm{lt}(I)\rangle=\langle\mathrm{lt}(g_1),\dots,\mathrm{lt}(g_t)\rangle.$$

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

Les deux dernières assertions de la proposition sont une conséquence de l'unicité de r. □

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

Il suit de la proposition précédente que la donnée d'une base de Gröbner permet de répondre au problème de l'appartenance à un idéal.

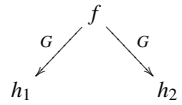
IV.10 Proposition. — Soient un idéal I de $\mathbb{K}[x_1,\dots,x_n]$ et une base $G=\{g_1,\dots,g_t\}$ de I. Si G est une base de Gröbner de I, alors pour tout polynôme f de $\mathbb{K}[x_1,\dots,x_n]$ on a

$$f\in I,\quad\text{si, et seulement si,}\quad f\xrightarrow{g_1,\dots,g_t}0\quad\text{si, et seulement si,}\quad f\xrightarrow{G}0.$$

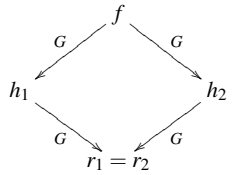
On verra dans le chapitre suivant que c'est en fait une caractérisation des bases de Gröbner. On verra également que G est une base de Gröbner, si, et seulement si, la relation de réduction modulo G est confluente. On peut déjà vérifier l'implication pour cette dernière assertion.

IV.4.1. Remarque.— Si $G=\{g_1,\dots,g_t\}$ est une base de Gröbner de l'idéal $\langle g_1,\dots,g_t\rangle$, alors la relation $\xrightarrow{G}$ est confluente.

Considérons une paire de réductions sur un même polynôme f modulo G



Soit r_1 et r_2 les formes normales de h_1 et h_2, respectivement, modulo G. Mais alors $f\xrightarrow{G}r_1$ et $f\xrightarrow{G}r_2$, donc $r_1=r_2$ est également la forme normale de f modulo G.



Exercice 89. — Soit I un idéal de $\mathbb{K}[x_1,\dots,x_n]$ et G une base de Gröbner de I. On note $\widehat{f}^G$, le reste de la division de f par G (ou forme normale de f modulo G).

1. Montrer que $\widehat{f}^G=\widehat{g}^G$ si, et seulement si, $f-g\in I$.

2. Montrer que

$$\widehat{f+g}^G=\widehat{f}^G+\widehat{g}^G.$$

3. Montrer que

$$\widehat{fg}^G=\widehat{\widehat{f}^G\,\widehat{g}^G}^G.$$

Exercice 90. — Soient G et G' deux bases de Gröbner d'un idéal I de $\mathbb{K}[x_1,\dots,x_n]$, relativement à un même ordre monomial. Montrer que pour tout polynôme f de $\mathbb{K}[x_1,\dots,x_n]$, si $f\xrightarrow{G}r$ et $f\xrightarrow{G'}r'$, où r et r' sont en forme normale respectivement pour G et G', alors $r=r'$.