CHAPITRE
VI

Premières applications des bases de Gröbner

Sommaire

1. **Description d'un idéal et appartenance à un idéal** 85
2. **Résolution d'équations polynomiales** 87
3. **Une méthode d'élimination** 89
4. **Problème d'impliciter une présentation paramétrée** 91

Les bases de Gröbner permettent de résoudre algorithmiquement de nombreux problèmes portant sur les idéaux d'anneaux de polynômes. Voici les principaux problèmes que l'on peut aborder en utilisant les bases de Gröbner et que nous allons présenter dans ce chapitre :

i) problème de l'appartenance à un idéal,

ii) problème de la résolution d'équations polynomiales,

iii) problème d'impliciter une présentation paramétrée.

§ 1 Description d'un idéal et appartenance à un idéal

VI.1.1. Problème de la description d'un idéal.—

- Est-ce que tout idéal I de $\mathbb{K}[x_1,\ldots,x_n]$ possède un nombre fini de générateurs ? Autrement dit, existe-t-il une famille de polynômes $f_1,\ldots,f_s$ tels que $I=\langle f_1,\ldots,f_s\rangle$?
- Existe-t-il une famille génératrice « plus intéressante » que les autres ?

Une réponse à la première question est donnée par le théorème de la base de Hilbert, théorème IV.5. Dans ce chapitre, nous allons voir que pour certains problèmes des familles de générateurs sont plus intéressantes que d'autres.

VI.1.2. Problème de l'appartenance à un idéal.—

Étant donné un idéal $I = \langle f_1, \ldots, f_s \rangle$ et un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$, déterminer si $f \in I$.

L'algorithme de division appliquée avec une base de Gröbner permet de résoudre le problème de l'appartenance à un idéal ; on procède en deux étapes :

— la première étape consiste à calculer une base de Gröbner $G = \{g_1, \ldots, g_t\}$ de I avec l'algorithme de Buchberger, théorème V.5 (après avoir choisi un ordre monomial) ;

— la deuxième étape calcule la division de f par G. D'après la proposition IV.10, un polynôme f de $\mathbb{K}[x_1, \ldots, x_n]$ est un élément de I, si, et seulement si, le reste de la division de f par G est égal à 0 :

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

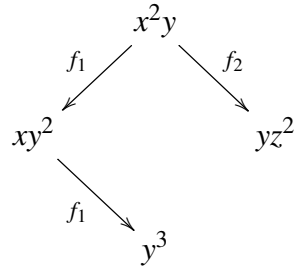
VI.1.3. Exemple.— Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{Q}[x, y, z]$, avec

$$f_1 = xy - y^2, \qquad f_2 = x^2 - z^2.$$

Soit $f = 2x^3y - xyz^2 - y^2z^2$, a-t-on $f \in I$? Considérons l'ordre lexicographique gradué, avec $z < y < x$, on a les réductions

$$xy \xrightarrow{f_1} y^2, \qquad x^2 \xrightarrow{f_2} z^2.$$

L'ensemble $\{f_1, f_2\}$ n'est pas une base de Gröbner de I, car la paire critique



n'est pas confluente. Pour obtenir une base de Gröbner, il suffit de compléter cette paire critique, car il n'apparaît pas d'autre paire critique non confluente. L'ensemble $G = \{f_1, f_2, f_3\}$, avec $f_3 = y^3 - yz^2$, est une base de Gröbner de I.

Pour tester l'appartenance de f à I, il suffit alors de diviser f par G, on a

$$f = 2xyf_1 + z^2 f_2.$$

Le reste de cette division est nul, ainsi $f \in I$. Cela revient à réduire le polynôme f par f_1 et f_2 et tester si la forme normale obtenue est nulle :

$$2x^3y - xyz^2 - y^2z^2 \xrightarrow{f_1} 2x^2y^2 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2xy^3 - xyz^2 - y^2z^2$$

$$\xrightarrow{f_1} 2y^4 - xyz^2 - y^2z^2 \xrightarrow{f_1} 2y^4 - y^2z^2 - y^2z^2 \xrightarrow{f_3} 2y^2z^2 - 2y^2z^2 = 0.$$

L'ordre d'application des réductions n'a pas d'influence sur le résultat, car G étant une base de Gröbner, le système est confluent.

Ainsi, tout polynôme f tel que $\mathrm{lt}(f)$ n'est pas dans l'idéal $\langle \mathrm{lt}(G) \rangle = \langle xy, x^2, y^3 \rangle$ n'est pas dans I. Par exemple, le polynôme $f = zy - y^2$ n'est pas dans I, car il est en forme normale par réduction par G.

On peut utiliser Sage pour calculer la base de Gröbner G :

```
sage: A.<x,y,z> = PolynomialRing(QQ, 'x,y,z', order='deglex')
sage: f1 = x*y-y^2
sage: f2 = x^2-z^2
sage: I = (f1, f2)*A
sage: G = I.groebner_basis()
sage: print G
        [y^3 - y*z^2, x^2 - z^2, x*y - y^2]
```

§ 2 Résolution d'équations polynomiales

VI.2.1. Problème de la résolution d'équations polynomiales.—

Étant donnés des polynômes $f_1,\dots,f_s$ de $\mathbb{K}[x_1,\dots,x_n]$, trouver les solutions dans $\mathbb{K}^n$ du système d'équations polynomiales

$$\left|\begin{array}{l} f_1(x_1,\dots,x_n)=0 \\ \qquad\vdots \\ f_s(x_1,\dots,x_n)=0 \end{array}\right.$$

D'après la proposition IV.7, pour tout idéal I de $\mathbb{K}[x_1,\dots,x_n]$,

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

est un ensemble algébrique affine. Si l'idéal I est défini par $I=\langle f_1,\dots,f_s\rangle$, alors $\mathbf{V}(I)=\mathbf{V}(f_1,\dots,f_s)$. On peut ainsi décrire $\mathbf{V}(I)$ à partir de toute base de I, en particulier avec une base de Gröbner calculée avec l'ordre lexicographique.

VI.2.2. Exemple.— On considère le système d'équations

$$\left|\begin{array}{rl} x^2+y^2+z^2 &= 1 \\ x^2+z^2 &= y \\ x &= z \end{array}\right.$$

dans $\mathbb{C}^3$. Ces équations déterminent l'idéal

$$I=\left\langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\right\rangle.$$

L'objectif est de décrire l'ensemble algébrique affine $\mathbf{V}(I)$. On calcule une base de Gröbner $G=\{g_1,g_2,g_3\}$ de l'idéal I en utilisant l'ordre lexicographique induit par l'ordre alphabétique $z<y<x$:

$$g_1=x-z,\quad g_2=-y+2z^2,\quad g_3=z^4+\frac{1}{2}z^2-\frac{1}{4}.$$

On a $\mathbf{V}(I)=\mathbf{V}(g_1,g_2,g_3)$. L'équation $g_3=0$ est de degré 4 en z, ses racines sont

$$z=\pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}.$$

Des équations $g_1=0$ et $g_2=0$, on déduit alors les valeurs de x et de y.

VI.2.3. Exemple : méthode des extrema liés de Lagrange sous une contrainte.— La méthode des extrema liés de Lagrange consiste à trouver les points extrema locaux d'une fonction $p \longmapsto f(p)$ de classe C^1 sur un ouvert U de $\mathbb{R}^n$, lorsque le point p est asujetti aux contraintes exprimées sous la forme

$$h_1(p) = 0\,, \quad \ldots \quad , h_k(p) = 0.$$

Considérons le cas d'une seule contrainte $h(p) = 0$, où h est une fonction de classe C^1 définie sur l'ouvert U et telle que le gradient $\mathrm{grad}_p(h)$ de h au point p est non nul si $h(p) = 0$.

La méthode de Lagrange montre que la fonction f présente un extremum local en un point p, si les vecteurs gradients $\mathrm{grad}_p(f)$ et $\mathrm{grad}_p(h)$ son colinéaires. C'est-à-dire s'il existe un réel λ tel que

$$\mathrm{grad}_p(f) = \lambda \mathrm{grad}_p(h). \tag{VI.1}$$

Rappelons que le gradient de f est le vecteur défini par

$$\mathrm{grad}(f) = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \right).$$

Les extrema p satisfont ainsi le système d'équations

$$\left| \begin{array}{rl} \frac{\partial f}{\partial x}(p) & = \lambda \frac{\partial h}{\partial x}(p) \\ \frac{\partial f}{\partial y}(p) & = \lambda \frac{\partial h}{\partial y}(p) \\ \frac{\partial f}{\partial z}(p) & = \lambda \frac{\partial h}{\partial z}(p) \\ h(p) & = 0 \end{array} \right.$$

Par exemple, on cherche les extrema de la fonction

$$f(x,y,z) = x^3 + 2xyz - z^2.$$

soumis à la contrainte $h(x,y,z) = x^2 + y^2 + z^2 - 1 = 0$. L'équation (VI.1) avec la contrainte $h(x,y,z) = 0$ donne ainsi un système de quatre équations

$$\left| \begin{array}{rl} 3x^2 + 2yz & = 2x\lambda \\ 2xz & = 2y\lambda \\ 2xy - 2z & = 2z\lambda \\ x^2 + y^2 + z^2 & = 1 \end{array} \right.$$

dont les solutions forment un ensemble algébrique affine. Posons

$$f_1 = 3x^2 + 2yz - 2x\lambda\,, \quad f_2 = 2xz - 2y\lambda\,,$$

$$f_3 = 2xy - 2z - 2z\lambda\,, \quad f_4 = x^2 + y^2 + z^2 - 1.$$

On construit une base de Gröbner de l'idéal $I = \langle f_1, f_2, f_3, f_4 \rangle$ de $\mathbb{R}[x,y,z,\lambda]$, avec l'ordre lexi-

cographique donné par $\lambda > x > y > z$. On obtient

$$\begin{aligned}
g_1 &= \lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2,\\
g_2 &= x^2 + y^2 + z^2 - 1,\\
g_3 &= xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z,\\
g_4 &= xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z,\\
g_5 &= y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z,\\
g_6 &= y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z,\\
g_7 &= yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2,\\
g_8 &= z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z.
\end{aligned}$$

Le polynôme g_8 ne dépend que de l'indéterminée z. Les solutions de l'équation $g_8(z) = 0$ sont

$$z = \pm\frac{1}{16}\sqrt{2}\sqrt{11}, \quad z = \pm\frac{2}{3}, \quad z = \pm 1, \quad z = 0.$$

Avec ces différentes valeurs de z, on peut obtenir les valeurs de x et y dans les autres équations :

$$\begin{aligned}
&z = 0,\ y = 0,\ x = 1; \quad z = 0,\ y = 0,\ x = -1;\\
&z = 0,\ y = 1,\ x = 0; \quad z = 0,\ y = -1,\ x = 0;\\
&z = 1,\ y = 0,\ x = 0; \quad z = -1,\ y = 0,\ x = 0;\\
&z = \frac{2}{3},\ y = \frac{1}{3},\ x = -\frac{2}{3}; \quad z = -\frac{2}{3},\ y = -\frac{1}{3},\ x = -\frac{2}{3};\\
&z = \frac{\sqrt{11}}{8\sqrt{2}},\ y = \frac{-3\sqrt{11}}{8\sqrt{2}},\ x = -\frac{3}{8}; \quad z = -\frac{\sqrt{11}}{8\sqrt{2}},\ y = \frac{3\sqrt{11}}{8\sqrt{2}},\ x = -\frac{3}{8}.
\end{aligned}$$

Le choix de l'ordre lexicographique avec l'ordre $\lambda > x > y > z$ permet d'éliminer des indéterminées dans les équations. L'indéterminée λ est éliminée en premier, puis x, ...

§ 3 Une méthode d'élimination

Les exemples vus dans la section précédente mettent en évidence le procédé d'élimination qui peut apparaître lorsque l'on calcule une base de Gröbner avec l'ordre lexicographique

VI.3.1. Exemple.— On considère le système d'équations

$$\left|\begin{array}{ll} x^2 + y + z &= 1,\\ x + y^2 + z &= 1,\\ x + y + z^2 &= 1. \end{array}\right. \tag{VI.2}$$

Soit I l'idéal de $\mathbb{R}[x,y,z]$ défini par ces équations :

$$I = \left\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 \right\rangle.$$

On calcule une base de Gröbner G de I pour l'ordre lexicographique induit par $z < y < x$. On a $G = \{g_1, g_2, g_3, g_4\}$, avec

$$\begin{aligned} g_1 &= x+y+z^2-1, \\ g_2 &= y^2-y-z^2+z, \\ g_3 &= 2yz^2+z^4-z^2, \\ g_4 &= z^6-4z^4+4z^3-z^2. \end{aligned}$$

Le système (VI.2) possède les mêmes solutions que le système

$$\left| \begin{array}{rl} x+y+z^2-1 &= 0, \\ y^2-y-z^2+z &= 0, \\ 2yz^2+z^4-z^2 &= 0, \\ z^6-4z^4+4z^3-z^2 &= 0. \end{array} \right. \tag{VI.3}$$

On remarque que le polynôme g_4 est d'une seule indéterminée :

$$g_4 \in I \cap \mathbb{R}[z].$$

Le polynôme g_4 se factorise en

$$g_4 = z^2(z-1)^2(z^2+2z-1).$$

Les racines du polynôme g_4 sont les valeurs de z, ainsi

$$0, \quad 1, \quad -1-\sqrt{2}, \quad -1+\sqrt{2}.$$

En substituant ces valeurs dans les polynômes g_2 et g_3, on obtient les valeurs de l'indéterminée y. Ensuite en substituant les valeurs de y et z dans le polynôme g_1, on obtient les valeurs de x. Le système d'équations (VI.2) admet ainsi cinq solutions :

$$(1,0,0), \quad (0,1,0), \quad (0,0,1),$$

$$(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}), \quad (-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}).$$

Pour résoudre ce système, nous avons procédé en deux étapes :

— une étape d'*élimination* qui a produit une équation $g_4 = 0$ d'une seule indéterminée z, obtenue après éliminitation des indéterminées x et y,

— une étape d'*extension*, après résolution de l'équation $g_4 = 0$, on étend ces solutions aux autres équations, pour déterminer les valeurs des autres indéterminées.

VI.3.2. Idéal d'élimination.— Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Le k - ième *idéal d'élimination* I_k est l'idéal de $\mathbb{K}[x_{k+1}, \ldots, x_n]$ défini par

$$I_k = I \cap \mathbb{K}[x_{k+1}, \ldots, x_n].$$

Les éléments de I_k sont des *conséquences* du système d'équations

$$f_1 = \ldots = f_s = 0,$$

après élimination des indéterminées $x_1, \ldots, x_k$.

Noter que $I_0 = I$ et que les idéaux d'élimination dépendent de l'ordre des indéterminées. Le résultat suivant montre comment extraire d'une base de Gröbner de I une base de Gröbner de I_k.

VI.1 Théorème (Théorème d'élimination). — Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$ et soit G une base de Gröbner de I, pour l'ordre lexicographique induit par l'ordre alphabétique donné par $x_n < \ldots < x_2 < x_1$. Alors, pour tout $k \in [\![0, n]\!]$, l'ensemble

$$G_k = G \cap \mathbb{K}[x_{k+1}, \ldots, x_n]$$

est une base de Gröbner de l'idéal d'élimination I_k.

Preuve. Fixons $k \in [\![1, n]\!]$. On a $G_k \subset I_k$, par définition G_k est une base de Gröbner de I_k si

$$\langle \mathrm{lt}(G_k) \rangle = \langle \mathrm{lt}(I_k) \rangle .$$

L'inclusion $\langle \mathrm{lt}(G_k) \rangle \subset \langle \mathrm{lt}(I_k) \rangle$ est immédiate. Montrons l'inclusion réciproque. Il suffit de montrer que pour tout polynôme f de I_k, le terme dominant $\mathrm{lt}(f)$ est divisible par un $\mathrm{lt}(g)$, où $g \in G_k$.

Soit donc $f \in I_k$. Comme G est une base de Gröbner de I et que $I_k \subset I$, alors $\mathrm{lt}(f)$ est divisible par $\mathrm{lt}(g)$, où $g \in G$. Le polynôme f est dans I_k, il ne possède donc que des indéterminées $x_{k+1}, \ldots, x_n$. Comme $\mathrm{lt}(f) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$, alors $\mathrm{lt}(g) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$.

D'après l'ordre lexicographique choisi, tout monôme de $\mathbb{K}[x_1, \ldots, x_n] \setminus \mathbb{K}[x_{k+1}, \ldots, x_n$ est plus grand que tout monôme de $\mathbb{K}[x_{k+1}, \ldots, x_n]$, de $\mathrm{lt}(g) \in \mathbb{K}[x_{k+1}, \ldots, x_n]$, on déduit que g est un polynôme de $\mathbb{K}[x_{k+1}, \ldots, x_n]$; ainsi $g \in G_k$. □

VI.3.3. Exemple.— Reprenons l'exemple VI.3.1. Le premier idéal d'élimination est

$$I_1 = I \cap \mathbb{R}[y, z] = \left\langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2 \right\rangle$$

et le deuxième est

$$I_2 = I \cap \mathbb{R}[z] = \left\langle z^6 - 4z^4 + 4z^3 - z^2 \right\rangle .$$

Du théorème d'élimination VI.1, on déduit que tout polynôme qui élimine les indéterminées x et y est un multiple du polynôme $g_4 = z^6 - 4z^4 + 4z^3 - z^2$.

§ 4 Problème d'impliciter une présentation paramétrée

VI.4.1. Problème d'impliciter une présentation paramétrée.— *Étant donné un paramétrage*

$$x_i = f_i(t_1, \ldots, t_m), \quad i \in [\![1, n]\!], \quad f_i \in \mathbb{K}[t_1, \ldots, t_m],$$

d'un ensemble algébrique affine $\mathbf{V}$ *de* $\mathbb{K}^n$*, déterminer des polynômes* $g_1,\ldots,g_s$ *de* $\mathbb{K}[x_1,\ldots,x_n]$*, tels que*

$$\mathbf{V} = \mathbf{V}(g_1,\ldots,g_s).$$

Considérons l'ensemble algébrique affine de $\mathbb{K}^{n+m}$ défini par le système d'équations suivant

$$\left|\begin{array}{ll} x_1 - f_1(t_1,\ldots,t_m) & = 0 \\ & \vdots \\ x_n - f_n(t_1,\ldots,t_m) & = 0 \end{array}\right.$$

en les indéterminées $x_1,\ldots,x_n,t_1,\ldots,t_m$. L'objectif est d'éliminer les indéterminées $t_1,\ldots,t_m$ dans ces équations. On utilise pour cela les bases de Gröbner, comme méthode d'élimination, avec l'ordre lexicographique sur $\mathbb{K}[x_1,\ldots,x_n,t_1,\ldots,t_m]$ avec l'ordre alphabétique suivant

$$t_1 > \ldots > t_m > x_1 > \ldots > x_n.$$

Le calcul d'une base de Gröbner de l'idéal $I = \langle x_1 - f_1,\ldots,x_n - f_n\rangle$ avec cet ordre permettra d'obtenir une base de polynômes où les indéterminées $t_1,\ldots,t_m$ ont été éliminées.

VI.4.2. Exemple.— Considérons la courbe paramétrée $\mathscr{C}$ dans $\mathbb{C}^3$ définie par les équations suivantes

$$\left|\begin{array}{ll} x & = t^4, \\ y & = t^3, \\ z & = t^2. \end{array}\right. \tag{VI.4}$$

Considérons l'ordre lexicographique sur $\mathbb{C}[t,x,y,z]$ avec $z < y < x < t$. On calcule une base de Gröbner G de l'idéal

$$I = \left\langle t^4 - x,\, t^3 - y,\, t^2 - z\right\rangle$$

On obtient

$$G = \{t^2 - z,\, ty - z^2,\, tz - y,\, x - z^2,\, y^2 - z^3\}.$$

Ainsi

$$I = \left\langle t^2 - z,\, ty - z^2,\, tz - y,\, x - z^2,\, y^2 - z^3\right\rangle.$$

L'ensemble algébrique affine

$$\mathbf{V}(x - z^2,\, y^2 - z^3) = \mathbf{V}(I \cap \mathbb{C}[x,y,z])$$

est-il le plus petit contenant la courbe paramétrée $\mathscr{C}$?

VI.4.3. Théorème de l'implicitation.— Considérons une paramétrisation polynomiale

$$\begin{array}{l} x_1 = f_1(t_1,\ldots,t_m) \\ \quad\vdots \\ x_n = f_n(t_1,\ldots,t_m) \end{array} \tag{VI.5}$$

où $f_1,\ldots,f_n \in \mathbb{K}[t_1,\ldots,t_m]$. On peut associer une fonction

$$F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$$

définie par

$$F(t_1,\dots,t_m) = (f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

Ainsi $F(\mathbb{K}^m)$ est le sous-ensemble de $\mathbb{K}^n$ paramétrisé par les équations VI.5.

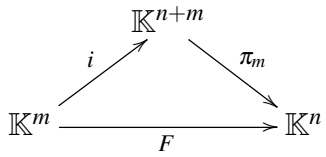
En général, $F(\mathbb{K}^m)$ n'est pas un ensemble algébrique affine. L'objectif est construire le plus petit ensemble algébrique affine de $\mathbb{K}^n$ contenant l'ensemble $F(\mathbb{K}^m)$. On considère pour cela l'ensemble algébrique affine

$$\mathbf{V} = \mathbf{V}(x_1 - f_1,\dots,x_n - f_n) \subset \mathbb{K}^{n+m}.$$

Les points de $\mathbf{V}$ s'écrivent

$$(t_1,\dots,t_m,f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

L'ensemble $\mathbf{V}$ est ainsi le graphe de la fonction F. On considère les applications i et π_m



définies par

$$i(t_1,\dots,t_m) = (t_1,\dots,t_m,f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)).$$

$$\pi_m(t_1,\dots,t_m,x_1,\dots,x_n) = (x_1,\dots,x_n).$$

On a $F = \pi_m \circ i$. Comme $i(\mathbb{K}^m) = \mathbf{V}$, on a

$$F(\mathbb{K}^m) = \pi_m(\mathbf{V}).$$

Ainsi, l'image de la paramétrisation est la projection de son graphe sur $\mathbb{K}^n$. Le théorème suivant construit le plus petit ensemble algébrique affine contenant $F(\mathbb{K}^n)$.

VI.2 Théorème (admis).— Soit $\mathbb{K}$ un corps infini. Soit $F : \mathbb{K}^m \longrightarrow \mathbb{K}^n$ une application définie par une paramétrisation polynomiale

$$x_i = f_i(t_1,\dots,t_m), \quad i \in [\![1,n]\!], \quad f_i \in \mathbb{K}[t_1,\dots,t_m].$$

Soit I l'idéal de $\mathbb{K}[t_1,\dots,t_m,x_1,\dots,x_n]$ défini par

$$I = \langle x_1 - f_1,\dots,x_n - f_n\rangle.$$

Soit $I_m = I \cap \mathbb{K}[x_1,\dots,x_n]$ le m-ième idéal d'intersection de I. Alors $\mathbf{V}(I_m)$ est le plus petit sous-ensemble algébrique affine de $\mathbb{K}^n$ contenant le sous-ensemble paramétré $F(\mathbb{K}^m)$.

VI.4.4. Algorithme pour rendre implicite une présentation paramétrée.—

ENTRÉE : $x_i = f_i(t_1,\dots,t_m), \quad i \in [\![1,n]\!], \quad f_i \in \mathbb{K}[t_1,\dots,t_m]$.

Considérer l'idéal $I = \langle x_1 - f_1,\dots,x_n - f_n\rangle$.

Calculer une base de Gröbner G de I avec un ordre lexicographique où chaque t_i est plus grand que chaque x_i.

D'après le théorème VI.1, $G \cap \mathbb{K}[x_1,\dots,x_n]$ est une base de Gröbner de I_m.

SORTIE : $\mathbf{V}(G \cap \mathbb{K}[x_1,\dots,x_n])$, qui est, d'après le théorème VI.2, le plus petit ensemble algébrique qui contient la paramétrisation.

VI.4.5. Exemple.— La cubique tordue est l'ensemble algébrique affine de $\mathbb{R}^3$ défini par $\mathbf{V} = \mathbf{V}(y-x^2, z-x^3)$, c'est l'intersection des deux surfaces de $\mathbb{R}^3$:

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

La surface tangente à la courbe $\mathbf{V}$ est obtenue comme la réunion des droites tangentes à la courbe.

Pour définir cette surface, on considère la description paramétrique de la courbe $\mathbf{V}$:

$$\left| \begin{array}{ll} x & = t \\ y & = t^2 \\ z & = t^3 \end{array} \right. \tag{VI.6}$$

Tout réel t défini un point $c(t) = (t, t^2, t^3)$ de la courbe. Le vecteur tangent en t à la courbe est $c'(t) = (1, 2t, 3t^2)$. La droite tangente à la courbe en t est paramétrée par

$$c(t) + uc'(t) = (t+u, t^2+2tu, t^3+3t^2u).$$

La surface tangente de la cubique tordue est ainsi paramétrée par

$$\left| \begin{array}{ll} x & = t+u, \\ y & = t^2+2tu, \\ z & = t^3+3t^2u. \end{array} \right. \tag{VI.7}$$

On calcule une base de Gröbner G de l'idéal

$$I = \left\langle t+u-x, t^2+2tu-y, t^3+3t^2u-z \right\rangle.$$

avec l'ordre lexicographique induit par l'ordre alphabétique $t > u > x > y > z$. On a $G = \{g_1,\dots,g_7\}$ avec

$$\begin{aligned}
g_1 &= t+u-x, \\
g_2 &= u^2-x^2+y, \\
g_3 &= ux^2-uy-x^3+\frac{3}{2}xy-\frac{1}{2}z, \\
g_4 &= uxy-uz-x^2y-xz+2y^2, \\
g_5 &= uxz-uy^2+x^2z-\frac{1}{2}xy^2-\frac{1}{2}yz, \\
g_6 &= uy^3-uz^2-2x^2yz+\frac{1}{2}xy^3-xz^2+\frac{5}{2}y^2z, \\
g_7 &= x^3z-\frac{3}{4}x^2y^2-\frac{3}{2}xyz+y^3+\frac{1}{4}z^2.
\end{aligned}$$

D'après le théorème d'élimination VI.1, on a

$$I_2 = I \cap \mathbb{R}[x,y,z] = \langle g_7 \rangle.$$

D'après le théorème d'implicitation VI.2, $\mathbf{V}(g_7)$ est le plus petit ensemble algébrique affine

contenant la surface tangente.

Le code Sage pour calculer la base de Gröbner G :

```
sage: A.<t,u,x,y,z> = PolynomialRing(RationalField(), 't,u,x,y,z', order='lex')
sage: f1 = t + u - x
sage: f2 = t^2 + 2*t*u - y
sage: f3 = t^3 + 3*t^2*u - z
sage: I = (f1,f2,f3)*A
sage: G = I.groebner_basis()
sage: G
[t + u - x, u^2 - x^2 + y, u*x^2 - u*y - x^3 + 3/2*x*y - 1/2*z, u*x*y -
u*z - x^2*y - x*z + 2*y^2, u*x*z - u*y^2 + x^2*z - 1/2*x*y^2 - 1/2*y*z,
u*y^3 - u*z^2 - 2*x^2*y*z + 1/2*x*y^3 - x*z^2 + 5/2*y^2*z, x^3*z -
3/4*x^2*y^2 - 3/2*x*y*z + y^3 + 1/4*z^2]
```

Pour tracer la surface :

```
sage: var('x,y,z')
sage: h = lambda x, y , z:x^3*z - 3/4*x^2*y^2 - 3/2*x*y*z + y^3 + 1/4*z^2
sage: f = implicit_plot3d(h, (x,-3,3), (y, -3,3), (z, -3,3),
                                        plot_points=100, adaptative = True)
sage: f
```