Notes de cours

Systèmes Polynomiaux

Cyrille CHENAVIER

Université de Limoges

Master 1 - semestre 2

Chapitre 1 :

Rappels d'algèbre commutative

De nombreux problèmes, issus des mathématiques ou d'autres domaines, se ramènent à résoudre ou prouver l'existence de solutions d'un système d'équations à une ou plusieurs inconnues. Deux approches complémentaires ont été développées dans ce sens : l'une numérique et l'autre symbolique, celles-ci pouvant naturellement s'articuler. *Grosso modo*, une approche numérique, par exemple la méthode de de Newton, vise à calculer des solutions approchées pour des fonctions différentiables, alors qu'une approche symbolique porte sur les solutions exactes de fonctions polynomiales. Dans ce cours, on s'intéresse à la deuxième approche.

Les premiers exemples faisant intervenir des systèmes d'équations polynomiales à plusieurs variables sont issus de la géométrie. Par exemple, dans le plan euclidien muni des coordonnées x, y, on veut calculer l'intersection d'un cercle de centre (a, b) et de rayon R d'équation $(x-a)^2 + (y-b)^2 = R$ avec une hyperbole d'équation $xy = \alpha$, et donc trouver les solutions du système

$$\begin{cases} x^2 + y^2 - 2ax - 2by + a^2 + b^2 - R = 0 \\ xy - \alpha = 0. \end{cases}$$

Dans le cadre des travaux dirigés et/ou pratiques, on verra également que des problèmes issus de la cryptologie ou de l'optimisation sous contraintes peuvent se ramener à des systèmes polynomiaux.

Comme on le verra, la recherche de solutions d'un système polynomial est étroitement lié à la théorie de l'élimination. On peut d'ores et déjà mentionner deux cas particuliers pour s'en convaincre. **1.** Pour savoir si deux polynômes en une variable ont une solution complexe commune, on calcule leur pgcd par l'algorithme d'Euclide, celui-ci consistant à éliminer itérativement des monômes de hauts degrés. **2.** Pour calculer les solutions d'un système linéaire de plusieurs inconnues, on trigonalise le système grâce au pivot de Gauss, méthode consistant à éliminer itérativement des inconnues dans les équations. Dans le cas des systèmes non linéaires à plusieurs variables, on aura besoin d'outils permettant d'étendre l'algorithme d'Euclide ou la méthode du pivot de Gauss. Ces outils sont appelés *résultant* et *bases de Gröbner*.

Le plan de ce cours est le suivant : on commence par quelques rappels d'algèbre commutative sur les polynômes dans le chapitre courant, on introduit le résultant et ses propriétés dans le chapitre 2, la théorie des bases de Gröbner dans le chapitre 3 et enfin les applications de ces outils à la géométrie algébrique sous un angle algorithmique dans le chapitre 4. L'adjectif algébrique provient du fait que les objets géométriques que l'on considère sont définis par des équations polynomiales, *i.e.*, qui ne dépendent que d'opérations algébriques en les inconnues : sommes, produits et produits par des scalaires.

1.1. Polynômes multivariés

On fixe un ensemble $x_1, \dots, x_d$ d'indéterminées. Les monômes en ces indéterminées sont les d-uplets d'entiers $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{N}^d$, qu'on note simplement $\mathbf{x}^\alpha = x_1^{\alpha_1} \dots x_d^{\alpha_d}$; on note de plus $1 = \mathbf{x}^{(0,\dots,0)}$. Le degré de $\mathbf{x}^\alpha$ est la somme $\alpha_1 + \dots + \alpha_d$. Un polynôme $f(x_1, \dots, x_d)$ à coefficients dans un corps $\mathbb{K}$ en les indéterminées $x_1 \dots, x_d$ est une combinaison linéaire formelle finie de monômes :

$$f(x_1, \dots, x_d) = \sum_{\alpha \in \mathbb{N}^d} f_\alpha \mathbf{x}^\alpha, \qquad f_\alpha \in \mathbb{K}, \quad \text{presque tout } f_\alpha = 0.$$

On note $\mathbb{K}[x_1, \dots, x_d]$ l'ensemble des polynômes en $x_1, \dots, x_d$ à coefficients dans $\mathbb{K}$. Afin d'alléger les notations, lorsque le contexte est clair, on ne note pas les indéterminées d'un polynôme, *i.e.*, on note simplement $f \in \mathbb{K}[x_1, \dots, x_d]$ l'élément $f(x_1, \dots, x_d)$. On appelle *degré* de f, noté $\deg(f)$, le plus haut degré d'un $\mathbf{x}^\alpha$ tel que $f_\alpha \neq 0$. Étant donnée une nouvelle indéterminée t, un polynôme multivarié $f(x_1, \dots, x_d, t)$ peut être vu comme un polynôme univarié en t à coefficients dans $\mathbb{K}[x_1, \dots, x_d]$:

$$f(x_1, \dots, x_d, t) = \sum_{k=0}^{n} f_k(x_1, \dots, x_d) t^k, \quad f_k(x_1, \dots, x_d) \in \mathbb{K}[x_1, \dots, x_d].$$

Quitte à supprimer des termes, on peut supposer que $f_n(x_1, \dots, x_d)$ est non nul, et on appelle n le *degré relativement à t* de $f(x_1, \dots, x_d, t)$, noté $\deg_t(f)$.

On appelle *support* de $f \in \mathbb{K}[x_1, \dots, x_d]$, noté $\operatorname{supp}(f)$, l'ensemble des monômes figurant avec un coefficient non nul dans f :

$$\operatorname{supp}(f) = \{\mathbf{x}^\alpha \mid f_\alpha \neq 0\}.$$

Exemple 1.1.1. Dans les exemples, on considère souvent polynômes de 2 ou 3 variables, notées x, y ou x, y, z au lieu de x_1, x_2 ou x_1, x_2, x_3, respectivement. Par exemple,

$$f(x, y, z) = 2x^3y^2z + \frac{3}{2}y^4z^2 - 3xyz + y^2$$

est un élément de $\mathbb{Q}[x, y, z]$ tel que $f_{(3,2,1)} = 2$, $f_{(0,4,2)} = 3/2$, $f_{(1,1,1)} = -3$ et $f_{(0,2,0)} = 2$. On a

$$\deg(f) = 6, \quad \deg_x(f) = 3, \quad \deg_y(f) = 4, \quad \deg_z(f) = 2, \quad \operatorname{supp}(f) = \{x^3y^2z, y^4z^2, xyz, y^2\}.$$

On rappelle que $\mathbb{K}[x_1, \dots, x_d]$ est muni d'une structure d'algèbre, où la multiplication par un scalaire consiste à multiplier les coefficients par ce scalaire, la somme de deux polynômes consiste à sommer les coefficients figurant devant le même monôme et le produit est obtenu en étendant par bilinéarité le produit de deux monômes $\mathbf{x}^\alpha \mathbf{x}^\beta = \mathbf{x}^{\alpha+\beta}$.

Un *idéal* de $\mathbb{K}[x_1, \dots, x_d]$ est un sous ensemble I de $\mathbb{K}[x_1, \dots, x_d]$ vérifiant les trois propriétés

- $0 \in I$,
- pour tout $f, g \in I$, on a $f + g \in I$,
- pour tout $f \in I$ et tout $g \in \mathbb{K}[x_1, \dots, x_d]$, on a $fg \in I$.

Étant donnée une famille de polynômes $F \subseteq \mathbb{K}[x_1, \dots, x_d]$, on note $I(F)$ l'idéal engendré par F, *i.e.*, l'ensemble des combinaison finies d'éléments de F à coefficients dans $\mathbb{K}[x_1, \dots, x_d]$:

$$I(F) = \{f \in \mathbb{K}[x_1, \dots, x_d] \mid \exists f_1, \dots, f_s \in F,\ g_1, \dots, g_s \in \mathbb{K}[x_1, \dots, x_d] \text{ tels que } f = f_1g_1 + \dots + f_sg_s\}.$$

On dit qu'un idéal I de $\mathbb{K}[x_1, \dots, x_d]$ est de *type fini* s'il existe une famille finie $F \subset I$ telle que $I = I(F)$. Si $F = \{f_1, \dots, f_s\}$, on note simplement $I(f_1, \dots, f_s)$ au lieu de $I(\{f_1, \dots, f_s\})$. On verra dans le théorème 3.3.3 que tout idéal de $\mathbb{K}[x_1, \dots, x_d]$ est de type fini.

Étant donné un idéal I de $\mathbb{K}[x_1,\dots,x_d]$, on note $\mathbb{K}[x_1,\dots,x_d]/I$ l'espace quotient induit par la relation d'équivalence

$$f \equiv_I g \quad \Leftrightarrow \quad f - g \in I.$$

Les opérations d'algèbre de $\mathbb{K}[x_1,\dots,x_d]$ passent toutes au quotient, de sorte que $\mathbb{K}[x_1,\dots,x_d]/I$ est une algèbre pour les opérations suivantes, où $[f]_I$ et $[g]_I$ désignent les classes de f et g dans $\mathbb{K}[x_1,\dots,x_d]/I$:

$$\lambda[f]_I = [\lambda f]_I, \qquad [f]_I + [g]_I = [f+g]_I, \qquad [f]_I[g]_I = [fg]_I.$$

Enfin, à tout polynôme $f \in \mathbb{K}[x_1,\dots,x_d]$, on peut associer une fonction polynomiale, que l'on note encore f par abus de notation :

$$\begin{aligned} f : \quad \mathbb{K}^d &\to \mathbb{K} \\ \mathbf{a} = (a_1,\dots,a_d) &\mapsto f(\mathbf{a}) = \sum_{\alpha\in\mathbb{N}^d} f_\alpha a_1^{\alpha_1}\dots a_d^{\alpha^d}. \end{aligned}$$

On note que si $\overline{\mathbb{K}}$ est une clôture algébrique de $\mathbb{K}$, alors tout $f \in \mathbb{K}[x_1,\dots,x_d]$ peut être vu comme un élément de $\overline{\mathbb{K}}[x_1,\dots,x_d]$, si bien qu'on peut associer à f une fonction de $\overline{\mathbb{K}}^d$ dans $\overline{\mathbb{K}}$. On note alors $Z(f)$ l'ensemble des zéros de cette fonction :

$$Z(f) = \left\{\mathbf{a} \in \overline{\mathbb{K}}^d \mid f(\mathbf{a}) = 0\right\}.$$

L'ensemble $Z(f)$ permet de donner un sens géométrique à la relation d'équivalence $\equiv_I$. Un ensemble de polynômes $F = \{f_1,\cdots,f_s\} \subseteq \mathbb{K}[x_1,\dots,x_d]$ peut être pensé comme un ensemble d'équations sur $\mathbb{K}^d$ ou $\overline{\mathbb{K}}^d$, l'ensemble des solutions de ces équations étant précisément $Z(F) = Z(f_1)\cap\dots\cap Z(f_s)$. Étant donnés deux polynômes $f,g \in \mathbb{K}[x_1,\dots,x_d]$, l'équivalence $f \equiv_{I(F)} g$ signifie que les restrictions de f et g sur Z induisent la même fonction. En d'autres termes, l'algèbre quotient $\mathbb{K}[x_1,\dots,x_d]/I(F)$ peut être pensée comme étant l'algèbre des polynômes sur Z.

1.2. Polynômes d'une seule variable

Dans cette section, on s'intéresse à la structure de l'algèbre $\mathbb{K}[x]$, *i.e.*, lorsque $d = 1$ et que l'on note simplement $x = x_1$. Dans le cas univarié, l'algèbre polynomiale a une structure plus riche que dans le cas multivarié puisqu'elle est munie d'une structure euclidienne, *i.e.*, il existe un algorithme de division euclidienne. Étant donnés $p(x), d(x) \in \mathbb{K}[x]$, la division euclidienne de $p(x)$ par $d(x)$ fournit un quotient $q(x)$ et un reste $r(x)$ tels que $p(x) = q(x)d(x) + r(x)$ et $\deg(r(x)) < \deg(d(x))$. L'existence d'une division euclidienne implique que $\mathbb{K}[x]$ est *principal*, *i.e.*, tous les idéaux de $\mathbb{K}[x]$ sont engendrés par un seul élément ; on dit qu'un tel idéal est *principal*.

L'algorithme d'Euclide permet de calculer par divisions euclidiennes successives un plus grand diviseur commun de deux polynômes $f(x)$ et $g(x)$. Ce plus grand commun diviseur est unique à multiplication par une constante non nulle près, et on note $\mathrm{pgcd}(f(x),g(x))$ le plus grand diviseur commun unitaire, *i.e.*, dont le coefficient de plus haut degré est égal à 1. On rappelle de plus que l'idéal $I\big(f(x),g(x)\big)$ engendré par $f(x)$ et $g(x)$ est l'idéal principal $I\big(\mathrm{pgcd}(f(x),g(x))\big)$, engendré par leur pgcd. Deux polynômes sont dits *premiers entre eux* si leur pgcd est égal à 1, ce qui signifie qu'ils n'ont aucun facteur commun. D'après le théorème de Bézout, il existe des polynômes $A(x)$ et $B(x)$ tels que $A(x)f(x) + B(x)g(x) = \mathrm{pgcd}(f(x),g(x))$, de sorte que $f(x)$ et $g(x)$ sont premiers entre eux si et seulement si ils n'ont aucune racine commune dans $\overline{\mathbb{K}}$. On rappelle enfin le théorème de Gauss.

Théorème 1.2.1 (Théorème de Gauss)**.** *Soient $f(x), g(x)$ et $h(x)$ trois polynômes à coefficients dans $\mathbb{K}$ tels que $f(x)$ divise le produit $g(x)h(x)$. Si $f(x)$ et $g(x)$ sont premiers entre eux, alors $f(x)$ divise $h(x)$.*

Chapitre 2 :

Résultants

2.1. Résultants et facteurs communs

Pour motiver le résultant, on commence par considérer deux polynômes $f(x)$ et $g(x)$ en une variable x à coefficients dans un corps $\mathbb{K}$ et de degrés respectifs n et m :

$$f(x) = \sum_{k=0}^{n} f_k x^k, \qquad g(x) = \sum_{k=0}^{m} g_k x^k, \qquad f_k, g_k \in \mathbb{K}, \qquad f_n g_m \neq 0.$$

On se pose la question de tester si les deux polynômes sont premiers entre eux, ou de façon équivalente s'ils n'ont aucun facteur commun. On pourrait calculer $\text{pgcd}(f(x), g(x))$ grâce à l'algorithme d'Euclide, ce qui amènerait à faire des divisions dans $\mathbb{K}$. On peut éviter de faire ces divisions en se ramenant à un calcul de déterminant, appelé le résultant de $f(x)$ et $g(x)$, noté $\text{res}(f(x), g(x))$. On a pour cela besoin du lemme suivant.

Lemme 2.1.1 ([1, Lemme 3.5.6])**.** *Les deux polynômes $f(x)$ et $g(x)$ ont un facteur commun si et seulement s'il existe $A(x), B(x) \in \mathbb{K}[x]$ tels que*

1. *$A(x)$ et $B(x)$ sont non nuls,*
2. *$\deg(A(x)) \leq m-1$ et $\deg(B(x)) \leq n-1$,*
3. *$A(x)f(x) + B(x)g(x) = 0$.*

Démonstration. On suppose d'abord que $f(x)$ et $g(x)$ ont un facteur commun $p(x) \in \mathbb{K}[x]$, de sorte qu'il existe $f_1(x), g_1(x) \in \mathbb{K}[x]$ non nuls avec $\deg(f_1(x)) \leq n-1, \deg(g_1(x)) \leq m-1$, $f(x) = f_1(x)p(x)$ et $g(x) = g_1(x)p(x)$. Les polynômes $A(x) = g_1(x)$ et $B(x) = -f_1(x)$ vérifient alors les trois conditions voulues. On suppose réciproquement l'existence des polynômes $A(x)$ et $B(x)$ vérifiant les trois conditions et on montre par l'absurde que $f(x)$ et $g(x)$ ont un facteur commun. Si $f(x)$ et $g(x)$ étaient premiers entre eux, alors d'après l'égalité $A(x)f(x) = -B(x)g(x)$, le théorème de Gauss implique que $f(x)$ divise $B(x)$. On arrive à une contradiction puisque $B(x)$ est non nul et que $\deg(B(x)) < \deg(f(x))$, de sorte que $f(x)$ et $g(x)$ ont un facteur commun. □

Étant donné un entier k, on désigne par $\mathbb{K}[x]_k$ l'ensemble des polynômes de degré au plus k : il s'agit d'un espace vectoriel de dimension $k+1$ avec pour base $1, x, \ldots, x^k$. On considère l'application

$$\begin{array}{rccc} \varphi_{f,g} : & \mathbb{K}[x]_{m-1} \oplus \mathbb{K}[x]_{n-1} & \to & \mathbb{K}[x]_{n+m-1} \\ & (A(x), B(x)) & \mapsto & A(x)f(x) + B(x)g(x). \end{array}$$

On remarque que $\varphi_{f,g}$ est une application linéaire, *i.e.*, étant donnés deux couples $(A(x),B(x))$ et $(A'(x),B'(x))$ dans $\mathbb{K}[x]_{m-1}\oplus\mathbb{K}[x]_{n-1}$ et un scalaire $\lambda\in\mathbb{K}$, on a

$$\begin{aligned}\varphi_{f,g}(A(x)+\lambda A'(x),B(x)+\lambda B'(x)) &= \big(A(x)+\lambda A'(x)\big)f(x)+\big(B(x)+\lambda B'(x)\big)g(x)\\ &= \big(A(x)f(x)+B(x)g(x)\big)+\lambda\big(A'(x)f(x)+B'(x)g(x)\big)\\ &= \varphi_{f,g}(A(x),B(x))+\lambda\varphi_{f,g}(A'(x),B'(x)).\end{aligned}$$

D'après le lemme 2.1.1, $f(x)$ et $g(x)$ admettent un facteur commun si et seulement si $\varphi_{f,g}$ a un noyau non trivial, c'est-à-dire, si et seulement si elle n'est pas injective. En remarquant que les deux espaces vectoriels $\mathbb{K}[x]_{m-1}\oplus\mathbb{K}[x]_{n-1}$ et $\mathbb{K}[x]_{n+m-1}$ ont même dimension $n+m$, l'injectivité de $\varphi_{f,g}$ peut être testée à partir d'un calcul de déterminant. On introduit donc la matrice de Sylvester et son déterminant, appelé le résultant.

Définition 2.1.2. Soient $f(x)=f_nx^n+f_{n-1}x^{n-1}\cdots+f_0$ et $g(x)=g_mx^m+g_{m-1}x^{m-1}+\cdots+g_0$ deux éléments de $\mathbb{K}[x]$ de degrés respectifs n et m, *i.e.*, $f_ng_m\neq 0$. La *matrice de Sylvester* de $f(x)$ et $g(x)$ est la matrice carrée de taille $n+m$:

$$\mathrm{Syl}(f(x),g(x)) = \begin{pmatrix} f_n & f_{n-1} & \cdots & \cdots & f_0 & & \\ & f_n & f_{n-1} & \cdots & \cdots & f_0 & \\ & & \ddots & \ddots & & & \ddots \\ & & & f_n & f_{n-1} & \cdots & f_0 \\ g_m & g_{m-1} & \cdots & \cdots & g_0 & & \\ & g_m & g_{m-1} & \cdots & \cdots & g_0 & \\ & & \ddots & \ddots & & & \ddots \\ & & & g_m & g_{m-1} & \cdots & g_0 \end{pmatrix} \begin{matrix}\left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}m\text{ lignes}\\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}n\text{ lignes}\end{matrix}$$

où les espaces vides sont des zéros. Le déterminant de cette matrice est appelé le *résultant* de $f(x)$ et $g(x)$:

$$\mathrm{res}(f(x),g(x)) = \det\big(\mathrm{Syl}(f(x),g(x))\big).$$

En munissant les deux espaces $\mathbb{K}[x]_{m-1}\oplus\mathbb{K}[x]_{n-1}$ et $\mathbb{K}[x]_{n+m-1}$ respectivement des bases

$$\Big\{\big(x^{m-1},0\big),\big(x^{m-2},0\big),\ldots,\big(1,0\big),\big(0,x^{n-1}\big),\big(0,x^{n-2}\big),\ldots,\big(0,1\big)\Big\} \qquad \text{et} \qquad \Big\{x^{n+m-1},x^{n+m-2},\ldots,1\Big\}$$

on remarque que $\mathrm{Syl}(f(x),g(x))$ n'est rien d'autre que la transposée de la matrice de $\varphi_{f,g}$ relativement à ces deux bases. En effet, les m premières lignes forment les images de $\big(x^{m-1},0\big),\ldots,\big(1,0\big)$ relativement à la deuxième base et les n dernières lignes forment les images de $\big(0,x^{n-1}\big),\ldots,\big(0,1\big)$. Ainsi, $\varphi_{f,g}$ est injective si et seulement si $\mathrm{res}(f(x),g(x))$ est non nul, de sorte que le lemme 2.1.1 permet d'obtenir le résultat suivant.

Théorème 2.1.3 ([1, Proposition 3.5.8])**.** *Soient $f(x)$ et $g(x)$ deux polynômes à coefficients dans un corps. Alors $f(x)$ et $g(x)$ sont premiers entre eux si et seulement si* $\mathrm{res}(f(x),g(x))$ *est non nul.*

On donne des exemples illustrant la définition et le théorème précédents.

Exemple 2.1.4. On considère d'abord un exemple provenant de [1], avec $\mathbb{K}=\mathbb{Q}$, $n=m=2$ et

$$f(x) = 2x^2+3x+1, \qquad g(x) = 7x^2+x+3.$$

On a

$$\mathrm{Syl}(f(x),g(x)) = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \\ 7 & 1 & 3 & 0 \\ 0 & 7 & 1 & 3 \end{pmatrix}$$

et on vérifie que $\mathrm{res}(f(x),g(x))=153$. Ainsi, $f(x)$ et $g(x)$ sont premiers entre eux.

Exemple 2.1.5. Considérons maintenant un exemple de polynômes qui ne sont pas premiers entre eux avec $\mathbb{K} = \mathbb{Q}$, $n = 3$, $m = 2$ et

$$f(x) = 2x^3 - x^2 + 7x + 4, \qquad g(x) = 2x^2 + 11x + 5.$$

On a

$$\mathrm{Syl}(f(x), g(x)) = \begin{pmatrix} 2 & -1 & 7 & 4 & 0 \\ 0 & 2 & -1 & 7 & 4 \\ 2 & 11 & 5 & 0 & 0 \\ 0 & 2 & 11 & 5 & 0 \\ 0 & 0 & 2 & 11 & 5 \end{pmatrix}$$

et on vérifie que $\mathrm{res}(f(x), g(x)) = 0$. Ainsi, $f(x)$ et $g(x)$ ne sont pas premiers entre eux.

On a vu dans l'exemple précédent comment montrer grâce au résultant que deux polynômes ne sont pas premiers entre eux, c'est-à-dire, que leur pgcd n'est pas un polynôme constant. On peut alors se demander comment calculer ce pgcd à partir de la matrice de Sylvester, ce qui est l'objet de la proposition suivante.

Proposition 2.1.6. *La dernière ligne non nulle d'une forme échelonnée en lignes de* $\mathrm{Syl}(f(x), g(x))$ *contient les coefficients d'un* pgcd *de* $f(x)$ *et* $g(x)$.

Démonstration. Soit $\overline{\mathrm{Syl}}(f(x), g(x))$ une forme échelonnée en lignes de $\mathrm{Syl}(f(x), g(x))$. Les lignes non nulles de $\overline{\mathrm{Syl}}(f(x), g(x))$ formant une base de $\mathrm{im}\left(\varphi_{f,g}\right)$, sa dernière ligne non nulle $R(x)$ correspond à un polynôme de degré minimal de la forme $A(x)f(x) + B(x)g(x)$. De plus, les polynômes de cette forme sont dans $I(f(x), g(x)) = I\left(\mathrm{pgcd}(f(x), g(x))\right)$, *i.e.*, sont des multiples de $\mathrm{pgcd}(f(x), g(x))$, de sorte que $R(x)$ est divisible par $\mathrm{pgcd}(f(x), g(x))$, avec $\deg(R(x)) \leq \deg\left(\mathrm{pgcd}(f(x), g(x))\right)$. Ainsi, $R(x)$ est un multiple de $\mathrm{pgcd}(f(x), g(x))$, *i.e.*, $R(x)$ est un pgcd (pas nécessairement unitaire) de $f(x)$ et $g(x)$. □

Avant d'illustrer la proposition 2.1.6, on remarque qu'en conjonction avec le théorème 2.1.3, celle-ci permet de retrouver que deux polynômes $f(x)$ et $g(x)$ sont premiers entre eux si et seulement si leur pgcd est un polynôme constant. En effet, $f(x)$ et $g(x)$ sont premiers entre eux si et seulement le déterminant de $\mathrm{Syl}(f(x), g(x))$ est non nul, c'est-à-dire, si et seulement si une forme échelonnée en ligne de $\mathrm{Syl}(f(x), g(x))$ ne contient aucune ligne de zéro, c'est-à-dire, si et seulement si sa dernière ligne correspond à un polynôme constant, c'est-à-dire, si et seulement si $\mathrm{pgcd}(f(x), g(x)) = 1$.

Exemple 2.1.7. On considère comme précédemment $f(x) = 2x^3 - x^2 + 7x + 4$, $g(x) = 2x^2 + 11x + 5$ et la matrice de Sylvester associée :

$$\mathrm{Syl}(f(x), g(x)) = \begin{pmatrix} 2 & -1 & 7 & 4 & 0 \\ 0 & 2 & -1 & 7 & 4 \\ 2 & 11 & 5 & 0 & 0 \\ 0 & 2 & 11 & 5 & 0 \\ 0 & 0 & 2 & 11 & 5 \end{pmatrix}$$

La forme échelonné réduite en ligne de $\mathrm{Syl}(f(x), g(x))$ est donnée par

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1/16 \\ 0 & 1 & 0 & 0 & 1/8 \\ 0 & 0 & 1 & 0 & 1/4 \\ 0 & 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ce qui signifie que $\mathrm{pgcd}(f(x), g(x)) = x + 1/2$.

2.2. Résultants et élimination de variables

Dans cette section, on étend la notion de résultant au cas des polynômes multivariés. En pratique, on considère l'une des variables comme étant à éliminer. Afin de faire apparaître explicitement la variable à éliminer, on la note différemment ; on considère ainsi l'algèbre polynomiale $\mathbb{K}[x_1,\dots,x_d,t]$, identifiée à l'algèbre $\mathbb{K}[x_1,\dots,x_d][t]$ des polynômes en la variable à éliminer t à coefficients dans $\mathbb{K}[x_1,\dots,x_d]$. Enfin, afin d'alléger les notations, on ne notera pas toujours les variables $x_1,\dots,x_d,t$ d'un polynôme : *i.e.*, les polynômes seront notés f,g au lieu de $f(x_1,\dots,x_d,t)$ et $g(x_1,\dots,x_d,t)$.

On considère deux polynômes $f,g\in\mathbb{K}[x_1,\dots,x_d,t]$ tels que $\deg_t(f)=n$ et $\deg_t(g)=m$:

$$f(x_1,\dots,x_d,t) \;=\; \sum_{k=0}^{n} f_k(x_1,\dots,x_d)\,t^k, \qquad g(x_1,\dots,x_d,t) \;=\; \sum_{k=0}^{m} g_k(x_1,\dots,x_d)\,t^k$$

avec

$$f_k(x_1,\dots,x_d), g_k(x_1,\dots,x_d)\in\mathbb{K}[x_1,\dots,x_d], \qquad f_n(x_1,\dots,x_d)g_m(x_1,\dots,x_d)\neq 0.$$

On définit comme précédemment la matrice de Sylvester et le résultant de f et g, à la différence près qu'il faut indiquer la variable d'élimination t. La matrice de Sylvester est cette fois-ci à coefficients dans $\mathbb{K}[x_1,\dots,x_d]$ et le calcul de son déterminant ne faisant intervenir que des additions et multiplications, celui-ci est également un élément de $\mathbb{K}[x_1,\dots,x_d]$. Comme précédemment, on ne note pas nécessairement les variables $x_1,\dots,x_d$ dans les coefficients f_k et g_k.

Définition 2.2.1. Soient $f=f_nt^n+f_{n-1}t^{n-1}\cdots+f_0$ et $g=g_mt^m+g_{m-1}t^{m-1}+\cdots+g_0$ deux éléments de $\mathbb{K}[x_1,\dots,x_d,t]$ de degrés respectifs n et m et t, *i.e.*, $f_ng_m\neq 0$. La *matrice de Sylvester relativement à t* de f et g est la matrice carrée de taille $n+m$:

$$\mathrm{Syl}_t(f,g) \;=\; \begin{pmatrix} f_n & f_{n-1} & \cdots & \cdots & f_0 & & \\ & f_n & f_{n-1} & \cdots & \cdots & f_0 & \\ & & \ddots & \ddots & & & \ddots \\ & & & f_n & f_{n-1} & \cdots & \cdots & f_0 \\ g_m & g_{m-1} & \cdots & \cdots & g_0 & & \\ & g_m & g_{m-1} & \cdots & \cdots & g_0 & \\ & & \ddots & \ddots & & & \ddots \\ & & & g_m & g_{m-1} & \cdots & \cdots & g_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix}$$

où les espaces vides sont des zéros. Le déterminant de cette matrice est appelé le *résultant relativement à t* de f et g :

$$\mathrm{res}_t(f,g) \;=\; \det\big(\mathrm{Syl}_t(f,g)\big)\in\mathbb{K}[x_1,\dots,x_d].$$

On voit que le résultant est relié est la théorie de l'élimination dans le sens où à partir de deux polynômes en les variables $x_1,\dots,x_d,t$, on produit un nouveau polynôme où la variable t a été éliminée. On finit ce chapitre par deux résultats, les proposition 2.2.2 et 2.2.4, portant sur les idéaux d'élimination que l'on introduit dans le chapitre 4, et qui seront utiles lorsque l'on s'intéressera à la résolution de systèmes polynomiaux en plusieurs variables.

Proposition 2.2.2 ([1, Proposition 3.5.9])**.** *Soient $f,g\in\mathbb{K}[x_1,\dots,x_d,t]$ avec $\deg_t(f)=n$ et $\deg_t(g)=m$. Il existe $A,B\in\mathbb{K}[x_1,\dots,x_d,t]$ tels que $\deg_t(A)<m$, $\deg_t(B)<n$ et*

$$Af+Bg \;=\; \mathrm{res}_t(f,g).$$

Démonstration. On note $C_1, \dots, C_{n+m}$ les colonnes de la matrice de Sylvester $\mathrm{Syl}_t(f,g)$. Le déterminant d'une matrice ne changeant pas en changeant l'une de ses colonnes par une combinaison linéaire (dont les scalaires sont dans un anneau des coefficients de $\mathrm{Syl}_t(f,g)$) de ses colonnes. Or, les coefficients de $\mathrm{Syl}_t(f,g)$ sont dans $\mathbb{K}[x_1,\dots,x_d]$, qui est inclus dans $\mathbb{K}[x_1,\dots,x_d,t]$, de sorte qu'on peut calculer $\mathrm{res}_t(f,g)$ en remplaçant C_{n+m} par

$$t^{n+m-1}C_1 + t^{n+m-2}C_2 + \cdots + t^2 C_{n+m-2} + tC_{n+m-1} + C_{n+m} \quad = \quad \begin{pmatrix} t^{m-1}f \\ t^{m-2}f \\ \vdots \\ tf \\ f \\ t^{n-1}g \\ t^{n-2}g \\ \vdots \\ tg \\ g \end{pmatrix}.$$

En développant relativement à cette colonne, on obtient que $\mathrm{res}_t(f,g)$ est bien de la forme annoncée. □

Le résultant relativement à t de $f, g \in \mathbb{K}[x_1,\dots,x_d,t]$ est un élément de $\mathbb{K}[x_1,\dots,x_d]$. On va maintenant caractériser l'ensemble $Z\big(\mathrm{res}_t(f,g)\big)$ des zéros de ce polynôme dans une clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$, où on rappelle que

$$Z\big(\mathrm{res}_t(f,g)\big) \;=\; \Big\{ \mathbf{a} \in \overline{\mathbb{K}}^d \;\mid\; \mathrm{res}_t(f,g)(\mathbf{a}) = 0 \Big\}.$$

Dans la preuve de la proposition 2.2.4, on aura besoin du lemme suivant.

Lemme 2.2.3 ([1, Proposition 3.6.3])**.** *Soit* $\mathbf{a} \in \overline{\mathbb{K}}^d$ *tel que* $\deg\big(f(\mathbf{a},t)\big) = n$ *et* $\deg\big(g(\mathbf{a},t)\big) = s \le m$*. On a :*

$$\mathrm{res}_t(f,g)(\mathbf{a}) \;=\; f_n(\mathbf{a})^{m-s}\,\mathrm{res}\big(f(\mathbf{a},t), g(\mathbf{a},t)\big),$$

où $\mathrm{res}\big(f(\mathbf{a},t), g(\mathbf{a},t)\big)$ *est le résultant de deux éléments de* $\overline{\mathbb{K}}[t]$.

Démonstration. On revient à la définition : pour calculer $\mathrm{res}_t(f,g)(\mathbf{a})$ il suffit de calculer le déterminant de $\mathrm{Syl}_t(f,g)$ dont les coefficients f_k, g_k sont évalués en $\mathbf{a}$. Tous les termes $g_k(\mathbf{a})$ tels que $k \ge s+1$ s'annulent, de sorte que les $m-s$ premières colonnes sont composées d'un bloc diagonal de taille $m-s$ avec des $f_n(\mathbf{a})$ comme termes diagonaux suivis de lignes de zéros. Il suffit alors de calculer le déterminant par blocs pour obtenir le résultat. En résumé :

$$\mathrm{res}_t(f,g)(\mathbf{a}) = \det\begin{pmatrix} f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & & \\ & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & \\ & & \ddots & \ddots & & & \ddots \\ & & & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) \\ g_m(\mathbf{a}) & g_{m-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) & & \\ & g_m(\mathbf{a}) & g_{m-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) & \\ & & \ddots & \ddots & & & \ddots \\ & & & g_m(\mathbf{a}) & g_{m-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix}$$

$$= \det\begin{pmatrix} f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & & \\ & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & \\ & & \ddots & \ddots & & & \ddots \\ & & & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) \\ & g_s(\mathbf{a}) & \dots & g_0(\mathbf{a}) & & & & \\ & & g_s(\mathbf{a}) & \dots & g_0(\mathbf{a}) & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & & g_s(\mathbf{a}) & \dots & g_0(\mathbf{a}) \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix}$$

$$= f_n(\mathbf{a})^{m-s} \det\begin{pmatrix} f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & & \\ & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) & \\ & & \ddots & \ddots & & & \ddots \\ & & & f_n(\mathbf{a}) & f_{n-1}(\mathbf{a}) & \dots & \dots & f_0(\mathbf{a}) \\ g_s(\mathbf{a}) & g_{s-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) & & & \\ & g_s(\mathbf{a}) & g_{s-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) & \\ & & \ddots & \ddots & & & \ddots \\ & & & g_s(\mathbf{a}) & g_{s-1}(\mathbf{a}) & \dots & \dots & g_0(\mathbf{a}) \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m-s \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix}$$

$$= f_n(\mathbf{a})^{m-s} \mathrm{res}\big(f(\mathbf{a},t), g(\mathbf{a},t)\big).$$

□

Dans la proposition 2.2.4, on note $\pi : \overline{\mathbb{K}}^{d+1} \to \overline{\mathbb{K}}^{d}$ la projection sur les n premières composantes :

$$\begin{aligned} \pi : \quad \overline{\mathbb{K}}^{d+1} &\to \overline{\mathbb{K}}^{d} \\ (a_1, \dots, a_d, b) &\mapsto (a_1, \dots, a_d). \end{aligned}$$

On note différemment la $d+1$-ième coordonnée de $\overline{\mathbb{K}}^{d+1}$ dans la mesure où elle correspond à la variable éliminée.

Proposition 2.2.4. *Soient $f, g \in \mathbb{K}[x_1, \dots, x_d, t]$ de degrés respectifs n et m en t,* i.e., *$f = f_n t^n + \dots + f_0$ et $g = g_m t^m + \dots + g_0$, avec $f_k, g_k \in \mathbb{K}[x_1, \dots, x_d]$ et $f_n g_m \neq 0$. On a :*

$$Z\big(\mathrm{res}_t(f,g)\big) = \pi\Big(Z(f) \cap Z(g)\Big) \cup \Big(Z(f_n) \cap Z(g_m)\Big). \tag{2.1}$$

Démonstration. On montre (2.1) par double inclusion.

$\subseteq$ **:** Soit $\mathbf{a} = (a_1, \ldots, a_d) \in Z\big(\mathrm{res}_t(f,g)\big)$. Il suffit de montrer que si $\mathbf{a}$ n'appartient pas à $Z(f_n) \cap Z(g_m)$, alors $\mathbf{a} \in \pi\big(Z(f) \cap Z(g)\big)$. On suppose sans perte de généralité que $\mathbf{a} \notin Z(f_n)$, de sorte que $f_n(\mathbf{a}) \neq 0$ et $\deg\big(f(\mathbf{a}, t)\big) = n$. En notant $s = \deg\big(g(\mathbf{a}, t)\big)$, on a d'après le lemme 2.2.3 et la condition $\mathbf{a} \in Z\big(\mathrm{res}_t(f,g)\big)$:

$$f_n(\mathbf{a})^{m-s}\,\mathrm{res}\big(f(\mathbf{a}, t), g(\mathbf{a}, t)\big) \;=\; 0.$$

Ainsi $\mathrm{res}\big(f(\mathbf{a}, t), g(\mathbf{a}, t)\big) = 0$ et d'après le théorème 2.1.3, on en déduit que $f(\mathbf{a}, t)$ et $g(\mathbf{a}, t)$ ont un facteur commun et donc qu'il existe $b \in \overline{\mathbb{K}}$ tel que $f(\mathbf{a}, b) = g(\mathbf{a}, b) = 0$. On a donc $(\mathbf{a}, b) \in Z(f) \cap Z(g)$, de sorte que $\mathbf{a} = \pi(\mathbf{a}, b)$ est bien dans $\pi\big(Z(f) \cap Z(g)\big)$.

$\supseteq$ **:** On commence par rappeler que d'après la proposition 2.2.2, on a une égalité $Af + Bg = \mathrm{res}_t(f,g)$, avec $A, B \in \mathbb{K}[x_1, \ldots, x_d, t]$ de degrés respectifs en t strictement inférieurs à m et n. Soit $\mathbf{a} \in \pi\big(Z(f) \cap Z(g)\big)$, de sorte qu'il existe $b \in \overline{\mathbb{K}}$, tel que $f(\mathbf{a}, b) = g(\mathbf{a}, b) = 0$. En évaluant en $(\mathbf{a}, b)$ l'égalité $Af + Bg = \mathrm{res}_t(f,g)$, on obtient que $\mathrm{res}_t(f,g)(\mathbf{a}) = 0$, *i.e.*, $\mathbf{a} \in Z\big(\mathrm{res}_t(f,g)\big)$, ce qui montre que $\pi\big(Z(f) \cap Z(g)\big)$ est inclus dans $Z\big(\mathrm{res}_t(f,g)\big)$. Maintenant, si $\mathbf{a} \in Z(f_n) \cap Z(g_m)$, on revient à la définition du résultant pour montrer que $\mathrm{res}_t(f,g)(\mathbf{a}) = 0$. Par définition, $\mathrm{res}_t(f,g)$ est le déterminant de la matrice

$$\begin{pmatrix} f_n & \cdots & \cdots \\ 0 & \cdots & \cdots \\ \vdots & \cdots & \cdots \\ g_m & \cdots & \cdots \\ 0 & \cdots & \cdots \\ \vdots & \cdots & \cdots \end{pmatrix}$$

Puisque $\mathbf{a} \in Z(f_n) \cap Z(g_m)$, la première colonne de la matrice de Sylvester évaluée en $\mathbf{a}$ est nulle, donc le déterminant de cette matrice, qui n'est rien d'autre que $\mathrm{res}_t(f,g)(\mathbf{a})$, s'annule. Ainsi, $\mathbf{a} \in Z\big(\mathrm{res}_t(f,g)\big)$, et donc $Z(f_n) \cap Z(g_m)$ est inclus dans $Z\big(\mathrm{res}_t(f,g)\big)$.

□

La proposition 2.2.4 est un cas particulier de [1, Théorème 3.2.2], qui étend le résultat au cas où on s'intéresse à l'intersection des zéros de plus de deux polynômes. Dans les exemples de ce cours, on traite principalement le cas de deux polynômes. On remarque que dans le cas où $f(x,y)$ et $g(x,y)$ sont des polynômes de deux variables, la proposition 2.2.4 a une interprétation géométrique portant sur l'intersection des deux courbes planes d'équations $f(x,y) = 0$ et $g(x,y) = 0$. Cela est l'objet du corollaire suivant, prouvé en prenant successivement y puis x comme variable à éliminer.

Corollaire 2.2.5. *Soient les deux polynômes en deux variables*

$$f(x,y) \;=\; \sum_{k=0}^{n} f_k(x)\,y^k, \qquad g(x,y) \;=\; \sum_{k=0}^{m} g_k(x)\,y^k,$$

où $f_n(x)\,g_m(x) \neq 0$, et soit $a \in \overline{\mathbb{K}}$. Si a est racine de $\mathrm{res}_y(f,g)$ *et que a n'est pas un zéro commun de $f_n(x)$ et $g_m(x)$, alors a est l'abscisse d'un point de $Z(f) \cap Z(g)$. Réciproquement, si a est l'abscisse d'un point dans l'intersection alors c'est une racine de* $\mathrm{res}_y(f,g)$.

De plus, on note

$$f(x,y) \;=\; \sum_{k=0}^{n'} f'_k(y)\,x^k, \qquad g(x,y) \;=\; \sum_{k=0}^{m'} g'_k(y)\,x^k,$$

où $f'_{n'}(y)\,g'_{m'}(y) \neq 0$, et soit $b \in \overline{\mathbb{K}}$. Si b est racine de $\mathrm{res}_x(f,g)$ *et que b n'est pas un zéro commun de $f'_{n'}(y)$ et $g'_{m'}(y)$, alors b est l'ordonnée d'un point de $Z(f) \cap Z(g)$. Réciproquement, si b est l'abscisse d'un point dans l'intersection alors c'est une racine de* $\mathrm{res}_y(f,g)$.

On illustre maintenant la proposition 2.2.4 et le corollaire 2.2.5 avec des exemples.

Exemple 2.2.6. Cet exemple est issu de [1, Chapitre 3.1] : on considère $\mathbb{K} = \mathbb{Q}$, $d = 2$, on note $x = x_1$ et $y = x_2$ et soient

$$f(x,y,t) \;=\; xt - 1 \qquad g(x,y,t) \;=\; yt - 1.$$

On prend t comme variable à éliminer et on a $\deg_t(f) = \deg_t(g) = 1$. De plus, on a

$$\mathrm{res}_t(f,g) \;=\; \det\begin{pmatrix} x & -1 \\ y & -1 \end{pmatrix} \;=\; y - x.$$

Les zéros de $\mathrm{res}_t(f,g)$ dans $\overline{\mathbb{Q}}^2$ sont donc de la forme (a,a), avec $a \in \overline{\mathbb{Q}}$. On remarque ici que les coefficients dominants $f_1(x,y) = x$ et $g_1(x,y) = y$ ont un unique zéro commun $(0,0)$, *i.e.*, $Z(f_1) \cap Z(g_1) = \{(0,0)\}$. De plus, tous les autres couples (a,a) avec $a \neq 0$ sont bien dans $\pi\big(Z(f) \cap Z(g)\big)$ puisque $Z(f) \cap Z(g)$ est l'ensemble des points de la forme $(a, a, 1/a)$ avec $a \neq 0$.

Exemple 2.2.7. On cherche à déterminer l'intersection des deux courbes planes d'équations $f(x,y) = 0$ et $g(x,y) = 0$, où

$$f(x,y) \;=\; 2x^2 + y^2 + 3xy - 2x - y \qquad \text{et} \qquad g(x,y) \;=\; 3x^2 + 2y^2 + 6xy.$$

On vérifie que

$$\mathrm{res}_y(f,g) \;=\; \det\begin{pmatrix} 1 & 3x-1 & 2x^2-2x & 0 \\ 0 & 1 & 3x-1 & 2x^2-2x \\ 2 & 6x & 3x^2 & 0 \\ 0 & 2 & 6x & 3x^2 \end{pmatrix} \qquad \mathrm{res}_x(f,g) \;=\; \det\begin{pmatrix} 2 & 3y-2 & y^2-y & 0 \\ 0 & 2 & 3y-2 & y^2-y \\ 3 & 6y & 2y^2 & 0 \\ 0 & 3 & 6y & 2y^2 \end{pmatrix}$$

$$=\; x^2(x^2-2x-2) \qquad\qquad =\; y^2(y^2-3).$$

On remarque que les coefficients de plus hauts degrés en x et y de $f(x,y)$ et de $g(x,y)$ sont tous des polynômes constants. Ainsi, les racines de $\mathrm{res}_y(f,g)$ et de $\mathrm{res}_x(f,g)$ sont respectivement les abscisses et les ordonnées des points d'intersection des deux courbes. Les zéros de $\mathrm{res}_y(f,g)$ sont 0, qui est racine double, et $1 \pm \sqrt{3}$ et ceux de $\mathrm{res}_x(f,g)$ sont 0, également racine double et $\pm\sqrt{3}$. On procède maintenant par analyse de cas :

- si $x = 0$, on montre que le seul $y \in \{0, \pm\sqrt{3}\}$ tel que $f(x,y) = g(x,y) = 0$ est $y = 0$,
- si $x = 1 + \sqrt{3}$, on montre que le seul $y \in \{0, \pm\sqrt{3}\}$ tel que $f(x,y) = g(x,y) = 0$ est $y = -\sqrt{3}$,
- si $x = 1 - \sqrt{3}$, on montre que le seul $y \in \{0, \pm\sqrt{3}\}$ tel que $f(x,y) = g(x,y) = 0$ est $y = \sqrt{3}$

Ainsi, l'intersection $Z(f) \cap Z(g)$ est composée des trois points $(0,0), (1+\sqrt{3}, -\sqrt{3}), (1-\sqrt{3}, \sqrt{3})$.

Avec les deux exemples précédents, on voit que l'élimination de variables est étroitement liée à la résolution de systèmes polynomiaux. On verra plus explicitement dans le chapitre 4 comment la généralisation [1, Théorème 3.2.2] de la proposition 2.2.4 et les bases de Gröbner permettent d'aborder le problème de résolution de tels systèmes sous un angle algorithmique.

Chapitre 3 :

Bases de Gröbner

3.1. Division euclidienne dans $\mathbb{K}[x]$

Afin de motiver les bases de Gröbner, on commence par rappeler le fonctionnement de l'algorithme de division euclidienne dans l'algèbre des polynômes $\mathbb{K}[x]$ en une variable à coefficients dans un corps. Cet algorithme permet, étant donnés deux polynômes $p(x), d(x) \in \mathbb{K}[x]$, de décider si $d(x)$ divise $p(x)$, *i.e.*, si $p(x)$ appartient à $I(d(x))$, ou bien de calculer un représentant canonique de la classe de $p(x)$ dans l'algèbre quotient $\mathbb{K}[x]/I(d(x))$. Les bases de Gröbner permettent de traiter le même type de problèmes dans le cas où on considère des polynômes à plusieurs variables.

On note respectivement n et m les degrés de $p(x)$ et $d(x)$:

$$p(x) = \sum_{k=0}^{n} p_k x^k, \qquad d(x) = \sum_{k=0}^{m} d_k x^k, \qquad p_k, d_k \in \mathbb{K}, \qquad p_n d_m \neq 0.$$

L'algorithme de division euclidienne consiste à supprimer les monômes de degrés strictement supérieurs à m dans $p(x)$ en les remplaçant par $\left(-d^{m-1}x^{m-1} - \cdots - d_0\right)/d_n$. En notant $q(x)$ le quotient et $r(x)$ le reste, on a

$$p(x) = q(x)d(x) + r(x), \qquad \deg(r(x)) < \deg(d(x)).$$

On illustre le fonctionnement de l'algorithme d'Euclide avec un exemple. La façon dont on va traiter cet exemple ne consiste pas à poser la division euclidienne mais à supprimer itérativement les puissances de x supérieures au degré du diviseur. C'est en effet cette méthode que l'on utilisera dans l'algorithme de division multivariée.

Exemple 3.1.1. On considère $\mathbb{K} = \mathbb{Q}$, $n = 5, m = 3$ et

$$p(x) = 3x^5 - 5x^4 + 5x - 3, \qquad d(x) = 2x^3 + x + 1.$$

Pour effectuer la division euclidienne, on part de $p(x)$ et on élimine successivement les puissances supérieures à $m = 3$ grâce à $d(x)$:

$$\begin{aligned} p(x) &= \frac{3}{2}x^2 d(x) - 5x^4 - \frac{3}{2}x^3 - \frac{3}{2}x^2 + 5x - 3 \\ &= \left(\frac{3}{2}x^2 - \frac{5}{2}x\right) d(x) - \frac{3}{2}x^3 + x^2 + \frac{15}{2}x - 3 \\ &= \left(\frac{3}{2}x^2 - \frac{5}{2}x - \frac{3}{4}\right) d(x) + x^2 + \frac{33}{4}x - \frac{9}{4} \end{aligned}$$

La première égalité provient du fait qu'on a éliminé le $3x^5$ de $p(x)$ en multipliant $d(x)$ par $3/2x^2$, la deuxième du fait qu'on a éliminé le $-5x^4$ en multipliant $d(x)$ par $-5/2x$ et la dernière du fait qu'on a éliminé le $-3/2x^3$ en multipliant $d(x)$ par $-3/4$. Enfin, la dernière égalité ne contient plus de puissances supérieures à 3 dans le reste et donc l'algorithme est fini. En résumé, on obtient le quotient $q(x)$ et le reste $r(x)$:

$$q(x) = \frac{3}{2}x^2 - \frac{5}{2}x - \frac{3}{4}, \qquad r(x) = x^2 + \frac{33}{4}x - \frac{9}{4}.$$

À partir du reste $r(x)$, on peut conclure les choses suivantes :

- $r(x)$ étant non nul, on en déduit que $p(x)$ n'appartient pas à l'idéal engendré par $d(x)$.
- L'algèbre quotient $\mathbb{K}[x]/I(d(x))$ est un espace vectoriel de dimension 3 dont une base est donnée par les classes des monômes $1, x, x^2$ modulo $I(d(x))$. Relativement à cette base, la classe de $p(x)$ a pour coordonnées $(-9/4, 33/4, 1)$.

3.2. Division multivariée dans $\mathbb{K}[x_1, \ldots, x_d]$

On se place maintenant dans $\mathbb{K}[x_1, \ldots, x_d]$. Comme précédemment, un polynôme $f(x_1, \ldots, x_d)$ est simplement noté f. Soit une famille de polynômes $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_d]$ engendrant l'idéal $I(f_1, \ldots, f_s)$. Ces polynômes doivent être pensés comme des diviseurs, *i.e.*, on cherche à étendre l'algorithme de division euclidienne en un algorithme de division multivariée d'un $f \in \mathbb{K}[x_1, \ldots, x_d]$ par $f_1, \ldots, f_s$. En se basant sur ce que l'on a vu pour les polynômes en une variable, on souhaite notamment que cet algorithme permette de répondre aux deux questions suivantes :

- Est-ce que f appartient à l'idéal $I(f_1, \ldots, f_s)$?
- Si f n'appartient pas à $I(f_1, \ldots, f_s)$, peut on exprimer la décomposition, relativement à une base bien choisie, de sa classe dans $\mathbb{K}[x_1, \ldots, x_d]/I(f_1, \ldots, f_s)$?

Contrairement au cas une variable où les monômes x^k sont ordonnées par la valeur de l'exposant, il n'existe pas d'ordre naturel sur les monômes en plusieurs variables. Or, on a vu que l'algorithme de division euclidienne consiste précisément à éliminer les monômes de degrés supérieurs à celui du monôme de plus haut degré du diviseur. Ainsi, avant d'introduire la division multivariée, on a besoin de considérer des ordres particuliers sur les monômes, que l'on appelle ordres monomiaux.

Définition 3.2.1. Un *ordre monomial* sur l'ensemble $[x_1, \ldots, x_d]$ des monômes est un ordre total $\prec$ sur $[x_1, \ldots, x_d]$ vérifiant les deux propriétés suivantes :

- le monôme 1 est minimal, *i.e.*, pour tout $m \in [x_1, \ldots, x_d] \setminus \{1\}$, on a $1 \prec m$
- $\prec$ est compatible à l'opération de multiplication monomiale, *i.e.*,

$$\forall m_1, m_2, m \in [x_1, \ldots, x_d] : \qquad m_1 \prec m_2 \quad \Rightarrow \quad mm_1 \prec mm_2.$$

Tout polynôme non nul $f \in \mathbb{K}[x_1, \ldots, x_d]$ admet donc un *monôme dominant* $\mathrm{lm}_\prec(f)$ (pour *leading monomial*) et un *coefficient dominant* $\mathrm{lc}_\prec(f)$ (pour *leading coefficient*) définis respectivement comme étant le plus grand élément de $\mathrm{supp}(f)$ relativement à $\prec$ et comme étant le coefficient de $\mathrm{lm}_\prec(f)$ dans f. Ainsi, f s'écrit sous la forme :

$$f \quad = \quad \mathrm{lc}_\prec(f)\,\mathrm{lm}_\prec(f) \quad + \quad \text{une combinaison linéaire de monômes inférieurs à } \mathrm{lm}_\prec(f).$$

Enfin, pour une partie $S \subseteq \mathbb{K}[x_1, \ldots, x_d]$, on note $\mathrm{lm}_\prec(S)$ l'ensemble des monômes dominants des éléments de S :

$$\mathrm{lm}_\prec(S) = \Big\{ \mathrm{lm}_\prec(f) \mid f \in S \Big\}.$$

Afin d'alléger les notations, on ne note pas la dépendance relative à $\prec$ dans la suite : on note simplement $\mathrm{lm}(f), \mathrm{lc}(f)$ et $\mathrm{lm}(S)$ respectivement le monôme et le coefficient dominant de $f \in \mathbb{K}[x_1, \ldots, x_d]$ et l'ensemble des monômes dominants de $S \subseteq \mathbb{K}[x_1, \ldots, x_d]$. On donne maintenant des exemples d'ordres monomiaux, appelés ordres *lex* et *deglex*. En pratique, lorsque l'on s'intéressera à la résolution de systèmes polynomiaux on travaillera avec d'autres ordres, dits d'élimination, que l'on introduira dans la suite.

Exemple 3.2.2.

1. On considère deux monômes $m = x_1^{\alpha_1} \ldots x_d^{\alpha_d}$ et $m' = x_1^{\beta_1} \ldots x_d^{\beta_d}$. Alors m est plus petit que m' pour l'ordre lex s'il existe $1 \leq i \leq n$ tel que $\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}$ et $\alpha_i < \beta_i$. On remarque que l'ordre lex est analogue à l'ordre utilisé pour classé les mots dans un dictionnaire, d'où son nom : lex étant le diminutif de lexicographique. Par exemple, pour $d = 3$, en notant $x_1 = x, x_2 = y$ et $x_3 = z$ et en notant $\prec$ l'ordre lex, alors on a $y^3 z^4 \prec xy^2$ et $x^3 y^4 z \prec x^3 y^4 z^2$.
2. On considère deux monômes m et m'. Alors m est plus petit que m' pour l'ordre deglex si on a $\deg(m) < \deg(m')$ ou si $\deg(m) = \deg(m')$ et m est plus petit que m' pour l'ordre lex. Le nom deglex vient du fait que les monômes sont d'abord comparés par degrés puis par ordre lex. Par exemple, pour $d = 3$, en notant $x_1 = x, x_2 = y$ et $x_3 = z$ et en notant $\prec$ l'ordre deglex, on a :

$$1 \prec z \prec y \prec x \prec zz \prec yz \prec yy \prec xz \prec xy \prec xx \prec \ldots.$$

Dans la suite, lorsqu'on travaille avec les variables x, y, z plutôt qu'avec des x_i, on parle d'ordre (deg)lex induit par un ordre sur les générateurs. Par exemple, l'ordre (deg)lex induit par $z \prec y \prec x$ est l'ordre (deg)lex pour $x_1 = x, x_2 = y, x_3 = z$.

On passe maintenant passer à l'algorithme de division multivariée de $f \in \mathbb{K}[x_1, \ldots, x_d]$ par une famille de polynômes $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_d]$. Cet algorithme consiste à éliminer les monômes apparaissant dans f qui sont divisibles par un monôme dominant d'un des $\mathrm{lm}(f_i)$ avec $1 \leq i \leq s$, en remplaçant $\mathrm{lm}(f_i)$ par $\Big(\mathrm{lm}(f_i) - f_i\Big)/\mathrm{lc}(f_i)$. Voici les étapes de cet algorithme.

1. On pose $p = f$ et $g_1 = \cdots = g_s = 0$.
2. Tant qu'il existe $m \in \mathrm{supp}(p)$ divisible par un $\mathrm{lm}(f_i)$, avec $1 \leq i \leq s$, et en notant c le coefficient de m dans p, on pose
$$p \;=\; p - \frac{cm}{\mathrm{lc}(f_i)\,\mathrm{lm}(f_i)} f_i, \qquad g_i \;=\; g_i + \frac{cm}{\mathrm{lc}(f_i)\,\mathrm{lm}(f_i)}$$
si bien que le monôme m ne figure plus dans p.
3. Une fois que tous les monômes de $\mathrm{supp}(p)$ ne sont divisibles par aucun des $\mathrm{lm}(f_i)$, l'algorithme est fini.

À chaque itération de la deuxième étape de l'algorithme on a $f = f_1 g_1 + \cdots + f_s g_s + p$, de sorte qu'on obtient le résultat suivant.

Proposition 3.2.3 ([1, Théorème 2.3.3])**.** *En reprenant les notations précédentes, et en notant r la dernière valeur de p obtenue, on a une décomposition :*

$$f \;=\; f_1 g_1 + \cdots + f_s g_s + r.$$

En particulier, si $r = 0$, alors f est dans $I(f_1, \ldots, f_s)$.

Le polynôme r de la proposition précédente est appelé *un reste* de f dans la division multivariée par $f_1, \ldots, f_s$. On illustre le fonctionnement de l'algorithme sur un exemple.

Exemple 3.2.4. Soient les polynômes de $\mathbb{Q}[x,y]$:

$$f_1(x,y) = xy - x - y, \quad f_2(x,y) = 2x^2 - y^2 - x, \quad f(x,y) = 3x^2y - x.$$

On effectuve la division multivariée de $f(x,y)$ par rapport à $f_1(x,y)$, $f_2(x,y)$ relativement à l'ordre deglex induit par $y \prec x$. On commence en posant $p(x,y) = f(x,y)$ et $g_1(x,y) = g_2(x,y) = 0$. On remarque que le monôme $x^2y \in \text{supp}(p)$ est divisible par $\text{lm}(f_1) = xy$ et que le quotient de ces deux monômes est x. On pose donc

$$p(x,y) = p(x,y) - 3xf_1(x,y) = 3x^2 + 3xy - x, \qquad g_1(x,y) = 3x.$$

Maintenant, le monôme $x^2 \in \text{supp}(p)$ est égal à $\text{lm}(f_2)$ et donc on pose :

$$p(x,y) = p(x,y) - \frac{3}{2}f_2(x,y) = 3xy + \frac{3}{2}y^2 + \frac{1}{2}x, \qquad g_2 = \frac{3}{2}.$$

Enfin, $xy \in \text{supp}(p)$ est égal à $\text{lm}(f_1)$ et donc on pose :

$$p(x,y) = p(x,y) - 3f_1(x,y) = \frac{3}{2}y^2 + \frac{7}{2}x + 3y, \qquad g_1 = g_1 + 3 = 3x + 3.$$

La dernière valeur de p obtenue ne contient aucun monôme divisible par $\text{lm}(f_1)$ ou $\text{lm}(f_2)$ de sorte que

$$r(x,y) = \frac{3}{2}y^2 + \frac{7}{2}x + 3y.$$

On observe qu'on a bien la décomposition $f(x,y) = f_1(x,y)g_1(x,y) + f_2(x,y)g_2(x,y) + r(x,y)$.

On peut observer que le monôme x^2y dans la première division de l'exemple précédent était en fait à la fois divisible par $\text{lm}(f_1)$ et $\text{lm}(f_2)$. On a choisi de faire la division par $\text{lm}(f_1)$, mais au vu de l'algorithme de division multivariée, on aurait pu faire la division par $\text{lm}(f_2)$. On regarde ce qu'il advient en procédant ainsi.

Exemple 3.2.5. On rerend $f_1(x,y) = xy - x - y$, $f_2(x,y) = 2x^2 - y^2 - x$ et $f(x,y) = 3x^2y - x$ et l'ordre deglex induit par $y \prec x$. On choisit cette fois-ci d'éliminer $3x^2y$ grâce à $(3/2)yf_2(x,y)$, *i.e.*, on pose

$$p(x,y) = f(x,y) - \frac{3}{2}yf_2(x,y) = \frac{3}{2}y^3 + \frac{3}{2}xy - x, \qquad g_2(x,y) = \frac{3}{2}y.$$

On élimine $(3/2)xy$ grâce à $3f_1(x,y)$:

$$p(x,y) = p(x,y) - 3f_1(x,y) = \frac{3}{2}y^3 + \frac{1}{2}x + \frac{3}{2}y, \qquad g_1(x,y) = \frac{3}{2}.$$

Maintenant, $p(x,y)$ ne contient aucun monôme divisible par $\text{lm}(f_1)$ ou $\text{lm}(f_2)$ de sorte qu'il s'agit de notre reste :

$$r(x,y) = \frac{3}{2}y^3 + \frac{1}{2}x + \frac{3}{2}y.$$

À la vue des deux exemples précédents, on voit que le reste de la division multivariée dépend des diviseurs que l'on choisit au moment d'éliminer les monômes. On considère comme autre exemple celui de [1, Exemple 2.3.5] : on prend $f_1(x,y) = xy + 1$, $f_2(x,y) = y^2 - 1$, $f(x,y) = xy^2 - x$ et l'ordre deglex induit par $y \prec x$. En éliminant d'abord xy^2 grâce à $f_1(x,y)$, on peut vérifier qu'on obtient le reste $r(x,y) = -x - y$, alors qu'en utilisant $f_2(x,y)$, on obtient $r(x,y) = 0$. Ainsi, en utilisant la deuxième division, on observe que $f(x,y)$ est dans l'idéal engendré par $f_1(x,y)$ et $f_2(x,y)$, ce que l'on ne peut pas conclure grâce à la première division. Les bases de Gröbner sont précisément les ensembles générateurs d'idéaux pour lesquels le choix du polynôme dans l'élimination de monômes dominants n'influe pas sur la valeur du reste. On verra qu'en particulier, la division multivariée induite par une base de Gröbner permet de décider si un polynôme appartient à un idéal.

3.3. Définition des bases de Gröbner et lemme de Dickson

Dans cette section, on fixe un idéal $I \subseteq \mathbb{K}[x_1,\dots,x_d]$ ainsi qu'un ordre monomial $\prec$ sur $[x_1,\dots,x_d]$. Comme précédemment, on n'indique pas explicitement les dépendances relativement à ce ordre.

Définition 3.3.1. Une partie G de I est appelée une *base de Gröbner* relativement à $\prec$ si pour tout $f \in I$ non nul, il existe $g \in G$ tel que $\mathrm{lm}(g)$ divise $\mathrm{lm}(f)$.

La définition peut être reformulée en termes d'*idéaux monomiaux*, un tel idéal monomial étant une partie J de $[x_1,\dots,x_d]$ telle que pour tout $m \in J$ et tout $m' \in [x_1,\dots,x_d]$, on a $mm' \in J$. On note qu'étant donné un idéal I de $\mathbb{K}[x_1,\dots,x_d]$, l'ensemble $\mathrm{lm}(I)$ est toujours un idéal monomial : étant donnés $m \in \mathrm{lm}(I)$ et $m' \in [x_1,\dots,x_d]$, alors il existe $f \in I$ tel que $m = \mathrm{lm}(f)$, si bien que $mm' = \mathrm{lm}(m'f)$ est dans $\mathrm{lm}(I)$ car $m'f \in I$. Dire qu'une partie G de I est une base de Gröbner signifie que l'idéal monomial $\langle \mathrm{lm}(G)\rangle$ engendré par $\mathrm{lm}(G)$ est précisément égal à $\mathrm{lm}(I)$. De plus, on note $\mathrm{nf}(G)$ (pour *normal form*, qui est le nom donné aux monômes ne pouvant pas être éliminés par G) l'ensemble des monômes qui ne sont divisibles par aucun élément de $\mathrm{lm}(G)$, *i.e.*,

$$\mathrm{nf}(G) \;=\; [x_1,\dots,x_d] \setminus \langle \mathrm{lm}(G)\rangle.$$

On remarque que G est une base de Gröbner de I si et seulement si $[x_1,\dots,x_d] = \mathrm{lm}(I) \sqcup \mathrm{nf}(G)$, où $\sqcup$ est l'opérateur d'union disjointe.

La première utilité des bases de Gröbner est que le reste de la division multivariée relativement à une telle base est unique, *i.e.*, il ne dépend pas des polynômes choisis pour éliminer des monômes dominants. De plus, elles permettent de décider le problème d'appartenance à I, de déterminer des bases naturelles de $\mathbb{K}[x_1,\dots,x_d]/I$ et un algorithme pour calculer la décomposition de la classe d'un polynôme $f \in \mathbb{K}[x_1,\dots,x_d]$ modulo I relativement à cette base. Enfin, on donnera plus tard des exemples d'applications portant sur la cryptographie et l'optimisation sous contrainte.

Proposition 3.3.2 ([1, Proposition 2.6.1])**.** *Soient I un idéal de $\mathbb{K}[x_1,\dots,x_d]$, $\prec$ un ordre monomial sur $[x_1,\dots,x_d]$ et G une base de Gröbner de I relativement à $\prec$.*

1. *Chaque $f \in \mathbb{K}[x_1,\dots,x_d]$ admet un unique reste dans la division multivariée par G. De plus, f appartient à I si et seulement si son reste est nul, de sorte que G est une partie génératrice de I.*
2. *En tant qu'espace vectoriel, l'algèbre $\mathbb{K}[x_1,\dots,x_d]/I$ a pour base les classes des élément de $\mathrm{nf}(G)$. De plus, les coefficients du reste d'un polynôme f sont les coordonnées de la classe de f modulo I relativement à cette base.*

Démonstration. On montre le premier point. Soient deux restes r_1 et r_2 d'un même $f \in \mathbb{K}[x_1,\dots,x_d]$ relativement à la division par G. Il existe des polynômes $g_1,\dots,g_s \in G$ et $f_1,\dots,f_s,h_1,\dots,h_s \in \mathbb{K}[x_1,\dots,x_d]$ tels que

$$f \;=\; g_1f_1+\cdots+g_sf_s+r_1 \;=\; g_1h_1+\cdots+g_sh_s+r_2$$

si bien que $r_1-r_2 = g_1(h_1-f_1)+\cdots+g_s(h_s-f_s)$ est un élément de I, qui de plus est une combinaison linéaire de monômes dans $\mathrm{nf}(G)$. Puisque G est une base de Gröbner, on en déduit que $r_1-r_2=0$, ce qui montre l'unicité du reste. De plus, si ce reste vaut 0 alors $f \in I$, et réciproquement si ce reste est non nul alors ce n'est pas un élément de I car son monôme dominant est dans $\mathrm{nf}(G)$. On montre maintenant le deuxième point. Par définition du reste, un polynôme $f \in \mathbb{K}[x_1,\dots,x_d]$ est dans la même classe que son reste modulo I. Or ce reste est une combinaison linéaire de monômes dans $\mathrm{nf}(G)$, de sorte que les classes de ces monômes forment une famille génératrice de $\mathbb{K}[x_1,\dots,x_d]/I$. Pour montrer que cette famille est libre, soit une combinaisons linéaire $\lambda_1m_1+\cdots+\lambda_nm_n$ avec $m_k \in \mathrm{nf}(G)$ et qui vaut 0 dans $\mathbb{K}[x_1,\dots,x_d]/I$, *i.e.*, telle que cette combinaison est un élément de I. Si l'un des coefficients était non nul, alors cette combinaison aurait un monôme dominant qui ne serait pas dans $\langle \mathrm{lm}(G)\rangle$, ce qui contredit l'hypothèse que G est une base de Gröbner. La deuxième phrase du deuxième point est simplement une conséquence du fait que f est égal à son reste modulo I. □

On finit cette section par le lemme de Dickson et une de ses conséquences qui est un résultat d'existence de bases de Gröbner finies de I.

Théorème 3.3.3 (Lemme de Dickson [1, Théorème 2.4.5])**.** *Tout idéal monomial est de type fini.*

Théorème 3.3.4 (Théorème de base de Hilbert [1, Corollaire 2.5.6])**.** *Étant donné un ordre monomial $\prec$ sur $[x_1,\dots,x_d]$, tout idéal I de $\mathbb{K}[x_1,\dots,x_d]$ admet une base de Gröbner finie relativement à $\prec$. En particulier, tout idéal de $\mathbb{K}[x_1,\dots,x_d]$ est de type fini.*

Démonstration. D'après le lemme de Dickson, $\mathrm{lm}(I)$ est de type fini, de sorte qu'il existe une partie finie G de I telle que $\mathrm{lm}(G)$ engendre $\mathrm{lm}(I)$, *i.e.*, G est une base de Gröbner finie de I. La deuxième assertion découle du premier point de la proposition 3.3.2. □

3.4. S-polynômes et algorithme de Buchberger

Jusqu'à présent, on a vu que tout idéal admet une base de Gröbner finie et que celles-ci permettent de traiter algorithmiquement les deux problèmes donnés en guise de motivations : le test d'appartenance à l'idéal et le calcul de représentants dans le quotient de $\mathbb{K}[x_1,\dots,x_d]$ par un idéal. Avant de s'intéresser à des applications portant sur d'autres domaines que l'algèbre, deux questions fondamentales d'un point de vue algorithmique subsistent :

- comment tester qu'une partie donnée est une base de Gröbner ?
- comment construire une base de Gröbner à partir d'une partie génératrice d'un idéal ?

Les réponses à ces deux questions reposent sur les S-polynômes. Dans toute la section, on fixe un ordre monomial $\prec$.

Définition 3.4.1. Soient $f,g \in \mathbb{K}[x_1,\dots,x_d]$ et soit m le plus petit commun multiple de $\mathrm{lm}(f)$ et $\mathrm{lm}(g)$. Le *S-polynôme* de f et g est le polynôme

$$\mathrm{spol}(f,g) \;=\; \frac{m}{\mathrm{lc}(f)\,\mathrm{lm}(f)}f - \frac{m}{\mathrm{lc}(g)\,\mathrm{lm}(g)}g.$$

Le S de S-polynôme signifie soustraction car $\mathrm{spol}(f,g)$ est défini par soustraction de deux polynômes. On peut à présent donner une caractérisation effective des bases de Gröbner.

Théorème 3.4.2 (Critère de Buchberger [1, Théorème 2.6.6])**.** *Soient I un idéal de $\mathbb{K}[x_1,\dots,x_d]$, G une partie de I et $\prec$ un ordre monomial. Alors G est une base de Gröbner de I si et seulement si pour tout $g,g' \in G$, le S-polynôme $\mathrm{spol}(g,g')$ a un reste nul dans la division multivariée par G.*

On peut à présent donner des exemples d'illustration du critère de Buchberger.

Exemple 3.4.3. On donne d'abord un exemple de base de Gröbner puis ensuite d'un ensemble qui n'est pas une base de Gröbner.

1. On considère l'exemple provenant de [1, Section 2.6] : $G = \{g_1(x,y,z), g_2(x,y,z)\}$ avec

$$g_1(x,y,z) \;=\; y - x^2, \qquad g_2(x,y,z) \;=\; z - x^3,$$

et $\prec$ est l'ordre lex induit par $x \prec z \prec y$. On a $\mathrm{ppcm}(\mathrm{lm}(g_1),\mathrm{lm}(g_2)) = \mathrm{ppcm}(y,z) = yz$, de sorte que

$$\mathrm{spol}(g_1,g_2) \;=\; \frac{yz}{y}g_1 - \frac{yz}{z}g_2 \;=\; -zx^2 + yx^3.$$

Par définition du S-polynôme, celui-ci permet de supprimer le ppcm des monômes dominants. On réduit à présent $\mathrm{spol}(g_1, g_2)$ par G. On pose $p(x,y,z) = -zx^2 + yx^3$ et on élimine $-zx^2$ grâce à $x^2 g_2$:

$$p(x,y,z) \;=\; p(x,y,z) + x^2 g_2(x,y,z) \;=\; -x^5 + x^3 y.$$

Maintenant, on éliminé $x^3 y$ grâce à $x^3 g_1$:

$$p(x,y,z) \;=\; p(x,y,z) - x^3 g_1 \;=\; 0.$$

Ainsi, G est une base de Gröbner de l'idéal qu'il engendre d'après le critère de Buchberger.

2. On reprend comme précédemment $G = \{g_1, g_2\}$, avec $g_1(x,y) = xy - x - y$, $g_2(x,y) = 2x^2 - y^2 - x$, et l'ordre deglex induit par $y \prec x$. Alors, on a $\mathrm{ppcm}(\mathrm{lm}(g_1), \mathrm{lm}(g_2)) = x^2 y$ et

$$\mathrm{spol}(g_1, g_2) \;=\; \frac{x^2 y}{xy} g_1 - \frac{x^2 y}{2x^2} g_2 \;=\; \frac{1}{2} y^3 - x^2 - \frac{1}{2} xy.$$

On effectue la division multivariée de ce S-polynôme par G. On pose $p(x,y) = 1/2\, y^3 - x^2 - 1/2\, xy$ et on élimine le $-x^2$ grâce à $g_2/2$:

$$p(x,y) \;=\; p(x,y) + \frac{1}{2} g_2(x,y) \;=\; \frac{1}{2} y^3 - \frac{1}{2} xy - \frac{1}{2} y^2 - \frac{1}{2} x.$$

Maintenant, on élimine $(-1/2)\, xy$ grâce à $g_1/2$:

$$p(x,y) \;=\; p(x,y) + \frac{1}{2} g_1 \;=\; \frac{1}{2} y^3 - \frac{1}{2} y^2 - x - \frac{1}{2} y.$$

Ce polynôme n'est plus réductible, de sorte qu'on obtient un reste non nul. Si on avait d'abord éliminé $(-1/2)\, xy$ puis $-x^2$, on serait arrivé au même résultat. On déduit du critère de Buchberger que G n'est pas une base de Gröbner de $I(G)$. Il était possible de déduire ce résultat des exemples 3.2.4 et 3.2.5, puisqu'on a vu que le polynôme $f(x,y) = 3x^2 y - x$ admet deux restes différents dans la division par G.

La dernière question à traiter dans cette section est la suivante : étant donnés un idéal I de $\mathbb{K}[x_1, \ldots, x_d]$ engendré par des éléments $f_1, \ldots, f_s$ et un ordre monomial $\prec$, comment peut-on construire une base de Gröbner finie de I ? La réponse est donnée par l'algorithme de Buchberger dont les étapes sont les suivantes.

1. On pose $G = \{f_1, \ldots, f_s\}$.
2. Tant qu'il existe $g, g' \in G$ tels que le reste r de la division de $\mathrm{spol}(g, g')$ est non nul, on ajoute r à G.
3. Une fois que tous les S-polynômes de G ont un reste nul, l'algorithme est fini et G est la base de Gröbner.

Le fait que G est une base de Gröbner provient du critère de Buchberger. De plus, la terminaison de l'algorithme est due au lemme de Dickson car à chaque fois qu'on ajoute un nouveau polynôme r dans G, on fait croitre $\langle \mathrm{lm}(G) \rangle \subseteq \mathrm{lm}(I)$, mais $\mathrm{lm}(I)$ étant de type fini, on ne peut pas rajouter infiniment des générateurs à $\mathrm{lm}(G)$.

Pour finir, on illustre l'algorithme de Buchberger.

Exemple 3.4.4. Soit l'idéal de $\mathbb{Q}[x,y]$ engendré par $G = \{g_1, g_2\}$, avec $g_1(x,y) = x^2 - y$ et $g_2(x,y) = xy - x$, et soit l'ordre $\prec$ deglex induit par $y \prec x$. On a $\mathrm{spol}(g_1, g_2) = x^2 - y^2$ dont le reste est $g_3(x,y) = -y^2 + y$. En rajoutant $g_3(x,y)$ à G, on a un nouveau S-polynôme $\mathrm{spol}(g_2, g_3) = 0$, dont le reste est évidemment 0. Ainsi, $G = \{g_1, g_2, g_3\}$ est une base de Gröbner de l'idéal engendré par $\{g_1, g_2\}$.

Chapitre 4 :

Géométrie algébrique

Dans ce chapitre on s'intéresse aux aspects algorithmiques de la résolution de systèmes polynomiaux. Comme mentionné dans l'introduction, ce problème est étroitement lié à la géométrie : trouver des points d'annulation d'une famille de polynômes revient à trouver les points qui sont dans l'intersection des hypersurfaces définies par ces équations. Avant de s'intéresser à ces aspects algorithmiques, on introduit les variétés algébriques affines et on rappelle deux versions du fameux Nullstellensatz (théorème des zéros de Hilbert en français) ; on aura en particulier un critère en termes d'idéaux garantissant l'existence de solutions d'un système polynomial. Il apparaîtra que les outils introduits dans les sections précédentes (résultants et bases de Gröbner) seront d'une grande utilité pour calculer ou prouver l'existence de solutions à l'aide des idéaux.

4.1. Variétés affines et Nullstellensatz

On fixe un corps $\mathbb{K}$, qui n'est pas supposé algébriquement clos, sauf mention du contraire dans les énoncés des versions faible et forte du Nullstellensatz. Les variétés algébriques affines sont les objets géométriques de l'espace $\mathbb{K}^d$, appelé *espace affine*, définis par des équations polynomiales.

Définition 4.1.1. Étant donnés $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_d]$, on pose

$$V_{\mathbb{K}}(f_1, \ldots, f_r) = \left\{ \mathbf{a} \in \mathbb{K}^d \mid f_1(\mathbf{a}) = \ldots = f_r(\mathbf{a}) = 0 \right\}.$$

L'ensemble $V_{\mathbb{K}}(f_1, \ldots, f_r)$ s'appelle *variété algébrique affine* définie par $f_1, \ldots, f_r$.

Dans la suite, on écrit simplement variété affine au lieu de variété algébrique affine. De plus, on remarque que dans le cas où $\mathbb{K}$ est un corps algébriquement clos, la variété algébrique définie par les polynômes $f_1, \ldots, f_r$ n'est rien d'autre que l'intersection des $Z(f_i)$. Voici quelques exemples de variétés affines :

- des courbes, *e.g.*, un cercle ou une hyperbole, dont les équations sont respectivement $x^2 + y^2 - 1 = 0$ et $xy - 1 = 0$,
- des surfaces, *e.g.*, une sphère ou un cylindre, dont les équations sont respectivement $x^2 + y^2 + z^2 - 1$ et $x^2 + y^2 - z^2 = 0$,
- des objets de plus haute dimension, *e.g.*, l'hypersphère $S^3 \subset \mathbb{R}^4$ d'équation $x^2 + y^2 + z^2 + t^2 - 1 = 0$.

Chacun de ces objets admet une dimension (correspondant au nombre de degré de liberté que l'on a en se déplaçant sur ceux-ci) : 1 pour les courbes, 2 pour les surfaces et 3 pour S^3. La théorie de la dimension des variétés algébriques est basée sur les idéaux, mais on ne l'aborde pas dans ce cours.

On se pose maintenant la question de la consistance d'un système polynomial, *i.e.*, étant donnés des polynômes $f_1, \dots, f_r$, est-ce que le système défini par ces polynômes admet des solutions, ou encore, est-ce que la variété $V_{\mathbb{K}}(f_1, \dots, f_r)$ est non vide ? La réponse à cette question est donnée par la version faible du Nullstellensatz et concerne les corps algébriquement clos.

Théorème 4.1.2 (Nullstellensatz, version faible [1, Théorème 4.1.1])**.** *Soient $\mathbb{K}$ un corps algébriquement clos et soient $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_d]$. On a l'équivalence :*

$$V_{\mathbb{K}}(f_1, \dots, f_r) = \emptyset \quad \Leftrightarrow \quad 1 \in I(f_1, \dots, f_r).$$

Démonstration. On montre l'implication de droite à gauche. Si 1 est dans l'idéal engendré par $f_1, \dots, f_r$, alors il existe une décomposition $g_1 f_1 + \cdots + g_r f_r = 1$, où les g_i sont des polynômes. Si $V_{\mathbb{K}}(f_1, \dots, f_r)$ était non vide, alors les f_i s'annuleraient simultanément en chacun de ses points $\mathbf{a}$, si bien que 1 évalué en $\mathbf{a}$ serait nul, ce qui est impossible.

Pour la réciproque, on montre par récurrence sur d la propriété

$$(P_d) : \qquad \forall r \in \mathbb{N},\ \forall f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_d] : \quad V_{\mathbb{K}}(f_1, \dots, f_r) = \emptyset \quad \Rightarrow \quad 1 \in I(f_1, \dots, f_r).$$

Si $d = 1$ et $f_1(x), \dots, f_r(x)$ sont des polynômes sans racine commune, alors $\mathbb{K}[x]$ étant principal, il existe un polynôme $g(x)$ qui engendre $I(f_1, \dots, f_r)$. En particulier $g(x)$ divise chaque $f_i(x)$. Ainsi défini, $g(x)$ est un polynôme constant, car sinon, $\mathbb{K}$ étant algébriquement clos, $g(x)$ aurait une racine qui, étant racine de tous ses multiples, serait racine commune des $f_i(x)$. Le fait que $g(x)$ soit constant implique que 1 est dans l'idéal engendré par les $f_i(x)$, ce qui montre (P_1).

On montre maintenant que $(P_{d-1}) \Rightarrow (P_d)$. Soit une famille fixée $f_1, \dots, f_r$ d'éléments de $\mathbb{K}[x_1, \dots, x_d]$ telle que $V_{\mathbb{K}}(f_1, \dots, f_r)$ est vide. On admet sans le démontrer que le polynôme f_1 peut être supposé unitaire en x_d, *i.e.*, son coefficient de plus haut degré en cette indéterminée est 1. On considère une nouvelle indéterminée t et on pose

$$g(t, x_1, \dots, x_d) = f_2(x_1, \dots, x_d) + t f_3(x_1, \dots, x_d) + \cdots + t^{r-2} f_r(x_1, \dots, x_d) \in \mathbb{K}[x_1, \dots, x_d, t].$$

Soit le résultant $r_{x_d}(f_1, g) \in \mathbb{K}[t, x_1 \dots, x_{d-1}]$ par rapport à x_d, et soit $r_i(x_1, \dots, x_{d-1})$ son coefficient en t^i. D'après la proposition 2.2.2, il existe une décomposition $r_{x_d}(f_1, g) = u(t, x_1, \dots, x_d) f_1 + v(t, x_1, \dots, x_d) g$, qui par identification des coefficients en les puissances de t^i permet de déduire que les $r_i(x_1, \dots, x_{d-1})$ sont dans $I(f_1, \dots, f_r)$. En notant $k = \deg_t\left(r_{x_d}(f_1, g)\right)$, on va montrer par l'absurde que $V_{\mathbb{K}}(r_1, \dots, r_k)$ est vide. On suppose donc qu'il existe un $\mathbf{a} \in \mathbb{K}^{d-1}$ dans la variété affine définie par les r_i, de sorte que le polynôme $r_{x_d}(f_1, g(t, \mathbf{a})) \in \mathbb{K}[t]$ est nul, si bien que pour tout $c \in \mathbb{K}$, le résultant de $f_1(\mathbf{a}, x_d)$ et $g(c, \mathbf{a}, x_d)$ est nul, *i.e.*, ces deux polynômes ont une racine commune. Puisque $f_1(x_1, \dots, x_d)$ est unitaire en x_d, le polynôme $f_1(\mathbf{a}, x_d)$ n'a qu'un nombre fini de racines, si bien qu'il en existe une b telle que $g(t, \mathbf{a}, b)$ a un nombre infini de racines. Ainsi, ce polynômes est nul, si bien que $f_i(\mathbf{a}, b) = 0$ pour tout $i \geq 2$, ce qui contredit que $V_{\mathbb{K}}(f_1, \dots, f_r)$ est vide. On a démontré que la variété définie par les $r_i(x_1, \dots, x_{d-1})$ est vide, si bien que l'hypothèse de récurrence (P_{d-1}) implique que 1 est dans l'idéal engendré par les $r_i(x_1, \dots, x_{d-1})$. Or, on a montré plus tôt que ces polynômes sont dans $I(f_1, \dots, f_r)$ de sorte que ce dernier contient également 1. Ainsi, $P_{(d-1)}$ implique (P_d), ce qui fini la démonstration du théorème. □

À partir du Nullstellensatz, on peut exploiter les bases de Gröbner pour montrer qu'un système polynomial admet ou non une solution lorsque le corps est algébriquement clos. Il suffit en effet de tester si 1 est dans l'idéal engendré par les équations, ce qui d'après la proposition 3.3.2, se ramène à un calcul de reste par une base de Gröbner. Or, pour que 1 soit réductible par une base de Gröbner, il faut que celle-ci contienne un polynôme constant : le monôme dominant d'un polynôme non constant ne divise en effet pas 1. Enfin, on rappelle qu'une base de Gröbner peut être calculée par l'algorithme de Buchberger. Ainsi, pour tester si le système défini par les équations $f_1, \dots, f_r$ admet une solution lorsque le corps est algébriquement clos, il suffit de calculer une base de Gröbner de $I(f_1, \dots, f_r)$ par l'algorithme de Buchberger et de tester si celle-ci contient un polynôme constant.

On a vu que la version faible du Nullstellensatz permet de ramener un problème de géométrie à un problème de calcul dans les idéaux. On finit cette section en exposant brièvement le "dictionnaire variétés affines - idéaux", *i.e.*, les méthodes de reformulation et de résolution de problèmes géométriques par la théorie des idéaux. On note, pour un idéal $I \subseteq \mathbb{K}[x_1,\dots,x_d]$ et une variété affine $V = V_{\mathbb{K}}(f_1,\dots,f_r) \subseteq \mathbb{K}^d$:

$$V(I) = \left\{\mathbf{a} \in \mathbb{K}^d \mid \forall\, f \in I :\, f(\mathbf{a}) = 0\right\} \qquad \text{et} \qquad \mathbf{I}(V) \qquad \text{et} \qquad \left\{f \in \mathbb{K}[x_1,\dots,x_d] \mid \forall\, \mathbf{a} \in V :\, f(\mathbf{a}) = \right\}.$$

En d'autres termes, $V(I)$ est le lieu des points annulés par tous les éléments de I et $\mathbf{I}(V)$ est l'ensemble des polynômes qui s'annulent sur V.

Proposition 4.1.3 ([1, Lemme 1.4.6])**.** *Soient $f_1,\dots,f_r \in \mathbb{K}[x_1,\dots,x_d]$, et soient I et V l'idéal engendré par $f_1,\dots,f_r$ et la variété affine définie par $f_1,\dots,f_r$, respectivement. On a $V_{\mathbb{K}}(f_1,\dots,f_r) = V(I)$. De plus, $\mathbf{I}(V)$ est un idéal de $\mathbb{K}[x_1,\dots,x_d]$.*

Démonstration. Tout d'abord, on note que $f_1,\dots,f_r$ étant dans I, $V(I)$ est inclus dans $V_{\mathbb{K}}(f_1,\dots,f_r)$. Soit maintenant $\mathbf{a} \in \mathbb{K}^d$ annulé par $f_1,\dots,f_r$, alors $\mathbf{a}$ est annulé par toutes les combinaisons $g_1 f_1 + \cdots + g_r f_r$, ou les g_i sont des polynômes, *i.e.*, $\mathbf{a} \in V(I)$. Ainsi, $V_{\mathbb{K}}(f_1,\dots,f_r) = V(I)$. De plus, $\mathbf{I}(V)$ est un idéal car le polynôme nul annule tous les points de $\mathbb{K}^d$, donc *a fortiori* ceux de V, et si f, f' annulent tous les points de V alors il en est de même pour leur somme et si g est un polynôme quelconque alors gf annule également tous les points de V. □

La proposition précédente signifie qu'il existe deux applications entre les ensembles des variétés affines et des idéaux :

$$V : \quad \left\{\text{variétés affines de } \mathbb{K}^d\right\} \to \left\{\text{idéaux de } \mathbb{K}[x_1,\dots,x_d]\right\}, \quad V \mapsto V(I)$$

$$\mathbf{I} : \quad \left\{\text{idéaux de } \mathbb{K}[x_1,\dots,x_d]\right\} \to \left\{\text{variétés affines de } \mathbb{K}^d\right\}, \quad I \mapsto \mathbf{I}(V).$$

On s'intéressera aux composées de ces deux fonctions lorsque la version forte du Nullstellensatz aura été énoncée. Avant cela, et comme annoncé plus haut, on va voir comment certains problèmes de géométrie sont reformulés en termes d'idéaux.

Proposition 4.1.4 ([1, Proposition 1.4.8])**.** *Soient V et W deux variétés affines. Alors on a $V \subseteq W$ si et seulement si $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. En particulier, on a $V = W$ si et seulement si $\mathbf{I}(V) = \mathbf{I}(W)$.*

Démonstration. Si V est inclus dans W, alors tout polynôme s'annulant sur W s'annule également sur V, *i.e.*, $\mathbf{I}(W) \subseteq \mathbf{I}(V)$. Réciproquement, on suppose que $\mathbf{I}(W) \subseteq \mathbf{I}(V)$ et on fixe des polynômes $g_1,\dots,g_r$ tels que $W = V_{\mathbb{K}}(g_1,\dots,g_r)$. Chacun de ces polynômes est dans $\mathbf{I}(W)$ et donc dans $\mathbf{I}(V)$. Ainsi, $g_i(\mathbf{a})$ est nul pour tout $\mathbf{a} \in V$ et tout $1 \le i \le r$, de sorte que $\mathbf{a} \in W$. Ainsi, V est incluse dans W. □

Il est naturel de se demander si l'est possible d'extraire de la proposition précédente un algorithme testant l'inclusion. Pour cela, il faudrait tester l'inclusion de $\mathbf{I}(V) \subseteq \mathbf{I}(W)$ à partir des équations de V et W. Ce test d'inclusion étant basé sur la version forte du Nullstellensatz, on l'énonce plus tard. De plus, il est important de noter que le critère d'inclusion de la proposition précédente n'est pas vrai si on considère les idéaux engendrés par les équations au lieu des idéaux des polynômes s'annulant sur les variétés, ce que est formalisé dans la remarque suivante.

Remarque 4.1.5. Soient I et J deux idéaux de $\mathbb{K}[x_1,\dots,x_d]$. Si I est inclus dans J, alors $V(J)$ est inclus dans $V(I)$ car tous les points annulés par les éléments de J le sont *a fortiori* par ceux de I. En revanche, la réciproque est fausse : en considérant les idéaux $I = (x^2)$ et $J = (x)$ de $\mathbb{K}[x]$, on a $V(I) = V(J) = \{0\} \subset \mathbb{K}$ et pourtant I n'est pas inclus dans J.

On s'intéresse maintenant à deux autres questions géométriques pouvant être résolues par la théorie des idéaux : est-ce que l'intersection et la réunion de deux variétés affines sont des variétés affines ? On rappelle qu'étant donnés deux idéaux I et J de $\mathbb{K}[x_1,\dots,x_d]$, l'intersection $I \cap J$ et la somme $I + J$ sont des idéaux de $\mathbb{K}[x_1,\dots,x_d]$, où $I + J$ est l'ensemble des polynômes de la forme $f + g$, avec $f \in I$ et $g \in J$.

Théorème 4.1.6 ([1, Théorèmes 4.3.4 et 4.3.15])**.** *Soient I et J deux idéaux de $\mathbb{K}[x_1,\dots,x_d]$. On a :*

$$V(I+J) \;=\; V(I)\cap V(J) \qquad \textit{et} \qquad V(I\cap J) \;=\; V(I)\cup V(J).$$

En particulier, la réunion et l'intersection de variétés affines sont des variétés affines.

Démonstration. On montre la première égalité. D'après la remarque 4.1.5, les idéaux I et J étant inclus dans $I+J$, l'inclusion $V(I+J)\subseteq V(I)\cap V(J)$ est vraie. Réciproquement, si $\mathbf{a}$ est un point de $V(I)\cap V(J)$, alors $(f+g)(\mathbf{a}) = f(\mathbf{a})+g(\mathbf{a}) = 0$ pour tout $f\in I$ et pour tout $g\in J$, si bien que $V(I)\cap V(J)$ est inclus dans $V(I+J)$. On montre maintenant la deuxième égalité. L'inclusion $V(I)\cup V(J)\subseteq V(I\cap J)$ provient des inclusions $I\cap J\subseteq I$ et $I\cap J\subseteq J$. Pour l'inclusion réciproque, on considère $\mathbf{a}\in V(I\cap J)$. Pour tout $f\in I$ et tout $g\in J$, le polynôme fg est dans $I\cap J$, si bien que $f(\mathbf{a})g(\mathbf{a}) = (fg)(\mathbf{a}) = 0$. Ainsi, si $\mathbf{a}$ n'appartient pas à $V(I)$, *i.e.*, il existe $f\in I$ tel que $f(\mathbf{a})\neq 0$, alors pour tout $g\in J$, $g(\mathbf{a}) = 0$, *i.e.*, $\mathbf{a}\in V(J)$. On montre de la même façon que si $\mathbf{a}$ n'appartient pas à $V(J)$, alors il est dans $V(I)$, si bien que $\mathbf{a}\in V(I)\cup V(J)$. Il reste à montrer la dernière assertion du théorème. Si V et W sont des variétés affines définies par des équations polynomiales, alors en notant I et J les idéaux engendrés par ces polynômes, $I+J$ et $I\cap J$ sont engendrés par un nombre fini d'éléments d'après le théorème 3.3.4. En notant $f_1,\dots,f_r$ et $g_1,\dots,g_s$ les générateurs respectifs de $I+J$ et $I\cap J$, la proposition 4.1.3 implique que $V\cap W = V(I+J) = V_{\mathbb{K}}\left(f_1,\dots,f_r\right)$ et $V\cup W = V(I\cap J) = V_{\mathbb{K}}\left(g_1,\dots,g_s\right)$, de sorte que $V\cap W$ et $V\cup W$ sont des variétés affines. □

Exemple 4.1.7. On considère les deux variétés affines de $\mathbb{R}^3$:

$$V \;=\; V_{\mathbb{R}}\left(x^2+y^2+z^2-1\right) \qquad \text{et} \qquad W \;=\; V_{\mathbb{R}}(z).$$

En d'autre termes, V est la sphère unité et W est le plan xOy. Géométriquement, il est clair que $V\cap W$ est le cercle unité de xOy. On retrouve ce résultat par les idéaux. En notant I et J les idéaux principaux engendrés par $x^2+y^2+z^2-1$ et z, respectivement, l'idéal $I+J$ est engendré par ces deux polynômes. De plus, puisque x^2+y^2-1 est égal à $(x^2+y^2+z^2-1)-z.z$, alors $I+J = I(x^2+y^2-1,z)$. Ainsi, on retrouve bien que $V\cap W$ est le cercle unité du plan xOy.

Exemple 4.1.8. On considère les deux variétés affines de $\mathbb{R}^3$:

$$V \;=\; V_{\mathbb{R}}(z) \qquad \text{et} \qquad W \;=\; V_{\mathbb{R}}\left(x,y\right).$$

En d'autre termes, V est le plan xOy et W est l'axe des z. En notant $I = I(z)$ et $I = I(x,y)$, on va voir que les générateurs de $I\cap J$ donnent bien des équations de $V\cup W$. On commence par montrer que $I\cap J$ est engendré par xz et yz. Tout d'abord, xz et xy sont bien dans $I\cap J$, de sorte que $I(xz,yz)\subseteq I\cap J$. On montre maintenant que $I\cap J$ est dans $I(xz,yz)$. Soit $f(x,y,z)\in I\cap J$, alors $f(x,y,z)\in I$, de sorte qu'il s'écrit $f(x,y,z) = zg(x,y,z)$. De plus, pour que $f(x,y,z)$ soit dans J, il faut que $g(x,y,z)$ soit dans J. Cela découle des faits que z n'est pas dans J et que J est un anneau intègre (en effet, $\mathbb{K}[x,y,z]/J$ est isomorphe à l'anneau intègre $\mathbb{K}[z]$). Ainsi, $g(x,y,z)$ s'écrit sous la forme $xh(x,y,z)+yl(x,y,z)$ et donc

$$f(x,y,z) \;=\; zg(x,y,z) \;=\; z\big(xh(x,y,z)+yl(x,y,z)\big) \;=\; xzh(x,y,z)+yzl(x,y,z)\in I(xz,yz).$$

On a donc montré que tout $f(x,y,z)$ de $I\cap J$ est dans $I(xz,yz)$ et donc que $I\cap J\subseteq I(xz,yz)$. On en déduit donc que $V\cup W = V_{\mathbb{R}}\left(xz,yz\right)$: en effet, les solutions du système d'équations $xz = yz = 0$ sont bien les points de l'union de l'axe des z et du plan xOy.

Il reste maintenant à énoncer la version forte du Nullstellensatz et en déduire un test d'inclusion de variétés. On a pour cela besoin pour cela d'une nouvelle construction sur les idéaux.

Définition 4.1.9. Soit $I\subseteq\mathbb{K}[x_1,\dots,x_d]$ un idéal. On appelle *radical* de I, noté $\sqrt{I}$, l'ensemble

$$\sqrt{I} \;=\; \left\{f^m \;\middle|\; f\in I,\; m\in\mathbb{N}\right\}.$$

On dit que I est *radiciel* si $I = \sqrt{I}$.

On admet les faits suivants, démontrés dans [1, Lemme 4.2.5] : $\sqrt{I}$ est un idéal, il contient I et il est radiciel. Il peut en fait être caractérisé de la façon suivante : il s'agit du plus petit idéal radiciel contenant I. On rappelle d'après [1, Proposition 4.2.8] qu'un polynôme g appartient au radical de l'idéal $I(f_1,\dots,f_r)$ si et seulement si 1 appartient à l'idéal de $I(f_1,\dots,f_r,1-tg) \subseteq \mathbb{K}[x_1,\dots,x_d,t]$, où t est une nouvelle variable. On rappelle enfin que tester si 1 est dans un idéal se fait par un calcul de base de Gröbner. On énonce maintenant la version forte du Nullstellensatz.

Théorème 4.1.10 (Nullstellensatz, version forte [1, Théorème 4.2.6])**.** *Soient $\mathbb{K}$ un corps algébriquement clos et I un idéal de $\mathbb{K}[x_1,\dots,x_d]$. Alors, on a :*

$$\mathbf{I}(V(I)) \;=\; \sqrt{I}.$$

On note qu'une conséquence importante de la version forte du Nullstellensatz est qu'elle permet d'établir la "correspondance variétés affines - idéaux", démontrée dans [1, Théorème 4.2.7]. Celle-ci s'énonce de la façon suivante : si $\mathbb{K}$ est un corps algébriquement clos, alors les deux applications

$$V : \quad \left\{\text{variétés affines de } \mathbb{K}^d\right\} \to \left\{\text{idéaux radiciels de } \mathbb{K}[x_1,\dots,x_d]\right\}, \quad V \mapsto V(I)$$

$$\mathbf{I} : \quad \left\{\text{idéaux radiciels de } \mathbb{K}[x_1,\dots,x_d]\right\} \to \left\{\text{variétés affines de } \mathbb{K}^d\right\}, \quad I \mapsto \mathbf{I}(V)$$

sont les réciproques l'une de l'autre, *i.e.*, $\mathbf{I}(V(I)) = I$ et $V(\mathbf{I}(V)) = V$, pour toute variété affine V et pour tout idéal radiciel I.

On termine cette section en présentant le test d'inclusion de variétés affines, valable sur les corps algébriquement clos. On considère deux variétés affines $V = V_{\mathbb{K}}(f_1,\dots,f_r)$ et $W = V_{\mathbb{K}}(g_1,\dots,g_s)$ et on note I et J les idéaux engendrés par les f_i et les g_j, respectivement. D'après la proposition 4.1.4, V est inclus dans W si et seulement si $\mathbf{I}(W)$ est inclus dans $\mathbf{I}(V)$, ce qui d'après la version forte du Nullstellensatz, équivaut à ce que $\sqrt{J}$ est inclus dans $\sqrt{I}$. Or, $\sqrt{J}$ étant le plus petit idéal radiciel contenant J et $\sqrt{I}$ étant radiciel, $\sqrt{J}$ est inclus dans $\sqrt{I}$ si et seulement si J est inclus dans $\sqrt{I}$. Ainsi, pour tester si V est incluse dans W, il suffit de tester si les g_i sont inclus dans $\sqrt{I}$, ce qui se ramène à des calculs de bases de Gröbner.

4.2. Résolution de systèmes polynomiaux

Dans l'exemple 2.2.7, on a vu comment utiliser le résultant pour calculer les solutions d'un système polynomial de deux équations à deux inconnues. Dans cette section, on présente une méthode de résolution alternative basée sur les bases de Gröbner et les idéaux d'élimination pour des systèmes contenant plus d'équations et/ou plus d'inconnues.

Soit un système d'équations polynomiales

$$\begin{cases} f_1(x_1,\dots,x_d) \;=\; 0 \\ \qquad\qquad \vdots \\ f_r(x_1,\dots,x_d) \;=\; 0, \end{cases} \tag{4.1}$$

dont on souhaite trouver les solutions dans $\overline{\mathbb{K}}$. Étant donné un ordre monomial, soit $G = \{g_1,\dots,g_s\}$ une base de Gröbner de l'idéal I engendré par les $f_1(x_1,\dots,x_d),\dots,f_r(x_1,\dots,x_d)$. L'idéal I est engendré par G

d'après la proposition 3.3.2, donc d'après la proposition 4.1.3, le système (4.1) a les mêmes solutions que le système

$$\begin{cases} g_1(x_1,\ldots,x_d) = 0 \\ \qquad\vdots \\ g_s(x_1,\ldots,x_d) = 0. \end{cases} \tag{4.2}$$

Ainsi, le problème de résoudre (4.1) se ramène à résoudre (4.2). On illustre l'intérêt qu'il y a à se ramener à un système exprimé par une base de Gröbner sur un exemple.

Exemple 4.2.1. On considère un exemple de [1, Section 3.1] : on cherche à résoudre sur $\mathbb{C}^3$ le système

$$\begin{cases} x^2+y+z = 1 \\ x+y^2+z = 1 \\ x+y+z^2 = 1. \end{cases} \tag{4.3}$$

On considère le système associé à une base de Gröbner de l'idéal engendré par les équations de (4.3), relativement à l'ordre lex induit par $z \prec y \prec x$:

$$\begin{cases} x+y+z^2 = 1 \\ y^2-y-z^2+z = 0 \\ 2yz^2+z^4-z^2 = 0 \\ z^6-4z^4+4z^3-z^2 = 0. \end{cases} \tag{4.4}$$

Alors, les solutions $\mathbf{a} = (a,b,c) \in \mathbb{C}^3$ de (4.4) doivent vérifier que c est solution de $z^6-4z^4+4z^3-z^2$. En remarquant que ce polynôme admet 0 et 1 comme racines doubles, on montre que c peut prendre les valeurs $0, 1$ et $-1\pm\sqrt{2}$. En remplaçant successivement z par ces valeurs dans les deux équations ne faisant intervenir que y et z, à savoir $2yz^2+z^4-z^2=0$ et $y^2-y-z^2+z=0$, on en déduit les valeurs que b peut prendre en fonction de c. Finalement, en remplaçant le couple (y,z) par les couples (b,c) calculés à partir des trois équations du bas dans la première équation $x+y+z^2=1$, on trouve la valeur de a. En notant $\alpha = -1\pm\sqrt{2}$, on obtient que le système (4.4), et donc le système (4.3), admet les 5 solutions :

$$(1,0,0,), \qquad (0,1,0), \qquad (0,0,1), \qquad (\alpha,\alpha,\alpha).$$

Sur l'exemple précédent, on observe que la résolution du système exprimé par une base de Gröbner s'apparente à celle d'un système triangulé en algèbre linéaire. En effet, l'approche consiste à exprimer une équation portant uniquement sur la dernière coordonnée de la solution, puis d'exprimer l'avant dernière coordonnée en fonction de la dernière jusqu'à exprimer la première coordonnée en fonction des autres. Il est naturel de se demander quel est le cadre d'application général de cette méthode de résolution. Pour cela, on a besoin des idéaux d'élimination et des théorèmes d'élimination et d'extension.

Définition 4.2.2. Soit I un idéal de $\mathbb{K}[x_1,\ldots,x_d]$ et soit $0 \le i \le d$. On appelle le *i-ème idéal d'élimination*, noté I_i, l'idéal de $\mathbb{K}[x_{i+1},\ldots,x_d]$

$$I_i = I \cap \mathbb{K}[x_{i+1},\ldots,x_d].$$

On note que $I_0 = I$ et que I_i est en effet un idéal de $\mathbb{K}[x_{i+1},\ldots,x_d]$ car I est un idéal de $\mathbb{K}[x_1,\ldots,x_d]$. De plus la terminologie "idéal d'élimination" provient du fait que les éléments de I_i sont les éléments de I dans lesquels les variables $x_1,\ldots,x_d$ ont été éliminées. On peut maintenant énoncer et prouver le théorème d'extension. On note que dans l'énoncé de celui-ci, on considère des bases de Gröbner relativement à un ordre lex. Il s'avère cependant que ce théorème reste valide pour des ordres monomiaux plus généraux, dits d'*élimination*, qu'on n'évoque pas dans ce cours.

Théorème 4.2.3 (Théorème d'élimination [1, Théorème 3.1.2])**.** *Soient I un idéal de $\mathbb{K}[x_1,\dots,x_d]$ et G une base de Gröbner de I relativement à l'ordre lex induit par $x_d \prec \cdots \prec x_1$. Alors pour tout $0 \leq i \leq d$, la famille $G_i = G \cap \mathbb{K}[x_{i+1},\dots,x_d]$ est une base de Gröbner de I_i.*

Démonstration. Tout d'abord, G_i est bien inclus dans I_i. Il s'agit maintenant de montrer que pour tout $f \in I_i$, il existe $g \in G_i$ tel que $\mathrm{lm}(g)$ divise $\mathrm{lm}(f)$. Puisque $f \in I$, il existe $g \in G$ tel que $\mathrm{lm}(g)$ divise $\mathrm{lm}(f)$ et puisque $f \in \mathbb{K}[x_{i+1},\dots,x_d]$, $\mathrm{lm}(g)$ ne dépend que des variables $x_{i+1},\dots,x_d$. Maintenant, puisque l'ordre monomial considéré est l'ordre lex induit par $x_d \prec \cdots \prec x_1$, $\mathrm{supp}(g)$ ne peut pas contenir de monôme dans lequel figure une des variables $x_1,\dots,x_i$: sinon $\mathrm{lm}(g)$ ne dépendrait pas uniquement des variables $x_{i+1},\dots,x_d$. On en déduit que $g \in \mathbb{K}[x_{i+1},\dots,x_d]$ et donc que $g \in G_i$, ce qui conclut la démonstration. □

On revient au système (4.1) : soit I l'idéal engendré par ses équations et soit $G = \{g_1,\dots,g_s\}$ une base de Gröbner de I relativement à l'ordre lex induit par $x_d \prec \cdots \prec x_1$. D'après le théorème d'élimination, une solution $\mathbf{a} = (a_1,\dots,a_d)$ de (4.2) est telle que pour chaque $1 \leq i \leq d$, a_i est solution du système

$$\begin{cases} g_{k_i}(x_i, a_{i+1},\dots,a_d) = 0 \\ \qquad\qquad \vdots \\ g_s(x_i, a_{i+1},\dots,a_d) = 0, \end{cases} \tag{4.5}$$

où les $g_{k_i},\dots,g_s$ sont les éléments de $G \cap I_{i-1}$. Pour trouver les solutions globales de (4.1), il faut donc calculer itérativement les solutions de (4.5) pour $i = d, d-1,\dots,1$. On note qu'à chaque étape, il peut exister plusieurs solutions a_i de (4.5) et que celles-ci dépendent de la solution partielle déjà calculée et notée $(a_{i+1},\dots,a_d)$. En résumé, la résolution de (4.1) basée sur les bases de Gröbner et les idéaux d'élimination repose donc sur les deux étapes suivantes :

- il faut d'abord calculer une base de Gröbner relativement à l'ordre lex induit par $x_d \prec \cdots \prec x_1$ de l'idéal engendré par les équations de (4.1)
- il faut résoudre itérativement les systèmes (4.5) pour $i = d,\dots,1$, ce qui se ramène à un problème de recherche de solutions d'un polynôme univarié.

Il est à noter que le système (4.5) n'a pas nécessairement de solution, et donc le calcul de solutions de (4.1) par itération n'aboutit pas nécessairement pour toutes les solutions partielles $(a_i,\dots,a_d)$. Bien que qu'on ne l'utilisera pas, on mentionne sans le démontrer le théorème d'extension, celui-ci fournissant un critère d'existence de solutions du système (4.5). Pour une démonstration, on renvoie à [1], cette démonstration étant basée sur la proposition 2.2.4 et donc sur le résultant.

Théorème 4.2.4 (Théorème d'extension [1, Théorème 3.6.4])**.** *Soient I un idéal de $\mathbb{K}[x_1,\dots,x_d]$, $1 \leq i \leq d$, $h_1(x_i,\dots,x_d),\dots,h_t(x_i,\dots,x_d)$ une famille génératrice de I_{i-1} et $\mathbf{a} = (a_{i+1},\dots,a_d) \in V_{\overline{\mathbb{K}}}(I_i)$. Si $\mathbf{a}$ n'est pas un zéro commun des coefficients $\mathrm{lm}(h_j) \in \mathbb{K}[x_{i+1},\dots,x_d]$ de $\deg_{x_i}(h_j)$ dans h_j, $1 \leq j \leq t$, alors il existe $a_i \in \overline{\mathbb{K}}$ tel que $(a_i,\dots,a_d) \in V_{\overline{\mathbb{K}}}(I_{i-1})$.*

On explicite le rôle que joue le théorème d'extension pour prouver l'existence de solutions de (4.5). En reprenant les notations du début de la section, on suppose que pour $1 \leq i \leq d$, on a calculé une solution partielle $\mathbf{a} = (a_{i+1},\dots,a_d)$ telle que $g_{k_{i+1}}(\mathbf{a}),\dots,g_s(\mathbf{a})$ sont nuls. Les $g_{k_i},\dots,g_s$ formant une base de Gröbner de I_{i-1}, ils en sont une famille génératrice. Ainsi, une solution a_i de (4.5) est telle que $(a_i,\dots,a_d) \in V_{\overline{\mathbb{K}}}(I_{i-1})$. D'après le théorème d'extension, un tel a_i existe si $\mathbf{a}$ n'est pas un zéro commun des coefficients de degré $\deg_{x_i}(g_k)$ des g_k, $k_i \leq k \leq s$, en x_i. Ainsi, le système (4.5) admet une solution a_i dès que les degrés des polynômes univariés $g_k(x_i, \mathbf{a})$ sont égaux à $\deg_{x_i}(g_k)$.

Exemple 4.2.5. Soit le système polynomial sur $\mathbb{C}^3$:

$$\begin{cases} x^2+y^2+z^2 &= 0 \\ xyz &= 1, \end{cases} \tag{4.6}$$

et soit le système associé à une base de Gröbner de l'idéal engendré par les équations de (4.6) relativement à l'ordre lex induit par $z \prec y \prec x$:

$$\begin{cases} x+y^3z+yz^3-yz &= 0 \\ y^4z^2+y^2z^4-y^2z^2+1 &= 0. \end{cases} \tag{4.7}$$

On remarque que $I_z = \{0\}$, de sorte que toute valeur $c \in \mathbb{C}$ est une solution partielle. Ensuite, l'idéal I_y est engendré par la deuxième équation $g_2(x,y,z) = g(y,z)$ de (4.7). On remarque que $g_2(y,0) = 0$ n'a pas de solution, cela étant cohérent avec le théorème d'extension puisque $\deg(g_2(y,0)) = 0$ alors que $\deg_y(g_2) = 4$. En revanche, pour $c \neq 0$, l'équation $g_2(y,c) = 0$ admet 4 solutions complexes. Finalement, si (b,c) est une solution de $g_2(y,z) = 0$, alors en posant $a = -b^3c - bc^3 + bc$, on obtient une solution de (4.7). Ainsi, les solutions de (4.6) sont les (a,b,c), où $c \neq 0$, b est solution de $c^2y^4 + (c^4-c^2)y^2 + 1$ et $a = -b^3c - bc^3 + bc$.

Dans les exemples 4.2.1 et 4.2.5, on a trouvé toutes les solutions grâce à la méthode basée sur les idéaux d'élimination et les bases de Gröbner. On remarque cependant que ces exemples sont de nature différentes : pour le premier il n'y a qu'un nombre fini de solutions, ce qui signifie qu'elles forment une variété de dimension 0, et pour le deuxième il en existe un nombre infini, dépendant du paramètre c, ce qui signifie qu'elles forment une variété de dimension 1. De façon générale, si on souhaite exprimer les points d'une variété de dimension non nulle, on a besoin de paramètres, dont le nombre est égal à la dimension de la variété, en fonction desquels sont exprimés les coordonnées des points de la variété. Une telle représentation de la variété est dite *paramétrique*, alors qu'une représentation par les équations est dite *implicite*. On note qu'en général, une représentation paramétrique ne recouvre pas globalement la variété et n'est pas polynomiale, mais dans ce cours on n'entre pas dans ces considérations et les exemples de la fin de cette section portent sur des variétés admettant une paramétrisation polynomiale globale. De plus, une représentation paramétrique est utile en pratique pour tracer les variétés, par exemple grâce à un logiciel de calcul : il suffit de faire varier les paramètres sur certains intervalles et d'en déduire les points de la variété. En revanche, la représentation paramétrique est moins appropriée pour tester si un point appartient à la variété, puisque cela se ramène à résoudre un système dont les inconnues sont les paramètres exprimés en fonction des coordonnées du point dont on teste l'appartenance à la variété. Il est beaucoup plus aisé de tester si ce point appartient à la variété grâce à la représentation implicite : il suffit de substituer les coordonnées du point dans les équations définissant la variété et vérifier si le résultat obtenu est nul. On termine cette section en présentant deux méthodes, l'une basée sur les bases de Gröbner et l'autre sur le résultant, permettant de passer d'une représentation paramétrique à une représentation implicite.

Résultant et représentation implicite. On considère une courbe plane $\mathscr{C}$ admettant une représentation paramétrique polynomiale, *i.e.*, $\mathscr{C}$ est l'ensemble des points du plan de la forme $(x(t), y(t))$, où $x(t)$ et $y(t)$ sont des polynômes en une variable t. On montre que $\mathscr{C}$ a pour équation implicite $f(x,y) = 0$, où

$$f(x,y) \;=\; \mathrm{res}_t(x - x(t), y - y(t)),$$

les polynômes $x - x(t)$ et $y - y(t)$ étant des polynômes de trois variables x, y, t. En effet, les coefficients de plus haut degrés en t de $x - x(t)$ et $y - y(t)$ sont constants, de sorte que d'après la proposition 2.2.4, on a

$$Z(f(x,y)) \;=\; \pi\big(Z(x - x(t)) \cap Z(y - y(t)\big),$$

où $\pi : \mathbb{K}^3 \to \mathbb{K}^2, (x,y,z) \mapsto (x,y)$. Or, (x,y,t) est un zéro commun de $x - x(t)$ et $y - y(t)$ si et seulement si on a $x = x(t)$ et $y = y(t)$, *i.e.*, si et seulement si $(x,y) \in \mathscr{C}$. Ainsi, les solutions de $f(x,y) = 0$ sont les points

de $\mathscr{C}$, ce qui signifie que $\mathscr{C}$ a pour équation implicite $f(x,y)=0$. À titre d'illustration, on considère la courbe $\mathscr{C}$ de $\mathbb{R}^2$ de représentation paramétrique $(x(t),y(t))=(-t^3+3t,3t^2)$. Alors, $\mathscr{C}$ a pour équation implicite $f(x,y)=0$, où

$$f(x,y) \;=\; \mathrm{res}_t(x+t^3-3t, y-3t^2) \;=\; y^3-18y^2-27x^2+81y.$$

Bases de Gröbner et représentation implicite. Une autre façon de trouver une représentation implicite d'une variété (pas nécessairement une courbe) est de passer par les idéaux d'élimination. On considère une variété $V\subseteq\mathbb{K}^d$ paramétrée par m paramètres : les points de V sont des la forme

$$(x_1(t_1,\ldots,t_m,),\ldots,x_d(t_1,\ldots,t_m)).$$

On admet [1, Théorème 3.3.1], qui stipule que $V(I\cap\mathbb{K}[x_1,\ldots,x_d])$, est la plus petite variété affine contenant V, où

$$I \;=\; I\Big(x_1-x_1(t_1,\ldots,t_m),\ldots,x_d-x_d(t_1,\ldots,t_m)\Big)\subseteq\mathbb{K}[t_1,\ldots,t_m,x_1,\ldots,x_d].$$

Comme précédemment, l'idéal I apparaît naturellement car les points de V sont les points de la forme $\pi\Big(t_1,\ldots,t_m,x_1,\ldots,x_d\Big)$, où $(t_1,\ldots,t_m,x_d,\ldots,x_d)\in V(I)$ et $\pi(t_1,\ldots,t_m,x_d,\ldots,x_d)=(x_1\ldots,x_d)$. On illustre cette méthode par un exemple. Soit la surface $\mathscr{S}\subset\mathbb{R}^3$ de représentation paramétrique

$$(x(t,u),y(t,u)) \;=\; (t+u,t^2+2tu,t^3+3t^2u).$$

On considère l'idéal $I=I\big(x-t-u,y-t^2-2tu,z-t^3-3t^2u\big)\subset\mathbb{R}[t,u,x,y,z]$. Alors, une base de Gröbner de I pour l'ordre lex induit par $z\prec y\prec x\prec u\prec t$ est composée de polynômes dont un seul est dans l'idéal d'élimination $I\cap\mathbb{R}[x,y,z]$:

$$g(x,y,z) \;=\; x^3z-\frac{3}{4}x^2y^2-\frac{3}{2}xyz+y^3+\frac{1}{4}z^2.$$

D'après le théorème d'élimination 4.2.3, $V(I\cap\mathbb{R}[x,y,z])$ est engendré par g, si bien qu'une représentation implicite de $\mathscr{S}$ est donnée par $g(x,y,z)=0$. Il s'avère que dans ce cas $\mathscr{S}$ est bien égal à $V_{\mathbb{R}}\big(g\big)$.

[1] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.