Chapitre 1

De l'algèbre linéaire à la résolution des systèmes polynomiaux

Jean-Charles Faugère et Mohab Safey El Din
chapitre d'introduction à la résolution des systèmes polynomiaux (avec exercices)
ouvrage collectif à paraître chez **Pearson Education**.

Ce chapitre traite de la résolution des systèmes d'équations polynomiales et fait suite au chapitre 4 du tome *Mathématiques L2*, Pearson Education, 2007, qui introduisait certains algorithmes fondamentaux du calcul formel. Même si le champ des problématiques abordées par le calcul formel est bien plus vaste que la résolution des systèmes polynomiaux, cette dernière problématique occupe une place importante du fait de ses très nombreuses applications dans divers domaines des sciences de l'ingénieur. De plus, des logiciels et bibliothèques efficaces permettent aujourd'hui de résoudre des applications importantes en robotique, théorie du signal, biologie, etc. La plupart des systèmes de calcul formel (notamment les plus répandus, comme MAPLE et MATHEMATICA) intègre des fonctionnalités pour la résolution des systèmes polynomiaux. Ce chapitre est une introduction aux algorithmes sur lesquels se fondent ces programmes de résolution. Il donne aussi un aperçu des idées centrales et importantes (réduction à l'algèbre linéaire, évaluation-interpolation) à partir desquelles sont menées des recherches toujours intenses et actives pour améliorer les implantations et algorithmes existants.

I. Introduction et généralités

Considérons un système d'équations linéaires en les variables $X_1, \ldots, X_n$ à coefficients dans un corps $\mathbb{K}$,

$$\begin{cases} a_{1,1}X_1 + \cdots + a_{1,n}X_n = b_1 \\ \quad\vdots \qquad\qquad \vdots \\ a_{n,1}X_1 + \cdots + a_{n,n}X_n = b_n \end{cases}. \tag{1.1}$$

On peut résoudre un tel système en appliquant l'algorithme du pivot de Gauss. Ce procédé consiste à ramener la résolution du système (1.1) à celle d'un système triangulaire

$$\begin{cases} c_{1,1}X_1 + \cdots + \cdots + c_{1,n}X_n = d_1 \\ \quad c_{2,2}X_2 + \cdots + c_{2,n}X_n = d_2 \\ \quad\ddots \qquad\qquad \vdots \\ \quad c_{n-1,n-1}X_{n-1} + c_{n-1,n}X_n = d_{n-1} \\ \quad\qquad\qquad c_{n,n}X_n = d_n \end{cases}. \tag{1.2}$$

Cette réduction est obtenue en effectuant des combinaisons linéaires des équations du système (1.1). Ces équations consistent à éliminer une à une les variables du système (1.1) en les multipliant par des éléments de $\mathbb{K}$ et en les soustrayant les unes aux autres.

À partir du système triangulaire (1.2), il est aisé de déduire si le système linéaire (1.1) admet des solutions ou pas (s'il n'admet pas de solutions, une des équations dans le système triangulaire obtenu est de la forme $0 = d$, avec $d \neq 0$). Le cas échéant, le système (1.1) admet soit une infinité de solutions dans $\mathbb{K}^n$, soit une solution unique dans $\mathbb{K}^n$.

Comparons la situation avec le cas des systèmes d'équations polynomiales. Dans tout ce chapitre, on notera $\mathbb{Q}$ le corps des rationnels, $\mathbb{R}$ le corps des réels et $\mathbb{C}$ le corps des complexes. Pour simplifier, on commence par considérer des polynômes de $\mathbb{Q}[X]$, notamment les polynômes $f_1 = X^2 + 1$ et $f_2 = X^2 - 2$. On vérifie sans peine que l'équation $f_1 = 0$ n'a aucune solution dans $\mathbb{Q}$. Elle n'a pas non plus de solutions dans $\mathbb{R}$, mais a évidemment deux solutions dans $\mathbb{C}$. La situation est un peu plus compliquée concernant l'équation $f_2 = 0$. Celle-ci n'a toujours pas de solutions dans $\mathbb{Q}$, mais en a deux dans $\mathbb{R}$. Ainsi, il est immédiat de constater qu'une équation polynomiale $f = 0$ en une variable de degré $d \geq 0$ à coefficients dans $\mathbb{Q}$ peut n'avoir aucune solution dans $\mathbb{Q}$, mais en avoir dans $\mathbb{R}$, ou n'avoir aucune solution dans $\mathbb{R}$, alors que le théorème fondamental de l'algèbre nous dit qu'elle en a toujours d dans $\mathbb{C}$. Ainsi, a contrario de ce qui se passe dans un contexte linéaire, la recherche de solutions devra se faire dans des corps *plus gros* que celui dans lequel vivent les coefficients du polynôme considéré. Dans ce chapitre, nous étudierons des algorithmes permettant d'étudier l'ensemble des solutions à coordonnées complexes de systèmes d'équations polynomiales à coefficients dans $\mathbb{Q}$.

Pour autant, le cas des polynômes en une variable n'est pas pleinement représentatif des situations qui peuvent se produire, notamment du point de vue du nombre de solutions. Considérons donc le système de deux équations $X_1X_2 - 1 = 0, X_1 = 0$, de degrés respectifs 2 et 1. Il est immédiat de constater que ce système n'admet aucune solution dans $\mathbb{C}^2$: la substitution de X_1 par 0 dans la première équation donne en effet $1 = 0$, ce qui est impossible. Remarquons que réduire le système initial à une telle identité contradictoire peut aussi se faire en multipliant la

deuxième équation $X_1 = 0$ par X_2 et en l'additionnant à l'opposé de la première : $-1.(X_1X_2 - 1) + X_1.X_2 = 1$. Ici, l'obtention d'une identité algébrique montrant la non-existence de solutions au système se fait en manipulant les équations de départ de manière similaire à celle de l'algorithme de Gauss, dans un contexte linéaire, sauf que l'on multiplie les équations de départ par des polynômes, et non plus par des scalaires. Cela constitue une différence essentielle.

Considérons maintenant le système d'équations $X_1^2 + X_2^2 - 1 = X_1 - X_2 = 0$, de degrés respectifs 2 et 1. Ce système admet deux solutions que l'on peut représenter sous une forme *triangulaire* obtenue en substituant X_2 par X_1 (opération permise puisque $X_2 - X_1 = 0$) dans la première équation, comme suit :

$$\begin{cases} X_2 = X_1 \\ 2X_1^2 - 1 = 0 \end{cases}.$$

Ici encore, une telle représentation aurait aussi pu être obtenue par des manipulations algébriques sur les équations de départ puisque $1.(X_1^2 + X_2^2 - 1) + (X_1 + X_2).(X_1 - X_2) = 2X_1^2 - 1$.

Le nombre de solutions peut donc varier, même lorsque celles-ci sont en nombre fini, ce qui constitue une différence importante avec le cas des systèmes linéaires. Bien évidemment, on peut exhiber des systèmes d'équations polynomiales ayant un nombre infini de solutions complexes. Par exemple, $X_1(X_1^2 + X_2^2 - 1) = X_1(X_1 - X_2) = 0$ admet comme solutions les deux points complexes représentés triangulairement ci-dessus, ainsi que tous les points de coordonnées $(0, x_2)$ (avec $x_2 \in \mathbb{R}$). Dans la suite, nous étudierons des algorithmes permettant de déterminer si un système d'équations polynomiales admet un nombre fini de solutions complexes. Dans ce cas, nous étudierons comment obtenir une *paramétrisation* de l'ensemble des solutions, c'est-à-dire une réécriture du système de départ sous la forme triangulaire suivante,

$$\begin{cases} X_n = \frac{q_n(T)}{q_0(T)} \\ \quad\vdots \\ X_1 = \frac{q_1(T)}{q_0(T)} \\ q(T) = 0 \end{cases},$$

où T est une nouvelle variable et $q, q_0, q_1, \ldots, q_n$ sont des polynômes de $\mathbb{Q}[T]$. Une telle écriture formelle de l'ensemble des solutions permet alors d'obtenir une approximation numérique de leurs coordonnées en isolant les racines de q et en étudiant les valeurs prises par $\frac{q_i}{q_0}$ en ces racines.

Nous avons constaté ci-dessus des différences essentielles entre systèmes polynomiaux et systèmes linéaires. Néanmoins, quelques convergences dans les méthodes de résolution ont été mises en évidence, notamment le principe d'élimination de variables pour ramener la résolution d'un système sans structure particulière, à celle d'un système triangulaire, et l'obtention de tels systèmes triangulaires par manipulations algébriques sur les équations de départ qui consistent à les multiplier par des polynômes et les additionner les unes aux autres.

Nous verrons de plus que les notions classiques et les algorithmes relevant de l'algèbre linéaire sont des briques de base pour les algorithmes de résolution des systèmes polynomiaux.

II. Liens entre algèbre et géométrie : projection et élimination

On a vu ci-dessus que, à partir d'un système d'équations polynomiales $f_1 = \cdots = f_k = 0$ dans $\mathbb{Q}[X_1, \ldots, X_n]$, on pouvait exhiber une identité algébrique prouvant la non-existence de solutions au système, ou même une représentation triangulaire des solutions en effectuant des manipulations du type $q_1 f_1 + \cdots + q_k f_k$, où $q_1, \ldots, q_k$ sont des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$. Dans la suite, on s'intéresse à l'ensemble de polynômes $\{q_1 f_1 + \cdots + q_k f_k \mid q_i \in \mathbb{Q}[X_1, \ldots, X_n],\ i = 1, \ldots, k\}$ que l'on appellera idéal de l'anneau $\mathbb{Q}[X_1, \ldots, X_n]$ engendré par $f_1, \ldots, f_k$.

II.1. Idéaux et équations : définitions et premières propriétés

Commençons par rappeler la notion d'anneau qui est introduite dans les tomes *Mathématiques L1 et L2*.

Rappel **Anneaux**

Un anneau est un triplet $(A, +, \times)$ tel que :

1) A est un ensemble, et $+$ et $\times$ sont des lois de composition interne (que l'on appellera respectivement addition et multiplication) ;
2) $(A, +)$ est un groupe commutatif, c'est-à-dire $\forall (a, b) \in A \times A$, $a + b = b + a \in A$, il existe $e \in A$ tel que $a + e = a$ et $\forall a \in A$, il existe $a' \in A$ tel que $a + a' = e$;
3) l'opération de multiplication $\times$ est associative et a un élément neutre dans A ;
4) l'opération de multiplication $\times$ est distributive sur $+$, i.e. pour tout x, y, z dans A, on a $(x+y)z = xz+yz$ et $z(x + y) = zx + zy$.

Dans la suite, par abus de langage, on dira que A est un anneau lorsqu'il n'y a pas d'ambiguïté sur les lois de composition interne $+$ et $\times$.

On peut maintenant définir les idéaux d'anneaux.

Définition 1.1. *Soit A un anneau commutatif. Un idéal I de A est un sous-ensemble de A tel que :*

1) $\forall (f,g) \in I \times I,\ f+g \in I$;

2) $\forall f \in I$, *et* $\forall p \in A,\ fp \in I$.

Test 1.1.

Soit I un idéal d'un anneau A. Montrer que I contient 0 (l'élément neutre pour l'addition dans A).

Test 1.2.

Soit I un idéal d'un anneau A. Montrer que $I = A$ si et seulement si I contient 1 (l'élément neutre pour la multiplication dans A).

Test 1.3.

Soient I et J deux idéaux d'un anneau A. Montrer que $I \cap J$ est un idéal de A.

Test 1.4.

Soient I et J deux idéaux d'un anneau A. Montrer que $I + J = \{p+q \mid p \in I\ q \in J\}$ est un idéal de A.

Proposition 1.2. *Considérons $\{f_1,\dots,f_k\} \subset A$. L'ensemble des éléments de A qui s'écrivent sous la forme $p_1f_1+\dots+p_kf_k$ (pour $(p_1,\dots,p_k) \in A^k$) est le plus petit idéal de A contenant $\{f_1,\dots,f_k\}$.*

Preuve. Posons $I = \{p_1f_1+\dots+p_kf_k \mid (p_1,\dots,p_k) \in A^k\}$ et montrons que I est bien un idéal contenant $\{f_1,\dots,f_k\}$. Le fait qu'il contienne f_i pour $i \in \{1,\dots,k\}$ est immédiat (en choisissant $p_j = 0$ pour $j \in \{1,\dots,k\} \setminus \{i\}$). Considérons maintenant $f = \sum_{i=1}^k p_if_i$ et $g = \sum_{i=1}^k q_if_i$ dans I, alors $f+g = \sum_{i=1}^k (p_i+q_i)f_j \in I$. Considérons maintenant $p \in A$. Puisque $pf = \sum_{i=1}^k (pp_i)f_i$, on a bien $pf \in I$. Cela achève de montrer que I est un idéal de A.

On montre maintenant que tout idéal J contenant $\{f_1,\dots,f_k\}$ est inclus dans I. On raisonne par l'absurde en supposant qu'il existe $p = \sum_{i=1}^k p_if_i \in I$ n'appartenant pas à un idéal J de A contenant $\{f_1,\dots,f_k\}$. Or, puisque J contient $\{f_1,\dots,f_k\}$, $p_if_i \in J$ pour tout $i \in \{1,\dots,k\}$. Ainsi, $p = \sum_{i=1} p_if_i \in J$, ce qui est contradictoire avec notre hypothèse. Ainsi, tout idéal J de A contenant $\{f_1,\dots,f_k\}$ contient I. ■

Définition 1.3. *On appelle idéal engendré par $\{f_1,\dots,f_k\} \subset A$ l'ensemble des éléments qui s'écrivent sous la forme $p_1f_1+\dots+p_kf_k$ (pour $(p_1,\dots,p_k) \in A^k$). On le notera $\langle f_1,\dots,f_k\rangle$.*

Définition 1.4. *On dit qu'un idéal $I \subset A$ est radical si pour tout $f \in A$ la relation $f^k \in I$ (pour $k \in \mathbb{N}$) implique $f \in I$.*

Exemple 1.5. Considérons l'idéal $I = \langle X^2\rangle$ de $\mathbb{Q}[X]$. Cet idéal n'est pas radical puisque, s'il l'était, on aurait $X^2 \in I \Rightarrow X \in I$, ce qui impliquerait que X est un multiple de X^2.

Définition 1.6. *Soit I un idéal de A. Le radical de I est l'ensemble des éléments f de A tels qu'il existe $k \in \mathbb{N}$ pour lequel $f^k \in I$. On le notera $\sqrt{I}$.*

Proposition 1.7. *Soit I un idéal de A. Le radical de I est un idéal de A.*

Preuve. Considérons un couple (f,g) du radical de I. Soient $k_f \in \mathbb{N}$ tel que $f^{k_f} \in I$ et $k_g \in \mathbb{N}$ tel que $g^{k_g} \in I$.

1) On montre que $f+g$ est un élément du radical de I. En effet, en choisissant $k = k_f + k_g$, $(f+g)^k = \sum_{i=0}^k \binom{k}{i} f^i g^{k-i} \in I$ puisque pour tout $i \in \{0,\dots,k\}$, $i < k_f$ implique $k-i > k_g$ et donc $f^i g^{k-i} \in I$ et $i \geq k_f$ impliquent $f^i g^{k-i} \in I$.
2) On montre que, pour tout $p \in A$, fp est un élément du radical de I : en effet, $(fp)^{k_f} \in I$ puisque $f^{k_f} \in I$.

■

Exemple 1.8. Le radical de $\langle X^2\rangle \subset \mathbb{Q}[X]$ est évidemment l'idéal $\langle X\rangle$.

Une spécificité des idéaux d'anneaux polynomiaux est qu'il existe toujours un ensemble fini de polynômes qui les engendre. Le lecteur intéressé pourra consulter la preuve de ce résultat fondamental (appelé parfois théorème de la base finie) dans le tome *Algèbre L3* à paraître à l'été 2009 chez le même éditeur.

Théorème 1.9. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. Il existe une famille finie $\{f_1,\dots,f_k\} \subset \mathbb{Q}[X_1,\dots,X_n]$ telle que $I = \langle f_1,\dots,f_k\rangle$.*

Définition 1.10. *Soit $I \subset A$ un idéal. On dit que I est principal s'il existe $f \in A$ tel que $I = \langle f\rangle$.*

Il est démontré dans le chapitre 4 du tome *Mathématiques L2* que tout idéal de $\mathbb{Q}[X]$ est principal. Dans le cas des anneaux de polynômes en plusieurs variables, cela est malheureusement faux comme le montre l'exemple ci-dessous.

EXEMPLE 1.11. Considérons l'idéal $\langle X, Y\rangle$ de $\mathbb{Q}[X, Y]$. Montrons que cet idéal n'est pas principal. En effet, s'il était principal, il existerait f dans $\mathbb{Q}[X, Y]$ tel que $\langle X, Y\rangle = \langle f\rangle$. Cela implique que f doit diviser X et Y et donc que $f = 1$. Or, $f = 1$ implique $1 \in \langle X, Y\rangle$, ce qui est impossible puisque, pour tout couple de polynômes $(q_1, q_2) \in \mathbb{Q}[X, Y] \times \mathbb{Q}[X, Y]$ non nuls, $q_1X + q_2Y$ est de degré strictement positif.

II.2. Idéaux et variétés : géométrie des solutions des systèmes d'équations

Définition 1.12. *On dit que $V \subset \mathbb{C}^n$ est une $\mathbb{Q}$-variété algébrique s'il existe $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[X_1, \ldots, X_n]$ tel que*

$$V = \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_k(x) = 0\}.$$

Soit $x \in \mathbb{C}^n$ tel que $f_1(x) = \cdots = f_k(x) = 0$. Il est alors immédiat que pour tout polynôme $p \in \langle f_1, \ldots, f_k\rangle$, $p(x) = 0$.

Définition 1.13. *Soit I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. On appelle variété algébrique associée à I (que l'on notera dans la suite $V(I)$) le sous-ensemble des points $x \in \mathbb{C}^n$ tels que pour tout $p \in I$, $p(x) = 0$.*

On a précédemment associé une variété algébrique à un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. Le résultat ci-dessous montre comment associer un idéal à une variété algébrique.

Proposition 1.14. *Soit $V \subset \mathbb{C}^n$ une $\mathbb{Q}$-variété algébrique. L'ensemble de polynômes $\{f \in \mathbb{Q}[X_1, \ldots, X_n] \mid \forall x \in V : \quad f(x) = 0\}$ est un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. On l'appelle idéal associé à V et on le note $\mathcal{I}(V)$..*

PREUVE. Soit (f, g) un couple de polynômes dans l'idéal associé à V.

1) On montre que $f + g$ est un élément de l'idéal associé à V : puisque pour tout $x \in V$ $f(x) = 0$ et $g(x) = 0$, on a $(f + g)(x) = 0$.
2) On montre que pour tout $p \in \mathbb{Q}[X_1, \ldots, X_n]$, pf est un élément de l'idéal associé à V : puisque pour tout $x \in V$ $f(x) = 0$, on a $(pf)(x) = 0$.

■

Le théorème ci-dessous est fondamental puisqu'il met en correspondance l'existence de solutions complexes communes à un ensemble de polynômes $f_1, \ldots, f_k$ avec le fait que l'idéal $\langle f_1, \ldots, f_k\rangle = \langle 1\rangle$. La preuve de ce résultat ne relevant pas d'un L3 mathématiques, on supposera ce résultat acquis dans la suite.

Théorème 1.15. (Nulltstellensatz de Hilbert) *Soit $\{f_1, \ldots, f_k\} \subset \mathbb{Q}[X_1, \ldots, X_n]$. La variété algébrique $V(f_1, \ldots, f_k)$ est vide si et seulement si il existe $A_1, \ldots, A_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ tel que $1 = A_1f_1 + \cdots + A_kf_k$*

Autrement dit, la variété algébrique $V(I)$ associée à un idéal I est vide si et seulement si I contient 1.

Théorème 1.16. *Soient I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ et $f \in \mathbb{Q}[X_1, \ldots, X_n]$. Le polynôme f s'annule en tout point de $V(I)$ si et seulement si il existe $k \in N$ tel que $f^k \in I$.*

PREUVE. Montrons d'abord qu'étant donné $f \in \mathbb{Q}[X_1, \ldots, X_n]$ tel qu'il existe $k \in \mathbb{N}$ pour lequel $f^k \in I$, $f \in \mathcal{I}(V(I))$. Si $f^k \in I$, alors pour tout $x \in V(I)$, $f^k(x) = 0$ (par définition de $V(I)$). Cela implique que pour tout $x \in V(I)$, $f(x) = 0$ et donc $f \in \mathcal{I}(V(I))$.

Montrons maintenant que si $f \in \mathcal{I}(V(I))$, alors il existe $k \in \mathbb{N}$ tel que $f^k \in I$. Soient U une nouvelle variable et $f_1, \ldots, f_r$ un ensemble fini de générateurs de I. Donc, la variété définie par $f_1 = \cdots = f_r = Uf - 1 = 0$ est vide dans $\mathbb{C}^n$.

Ainsi, d'après le Nullstellensatz (théorème 1.15), il existe $p_1, \ldots, p_r, p_{r+1}$ dans $\mathbb{Q}[U, X_1, \ldots, X_n]$ tel que $1 = p_1f_1 + \cdots + p_rf_r + p_{r+1}(Uf - 1)$. En substituant U par $1/f$ et en multipliant la relation ci-dessus par une puissance assez grande de f, on obtient bien l'existence de polynômes $g_1, \ldots, g_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ tels que

$$f^k = g_1f_1 + \cdots + g_rf_r.$$

■

Corollaire 1.17. *Soient I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ et $V(I) \subset \mathbb{C}^n$ sa variété algébrique associée, alors $\mathcal{I}(V(I)) = \sqrt{I}$, où $\sqrt{I}$ désigne le radical de I.*

PREUVE. Par définition, $\mathcal{I}(V(I))$ est l'ensemble des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ qui s'annulent en tous les points de $V(I)$. D'après le théorème 1.16, un polynôme f de $\mathbb{Q}[X_1, \ldots, X_n]$ appartient à $\mathcal{I}(V(I))$ si et seulement si il existe $k \in \mathbb{N}$ tel que $f^k \in I$. Par définition du radical d'un idéal, cela est équivalent à dire que $f \in \sqrt{I}$. ■

Une conséquence immédiate du résultat ci-dessus est le corollaire suivant.

Corollaire 1.18. *Soit I un idéal. On a $\mathcal{I}(V(I)) = I$ si et seulement si $\sqrt{I} = I$.*

Exemple 1.19. Considérons l'idéal $I = \langle X, Y^2 \rangle$ de $\mathbb{Q}[X, Y]$. L'ensemble des points de $\mathbb{C}^2$ en lesquels chaque polynôme de I s'annule est constitué de l'origine uniquement. En l'origine, les polynômes X et Y s'annulent. Or X est bien dans I, mais Y n'y est pas. Montrons ce dernier point. Si Y était dans I, il existerait q_1 et q_2 dans $\mathbb{Q}[X, Y]$ tels que $Y = q_1 X + q_2 Y^2$. Ici q_1 est forcément non nul, sinon Y serait un multiple de Y^2, ce qui n'est pas possible. De même, q_2 est non nul sinon Y serait un multiple de X. Donc q_1 et q_2 sont non nuls. Or tous les monômes de $q_1 X$ ont des degrés en X supérieurs à 1. Aussi, tous les monômes de $q_2 Y^2$ ont des degrés en Y supérieurs à 2. Si $q_1 X + q_2 Y^2$ contient des monômes de degrés en X supérieurs à 1, on a une contradiction puisque Y est de degré 0 en X. Donc $q_1 X + q_2 Y^2$ ne contient que des monômes de degré 2 en Y, ce qui n'est pas possible non plus puisque Y est de degré 1 en Y.

En revanche, on vérifie aisément que $Y \in \sqrt{I}$. On peut même montrer que $\langle X, Y \rangle = \sqrt{I}$. En effet, considérons un polynôme $p \in \mathbb{Q}[X, Y]$ qui s'annule en $(0, 0)$. Considérons la division euclidienne de p par X (lorsque p est vu comme un polynôme de $\mathbb{Q}[Y][X]$). On obtient alors l'identité $p = q_1 X + r$ avec $\deg(r, X) = 0$, ce qui implique $r \in \mathbb{Q}[Y]$. Puisque p s'annule en $(0, 0)$, on obtient immédiatement le fait que r s'annule en 0, si bien que Y est un facteur de r. Autrement dit, il existe un polynôme q_2 tel que $r = q_2 Y$. Ainsi tous les polynômes qui s'annulent sur l'origine peuvent s'écrire $q_1 X + q_2 Y$, ce qui achève de montrer que $\langle X, Y \rangle = \sqrt{I}$.

Synthèse — **Idéaux (algèbre) et variétés algébriques (géométrie)**

1) Tout idéal I de $\mathbb{Q}[X_1, \ldots, X_n]$ est engendré par un ensemble fini d'éléments de $\mathbb{Q}[X_1, \ldots, X_n]$.
2) On associe à un idéal I de $\mathbb{Q}[X_1 \ldots, X_n]$ un ensemble de points $V(I)$ de $\mathbb{C}^n$, que l'on appelle $\mathbb{Q}$-variété algébrique, tel que tout polynôme de I s'annule en chaque point de $V(I)$.
3) L'ensemble des polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ qui s'annulent en chaque point de $V(I)$ est un idéal radical qui contient I. C'est en fait le radical de I.

II.3. Notion de dimension

On a établi dans la section précédente une correspondance entre objets algébriques (les idéaux) et objets géométriques (les variétés algébriques). Par ailleurs, on a vu en introduction que la *nature* des objets géométriques pouvait être changeante puisque l'on pouvait avoir affaire à un ensemble fini de points (c'est le cas de la variété algébrique associée à $\langle X, Y \rangle$) ou à un ensemble infini de points (par exemple, la droite associée à $\langle X - Y \rangle$). Dans le premier cas (nombre fini de points), on n'a aucun degré de liberté pour se déplacer sur la variété algébrique associée à l'idéal considéré, alors que dans le second, on peut se déplacer en suivant une direction donnée par le vecteur directeur de la droite définie par $X - Y = 0$. Cette notion intuitive de degré de liberté porte un nom, il s'agit de la dimension de la variété algébrique considérée. L'objet de cette sous-section est de définir rigoureusement une telle notion.

Définition 1.20. *Soit $V \subset \mathbb{C}^n$ une $\mathbb{Q}$-variété algébrique. La dimension de V est le plus grand entier d tel que la propriété suivante est satisfaite : il existe une $\mathbb{Q}$-variété algébrique W de $\mathbb{C}^d$ telle que la projection $(x_1, \ldots, x_n) \in \mathbb{C}^n \to (x_{i_1}, \ldots, x_{i_d}) \in \mathbb{C}^d$ (où $\{i_1, \ldots, i_d\}$ est un sous-ensemble de $\{1, \ldots, n\}$) est surjective en dehors de W.*

Par convention, on dira que la dimension d'une variété algébrique vide est -1.

Exemple 1.21. Considérons la variété de $\mathbb{C}^2$ définie par $X = Y = 0$. Il s'agit de l'origine. Cette variété est de dimension 0 car elle est non vide et que l'on ne peut projeter surjectivement un point sur une droite.

Considérons maintenant la variété algébrique de $\mathbb{C}^2$ définie par $Y - X^2 = 0$. Celle-ci est de dimension au plus 1 car il existe des points de $\mathbb{C}^2$ qui ne lui appartiennent pas. Elle est de dimension 1 exactement car la projection sur l'axe des X dans $\mathbb{C}^2$ restreinte à cette variété est clairement surjective (pour tout $a \in \mathbb{C}$, il existe $b \in \mathbb{C}$ tel que $b = a^2$).

Considérons maintenant la variété algébrique V de $\mathbb{C}^2$ définie par $XY - 1 = 0$, ainsi que la projection $\pi : (x, y) \to x$. Clairement, $V \cap \pi^{-1}(0)$ est vide puisqu'elle serait alors définie par l'équation $1 = 0$ qui est inconsistante. Néanmoins, pour toute valeur complexe $a \neq 0$, $V \cap \pi^{-1}(a)$ est non vide (puisque $aY - 1 = 0$ a forcément une solution dans le cas où $a \neq 0$). La dimension de cette variété algébrique est donc 1.

Définition 1.22. *On appelle $\mathbb{Q}$-hypersurface $\mathcal{H}$ de $\mathbb{C}^n$ une $\mathbb{Q}$-variété algébrique de dimension $n - 1$.*

On définit la dimension des idéaux à partir de la définition des variétés algébriques donnée ci-dessus.

Définition 1.23. *Soit I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$. On appelle dimension de I la dimension de la variété algébrique $V(I)$ associée à I.*

Une conséquence immédiate de la définition de dimension est le résultat suivant.

Proposition 1.24. *Une $\mathbb{Q}$-variété algébrique de dimension zéro est un ensemble fini de points de $\mathbb{C}^n$.*

II.4. Anneaux-quotients : définition et propriétés

La structure algébrique d'anneau-quotient que nous introduisons ici est celle qui permet d'effectuer des calculs *modulo* l'idéal engendré par un système d'équations polynomiales. Dans le cas de polynômes à une variable, cette structure algébrique est déjà introduite dans le chapitre 5 du tome *Mathématiques L2*. L'exposé que nous en faisons ici est plus général, considérant les situations en plusieurs variables.

Définition 1.25. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$ et $f \in \mathbb{Q}[X_1,\dots,X_n]$. On appelle classe d'équivalence de f modulo I l'ensemble de polynômes $\{g \in \mathbb{Q}[X_1,\dots,X_n] \mid f-g \in I\}$.*

Soient $f \in \mathbb{Q}[X_1,\dots,X_n]$ et I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. On note $\overline{f}^I$ la classe d'équivalence de f modulo I. S'il n'y a pas d'ambiguïté sur l'idéal concerné, on utilisera aussi la notation $\overline{f}$.

Test 1.5.

Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. Montrer que la classe d'équivalence de 0 modulo I est l'idéal I.

Test 1.6.

Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$ contenant 1. Montrer que la classe d'équivalence de 1 modulo I est $\mathbb{Q}[X_1,\dots,X_n]$.

Test 1.7.

Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. Pour f et g dans $\mathbb{Q}[X_1\dots,X_n]$, on dit qu'ils sont équivalents (et l'on note $f \sim_I g$) si et seulement si g appartient à la classe d'équivalence de f modulo I. Montrer que $\sim_I$ est une relation d'équivalence, c'est-à-dire qu'elle est réflexive, symétrique et transitive.

Proposition 1.26. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. On note A l'ensemble des classes d'équivalence des polynômes de $\mathbb{Q}[X_1,\dots,X_n]$.*
Soit $\phi : (\overline{f},\overline{g}) \in A\times A \to \{p+q \mid p \in \overline{f}^I \ q \in \overline{g}^I\}$ et $\psi : (\overline{f},\overline{g}) \in A\times A \to \{pq \mid p \in \overline{f}^I \ q \in \overline{g}^I\}$, alors (A,ϕ,ψ) est un anneau.

PREUVE. On vérifie chacune des propriétés caractérisant un anneau.

1) Il est clair que $\phi(\overline{f},\overline{g}) = \phi(\overline{g},\overline{f})$ par commutativité de l'addition dans $\mathbb{Q}[X_1,\dots,X_n]$. De plus, $\phi(\overline{f},\overline{0}) = \overline{f}$ puisque pour tout $p \in \overline{f}$ et tout $g \in I$, on a $p+g-f \in I$. Enfin, $\phi(\overline{f},\overline{-f}) = \overline{0}$ puisque, pour tout $(p,q) \in \overline{f}\times\overline{-f}$, on a $p-q = p-f-(q-f) \in I$. Donc, (A,ϕ) est bien un groupe commutatif.
2) Il nous faut aussi montrer que $\psi(\overline{f},\overline{g}) \in \frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$. Soient $p \in \overline{f}$ (donc $p-f \in I$) et $q \in \overline{g}$ (donc $q-g \in I$). Il suffit alors de montrer que $pq-fg \in I$. Pour cela, remarquons que $pq-fg = (p-f+f)(q-g+g)-fg = (p-f)g+f(q-g)+fg-fg = (p-f)g+f(q-g)$, qui est bien dans I puisque $p-f \in I$ et $q-g \in I$.
3) Montrons que $\overline{1}$ est un élément neutre pour ψ. Soient $p \in \overline{f}$ et $q \in \overline{1}$, donc on a $q-1 \in I$ et $p-f \in I$. Il suffit de montrer que $qp \in \overline{f}$. Pour cela, remarquons que $qp-f = (q-1+1)p-f = (q-1)p+p-f$. Comme $(q-1) \in I$ et $p-f \in I$, on a bien $qp-f \in I$.
4) L'associativité de ψ est une conséquence directe de celle de $\times$ dans $\mathbb{Q}[X_1,\dots,X_n]$.
5) La distributivité de la multiplication sur l'addition dans $\mathbb{Q}[X_1,\dots,X_n]$ implique la distributivité de ψ sur ϕ.

■

Définition 1.27. *Dans la suite, l'anneau A sera noté $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$. On l'appellera anneau-quotient de $\mathbb{Q}[X_1,\dots,X_n]$ par I (ou plus simplement, lorsqu'il n'y a pas d'ambiguïté, anneau-quotient). De plus, pour $\overline{f},\overline{g}$ dans $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$, $\phi(\overline{f},\overline{g})$ et $\psi(\overline{f},\overline{g})$ seront respectivement notées $\overline{f}+\overline{g}$ et $\overline{f}.\overline{g}$.*

Proposition 1.28. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. Pour tout $(\lambda,\mu) \in \mathbb{Q}\times\mathbb{Q}$ et pour tout $(f,g) \in \mathbb{Q}[X_1,\dots,X_n]\times\mathbb{Q}[X_1,\dots,X_n]$, on a $\overline{\lambda f+\mu g} = \lambda\overline{f}+\mu\overline{g}$.*

PREUVE. Montrer cette égalité entre classe d'équivalence revient à montrer ce qui suit.

1) Tout polynôme $p \in \mathbb{Q}[X_1,\dots,X_n]$ équivalent à $\lambda f+\mu g$ s'écrit sous la forme $\lambda p_f+\mu p_g$ telle que p_f et p_g sont des polynômes de $\mathbb{Q}[X_1,\dots,X_n]$ respectivement équivalents à f et g.
2) Tout polynôme qui s'écrit $\lambda p_f+\mu p_g$, tel que p_f et p_g sont des polynômes de $\mathbb{Q}[X_1,\dots,X_n]$ respectivement équivalents à f et g, est équivalent à $\lambda f+\mu g$.

Dans la suite, on note $f_1,\dots,f_r$ un ensemble fini de générateurs de I (un tel ensemble existe d'après le théorème 1.9). Considérons donc $p \in \overline{\lambda f+\mu g}$. Il existe alors $p_1,\dots,p_r$ dans $\mathbb{Q}[X_1,\dots,X_n]$ tels que $p = \lambda f+\mu g+\sum_{i=1}^r p_i f_i$. On récrit cette relation sous la forme $p = \lambda f+\frac{1}{2}(\sum_{i=1}^r p_i f_i)+\mu g+\frac{1}{2}(\sum_{i=1}^r p_i f_i)$. Il est alors clair que $q_f = \lambda f+\frac{1}{2}(\sum_{i=1}^r p_i f_i)$ et $q_g = \mu g+\frac{1}{2}(\sum_{i=1}^r p_i f_i)$ appartiennent respectivement à $\overline{\lambda f}$ et $\overline{\mu g}$. Il est ensuite immédiat (en considérant $p_f = q_f/\lambda$ et $p_g = q_f/\mu$) d'obtenir la première assertion.

Considérons maintenant p_f et p_g respectivement équivalents à f et g et montrons que $\lambda p_f+\mu p_g$ est équivalent à $\lambda f+\mu g$. Du fait que p_f et p_g sont respectivement équivalents à f et g, on a l'existence de $q_1,\dots,q_r$ et $g_1,\dots,g_r$ dans $\mathbb{Q}[X_1,\dots,X_n]$ tels que $p_f = f+\sum_{i=1}^r q_i f_i$ et $p_g = g+\sum_{i=1}^r g_i f_i$, ce qui implique que $\lambda p_f+\mu p_g = (\lambda f+\mu g)+\sum_{i=0}^r (g_i+q_i)f_i$. ■

Une conséquence immédiate du résultat ci-dessus est que $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un $\mathbb{Q}$-espace vectoriel.

Corollaire 1.29. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. L'anneau-quotient $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un $\mathbb{Q}$-espace vectoriel.*

Proposition 1.30. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. L'anneau-quotient $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$, en tant que $\mathbb{Q}$-espace vectoriel, est engendré par l'ensemble des classes d'équivalence de tous les monômes de $\mathbb{Q}[X_1,\dots,X_n]$.*

Preuve. L'anneau $\mathbb{Q}[X_1,\dots,X_n]$ est engendré, en tant que $\mathbb{Q}$-espace vectoriel, par l'ensemble des monômes de $\mathbb{Q}[X_1,\dots,X_n]$ (tout polynôme s'écrit comme somme finie de termes, c'est-à-dire somme de monômes multipliés par des éléments de $\mathbb{Q}$). Le résultat est alors une conséquence de la proposition 1.28. ■

Exemple 1.31. On peut alors sans peine donner une description de $\frac{\mathbb{Q}[X,Y]}{\langle X,Y\rangle}$. On regarde d'abord les images des monômes de degrés inférieurs ou égaux à 1. On obtient comme classes d'équivalence celles de 1 et de 0 (puisque trivialement $X \in \langle X,Y\rangle$ et $Y \in \langle X,Y\rangle$). On vérifie alors sans peine que tout monôme de degré supérieur ou égal à 2 est dans la classe d'équivalence de 0. Pour cela, on montre la relation suivante : si $f \in \overline{0}$, alors pour tout $g \in \mathbb{Q}[X_1,\dots,X_n]$, $\overline{fg} = \overline{0}$. Il suffit de montrer que $fg \in I$, qui est une conséquence directe de $f \in \overline{0} \Leftrightarrow f \in I$ et du fait que I est un idéal. On a donc un espace vectoriel de dimension 1 (engendré par $\overline{1}$).

Méthode **Description d'un anneau-quotient $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$**

On voit ici que pour obtenir une description de $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ en tant que $\mathbb{Q}$-espace vectoriel, il suffit de décrire les images des monômes de $\mathbb{Q}[X_1,\dots,X_n]$ degré par degré. La description est *complète* lorsque, à partir d'un certain degré :

1) tous les monômes de ce degré sont dans la classe d'équivalence de 0 (ils sont alors dans I) et, dans ce cas, $\frac{\mathbb{Q}[X_1,\dots,X_n}{I}$ est un $\mathbb{Q}$-espace vectoriel de dimension finie ;
2) on sait identifier les monômes qui ont une même classe d'équivalence, ce qui revient à tester si la différence de deux monômes appartient à l'idéal.

Exemple 1.32. Appliquons cette méthode à $\frac{\mathbb{Q}[X,Y]}{\langle X,Y^2\rangle}$. La classe d'équivalence de 1 est toujours dans le quotient. Les classes d'équivalence de X et Y sont respectivement $\overline{0}$ (car $X \in \langle X,Y^2\rangle$) et $\{f \in \mathbb{Q}[X,Y] \mid f - Y \in \langle X,Y^2\rangle\}$. Les classes d'équivalence de X^2, Y^2 et XY sont celles de 0 (il est immédiat de voir que ces monômes appartiennent à l'idéal $\langle X,Y^2\rangle$). On obtient un espace vectoriel de dimension 2 car on peut montrer sans peine que $\overline{1} \neq \overline{X}$: en effet, dans le cas contraire, $X - 1$ s'annule en la variété associée à $\langle X,Y^2\rangle$ constituée de l'origine, ce qui n'est évidemment pas le cas.

Voyons maintenant un cas où l'idéal considéré n'est pas de dimension 0. Considérons l'idéal $I = \langle XY\rangle$ dans $\mathbb{Q}[X,Y]$. La classe de 1 est $\{f \in \mathbb{Q}[X,Y] \mid f - 1 \in I\}$ (par exemple $XY + 1$ est dedans). Les classes de X et Y sont respectivement $\{f \in \mathbb{Q}[X,Y] \mid f - X \in I\}$ et $\{f \in \mathbb{Q}[X,Y] \mid f - Y \in I\}$. À titre d'exemple, elles contiennent respectivement $XY + X$ et $XY + Y$. Elles sont bien différentes car $X - Y \notin I$. En effet, I est principal donc si $X - Y \in I$, c'est un multiple de XY, ce qui n'est évidemment pas le cas. On décrit de la même manière les classes d'équivalence de X^i et Y^i dont on montre qu'elles sont bien différentes les unes des autres par l'argument que l'on vient d'utiliser. En revanche, il est facile de remarquer que pour tout $i > 0, j > 0$, on a $\overline{X^iY^j} = \overline{0}$ puisque X^iY^j sont multiples de XY si et seulement si $i > 0, j > 0$. Finalement, on a les classes d'équivalence (toutes distinctes deux à deux) des monômes X^i et Y^j pour $i \geq 0$ et $j \geq 0$, ainsi que celles de 0.

Test 1.8.

Décrire l'anneau-quotient $\frac{\mathbb{Q}[X,Y]}{\langle X-1,Y-1\rangle}$ en tant que $\mathbb{Q}$-espace vectoriel. Cet espace vectoriel est-il de dimension finie ?

Si oui quel est sa dimension ? La variété associée à $\langle X-1,Y-1\rangle$ est-elle de dimension 0 ? Si oui, combien a-t-elle de solutions ?

II.5. Des idéaux de dimension zéro à l'algèbre linéaire

On se propose de montrer le résultat fondamental ci-dessous. Ce résultat est important car il permet de réduire la résolution des systèmes polynomiaux à la résolution de systèmes linéaires.

Théorème 1.33. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$, alors I est de dimension 0 si et seulement si $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un $\mathbb{Q}$-espace vectoriel de dimension finie.*
Dans ce cas, le nombre d'éléments de $V(I)$ est borné par la dimension de $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$.
De plus, pour tout $1 \leq i \leq n$, l'idéal $I \cap \mathbb{Q}[X_i]$ est un idéal principal de générateur non nul.

La preuve de ce théorème nécessite quelques résultats intermédiaires.

Étant donné un idéal I engendré par $f_1,\dots,f_k$ dans $\mathbb{Q}[X_1,\dots,X_n]$, on note $I_{\mathbb{C}}$ l'idéal $\{\sum_i p_i f_i \mid p_i \in \mathbb{C}[X_1,\dots,X_n]\}$ de $\mathbb{C}[X_1,\dots,X_n]$.

Lemme 1.34. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$, alors on a $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I} \subset \frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$.*

Preuve. Montrer que $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I} \subset \frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ revient à montrer que $\forall f \in \mathbb{Q}[X_1,\dots,X_n], \overline{f}^I = \overline{f}^{I_{\mathbb{C}}} \cap \mathbb{Q}[X_1,\dots,X_n]$. Par définition de $I_{\mathbb{C}}$, il est évident que $\overline{f}^I \subset \overline{f}^{I_{\mathbb{C}}}$. Dans la suite, on montre que si $g \in \overline{f}^{I_{\mathbb{C}}} \cap \mathbb{Q}[X_1,\dots,X_n]$, alors $g \in \overline{f}^I$.

On considère $f_1,\dots,f_k$ une famille finie de générateurs de I (l'existence d'une telle famille est une conséquence directe du théorème 1.9). Soient f et g des éléments de $\mathbb{Q}[X_1,\dots,X_n]$ tels que $\overline{f}^{I_{\mathbb{C}}} = \overline{g}^{I_{\mathbb{C}}}$. Il existe des polynômes $p_1,\dots,p_k$ dans $\mathbb{C}[X_1,\dots,X_n]$ tels que

$$f - g = \sum_{i=1}^{k} p_i f_i.$$

L'identité ci-dessus peut être vue comme un système d'équations linéaires à résoudre (les inconnues étant les coefficients des polynômes p_i) *à coefficients rationnels*. L'existence de polynômes $p_1,\dots,p_k$ dans $\mathbb{C}[X_1,\dots,X_n]$, satisfaisant l'identité ci-dessus, assure l'existence de solutions à ce système linéaire à coefficients rationnels. Comme on l'a rappelé en introduction de ce chapitre, le fait que ce système linéaire soit consistant et à coefficients rationnels finit de montrer l'existence de solutions à coefficients rationnels. On peut donc choisir les polynômes p_i dans $\mathbb{Q}[X_1,\dots,X_n]$. Ainsi $\overline{f}^{I_{\mathbb{C}}} = \overline{g}^{I_{\mathbb{C}}}$ implique que $\overline{f}^I = \overline{g}^I$. On a donc bien montré que si $g \in \overline{f}^{I_{\mathbb{C}}} \cap \mathbb{Q}[X_1,\dots,X_n]$, alors $g \in \overline{f}^I$. ■

Lemme 1.35. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$. L'anneau-quotient $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un espace vectoriel de dimension finie si et seulement si $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ est un espace vectoriel de dimension finie. Dans ce cas, ils ont la même dimension.*

Preuve. On suppose dans un premier temps que $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ est un espace vectoriel de dimension finie D. Considérons les classes d'équivalence d'un ensemble fini de $D' > D$ monômes de $\mathbb{Q}[X_1,\dots,X_n]$. Ces classes sont évidemment linéairement dépendantes dans $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ puisque $D' > D$, ce qui implique qu'elles sont aussi linéairement dépendantes dans $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$. Cela étant valable pour toute famille de monômes de cardinalité supérieure à D, et $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ étant engendré par les classes d'équivalence de monômes, on a donc $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ de dimension finie, sa dimension n'étant pas supérieure à celle de $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$.

Supposons maintenant que $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ est un espace vectoriel de dimension finie D. Soient $f_1,\dots,f_{D'}$ des éléments de $\mathbb{Q}[X_1,\dots,X_n]$ (avec $D' > D$) et $g_1,\dots,g_k$ une famille finie de polynômes de $\mathbb{Q}[X_1,\dots,X_n]$ engendrant I.

Puisque $D' > D$, il existe donc $\lambda_1,\dots,\lambda_{D'}$ dans $\mathbb{C}^{D'}$ et $p_1,\dots,p_k$ dans $\mathbb{C}[X_1,\dots,X_n]$ tels que

$$\sum_{i=1}^{D'} \lambda_i f_i = \sum_{j=1}^{k} p_j g_j.$$

Comme précédemment, on interprète la relation ci-dessus en termes de résolution de système linéaire à coefficients rationnels qui aurait une solution à coefficients complexes (les inconnues étant ici les λ_i et les coefficients des polynômes p_i). De tels systèmes ont forcément des solutions rationnelles. Ainsi il existe $q_1,\dots,q_k$ dans $\mathbb{Q}[X_1,\dots,X_n]$ et des rationnels $\mu_1,\dots,\mu_{D'}$ tels que

$$\sum_{i=1}^{D'} \mu_i f_i = \sum_{j=1}^{k} q_j g_j.$$

La dimension de $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ (en tant qu'espace vectoriel) est donc inférieure ou égale à celle de $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$. ■

Définition 1.36. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$ de dimension zéro. On dit qu'un élément u de $\mathbb{Q}[X_1,\dots,X_n]$ est un élément séparant pour $V(I)$ si u prend des valeurs distinctes en les éléments distincts de $V(I)$.*

Exemple 1.37. Considérons l'idéal $I = \langle X, Y^2 - 1\rangle$ dans $\mathbb{Q}[X,Y]$. Il est clair que cet idéal est de dimension zéro puisque sa variété associée est l'ensemble fini de points $V(I) = \{(0,1),(0,-1)\}$. On vérifie alors aisément que X n'est pas un élément séparant pour $V(I)$, alors que Y l'est.

Étant donné deux entiers i et j, on note $\binom{i}{j}$ le binomial $\frac{i!}{(i-j)!j!}$.

Lemme 1.38. *Soient I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$ de dimension 0 et D le nombre d'éléments de $V(I)$. Alors il existe $i \in \{0,\dots,(n-1)\binom{D}{2}\}$ tel que la forme linéaire*

$$u_i = X_1 + iX_2 + \cdots + i^{n-1}X_n$$

est un élément séparant de $V(I)$.

Preuve. Soit $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ deux éléments distincts de $V(I)$. On considère $\ell(x, y)$ le nombre d'entiers i compris entre 0 et $(n-1)\binom{D}{2}$ tels que $u_i(x) = u_i(y)$. Puisque le polynôme

$$(x_1 - y_1) + (x_2 - y_2)T + \cdots + (x_n - y_n)T^{n-1}$$

n'est pas identiquement nul (puisque $x \neq y$), il ne peut avoir plus de $n-1$ racines distinctes. Il s'ensuit que $\ell(x, y) \leq n-1$ puisque, par définition, $\ell(x, y)$ est aussi le nombre de racines entières du polynôme ci-dessus, comprises entre 0 et $(n-1)\binom{D}{2}$. Comme le nombre de couples de $V(I)$ est $\binom{D}{2}$, on obtient le résultat recherché. ■

Lemme 1.39. *Soit D le nombre d'éléments de $V(I)$. Alors u est un élément séparant de $V(I)$ si et seulement si $1, u, \ldots, u^{D-1}$ sont linéairement indépendants dans $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$.*

Preuve. On raisonne par l'absurde. Supposons qu'il existe des rationnels c_i tels que la classe d'équivalence de $\sum_{i=0}^{D-1} c_i u^i$ est celle de 0 dans $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$. Cela équivaut à dire que $\sum_{i=0}^{D-1} c_i u^i$ appartient à I. Ainsi, pour tout $x \in V(I)$, $\sum_{i=0}^{D-1} c_i u^i(x) = 0$ et le polynôme $\sum_{i=0}^{D-1} c_i T^i$ de degré $D-1$ auraient D racines complexes, ce qui est évidemment impossible. ■

Nous disposons maintenant de tous les éléments nécessaires à la preuve du théorème 1.33.

Preuve. (du théorème 1.33) Si I est de dimension 0, alors $V(I)$ est un ensemble fini de points dans $\mathbb{C}^n$. On note π_i la projection

$$\begin{array}{rccc} \pi_i : & \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ & (x_1, \ldots, x_n) & \to & x_i. \end{array}$$

Notons $\xi_1, \ldots, \xi_d$ les nombres complexes constituant $\pi_i(V(I))$. Pour tout $j \in \{1, \ldots, d\}$, il existe $g_j \in \mathbb{C}[X_i]$ tel que $g_j(\xi_j) = 0$. Le polynôme $g = \prod_{j=1}^{d} g_j$ s'annule sur $V(I)$. D'après le théorème 1.16, cela implique l'existence d'un entier k tel que $g^k \in I_{\mathbb{C}} \cap \mathbb{C}[X_i]$.

Ainsi, pour tout $i \in \{1, \ldots, n\}$, $I_{\mathbb{C}} \cap \mathbb{C}[X_i] \neq \varnothing$. On note q_i un élément de l'intersection $I_{\mathbb{C}} \cap \mathbb{C}[X_i]$. Il est alors facile de vérifier que $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$ est engendré en tant qu'espace vectoriel par les classes d'équivalence des monômes $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, avec pour tout $1 \leq i \leq n$, $0 \leq \alpha_i \leq \deg(q_i)$. $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$ est donc bien un espace vectoriel de dimension finie. Le lemme 1.35 permet alors de conclure que $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est lui aussi un espace vectoriel de dimension finie (sa dimension est la même que celle de $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$).

Montrons maintenant que le fait que $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ soit un espace vectoriel de dimension finie implique que I est de dimension 0. Soit D la dimension de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$. Donc les classes d'équivalence $1, X_1, \ldots, X_1^D$ sont linéairement dépendantes. En termes équivalents, il existe $\lambda_0, \ldots, \lambda_D$ dans $\mathbb{Q}^{D+1}$ tels que $\sum_{i=0}^{D} \lambda_i X_1^i$ est dans la même classe d'équivalence que 0.

Il existe ainsi $p \in \mathbb{Q}[X_1] \cap I$ non nul. Ce polynôme p s'annule en chaque point de $V(I)$. Cela est valable pour toutes les variables X_i. Donc, $V(I)$ est bien un ensemble fini de points dans $\mathbb{C}^n$, elle est bien de dimension 0. Par définition, I est donc lui aussi de dimension 0.

La deuxième partie du théorème est une conséquence immédiate des lemmes 1.38 et 1.39. ■

Synthèse — **Idéaux de dimension 0 et anneaux-quotients**

Soit $I \subset \mathbb{Q}[X_1, \ldots, X_n]$ un idéal de dimension 0. Sa variété associée $V(I) \subset \mathbb{C}^n$ est donc un ensemble fini de points. On notera D la cardinalité de $V(I)$.

1) L'anneau-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est un $\mathbb{Q}$-espace vectoriel de dimension finie.
2) Un élément $u \in \mathbb{Q}[X_1, \ldots, X_n]$ est un élément séparant de $V(I)$ si et seulement si pour tout $(x, y) \in V(I) \times V(I)$, on a $u(x) = u(y) \Leftrightarrow x = y$.
3) Les classes d'équivalence de $1, u, \ldots, u^{D-1}$ sont des vecteurs libres dans $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$.

Un point essentiel, qui apparaît dans la preuve du théorème 1.33, est la relation entre élimination de variables et projection des solutions.

4) En effet, on a aussi montré que, pour tout $1 \leq i \leq n$, $I \cap \mathbb{Q}[X_i]$ est non vide et le polynôme générateur de cet idéal s'annule en tous les éléments de $\{\pi_i(\alpha) \mid \alpha \in V(S)$, où π_i est la projection $(x_1, \ldots, x_n) \to x_i\}$.

II.6. Notion de degré et multiplicité

On a vu précédemment que dans le cas où un idéal I de $\mathbb{Q}[X_1, \ldots, X_n]$ est de dimension 0, l'anneau-quotient $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est un espace vectoriel de dimension finie. On est donc naturellement enclin à exploiter cette structure algébrique pour y faire des opérations d'algèbre linéaire. Évidemment, la dimension de l'espace vectoriel

$\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ va jouer un rôle essentiel dans la taille des calculs que nous devrons effectuer, puisque les matrices représentant les endomorphismes de $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$ auront pour taille cette dimension.

Définition 1.40. *Soit I un idéal de $\mathbb{Q}[X_1,\dots,X_n]$ de dimension 0. Le degré de I est la dimension de l'espace vectoriel $\frac{\mathbb{Q}[X_1,\dots,X_n]}{I}$.*

On peut aussi définir le degré d'une $\mathbb{Q}$-variété algébrique de dimension 0 comme suit.

Définition 1.41. *Le degré d'une variété algébrique V de dimension 0 est défini comme étant le degré de $\mathcal{I}(V)$.*

Le théorème 1.33 nous indique que le degré d'un idéal $I \subset \mathbb{Q}[X_1,\dots,X_n]$ borne le nombre d'éléments de la variété algébrique $V \subset \mathbb{C}^n$ définie par I. Se posent alors les questions suivantes : à quelle condition ces deux quantités sont-elles égales et qu'est-ce qui quantifie une éventuelle différence ? La résolution des exercices ci-dessous donne l'intuition permettant de répondre à cette question : à chaque élément de V, est attachée une quantité – la multiplicité – relative à I.

Test 1.9.

Quel est le degré de l'idéal $\langle X, Y\rangle \subset \mathbb{Q}[X,Y]$?

Test 1.10.

Quel est le degré de l'idéal $\langle X^2, Y\rangle \subset \mathbb{Q}[X,Y]$?

Dans la suite, nous introduisons les notions nécessaires permettant de définir rigoureusement la notion de multiplicité dans notre contexte.

Définition 1.42. *On appelle anneau local A un anneau tel que pour tout $a \in A$, a est inversible ou $a+1$ est inversible.*

Ainsi, tout corps est un anneau local.

Étant donné un sous-ensemble multiplicatif S d'un anneau A (c'est-à-dire un sous-ensemble clos par multiplication), on définit une relation d'équivalence entre des couples (a,s) de $A \times S$ par

$$(a,s) \sim (a',s') \Leftrightarrow \exists t \in S \mid t(as' - a's) = 0.$$

La classe d'équivalence d'un couple (a,s) est notée dans la suite $\frac{a}{s}$.

Définition 1.43. *On appelle anneau des fractions (et l'on note $S^{-1}A$), l'ensemble des classes d'équivalence $\frac{a}{s}$ avec $(a,s) \in A \times S$ muni des opérations d'addition et de multiplication ci-dessous :*

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'},$$
$$\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}.$$

Dans la suite, étant donné un idéal $I \subset \mathbb{Q}[X_1,\dots,X_n]$ de dimension 0, on note $\bar{A}$ l'anneau-quotient $\frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$. Étant donné $x \in V(I)$, on note S_x les éléments de $\bar{A}$ qui ne s'annulent pas en x. On vérifie sans peine qu'il s'agit bien d'un sous-ensemble clos par multiplication de $\bar{A}$.

Définition 1.44. *La localisation $\bar{A}_x$ de $\bar{A}$ en $x \in V(I_{\mathbb{C}})$ est l'anneau des fractions $S_x^{-1}\bar{A}$.*

Lemme 1.45. *L'anneau $S_x^{-1}\bar{A}$ est un anneau local.*

Preuve. Un élément $\frac{a}{b}$ de $\bar{A}_x$ est inversible si et seulement si $a \neq 0$. De plus, si $\frac{a}{b}$ n'est pas inversible, $1+\frac{a}{b} = \frac{a+b}{b}$ l'est forcément puisque, par définition, $b \neq 0$. ∎

Proposition 1.46. *Soit I un idéal de dimension zéro. Pour tout $x \in V(I)$, il existe un élément $e_x \in \bar{A} = \frac{\mathbb{C}[X_1,\dots,X_n]}{I_{\mathbb{C}}}$ tel que :*

1) $\sum_{x\in V(I)} e_x = 1$;
2) $e_x e_y = 0$ *pour x et y deux éléments distincts de $V(I)$;*
3) $e_x^2 = e_x$;
4) $e_x(x) = 1$ *pour $x \in V(I)$;*
5) $e_x(y) = 0$ *pour $y \in V(I)\setminus\{x\}$.*

Preuve. La seule difficulté de la preuve consiste à savoir comment définir e_x. Sans nuire à la généralité, supposons que X_1 est un élément séparant de $V(I)$. Pour tout $x \in V(I)$, on notera x_1 sa première coordonnée. La formule d'interpolation de Lagrange (voir le chapitre 2 de ce tome) définit le polynôme

$$\ell_x = \prod_{y\in V(I)\setminus\{x\}} \frac{X_1 - y_1}{x_1 - y_1}.$$

On vérifie sans peine que l'on a $\ell_x(x) = 1$ et $\ell_x(y) = 0$ pour $y \in V(I) \setminus \{x\}$.

Ainsi, pour x et y deux éléments distincts de $V(I)$, $\ell_x\ell_y$ s'annule en chaque élément de $V(I)$. Le Nullstellensatz (voir théorème 1.16) permet alors de déduire que pour tout $x \in V(I)$, il existe $n_x \in \mathbb{N}$ tel que $\ell_x^{n_x}\ell_y^{n_y} = 0$ dans $\bar{A}$ si $y \neq x$ et $\ell_x^{n_x}(x) = 1$. Dans la suite, le polynôme $\ell_x^{n_x}$ est noté p_x. De plus, $V(I)$ et l'ensemble des solutions communes de $\{p_x \mid x \in V(I)\}$ ont une intersection vide (puisque pour tout $x \in V(I)$, on a $p_x(x) = 1$). D'après le théorème 1.15, il existe donc des polynômes q_x (pour $x \in V(I)$) tels que $1 = \sum_{x\in V(I)} q_x p_x$ dans $\bar{A}$. En choisissant $e_x = q_x p_x$, il est alors immédiat de vérifier les propriétés annoncées.

En effet, par construction, on a $1 = \sum_{x\in V(I)} e_x$. De plus, pour x et y deux éléments distincts de $V(I)$, on a $e_x e_y = 0$ en chaque point de $V(I)$ puisqu'ils sont multiples de ℓ_x et ℓ_y et que l'on a vu plus haut que $\ell_x\ell_y$ s'annule en chaque point de $V(I)$. Cela implique immédiatement que $e_x e_y = 0$ dans $\bar{A}$. En multipliant par e_x la relation $1 = \sum_{x\in V(I)} e_x$ et en utilisant le fait que $e_x e_y = 0$ pour $x \neq y$ dans $V(I)$, on déduit que $e_x^2 = e_x$. Enfin, étant donné $x \in V(I)$, montrer que $e_x(x) = 1$ et $e_x(y) = 0$ pour $y \in V(I) \setminus \{x\}$ est une conséquence immédiate du fait que e_x est multiple de ℓ_x. ■

L'élément e_x est appelé idempotent associé à x dans la suite.

Proposition 1.47. *Soit e_x l'idempotent associé à $x \in V(I)$. L'ensemble $e_x\bar{A} = \{e_x a \mid a \in \bar{A}\}$, muni des restrictions de l'addition et de la multiplication de $\bar{A}$ à $e_x\bar{A}$, est un anneau dont l'élément neutre est e_x. De plus, il est isomorphe à $\bar{A}_x$.*

La preuve de ce résultat nécessite de manipuler la notion de morphisme d'anneau que nous rappelons ci-dessous.

Rappel — Morphisme d'anneau

Soient R et R' deux anneaux. Un morphisme d'anneau $\varphi : R \to R'$ vérifie

$$\varphi(1) = 1, \quad \varphi(a+b) = \varphi(a) + \varphi(b) \text{ et } \varphi(ab) = \varphi(a)\varphi(b).$$

Preuve. Soit $p \in e_x\bar{A}$. Il existe donc $q \in \bar{A}$ tel que $p = e_x q$ et puisque $e_x^2 = e_x$, on a $e_x p = e_x q = p$. Montrons maintenant que $e_x\bar{A}$ est isomorphe à $\bar{A}_x$.

Considérons maintenant un élément g de $\bar{A}$ tel que $g(x) \neq 0$. Nous allons montrer que cela implique que $e_x g$ est inversible dans $e_x\bar{A}$. En effet, $g - g(x)$ s'annule en 0 alors que $g(x) \neq 0$ par hypothèse. Donc il existe h tel que $g = g(x)(1+h)$, avec $h(x) = 0$. Puisque pour tout $y \in V(I)$, $(he_x)(y) = 0$, il existe $N \in \mathbb{N}$ tel que $(he_x)^N$ a la même classe d'équivalence que 0 dans $\bar{A}$. Ainsi $e_x(1+h)$ est inversible dans $\bar{A}$. Son inverse est

$$(1 - e_x h + \cdots + (-h)^{N-1})e_x$$

et il s'ensuit que $e_x g$ est inversible.

Ainsi, en notant $(e_x g)^{-1}$ l'inverse de $e_x g$ dans $e_x\bar{A}$, considérons l'application de $\bar{A}_x$ dans $\bar{A}$ qui associe $f(e_x g)^{-1}$ à $\frac{f}{g}$. Vérifier qu'il s'agit d'un morphime d'anneau est aisé. Réciproquement, on associe $\frac{f}{1}$ à fe_x. Il s'agit, là aussi, d'un morphisme d'anneau de $e_x\bar{A}$ dans $\bar{A}$. Il reste à vérifier que ces deux morphismes sont inverses l'un de l'autre. Cela revient à prouver que $\frac{f(e_x g)^{-1}}{1} = \frac{f}{g}$ dans $\bar{A}_x$, ce qui est une conséquence du fait que $fe_x((e_x g)(e_x g)^{-1} - 1) = 0$ puisque $e_x(x) = 1$. ■

Théorème 1.48. *Pour tout $x \in V(I)$, il existe un idempotent e_x tel que $e_x\bar{A}$ est isomorphe à $\bar{A}_x$ et $\bar{A}$ est isomorphe (en tant qu'espace vectoriel) au produit cartésien d'anneaux locaux*

$$\prod_{x\in V(I)} \bar{A}_x.$$

Preuve. C'est une conséquence immédiate du fait que $\sum_{x\in V(I)} e_x = 1$ dans $\bar{A}$. Chaque élément p de $\bar{A}$ est envoyé sur $\prod_{x\in V(I)} e_x p$ et chaque élément du produit cartésien $\prod_{x\in V(I)}$ peut s'écrire sous la forme $\prod_{x\in V(I)} e_x p$, puisque $\bar{A}_x$ est isomorphe à $e_x\bar{A}$ d'après la proposition 1.47. ■

Notons maintenant $\mu(x)$ la dimension de $\bar{A}_x$. Cette quantité est appelée multiplicité de x en tant qu'élément de la variété définie par I. Bien évidemment, $\sum_{x\in V(I)} \mu(x)$ est égale à la dimension de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ puisque l'on a vu précédemment que $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ est isomorphe à $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$. Nous verrons, un peu plus loin dans ce chapitre, pourquoi dans le cas où I est radical, $\mu(x) = 1$ pour tout $x \in V(I)$.

Synthèse **Degré d'un idéal et multiplicité**

1) Le degré d'un idéal $I \subset \mathbb{Q}[X_1, \ldots, X_n]$ de dimension 0 est la dimension (nécessairement finie) de l'espace vectoriel $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$.
2) Le degré d'une $\mathbb{Q}$-variété algébrique V de dimension 0 est la dimension (nécessairement finie) de l'espace vectoriel $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{\mathcal{I}(V)}$, où $\mathcal{I}(V)$ est l'idéal associé à V.
3) Si S_x est l'ensemble (clos par multiplication) des éléments de l'anneau-quotient $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$ qui ne s'annulent pas en x, $S_x^{-1}\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$ est un anneau local que l'on note $\bar{A}_x$. Alors l'espace vectoriel $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$ est isomorphe au produit cartésien $\prod_{x\in V(I)} \bar{A}_x$. La dimension de $\bar{A}_x$ est la multiplicité de x.

III. Résolution des systèmes polynomiaux en deux variables – Introduction du résultant

Dans la suite de ce chapitre, on s'intéresse aux algorithmes permettant de résoudre les systèmes d'équations polynomiales engendrant un idéal de dimension zéro. Avant d'étudier le cas général, on se concentre sur le cas des systèmes polynomiaux en deux variables, pour lequel nous introduisons des outils de résolution dédiés, corrélés au calcul de PGCD de deux polynômes par l'algorithme d'Euclide déjà évoqué dans le chapitre 5 du tome *Mathématiques L2*.

III.1. Introduction

Pour mieux comprendre comment le calcul de plus grand commun diviseur intervient dans la résolution de systèmes polynomiaux, considérons le cas extrêmement simple d'un système de deux polynômes en une variable

$$X^3 - X = 0, \quad X^2 - 3X + 2 = 0.$$

Résoudre ce système signifie au moins déterminer l'existence de solutions communes à ces deux polynômes. On vérifie sans peine que $X^3 - X = X(X+1)(X-1)$ et $X^2 - 3X + 2 = (X-2)(X-1)$. Il est alors immédiat que $X - 1$ est un plus grand commun diviseur de $X^3 - X$ et $X^2 - 3X + 2$ dans $\mathbb{Q}[X]$. Or, un calcul simple montre que

$$(X+5)(X^2 - 3X + 2) + 1(X^3 - X) = X - 1.$$

Il s'agit là de la relation de Bézout introduite et étudiée dans le chapitre 5 du tome *Mathématiques L2*. En langage algébrique, on vient de montrer que le plus grand commun diviseur que nous avons considéré appartient à l'idéal $\langle X^3 - X, \quad X^2 - 3X + 2\rangle$ de $\mathbb{Q}[X]$. Notons que si nous avions considéré deux polynômes A et B de $\mathbb{Q}[X]$ n'ayant aucune racine complexe commune, d'après le théorème 1.15, on aurait pu trouver deux polynômes U et V de $\mathbb{Q}[X]$ tels que $UP + VQ = 1$.

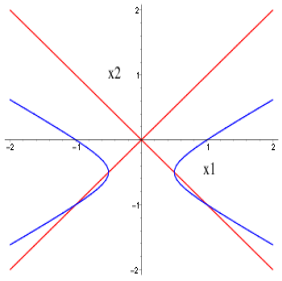


Fig. 1.1. Intersection de courbes

Revenons au cas des systèmes de deux équations polynomiales en deux variables. Considérons les polynômes $A = -3Y^2 - 3Y + X^2 - 1$ et $B = -Y^2 + X^2$. Ils définissent des courbes dans $\mathbb{R}^2$ que l'on peut visualiser sur la figure III.1. L'intersection de ces courbes définit un ensemble fini de points dont on donne les coordonnées ci-dessous :

$$(-1,-1), (1,-1), (-\frac{1}{2}, -\frac{1}{2}), (\frac{1}{2}, -\frac{1}{2}).$$

Substituons X par -1 dans A et B. On obtient alors les polynômes $-3Y^2 - 3Y$ et $1 - Y^2$, dont $Y - 1$ est un plus grand commun diviseur (remarquons d'ailleurs que ce dernier polynôme s'annule en $Y = 1$ qui est l'ordonnée du point solution à notre système initial dont l'abscisse est 1).

De la même manière, on remarque que :

1) $\deg\left(\mathrm{Gcd}(A(1,Y), B(1,Y)\right) \geq 1$;
2) $\deg\left(\mathrm{Gcd}(A(1/2,Y), B(1/2,Y)\right) \geq 1$;
3) $\deg\left(\mathrm{Gcd}(A(-1/2,Y), B(-1/2,Y)\right) \geq 1$.

Plus généralement, il est aisé de montrer que si $(\alpha, \beta) \in \mathbb{C}^2$ est une solution de $A = B = 0$, alors $A(\alpha, Y)$ et $B(\alpha, Y)$ ont un plus grand commun diviseur de degré supérieur ou égal à 1.

Ainsi, on peut chercher à caractériser les abscisses des solutions de notre système comme l'ensemble des racines $\alpha_1, \ldots, \alpha_D$ d'un polynôme univarié pour lesquelles $\mathrm{Gcd}(A(\alpha_i, Y), B(\alpha_i, Y)$ est de degré supérieur ou égal à 1. Cela revient finalement à calculer les projections des solutions du système $A = B = 0$ sur l'axe de première coordonnée. Comme on l'a vu dans la section précédente, cela se traduit algébriquement par le calcul du générateur de $\langle A, B\rangle \cap \mathbb{Q}[X]$.

Dans la suite, nous verrons comment décider si, étant donné un système $A = B = 0$ dans $\mathbb{Q}[X, Y]$, l'idéal $\langle A, B\rangle$ est de dimension 0 et, dans ce cas, comment calculer une paramétrisation de la forme

$$\begin{cases} X &= q_1(T) \\ Y &= q_2(T) \\ q(T) &= 0 \end{cases}$$

(où T est une nouvelle variable et q, q_1 et q_2 sont des polynômes de $\mathbb{Q}[T]$), à partir de laquelle on peut obtenir des approximations numériques des solutions aussi précises que souhaitées. On s'intéressera aussi au nombre maximal de solutions pour un tel système et à la complexité des algorithmes présentés.

III.2. Résultant – définition et propriétés

Considérons donc deux polynômes A et B dans $\mathbb{Q}[X]$ de degrés respectifs p et q et supposons qu'ils aient une racine commune dans $\mathbb{C}$. Cela implique qu'ils ont un plus grand diviseur commun dans $\mathbb{Q}[X]$, que l'on notera G. Il existe donc des polynômes P et Q dans $\mathbb{Q}[X]$ tels que $A = PG$ et $B = QG$. Notons que $\deg(P) = \deg(A) - \deg(G) < \deg(A)$ et $\deg(Q) = \deg(B) - \deg(G) < \deg(B)$. Remarquons aussi que $QA - PB = 0$. De plus, si pour $i \in \mathbb{N}$, on note $\mathbb{Q}_i[X]$ l'ensemble des polynômes de $\mathbb{Q}[X]$ de degré inférieur ou égal à i, on se convainc aisément que $\mathbb{Q}_i[X]$ est un $\mathbb{Q}$-espace vectoriel de dimension $i + 1$. On montrera ci-dessous que l'application $\phi : (U, V) \in \mathbb{Q}_{q-1}[X] \times \mathbb{Q}_{p-1} \to AU + BV \in \mathbb{Q}_{p+q-1}[X]$ est linéaire. Considérons ce point comme acquis pour le moment. Il devient alors clair que le vecteur $(Q, -B)$ appartient au noyau de ϕ. Nous venons de corréler la présence de racines communes de deux polynômes à l'annulation du déterminant d'une matrice. C'est ce point qui est développé ci-dessous.

Plus généralement, on considère deux polynômes $A = a_pX^p + \cdots + a_0$ et $B = b_qX^q + \cdots + b_0$ dans $\mathbb{D}[X]$ de degrés respectifs p et q, où $\mathbb{D}$ est un anneau.

Dans la suite, on note $\mathbb{K}$ le corps de fractions de $\mathbb{D}$. Pour $i \in \mathbb{N}$, on note $\mathbb{D}_i[X]$ l'ensemble des polynômes de $\mathbb{D}[X]$ de degrés inférieurs ou égaux à i qui est donc un espace vectoriel de dimension $i + 1$. Considérons l'application linéaire

$$\begin{aligned} \Phi_{A,B} : \mathbb{D}_{q-1}[X] \times \mathbb{D}_{p-1}[X] &\to \mathbb{D}_{p+q-1}[X] \\ (U, V) &\to AU + BV. \end{aligned}$$

On vérifie sans peine que pour $(\lambda, \mu) \in \mathbb{D} \times \mathbb{D}$, $\Phi_{A,B}(\lambda U + \mu U', \lambda V + \mu V') = \lambda\Phi_{A,B}(U, V) + \mu\Phi_{A,B}(U', V')$. Il est aisé de se convaincre que la transposée de la matrice ci-dessous est la matrice associée à $\Phi_{A,B}$ lorsque l'on écrit les polynômes dans la base monomiale canonique.

$$\mathrm{Sylv}(A, B)^t = \begin{array}{c} X^{q-1}A \\ \vdots \\ \\ \vdots \\ A \\ X^{p-1}B \\ \vdots \\ \\ \vdots \\ \\ \vdots \\ B \end{array} \begin{bmatrix} a_p & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_p & \cdots & \cdots & \cdots & a_0 \\ b_q & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_q & \cdots & \cdots & b_0 \end{bmatrix}$$

On appelle cette matrice la matrice de Sylvester associée à A et B.

Définition 1.49. *Le résultant associé à un couple de polynômes (A, B) de $\mathbb{D}[X]$ est défini comme étant le déterminant de la matrice de Sylvester associée au couple (A, B). On le note* $\mathrm{Res}(A, B)$.

Proposition 1.50. *On a $\mathrm{Res}(A, B) = 0$ si et seulement si il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ non identiquement nuls avec $\deg(U) < q$ et $\deg(V) < p$ tels que $UA + VB = 0$.*

Preuve. Il existe $U \in \mathbb{K}[X]$ et $V \in \mathbb{K}[X]$ non identiquement nuls avec $\deg(U) < q$ et $\deg(V) < p$ tels que $UA + VB = 0$ si et seulement si le noyau de $\Phi_{A,B}$ est un sous- espace vectoriel de dimension supérieure à un. Cela équivaut à dire que le déterminant de la matrice de Sylvester est nul. Par définition, ce déterminant est le résultant associé à (A, B). ■

Notons que ce résultat peut aussi être vu comme la conséquence d'une élimination de Gauss sur la matrice de Sylvester, dont le résultat serait la présence d'un zéro sur la diagonale.

Proposition 1.51. *On a $\mathrm{Res}(A, B) = 0$ si et seulement si A et B ont un facteur commun dans $\mathbb{K}[X]$ de degré supérieur ou égal à 1.*

Preuve. Supposons qu'il existe G, P et Q dans $\mathbb{K}[X]$ de degrés supérieurs ou égaux à 1 tels que $A = PG$ et $B = QG$. Ainsi, on a $\deg(Q) < \deg(B)$ et $\deg(P) < \deg(A)$. On remarque que $QA + (-P)B = 0$. La proposition 1.50 permet alors de conclure. ■

Proposition 1.52. *Soient A et B dans $\mathbb{D}[X]$. Il existe U et V dans $\mathbb{D}[X]$ tels que $\deg(U) < q$, $\deg(V) < p$ et $\mathrm{Res}(A,B) = UA + VB$.*

Preuve. Considérons la matrice obtenue en ajoutant à la dernière colonne de la matrice de Sylvester la $p+q-i$-ième colonne multipliée par X^i. La dernière colonne de la matrice contient alors les polynômes $X^{q-1}A, \ldots, A, X^{p-1}B, \ldots, B$.

$$\begin{bmatrix}
a_p & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & X^{q-1}A \\
0 & \ddots & & & \ddots & \ddots & \vdots & \\
\vdots & \ddots & \ddots & & & \ddots & XA & \\
0 & \cdots & 0 & a_p & \cdots & a_1 & A & \\
b_q & \cdots & \cdots & b_0 & 0 & \cdots & X^{p-1}B & \\
0 & \ddots & & & \ddots & \ddots & \vdots & \\
\vdots & \ddots & \ddots & & & \ddots & \vdots & \\
\vdots & \ddots & \ddots & & & \ddots & XB & \\
0 & \cdots & 0 & b_q & \cdots & b_1 & B &
\end{bmatrix}$$

On montre maintenant que le déterminant de cette nouvelle matrice est exactement celui de la matrice de Sylvester, c'est-à-dire $\mathrm{Res}(A,B)$. En effet, le déterminant de la matrice ci-dessus – obtenu en le développant par rapport à la dernière colonne – est une fonction linéaire de sa dernière colonne (qui est une somme de vecteurs de coefficients multipliés par X élevé à une certaine puissance). Ce déterminant s'écrit donc sous la forme $\mathrm{Res}(A,B) + \sum_j s_j X^j$, où s_j est le déterminant d'une matrice contenant deux colonnes identiques. Le résultat est alors immédiat en développant le déterminant de la matrice ci-dessus par rapport à sa dernière colonne. ■

Test 1.11.

Étant donné deux polynômes A et B dans $\mathbb{Q}[X]$, de degrés respectifs p et q, quelle est la complexité du calcul de résultant de A et B obtenu en effectuant une élimination de Gauss sur la matrice de Sylvester ?

Test 1.12.

Calculer le résultant de aX^2+bX+c et $2aX+b$ vus comme des polynômes de $\mathbb{Q}(a,b,c)[X]$. Que remarquez-vous ?

Théorème 1.53. *Soient $A = a_p \prod_{i=1}^{p}(X - x_i)$ et $B = b_q \prod_{j=1}^{q}(X - y_j)$, alors*

$$\mathrm{Res}(A,B) = a_p^q b_q^p \prod_{i=1}^{p}\prod_{j=1}^{q}(x_i - y_j).$$

Preuve. Pour prouver ce résultat, on considère $x_1, \ldots, x_p$ et $y_1, \ldots, y_q$ comme des indéterminées. On peut d'abord remarquer que s'il existe $1 \leq i \leq p$ et $1 \leq j \leq q$ tels que $x_i = y_j$, alors A et B ont un facteur en commun et donc $\mathrm{Res}(A,B)$ est nul (d'après la proposition 1.51). Donc toutes les différences $x_i - y_j$ sont des facteur de $\mathrm{Res}(A,B)$. Par ailleurs, le résultant est le déterminant de la matrice de Sylvester. En considérant le développement de ce déterminant, il apparaît que chacune des indéterminées x_i (et y_j) apparaît exactement en degré $p+q$. Donc $\prod_{i=1}^{p}\prod_{j=1}^{q}(x_i - y_j)$ est bien un facteur du résultant. Reste à connaître le coefficient multiplicateur de ce facteur, qui s'obtient aisément en remplaçant chaque y_j par 0. ■

Une première conséquence directe du théorème ci-dessus est le corollaire suivant.

Corollaire 1.54. *On a* $\mathrm{Res}(A,BC) = \mathrm{Res}(A,B)\mathrm{Res}(A,C)$.

Une seconde conséquence est la relation ci-dessous.

Corollaire 1.55. *Si $A = a_p \prod_{i=1}^{p}(X - x_i)$ et $B = b_q \prod_{j=1}^{q}(X - y_j)$, alors on a* $\mathrm{Res}(A,B) = a_p^q \prod_{i=1}^{p} B(x_i)$.

Preuve. C'est une conséquence immédiate du théorème 1.53 ci-dessus. En effet, $B(x_i) = b_q \prod_{j=1}^{q}(x_i - y_j)$, on a donc $\prod_{i=1}^{p} B(x_i) = b_q^p \prod_{j=1}^{q}(x_i - y_j)$, ce qui implique le résultat d'après le théorème 1.53. ■

Test 1.13.

Calculer le résultant de $(X-1)(X-2)$ et $(X-3)(X-4)$.

Ci-dessus, on a mis en évidence l'équivalence entre l'annulation du résultant de deux polynômes et l'existence d'un plus grand commun diviseur de degré supérieur ou égal à 1. Or, ce plus grand commun diviseur s'obtient par le calcul de la suite des restes euclidiens des deux polynômes considérés (voir le chapitre 5 du tome *Mathématiques L2*). Le résultat ci-dessous montre la relation de proportionnalité qui existe entre le résultant de deux polynômes A et B et le résultant de B et R, où R est le reste de la division euclidienne de A par B.

Théorème 1.56. *Soient $\mathbb{K}$ un corps, A et B deux polynômes de $\mathbb{K}[X]$, et $R \in \mathbb{K}[X]$ le reste de la division euclidienne de A par B, si bien que $A = BQ + R$ (avec $\deg(R) < \deg(B)$). Alors on a*

$$\mathsf{Res}(A,B) = (-1)^{\deg(A)\deg(B)} b_q^{\deg(A)-\deg(R)} \mathsf{Res}(B,R),$$

où b_q est le coefficient dominant de B.

Preuve. Soit $R = c_r X^r + \cdots + c_0$ le reste de la division euclidienne de A par B. En remplaçant les coefficients des polynômes $X^{q-1}A, \ldots, A$ par des lignes de coefficients des polynômes $X^{q-1}R, \ldots, R$ dans la matrice de Sylvester associée à A et B, on obtient la matrice

$$M = \begin{bmatrix}
0 & 0 & c_r & \cdots & \cdots & c_0 & 0 & \cdots & 0 \\
\vdots & \ddots & & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & & \ddots & 0 \\
\vdots & \cdots & 0 & 0 & c_r & \cdots & \cdots & \cdots & c_0 \\
b_q & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & b_q & \cdots & \cdots & \cdots & b_0
\end{bmatrix}$$

telle que $\det(M) = \mathsf{Res}(A,B)$. En effet, R s'écrit $R = A - \sum_{i=0}^{p-q} d_i X^i B$, où $Q = \sum_{i=0}^{p-q} d_i X^i$ est le quotient de la division euclidienne de A par B et ajouter dans une matrice un multiple d'une rangée à une autre rangée ne modifie pas le déterminant de la matrice considérée.

En notant N la matrice dont les lignes sont $X^{q-1}B, \ldots, X^{r-1}B, \ldots, B, X^{q-1}R, \ldots, R$,

$$N = \begin{bmatrix}
b_q & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & b_q & \cdots & \cdots & \cdots & b_0 \\
\vdots & \cdots & c_r & \cdots & \cdots & c_0 & 0 & \cdots & 0 \\
\vdots & \ddots & & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & & \ddots & 0 \\
\vdots & \cdots & 0 & 0 & c_r & \cdots & \cdots & \cdots & c_0
\end{bmatrix}$$

on remarque que N est obtenue à partir de M en échangeant l'ordre des lignes, si bien que $\det(N) = (-1)^{pq}\det(M)$. Il est alors clair, en développant le déterminant de N par ses $p-r$ premières colonnes, que $\det(N) = b_q^{p-r}\mathsf{Res}(B,R)$. ■

Test 1.14. Utiliser le théorème ci-dessus pour calculer le résultant de $X^3 + X^2 + X$ et $X^2 - 1$.

Considérons maintenant un morphisme d'anneau $h : D \to D'$ et notons que h induit un morphisme d'anneau $\tilde{h} : D[X] \to D'[X]$ en définissant $\tilde{h}(\sum_{i=0}^{d} a_i X^i)$ par $\sum_{i=0}^{d} h(a_i) X^i$. On suppose dorénavant que D est euclidien, c'est-à-dire qu'il est doté d'une division euclidienne.

Proposition 1.57. *Soient $A \in \mathbb{D}[X]$, $B \in \mathbb{D}[X]$ et $h : \mathbb{D} \to \mathbb{D}'$ un morphisme d'anneau tel que $h(a_p) \neq 0$ (ou $h(b_q) \neq 0$), alors*

$$\mathsf{Res}(h(A), h(B)) = h(\mathsf{Res}(A,B)).$$

Preuve. Rappelons que le résultant $\mathsf{Res}(A,B)$ de A et B est le déterminant de la matrice de Sylvester associée à A et B. Ainsi, son image par h est l'image du déterminant de la matrice de Sylvester associée à A et B. Par ailleurs, le résultant $\mathsf{Res}(h(A), h(B))$ est le déterminant de la matrice de Sylvester associée à $h(A)$ et $h(B)$.

Le résultat est immédiat dès lors que l'on remarque que la structure des matrices de Sylvester implique que dans un calcul de déterminant par l'algorithme de Bareiss (qui est équivalent à un algorithme de Gauss sans fractions), seuls les $h(a_p)$ (ou les $h(b_q)$) apparaîtront dans les divisions exactes effectuées par l'algorithme de Bareiss. ■

EXEMPLE 1.58. Du point de vue de l'efficacité des calculs, le résultat ci-dessus n'est pas anodin. Dans le cas où $\mathbb{D} = \mathbb{Z}$, on peut prendre comme morphisme d'anneau $h(z) = z \mod p$, avec p premier. En appliquant alors le théorème des restes chinois, on ramène le calcul du résultant de deux polynômes de $\mathbb{Z}[X]$ au calcul de plusieurs résultants de polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ (voir tome *Mathématiques L2*). Nous verrons une application de ce résultat au cas où $\mathbb{D} = \mathbb{Q}[Y]$ et $h(P(Y)) = P(y)$ pour $y \in \mathbb{Q}$ pour le calcul du résultant de polynômes dans $\mathbb{Q}[Y][X]$ dans la sous-section qui suit.

Test 1.15.

Calculer le résultant de $X^2 + 1$ et $X + 1$ dans $\frac{\mathbb{Z}}{2\mathbb{Z}}[X]$.

Test 1.16.

Soit p un nombre premier. Quel est le résultant de $X^p + 1$ et $X + 1$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$?

Synthèse — **Résultant**

1) Il s'agit du déterminant de la matrice de Sylvester.
2) Le résultant associé au couple $(A, B) \in \mathbb{D}[X]^2$ (où $\mathbb{D}$ est un anneau) est nul si et seulement si A et B ont un facteur commun de degré supérieur ou égale à 1.
3) Si R est le reste de la division euclidienne de A par B, le résultant associé au couple (A, B) est un multiple du résultant associé au couple (B, R).

III.3. Algorithmes de calcul du résultant

Dans cette sous-section, nous étudions différents algorithmes pour le calcul du résultant de deux polynômes. Pour chacun des algorithmes présentés ci-dessous, nous étudions sa complexité théorique.

III.3.1. Calcul du résultant et algorithme d'Euclide

Une première stratégie consiste à s'appuyer sur la relation entre suite des restes euclidiens et résultant de deux polynômes, relation mise en évidence par le théorème 1.56. Notons que dans ce cas, nous supposons implicitement que les coefficients des polynômes A et B vivent dans un corps $\mathbb{K}$. Commençons par rappeler l'algorithme d'Euclide. Dans la suite, si A et B sont deux polynômes univariés, $A \mod B$ est le reste de la division euclidienne de A par B.

Rappel — **Algorithme d'Euclide**

Algorithme 1 Algorithme d'Euclide

ENTRÉES : A et B dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps.

$A_1 \leftarrow A$
$A_2 \leftarrow B$
$i \leftarrow 2$
tant que $A_i \neq 0$ **faire**
  $A_{i+1} \leftarrow A_{i-1} \mod A_i$
  $i \leftarrow i + 1$
fin tant que
Retourner A_{i-1}

Rappelons aussi que la division euclidienne d'un polynôme A de degré n et d'un polynôme B de degré m s'effectue en $\mathcal{O}((n - m)m)$ opérations. Dans le pire des cas, la suite des restes euclidiens A_i calculés par l'algorithme d'Euclide est une suite de polynômes tels que $\deg(A_{i+1}) = \deg(A_i) - 1$. Ainsi, si p est le degré maximal des polynômes A et B donnés en entrée de l'algorithme d'Euclide, sa complexité est en $\mathcal{O}(p^2)$ opérations dans le corps $\mathbb{K}$.

Rappelons maintenant l'énoncé du théorème 1.56 : *soit R tel que $A = BQ + R$ (avec $\deg(R) < \deg(B)$), alors on a*

$$\mathrm{Res}(A, B) = (-1)^{\deg(A)\deg(B)} \mathrm{lcoeff}(B)^{\deg(A) - \deg(R)} \mathrm{Res}(B, R),$$

où $\mathrm{lcoeff}(B)$ est le coefficient dominant de B.

On en déduit immédiatement la correction de l'algorithme ci-dessous.

Algorithme **Calcul du résultant via la suite des restes euclidiens**

ENTRÉES : A et B dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps.
$A_1 \leftarrow A$
$A_2 \leftarrow B$
$R_1 \leftarrow 1$
$i \leftarrow 2$
tant que $A_i \neq 0$ **faire**
$A_{i+1} \leftarrow A_{i-1} \mod A_i$
$R_i \leftarrow (-1)^{\deg(A_i)\deg(A_{i-1})}\mathrm{lcoeff}(A_i)^{\deg(A_{i-1})-\deg(A_{i+1})}R_{i-1}$
$i \leftarrow i+1$
fin tant que
Retourner A_{i-1}

Notons que, comparativement à l'algorithme d'Euclide, les seules opérations supplémentaires effectuées par l'algorithme ci-dessus sont les trois nouvelles multiplications

$$(-1)^{\deg(A_i)\deg(A_{i-1})}\mathrm{lcoeff}(A_i)^{\deg(A_{i-1})-\deg(A_{i+1})}R_{i-1}$$

effectuées à chaque itération du corps de boucle dans lequel sont effectuées les divisions euclidiennes. Ce nombre d'itérations n'excède pas le degré maximal p des polynômes donnés en entrée. Cet algorithme effectue $\mathcal{O}(p^2)$ opérations arithmétiques dans le corps $\mathbb{K}$.

EXEMPLE 1.59. Tentons de calculer le résultant des polynômes

$$A = 6\,x^5 + 5\,x^4 + 4\,x^3 + 3\,x^2 + 2\,x + 1 \text{ et } B = 16\,x^4 + 9\,x^3 + 4\,x^2 + x.$$

La commande `resultant(A,B,x)` du système de calcul formel MAPLE permet d'effectuer facilement ce calcul. Le résultat trouvé est 302922.

Examinons la suite des restes euclidiens calculés dans l'algorithme donné ci-dessus. Le programme écrit en MAPLE ci-dessous permet d'effectuer facilement ce calcul.

```
euclide:=proc(A, B, var)
local R0, R1, R2:
  if not(member(var, indets(A))) and not(member(var, indets(B))) then
    error "var does not belong to the set of variables":
  fi:
  R0:=A:
  R1:=B:
  while degree(R1,var)>0 do
    R2:=rem(R0, R1, var):
    R0:=R1:
    R1:=R2:
  od:
  return R1:
end:
```

On constate alors que la suite des restes euclidiens est

$$\left\{\begin{array}{l} \frac{203}{128}\,x^3 + \frac{71}{32}\,x^2 + \frac{243}{128}\,x + 1 \\ \frac{147200}{41209}\,x^2 + \frac{285696}{41209}\,x + \frac{347776}{41209} \\ -\frac{15288539}{84640000}\,x + \frac{16030301}{5290000} \\ \frac{6409829520000}{5672047969} \end{array}\right. .$$

On constate une croissance des coefficients que l'on peut qualifier d'anormale puisque les coefficients apparaissant en cours de calcul sont de taille largement supérieure à la taille du résultat que l'on souhaite obtenir.

Dans le chapitre 5 du tome *Mathématiques L2*, l'utilisation conjointe de l'inégalité de Hadamard (pour borner la valeur absolue du résultant de deux polynômes A et B de $\mathbb{Z}[X]$), du théorème des restes chinois et de la proposition 1.57 permet de contourner cette croissance de coefficients en ramenant le calcul du résultant de A et B à effectuer sur $\mathbb{Q}$ à plusieurs calculs dans l'image de A et B dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ (avec p premier) pour plusieurs nombres premiers, ce qui permet de limiter la taille des données intermédiaires apparaissant en cours de calcul.

L'objectif de la sous-section qui suit est de montrer comment utiliser un procédé similaire d'évaluation-interpolation dans le cas où l'on cherche à calculer le résultant de deux polynômes de $\mathbb{Q}[X][Y]$.

III.3.2. Évaluation-Interpolation pour le calcul du résultant

L'idée est de calculer les valeurs prises par R en suffisamment de valeurs de X qui n'annulent pas les coefficients dominants de A ou B, puis d'interpoler R (voir le chapitre 2 de ce tome). Mettre en place une telle stratégie

nécessite dans un premier temps d'avoir une borne sur le degré de R afin de déterminer le nombre minimal de valeurs de spécialisation nécessaire pour l'interpolation.

Théorème 1.60. *Soient A et B dans $\mathbb{Q}[X][Y]$, de degrés respectifs p et q et tels que leurs coefficients soient de degrés bornés par d, alors le degré du résultant de A et B est borné par $(p+q)d$.*

PREUVE. Le résultant de A et B est le déterminant de la matrice de Sylvester. Lorsque l'on écrit ce déterminant comme la somme habituelle de $(p+q)!$ termes, on constate que chacun des termes non nuls contient q facteurs qui sont les coefficients de A et p facteurs qui sont les coefficients de B. Ainsi, le degré de chacun de ces termes est borné par $pd+qd$. ■

Reste à savoir comment interpoler R à partir d'une liste de ses spécialisations. Cela se fait facilement au moyen de l'interpolation de Lagrange déjà étudiée dans le chapitre 5 du tome *Mathématiques L2* et que nous rappelons ci-dessous.

Algorithme — **Interpolation de Lagrange**

ENTRÉES : $\ell+1$ rationnels distincts $a_0,\dots,a_\ell$ et $\ell+1$ rationnels $v_0,\dots,v_\ell$.
SORTIES : l'unique polynôme F de degré $\leq \ell$ tel que pour tout $0\leq i\leq \ell$, $F(a_i)=v_i$. F est donné par

$$F=\sum_{i=0}^{\ell} v_i \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$$

Calculer $P=\prod_{i=0}^{\ell}(X-a_i)$
En déduire tous les $\prod_{j\neq i}(X-a_j)$
En déduire tous les $\prod_{j\neq i}(a_i-a_j)$
Calculer la combinaison $F=\sum_{i=0}^{\ell} v_i \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$ à partir des polynômes et valeurs précédemment calculées
Retourner F

On montre sans peine que l'algorithme ci-dessus effectue $\mathcal{O}(\ell^2)$ opérations arithmétiques.

Du théorème 1.60, de la proposition 1.57 et de l'algorithme ci-dessus, on obtient immédiatement un algorithme de calcul du résultant de deux polynômes A et B de $\mathbb{Q}[X][Y]$ de degrés respectifs p et q et tels que d domine le degré de leurs coefficients : il suffit de spécialiser X en $(p+q)d$ valeurs n'annulant pas les coefficients dominants de A et de B, de calculer le résultant pour chacun des couples de polynômes obtenus après spécialisation de X et d'appliquer l'interpolation de Lagrange.

Évaluons la complexité de cette stratégie. On suppose dans la suite que $p\geq q$. On a $\mathcal{O}(pd)$ résultants à calculer pour des couples de polynômes de $\mathbb{Q}[Y]$ de degrés bornés par p. On effectue donc $\mathcal{O}(dp^3)$ opérations arithmétiques dans $\mathbb{Q}$. L'interpolation de Lagrange s'effectue à partir d'une liste de valeurs de cardinalité $\mathcal{O}(pd)$. Son coût est donc en $\mathcal{O}((pd)^2)$. Si D est le degré total des deux polynômes donnés en entrée, on a une complexité en $\mathcal{O}(D^4)$ opérations arithmétiques dans $\mathbb{Q}$.

Synthèse — **Algorithmes de calcul du résultant**

Ce qu'il faut avoir retenu :

1) le résultant peut être obtenu via une variante de l'algorithme d'Euclide pour le calcul de la suite des restes euclidiens ;
2) cette variante induit un grossissement des données intermédiaires qui rend délicats les calculs en pratique lorsque les polynômes donnés en entrée vivent dans $\mathbb{Q}[X][Y]$;
3) les propriétés de spécialisation du résultant et l'interpolation de Lagrange permettent d'avoir de meilleures performances pratiques.

III.4. Algorithme de résolution de systèmes d'équations en 2 variables

Nous pouvons maintenant décrire un algorithme de résolution des systèmes de polynômes $A=B=0$ dans $\mathbb{Q}[X,Y]$ définissant une variété algébrique de dimension au plus 0. Notre outil de calcul fondamental sera le résultant, on considérera donc les polynômes A et B dans $\mathbb{Q}[X][Y]$.

Dans le cas où le système admet un nombre fini de solutions dans $\mathbb{C}^2$, notre objectif est de calculer une paramétrisation rationnelle des solutions, c'est-à-dire, d'obtenir une représentation des solutions sous la forme

$$\begin{cases} Y=q_2(X) \\ q_1(X)=0 \end{cases}.$$

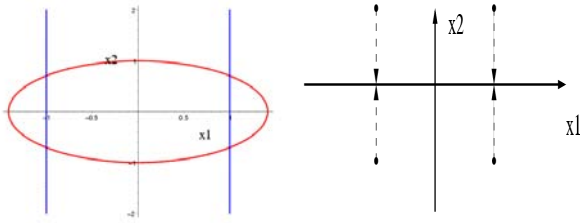


FIG. 1.2. Séparation des solutions

Une telle représentation ne peut évidemment être obtenue que dans le cas où X est séparant pour l'ensemble des solutions complexes du système $A = B = 0$.

III.4.1. Vue d'ensemble

La première des tâches est d'exhiber un **algorithme permettant de décider si l'idéal $\langle A, B\rangle$ est de dimension zéro**. Cela sera effectué par des calculs de résultants.

Remarque. Dans le cas où $\langle A, B\rangle \subset \mathbb{Q}[X, Y]$ n'est pas de dimension zéro, on verra que cela implique que A et B ont un facteur commun.

Une fois que l'on a déterminé que l'idéal $\langle A, B\rangle$ est de dimension zéro, une paramétrisation rationnelle de la forme

$$\begin{cases} Y = q_2(X) \\ q_1(X) = 0 \end{cases}$$

ne peut être obtenue que si X est une variable séparante. Si ce n'est pas le cas, on devra procéder à un changement de variables, comme l'illustre la figure 1.2.

Le deuxième algorithme que nous allons étudier permet donc de **trouver un élément séparant de l'ensemble des solutions** du système étudié. Ici encore, les calculs de résultants jouent un rôle central.

Une fois cette tâche effectuée, il s'agira d'étudier la correspondance entre les racines de $\mathrm{Res}_Y(A, B)$ et l'ensemble des premières coordonnées des solutions du système $A = B = 0$. Nous établirons un critère permettant de mettre en correspondance bijective ces deux ensembles.

Enfin, nous verrons comment déduire de tout cela un paramétrisation rationnelle de l'ensemble des solutions.

III.4.2. Calcul de la dimension

On considère donc deux polynômes A et B dans $\mathbb{Q}[X, Y]$ non identiquement nuls, et l'on cherche un algorithme permettant de déterminer si l'idéal $\langle A, B\rangle$ est de dimension au plus zéro. D'après le théorème 1.33, cela revient à montrer que $\langle A, B\rangle \cap \mathbb{Q}[X]$ et $\langle A, B\rangle \cap \mathbb{Q}[Y]$ sont des idéaux principaux de générateurs non nuls.

Notons $\mathrm{Res}_X(A, B)$ le résultant de A et B lorsqu'ils sont considérés comme des polynômes de $\mathbb{Q}[X][Y]$ et $\mathrm{Res}_Y(A, B)$ le résultant de A et B lorsqu'ils sont considérés comme des polynômes de $\mathbb{Q}[Y][X]$. On a vu dans la proposition 1.52 que l'un comme l'autre appartiennent à l'idéal $\langle A, B\rangle$. Il suffit donc qu'ils soient tous les deux non identiquement nuls pour que $\langle A, B\rangle$ soit de dimension au plus zéro.

Montrons la réciproque. Plus précisément, nous allons montrer que si l'un de ces deux résultants est identiquement nul, alors $\langle A, B\rangle$ n'est pas de dimension zéro. Sans nuire à la généralité, on suppose que $\mathrm{Res}_X(A, B) = 0$. D'après la proposition 1.51, cela implique que A et B ont un facteur commun de degré supérieur à 1 dans $\mathbb{Q}(X)[Y]$. Soit G le numérateur de ce facteur. L'équation $G = 0$ définit une courbe dans $\mathbb{C}^2$ qui est clairement incluse dans la variété algébrique associée à $\langle A, B\rangle$. Cet idéal est donc de dimension positive. On vient de montrer le résultat ci-dessous, sur lequel s'appuie l'algorithme déterminant si $\langle A, B\rangle$ est de dimension au plus zéro.

Proposition 1.61. *L'idéal $\langle A, B\rangle \subset \mathbb{Q}[X, Y]$ est de dimension au plus zéro si et seulement si $\mathrm{Res}_X(A, B)$ et $\mathrm{Res}_Y(A, B)$ sont tous les deux non identiquement nuls.*

On a donc ramené notre premier test à un calcul de deux résultants pouvant être effectué par l'un des deux algorithmes présentés dans la section précédente.

Remarque. La proposition 1.57 peut ici être utilisée pour accélérer les calculs. En particulier, s'il s'agit de s'assurer qu'un résultant de deux polynômes de $\mathbb{Q}[X][Y]$ est non identiquement nul, l'étape d'interpolation de Lagrange utilisée dans la sous-section précédente est inutile. Mieux, si le résultant étudié est effectivement non nul, une valeur de spécialisation choisie de façon aléatoire a toutes les chances de produire un résultant spécialisé non nul lui aussi (il suffit que la valeur de spécialisation vive en dehors de l'ensemble des racines du résultant). Ainsi dans le cas où $\langle A, B\rangle$ est de dimension zéro, le test de dimension peut être très rapide.

III.4.3. Projection des solutions et résultant

Une fois que l'on s'est assuré que l'idéal $\langle A, B\rangle$ est de dimension au plus zéro, on va chercher à calculer les projections des solutions du système $A = B = 0$ sur une droite du plan. Supposons que cette droite soit l'axe de coordonnées X. Comme on l'a vu plus haut, cette opération géométrique se traduit algébriquement par

l'élimination de la variable Y dans les équations $A = B = 0$. Cette opération peut se faire, *en général*, par le calcul du résultant de A et B vus comme des polynômes de $\mathbb{Q}[X][Y]$, mais pas toujours.

En effet, supposons $A = X^2Y + X + 1$ et $B = XY - 1$ dont le résultant (par rapport à Y) est $R = -X(2X + 1)$.

La racine 0 de R ne correspond à aucune solution de $A = B = 0$, mais à une asymptote verticale commune. En fait, chaque fois que les courbes définies respectivement par $A = 0$ et $B = 0$ auront une asymptote commune relativement à l'axe de coordonnées X, le résultant de A et B aura une racine correspondant à cette asymptote. Si ce n'est pas le cas, l'ensemble des racines du résultant est exactement l'ensemble des projections des solutions du système $A = B = 0$.

Voyons pourquoi. On sait que le résultant de deux polynômes univariés vaut zéro si et seulement si ces deux polynômes ont un facteur commun de degré suppérieur à 1 (voir proposition 1.51). Donc dire que le résultant de A et B par rapport à la variable Y est nul signifie que, soit $A(\alpha, Y)$ et $B(\alpha, Y)$ ont un facteur commun dans $\mathbb{Q}(\alpha)[Y]$, soit la spécialisation de X en α n'annule pas au moins un des coefficients dominants de A et B (voir proposition 1.57). Dans ce cas, il existe donc $\beta \in \mathbb{C}$ tel que $A(\alpha, \beta) = B(\alpha, \beta) = 0$ (β est une racine du facteur commun à $A(\alpha, Y)$ et $B(\alpha, Y)$). Supposons maintenant que α soit une racine commune aux coefficients dominants de A et B (vus comme des polynômes de $\mathbb{Q}[X][Y]$). Dans ce cas, la matrice de Sylvester (spécialisée en α) a une colonne ne contenant que des zéros. Son déterminant (le résultant) est donc nul, ce qui implique la nullité du résultant de A et B.

Finalement, on a prouvé que :

1) $\alpha \in \mathbb{C}$ est une racine du résultant n'annulant pas l'un des coefficients dominants de A et B si et seulement si il existe $\beta \in \mathbb{C}$ tel que $A(\alpha, \beta) = B(\alpha, \beta) = 0$;
2) si $\alpha \in \mathbb{C}$ est une racine des coefficients dominants de A et B, alors le résultant de A et B s'annule en α.

Ainsi, si on se rapporte à une situation où les courbes définies respectivement par $A = 0$ et $B = 0$ n'ont pas d'asymptote commune, les racines du résultant sont en correspondance bijective avec les projections des solutions de $A = B = 0$.

Tester l'existence d'une asymptote commune se fait simplement en calculant le PGCD des coefficients dominants de A et B. Ici aussi, le résultant s'avère utile (on peut calculer le résultant des coefficients dominants de A et B pour tester l'existence d'un PGCD de degré supérieur à 1).

Si les coefficients dominants de A et B ont un PGCD commun, un simple calcul laissé en exercice au lecteur montre qu'en effectuant un changement de variables $X \leftarrow X + kY$ (pour $k \in \mathbb{Z}, k \neq 0$) un nombre suffisant de fois, on finit par obtenir des polynômes dont les coefficients dominants sont dans $\mathbb{Z}$, et qui ne peuvent donc pas avoir d'asymptote commune.

III.4.4. Recherche d'un élément séparant et calcul des paramétrisations

Supposons que X soit un élément séparant de l'ensemble des solutions du système $A = B = 0$ (c'est-à-dire que toutes les solutions du système aient des abscisses distinctes) et que les coefficients dominants de A et B (lorsqu'ils sont vus comme des polynômes de $\mathbb{Q}[Y][X]$) n'aient pas de racine complexe commune. On sait alors que la projection sur l'axe de coordonnées X des solutions du système est bijective et envoie cet ensemble de solutions sur l'ensemble des racines du résultant de A et B. Obtenir une description des ordonnées des solutions devient alors une chose aisée : en effet, l'avant-dernier polynôme de la suite des restes euclidiens associée à A et B (toujours lorsqu'ils sont vus comme des polynômes de $\mathbb{Q}[X][Y]$) est de degré 1, puisque la variable X est séparante. Son numérateur s'écrit donc sous la forme $a(X)Y + b(X)$. Obtenir une paramétrisation de Y est alors immédiat.

Reste à savoir comment tester si X est un élément séparant de l'ensemble des solutions du système $A = B = 0$ (et si ce n'est pas le cas, se ramener à une telle situation). Supposons que X ne soit pas séparant. Dans ce cas, il existe α, β_1 et β_2 dans $\mathbb{C}$ tels que (α, β_1) et (α, β_2) soient solutions du système $A = B = 0$. Mais alors, dans ce cas, α est fatalement une racine de $a(X)$ et $b(X)$ (tels qu'ils sont définis ci-dessus). On a ramené ici notre test au calcul du PGCD de $a(X)$ et $b(X)$.

Dans le cas où X n'est pas un élément séparant, on peut utiliser les changements de variables $X \leftarrow X + kY$ (pour un nombre suffisamment grand de $k \in \mathbb{Z}$). D'après le lemme 1.38, une telle famille contiendra forcément un élément séparant.

Test 1.17.

Résoudre le système d'équations polynomiales $X^2 + Y^2 - 1 = XY - 1 = 0$.

IV. Algorithme de division pour les polynômes en plusieurs variables

L'algorithme de résolution des systèmes polynomiaux en deux variables que l'on vient d'étudier repose sur des calculs de résultants. Dans ce cas précis, les polynômes de $\mathbb{Q}[X, Y]$ sont vus comme des polynômes de $\mathbb{Q}[Y][X]$. Les calculs de résultants s'appuient sur l'algorithme d'Euclide, qui lui-même consiste en des calculs de divisions euclidiennes itérés. Dans ce contexte, la division euclidienne permet de *réduire* un polynôme A donné par un polynôme B, de façon à obtenir une réécriture de A – le reste de la division euclidienne – sous la condition $B = 0$, cette réécriture s'exprimant en un degré plus faible que celui de B. Ce procédé de réduction utilise implicitement

un ordre naturel sur les monômes en une variable $1 < X < X^2 < \cdots < X^i < \cdots$ induit par l'isomorphisme $X^i \to i$ entre les monômes en une variable et $\mathbb{N}$.

Dans le cas des polynômes en plusieurs variables, la situation est évidemment plus compliquée. On verra qu'il n'existe pas *un*, mais *plusieurs* ordres possibles sur les monômes multivariés. De ce fait, une généralisation du procédé de réécriture induit par la division euclidienne est délicate : l'existence même de plusieurs ordres monomiaux *admissibles* va impliquer une perte de canonicité. On verra en effet que, contrairement au cas univarié, la *réécriture* d'un polynôme modulo une famille donnée de polynômes n'est pas forcément unique si l'on ne prend pas quelques précautions. Cette section introduit la notion d'ordre *admissible* sur les monômes et montre comment, étant donné un ordre admissible, on peut obtenir un algorithme de réduction (ou de division) d'un polynôme modulo une famille de polynômes.

IV.1. Ordres monomiaux

Définition 1.62. *Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$ non identiquement nul, s'écrivant $f = \sum c(\alpha_1, \ldots, \alpha_n) X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ (où $c(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$). L'ensemble $T(f)$ des* termes de f *est*

$$T(f) = \{c(\alpha_1, \ldots, \alpha_n) X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid c(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

On définit l'ensemble $M(f)$ des monômes de f *comme*

$$M(f) = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid c(\alpha_1, \ldots, \alpha_n) \neq 0\}.$$

Dans la suite, $M(X_1, \ldots, X_n) = M$ est l'ensemble des monômes que l'on peut former avec les variables $(X_1, \ldots, X_n)$. Il s'ensuit que M est isomorphe à $\mathbb{N}^n$. Si $m = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in M$, on note $\deg(m)$ le *degré total* de m qui est égal à $\sum_{i=1}^n \alpha_i$. Le *degré total* de $f \neq 0$ est défini par $\deg(f) = \max\{\deg(t) \mid m \in M(f)\}$.

Étant donné $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n)$ deux éléments de $\mathbb{N}^n$, on notera $\alpha + \beta$ le n-uplet $(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$. Enfin, on notera X^α le monôme $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$.

Définition 1.63. *Soit $<$ un ordre total sur les exposants (donc dans $M \approx \mathbb{N}^n$). Les assertions suivantes sont équivalentes.*

1) *$0 \leq \alpha$ pour tout $\alpha \in M$ (autrement dit $<$ est un ordre total).*
2) *$\alpha < \beta$ implique $\alpha + \gamma < \beta + \gamma$ pour tout $\gamma \in M$ (c'est-à-dire que l'ordre monomial est compatible avec la multiplication).*
3) *Il n'y a pas de suite infinie $(\alpha_i)_{i \in \mathbb{N}}$ strictement décroissante.*

On dit que l'ordre $<$ est admissible si l'une des conditions ci-dessus est vérifiée.

Dans la suite, on munit M d'un ordre admissible. Plusieurs ordres admissibles sont possibles. On donne quelques exemples importants ci-dessous.

Exemple 1.64. Donnons quelques exemples d'ordres admissibles que nous utiliserons dans la suite.

L'ordre *lexicographique* est défini comme suit :

$$X^\alpha = X^{(\alpha_1, \ldots, \alpha_n)} <_{\text{Lex}} X^\beta = X^{(\beta_1, \ldots, \beta_n)}, \text{ s'il existe } i \text{ tel que } \begin{cases} \alpha_j = \beta_j \text{ pour } j < i \\ \alpha_i < \beta_i \end{cases}.$$

L'ordre du *degré lexicographique inversé* (que l'on appelle aussi ordre DRL) est défini de la manière suivante :

$$X^\alpha = X^{(\alpha_1, \ldots, \alpha_n)} <_{\text{DRL}} X^\beta = X^{(\beta_1, \ldots, \beta_n)} \text{ si } \begin{cases} \alpha_1 + \cdots + \alpha_n < \beta_1 + \cdots + \beta_n \\ \text{ou} \\ \alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n \\ \text{et } \begin{cases} \alpha_j = \beta_j \text{ pour } j > i \\ \alpha_i > \beta_i \end{cases} \end{cases}.$$

Remarquons que l'inégalité est inversée $\alpha_i > \beta_i$: c'est donc l'ordre obtenu en filtrant par le degré, puis en inversant l'ordre des variables et en prenant l'ordre lexicographique *opposé*.

Voyons plus concrètement comment ces ordres permettent de trier les monômes.

Exemple 1.65.

1) Pour l'ordre lexicographique tel que $Z <_{\text{Lex}} Y <_{\text{Lex}} X$, on a

$$X^3 > X^2Y > X^2Z > XY^2 > XYZ > XZ^2 > Y^3 > Y^2Z > YZ^2 > Z^3.$$

2) Pour l'ordre DRL tel que $Z <_{\text{DRL}} Y <_{\text{DRL}} X$, on a

$$X^3 > X^2Y > XY^2 > Y^3 > X^2Z > XYZ > Y^2Z > XZ^2 > YZ^2 > Z^3.$$

IV.2. Monômes et termes de tête

Une fois un ordre admissible $<$ sur M fixé, il est facile de trier l'ensemble $M(f)$ des monômes de f. On note $M_<(f)$ l'ensemble $M(f)$ trié par $<$. Le monôme de tête de f, que l'on note $\mathrm{LM}_<(f)$, est le plus grand élément de $M_<(f)$. Le coefficient de $LM_<(f)$ dans l'écriture monomiale de f est noté $\mathrm{LC}(f)$; on l'appelle coefficient de tête de f. Enfin, le terme de tête $\mathrm{LT}_<(f)$ de f est le produit $\mathrm{LC}(f)\mathrm{LM}(f)$.

Lorsqu'il n'y a pas d'ambiguïté sur l'ordre monomial utilisé, le monôme de tête, le terme de tête et le coefficient de tête de f seront simplement notés $\mathrm{LM}(f)$, $\mathrm{LT}(f)$ et $\mathrm{LC}(f)$.

Si F est un sous-ensemble de $\mathbb{Q}[X_1,\dots,X_n]$, on peut étendre ces définitions :

1) $\mathrm{LM}_<(F) = \{\mathrm{LM}_<(f) \mid f \in F\}$;
2) $\mathrm{LT}_<(F) = \{\mathrm{LT}_<(f) \mid f \in F\}$;
3) $M(F) = \bigcup_{f\in F} M(f)$ et $T(F) = \bigcup_{f\in F} T(f)$.

Définition 1.66. *Soient $\alpha = (\alpha_1,\dots,\alpha_n)$ et $\beta = (\beta_1,\dots,\beta_n)$ deux éléments de $\mathbb{N}^n$. On définit le plus petit commun multiple de deux monômes par la formule*

$$X_1^{\max(\alpha_1,\beta_1)} \cdots X_n^{\max(\alpha_n,\beta_n)}.$$

On le notera $\mathrm{ppcm}(X^\alpha, X^\beta)$.
Par extension, si $<$ est un ordre admissible, on définit $\mathrm{ppcm}(f,g) = \mathrm{ppcm}(\mathrm{LM}_<(f), \mathrm{LM}_<(g))$, où f et g sont des polynômes de $\mathbb{Q}[X_1,\dots,X_n]$.

Dans la suite, on exploitera la propriété ci-dessous.

Proposition 1.67. *Soient f un polynôme de $\mathbb{Q}[X_1,\dots,X_n]$ et $<_{Lex}$ l'ordre lexicographique tel que $X_1 > \cdots > X_n$. Si $\mathrm{LT}_{<_{Lex}}(f) \in \mathbb{Q}[X_i,\dots,X_n]$, alors on a $f \in \mathbb{Q}[X_i,\dots,X_n]$. En particulier si $\mathrm{LT}_{<_{Lex}}(f) \in \mathbb{Q}[X_n]$, alors on a $f \in \mathbb{Q}[X_n]$.*

Preuve. Soit $f \in \mathbb{Q}[X_1,\dots,X_n]$ tel que $t' = \mathrm{LM}_{<_{\mathrm{Lex}}}(f) \in \mathbb{Q}[X_i,\dots,X_n]$, donc on a $t' = X_i^{\beta_i}\cdots X_n^{\beta_n}$ (avec la convention $\beta_1 = \cdots = \beta_{i-1} = 0$). Si $t = X_1^{\alpha_1}\cdots X_n^{\alpha_n} \in M_{<_{\mathrm{Lex}}}(f)$ et $t \neq t'$, alors on a $t <_{\mathrm{Lex}} t'$ puisque $t' = \mathrm{LM}_{<_{\mathrm{Lex}}}(f)$. Donc, par définition de l'ordre lexicographique, il existe $k \in \{1,\dots,n\}$ tel que $\alpha_j = \beta_j$ pour $j < k$ et $\alpha_k < \beta_k$. Comme $\beta_j = 0$ pour $j < i$, on a nécessairement $\alpha_j = 0$ pour $j < i$. Cela implique $t \in \mathbb{Q}[X_i,\dots,X_n]$ et donc $f \in \mathbb{Q}[X_i,\dots,X_n]$. ∎

IV.3. Réduction d'un polynôme

Maintenant que nous disposons d'ordres sur les monômes en plusieurs variables, nous pouvons *réduire* un polynôme en plusieurs variables par une famille de polynômes en plusieurs variables.

Pour commencer, nous introduisons dans la suite deux notions proches de réduction d'un polynôme f par rapport à un polynôme p. La première notion de réduction $f \xrightarrow{p} g$ est purement *mathématique* – on pourrait la paraphraser par f *peut* se réduire en g modulo p. La seconde est *algorithmique*. Ces deux définitions sont ensuite étendues pour réduire un polynôme f par plusieurs polynômes : alors que mathématiquement, on considère un sous-ensemble fini P de $\mathbb{Q}[X_1,\dots,X_n]$, il est nécessaire d'ordonner les polynômes d'un point de vue algorithmique puisque l'on manipule alors des *listes de polynômes* $F = [f_1,\dots,f_m]$.

L'ordre admissible $<$ est supposé fixé dans la suite.

Définition 1.68. *Soient f, g, et p dans $\mathbb{Q}[X_1,\dots,X_n]$ tels que $p \neq 0$. Alors on dit que :*

1) *f se réduit en g modulo p (notation $f \xrightarrow{p} g$), s'il existe $t \in M(f)$, et s'il existe $s \in M$ tels que $s\,\mathrm{LM}(p) = t$ et $g = f - \frac{a}{\mathrm{LC}(p)}\,s\,p$, où a est le coefficient de t dans f ;*
2) *f se réduit en g modulo P (notation $f \xrightarrow{P} g$) si $f \xrightarrow{p} g$ pour un certain $p \in P$;*
3) *f est réductible modulo p s'il existe $g \in \mathbb{Q}[X_1,\dots,X_n]$ tel que $f \xrightarrow{p} g$.*

Définition 1.69. *Soient f et g dans $\mathbb{Q}[X_1,\dots,X_n]$, et soit P un sous-ensemble fini de $\mathbb{Q}[X_1,\dots,X_n]$.*

1) *f est réductible modulo P s'il existe $g \in \mathbb{Q}[X_1,\dots,X_n]$ tel que $f \xrightarrow{P} g$;*
2) *f est top-réductible modulo P s'il existe $g \in \mathbb{Q}[X_1,\dots,X_n]$ tel que $f \xrightarrow{P} g$ et $\mathrm{LM}(g) < \mathrm{LM}(f)$;*
3) *f se réduit en g modulo P ($f \xrightarrow[P]{*} g$) si $g = f$ ou s'il existe $k \in \mathbb{N}$ et $g_1,\dots,g_k$ dans $\mathbb{Q}[X_1,\dots,X_n]$ tels que $g_k = g$, $f \xrightarrow{P} g_1$, et pour $1 \leq i \leq k-1$, $g_i \xrightarrow{P} g_{i+1}$.*

On donne maintenant un algorithme de réduction d'un polynôme par une liste de polynômes.

Algorithme **RÉDUCTION**

ENTRÉES : Un polynôme p, une liste de polynômes $F = [f_1, \ldots, f_m]$ et ordre admissible $<$
SORTIES : Un polynôme r tel que $p \xrightarrow{F} r$.
tant que $p \neq 0$ **et** p est top-réductible modulo F **faire**
$k = \min(i \in \{1, \ldots, m\} \mid LM(f_i)$ divise $LM(p))$
$p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_k)} f_k$
fin tant que
Retourner p

L'algorithme RÉDUCTION est le pendant multivarié de la division euclidienne de polynômes en une variable.

Proposition 1.70. *L'algorithme* RÉDUCTION *se termine.*

PREUVE. Supposons que l'algorithme ne se termine pas. Dans ce cas, on peut construire une suite infinie $(p_i)_{i\in\mathbb{N}}$ de polynômes telle que $p_0 = p$ et

$$p_{i+1} := p_i - \frac{\mathrm{LT}(p_i)}{\mathrm{LT}(f_{j_i})} f_{j_i}.$$

On en déduit que pour tout $i \in \mathbb{N}$, $\mathrm{LM}(p_{i+1}) < \mathrm{LM}(p_i) < \cdots$, ce qui contredit le point 3) de la définition 1.63 d'admissibilité de l'ordre $<$. ■

Il est important de noter que la réduction d'un polynôme par un ensemble de polynômes n'est pas unique et que le résultat dépend, a priori, de la façon d'ordonner les polynômes dans la liste F. Ce point est illustré par l'exemple suivant.

EXEMPLE 1.71. Voici un exemple de réduction dont le résultat change selon l'ordre des calculs : $f = X^2 + X, f_1 = X^2 + 1, f_2 = X + 2$ (l'ordre monomial $<$ choisi ici est l'ordre lexicographique).

1) On calcule RÉDUCTION$(f, [f_1, f_2], <)$: f est top-réductible modulo $[f_1, f_2]$ puisque $\mathrm{LM}(f_1) = X^2$ divise $\mathrm{LM}(f) = X^2$.
On calcule donc $f' := f - \frac{1}{1} f_1 = X - 1$; de nouveau f' est top-réductible modulo $[f_1, f_2]$ puisque $\mathrm{LM}(f_2) = X$ divise $\mathrm{LM}(f') = X$ et
On calcule donc $f'' := f' - \frac{1}{1} f_2 = -3$; l'algorithme se termine car $\mathrm{LM}\left(f''\right) = 1$ n'est plus top-réductible.
2) On calcule maintenant RÉDUCTION$(f, [f_2, f_1, <])$: cette fois $\mathrm{LM}(f_2) = X$ divise $\mathrm{LM}(f) = X^2$.
On calcule donc $f' := f - \frac{X}{1} f_2 = X - 1 = X - 2X = -X$; encore une fois $\mathrm{LM}(f_2) = X$ divise $\mathrm{LM}(f') = X$ et on calcule $f'' := f' - \frac{-1}{1} f_2 = 2$; l'algorithme termine car $\mathrm{LM}\left(f''\right) = 1$ n'est plus top-réductible.
3) On a donc RÉDUCTION$(f, [f_1, f_2], <) = 3 \neq 2 =$ RÉDUCTION$(f, [f_2, f_1], <)$.
4) Avec la notion mathématique, on a simultanément $f \xrightarrow[[f_1,f_2]]{*} -3$ et $f \xrightarrow[[f_2,f_1]]{*} 2$.

Proposition 1.72. *Soit F une famille de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$.*
1) Si $r =$ RÉDUCTION$(p, F, <)$, alors $r - p \in \langle F \rangle$;
2) Si $p \xrightarrow[F]{*} r$, alors $r - p \in \langle F \rangle$.

PREUVE. Si $r =$ RÉDUCTION$(p, F, <)$, alors d'après la proposition 1.70, il existe une suite *finie* $(p_i)_{i\in\{1,\ldots,k\}}$ telle que $p_0 = p$, $p_k = r$ et

$$p_{i+1} := p_i - \frac{\mathrm{LT}(p_i)}{\mathrm{LT}(f_i)} f_i \text{ avec } f_i \in F.$$

On en déduit que

$$p_j := p + \sum_{i=0}^{i-1} \frac{\mathrm{LT}(p_i)}{\mathrm{LT}(f_i)} f_i, \tag{1.3}$$

et $p - r = p - p_k$ est dans l'idéal $\langle F \rangle$.
De même si $p \xrightarrow[F]{*} r$, il existe une suite finie $p_0 = p \xrightarrow{f_1} p_1 \xrightarrow{f_2} \cdots \xrightarrow{f_k} p_k = r$, où $f_i \in F$ et

$$p_{i+1} := p_i - a_i\, s_i\, f_i \text{ avec } a_i \in \mathbb{Q}, s_i \in M, \text{ et } \mathrm{LM}(a_i\, s_i\, f_i) \leq \mathrm{LM}(p_{i+1}).$$

On en déduit

$$p_k := p + \sum_{i=0}^{k-1} a_i\, s_i\, f_i, \tag{1.4}$$

et donc $p - r = p - p_k \in \langle F \rangle$. ■

Corollaire 1.73.

1) Si $r = \text{RÉDUCTION}(p, F, <)$, alors il existe deux suites finies $(g_i)_{i=0,\dots,k}$ et des termes $(m_i)_{i=0,\dots,k}$ tels que $g_i \in F$ et $r - p = \sum_{i=1}^{k} m_i g_i$, avec $\mathrm{LM}(p) = \mathrm{LM}(m_1 g_1) > \mathrm{LM}(m_2 g_2) > \cdots > \mathrm{LM}(m_k g_k)$,

2) Si $p \xrightarrow[F]{*} r$, alors il existe deux suites finies $(g_n)_{n=0,\dots,k}$ et des termes $(m_j)_{j=0,\dots,k}$ tels que $g_n \in F$ et $r - p = \sum_{i=1}^{k} m_i g_i$ avec $\mathrm{LM}(p) \geq \mathrm{LM}(m_i g_i)$ pour tout $i \in \{1, \dots, k\}$.

PREUVE. Le corollaire se déduit facilement de la preuve de la proposition 1.72 et des formules 1.3 et 1.4. ■

Test 1.18.

On considère un ordre monomial admissible $<$ et la fonction $\varphi : \mathbb{Q}[X_1, \dots, X_n] \longrightarrow \mathbb{Q}[X_1, \dots, X_n]$, définie par $\varphi(p) = \text{RÉDUCTION}(f, F, <)$, où $F = [f_1, \dots, f_m] \in \mathbb{Q}[X_1, \dots, X_n]^m$. Montrer que :

1) pour tout $p \in \mathbb{Q}[X_1, \dots, X_n]$ et $\lambda \in \mathbb{Q}$, alors $\varphi(\lambda p) = \lambda \varphi(p)$;
2) $\mathrm{Ker}(\varphi) \subset \langle F \rangle$;
3) l'inclusion est-elle stricte ?

Test 1.19.

Soit la fonction $\varphi : \mathbb{Q}[X_1, \dots, X_n] \longrightarrow \mathbb{Q}[X_1, \dots, X_n]$, définie par $\varphi(p) = \text{RÉDUCTION}(f, F, <)$. Montrer que dans le cas où F est constitué de monômes ($t_i \in T$), alors $\mathrm{Ker}(\varphi) = \langle F \rangle$.

Proposition 1.74. *Si $p = \text{RÉDUCTION}(f, F, <)$ et $p \neq 0$, alors on a $\mathrm{LT}(p) \notin \langle \mathrm{LT}(F) \rangle$.*

PREUVE. Si $p = \text{RÉDUCTION}(f, F, <)$ est non nul, alors p n'est pas top-réductible par F, donc $\mathrm{LT}(p)$ n'est pas réductible par un élément de F ; autrement dit $\mathrm{LT}(p) \notin \langle \mathrm{LT}(F) \rangle$. ■

Lorsque l'on considère deux polynômes f et g, on ne peut pas, en général, réduire f par g ou g par f (le monôme dominant de f n'est pas nécessairement divisible par celui de g et réciproquement). Par exemple, considérons le cas où $f_1 = X^2Y + X + 1$ et $f_2 = XY^2 - 3$. Ici, il est nécessaire, pour *éliminer les termes de tête* de multiplier f_1 et f_2 par des monômes

$$Y\, f_1 - X\, f_2 = Y\,(X + 1) - X\,(-3) = XY + 3X + Y.$$

La formule suivante du S-polynôme donne une définition précise pour cette opération dans le cas général.

Définition 1.75. *Le S-polynôme de f et g est défini par*

$$\mathrm{Spol}(f, g) = \mathrm{LC}(g)\frac{\mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(f)} f - \mathrm{LC}(f)\frac{\mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LM}(g)} g.$$

Test 1.20.

Calculer $\mathrm{Spol}(2\,X^2Y + X^2, 7\,XY^2 + 3X^2)$ lorsque l'on considère l'ordre lexicographique (respectivement DRL) tel que $X > Y$.

Test 1.21.

On suppose que f est *top-réductible par le polynôme* g. Quelle est la valeur de $\mathrm{Spol}(f, g)$?

IV.4. Réduction totale d'un polynôme

La fonction RÉDUCTION se contente de simplifier (réduire) le monôme de tête d'un polynôme, mais il est possible que d'autres monômes de ce polynôme soient réductibles. La fonction RÉDUCTIONTOTALE permet de réduire *tous les monômes* d'un polynôme (et donc d'obtenir une expression plus canonique). L'algorithme ci-dessous permet d'obtenir une telle représentation.

Algorithme **RÉDUCTIONTOTALE**

ENTRÉES : : Un polynôme f, une liste de polynômes $F = [f_1, \ldots, f_m]$ et un ordre admissible $<$
SORTIES : un polynôme totalement réduit.

$p := f$ et $p_0 := 0$
tant que $p \neq 0$ **faire**
  $p :=$RÉDUCTION$(p, F, <)$
  $p_0 := p_0 + \mathrm{LT}(p)$
  $p := p - \mathrm{LT}(p)$
fin tant que
Retourner p_0

Proposition 1.76. *L'algorithme* RÉDUCTIONTOTALE *termine.*

PREUVE. Supposons que l'algorithme ne termine pas : comme la fonction RÉDUCTION termine (d'après la proposition 1.70), cela implique que l'on passe un nombre infini de fois dans la boucle **tant que**. Si l'on note $p^{(i)}$ la valeur de la variable p à la fin de la boucle lors du i-ième passage, on en déduit

$$\mathrm{LM}(p^{(i)}) = \mathrm{LM}\left(p^{(i-1)} - \mathrm{LT}(p^{(i-1)})\right) < \mathrm{LM}(p^{(i-1)}).$$

On a donc construit une suite infinie strictement décroissante de monômes, ce qui est contradictoire avec le fait que $<$ est un ordre admissible. ■

Proposition 1.77.

1) Si $p =$ RÉDUCTIONTOTALE$(f, F, <)$, *alors on a* $M(p) \cap \langle \mathrm{LM}(F) \rangle = \varnothing$

2) Si $r =$ RÉDUCTIONTOTALE$(f, F, <)$, *alors on a* $r - f \in \langle F \rangle$.

PREUVE.

1) La première assertion de la proposition équivaut à dire que tous les termes d'un polynôme totalement réduit ne sont plus top-réductibles par un élément de la liste F, ce qui est immédiat.

2) On montre par récurrence, qu'à tout moment de l'algorithme, on a $p + p_0 - f \in \langle F \rangle$.

   a) Au début de l'algorithme, on a $p = f$ et $p_0 = 0$, donc $p + p_0 - f = f + 0 - f = 0$.

   b) On suppose maintenant que l'assertion ci-dessus est vérifiée à une itération de la boucle **tant que**. On a $\tilde{p} =$ RÉDUCTION$(p, F, <)$, puis $p_0' := p_0 + \mathrm{LT}(\tilde{p})$ et $p' := \tilde{p} - \mathrm{LT}(\tilde{p})$; par conséquent

$$\begin{aligned} p' + p_0' - f &= (\tilde{p} - \mathrm{LT}(\tilde{p})) + (p_0 + \mathrm{LT}(\tilde{p})) - f \\ &= \tilde{p} + p_0 - f = (\tilde{p} - p) + (p + p_0 - f)\,. \end{aligned}$$

   Comme $\tilde{p} - p \in \langle F \rangle$ d'après la proposition 1.72 et que $p + p_0 - f \in \langle F \rangle$ par hypothèse de récurrence, on déduit que $p' + p_0' - f \in \langle F \rangle$.

   c) Lorsque l'on sort de la boucle **tant que**, $p = 0$ et $p_0 =$ RÉDUCTIONTOTALE$(f, F, <)$: on a donc bien RÉDUCTIONTOTALE$(f, F, <) - f \in \langle F \rangle$.

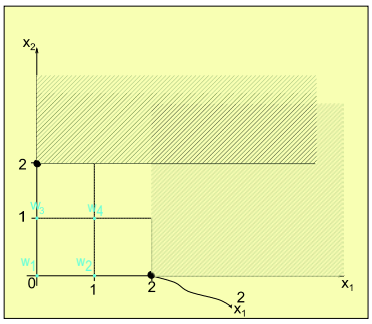
■

V. DÉFINITION ET PROPRIÉTÉS DES BASES DE GRÖBNER

V.1. Définition d'une base de Gröbner

La définition suivante d'une base de Gröbner est purement mathématique et permet donc de définir indépendamment de tout algorithme une base *canonique* d'un idéal.

Définition 1.78. *Soit* I *un idéal de* $\mathbb{Q}[X_1, \ldots, X_n]$. *On dit qu'un sous-ensemble fini* $G = (g_1, \ldots, g_k)$ *de* $\mathbb{Q}[X_1, \ldots, X_n]$ *est une base de Gröbner de* I *pour l'ordre admissible* $<$ *si pour tout* $f \in I$, *il existe* $1 \leq i \leq k$ *tel que* $\mathrm{LM}(g_i)$ *divise* $\mathrm{LM}(f)$.



Afin de visualiser le concept de base de Gröbner, il est commode de reporter sur un dessin (voir figure 1.3) les points $\mathrm{LM}(f)$ pour $f \in I$. Par exemple, lorsque $n = 2$, s'il existe un polynôme f_0 de l'idéal I tel que $\mathrm{LM}(f_0) = X^4Y^2$, on reporte sur le dessin le point de coordonnées $(4, 2)$. On itère le processus pour tous les polynômes f de l'idéal I. Dans notre exemple, on sait que $X^iY^j\, f_0 \in I$ pour tout $(i, j) \in \mathbb{N}^2$; ainsi $\mathrm{LM}\left(X^iY^j\, f_0\right) = X^iY^j\, \mathrm{LT}(f_0) = X^{4+i}Y^{2+j}$ et on reporte sur le dessin tous les points $(4 + i, 2 + j)$ pour tout $0 \leq i, j$. C'est donc tout le quadrant supérieur au point $(4, 2)$ qui est ainsi hachuré sur la figure. Le dessin met en évidence la *structure d'escalier* : les points minimaux sont justement les éléments de la base de Gröbner.

Théorème 1.79. *On fixe un ordre admissible $<$. Tout idéal I possède une base de Gröbner G.*

FIG. 1.3. Structure d'escalier

On pourrait démontrer ce théorème par une preuve non constructive, mais nous allons donner un *algorithme* permettant de calculer une base de Gröbner à partir d'un système de générateurs.

Le théorème ci-dessous montre que les bases de Gröbner permettent de tester l'appartenance d'un polynôme à l'idéal qu'elles engendrent. En un certain sens, la réduction d'un polynôme modulo une base de Gröbner est donc canonique.

Théorème 1.80. *(**Buchberger**) Soient $G = [g_1, \ldots, g_k] \subset \mathbb{Q}[x_1, \ldots, x_n]$ et $<$ un ordre admissible fixé. Les conditions suivantes sont équivalentes :*

1) G est une base de Gröbner de $\langle g_1, \ldots, g_k\rangle$ pour $<$;

2) $\textsc{Réduction}(p, G, <) = 0$ si et seulement si $p \in \langle G\rangle$.

PREUVE. Soit G une base de Gröbner de $I = \langle g_1, \ldots, g_k\rangle$. Supposons qu'il existe $p \in I$ tel que $r = \textsc{Réduction}(p, G, <)$ avec $r \neq 0$. Alors, d'après la proposition 1.72, on a $r - p \in I$ et donc $r = p + (r - p) \in I$. Par définition d'une base de Gröbner, il existe $g \in G$ tel que $\mathrm{LM}(g)$ divise $\mathrm{LM}(r)$. Cela contredit la proposition 1.74 et achève de démontrer que 1) implique 2). Supposons maintenant que la propriété 2) soit vérifiée : pour tout $p \in \langle G\rangle$ non identiquement nul, on a $\textsc{Réduction}(p, G, <) = 0$. Par conséquent, tout $p \in \langle G\rangle$ est top-réductible par G et donc il existe $g \in G$ tel que $\mathrm{LM}\,(g)$ divise $\mathrm{LM}\,(f)$. Par définition, G est alors une base de Gröbner. ■

Théorème 1.81. *(**Buchberger**) Soit $G = [g_1, \ldots, g_k]$ une base de Gröbner de $\langle g_1, \ldots, g_k\rangle$ pour un ordre $<$ fixé, alors $\textsc{RéductionTotale}(p, G, <)$ est unique quelle que soit la stratégie de réduction (c'est-à-dire quelle que soit la façon d'ordonner G).*

PREUVE. Étant donné une permutation σ de $\{1, \ldots, k\}$, on note $\sigma G = \left[g_{\sigma(1)}, \ldots, g_{\sigma(k)}\right]$. Supposons qu'il existe une permutation σ de $\{1, \ldots, k\}$ telle que

1) $r_1 := \textsc{RéductionTotale}(p, G, <)$;

2) $r_2 := \textsc{RéductionTotale}(p, \sigma G, <)$;

3) $r_1 \neq r_2$.

D'après la proposition 1.77, il existe (g_1, g_2) dans $\langle G\rangle \times \langle G\rangle$ tels que $r_1 = p + g_1$ et $r_2 = p + g_2$ et donc $r_1 - r_2 = g_1 - g_2 \in \langle G\rangle$. Comme G est une base de Gröbner, il existe $g \in G$ tel que $\mathrm{LM}(g)$ divise $\mathrm{LM}(r_1 - r_2)$. Ainsi, $\mathrm{LM}(g)$ divise un élément de $M(r_1) \cup M(r_2)$, ce qui contredit la proposition 1.77. ■

Définition 1.82. *Soit $G = [g_1, \ldots, g_k]$ une base de Gröbner d'un idéal I pour un ordre admissible $<$. Pour tout polynôme f, on note $\textsc{NormalForm}(f, G, <)$ le résultat de la fonction $\textsc{RéductionTotale}(f, G, <)$. On notera aussi $\mathrm{NF}(f, G, <)$ cette forme normale.*

V.2. Algorithme de Buchberger

On décrit ci-dessous l'algorithme dit de Buchberger (du nom de son concepteur, Bruno Buchberger) pour le calcul de bases de Gröbner. On en donne la version la plus simple. Celle-ci repose sur la notion de *paire critique*. Une paire critique est simplement un couple de polynômes (f, g) pour lesquels on va calculer un S-polynôme. L'algorithme maintient une liste de tels couples (ou encore liste des paires critiques) qu'il faudra entièrement explorer.

Algorithme **Calcul de bases de Gröbner (algorithme de Buchberger)**

ENTRÉES : Une liste de polynômes $F = [f_1, \dots, f_s]$ et un ordre admissible $<$
SORTIES : G un sous-ensemble (fini) de $\mathbb{Q}[X_1, \dots, X_n]$ qui est une base de Gröbner de $\langle f_1, \dots, f_s \rangle$.

$G := F$ et $m := s$
$P := \{(f_i, f_j) \mid 1 \leq i < j \leq m\}$ la liste des paires critiques
tant que $P \neq \varnothing$ **faire**
  Choisir et retirer de P une paire critique (f, g)
  $f_{m+1} := \mathrm{Spol}(f, g)$
  $f_{m+1} :=$ RÉDUCTION$(f_{m+1}, G, <)$
  si $f_{m+1} \neq 0$ **alors**
    $m := m + 1$
    $P := P \cup \{(f_i, f_m) \mid 1 \leq i < m\}$
    $G := G \cup \{f_m\}$
  fin si
fin tant que
Retourner G

Étudions d'abord un exemple montrant comment fonctionne cet algorithme.

EXEMPLE 1.83. On considère l'ordre lexicographique avec $x > y$ et la liste de polynômes $F = [f_1 = X^2Y - 1, f_2 = XY^2 - 3]$ et l'on applique l'algorithme de Buchberger.
Initialement, on a $P = \{[f_1, f_2]\}$ et $G = [f_1, f_2]$.

1) $P = \{[f_1, f_2]\}$: on calcule $f_3 := \mathrm{Spol}(f_1, f_2) = -Y + 3X$ puis $f_3 :=$ RÉDUCTION$(f_3, G, <) = 3X - Y$.
   On ajoute donc un nouvel élément dans G : $G = [f_1, f_2, f_3]$ et $P = \{[f_1, f_3], [f_2, f_3]\}$.
2) $P = \{[f_1, f_3], [f_2, f_3]\}$: on calcule $f_4 := \mathrm{Spol}(f_1, f_3) = XY^2 - 3$ puis RÉDUCTION$(f_4, G, <) = 0$.
3) $P = \{[f_2, f_3]\}$: on calcule $f_4 := \mathrm{Spol}(f_2, f_3) = -9 + Y^3$ puis $f_4 :=$ RÉDUCTION$(f_4, G, <) = Y^3 - 9$.
   On ajoute donc un nouvel élément dans G : $G = [f_1, f_2, f_3, f_4]$ et $P = \{[f_1, f_4], [f_2, f_4], [f_3, f_4]\}$.
4) $P = \{[f_1, f_4], [f_2, f_4], [f_3, f_4]\}$: on calcule $f_5 := \mathrm{Spol}(f_1, f_4) = -Y^2 + 9X^2$ puis RÉDUCTION$(f_5, G, <) = 0$.
5) $P = \{[f_2, f_4], [f_3, f_4]\}$: on calcule $f_5 := \mathrm{Spol}(f_1, f_4) = -3Y + 9X$ puis RÉDUCTION$(f_5, G, <) = 0$.
6) $P = \{[f_3, f_4]\}$: on calcule $f_5 := \mathrm{Spol}(f_1, f_4) = -Y^4 + 27X$ puis RÉDUCTION$(f_5, G, <) = 0$.
7) $P = \varnothing$: l'algorithme termine et retourne $G = [X^2y - 1, XY^2 - 3, 3X - Y, Y^3 - 9]$.

Test 1.22.

Calculer une base de Gröbner de $[X^2 - Y, Y^2 - X - 1]$ pour l'ordre lexicographique tel que $x > y$, puis pour l'ordre DRL tel que $X > Y$. Dans les deux cas, calculer la forme normale du polynôme $X^4 - X - 1$.

Test 1.23.

Écrire dans un système de calcul formel (comme Maple) l'algorithme de Buchberger.

Dans un premier temps, on montre de façon non constructive la terminaison de l'algorithme de Buchberger. La preuve de sa correction est donnée dans la section suivante.

Théorème 1.84. *L'algorithme de Buchberger se termine.*

PREUVE. D'après la proposition 1.70, les appels à la fonction RÉDUCTION se terminent. La preuve de la terminaison de l'algorithme de Buchberger se fait alors en remarquant que le seul moment où $\langle G \rangle$ change, est lorsque l'on passe par la ligne $G := G \cup \{f_m\}$ dans l'algorithme de Buchberger. Dans ce cas, $\langle G \cup \{f_m\} \rangle \supseteq \langle G \rangle$ et, a fortiori, $\langle \mathrm{LM}(G) \cup \{\mathrm{LM}(f_m)\} \rangle \supset \langle \mathrm{LM}(G) \rangle$.

Comme $f_m =$ RÉDUCTION$(f_m, G, <)$, on sait que f_m n'est pas réductible par G, autrement dit $\mathrm{LM}(f_m)$ n'est pas dans $\langle \mathrm{LM}(G) \rangle$ (proposition 1.74), d'où l'inclusion stricte

$$\langle \mathrm{LM}(G \cup \{f_m\}) \rangle \supsetneq \langle \mathrm{LM}(G) \rangle.$$

Par conséquent, si l'algorithme de Buchberger ne se terminait pas, on pourrait construire une suite infinie strictement croissante d'idéaux monomiaux : $I_m = I_{m-1} + \langle \mathrm{LM}(f_m) \rangle$ pour $m > s$ et $I_s = \langle F \rangle$. Puisque l'anneau de polynômes $\mathbb{Q}[X_1 \dots, X_n]$ est nœthérien (voir le tome *Algèbre L3*), il ne peut contenir une suite strictement croissante d'idéaux, d'où la contradiction. ■

Test 1.24.

On dit qu'une base de Gröbner G est minimale si pour tout $g \in G$, g est unitaire et $\mathrm{LM}_<(g) \notin \langle \mathrm{LM}_<(G \backslash \{g\}) \rangle$. Montrer que si G_1, G_2 sont des bases de Gröbner minimales d'un même idéal I pour un même ordre $<$ alors :

1) $\mathrm{LM}(G_1) = \mathrm{LM}(G_2)$;
2) G_1 et G_2 ont même cardinalité.

V.3. Caractérisation d'une base de Gröbner

L'objectif de cette sous-section est d'obtenir un théorème de caractérisation des bases de Gröbner qui va nous permettre de démontrer que l'algorithme de Buchberger calcule effectivement une base de Gröbner. L'énoncé de ce théorème dépend de la notion de $t-$représentation, où t est un monôme : lorsque l'on considère un élément f d'un idéal $\langle p_1, \ldots, p_k \rangle$, il existe, souvent, une infinité d'écritures possibles de f sous la forme $\sum_{i=1}^k g_i\, p_i$, avec $g_i \in \mathbb{Q}[x_1, \ldots, x_n]$. Une $t-$représentation permet de *borner* (relativement à un ordre monomial fixé) une telle écriture en imposant $t \geq \mathrm{LM}(g_i\, p_i)$ pour tout $i \in \{1, \ldots, k\}$.

Définition 1.85. *Soient $P = [p_1, \ldots, p_k]$ un sous-ensemble fini de $\mathbb{Q}[X_1, \ldots, X_n]$, $f \in \mathbb{Q}[X_1, \ldots, X_n]$ non identiquement nul, et $t \in M$. S'il existe $(g_1, \ldots, g_k) \in \mathbb{Q}[X_1, \ldots, X_n]^k$ tels que*

$$f = \sum_{i=1}^{k} g_i p_i,$$

alors on dit que c'est une t-représentation de f par rapport à P si $t \geq \mathrm{LM}(g_i p_i)$ pour tout $1 \leq i \leq k$.
On note $f = \mathcal{O}_P(t)$ cette propriété et l'on note $f = o_P(t)$ lorsqu'il existe $t' \in T$ tel que $t' < t$ et $f = \mathcal{O}_P(t')$.

Exemple 1.86. On considère l'exemple suivant dans $\mathbb{Q}[X, Y, Z]$, avec l'ordre DRL $X < Y < Z$ et les polynômes $f = X^2YZ - XY^2Z$, $f_1 = XY^2 + XYZ$, $f_2 = X^2Y + XYZ$, alors on a $f = X\, f_1 + Y\, f_2$.
On a donc une écriture de $f \in \langle f_1, f_2 \rangle$ sous la forme $f = g_1\, f_1 + g_2\, f_2$, mais ce n'est pas une $\mathrm{LM}(f)-$représentation puisque $\mathrm{LM}(X\, f_1) = \mathrm{LM}(Y\, f_2) = X^2Y^2 > \mathrm{LM}(f)$.

Le résultat ci-dessous est une conséquence immédiate du corollaire 1.73.

Proposition 1.87.

1) Si Réduction$(p, P, <) = 0$, *alors on a $p = \mathcal{O}_P(\mathrm{LM}(p))$.*

2) Si $p \xrightarrow[P]{*} 0$, alors on a $p = \mathcal{O}_P(\mathrm{LM}(p))$.

Si Réduction$(p, P, <) = 0$, *alors p admet une $\mathrm{LM}(p)-$représentation.*

Le théorème suivant donne une caractérisation non algorithmique des bases de Gröbner.

Théorème 1.88. *G est une base de Gröbner si et seulement si pour tout $f \in \langle G \rangle$ non identiquement nul, on a $f = \mathcal{O}_G(\mathrm{LM}(f))$.*

Preuve.

1) D'après la proposition 1.87, si G est une base de Gröbner (constituée de polynômes unitaires), alors pour tout $f \in \langle G \rangle$ non identiquement nul, on a Réduction$(f, G, <) = 0$, donc $f = \mathcal{O}_G(\mathrm{LM}(f))$.
2) Réciproquement, soit f un élément quelconque de $\langle G \rangle$; par hypothèse, on peut écrire f sous la forme $f = \sum_{i=1}^k h_i g_i$ avec $\mathrm{LM}(f) \geq \max_i \mathrm{LM}(h_i g_i)$. L'inégalité stricte est impossible donc il existe $i \in \{1, \ldots, k\}$ tel que $\mathrm{LM}(f) = \mathrm{LM}(h_i g_i)$. Donc f est top-réductible par g_i, donc par G, et G est une base de Gröbner.

■

Le théorème suivant est plus puissant et est à la base de l'algorithme de Buchberger.

Théorème 1.89. *Soit $G \subset \mathbb{Q}[X_1, \ldots, X_n]$ un ensemble fini de polynômes ne contenant pas zéro. On suppose que pour tout $(g_1, g_2) \in G^2$, on a $\mathrm{Spol}(g_1, g_2) = 0$ ou $\mathrm{Spol}(g_1, g_2) = o_G(\mathrm{ppcm}(g_1, g_2))$, alors G est une base de Gröbner de $\langle G \rangle$.*

Preuve. Soit f un élément non nul de l'idéal $\langle G \rangle$ fixé. Il existe donc $h_1, \ldots, h_k$ dans $\mathbb{Q}[X_1, \ldots, X_n]$ tels que $f = \sum_{i=1}^k h_i g_i$. Parmi toutes ces représentations, on peut choisir celles qui rendent minimales $\mathrm{LM}(h_1 g_1)$. On considère donc l'ensemble non vide

$$\mathcal{A}_f = \left\{ (h_1, \ldots, h_k) \in \mathbb{K}[x_1, \ldots, x_n]^k \mid \sum_{i=1}^{k} h_i g_i = f \right\},$$

pour lequel on définit un ordre total par

$$(h_1, \ldots, h_k) \in \mathcal{A}_f \prec (f_1, \ldots, f_k) \in \mathcal{A}_f, \text{ si}$$
$$\begin{cases} \max_{i \in \{1,\ldots,k\}} \mathrm{LM}(h_i g_i) < \max_{i \in \{1,\ldots,k\}} \mathrm{LM}(f_i g_i) \\ \text{ou } \begin{cases} s = \max_{i \in \{1,\ldots,k\}} \mathrm{LM}(h_i g_i) = \max_{i \in \{1,\ldots,k\}} \mathrm{LM}(f_i g_i) \\ \text{et } \#\{i \in \{1, \ldots, k\} \mid \mathrm{LM}(h_i g_i) = s\} < \#\{i \in \{1, \ldots, k\} \mid \mathrm{LM}(f_i g_i) = s\} \end{cases} \end{cases}.$$

On choisit alors $h = (h_1, \ldots, h_k)$ dans $\min_{\prec} \mathcal{A}_f$.

Quitte à renuméroter G, on peut supposer $\mathrm{LM}(h_1 g_1) = \mathrm{LM}(h_2 g_2) = \cdots = \mathrm{LM}(h_r g_r) > \mathrm{LM}(h_{r+1} g_{r+1}) \geq \cdots \geq \mathrm{LM}(h_k g_k)$.

La preuve s'appuie sur la caractérisation des bases de Gröbner donnée par le théorème 1.88. Elle consiste donc à montrer que $t = \mathrm{LM}(h_1 g_1) \leq \mathrm{LM}(f)$.

On raisonne par l'absurde en supposant que $t > \mathrm{LM}(f)$. Cela implique nécessairement $r \geq 2$. On peut écrire f sous la forme

$$f = h_1 g_1 - \frac{\mathrm{LC}(h_1)}{\mathrm{LC}(h_2)} h_2 g_2 + \left[1 + \frac{\mathrm{LC}(h_1)}{\mathrm{LC}(h_2)}\right] h_2 g_2 + h_3 g_3 + \cdots + h_k g_k.$$

On pose $h'_1 = h_1$ et $h'_2 = \frac{\mathrm{LC}(h_1)}{\mathrm{LC}(h_2)} h_2$, et $r'_i = h'_i - \mathrm{LT}(h'_i)$ pour $i = 1, 2$. On a donc $t = \mathrm{LM}(h'_1 g_1) = \mathrm{LM}(h'_2 g_2)$, et par conséquent $\mathrm{ppcm}(\mathrm{LM}(g_1), \mathrm{LM}(g_2))$ divise t, c'est-à-dire

$$\begin{aligned} h'_1 g_1 - h'_2 g_2 &= \tfrac{\mathrm{LC}(h_1) t}{\mathrm{ppcm}(g_1, g_2)} spol(g_1, g_2) + (r'_1 g_1 - r'_2 g_2) \\ &= \tfrac{t}{\mathrm{ppcm}(g_1, g_2)} o_G(\mathrm{ppcm}(g_1, g_2)) + o_G(t) \\ &= o_G(t), \end{aligned}$$

d'où une nouvelle écriture de f sous la forme

$$f = \alpha\, h_2 g_2 + h_3 g_3 + \cdots + h_k g_k + o_G(t),$$

avec $\alpha = 1 + \frac{\mathrm{LC}(h_1)}{\mathrm{LC}(h_2)}$.

Si $\alpha \neq 0$, on obtient une écriture de f avec $(r-1)$ termes de têtes au lieu de r et, si $\alpha = 0$, on obtient une écriture avec un nombre de termes inférieur ou égal à $(r-2)$ termes. Dans les deux, cas on a trouvé un élément de $\mathcal{A}_f$ qui est $\prec h$, d'où la contradiction.

Par conséquent, on a $\mathrm{LM}(h_1 g_1) = \mathrm{LM}(f)$ et l'on peut utiliser le théorème 1.88 pour montrer que G est une base de Gröbner. ■

Le corollaire suivant donne un moyen algorithmique permettant de vérifier qu'une liste de polynômes est une base de Gröbner.

Corollaire 1.90. *(**Buchberger**) Soit G un sous-ensemble fini de polynômes dans $\mathbb{Q}[X_1, \ldots, X_n]$. G est une base de Gröbner si et seulement si*

1) $\mathrm{Spol}(f, g) \xrightarrow[G]{*} 0$ *pour tout* $(f, g) \in G^2$ *tels que* $f \neq g$ *;*

2) $\textsc{Réduction}(\mathrm{Spol}(f, g), G, <) = 0$ *pour tout* $(f, g) \in G^2$.

Preuve. Les preuves des deux assertions sont très similaires.

Le théorème 1.80 implique immédiatement que si G est une base de Gröbner, alors on a $\textsc{Réduction}(\mathrm{Spol}(f, g), G, <) = 0$ pour tout $(f, g) \in G^2$ et $\mathrm{Spol}(f, g) \xrightarrow[G]{*} 0$ pour tout $(f, g) \in G^2$ tels que $f \neq g$, puisque $\mathrm{Spol}(f, g)$ est un élément de $\langle G \rangle$ par définition.

Considérons $(f, g) \in G^2$, tels que $f \neq g$. On pose $t = \mathrm{LM}(\mathrm{Spol}(f, g) < \mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

1) Si $\mathrm{Spol}(f, g) \xrightarrow[G]{*} 0$, alors d'après la proposition 1.87, on a $\mathrm{Spol}(f, g) = \mathcal{O}_G(\mathrm{LT}(\mathrm{Spol}(f, g))) = \mathcal{O}_G(t) = o_G(\mathrm{ppcm}(f, g))$.
2) De même, si $\textsc{Réduction}(\mathrm{Spol}(f, g), G, <) = 0$, alors d'après la proposition 1.87, on a $\mathrm{Spol}(f, g) = \mathcal{O}_G(\mathrm{LT}(\mathrm{Spol}(f, g))) = \mathcal{O}_G(t) = o_G(\mathrm{ppcm}(f, g))$.

■

On peut maintenant terminer la preuve du théorème de Buchberger.

Théorème 1.91. *L'algorithme de Buchberger calcule une base de Gröbner de l'idéal engendré par* $(f_1, \ldots, f_m)$.

Preuve. On note G_m la base G à l'étape m et $G_s = F$ et $G_k = G$ la base finale. On a $G_s \subset G_{s+1} \subset \cdots \subset G_k$. Pour tout $1 \leq i < j \leq k$, on a (f_i, f_j) est une paire critique. Donc il existe une étape $m \leq k$ où cette paire a été considérée. Deux cas peuvent se présenter :

1) soit $\textsc{Réduction}(\mathrm{Spol}(f_i, f_j), G_m, <) = 0$ et donc $\mathrm{Spol}(f_i, f_j) \xrightarrow[G_k]{*} 0$;
2) soit $\textsc{Réduction}(\mathrm{Spol}(f_i, f_j), G_m, <) = f_{m+1} \neq 0$ et donc $G_{m+1} = \{f_{m+1}\} \cup G_m$, ce qui implique $\textsc{Réduction}(\mathrm{Spol}(f_i, f_j), G_{m+1}, <) = 0$ et donc $\mathrm{Spol}(f_i, f_j) \xrightarrow[G_k]{*} 0$.

La preuve est terminée grâce au corollaire 1.90. ■

Test 1.25.

Soit $F = [t_1, \ldots, t_m]$ une liste de monômes. Montrer que F est une base de Gröbner.

V.4. Propriétés des bases de Gröbner

V.4.1. Élimination

On donne ci-dessous une propriété fondamentale des bases de Gröbner pour l'ordre lexicographique.

Théorème 1.92. (Théorème d'élimination) *Soient I un idéal de $\mathbb{Q}[X_1, \ldots, X_n]$ et $k \in \{1, \ldots, n\}$. Si G est une base de Gröbner pour l'ordre lexicographique ou un ordre par blocs de I, alors $G_k = G \cap \mathbb{Q}[X_k, \ldots, X_n]$ est une base de Gröbner de $I_k = I \cap \mathbb{Q}[X_k, \ldots, X_n]$.*

PREUVE. On fixe $k \in \{1, \ldots, n\}$. On veut montrer que $G_k = G \cap \mathbb{Q}[X_k, \ldots, X_n]$ est une base de Gröbner de I_k. Considérons $f \in I_k \subset I$. Il existe donc $g \in G$ tel que $\mathrm{LM}(g)$ divise $\mathrm{LM}(f) \in \mathbb{Q}[X_k, \ldots, X_n]$, d'où $\mathrm{LM}(g) \in \mathbb{Q}[X_k, \ldots, X_n]$. En appliquant la proposition 1.67, on obtient que $g \in \mathbb{Q}[X_k, \ldots, X_n]$. Donc G_k est une base de Gröbner de I_k. ■

Remarque. En particulier, si on applique le théorème 1.92 avec $l = n$, on obtient que $G \cap \mathbb{Q}[X_n]$ est une base de Gröbner de $I_n = I \cap \mathbb{Q}[X_n]$ dans $\mathbb{Q}[X_n]$. Comme I_n est un idéal principal, il est donc engendré par un polynôme $P_n(x_n)$ (éventuellement identiquement nul).

Test 1.26.

On se donne la courbe $\mathcal{C}$ de $\mathbb{R}^2$ sous forme paramétrique

$$\mathcal{C} \begin{cases} x = t^2 + t \\ y = 2\,t^2 - 2 \end{cases}.$$

1) Calculer une base de Gröbner de $[-x + t^2 + t, -y + 2\,t^2 - 2]$ pour l'ordre lexicographique tel que $t > x > y$.
2) En déduire une équation implicite $f(x, y) = 0$ vérifiée par la courbe $\mathcal{C}$.

V.4.2. Nombre fini de solutions

Si $(f_1, \ldots, f_m) \in \mathbb{Q}[X_1, \ldots, X_n]$ est un système d'équations, on lui associe I l'idéal $\langle f_1, \ldots, f_m \rangle$ et l'on calcule une base de Gröbner G de I pour un ordre admissible $<$ fixé.

On peut détecter facilement si le système admet des solutions.

Proposition 1.93. *Le système admet des solutions dans $\mathbb{C}^n$ si et seulement si G ne contient pas $\{1\}$.*

PREUVE.

En effet, si $1 \in G$, alors tout polynôme de $\mathbb{Q}[X_1, \ldots, X_n]$ se réduit à 0 par 1 donc $I = \mathbb{Q}[X_1, \ldots, X_n]$ et $V(I) = \varnothing$.

Réciproquement, si $V = \varnothing$, alors l'idéal associé à V est égal à $\mathbb{Q}[X_1, \ldots, X_n]$. En particulier $1 \in I$ et comme G est une base de Gröbner, il existe $g \in G$ tel que $\mathrm{LM}(g)$ divise 1, ce qui implique $g = 1$. ■

Le résultat suivant donne une caractérisation des bases de Gröbner des idéaux de dimension zéro. On peut ici faire la corrélation avec le théorème 1.33.

Théorème 1.94. *Soit G une base de Gröbner dans $\mathbb{Q}[X_1, \ldots, X_n]$. Si pour tout $i \in \{1, \ldots, n\}$, il existe $p_i \in G$ tel que $\mathrm{LM}(p) = X_i^{k_i}$ où $k_i \in \mathbb{N}$, alors l'ensemble des points annulant les polynômes de G est de dimension zéro.*

PREUVE. D'après le théorème 1.33, il suffit de montrer que l'anneau-quotient $\frac{\mathbb{Q}[X_1, \ldots, X_n]}{\langle G \rangle}$ est un espace vectoriel de dimension finie.

Définissons $\mathcal{A}_i$ comme l'ensemble des monômes inférieurs à tous les monômes de l'ensemble $\{X_1^{\alpha_1} \cdots X_{i-1}^{\alpha_{i-1}} X_i^{k_i} X_{i+1}^{\alpha_{i+1}} \cdots X_n^{\alpha_n} \mid 0 \leq \alpha_j \leq k_j\}$. Considérons l'intersection des $\mathcal{A}_i$ (pour $1 \leq i \leq n$). On note $\mathcal{A}$ cette intersection.

D'après la définition 1.63 d'ordre admissible, il est clair que $\mathcal{A}$ est fini (voir la propriété 3)).

Ainsi, tous les monômes de $\mathbb{Q}[X_1, \ldots, X_n]$ se récrivent comme combinaison linéaire de monômes de $\mathcal{A}$ dans $\frac{\mathbb{Q}[X_1, \ldots, X_n]}{\langle G \rangle}$. ■

VI. Algèbre linéaire dans les anneaux-quotients – Résolution des systèmes de dimension zéro

Dans cette section, nous étudions comment obtenir une paramétrisation rationnelle de l'ensemble des solutions complexes d'une système d'équations polynomiales F de $\mathbb{Q}[X_1, \ldots, X_n]$ engendrant un idéal de dimension zéro.

Si F est de dimension 0 et $I = \langle F \rangle$, l'anneau-quotient $A = \mathbb{Q}[X_1, \ldots, X_n]/I$ est un $\mathbb{Q}$-espace vectoriel dont la dimension (que l'on note δ dans la suite) est égale au nombre de solutions de S comptées avec multiplicités dans $\mathbb{C}^n$.

À partir d'une base de Gröbner de I, on peut effectuer des calculs dans A puisque l'opération de forme normale est alors canonique. L'idée est alors d'essayer d'exploiter la structure d'espace vectoriel de dimension finie en effectuant des calculs d'algèbre linéaire. Précisons ce point.

Comme dans la première section de ce chapitre, on notera $\bar{A}$ l'anneau-quotient $\frac{\mathbb{C}[X_1,\ldots,X_n]}{I_{\mathbb{C}}}$.

On considère dans A les endomorphismes de multiplication M_f pour tout $f \in A$,

$$\begin{array}{rccc} M_f : & A & \longrightarrow & A \\ & p & \to & fp. \end{array}$$

Évidemment, M_f est une application linéaire et pour tout couple de polynômes f, g, on a $M_f M_g = M_{fg}$. De manière similaire, pour $f \in \bar{A}$, on définit l'application linéaire

$$\begin{array}{rccc} M_f : & \bar{A} & \longrightarrow & \bar{A} \\ & p & \to & fp. \end{array}$$

On a vu précédemment que $\bar{A}$ est isomorphe au produit cartésien d'anneaux locaux $\prod_{x \in V(I)} \bar{A}_x$ (voir théorème 1.48). Dans la suite, pour $x \in V(I)$, on note $\mu(x)$ la multiplicité de x (c'est-à-dire la dimension, en tant qu'espace vectoriel, de l'anneau local $\bar{A}_x$). On notera alors $M_{f,x}$ l'application linéaire de $\bar{A}_x$ dans $\bar{A}_x$ définie par $M_f(\frac{p}{q}) = f\frac{p}{q}$. En considérant $\bar{A}_x$ comme un sous-espace vectoriel de $\bar{A}$, la restriction de M_f à $\bar{A}_x$ sera aussi naturellement notée $M_{f,x}$.

Dans la suite, nous allons étudier comment obtenir des représentations matricielles de ces endomorphismes de multiplication à partir d'une base de Gröbner. Dès lors, nous pourrons effectuer des opérations d'algèbre linéaire dans A en exploitant les propriétés de ces endomorphismes qui seront étudiées dans un second temps. Enfin, nous montrerons comment obtenir un algorithme de résolution des systèmes polynomiaux de dimension zéro.

VI.1. Calcul d'une représentation matricielle des endomorphismes de multiplication

VI.1.1. Escalier et frontière d'un idéal

Définition 1.95. *On considère un idéal de dimension zéro I dans $\mathbb{Q}[X_1, \ldots, X_n]$ et $(G, <)$ une base de Gröbner de I, ainsi que l'ensemble*

$$\mathcal{E}(G) = \{t \in T \mid t \text{ n'est pas réductible par } G\} \text{ trié pour l'ordre } <.$$

On dit que $\mathcal{E}(G)$, l'escalier de I, est une base canonique par rapport à G du $\mathbb{Q}$-espace vectoriel $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$. Rappelons que, dans la suite, on note δ la dimension de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$ en tant qu'espace vectoriel. On note $\mathcal{E}(G) = \{w_1 = 1 < w_2 < \cdots < w_\delta\}$.

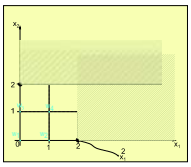


Fig. 1.4. Vecteur dans l'escalier

Exemple 1.96. On considère une base de Gröbner $G_{<_{\text{DRL}}} = \left[X_1^2 - 3\,X_2 - X_1 + 1, X_2^2 - 2\,X_1 + X_2 - 1\right]$ pour l'ordre DRL avec $X_2 > X_1$. Son escalier est $\mathcal{E}(G) = \{t \in T \mid t \text{ n'est pas réductible par } G\} = \{w_1 = 1, w_2 = X_1, w_3 = X_2, w_4 = X_1\,X_2\}$.

Ainsi $\{\overline{w_1}, \overline{w_2}, \overline{w_3}, \overline{w_4}\}$ est une base de l'espace vectoriel quotient $\mathbb{Q}[X_1, \ldots, X_n]/I$.

Dans cette base, le polynôme $-X_1^2 - X_2^2 + 7\,X_1\,X_2 \longrightarrow -3\,X_1 - 2\,X_2 + 7\,X_1\,X_2$ est le vecteur $[0, -3, -2, 7]$.

Proposition 1.97. *Si $1 \neq e \in \mathcal{E}(G)$, alors pour tout i tel que X_i divise e, on a $\frac{e}{X_i} \in \mathcal{E}(G)$.*

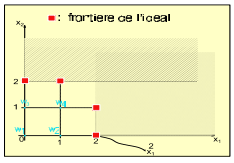


Fig. 1.5. Frontière

Comme expliqué précédemment, on cherche à calculer incrémentalement les formes normales en se restreignant à des opérations élémentaires du type $\varphi(X_i p)$, où $e \in E$. On peut donc supposer que $p = \sum_{i=1}^{\delta} \lambda_i w_i$ et on peut donc calculer des formes normales de la forme $\varphi(X_i e)$, où $e \in \mathcal{E}(G)$. Le cas où $X_i e \in \mathcal{E}(G)$ est trivial car $\varphi(X_i e) = X_i e$ s'obtient sans calcul. Reste le cas où $X_i e \notin \mathcal{E}(G)$. Pour estimer le nombre de tels éléments, on introduit la notion de frontière, c'est-à-dire les points qui sont à distances 1 de l'escalier.

Définition 1.98. *Soit $\mathcal{E}(G)$ la base canonique de $\mathbb{Q}[X_1, \ldots, X_n]/I$, alors*

$$\mathcal{F}(G) = \{X_i e \mid e \in \mathcal{E}(G),\ 1 \leq i \leq n \text{ et } X_i\, e \notin \mathcal{E}(G)\}$$

est la frontière de G.

Exemple 1.99. On considère une base de Gröbner $G_{<_{\text{DRL}}} = \left[X_1^2 - 3\,X_2 - X_1 + 1, X_2^2 - 2\,X_1 + X_2 - 1\right]$ pour l'ordre DRL avec $X_2 > X_1$.

Par définition, la frontière de G est l'ensemble $\mathcal{F}(G) = \{X_i e \mid e \in \mathcal{E}(G),\ 1 \leq i \leq n \text{ et } X_i\, e \notin \mathcal{E}(G)\}$.

Donc, on a $\mathcal{F}(G) = \left\{X_1^2,\ X_2^2,\ X_1^2 X_2,\ X_1 X_2^2\right\}$.

Définition 1.100. *Une base de Gröbner réduite est une base dont aucun élément n'est réductible par les autres.*

Proposition 1.101. *Si I est un idéal de dimension zéro et $(G,<)$ une base de Gröbner réduite par rapport à un ordre admissible $<$, alors pour tout élément $t \in \mathcal{F}(G)$*

1) soit il existe $g \in G$ tel que $t = \mathrm{LM}(g)$;

2) soit il existe j et $t' \in \mathcal{F}(G)$ tels que $t = X_j t'$.

PREUVE. On fixe $t \in \mathcal{F}(G)$ et l'on considère l'ensemble $A_t = \{1 \leq j \leq n \text{ tel que } X_j \text{ divise } t \text{ et} \frac{t}{X_j} \notin \mathcal{E}(G)\}$.

1) Si A_t est vide, comme $t \notin \mathcal{E}(G)$, il existe $g \in G$ tel que $\mathrm{LM}(g)$ divise t : soit $u = \frac{t}{\mathrm{LM}(g)}$. S'il existait X_j divisant u, alors en posant $v = \frac{u}{X_j}$, on aurait $\frac{t}{X_j} = \mathrm{LM}(g)\, v \notin \mathcal{E}(G)$ et donc $j \in A_t$ ce qui est absurde. Donc on a $u = 1$ et $\mathrm{LM}(g) = t$.
2) Si A_t n'est pas vide, il existe donc j tel que X_j divise t et $t' = \frac{t}{X_j} \notin \mathcal{E}(G)$. Comme $t \in \mathcal{F}(G)$, il existe $e \in \mathcal{E}(G)$ tel que $t = X_i\, e$. Comme $X_i\, e = t$ et $t = X_j\, t'$, l'égalité $i = j$ est impossible puisqu'elle impliquerait $t' = e$ et donc $e \in \mathcal{E}(G)$, ce qui est contradictoire avec le fait que $e \in \mathcal{E}(G)$. Donc $i \neq j$ et X_j divise e ; de plus, $e' = e/X_j$ (d'après la proposition 1.97) est dans $\mathcal{E}(G)$. Ainsi $t' = X_i \cdot e' \in \mathcal{F}(G)$ et t est de la forme $t = X_j\ t'$.

■

Corollaire 1.102. *Le nombre de générateurs d'une base de Gröbner réduite d'un idéal zéro dimensionnel I est inférieur à $n\delta$.*

PREUVE. Si $g \in G$, alors $\mathrm{LM}(g) \notin \mathcal{E}(G)$ et pour tout k tel que X_k divise $\mathrm{LM}(g)$, on a $\frac{\mathrm{LM}(g)}{X_k} \in \mathcal{E}(G)$; donc on a $\mathrm{LM}(g) \in \mathcal{F}(G)$. La borne découle du fait que $\mathrm{LM}(G) \subseteq \mathcal{F}(G)$. ■

VI.1.2. Construction des matrices de multiplication

Dans la suite, on travaille dans l'espace vectoriel $\mathbb{Q}[X_1,\ldots,X_n]/I$ (de dimension δ) et l'on considère la base canonique pour l'ordre $<$ associée à G :

$$\mathcal{E}(G) = \{w_1 = 1 < w_2 < \cdots < w_\delta\}\,.$$

Pour trouver l'expression d'un polynôme f dans cette base, on doit calculer $\mathrm{NF}(f,G)$ en utilisant l'algorithme **Réduction totale**. Cependant, il est difficile d'obtenir une borne de complexité précise en théorie ou en pratique. C'est la raison pour laquelle on va ramener ce calcul à un produit matrice-vecteur dont il sera facile de borner la complexité.

Dans la suite, on suppose que l'on connaît une fonction linéaire

$$\varphi_I : \begin{pmatrix} \mathbb{Q}[X_1,\ldots,X_n] & \longrightarrow & \mathbb{Q}[X_1,\ldots,X_n]/I \\ p & \longmapsto & \overline{p} \end{pmatrix}$$

qui soit une forme normale, c'est-à-dire qui vérifie les propriétés

$$\begin{array}{l} \varphi_I(p) = 0 \text{ si et seulement si } p \in I \\ \text{et } \varphi_I(p\cdot q) = \varphi_I(p\cdot\varphi_I(q)) = \varphi_I(\varphi_I(p)\cdot\varphi_I(q)). \end{array}$$

Un moyen pour se donner une telle forme normale est de calculer une base de Gröbner G de I pour l'ordre admissible $<$ et ensuite de prendre $\varphi_I(p) = \mathrm{NF}(p,G,<)$. Dans ce cas, on sait que le noyau de φ_I est égal à I : $\ker(\varphi_I) = I$. Dans la suite, on note $\varphi_I(p) = \mathrm{NF}(p)$ cette fonction de forme normale. Pour optimiser le calcul, on va exploiter la structure de $\mathcal{F}(G)$ donnée par la proposition 1.101 : on va calculer uniquement des formes normales de la forme $\varphi_I(X_i \cdot p)$, où p est déjà réduit. On considère donc les applications linéaires de multiplication par une variable

$$\phi_i : f \longmapsto \varphi_I(X_i\, f).$$

Définition 1.103. *Pour tout $1 \leq k \leq n$, on définit la matrice $M^{(k)}$ de taille $\delta \times \delta$ telle que $M^{(k)}_{i,j}$ est le coefficient de w_i dans $X_k\, w_j$.*

Afin de décrire l'algorithme permettant de calculer les matrices de multiplication par une variable, on utilise comme notation le symbole $\delta_{i,j}$, dit de Kronecker, qui vaut 1 si $i = j$ et 0 sinon. Si M est une matrice, alors $\mathrm{Col}(M,j)$ désigne la j-ième colonne de M.

Algorithme **Matrices de multiplications**

ENTRÉES : G une base de Gröbner réduite pour l'ordre $<$, $\mathcal{E}(G) = \{w_1 = 1 < w_2 < \cdots < w_\delta\}$ une base canonique pour G. une table de polynômes indexée par T
SORTIES : La matrice d emultiplication par X_k.

$N := [\,]$
pour $1 \leq i \leq \delta$ **faire**
  $N[w_i] := w_i$
  pour tout k tel que $w_i = X_k\, w_j$ **faire**
    $M_{l,j}^{(k)} := \delta_{l,i}$ pour tout $l \in \{1, \ldots, n\}$
    $F := [X_j\, w_i$ pour $j = 1, \ldots, n$, $i = 1, \ldots, \delta]$
    trier F pour $<$, éliminer les doublons et les éléments de F se trouvant dans $\mathcal{E}(G)$
  fin pour
fin pour
pour t dans F **faire**
  si t est un multiple strict d'un terme de tête de G **alors**
    $t = X_j\, t'$ avec $t' < t$
    On a déjà calculé $N[t'] = \sum_{i=1}^{s} \mu_i w_i$ avec $\mu_i \in \mathbb{Q}$ et $w_s < t'$
    $N[t] = \sum_{i=1}^{s} \mu_i \operatorname{Col}(M^{(j)}, i) = \sum_{i=1}^{\delta} \lambda_i w_i$
    pour tout k tel que $t = X_k\, w_l$ pour un certain l **faire**
      $M_{i,j}^{(k)} := \lambda_i$ pour tout $i \in \{1, \ldots, n\}$
    fin pour
  sinon
    il existe $g = t + \sum_{i=1}^{\delta} \lambda_i w_i$ et $\lambda_i \in \mathbb{Q} \in G$ tels que $t = \operatorname{LM}(g)$
    $N[t] := -\sum_{i=1}^{\delta} \lambda_i\, w_i$
    pour tout k tel que $t = X_k\, w_j$ pour un certain j **faire**
      $M_{i,j}^{(k)} := -\lambda_i$ pour tout $i \in \{1, \ldots, n\}$
    fin pour
  fin si
fin pour
Retourner $M^{(k)}$.

Théorème 1.104. *L'algorithme ci-dessus calcule les matrices $M^{(k)}$ et la complexité arithmétique est bornée par $O(n\,\delta^3)$.*

PREUVE. Pour montrer la correction de l'algorithme, il suffit de montrer que dans l'expression $N[t] = \sum_{i=1}^{s} \mu_i \operatorname{Col}(M^{(j)}, i)$, la colonne i de la matrice $M^{(j)}$ a déjà été calculée auparavant. Comme $N[t'] = \sum_{i=1}^{s} \mu_i w_i$ avec $w_s < t'$, on a $\operatorname{NF}(t) = \operatorname{NF}(X_j\, t') = \sum_{i=1}^{s} \mu_i \operatorname{NF}(X_j\, w_i)$. De plus, l'ordre est admissible, si bien que l'on a $X_j w_i < X_j w_s < X_j\, t' = t$. Donc tous les termes $X_j\, w_i$ ont été traités et la colonne i de la matrice $M^{(j)}$ a été remplie.

Dans l'algorithme, il est clair que F est la frontière $\mathcal{F}(G)$ et donc le nombre d'itérations dans la boucle principale est borné par $n\,\delta$; de plus, le calcul de $\sum_{i=1}^{s} \mu_i \operatorname{Col}(M^{(j)}, i)$ nécessite au plus $s\,\delta \leq \delta^2$ opérations. ■

VI.2. Propriétés des endomorphismes de multiplication

Les propriétés ci-dessous permettent de relier les valeurs propres des endomorphismes de multiplication M_f aux valeurs prises par f en les éléments de $V(I)$.

Théorème 1.105. *Soit $x \in V(I)$, alors $f(x)$ est une racine du polynôme caractéristique de M_f et sa multiplicité est $\mu(x)$.*

PREUVE. Considérons un idempotent e_x associé à x. Puisque $e_x(f - f(x))$ s'annule en chaque point de $V(I)$ (voir proposition 1.46), d'après le théorème 1.16, il existe $k \in \mathbb{N}$ tel que $(e_x(f - f(x)))^k = 0$ dans $\bar{A}$. Cela implique que l'endomorphisme de multiplication $M_{e_x(f-f(x))}$ est nilpotent et a comme unique valeur propre 0, avec une multiplicité égale à $\mu(x)$. Ainsi $M_{f,x}$ a une unique valeur propre $f(x)$ de multiplicité $\mu(x)$. Le théorème 1.48 permet alors de conclure. ■

Remarque. Si I est supposé radical et u un élément séparant de $V(I)$, on a immédiatement dans la preuve ci-dessus que $e_x(u - u(x)) = 0$ dans $\bar{A}$, ce qui implique que $\mu(x) = 1$. On vient de montrer que si I est radical, on a $\mu(x) = 1$ pour tout $x \in V(I)$. Dans ce cas, on sait alors que la dimension de A coïncide avec le nombre d'éléments de $V(I)$ puisque l'on a précédemment montré qu'elle est égale à $\sum_{x \in V(I)} \mu(x)$.

Le résultat ci-dessus induit immédiatement le thèorème ci-dessous, connu sous le nom de théorème de Stickelberger.

Théorème 1.106. *(**Théorème de Stickelberger**) Soit $f \in \bar{A}$, alors l'application linéaire M_f a les propriétés suivantes :*

1) *la trace de M_f est égale à $\sum_{x\in V(I)} \mu(x)f(x)$;*
2) *le déterminant de M_f est égal à $\prod_{x\in V(I)} f(x)^{\mu(x)}$;*
3) *le polynôme caractéristique de M_f est égal à $\prod_{x\in V(I)}(T - f(x))^{\mu(x)}$.*

Le théorème de Stickelberger va permettre de déduire un algorithme permettant de tester si un idéal de dimension zéro est radical ou pas.

Pour $f \in A$, on définit l'application bilinéaire suivante :

$$\begin{array}{rccc} \mathrm{Herm}_{f,I} : & A \times A & \longrightarrow & \mathbb{Q} \\ & (p,q) & \to & \mathrm{Tr}(M_{pqf}). \end{array}$$

La forme quadratique – que l'on appellera dans la suite forme quadratique de Hermite associée à f – est alors

$$\begin{array}{rccc} \mathrm{QuadHerm}_{f,I} : & A & \longrightarrow & \mathbb{Q} \\ & p & \to & \mathrm{Tr}(M_{p^2f}). \end{array}$$

Dans la suite, si $f = 1$, on notera Herm_I (respectivement $\mathrm{QuadHerm}_I$) en lieu et place de $\mathrm{Herm}_{1,I}$ (respectivement $\mathrm{QuadHerm}_{f,I}$). On appellera $\mathrm{QuadHerm}_I$ la forme quadratique de Hermite.

Théorème 1.107. *Le rang de la forme quadratique de Hermite est égal au nombre de points de $V(I)$ (comptés sans multiplicité).*

Preuve. Soient D le nombre d'éléments de $V(I)$ et δ la dimension de A. On a évidemment $D \leq \delta$. Soit u un élément séparant. D'après le lemme 1.39, les éléments $\omega_1 = 1, \omega_2 = u, \ldots, \omega_D = u^{D-1}$ forment une famille de vecteurs libres dans A et cette famille peut donc être complétée par $\delta - D$ éléments $\omega_{D+1}, \ldots, \omega_\delta$ de A, formant ainsi une base du $\mathbb{Q}$-espace vectoriel A.

Considérons $g = \sum_{i=1}^{\delta} g_i\omega_i \in A$. On déduit du théorème de Stickelberger (théorème 1.106 ci-dessus) une expression de la forme quadratique de Hermite

$$\mathrm{QuadHerm}_I(g) \sum_{x\in V(I)} \mu(x)f(x)\left(\sum_{i=1}^{\delta} g_i\omega_i\right).$$

Ainsi, si l'on note $\alpha_1, \ldots, \alpha_\delta$ les éléments de $V(I)$, la forme quadratique de Hermite associée à f est l'application qui à g associe

$$(g_1, \ldots, g_\delta)M^t\Delta(\mu(\alpha_1), \ldots, \mu(\alpha_\delta))M(g_1, \ldots, g_\delta)^t,$$

où M est la matrice

$$\begin{bmatrix} 1 & u(\alpha_1) & \cdots & u(\alpha_1)^{D-1} & \omega_{D+1}(\alpha_1) & \cdots & \omega_\delta(\alpha_1) \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & u(\alpha_1) & \cdots & u(\alpha_1)^{D-1} & \omega_{D+1}(\alpha_1) & \cdots & \omega_\delta(\alpha_1) \end{bmatrix}$$

et $\Delta(\mu(\alpha_1), \ldots, \mu(\alpha_\delta))$ est la matrice diagonale dont les éléments sur la diagonale sont $(\mu(\alpha_1), \ldots, \mu(\alpha_\delta))$. Il est alors immédiat que le rang de M est égal à D puisque u est séparant et que le mineur principal de M est un déterminant de Vandermonde. Ainsi, le rang de la forme quadratique de Hermite est égal à D. ■

VI.3. Calcul des paramétrisations rationnelles

Voyons maintenant comment déduire des résultats ci-dessus un algorithme de résolution de systèmes d'équations polynomiales $f_1 = \cdots = f_p = 0$, dans le cas où $\langle f_1, \ldots, f_p\rangle$ est radical et zéro-dimensionnel. Cet idéal de I est décrit par une base de Gröbner qui aura été préalablement calculée, si bien que l'on dispose d'une base de Gröbner et d'une base monomiale de l'anneau-quotient $A = \frac{\mathbb{Q}[X_1,\ldots,X_n]}{I}$.

L'algorithme va se décomposer en trois étapes :

1) on va d'abord chercher un élément séparant de $V(I)$;
2) puis on va tester si l'idéal I est radical ;
3) s'il est radical, on va calculer des paramétrisations rationnelles des solutions de I ; s'il n'est pas radical, on verra comment ajouter un polynôme au système initial, de manière à obtenir un nouveau système d'équations polynomiales définissant le même ensemble de solutions complexes, mais engendrant un idéal radical.

Pour les deux premières étapes, le théorème 1.107 joue un rôle essentiel.

VI.3.1. Tester si I est radical et rechercher un élément séparant

Soit δ le degré de I (que l'on obtient facilement en comptant le nombre d'éléments d'une base monomiale de A). D'après le théorème 1.107, le nombre d'éléments de $V(I)$ est égal au rang de la forme quadratique de Hermite. Ce rang D peut aisément être calculé en construisant la matrice associée à cette forme quadratique dans A.

Ainsi, tester si $\delta = D$ revient à tester si I est radical. D'après le lemme 1.39, u est un élément séparant de $V(I)$ si et seulement si $1, u, \ldots, u^{D-1}$ est une famille de vecteurs linéairement indépendants de A. Ainsi, tester si u est un élément séparant de $V(I)$ revient à tester que $1, u, \ldots, u^{D-1}$ sont linéairement indépendants dans A, ce qui revient à s'assurer que la matrice dont les colonnes sont les vecteurs $1, u, \ldots, u^{D-1}$ (exprimés dans une base monomiale de A) a un déterminant non nul.

On effectuera alors ce test dans la famille $X_1 + iX_2 \cdots + i^{n-1}X_n$ (pour $0 \leq i \leq (n-1)\binom{D}{2}$ qui contient forcément un élément séparant d'après le lemme 1.38.

Notons que tous les calculs intervenant ci-dessus consistent à évaluer le rang d'une matrice.

VI.3.2. Calcul de paramétrisations rationnelles de $V(I)$ lorsque I est radical

On dispose d'un élément séparant u de $V(I)$ et l'on suppose que I est radical. D'après le théorème 1.106 de Stickelberger, puisque I est radical, le polynôme caractéristique q de M_u est donné par $\prod_{\alpha_i \in V(I)}(T - u(\alpha_i))$. Par ailleurs, toujours parce que I est radical, $1, u, \ldots, u^{D-1}$ est une base de A. Ainsi pour tout $1 \leq i \leq n$, il existe $(\lambda_{1,i}, \ldots, \lambda_{D,i}) \in \mathbb{Q}^D$ tel que $X_1 = \sum_{j=1}^{D} \lambda_{j,i} u^{j-1}$ dans A. Notons q_i le polynôme $\sum_{j=1}^{D} \lambda_{j,i} T^{j-1}$. Il est alors immédiat que la paramétrisation

$$\begin{cases} X_n &= q_n(T) \\ &\vdots \\ X_1 &= q_1(T) \\ q(T) &= 0 \end{cases}$$

définit l'ensemble des points de $V(I)$ puisque pour tout i, on a $X_i - \sum_{j=1}^{D} \lambda_{j,i} u^{j-1} \in I$.

Remarquons que le calcul des polynômes q_i revient à résoudre un système d'équations linéaires.

VI.3.3. Gestion des cas où I n'est pas radical

Supposons maintenant que I ne soit pas radical, mais que l'on dispose d'un élément séparant u de $V(I)$. Considérons le polynôme caractéristique $q(T)$ de M_u et notons par q_u le polynôme $q(u)$. D'après le théorème de Cayley-Hamilton, $q_u(M_u(1))$ vaut 0 dans A, si bien que $q_u(u) \in I$ et la partie sans facteur carré de q_u appartient à $\sqrt{I}$. D'après le théorème 1.106 de Stickelberger, la partie sans facteur carré de q_u est exactement le polynôme caractéristique, évalué en u, de l'endomorphisme de multiplication par u dans $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{\sqrt{I}}$. Dans la suite, on note m_u la partie sans facteur carré de q_u. Nous allons montrer que $I + \langle m_u \rangle$ est égal à $\sqrt{I}$.

Remarquons d'abord que $I + \langle m_u \rangle$ est contenu dans $\sqrt{I}$ puisque $I \subset \sqrt{I}$ et $m_u \in \sqrt{I}$. Remarquons aussi que $1, u, \ldots, u^{D-1}$ est une base de $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I+\langle m_u \rangle}$ puisque, d'après le théorème 1.106 de Stickelberger, $m_u = \prod_{\alpha_i \in V(I)}(u - u(\alpha_i))$. Donc $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{I+\langle m_u \rangle}$ et $\frac{\mathbb{Q}[X_1,\ldots,X_n]}{\sqrt{I}}$ ont même dimension alors que $V(I + \langle m_u \rangle) = V(\sqrt{I})$ puisque $m_u \in \sqrt{I}$. On a donc bien $I + \langle m_u \rangle = \sqrt{I}$.

Finalement, si I n'est pas radical, le calcul de la partie sans facteur carré du polynôme caractéristique de M_u permet d'obtenir m_u. Le système d'équations polynomiales $f_1 = \cdots = f_p = m_u = 0$ définit alors $V(I)$, mais engendre un idéal radical.

VII. Exercices

1.1. ⋆

Soit k un corps. On note $k[X]_{<m}$ l'ensemble des polynômes de degré strictement inférieur à m. Soient $P, Q \in k[X]$ des polynômes de degrés respectifs $m \geq n$. On considère l'application de Sylvester

$$\begin{array}{rl} \phi_{P,Q} : k[X]_{<n} \times k[X]_{<m} & \to k[X]_{<m+n} \\ (U, V) & \mapsto U.P + V.Q. \end{array}$$

1) Donner la matrice de $\phi_{P,Q}$ dans la base $(1,0), (X,0), \ldots, (X^{n-1},0)$, $(0,1), \ldots, (0, X^{m-1})$.
2) Rappeler pourquoi le noyau de $\phi_{P,Q}$ est non trivial si et seulement si P et Q ont un facteur commun.
3) On suppose que P et Q ont un PGCD D de degré $d > 0$. Donner un couple (U, V) du noyau de $\phi_{P,Q}$; quels sont les degrés des polynômes U et V correspondant ?
4) En déduire une base du noyau de $\phi_{P,Q}$ en fonction de d. Quel lien trouvez-vous entre le rang de l'application de Sylvester $\phi_{P,Q}$ et le degré d du PGCD de P et Q ?
5) Montrer que si P et Q sont premiers entre eux, il existe un unique couple $(S, T) \in k[X]_{<n} \times k[X]_{<m}$ tel que $\phi_{P,Q}(S, T) = 1$. Que vous rappelle cette relation ? Comment aurait-on pu trouver ces polynômes S et T autrement ?

1.2. ⋆

1) Calculer le résultant des polynômes P et Q dans les cas suivants :
$$P = x^2 - x + 4,\ Q = x^2 - 3x + 1\,;$$
et $P = 2x^3 - x^2 + 7x + 4,\ Q = 2x^2 + 11x + 5.$
2) Dans les deux cas, appliquer l'algorithme d'Euclide à P et Q. Écrire la matrice de Sylvester de P et

Q, et lui appliquer la réduction par pivot de Gauss. Qu'observez-vous ?

3) On considère la quadrique réelle $\mathcal{C}$ d'équation $x^2 - y^2 - z^2 + 1 = 0$ et le plan $\mathcal{P}$ d'équation $2x + 2y - z = 0$. Trouver l'équation de la projection orthogonale de l'intersection $\mathcal{C} \cap \mathcal{P}$ sur le plan $z = 0$.

1.3. ⋆

L'algorithme de Buchberger, tel qu'il a été présenté dans ce chapitre, est trop peu efficace. Il a été amélioré de diverses manières, notamment en intégrant des critères de sélection des paires critiques. Dans cet exercice, on étudie le premier critère de Buchberger. Soit $<$ un ordre monomial admissible fixé.

1) Si $F = [g_1, g_2]$ où les polynômes g_1, g_2 vérifient $\mathrm{ppcm}(g_1, g_2) = \mathrm{LM}(g_1)\,\mathrm{LM}(g_2)$, montrer que F est une base de Gröbner (utiliser le théorème 1.89).
2) En déduire la valeur de RÉDUCTION$(\mathrm{Spol}\,(g_1, g_2)\ , G, <\ )$.
3) Calculer une base de Gröbner de $\left[x^2 - y, y^2 - x - 1\right]$ pour l'ordre DRL $x > y$.
4) Généraliser pour plusieurs polynômes.
5) Expliquer comment on peut améliorer l'algorithme de Buchberger en utilisant ce critère.

1.4. ⋆

On étudie dans cet exercice un algorithme pour calculer l'intersection de deux idéaux.

1) Si I et J sont des idéaux, montrer que $I \cap J$ est idéal.
2) Soient I et J des idéaux de $\mathbb{Q}[X_1, \ldots, X_n]$, et t une nouvelle variable. On note $t \cdot I = \{t \cdot h : h \in I\}$ et $(1-t)\cdot J = \{(1-t)\cdot h : h \in J\}$ dans $\mathbb{Q}[t, X_1, \ldots, X_n]$. Montrer que $I \cap J = (t \cdot I + (1-t)\cdot J) \cap \mathbb{Q}[X_1, \ldots, X_n]$.
3) En utilisant le théorème 1.92 d'élimination, donner un algorithme pour calculer une base de l'idéal $\langle f_1, \ldots, f_s\rangle \cap \langle h_1, \ldots, h_m\rangle$.
4) Si I est un idéal et f un polynôme, on définit $I : f = \{h \in \mathbb{Q}[X_1, \ldots, X_n] \mid f \cdot h \in I\}$. Montrer que si l'idéal $I \cap \langle f\rangle$ est engendré par $(g_1, \ldots, g_s)$, alors $I : f = \langle \frac{g_1}{f}, \ldots, \frac{g_s}{f}\rangle$. En déduire un algorithme pour calculer $I : f$.

COMPLÉMENT 1. ALGORITHME DE CHANGEMENT DE BASE FGLM

D'une base de Gröbner à une autre via l'algèbre linéaire

L'algorithme FGLM permet de transformer une base de Gröbner engendrant un idéal de dimension zéro calculée pour un premier ordre admissible (par exemple l'ordre DRL) en une base de Gröbner pour un second ordre admissible (par exemple l'ordre lexicographique). On parle dans tous les cas d'algorithme de changement d'ordre.

1.1. Algorithme FGLM

1.2. Introduction

L'algorithme FGLM permet de ramener à un calcul d'algèbre linéaire l'opération de changement d'ordre d'une base de Gröbner d'un idéal zéro-dimensionnel. Un avantage théorique de cet algorithme est de pouvoir dériver une estimation très précise de la complexité de cet algorithme.

Pour appliquer l'algorithme FGLM, il suffit d'une base de Gröbner calculée pour un ordre admissible ; à partir de cette base, on calcule des matrices de multiplications par les variables. Comme on l'a vu dans le chapitre précédent, ces matrices peuvent être utilisées pour calculer numériquement les racines d'un système algébrique : les valeurs propres des matrices de multiplications donnent les projections des solutions du système (voir théorème 1.106). Symboliquement, le plus petit polynôme de la base de Gröbner pour l'ordre lexicographique est aussi le polynôme minimal de la matrice de multiplication par la plus petite variable.

Pour simplifier l'écriture des algorithmes, on écarte également le cas trivial où $I = \mathbb{Q}[X_1, \ldots, X_n]$.

1.3. Espace vectoriel quotient - idée de l'algorithme

On suppose que l'on connaît une base de Gröbner G de l'idéal I, supposé de dimension zéro, pour un certain ordre (par exemple l'ordre DRL). Alors l'application $\varphi : p \longmapsto \text{NORMALFORM}(p, G)$ est linéaire et son noyau est $\ker(\varphi) = I = \langle G \rangle$.

On peut définir une relation d'équivalence $p \equiv q$ si et seulement si $\varphi(p) = \varphi(q)$.

On définit ensuite la classe d'équivalence d'un polynôme p par $\overline{p} = \{q \in \mathbb{Q}[X_1, \ldots, X_n] \mid \varphi(q) = \varphi(p)\}$. L'ensemble de ces classes d'équivalences constitue l'algèbre-quotient

$$A = \mathbb{Q}[X_1, \ldots, X_n]/I = \{\overline{p} \mid p \in \mathbb{Q}[X_1, \ldots, X_n]\}.$$

Une conséquence du théorème 1.94 est que cet espace vectoriel est un espace vectoriel de dimension finie $D = \deg(I)$.

Pour donner une idée de l'algorithme, supposons que l'on cherche à calculer un polynôme en une variable, disons X_i, dans l'idéal. On considère alors les éléments suivants de $\mathbb{E}$:

$$\overline{1}, \overline{X_i}, \overline{X_i^2}, \cdots, \overline{X_i^D}.$$

Comme E est de dimension D, on sait que ces vecteurs ne sont pas linéairement indépendants. Il existe $(\lambda_i)_{i=0,\ldots,D}$ de $\mathbb{Q}$ non tous nuls tels que :

$$\lambda_0 \overline{1} + \lambda_1 \overline{X_i}, \overline{X_i^2} + \cdots + \lambda_D \overline{X_i^D} = 0.$$

Autrement dit, on a trouvé le polynôme $P_i(X_i) = \sum_{j=0}^{D} \lambda_j X_i^j$ tel que $\overline{P_i} \equiv 0$ c'est-à-dire $P_i \in I$.

Pour l'évaluation de la complexité d'un tel algorithme, la principale difficulté est de compter le nombre d'opérations pour le calcul de

$$\varphi(1), \varphi(X_i), \varphi\left(X_i^2\right), \cdots, \varphi\left(X_i^D\right).$$

En fait, on remarque que l'on peut toujours écrire le calcul de la forme normale X_i^k comme : $\varphi\left(X_i^k\right) = \varphi\left(X_i \varphi\left(X_i^{k-1}\right)\right)$; on peut calculer incrémentalement ces formes en se contentant des opérations élémentaires suivantes :

$$p \longmapsto \psi(p) = \varphi(X_i\, p).$$

1.4. Description de l'algorithme FGLM

Dans l'algorithme suivant si S est une liste alors :

1) $\#S$ désigne le nombre d'éléments de S ;
2) $\text{first}(S)$ est le premier élément de la liste ou $\varnothing$ si S est vide.

Algorithme **FGLM**

Entrée : $<_2$un ordre admissible et NF une forme normale.
Sortie : base de Gröbner réduite de l'idéal I pour $<_2$
où $I = \{f \in \mathbb{Q}[X_1, \ldots, X_n] \mid \mathrm{NF}(f) = 0\}$
$L := [\,]$ // liste des prochains termes à étudier
$S := [\,]$ // l'escalier pour le nouvel ordre $<_2$
$V := [\,]$ // $V = \mathrm{NF}(S)$
$G := [\,]$, $t := 1$
Répéter
$v := \mathrm{NF}(t)$ et $s := \#S$ le nombre d'éléments de S.
Si $v \in \mathrm{Vect}_{\mathbb{Q}}(V)$ **alors**
on peut trouver (λ_i) t.q. $v = \sum_{i=1}^{s} \lambda_i \cdot V_i$
$G := G \cup \left[v - \sum_{i=1}^{s} \lambda_i \cdot S_i \right]$
sinon
$S := S \cup [t]$ et $V := V \cup [v]$
$L := \mathrm{Sort}(L \cup [X_i\, t \mid i = 1, \ldots, n], <_2)$
Éliminer de L les doublons et les multiples de $\mathrm{LM}(G)$
if $L = \varnothing$ then
Retourner G
$t := \mathrm{first}(L)$ et supprime t de L.

Le théorème 1.108 prouve que cet algorithme se termine et retourne le bon résultat.

1.5. Version matricielle de FGLM

Afin de rendre explicite la détection de la dépendance linéaire des vecteurs du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[X_1, \ldots, X_n]/I$, on introduit la matrice de passage P entre l'ancienne base $\mathcal{E}(G) = \{w_1 = 1 < w_2 < \cdots < w_{\deg(I)}\}$ et la nouvelle base S en cours de construction. Si l'on note $S = [\varepsilon_1, \ldots, \varepsilon_{\deg(I)}]$ cette base, alors à tout moment de l'algorithme on a

$$S = P \cdot \mathcal{E}(G).$$

Initialement $S = [w_1]$, et on construit incrémentalement des vecteurs $v = \varphi(X_k\, w) = M^{(k)} \cdot w$ où v, w sont des vecteurs exprimés dans la base $\mathcal{E}(G)$ définie par $v = \sum_{i=1}^{\deg(I)} v_i\, w_i$.

Pour tester l'indépendance linéaire, il suffit de calculer $\lambda = P \cdot v = \sum_{i=1}^{\deg(I)} \lambda_i\, w_i$.

1 Si $\lambda_{s+1} = \cdots = \lambda_{\deg(I)} = 0$, où s est le nombre d'éléments de S, alors le vecteur v appartient au $\mathbb{Q}$-espace vectoriel engendré par S.

2 S'il existe $k > s$ tel que $\lambda_k \neq 0$, alors $\varepsilon_{s+1} = \lambda$ est un vecteur linéairement indépendant. On calcule une nouvelle matrice P' telle que

$$P' \cdot v =^T [0, \ldots, 0, 1, 0, \ldots, 0] = \varepsilon_{s+1}. \tag{1.5}$$

La procédure MISE À JOUR met à jour la matrice P pour que l'équation (1.5) soit vérifiée.

Algorithme **MISE À JOUR**

Entrée : $s \in \mathbb{N}$, le vecteur λ, la matrice P
Sortie : la matrice P mise à jour
$k := \min\{j > s$ tel que $\lambda_j \neq 0\}$
Pour j **de** 1 **à** $\deg(I)$ **faire**
$\alpha := \frac{P_{j,k}}{P_{k,k}}$, $P_{j,k} := P_{s+1,j}$, $P_{s+1,j} := \alpha$
si $\alpha \neq 0$ **alors**
Pour i **de** 1 **à** $\deg(I)$ tel que $i \neq s+1$ **Faire**
$P_{i,j} := P_{i,j} - \alpha\, \lambda_i$
Retourner P

On peut donc maintenant décrire explicitement l'algorithme FGLM.

Algorithme **FGLM Matriciel**

Entrée : $<$ un ordre, $M^{(k)}$ les matrices de multiplications, φ forme normale
Sortie : base de Gröbner réduite pour l'ordre $<$ de $\ker(\varphi)$.
$S := [1]$ // l'escalier pour le nouvel ordre $<$.
$V := [w_1]$ // $V = \mathrm{NF}(S)$
$L := [(i,1), i = 1,\dots,(n-1)]$ // liste de paires (k,l) correspondant à $X_i \cdot S_l$
$G := [\,], t := (n,1)$
$P := I_{\deg(I)}$ matrice de passage entre la nouvelle base S et $\mathcal{E}(G)$
Répéter
$s := \#S$ le nombre d'éléments de S.
$t = (k,l)$: on calcule $v = M^{(k)} \cdot V_l$ puis $\lambda = P \cdot v$
si $\lambda_{s+1} = \cdots = \lambda_{\deg(I)} = 0$ **alors**
$G := G \cup \left[X_k S_l - \sum_{i=1}^{s} \lambda_i \cdot S_i \right]$
sinon
$P :=$MISE À JOUR(s, λ, P)
$S := S \cup [X_k S_l]$ et $V := V \cup [v]$
$L := \mathrm{Sort}(L \cup [(i,s) \mid i = 1,\dots,n], <)$
Éliminer de L les doublons et les multiples de $\mathrm{LM}(G)$
Si $L = \varnothing$ alors
Retourner G
$t := \mathrm{first}(L)$ et supprime t de L.

1.6. Exemple pas à pas

On se place dans $\mathbb{Q}[X_1, X_2]$ et soit $G_{<_{\mathsf{DRL}}} = \left[X_1^2 - 3\,X_2 - X_1 + 1, X_2^2 - 2\,X_1 + X_2 - 1\right]$ qui est une base de Gröbner pour l'ordre DRL avec $X_2 > X_1$. On chercher à calculer la base pour l'ordre lexicographique avec $X_2 > X_1$

$$\mathcal{E}(G) = \{w_1 = 1, w_2 = X_1, w_3 = X_2, w_4 = X_1\,X_2\}\,.$$

On obtient les matrices de multiplication par X_1 et par X_2 :

$M^{(1)} =$

	$X_1\,w_1$	$X_1\,w_2$	$X_1\,w_3$	$X_1\,w_4$
w_1	0	-1	0	3
w_2	1	1	0	6
w_3	0	3	0	-4
w_4	0	0	1	1

, $M^{(2)} =$

	$X_2\,w_1$	$X_2\,w_2$	$X_2\,w_3$	$X_2\,w_4$
w_1	0	0	1	-2
w_2	0	0	2	3
w_3	1	0	-1	6
w_4	0	1	0	-1

On commence par $L := [(2,1)], S := [1], V := [w_1], G := [\,]$ et $t := (1,1)$ correspondant au monôme $1 \cdot S_1 = 1, P := I_4$

1) On calcule $v := M^{(1)} \cdot V_1 = M^{(1)} \cdot 1 = w_2$, puis $\lambda = P \cdot v = w_2$
comme $\lambda_2 \neq 0$, $S := [1, X_1]$, $V := [w_1, w_2]$ et la matrice P reste inchangée, puis $L := [(1,2),(2,1),(2,2)]$.
2) $t = (1,2)$. On calcule $v := M^{(1)} \cdot V_2 = M^{(1)} \cdot w_2 =^T [-1,1,3,0]$, puis $\lambda = P \cdot v =^T [-1,1,3,0]$
comme $\lambda_3 \neq 0$, $S := [1, X_1, X_1^2]$, $V := [w_1, w_2,^T [-1,1,3,0]]$, puis $P := \begin{bmatrix} 1 & 0 & 1/3 & 0 \\ 0 & 1 & -1/3 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $L := [(1,3),(2,1),(2,2),(2,3)]$.
3) $t = (1,3)$. On calcule $v := M^{(1)} \cdot V_3 = M^{(1)} .^T [-1,1,3,0] =^T [-1,0,3,3]$, puis $\lambda = P \cdot v =^T [0,-1,1,3]$
comme $\lambda_4 \neq 0$, $S := [1, X_1, X_1^2, X_1^3]$, $V := [w_1, w_2, V_3,^T [-1,0,3,3]]$, puis $P := \begin{bmatrix} 1 & 0 & 1/3 & 0 \\ 0 & 1 & -1/3 & 1/3 \\ 0 & 0 & 1/3 & -1/3 \\ 0 & 0 & 0 & 1/3 \end{bmatrix}$,
$L := [(1,4),(2,1),(2,2),(2,3),(2,4)]$.
4) $t = (1,4)$. On calcule $v := M^{(1)} \cdot V_4 = M^{(1)} .^T [-1,0,3,3] =^T [9,17,-12,6]$, puis $\lambda = P \cdot v =^T [5,23,-6,2]$
comme $\lambda_5 = 0$, $G := [X_1^4 - 2\,X_1^3 + 6\,X_1^2 - 23\,X_1 - 5]$, puis $L := [(2,1),(2,2),(2,3),(2,4)]$.
Étape 5 : $t = (X_2, 1)$. On calcule $v := M^{(2)} \cdot V_1 = M^{(2)} \cdot w_1 = w_3$, puis $\lambda = P \cdot w_3 =^T \left[\frac{1}{3}, \frac{-1}{3}, \frac{1}{3}, 0\right]$
comme $\lambda_5 = 0$, $G := [X_1^4 - 2\,X_1^3 + 6\,X_1^2 - 23\,X_1 - 5, X_2 - \frac{1}{3}X_1^2 + \frac{1}{3}X_1 - \frac{1}{3}]$, puis en éliminant les multiples de $\mathrm{LM}(G_2) = X_2$, on obtient $L := []$ et l'algorithme FGLM se termine.

1.7. Preuve de l'algorithme

Théorème 1.108. *Les algorithmes* **FGLM** *et* **FGLM Matriciel** *se terminent et calculent une base de Gröbner. Le nombre d'opérations dans* $\mathbb{Q}$ *de l'algorithme* **FGLM Matriciel** *est borné par* $O(n \deg(I)^3)$.

Preuve. On établit la preuve de l'algorithme **FGLM Matriciel**, la preuve de l'algorithme non matriciel étant similaire.

L'entrée de l'algorithme étant la forme normale φ, on note I le noyau de cette forme normale ; par hypothèse, I est un idéal et soient $G' = [g'_1, g'_2, \ldots]$ la base de Gröbner réduite de I pour l'ordre $<$ (on suppose que $\mathrm{LM}_<(g'_1) < \mathrm{LM}_<(g'_2) < \cdots$) et $\mathcal{E}_<(G') = \{w'_1 = 1 < w'_2 < \cdots < w'_D\}$ l'escalier de G' pour l'ordre $<$ avec $D = \deg(I)$.

On note $G_i = [g_1, g_2, \ldots, g_i]$ (respectivement S_i) la valeur de la variable G (respectivement S) lorsqu'on ajoute g_i dans G (respectivement lorsque $S := S \cup [X_k S_l]$) dans l'algorithme **FGLM Matriciel**. Pour tout i, tous les éléments de G_i sont dans l'idéal I : en effet lorsque l'on rajoute le polynôme $p = X_k S_l - \sum_{i=1}^{\#S} \lambda_i \cdot S_i$, on a, par construction, $\varphi(p) = 0$ et donc $p \in I = \ker(\varphi)$. De plus, il est clair que les éléments de S_i sont linéairement indépendants modulo I : comme l'espace vectoriel $\mathbb{Q}[X_1, \ldots, X_n]/I$ est de dimension finie, cela implique la terminaison de l'algorithme. Soit s le nombre d'éléments de $G = G_s$ lorsque l'algorithme se termine.

Supposons que $\mathcal{E}_<(G') \neq S_s$, on note $i := \min\{j \mid S_j \neq \{w'_1, \ldots, w'_i\}\}$ (ce nombre existe car $S_1 = \{1\} = \{w'_1\}$ donc $i > 1$). On note $S_i = \{w_1 = 1 < w_2 < \cdots < w_i\}$; par hypothèse on a $w_i \neq w'_i$. Il y a deux cas :

1. $w_i > w'_i$: pour tout X_j divisant w'_i, on sait que $\frac{w'_i}{X_j} \in \mathcal{E}_<(G')$, donc il existe $k_j < i$ tel que $\frac{w'_i}{X_j} = w'_{k_j} = w_{k_j}$. On a donc traité le monôme $t = w_{k_j}$ dans une étape précédente et on a ajouté dans L tous les multiples $X_l w_{k_j}$, donc en particulier w'_i. Comme $[\varphi(w'_1), \ldots, \varphi(w'_i)]$ sont linéairement indépendants et que $w'_i < w_i$, on a donc ajouté w_i dans S. Cela est absurde.
2. $w_i < w'_i$: on a $w_i \notin \mathcal{E}_<(G')$ et donc $[\varphi(w'_1), \ldots, \varphi(w'_{i-1}), \varphi(w_i)]$ ne sont pas linéairement indépendants. Donc, dans l'algorithme FGLM, lorsque l'on traite le monôme w_i, on trouve une combinaison linéaire $\varphi(w_i) = \lambda_1 \varphi(w'_1) + \cdots + \lambda_{i-1} \varphi(w'_{i-1})$ et l'on ajoute le polynôme $g = w_i - \lambda_1 w'_1 - \cdots - \lambda_{i-1} w'_{i-1}$ dans G et w_i n'est jamais dans S.

Comme dans les deux cas, on obtient une contradiction, alors on a $\mathcal{E}_<(G') = S_s$. Maintenant, pour tout polynôme $g \in G'$ (unitaire) et pour tout j tel que $X_j | \mathrm{LM}(g)$, on sait que $\frac{\mathrm{LM}(g)}{X_j} \in \mathcal{E}_<(G')$ donc il existe k_j tel que $\frac{\mathrm{LM}(g)}{X_j} = w'_{k_j}$ et donc a ajouté $X_j w'_{k_j} = \mathrm{LM}(g)$ dans L. De plus, pour tout $t \in T(g - \mathrm{LM}(g))$, on a $t \in \mathcal{E}_<(G')$ et donc $t = w_{j_t}$ pour un certain j_t. En notant $l = \max\{k_j\}$, on a donc $j_t < l$ et $\{w'_1, \ldots, w'_l\}$ sont linéairement indépendants. Or, $\{\mathrm{LM}(g)\} \cup \{w'_1, \ldots, w'_l\}$ sont linéairement dépendants : l'algorithme FGLM trouve la relation de dépendance linéaire $\varphi(\mathrm{LM}(g)) = \lambda_1 \varphi(w'_1) + \cdots + \lambda_l \varphi(w'_l)$ et ajoute à G le polynôme $\mathrm{LM}(g) - \lambda_1 w'_1 - \cdots - \lambda_{i-1} w'_{i-1} = g$. Par conséquent, $G_s = G'$.

Il est clair que la complexité de l'algorithme **Mise à Jour** est bornée par $O(n \deg(I)^2)$. De plus, dans l'algorithme principal FGLM, on augmente L seulement lorsque l'on détecte un vecteur linéairement indépendant. Par conséquent, la taille de L et le nombre d'itérations de l'algorithme sont bornés par $n\,D$. Les autres opérations arithmétiques sont des produits $M \cdot v$ dont la complexité est bornée par $O(D^2)$. Par conséquent, la complexité globale est $O\left(n\,D^3\right)$.

■

Première partie
SOLUTIONS DES TESTS

Chapitre 1

1.1. C'est immédiat puisque pour tout $f \in A$, la multiplication de f par 0, qui donne 0, est dans I.

1.2. Si $I = A$, $1 \in I$ puisque $1 \in A$. Montrons maintenant la réciproque. Puisque $1 \in I$ et que I est un idéal, on a pour tout $f \in A$, $1.f \in I$ et $1.f = f$.

1.3. Il suffit de montrer que pour tout (f, g) dans $I \cap J$ et tout $h \in A$, $f + g \in I \cap J$ et $hf \in I \cap J$. Puisque (f, g) est un couple d'éléments de $I \cap J$, c'est un couple d'éléments de I et de J. Puisque I et J sont des idéaux, $f + g$ est un élément de I et de J et donc c'est un élément de $I \cap J$. De même, puisque I et J sont des idéaux, hf est un élément de I et de J et donc c'est un élément de $I \cap J$.

1.4. Soient f et g deux éléments de $I + J$. Donc il existe (p_1, p_2) dans I et (q_1, q_2) dans J tels que $f = p_1 + q_1$ et $g = p_2 + q_2$. Ainsi $f + g = (p_1 + p_2) + (q_1 + q_2)$. Puisque I et J sont des idéaux, $p_1 + p_2 \in I$ et $q_1 + q_2 \in J$, si bien que $f + g \in I + J$. Considérons maintenant $h \in A$. On a $hf = hp_1 + hq_1$. Comme I et J sont des idéaux, $hp_1 \in I$ et $hq_1 \in J$ si bien que $hf \in I + J$.

1.5. On a vu précédemment que $0 \in I$. Considérons $f \in I$. Ainsi $f - 0 = f \in I$. Donc tous les polynômes de I appartiennent à la classe d'équivalence de I. L'inclusion inverse est immédiate.

1.6. C'est une conséquence du test précédent. Puisque 1 est dans I, il est dans la classe d'équivalence de 0. Donc 0 et 1 ont même classe d'équivalence. Par ailleurs, puisque $1 \in I$, $I = \mathbb{Q}[X_1, \ldots, X_n]$. Donc tous les polynômes de $\mathbb{Q}[X_1, \ldots, X_n]$ appartiennent à la classe d'équivalence de 0, donc à celle de 1.

1.7. On a évidemment $f \sim_I f$ puisque $f - f = 0 \in I$. On a $f \sim_I g \Rightarrow g \sim_I f$ puisque $f - g \in I \Rightarrow g - f \in I$. Enfin, $f \sim_I g$ et $g \sim_I h$ impliquent $f \sim_I h$ puisque $f - g \in I$ et $g - h \in I$ impliquent $f - g + g - h = f - h \in I$.

1.8. En raisonnant comme dans l'exemple donné précédemment, on obtient que $\frac{\mathbb{Q}[X,Y]}{\langle X-1, Y-1\rangle}$ est un espace vectoriel de dimension 1 : la classe d'équivalence de 1 est celle de X (car $X - 1 \in I$) ainsi que celle de Y (car $Y - 1 \in I$).

Comme on vient de le voir, cet espace vectoriel est de dimension 1. La variété algébrique associée à l'idéal considéré est constituée du point de coordonnée $(1, 1)$ (il n'y a qu'une seule solution).

1.9. Le degré de $\langle X, Y\rangle$ est 1 puisque l'anneau-quotient $\frac{\mathbb{Q}[X,Y]}{\langle X,Y\rangle}$ est un espace vectoriel de dimension 1.

1.10. Le degré est 2 (ici l'anneau-quotient $\frac{\mathbb{Q}[X,Y]}{\langle X^2,Y\rangle}$ est de dimension 2).

1.11. La complexité est $(p + q)^3$ puisque la taille de la matrice de Sylvester est $p + q$.

1.12. On trouve $4\,a^2c - ab^2$ qui est un multiple du discriminant du trinôme $aX^2 + bX + c$.

1.13. En appliquant les formules corrélant les différences des racines des deux polynômes considérés au résultant (ou la formule $\mathrm{Res}(A, BC) = \mathrm{Res}(A, B)\mathrm{Res}(A, C)$), on trouve 12.

1.14. Il s'agit de calculs de suites des restes euclidiens faciles. Le résultat est -3.

1.15. On trouve 0.

1.16. Pour tout $a \in \frac{\mathbb{Z}}{p\mathbb{Z}}[X]$, on a $a^p = a$, si bien que le résultant recherché est 0. **1.17.** On obtient le résultant de ces deux polynômes, par rapport à la variable Y, de manière quasi immédiate en appliquant l'algorithme de calcul du résultant fondé sur la suite des restes euclidiens. On trouve $X^4 - X^2 + 1$. Ce résultant est la projection des solutions complexes du système étudié puisque les coefficients dominants (par rapport à la variable Y) des deux polynômes du système n'ont pas de PGCD de degré supérieur à 1. Ainsi, on obtient finalement la paramétrisation

$$\begin{aligned} Y &= 1/X \\ X^4 - X^2 + 1 &= 0. \end{aligned}$$

1.18.

1) Si $r = \text{RÉDUCTION}(p, F, <)$, alors d'après le corollaire 1.73 il existe deux suites finies $(g_i)_{i=1,\ldots,k}$ et $(m_i)_{i=1,\ldots,k}$ des monômes telles que $g_n \in F$ et $r - p = \sum_{i=1}^{k} m_i g_i$ avec $\mathrm{LM}(p) = \mathrm{LM}(m_1 g_1) > \mathrm{LM}(m_2 g_2) > \cdots > \mathrm{LM}(m_k g_k)$. Si $\lambda \in \mathbb{Q}$ et $\lambda \neq 0$, on a $\lambda r - \lambda p = \sum_{i=1}^{k} (m_i \lambda) g_i$ et on montre par récurrence que $\mathrm{LM}(\lambda m_i g_i) = \mathrm{LM}(m_i g_i)$; on déduit que $\varphi(\lambda p) = \lambda r = \lambda\, \varphi(p)$.
2) Si $\varphi(p) = 0$ alors d'après le corollaire 1.73, il existe deux suites finies $(g_i)_{i=1,\ldots,k}$ et $(m_i)_{i=1,\ldots,k}$ des monômes telles que $g_i \in F$ et $0 - p = \sum_{i=1}^{k} m_i g_i$ et, par suite, $p \in \langle F\rangle$.
3) On considère $F = [X, X + 1]$ et l'ordre lexicographique sur les monômes, alors 1 n'est pas réductible par F et donc $\varphi(1) = 1$. Pourtant $I = \langle F\rangle = \langle x, x + 1\rangle = \langle 1\rangle$. En général, on a inclusion stricte. Si F est une base de Gröbner, alors on a égalité.

1.19. On suppose les t_i deux à deux distincts ; supposons la propriété fausse soit $f = \min\{p \in \mathrm{Id}([t_1, \ldots, t_m]) \mid \varphi(p) \neq 0\}$. Il existe donc des polynômes (g_i) tels que $f = \sum_{i=1}^{m} g_i t_i$: pour tout i on peut écrire g_i sous la forme $g_i = g_i' + g_i'' + r_i$ tel que $\forall t \in T\left(g_i'\right)$. On a $g_i' t_i > \mathrm{LT}(f)$, $T\left(g_i'\right)\, g_i' t_i = \mathrm{LT}(f)$ et $r_i = g_i - g_i' - g_i''$, donc $r_i t_i > \mathrm{LT}(f)$. On en déduit $\sum_{i=1}^{m} g_i' t_i = 0$ et $\sum_{i=1}^{m} g_i'' t_i = \mathrm{LM}\,(f) = c\, g_1' t_1$ (en supposant que $g_1' \neq 0$, ce qui est toujours possible à renumérotation près). Comme $f = c\, g_1' t_1 + \sum_{i=1}^{m} r_i t_i$, le premier pas de l'algorithme RÉDUCTION est donc $f' := f - \frac{\mathrm{LM}(f)}{\mathrm{LM}(t_1)} t_1 = \sum_{i=1}^{m} r_i t_i$; comme $\varphi(f) = \varphi(f') \neq 0$, on a construit un $f' < f$, ce qui est absurde.

1.20. Soient $f = 2\,X^2Y + X^2$ et $g = 7\,XY^2 + 3X^2$. Pour l'ordre DRL, $\mathrm{Spol}(f, g) = 7Yf - 2Xg = -6X^3 + 7X^2Y$.
Pour l'ordre lexicographique, $\mathrm{Spol}(f, g) = 3f - 2Yg = 3X^2 - 14XY^3$.

1.21. Dans ce cas, $\mathrm{Spol}(f, g)$ est égal (à une constante près) à la réduction de f par g.

1.22. Pour l'ordre lexicographique, $\left[X - Y^2 + 1, Y^4 - 2Y^2 - Y + 1\right]$ une base de Gröbner de $\left[X^2 - Y, Y^2 - X - 1\right]$.
Pour l'ordre DRL, le système initial $[X\hat{}2 - Y, Y\hat{}2 - X - 1]$ est déjà une base de Gröbner. La forme normale de $X^4 - X - 1$ est nulle dans les deux cas. Ce polynôme est donc dans l'idéal.

1.23.

buchberger :=proc(F,ordre)

```
  local G,P,n,p,f,i,j:
  n:=nops(F):  G:=F:
  P:={seq(seq([F[i],F[j]],j=(i+1)..n),i=1..n)}:
  while nops(P)>0 do
    p:=op(1,P):  P:=P minus {p}:
    f:=spol(p[1],p[2],ordre):
    f:=ReductionTotale(f,G,ordre):
    if (f<>0) then
      G:=[op(G),f]:  n:=n+1:
      P:=P union {seq([G[i],f],i=1..(n-1))}:
    fi:
  od:
  G:
end:
ReductionTotale:=proc(f0,F,ordre)
  local q,f:
  f:=f0:
  while (f<>0) do
    q:=topReduction(f,F,ordre):
    if (q=f) then RETURN(f): else f:=q: fi:
  od:
  f:
end:
topReduction:=proc(f,F,ordre)
  local m1,i,m2,u:
  m1:=ordre(f):
  for i from 1 to nops(F) do
    m2:=ordre(F[i]): u:=m1/m2:
    if (type(u,polynom)) then
      RETURN(expand(f-u*F[i])):
    fi:
  od:
  f:
end:
spol:=proc(p1,p2,ordre)
  local m1,m2,m:
  m1:=ordre(p1):
  m2:=ordre(p2):
  m:=lcm(m1,m2):
  expand((m/m1)*p1-(m/m2)*p2):
end:
# retourne le terme de tete pour l'ordre lexicographique
# les variables sont dans la variable globale vars
lexico:=proc(p)
  global vars:
  if (type(p,`+`)) then
    op(1,sort(p,vars,plex)):
  else
    p:
  fi:
end:
```

Voici un exemple d'utilisation de la procédure :

```
vars:=[x,y,z]:
G:=buchberger([x^2*y-1,x*y^2-3],lexico);
```

1.24. Si l'on pouvait trouver $g \in G_1$ tel que $\mathrm{LM}(g) \notin \mathrm{LM}(G_2)$, alors $g \in Id(G_1) = Id(G) = Id(G_2)$, donc il existe $g_2 \in G_2$ tel que $\mathrm{LM}(g_2)$ divise $\mathrm{LM}(g)$. De même, il existe $g_1 \in G_1$ tel que $\mathrm{LM}(g_1)$ divise $\mathrm{LM}(g_2)$. Si l'on avait $g = g_1$, alors $\mathrm{LM}(g_2) = \mathrm{LM}(g) = \mathrm{LM}(g_1)$, ce qui est absurde car $\mathrm{LM}(g) \notin \mathrm{LM}(G_2)$, donc $g \neq g_1$. Mais alors on a trouvé $g_1 \in G \backslash \{g\}$ tel que $\mathrm{LM}(g_1)$ divise $\mathrm{LM}(g)$, ce qui est contraire à la minimalité de G_1.

1.25. Comme $\mathrm{Spol}\,(t_i, t_j) = 0$, cela résulte du corollaire 1.90.

1.26.

1) La base pour l'ordre lexicographique est $\left[2t - 2x + y + 2, 4x^2 - 4xy - 8x + y^2 + 2y\right]$.
2) Par application du théorème 1.92 d'élimination, l'équation implicite est $f\,(x, y) = 4x^2 - 4xy - 8x + y^2 + 2y$.

Deuxième partie
SOLUTIONS DES EXERCICES

Chapitre 1

1.1.

1) Il s'agit simplement de la matrice de Sylvester.
2) Dire que P et Q ont un facteur commun G est équivaut à dire qu'il existe des polynômes P_1 et Q_1 de degrés positifs tels que $P = P_1 G$ et $Q = Q_1 G$, ce qui est équivalent à dire que $-Q_1 P + Q P_1 = 0$. On remarque alors que le couple (Q_1, P_1) vit dans $k[X]_{<n} \times k[X]_{<m}$.
3) D'après la construction ci-dessus, en choisissant $G = D$, on trouve que U_D est de degré $\deg(Q) - d$ et V_D est de degré $\deg(P) - d$ avec $U_D P = -V_D Q$.
4) On a donc $U_D P = -V_D Q$. Ainsi pour tout $0 \leq i \leq d-1$, on a $X^i U_D P = -X^i V_D Q$, ce qui nous permet de construire la base $(U_D, V_D), (XU_D, XV_D), \ldots, (X^{d-1}U_D, X^{d-1}V_D)$. En appliquant la relation $\dim(\mathrm{Im}(\phi_{P,Q})) + \dim(\mathrm{Ker}(\phi_{P,Q})) = p + q$, on trouve que le rang de la matrice de Sylvester est $p + q - d$.
5) Si P et Q sont premiers entre eux, $\phi_{P,Q}$ est injective. Ainsi il existe un unique couple (U, V) dans $k[X]_{<n} \times k[X]_{<m}$ tel que $UP + VQ = 1$. On retrouve la relation de Bézout.

1.2.

1) On trouve 31 pour le premier couple et 0 pour le second.
2) On laisse les détails techniques au lecteur, la question étant une application directe du cours. En effectuant la réduction par pivot de Gauss, on constatera que les coefficients des polynômes de la suite des restes euclidiens des couples considérés apparaissent dans la matrice.
3) On utilise ici le résultant pour calculer la projection (l'élimination d'une variable permettant d'obtenir une telle projection). Il suffit ici d'éliminer z du système d'équation $x^2 - y^2 - z^2 + 1 = 0$ et $2x + 2y - z = 0$ (ou plus précisément de calculer l'intersection de l'idéal engendré par ces deux polynômes avec $\mathbb{Q}[x, y]$). Puisque les coefficients dominants en z de ces deux polynômes ont un PGCD égal à 1, un calcul de résultant suffit à calculer cette intersection. On trouve alors $-3\,x^2 - 5\,y^2 + 1 - 8\,xy$.

1.3.

1) On peut supposer g_1 et g_2 unitaires.
On a $\mathrm{ppcm}(g_1, g_2) = \mathrm{LM}(g_1)\,\mathrm{LM}(g_2)$ et donc
$$\mathrm{Spol}(g_1, g_2) = \mathrm{LM}(g_2) g_1 - \mathrm{LM}(g_1) g_2 = -r_2 g_1 + r_1 g_2$$
où $r_i = g_i - \mathrm{LM}(g_i)$ pour $i \in \{1, 2\}$. Comme $\mathrm{LM}(r_i) < \mathrm{LM}(g_i)$, on a
$$\begin{aligned}\mathrm{Spol}(g_1, g_2) &= \mathcal{O}_{g_1,g_2}(\max(r_1\,\mathrm{LM}(g_1), r_2\,\mathrm{LM}(g_2))) = o_{g_1,g_2}(\mathrm{LM}(g_1)\,\mathrm{LM}(g_2)) \\ &= o_{g_1,g_2}(\mathrm{ppcm}(g_1, g_2)).\end{aligned}$$
2) F est une base de Gröbner donc RÉDUCTION$(\mathrm{Spol}\,(g_1, g_2)\ , F) = 0$.
3) Pour la généraliser à k polynômes $[g_1, \ldots, g_k]$, il faut $\mathrm{ppcm}(g_i, g_j) = \mathrm{LM}(g_i)\,\mathrm{LM}(g_j)$ pour tout $i \neq j$. Dans ce cas, $[g_1, \ldots, g_k]$ est une base de Gröbner.
4) On peut éliminer de la liste des paires critiques P toutes les $(f, g) \in P$ telles que $\mathrm{ppcm}(f, g) = \mathrm{LM}(f)\,\mathrm{LM}(g)$.

1.4.

1) Il suffit de vérifier la définition d'un idéal : par exemple si $(f, g) \in (I \cap J)^2$, on a $f + g \in I$ et $f + g \in J$ et donc $f + g \in I \cap J$.
2) Il est facile de vérifier que $(t \cdot I + (1-t) \cdot J)$ est un idéal dans $\mathbb{Q}[X_1, \ldots, X_n, t]$.

   2)) On montre d'abord $I \cap \mathcal{J} \subset (t \cdot \mathcal{I} + (1-t) \cdot J) \cap \mathbb{Q}[X_1, \ldots, X_n]$.
   Soit $f \in I \cap J$. Comme $f \in I$, on a $t\,f \in t \cdot I$ et de même $(1-t)\,f \in (1-t) \cdot J$. Par suite, $f = (t\,f + (1-t)\,f) \in t \cdot I + (1-t) \cdot J$. Comme $I, J \subset \mathbb{Q}[X_1, \ldots, X_n]$, on a $f \in \mathbb{Q}[X_1, \ldots, X_n]$ et donc $f \in (t \cdot I + (1-t) \cdot J) \cap \mathbb{Q}[X_1, \ldots, X_n]$.

   2)) Réciproquement, si $f \in (t \cdot I + (1-t) \cdot J) \cap \mathbb{Q}[X_1, \ldots, X_n]$, on a $f(x) = t\,g(x,t) + (1-t)h(x,t)$, où $t\,g(x,t) \in t\,I$ et $(1-t)h(x,t) \in (1-t)J$.
   - on fait $t = 0$ dans cette expression : $f(x) = 0 + h(x, 0) \in J$;
   - on fait $t = 1$ dans cette expression : $f(x) = g(x, 1) + 0 \in I$
     on en déduit $f \in I \cap J$.

3) Soient $F = [f_1, \ldots, f_s]$ et $H = [h_1, \ldots, h_m]$.

   3)) On introduit une nouvelle variable t et l'on considère l'ordre lexicographique $t > X_1 > \cdots > X_n$.

   3)) On calcule une base de Gröbner G pour cet ordre de $[t\,f_1, \ldots, t\,f_s, (1-t)h_1, \ldots, (1-t)\,h_m]$.

   3)) Soit G' :=les éléments de G qui ne dépendent pas de t

   3)) G' est une base de Gröbner (pour l'ordre lexicographique $X_1 > \cdots > X_n$) de $I \cap J$.

4) On suppose que $I \cap \langle f \rangle = \langle g_1, \ldots, g_s \rangle$.

   (a) Si $g \in \langle \frac{g_1}{f}, \ldots, \frac{g_s}{f} \rangle$, alors $g = \sum_{i=1}^{s} h_i \frac{g_i}{f}$ pour certains polynômes h_i, alors $f\,g = \sum_{i=1}^{s} h_i g_i \in \langle g_1, \ldots, g_s \rangle \subset I$ et donc $g \in I : f$.

   (b) Si $g \in I : f$, alors $f\,g \in I$. Comme $f\,g \in \langle f \rangle$, on a $fg \in I \cap \langle f \rangle = \langle g_1, \ldots, g_s \rangle$ et $f\,g = \sum_{i=1}^{s} h_i g_i$ pour $h_i \in \mathbb{Q}[X_1, \ldots, X_n]$.
   Comme $g_i \in \langle f \rangle$, on sait que f divise g_i et on a donc $g = \sum_{i=1}^{s} h_i \frac{g_i}{f}$.
   On a donc $\langle \frac{g_1}{f}, \ldots, \frac{g_s}{f} \rangle = I : f$.
   Pour calculer une base de l'idéal $\langle f_1, \ldots, f_m \rangle : f$, on applique l'algorithme suivant :
   - calculer une base de Gröbner G de $[tf_1, \ldots, tf_m, (1-t)\,f]$ pour l'ordre lexicographique $t > X_1 > \cdots > X_n$;
   - soit G' :=les éléments de G qui ne dépendent pas de t ;
   - alors $[\frac{g}{f} \mid g \in G']$ est une base de $I : f$.

Index