Bases de Gröbner

Antoine BOIVIN

19 juin 2024

Introduction

La notion de base de Gröbner d'un idéal d'un anneau de polynômes a été introduite de manière indépendante par Heisuke Hironaka (qu'il nomma "bases standard") et un peu plus tard par Bruno Buchberger (qu'il nomma "Bases de Gröbner" en l'honneur de son directeur de thèse Wolgang Gröbner).
Une base de Gröbner d'un idéal est une famille de "bons" générateurs de cet idéal afin de décrire plus facilement celui-ci.
Dans ce mémoire, nous allons, à travers l'étude des bases de Gröbner, traiter les quatre problèmes suivants :

1. La description d'un idéal : Peut-on trouver une famille génératrice préférée pour chaque idéal $I \subset k[X_1, \dots, X_n]$?
2. L'appartenance à un idéal : Soit $f \in k[X_1, \dots, X_n]$ et un idéal $I := \langle f_1, \dots, f_s \rangle$. Comment montrer que $f \in I$?
3. La résolution de systèmes polynomiaux : Trouver les zéros communs dans k^n d'une famille de polynômes.
4. Le problème d'implicitation : Soit V le sous-ensemble de k^n paramétré par : $x_i = g_i(t_1, \dots, t_n), 1 \leq i \leq n$ où les g_i sont des polynômes ou des fractions rationelles. Peut-on trouver des équations polynomiales en X_i décrivant V ?

En premier lieu, nous allons introduire la notion de base de Gröbner et répondre aux problèmes 1 et 2 grâce, notamment, à un algorithme de division généralisant l'algorithme d'Euclide pour les polynômes à une indéterminée. Nous allons ensuite discuter de l'élimination des variables dans les systèmes polynomiaux (afin de résoudre le problème 3) et de sa géométrie. Pour finir, nous allons utiliser ses résultats pour trouver les équations décrivant un ensemble dont on a la paramétrisation.

Conventions et Notations

Dans ce rapport, k est un corps commutatif de caractéristique 0 et n un entier naturel strictement positif.
On considérera l'anneau de polynômes $k[X_1, \dots, X_n]$ à n indéterminées $X_1, \dots, X_n$ construit par récurrence comme suit : $\forall p < n, k[X_1, \dots, X_{p+1}] := k[X_1, \dots, X_p][X_{p+1}]$. On pourra identifier cet anneau à celui des fonctions polynômiales à n variables (grâce à l'infinité de k).
On appelle monôme tout polynôme de la forme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ où $\alpha_i \in \mathbb{N}$ que l'on abrégera $X^{(\alpha_1, \dots, \alpha_n)}$. On notera $\mathscr{M}$ l'ensemble des monômes. Pour tout $p \in \mathbb{N}$ et pour tout anneau commutatif A, on notera $A[X]_{\leq p}$ (resp. $A[X]_{<p}$) l'ensemble des polynômes de degré supérieur ou égal (resp strictement supérieur) à p.
On appelera base d'un idéal I une famille $F = (f_1, \dots, f_s)$ telle que $I = \langle F \rangle$.

1 Description des idéaux de $k[X_1, \ldots, X_n]$

1.1 Exemple introductif

On va commencer par traiter le cas simple de l'anneau des polynômes à un indéterminée $k[X]$. $k[X]$ est un anneau euclidien et donc principal. De ce fait, on a un description simple des idéaux de $k[X]$ qui sont tous engendrés par un unique élément. De plus, grâce à l'algorithme d'Euclide, on peut aisément vérifier l'appartenance d'un polynôme à un idéal de $k[X]$.
Soient $I = \langle P \rangle \subset k[X]$ et $f \in k[X]$. En effectuant la division euclidienne de f par P, on a : $f = PQ + R$ où $\deg(R) < \deg(P)$. On a alors la caractérisation suivante : $f \in I \Leftrightarrow R = 0$. Ce qui règle les problèmes 1 et 2 de l'introduction pour $k[X]$.

1.2 $k[X_1, \ldots, X_n]$ est noethérien

Contrairement au cas à une indéterminée, lorsque $n > 1$, $k[X_1, \ldots, X_n]$ n'est plus euclidien et même plus principal (il est, tout de même, factoriel). Nous allons montrer ce résultat et afin de décrire ses idéaux, définir la notion plus faible d'anneau noethérien qui convient mieux à $k[X_1, \ldots, X_n]$

Théorème 1.1. *$k[X_1, \ldots, X_n]$ n'est pas principal pour $n > 1$.*

Démonstration. Supposons, par l'absurde, que $k[X_1, \ldots, X_n]$ est principal et considérons l'idéal $\langle X_1, \ldots, X_n \rangle$ qui serait donc engendré par un polynôme P non nul. On a alors : $\deg_{X_i}(P) \leq \deg_{X_i}(X_j) = 0$ pour $i \neq j$ et donc $\deg_{X_i}(P) = 0$ pour tout $1 \leq i \leq n$. On en déduit que P est un polynôme constant non nul. Comme $P \in \langle X_1, \ldots, X_n \rangle$ alors $P(0, \ldots, 0) = 0$, d'où une contradiction. □

Définition 1.2. Soit A un anneau commutatif. On dit que A est un anneau noethérien si tout idéal I de A est engendré par un nombre fini d'éléments.

Dans la suite, on aura aussi besoin d'une autre caractérisation des anneaux noethériens

Proposition 1.3. *Une suite croissante d'idéaux d'un anneau noethérien est stationnaire.*

Exemple 1.4. Tout anneau principal est noethérien car chaque idéal d'un anneau principal A est de la forme aA où $a \in A$. En particulier, tout corps est noethérien (les idéaux d'un corps sont $\{0\}$ et lui-même).

Maintenant que nous avons la définition d'anneau noethérien, nous allons montrer que $k[X_1, \ldots, X_n]$ est noethérien grâce au théorème de transfert suivant :

Théorème 1.5 (de la base de Hilbert)**.** *Soit A un anneau noethérien. Alors $A[X]$ est aussi un anneau noethérien.*

Démonstration. Soient I un idéal de $A[X]$. Soit J l'idéal engendré par les coefficients dominants des polynômes de $A[X]$ et pour tout $d \in \mathbb{N}$, J_d l'idéal engendré par les coefficients dominants des polynômes de I de degré d.
Comme A est noethérien alors il existe $x_1, \ldots, x_r \in I$,tels que $J = \langle x_1, \ldots, x_r \rangle$ et pour tout $d \in \mathbb{N}, y_{1,d}, \ldots, y_{m_d,d}$ tels que $J_d = \langle y_{1,d}, \ldots, y_{m_d,d} \rangle$.
Il existe donc des polynômes $Q_1, \ldots, Q_r$ de I ayant pour coefficient dominant x_i et pour tout $d \in \mathbb{N}$, il existe des polynômes $R_{1,d}, \ldots R_{m_d,d} \in I \cap A[X]_{\leq d}$ dont le coefficient en X^d est, respectivement, $y_{1,d}, \ldots, y_{m_d,d}$.
Montrons que $I = \langle Q_1, \ldots, Q_r, R_{1,1}, \ldots, R_{m_1,1}, \ldots, R_{1,N}, \ldots, R_{m_N,N} \rangle$ où $N := \max_i \deg(Q_i)$.
Notons I' cet idéal (inclus dans I car engendré par des éléments de I).
Pour montrer l'inclusion réciproque, il suffit de montrer que, pour tout $d \in \mathbb{N}$, $I \cap A[X]_{<d} \subset I'$. Montrons donc,par récurrence, que la propriété $\forall P \in I, \deg(P) < d \Rightarrow P \in I'$ est vraie pour tout $d \in \mathbb{N}$.
Initialisation : Si $d = 0$, $I \cap A[X]_{<0} = \{0\} \subset I'$ (car 0 est le seul polynôme de degré strictement négatif et 0 est dans tout idéal de $A[X]$)
Hérédité : Soit $d \in \mathbb{N}$ et supposons que tout polynôme de I de degré strictement inférieur à d appartient à I'.
Soit $P := \sum_{k=0}^{d} a_k X^k \in I, a_d \neq 0$.

- Si $d \leq N - 1$ alors $a_d \in J_d$, il existe donc $\lambda_1, \ldots, \lambda_{m_d}$ tel que $a_d = \sum_{k=1}^{m_d} \lambda_k y_{k,d}$. On en déduit que $T := P - \sum_{k=1}^{m_d} \lambda_k R_{k,d}$ est de degré strictement inférieur à d. Comme P et les $R_{k,d}$ sont dans I alors T aussi et par hypothèse de récurrence, $T \in I'$. Comme les $R_{k,d}$ sont aussi dans I' alors $P = T + \sum_{k=1}^{m_d} \lambda_k R_{k,d}$ est dans I'.

— Si $d \geq N$, alors $a_d \in J$,il existe donc $\lambda_1, \ldots, \lambda_r \in A$ tel que $a = \sum_{k=1}^{r} \lambda_k x_k$ et donc $P - \sum_{k=1}^{m} \lambda_i X^{d-deg(Q_i)} Q_i$ est de degré strictement inférieur à d. On en déduit de la même façon que dans le cas précédent que $P \in I'$.

Conclusion : D'après le principe de récurrence, pour tout $d \in \mathbb{N}$, $I \cap A[X]_{<d} \subset I'$.
On en déduit que $I \subset I'$ et donc $I = I'$. Ce qui nous permet de conclure que I est engendré par un nombre fini d'éléments.
Ce qui montre que $A[X]$ est donc noethérien. □

Corollaire 1.6. *$k[X_1, \ldots, X_n]$ est un anneau noethérien.*

Ce qui clôt le problème 1 de l'introduction : la description des idéaux de $k[X_1, \ldots, X_n]$

2 Algorithme de division

Nous avons rappelé, dans la première section, que l'on a la caractérisation suivante dans $k[X]$: pour tout idéal $I := \langle P \rangle$ et pour tout $f \in k[X]$, on peut écrire f sous la forme $QP + R$ (grâce à l'algorithme d'Euclide) où $\deg R < \deg P$ et $f \in I \Leftrightarrow R = 0$.

Pour le cas général, pour montrer que le polynôme f de $k[X_1, \ldots, X_n]$ appartient à un idéal $I := \langle f_1, \ldots, f_s \rangle$, nous allons décrire un algorithme permettant d'écrire f sous la forme $\sum g_i f_i + r$. Avant cela,en analogie à l'algorithme en une indéterminée, il nous faut définir un ordre, afin qu'à chaque étape, on puisse dire que le "terme dominant" du reste est strictement inférieur à celui d'avant (celui sur $k[X]$ est $X^n \geq X^m \Leftrightarrow n \geq m$). Cet ordre doit être, de plus, un bon ordre pour ne pas avoir de suites infinies strictement décroissantes et donc pour que l'algorithme finisse.

2.1 Ordres monomiaux

2.1.1 Définitions

Définition 2.1. Un ordre monomial est une relation d'ordre total $\geq$ de $\mathscr{M}$ telle que :

1. $\forall \alpha, \beta, \gamma \in \mathbb{N}^n, X^\alpha \geq X^\beta \Rightarrow X^{\alpha+\gamma} \geq X^{\beta+\gamma}$(compatibilité avec le produit)
2. $\geq$ est un bon ordre

On peut remarquer que l'ordre induit par le degré dans $k[X]$ est un ordre monomial.
On peut ensuite définir quelques termes associés à un ordre sur les polynômes.

Définition 2.2. Soit $P := \sum_\alpha p_\alpha X^\alpha \in k[X_1, \ldots, X_n]$ et $\geq$ un ordre monomial.

1. Le monôme dominant de P est : $\mathrm{LM}(P) := \max\{X^\alpha \in \mathscr{M} | p_\alpha \neq 0\}$
2. Le multidegré de P est l'élément de $\mathbb{N}^n$, noté multideg(P), tel que $X^{\mathrm{multideg}(P)} = LM(P)$
3. Le coefficient dominant de P est $\mathrm{LC}(P) := p_{\mathrm{multideg}(P)}$
4. Le terme dominant de P est $\mathrm{LT}(P) := \mathrm{LC}(P) \cdot \mathrm{LM}(P)$

2.1.2 Exemples d'ordres monomiaux

Nous allons maintenant donner quelques exemples d'ordres monomiaux et en premier lieu, l'ordre lexicographique que nous allons utiliser pour l'élimination.

Définition 2.3 (Ordre lexicographique $\geq_{lex}$)**.** Soient $\alpha, \beta \in \mathbb{N}^n$ alors $X^\alpha \geq_{lex} X^\beta$ si, et seulement si, $\alpha = \beta$ ou le premier coefficient non nul en lisant par la gauche de $\alpha - \beta$ est positif.

Proposition 2.4. *$\geq_{lex}$ est un ordre monomial.*

Démonstration. Montrons, par l'absurde, que $\geq_{lex}$ est un bon ordre.
Supposons donc que $\geq_{lex}$ n'est pas un bon ordre et donc qu'il existe une suite $u := \left(X^{(a_{1,i} \ldots, a_{n,i})}\right)_{i \in \mathbb{N}}$ strictement décroissante.
On en déduit que la suite $(a_{1,i})_{i \in \mathbb{N}}$ est décroissante (sinon u ne serait pas décroissante) et est donc stationnaire car $\mathbb{N}$ est bien ordonné. Alors il existe $N_1 \in \mathbb{N}$ tel que $\forall p \geq N, u_{1,p} = u_{1,N_1}$. Considérons maintenant la suite $(a_{2,i})_{i \geq N_1}$. Elle est décroissante et donc stationnaire,et ainsi de suite...

On construit, de cette façon, une suite $(N_i)_{i\geq 1}$ telle que : $\forall i \in \mathbb{N}^*, \forall n \geq N_i, u_{i,n} = u_{i,N_i}$.On en déduit que $\forall p \geq N_n, \forall i \in [\![1,n]\!], u_{i,p} = u_{i,N_n}$ ou encore $\forall p \geq N_n, X^{u_{1,p},\ldots,u_{n,p}} = X^{u_{1,N_n},\ldots,u_{n,N_n}}$, ce qui est contradictoire avec la stricte décroissance de u. □

Les deux ordres suivants comparent les degrés totaux des monômes.

Définition 2.5. Le degré total du monôme $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ est $|(\alpha_1, \ldots, \alpha_n)| := \sum_{i=1}^n \alpha_i$
Le degré d'un polynôme $f \in k[X_1, \ldots, X_n]$ est le maximum des degrés totaux des monômes le constituant.

Définition 2.6 (Ordre lexicographique gradué $\geq_{grlex}$)**.** Soient $\alpha, \beta \in \mathbb{N}^n$ alors $X^\alpha \geq_{grlex} X^\beta$ si, et seulement si, $|\alpha| > |\beta|$ ou ($|\alpha| = |\beta|$ et $\alpha \geq_{lex} \beta$).

Définition 2.7 (Ordre lexicographique gradué renversé $\geq_{grevlex}$)**.** Soient $\alpha, \beta \in \mathbb{N}^n$ alors $X^\alpha \geq_{grevlex} X^\beta$ si, et seulement si, $|\alpha| > |\beta|$ ou ($|\alpha| = |\beta|$ et le premier coefficient non nul en lisant par la droite de $\beta - \alpha$ est positif).

La différence entre ses deux ordres est dans la manière où ils départagent les égalités entre monômes de même degré total : le premier se base sur l'ordre lexicographique et le second sur un ordre lexicographique "renversé", dans le sens où il commence par la droite et regarde la première entrée négative de $\alpha - \beta$.

Exemple 2.8. On va comparer les polynômes $f = X^2Z^2$,$g = X^2Z$ et $h = XY^2Z$ de $k[X, Y, Z]$ avec ces trois différents ordres : $f >_{lex} g >_{lex} h$,$f >_{grlex} h >_{grlex} g$, $h >_{grevlex} f >_{grevlex} g$

2.2 Algorithme de division

Dans ce paragraphe, nous allons énoncer et démontrer l'algorithme de division.

Lemme 2.9. *Soit* $f, g \in k[X_1, \ldots, X_n]$ *tels que* $\mathrm{LT}(f) = \mathrm{LT}(g)$ *alors* $\mathrm{LM}(f - g) < \mathrm{LM}(f) = \mathrm{LM}(g)$

Démonstration. Soient $\alpha, \alpha_1, \ldots, \alpha_p \in \mathbb{N}^n, p \in k^*, p_i, q_i \in k$ tels que : $X^\alpha > X^{\alpha_1} > \ldots > X^{\alpha_p}$ et tels que $f = pX^\alpha + \sum p_{\alpha_i} X^{\alpha_i}$ et $g = pX^\alpha + \sum q_{\alpha_i} X^{\alpha_i}$ alors $\mathrm{LM}(f-g) = \mathrm{LM}(\sum (p_{\alpha_i} - q_{\alpha_i}) X^{\alpha_i}) \leq X^{\alpha_1} < X^\alpha = \mathrm{LM}(f) = \mathrm{LM}(g)$ □

Lemme 2.10. *Soit* $f \in k[X_1, \ldots, X_n]$, $\alpha \in \mathbb{N}^n$ *et* $p \in k^*$. *Alors* $\mathrm{LT}(pX^\alpha f) = pX^\alpha \mathrm{LT}(f)$

Démonstration. Soit $f = \sum a_l X^l$ et posons $\beta := \mathrm{LM}(f)$.
Alors $\mathrm{LT}(pf) = pa_\beta X^\beta = p\,\mathrm{LT}(f)$ et $\mathrm{LT}(X^\alpha f) = a_\beta X^{\beta+\alpha} = X^\alpha \mathrm{LT}(f)$ car si, pour tout $l \in \mathbb{N}^n, X^l \leq X^\beta$ alors, par compatibilité de l'ordre monomial avec le produit,$\forall l \in \mathbb{N}^n, X^{l+\alpha} \leq X^{\alpha+\beta}$

□

Théorème 2.11 (Algorithme de division)**.** *Soit* $\geq$ *un ordre monomial et* $(f_1, \ldots, f_s)$ *un s-uplet de polynôme de* $k[X_1, \ldots, X_n]$. *Alors tout polynôme* f *de* $k[X_1, \ldots, X_n]$ *peut s'écrire sous la forme* $f = \sum_{i=1}^n a_i f_i + r$ *où* $a_i \in k[X_1, \ldots, X_n]$ *et* r *est une combinaison linéaire de monômes qui ne sont pas divisibles par les* $\mathrm{LT}(f_i)$

Algorithme 1 Algorithme de division

Entrées : $f_1, \ldots, f_s, f$
Sortie : $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
Tant que $p \neq 0$ **faire**
  $i := 1$
  div :=false
  Tant que $i \leq s$ et div = false **faire**
    Si $\mathrm{LT}(f_i) | \mathrm{LT}(p)$ **alors**
      $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$

Sinon
$i := i + 1$
fin Si
fin Tant que
Si div=false **alors**
$r := r + \mathrm{LT}(p)$
$p := p - \mathrm{LT}(p)$
fin Si
fin Tant que

Démonstration. Pour montrer ce théorème, nous allons montrer que l'algorithme ci-dessus donne le bon résultat et finit pour tout polynôme mis en entrée de l'algorithme.
Remarquons tout d'abord que lors de chaque itération de la boucle, une de ses deux instructions est exécutée :

1. Si $\mathrm{LT}(f_i) | \mathrm{LT}(p)$ alors on fait la division de p par f_i
2. Sinon on ajoute $\mathrm{LT}(p)$ à r (et on retire $\mathrm{LT}(p)$ à p).

Montrons d'abord que l'algorithme s'arrête i.e. il existe une étape où $p = 0$.
Pour cela, montrons que la suite des monômes dominants des différentes valeurs de p est strictement décroissante tant que $p \neq 0$. Si l'algorithme ne s'arrêtait pas, on aurait alors une suite infinie strictement croissante ce qui contredirait le fait que $\geq$ soit un bon ordre.
-Si on fait une division (par f_j) alors p prend la valeur $p' := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)} f_j$.
Si cette valeur est nulle alors l'algorithme s'arrête sinon, grâce à l'égalité obtenue avec le lemme 2.10 :
$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)}\right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)} \mathrm{LT}(f_j) = \mathrm{LT}(p)$ car $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)} \in k^* \mathscr{M}$. Alors, d'après le lemme 2.9, on a que $LM(p') < LM(p)$.
-Sinon, p prend la valeur $p - \mathrm{LT}(p)$. Par le même argument que précédemment, $LM(p - \mathrm{LT}(p)) < \mathrm{LT}(p)$.
Ce qui permet de conclure.
Montrons maintenant qu'à chaque étape que $f = \sum_{i=0}^{s} a_i f_i + p + r$.
Initialisation de l'algorithme ("0ème itération") : Comme $a_1 = \ldots = a_s = r = 0$ et $p = f$ alors l'égalité est vérifiée.
Hérédité : Soit $n \in \mathbb{N}$ et supposons qu'à la $n$ème itération de la boucle, $f = \sum_{i=0}^{s} a_i f_i + p + r = \sum_{i=0, i\neq j}^{s} a_i f_i + a_j f_j + p + r$ pour tout $j \in [\![1, n]\!]$ alors :
- si on fait une division (p avec f_j) alors : la nouvelle valeur p' de p est $p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)} f_j$ et celle de a_i est $a'_j = a_j + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)}$.
et donc : $\begin{aligned} \sum_{i=0, i\neq j}^{s} a_i f_i + a'_j f_j + p' + r &= \sum_{i=0, i\neq j}^{s} a_i f_i + \left(a_j + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)}\right) f_j + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_j)} f_j + r \\ &= \sum_{i=0, i\neq j}^{s} a_i f_i + a_j f_j + p + r = f. \end{aligned}$
- sinon, $f = \sum_{i=0, i\neq j}^{s} a_i f_i + a_j f_j + p + r = \sum_{i=0, i\neq j}^{s} a_i f_i + a_j f_j + (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p))$.
On finit par obtenir que,lorsque $p = 0$ (et on sait que cela arrivera), $f = \sum_{i=1}^{s} a_i f_i + r$ où r est, par définition, une somme d'éléments non divisibles par les $\mathrm{LT}(f_i)$ □

Cet algorithme ne permet pas de savoir, en général, si un polynôme appartient à un idéal. En effet, le reste dépend du s-uplet choisi et dans quel ordre sont les polynômes de celui-ci, comme l'illustre cet exemple.

Exemple 2.12. Soient $f = X^2 + Y^2 + Z^2 - 4$, $g = Y^2 + 2Z^2 - 5$ et $h = XY - 1$ trois polynômes de $k[X, Y, Z]$ et appliquons au polynôme $P = YZf - Yg + 2Zh$ l'algorithme de division pour l'ordre lexicographique.
— Avec la famille (f, g, h), on obtient $P = 2Zf + (XZ - Y)g + (-2XZ^3 + 5XZ - YZ)$
— Avec la famille (h, g, f), on obtient $P = YZf - Yg + 2Zh$
Ce phénomène n'existe pas lorsque les f_i forment une "base de Gröbner" que l'on étudiera dans la section prochaine.

3 Bases de Gröbner

Dans cette section, nous allons commencer par définir et donner quelques propriétés des bases de Gröbner. Puis nous allons énoncer l'algorithme de Buchberger permettant de créer une base de Gröbner à partir d'une base d'un idéal.

3.1 Généralités

Notation 3.1. Soit I un idéal de $k[X_1, \ldots, X_n]$ non nul.
$LT(I)$ est l'ensemble des termes dominants des polynômes de I i.e. $\mathrm{LT}(I) := \{\mathrm{LT}(f) | f \in I\}$.

Définition 3.2. Soit $\geq$ un ordre monomial. Un sous-ensemble $G = \{g_1, \ldots, g_s\}$ d'un idéal I est une base de Gröbner si $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.

On va commencer par montrer qu'une base de Gröbner de I est effectivement une base de I.

Lemme 3.3. *Soit $I := \langle X^\alpha | \alpha \in A \rangle$ un idéal de $k[X_1, \ldots, X_n]$. Alors $X^\beta \in I$ si, et seulement si, il existe un $\alpha \in A$ tel que X^α divise X^β.*

Démonstration. $\Rightarrow$ Si $X^\beta \in I$ alors il existe une famille de polynômes $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ et d'exposants $\alpha_1, \ldots, \alpha_s \in A$ telle que $X^\beta = \sum_{i=1}^{s} P_i X^{\alpha_i}$.
On peut alors remarquer, en utilisant les expressions $P_i := \sum p_{i,\alpha} X^\alpha$, que X^β est de la forme $\sum_{\gamma \in \Gamma} p_\gamma X^\gamma$ où $\Gamma := \{\gamma \in \mathbb{N}^n | \exists p \in \mathbb{N}^n, \exists i \in [\![1, s]\!], \gamma = \alpha_i + p\}$. Et donc $X^\beta - \sum_{\gamma \in \Gamma} p_\gamma X^\gamma = 0$ $(*)$
Comme $k[X_1, \ldots, X_n]$ est un k-espace vectoriel de base canonique $\mathscr{M}$, on déduit de $(*)$ que $p_\gamma = \begin{cases} 0 \text{ si } \gamma \neq \beta \\ 1 \text{ sinon} \end{cases}$ (dans le cas contraire, on aurait une combinaison linéaire (d'élément d'une base) nulle à coefficients non nuls). On en déduit que $\beta \in \Gamma$ et donc qu'il existe un $p \in \mathbb{N}^n$ et un $i \in [\![1, s]\!]$, $\beta = a_i + p$ c'est-à-dire qu'il existe un $i \in [\![1, s]\!]$ tel que X^{α_i} divise X^β. □

Proposition 3.4. *Soient $\geq$ un ordre monomial et I un idéal de de $k[X_1, \ldots, X_n]$. Toute base de Gröbner de I est une base de I.*

Démonstration. Soit I un idéal de $k[X_1, \ldots, X_n]$ non réduit à $\{0\}$ et $g_1, \ldots, g_s \in I$ tels que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.
Comme les g_i appartiennent à I alors $I' := \langle g_1, \ldots, g_s \rangle \subset I$. Montrons l'inclusion réciproque :
Soit $f \in I$. Si $f = 0$ alors, comme I' est un idéal, $f \in I'$.
Supposons donc $f \neq 0$. Comme $\mathrm{LT}(f) \in \langle \mathrm{LT}(I) \rangle$ alors il existe un i tel que $\mathrm{LT}(g_i)$ divise $\mathrm{LT}(f)$ (d'après le lemme 3.2) et donc $f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g_i)} g_i \in I$ (car f et g_i sont dans I).
En itérant ce raisonnement, on obtient que le reste de la division de f par $g_1, \ldots, g_s$ est nul car tous les termes dominants de polynôme de I sont divisibles par un $LT(g_i)$. On en déduit que f est de la forme $\sum g_i h_i$ et donc $f \in I'$.
□

Cette démonstration nous montre aussi que tout idéal de $k[X_1, \ldots, X_n]$ non réduit à $\{0\}$ a une base de Gröbner car la base $\{g_1, \ldots, g_s\}$ est une base de Gröbner par construction.
Nous allons maintenant montrer la propriété des bases de Gröbner promise à la fin de la section précédente : l'unicité du reste de la division par une base de Gröbner.

Proposition 3.5. *Soit $G = \{g_1, \ldots, g_s\}$ une base de Gröbner d'un idéal I de $k[X_1, \ldots, X_n]$ et $f \in k[X_1, \ldots, X_n]$. Alors il existe un unique $r \in k[X_1, \ldots, X_n]$ vérifiant :*

1. *Tous les termes de r ne sont divisible par aucun des* $\mathrm{LT}(g_i)$
2. *Il existe $g \in I$ tel que $f = g + r$*

Démonstration. L'algorithme de division nous donne l'existence d'un tel r. Montrons son unicité.
Supposons, par l'absurde, l'existence de deux restes r_1 et r_2, $r_1 \neq r_2$ vérifiant (1) et (2).
Alors : $\begin{cases} f = g_1 + r_1 \\ f = g_2 + r_2 \end{cases}$ et donc $r_1 - r_2 = g_1 - g_2 \in I$. D'où, comme $r_1 \neq r_2$ alors $LT(r_1 - r_2) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ et donc $\mathrm{LT}(r_1 - r_2)$ est divisible par un des $\mathrm{LT}(g_i)$ (cf Lemme 3.2). On obtient donc une contradiction car aucun terme de r_1 et r_2 n'est divisible par des $\mathrm{LT}(g_i)$. D'où $r_1 = r_2$.

□

Corollaire 3.6. *Soit $G = \{g_1, \ldots, g_s\}$ une base de Gröbner d'un idéal I de $k[X, \ldots, X_n]$ et $f \in k[X_1, \ldots, X_n]$. Alors $f \in I$ si, et seulement si, le reste de la division de f par G est nul.*

Ce corollaire nous permet de répondre au problème 2 de l'introduction : l'appartenance d'un polynôme à un idéal donné. Maintenant pour pouvoir appliquer ce corollaire, on va énoncer une caractérisation des bases de Gröbner plus maniable que celle de la définition.

Notation 3.7. On notera $\overline{f}^F$ le reste de f par la famille $F = (f_1, \ldots, f_s)$.

Si F est une base de Gröbner, on peut juste considérer F comme un ensemble.

Définition 3.8. Soient $f, g \in k[X_1, \ldots, X_n]$ des polynômes non nuls.

1. Posons multideg$(f) = (\alpha_1, \ldots, \alpha_n)$ et multideg$(g) = (\beta_1, \ldots, \beta_n)$. Soit $\gamma = (\gamma_1, \ldots, \gamma_n)$ où $\gamma_i = \max(\alpha_i, \beta_i)$. X^γ est appelé plus petit multiple commun de LM(f) et LM(g) et noté PPCM(LM(f), LM(g)) $:= X^\gamma$.
2. Le S-polynôme de f et g est le polynôme : $S(f, g) := \frac{X^\gamma}{\mathrm{LT}(f)} f - \frac{X^\gamma}{\mathrm{LT}(g)} g$

Une obstruction au fait que $\{f_1, \ldots, f_s\}$ soit une base de Gröbner est que le monôme dominant d'une combinaison de f_i, $\sum \alpha_i f_i$ ne soit pas une combinaison de ceux des LT(f_i). Pour cela, il est nécessaire que $\sum \mathrm{LT}(\alpha_k f_k) = 0$. Les S-polynômes vérifient cette égalité et nous donnent une condition nécessaire et suffisante pour qu'il n'ait pas cette obstruction.

Théorème 3.9. *Soit I un idéal de $k[X_1, \ldots, X_n]$. Alors une base $G = \{g_1, \ldots, g_n\}$ de I est une base de Gröbner de I si, et seulement si, pour tout couple (i, j), $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$*

On admettra ici ce théorème.

3.2 Algorithme de Buchberger

Maintenant que l'on a une caractérisation simple à vérifier d'une base de Gröbner, on va l'utiliser afin de créer un algorithme permettant d'en construire une. On va présenter l'algorithme dit de Buchberger créé par celui-ci. Cet algorithme consiste, pour un ensemble F de polynômes, à calculer tous les restes $\overline{S(g_i, g_j)}^F$ et les ajouter à l'ensemble s'ils sont non nuls et recommencer avec le nouvel ensemble obtenu jusqu'à ce que cela stationne.

Théorème 3.10. *Soit $I := \langle f_1, \ldots, f_s \rangle$ un idéal non nul de $k[X_1, \ldots, X_n]$. Alors on peut construire, en temps fini, une base de Gröbner de I grâce à l'algorithme suivant.*

Algorithme 2 Algorithme de Buchberger

Entrées : $F = (f_1, \ldots, f_s)$
Sortie : Une base de Gröbner $G = (g_1, \ldots, g_t)$ de I, avec $F \subset G$
  $G := F$
  Répéter
    $G' := G$
    Pour chaque paire $\{p, q\} \in G'^2$, $p \neq q$ **faire**
      $S := \overline{S(p, q)}^{G'}$
      Si $S \neq 0$ **alors**
        $G := G \cup \{S\}$
      fin Si
    fin Pour
  Jusqu'à $G = G'$

Démonstration. Tout d'abord, on peut remarquer que $G \subset I$ à chaque étape de l'algorithme car pour tout polynôme $p, q \in I$, $S(p, q)$ est de la forme $fp + gq$ et est donc dans I. De ce fait, $S := \overline{S(p, q)}^G$ appartient à I et donc $G \cup \{S\} \subset I$.
Montrons maintenant que l'algorithme termine, c'est-à-dire que l'on a obtenu un ensemble G tel que pour tout $p, q \in G$, $\overline{S(p, q)}^G = 0$ c'est-à-dire une base de Gröbner.
Considérons pour cela la suite $(G_j)_{j \in \mathbb{N}}$ définie comme la suite d'ensemble obtenu grâce à cet algorithme.
Comme pour tout $j \in \mathbb{N}$, $G_j \subset G_{j+1}$ alors $\langle \mathrm{LT}(G_j) \rangle \subset \langle \mathrm{LT}(G_{j+1}) \rangle$. De plus, si $G_j \neq G_{j+1}$ alors $\langle \mathrm{LT}(G_j) \rangle \neq \langle \mathrm{LT}(G_{j+1}) \rangle$. En effet, si $r \in G_{j+1} \setminus G_j$ alors, par définition du reste, LT(r) n'est pas divisible par aucun des éléments

de G_j et donc n'appartient pas à $\mathrm{LT}(G_j)$. De plus, comme $k[X_1,\dots,X_n]$est noethérien alors la suite $(\langle \mathrm{LT}(G_j)\rangle)$ croissante est stationnaire (c.f. propriété) et donc la suite (G_j) est stationnaire, ce qui montre que l'algorithme termine. □

La base de Gröbner obtenue par cet algorithme contient trop d'éléments que nécessaire comme l'illustre cet exemple :

Exemple 3.11. Lorsqu'on calcule une base de Gröbner pour l'idéal $\langle X^2+Y^2+Z^2-4, Y^2+2Z^2-5, XY-1\rangle$, on obtient la famille $G = \{X^2+Y^2+Z^2-4, Y^2+2Z^2-5, XY-1, X-YZ^2+Y, 2XZ^2-5X+Y, -Z^4+7/2Z^2-3, 2YZ^6-12YZ^4+47/2YZ^2-15Y, -2Z^4+7Z^2-6, -YZ^4+7/2YZ^2-3Y\}$. On peut remarquer que $X^2+Y^2+Z^2-4 = Y^2+2Z^2-5+(Z^2-1)(XY-1)+X(X-YZ^2+Y)$ et que $G\setminus\{X^2+Y^2+Z^2-4\}$ est toujours une base de Gröbner.

Le lemme suivant généralise cette remarque :

Lemme 3.12. *Soit G une base de Gröbner d'un idéal I de $k[X_1,\dots,X_n]$ et $P\in G$ tel que $\mathrm{LT}(P)\in\langle LT(G\setminus\{P\})\rangle$. Alors $G\setminus\{P\}$ est une base de Gröbner de I.*

Démonstration. Comme G est une base de Gröbner de I alors $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. Si $\mathrm{LT}(P)\in\langle \mathrm{LT}(G\setminus\{P\})\rangle$ alors $\langle \mathrm{LT}(G\setminus\{P\})\rangle = \langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$, d'où $G\setminus\{P\}$ est une base de Gröbner de I. □

En itérant ce processus, on obtient une base de Gröbner minimale :

Définition 3.13. Une base de Gröbner minimale G d'un idéal I de $k[X_1,\dots,X_n]$ est une base de Gröbner de I telle que :

1. $\forall P\in G, \mathrm{LC}(P)=1$
2. $\forall P\in G, \mathrm{LT}(P)\notin\langle \mathrm{LT}(G\setminus\{P\})\rangle$

Cependant pour un idéal donné, on n'a pas l'unicité de la base de Gröbner minimale, comme l'illustre cet exemple :

Exemple 3.14. Soit $I := \langle X^2, XY, Y^2-1/2X\rangle$ alors les familles $G_a = \{X^2+aXY, XY, Y^2-1/2X\}$ sont des bases de Gröbner minimales de I pour tout $a\in k$.

L'unicité est perdue à cause du fait qu'il y a des monômes d'un élément f de la base de G_a qui sont dans $G\setminus\{f\}$. La notion de base de Gröbner réduite permet de contourner ce problème.

Définition 3.15. Une base de Gröbner réduite G d'un idéal I de $k[X_1,\dots,X_n]$ est une base de Gröbner de I telle que :

1. $\forall P\in G, \mathrm{LC}(P)=1$
2. Pour tout $P\in G$, aucun monôme de P n'appartient à $\langle \mathrm{LT}(G\setminus\{P\})\rangle$.

On obtient ainsi l'unicité voulue :

Proposition 3.16. *Soit I un idéal non nul de $k[X_1,\dots,X_n]$. Alors, pour un ordre monomial fixé, I a une unique base de Gröbner réduite.*

Démonstration. Soit I un idéal non nul de $k[X_1,\dots,X_n]$.
Commençons par montrer l'existence d'une base de Gröbner réduite d'un idéal I.
Soit G une base de Gröbner minimale de I. $g\in G$ est dit réduit pour G si aucun monôme de g n'est dans $\langle \mathrm{LT}(G\setminus\{g\})\rangle$. On peut remarquer que g est aussi réduite pour n'importe quel base de Gröbner minimale G' telle que $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G')\rangle$.
Pour $g\in G$, posons $g' := \overline{g}^{G\setminus\{g\}}$ et $G' := (G\setminus\{g\})\cup\{g'\}$. Montrons que G' est une base de Gröbner minimale pour I. Comme G est une base de Gröbner minimale alors $\mathrm{LT}(g)\notin\langle \mathrm{LT}(G\setminus\{g\})\rangle$ et donc lorsqu'on divise g par $G\setminus\{g\}$, $\mathrm{LT}(g')$ est ajouté au reste. De ce fait, $\mathrm{LT}(g)=\mathrm{LT}(g')$ et donc $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G')\rangle$. Comme $g'\in I$ alors $G'\subset I$ et donc G est une base de Gröbner de I. De plus, la minimalité de G' se déduit de celle de G et g' est réduit pour G' par construction (grâce à la condition sur le reste de l'algorithme de division)
En itérant ce procédé pour tous les éléments de G, on finit par obtenir une base de Gröbner réduite G' car tous les g sont réduits pour G' (grâce à la remarque faite au début de la preuve).
Montrons maintenant l'unicité.
Soit $G, \widetilde{G}$ deux bases de Gröbner réduites de I.

Montrons tout d'abord que $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$. Comme G et G' sont des bases de Gröbner de I alors $\langle \mathrm{LT}(G)\rangle = \left\langle \mathrm{LT}(\widetilde{G})\right\rangle$. Soit $g \in G$ alors $\mathrm{LT}(g) \in \langle \mathrm{LT}(G')\rangle$ et donc d'après le lemme il existe $g' \in \widetilde{G}$ tel que $\mathrm{LT}(g')$ divise $\mathrm{LT}(g)$. De la même façon, comme $\mathrm{LT}(g') \in \langle \mathrm{LT}(G)\rangle$ alors il existe $g'' \in G$ tel que $\mathrm{LT}(g'')$ divise $\mathrm{LT}(g')$ (et donc $\mathrm{LT}(g)$. Par minimalité de G et G', $\mathrm{LT}(g) = \mathrm{LT}(g') = \mathrm{LT}(g'')$ et donc $\mathrm{LT}(g) \in G'$. D'où $\mathrm{LT}(G) \subset \mathrm{LT}(\widetilde{G})$. Par symétrie de rôle, $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$. Soit $g \in G$ alors il existe un élément $\widetilde{g}$ tel que $\mathrm{LT}(g) = \mathrm{LT}(\widetilde{g})$. Pour montrer que $G = \widetilde{G}$, il suffit de montrer que $g = \widetilde{g}$. Comme G est une base de Gröbner de I et que $g - \widetilde{g} \in I$ alors $\overline{g - \widetilde{g}}^{G} = 0$. Comme G et $\widetilde{G}'$ sont réduites, alors aucun monôme de $g - \widetilde{g}$ n'est divisible par un élément de $\mathrm{LT}(G)$ d'où par l'algorithme de division, $\overline{g - \widetilde{g}}^{G} = g - \widetilde{g}$ et donc $g - \widetilde{g} = 0$ □

On en déduit un critère d'égalité entre idéaux :

Corollaire 3.17. *Soient I, J deux idéaux non nuls de $k[X_1, \ldots, X_n]$. Soient G, H deux bases de Gröbner réduites de respectivement I, J. Alors $G = H \Leftrightarrow I = J$.*

Exemple 3.18. Soit f, g, h définie dans l'exemple 2.12. Alors la base réduite de $\langle f, g, h\rangle$ est : $\{X - YZ^2 + Y, Y^2 + 2Z^2 - 5, Z^4 - 7/2Z^2 + 3\}$

4 Résolution de systèmes polynomiaux

Dans cette section, nous allons étudier comment utiliser les bases de Gröbner afin de résoudre les systèmes d'équations polynomiales. On va commencer par donner l'exemple des polynômes de degré 1 qui peuvent se résoudre avec le pivot de Gauss et voir que les idées du pivot peuvent se généraliser pour toutes familles de polynômes.

4.1 Exemples préliminaires

Comme dit plus haut, lorsque les f_i sont des polynômes de degré 1, on peut résoudre les systèmes de la forme $f_i(x_1, \ldots, x_n) = 0, 1 \leq i \leq s$ $(*)$ en utilisant le pivot de Gauss. Le système $(*)$ se résume à : $AX = B$ où A est la matrice représentative de la partie linéaire de $(f_1, \ldots, f_s)$ et $-B$ sa partie constante. Avec le pivot de Gauss, on obtient une matrice échelonnée $\widetilde{A}$ et une colonne de constante $\widetilde{B}$ telles que : $(*) \Leftrightarrow \widetilde{A}X = \widetilde{B} = {}^t(\widetilde{b_1}, \ldots, \widetilde{b_s})$. Ce qui nous permet de trouver les solutions de $(*)$:
Soit $r = rg(A)(\leq \min(n, s))$

- S'il existe un $\widetilde{b_k} \neq 0$ avec $k > r$ alors $(*)$ n'a pas de solution.
- Si $r < n$ alors on peut exprimer les r premières coordonnées des solutions de $(*)$ grâce aux $n - r$ dernières. L'ensemble des solutions de $(*)$ est un espace affine de dimension $n - r$.
- Si $r = n$ alors $(*)$ admet une seule solution.

On peut voir que le pivot de Gauss consiste à obtenir, à partir des polynômes données au départ, des polynômes ayant une variable en moins puis continuer jusqu'à ce que l'on obtienne un système échelonné. On "remonte" ensuite le système afin de trouver les solutions du système.
Dans la suite, nous allons montrer le théorème d'élimination qui va nous permettre d'éliminer les variables dans les système polynomiaux et ensuite le théorème d'extension pour obtenir les solutions dudit système à partir de celles obtenues par les sytèmes ayant des variables éliminées.
Voici un exemple illustrant cette idée pour des polynômes non linéaires :
Considérons le système : $\begin{cases} x^2 - yz = 4 \\ y^2 - xz = 5 \\ z^2 - xy = 6 \end{cases}$ et son idéal associé $\left\langle X^2 - YZ - 4, Y^2 - XZ - 5, Z^2 - XY - 6\right\rangle$.
Lorsque l'on calcule la Base de Gröbner réduite de I, on obtient $\{X + 7/8Z, Y - 1/16Z, Z^2 - 256/45\}$, on remarque que l'on a obtenu des polynômes de l'idéal où l'on a éliminé les variables et que l'on peut résoudre le système en partant de l'équation $z^2 = 256/45$ où l'on a éliminé X et Y et en complétant ses solutions $\{\pm 16/(3\sqrt{5})\}$ avec les deux autres équations. On obtient donc les deux solutions du système : $\{\pm(-14/(3\sqrt{5}), 1/(3\sqrt{5}), 16/(3\sqrt{5}))\}$.

4.2 Théorème d'élimination

Définition 4.1. Soit $I = \langle f_1, \dots, f_s \rangle$ un idéal de $k[X_1, \dots, X_n]$. On appelle $p$ème idéal d'élimination de I l'idéal I_p de $k[X_{p+1}, \dots, X_n]$ définit par : $I_p = k[X_{p+1}, \dots, X_n] \cap I$, $0 \leq p \leq n-1$

Théorème 4.2 (d'élimination)**.** *Soit I un idéal de $k[X_1, \dots, X_n]$ et G une base de Gröbner de I selon l'ordre lexicographique (que l'on notera ici seulement $\geq$). Alors, pour tout $p \in [\![0, n]\!]$, l'ensemble $G_p = G \cap k[X_{p+1}, \dots, X_n]$ est une base de Gröbner du pème idéal d'élimination I_p.*

Démonstration. Soit $p \in [\![0, n]\!]$. Posons $G = \{g_1, \dots, g_m\}$ et tel que $G_p = \{g_1, \dots, g_r\}$ (quitte à renommer les éléments).
Montrons que G_p est une base de I_p.
Comme $G_p \subset I_p$ (car $G \subset I$) alors $\langle G_p \rangle \subset I_p$. On peut écrire, grâce à l'algorithme de division, $f \in I$ sous la forme $f = \sum_{k=1}^{m} h_i g_i$, l'absence de reste est assuré par le fait que G est une base de Gröbner de I et $f \in I$.
Or pour tout $p > r, \mathrm{LM}(g_i) > X^{p+1} \geq \mathrm{LM}(f)$ et donc aucun terme de f ne peut être divisible par un $\mathrm{LT}(g_i)$. L'algorithme n'incrémente pas les h_p(avec $p > r$) et donc ceux-ci sont tous nuls.
D'où, $f = \sum_{k=1}^{r} h_i g_i$ et donc $f_p \in \langle G_p \rangle$, ce qui finit de montrer l'égalité $\langle G_p \rangle = I_p$.
(Le même argument permet de montrer que si $f \in I_p$, $\overline{f}^{G} = \overline{f}^{G_p}$ $(*)$).
Montrons maintenant que G est une base de Gröbner de I_p. Il suffit, pour cela, de montrer que pour tout $1 \leq i < j \leq r$, $\overline{S(g_i, g_j)}^{G_p} = 0$.
Soit $i, j \in [\![1, r]\!], i < j$. Comme $S(g_i, g_j)$ est de la forme $Pg_i + Qg_j$ $(P, Q \in k[X_{p+1}, \dots, X_n])$ et I_p est un idéal alors $S(g_i, g_j) \in I_p \subset I$ d'où comme G est une base de Gröbner alors $\overline{S(g_i, g_j)}^{G} = 0$ et donc d'après $(*)$, $\overline{S(g_i, g_j)}^{G_k} = 0$.
Ce qui permet de conclure. □

Exemple 4.3. Avec les f, g, h de l'exemple 2.12, le premier idéal d'élimination est :
$I_1 = \langle X - YZ^2 + Y, Y^2 + 2Z^2 - 5, Z^4 - 7/2Z^2 + 3 \rangle$ et le second $I_2 = \langle Z^4 - 7/2Z^2 + 3 \rangle$

Lorsque l'on a calculé le $(n-1)$ème idéal d'élimination, on obtient lorsqu'il n'est pas réduit à $\{0\}$, un idéal de la forme $\langle P \rangle$ (car $k[X_n]$ est principal) et donc un nombre fini de solutions. On va essayer d'étendre les solutions partielles des idéaux d'élimination en des solutions de l'idéal de départ. Pour cela, on va commencer par présenter des résultats sur les résultants qui vont permettre de montrer le théorème d'extension.

4.3 Résultant

Soient A un anneau commutatif intègre et K son corps de fractions.
Soient $f \in A[X]$ et $g \in A[X]$. Soient $p, q \in \mathbb{N}$, tels que $p \geq \deg f$ et $q \geq \deg g$.
Soit $\varphi_{f,g} : K[X]_{<q} \times K[X]_{<p} \to K[X]_{<p+q}$ l'application linéaire définie par : $\forall (u, v) \in K[X]_{<q} \times K[X]_{<p}, \varphi(u, v) = fu + gv$.
On appelle matrice de Sylvester la matrice associée à l'application $\varphi_{f,g}$ dans la base $\mathcal{B} = ((X^i, 0), (0, X^j) | 0 \leq i \leq q-1; 0 \leq j \leq p-1)$ de $K[X]_{<q} \times K[X]_{<p}$ et dans la base canonique de $K[X]_{<p+q}$ que l'on notera $\mathrm{Syl}_{p,q}(f, g)$.
On notera $\mathrm{Res}_{p,q}(f, g)$ le déterminant de $\mathrm{Syl}_{p,q}(f, g)$. On appelle résultant de f et g l'élément $\mathrm{Res}_{\deg(f),\deg(g)}(f, g)$.

Notation 4.4.
- On note $Z(I)$ l'ensemble des zéros communs à tous les polynômes de I i.e. $Z(I) := \{a \in k^n | \forall f \in I, f(a) = 0\}$.
- Soient $f, g \in k[X_1, \dots, X_n]$. On note par $\mathrm{Syl}_{X_i}(f, g), \mathrm{Res}_{X_i}(f, g)$ la matrice de Sylvester (resp. résultant) de f et g vus comme polynômes de $k[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$

Proposition 4.5. $\mathrm{Res}(f, g) \in \langle f, g \rangle \cap k[X_2, \dots, X_n] = I_1$

Démonstration. $\mathrm{Res}(f, g) \in k[X_2, \dots, X_n]$ car le déterminant est polynomial en les coordonnées de la matrice et les composantes de $\mathrm{Syl}(f, g)$ sont dans $k[X_2, \dots, X_n]$.
Montrons maintenant que $\mathrm{Res}(f, g) \in \langle f, g \rangle$.
Notons M la matrice de Sylvester de f et g. Alors $M^t \,\mathrm{Com}(M) = \det(M) I_{\deg(f)+\deg(g)}$ $(*)$ où $\mathrm{Com}(M)$ est la matrice des cofacteurs de M.
Comme les cofacteurs de M sont dans $k[X_2, \dots, X_n]$ (car ceux-ci sont polynomiaux en les coordonnées) alors $\mathrm{Com}(M)$ est dans $\mathcal{M}_{\deg(f)+\deg(g)}(k[X_2, \dots, X_n])$. Donc, en posant $M = (C_1, \dots, C_{\deg(f)+\deg(g)})$, on a, d'après $(*)$, $MC_1 = {}^t\big(\det(M) \quad 0 \quad \dots \quad 0\big)$.
En notant par c l'élément de $(k[X_2, \dots, X_n])[X]_{<\deg(g)} \times (k[X_2, \dots, X_n])[X]_{<\deg(f)}$ de colonne de coordonnées C_1 dans la base $\mathcal{B}$ définie plus haut, on a : $\varphi_{f,g}(c) = \det(M)$, ce qui permet de conclure. □

Si $f = a_1(X_2, \ldots, X_n)X_1 + a_0(X_2, \ldots, X_n)$ et $g = b_1(X_2, \ldots, X_n)X_1 + b_0(X_2, \ldots, X_n)$ sont des polynômes de degré 1 alors leur résultant est $a_0b_1 - a_1b_0$, ce qui est le même résultat que l'on obtient lorsqu'on applique le pivot de Gauss à f et g.

Exemple 4.6. En reprenant les polynômes de l'exemple 2.12, on a $P := \mathrm{Res}_X(f, g) = g^2$, $Q := \mathrm{Res}_X(f, h) = Y^4 + Y^2Z^2 - 4Y^2 + 1$. Ensuite on a $\mathrm{Res}_Y(P, Q) = 4Z^8 - 28Z^6 + 73Z^4 - 84Z^2 + 36 = 4(Z^4 - 7/2Z^2 + 3)^2$

Proposition 4.7.
- *Si* $p = \deg(A)$ *et* $q = \deg(B)$ *alors, par définition,* $\mathrm{Res}(A, B) = \mathrm{Res}_{p,q}(A, B)$
- *Si* $p = \deg(A)$ *et* $q > \deg(B)$ *alors* $\mathrm{Res}_{p,q}(A, B) = ((-1)^p a_p)^{q-degB} \mathrm{Res}(A, B)$
- *Si* $p > \deg(A)$ *et* $q = \deg(B)$ *alors* $\mathrm{Res}_{p,q}(A, B) = b_q^{p-degA} \mathrm{Res}(A, B)$
- *Si* $p > \deg(A)$ *et* $q > \deg(B)$ *alors* $\mathrm{Res}_{p,q}(A, B) = 0$

Démonstration. On écrit la matrice de Sylvester et on développe le déterminant en ligne. □

Théorème 4.8. *Supposons le corps K algébriquement clos. Alors $Res(A, B) = 0$ si, et seulement si, les polynômes A et B ont une racine commune.*

Théorème 4.9. *Soient* $f = \sum_{i=0}^{p} f_i(X_2, \ldots, X_n)X_1^i, f = \sum_{i=0}^{m} g_i(X_2, \ldots, X_n)X_1^i \in k[X_1, \ldots, X_n]$. *Soit* $c \in k^{n-1}$. *Alors* $\mathrm{Res}_{X_1}(f, g)(c) = \mathrm{Res}_{p,q}(f(X_1, c), g(X_1, c))$.

Démonstration. Considérons le morphisme d'anneaux $\varphi : k[X_1, \ldots, X_n] \to k[X_1]$ défini par : $\forall f \in k[X_1, \ldots, X_n], \varphi(f) = f(X_1, c)$.
On a donc $\mathrm{Res}_{X_1}(f, g)(c) = \varphi(\mathrm{Res}_{X_1}(f, g))$ (en identifiant $k[X_2, \ldots, X_n]$ avec le sous-anneau de $k[X_1, \ldots, X_n]$ des polynômes de degré 0 en X_1). Notons $(a_{i,j}(X_2, \ldots, X_n))$ les coefficients de $\mathrm{Syl}_{X_1}(f, g)$. Alors, comme φ est un morphisme d'anneaux, $\mathrm{Res}_{X_1}(f, g)(c) = \varphi(\mathrm{Res}_{X_1}(f, g)) = \det(\varphi((a_{i,j}(X_2, \ldots, X_n)))) = \det((a_{i,j}(c)))$.
Ce qui montre que $\mathrm{Res}_{X_1}(f, g)(c) = \mathrm{Res}_{p,q}(f(X_1, c), g(X_1, c))$. □

Ce sont ces deux théorèmes qui vont faire marcher la preuve du théorème d'extension. On va donner une utilisation du théorème 4.9 pour l'intersection des courbes algébriques planes. L'élimination par le résultant dans le cas à deux variables marche bien. En effet, le résultant de deux polynômes à deux variables est un multiple du générateur de l'idéal d'élimination (car $k[X]$ est principal).

4.3.1 Intersection de deux courbes algébriques planes

Soient les deux courbes algébriques planes $\mathscr{C} = \{f = 0\}, \mathscr{D} = \{g = 0\} \subset \mathbb{C}^2$ où $f = \sum_{i=0}^{m} f_i(X)Y^i, g = \sum_{i=0}^{n} g_i(X)Y^i \in \mathbb{C}[X, Y]$.
Pour trouver les points d'intersection de X et de Y, nous allons tout d'abord trouver les éléments du projeté $\pi_x(\mathscr{C} \cap \mathscr{D})$ de leur intersection sur un des axes (celui des x ici) grâce à la caractérisation suivante :
Soit $a \in \mathbb{C}$ tel que $f_m(a)$ et $g_n(a)$ ne sont pas simultanément nuls.
$a \in \pi_x(\mathscr{C} \cap \mathscr{D}) \Leftrightarrow \exists b \in \mathbb{C}, (a, b) \in X \cap Y \Leftrightarrow \exists b \in \mathbb{C}, f(a, b) = g(a, b) = 0$
$\Leftrightarrow \mathrm{PGCD}(f(a, Y), g(a, Y)) \neq 1$ car le PGCD de ces deux polynômes est divisible par $(X - b)$ grâce à l'équivalence précédente
$\Leftrightarrow \mathrm{Res}(f(a, Y), g(a, Y)) = 0$ (cf théorème 4.8
$\Leftrightarrow \mathrm{Res}_Y(f, g)(a) = 0$ car $f_m(a)$ et $g_n(a)$ ne sont pas simultanément nuls (cf théorème 4.9).
Autrement dit, $\pi_x(\mathscr{C} \cap \mathscr{D}) \subset Z(\mathrm{Res}_Y(f, g))$.
On en déduit que pour pouvoir (éventuellement) compléter une solution partielle a de $\pi_x(\mathscr{C} \cap \mathscr{D})$ en une solution de $X \cap Y$, il suffit de calculer les racines $\{x_1, \ldots, x_n\}$ de $\mathrm{PGCD}(f(a, Y), g(a, Y))$ (comme on peut le voir à la première équivalence ci-dessus) et ensuite de vérifier si les couples (a, x_i) appartiennent à $\mathscr{C} \cap \mathscr{D}$.

Exemple 4.10. Soit $f = (Y^2 + 6)(X^2 - 1) - Y(X^2 + 1), g = (Y^2 + 6)(X^2 - 1) - Y(X^2 + 1)$.
On commence par calculer le résultant de ces polynômes (en Y) : $\mathrm{Res}_Y(f, g) = 2(X - 2)^2(X - 3)^2(X^2 - X + 4)$. Ce polynôme a 4 racines $2, 3, \frac{1+i\sqrt{15}}{2}, \frac{1-i\sqrt{15}}{2}$.
On essaie ensuite de compléter ces solutions partielles en calculant et en trouvant les racines de $\mathrm{PGCD}(f(\cdot, Y), g(\cdot, Y))$:
$\mathrm{PGCD}(f(2, Y), g(2, Y)) = (Y - 2)(Y - 3)$, $\mathrm{PGCD}(f(3, Y), g(3, Y)) = (Y - 2)(Y - 3)$
$\mathrm{PGCD}(f(\frac{1-i\sqrt{15}}{2}, Y), g(\frac{1-i\sqrt{15}}{2}, Y)) = Y - \frac{1+i\sqrt{15}}{2}$, $\mathrm{PGCD}(f(\frac{1+\sqrt{15}i}{2}, Y), g(\frac{1+\sqrt{15}i}{2}, Y)) = Y - \frac{1-i\sqrt{15}}{2}$
On obtient donc les 6 points d'intersection de $\mathscr{C}$ et $\mathscr{D}$: $(2, 2), (2, 3), (3, 2), (3, 3), \left(\frac{1+i\sqrt{15}}{2}, \frac{1-i\sqrt{15}}{2}\right), \left(\frac{1+i\sqrt{15}}{2}, \frac{1-i\sqrt{15}}{2}\right)$

4.4 Théorème d'extension

Théorème 4.11 (d'extension)**.** *Soit $I = \langle f_1, \dots, f_s \rangle$ un idéal de $\mathbb{C}[X_1, \dots, X_n]$ et I_1 le premier idéal d'élimination. Ecrivons, pour $i \in [\![1, s]\!]$, f_i sous la forme : $f_i = g(X_2, \dots, X_n)X_1^{N_i}$ +termes de degré $< N_i$ en X_1*
où $N_i \geq 0$ et $g_i \in \mathbb{C}[X_2, \dots, X_n]$ non nul si $f_i \neq 0$ ($g_i = 0$ si $f_i = 0$).
Supposons qu'on ait une solution partielle $(a_2, \dots, a_n) \in Z(I_1)$. Si $(a_2, \dots, a_n) \notin Z(g_1, \dots, g_s)$ alors il existe $a_1 \in \mathbb{C}$ tel que $(a_1, \dots, a_n) \in Z(I)$.

Démonstration. Montrons ce résultat pour $s = 2$.
Soient $f = \sum_{i=0}^{p} f_i(X_2, \dots, X_n)X_1^i$ et $g = \sum_{j=0}^{q} g_j(X_2, \dots, X_n)X_1^j$ où $f_p \neq 0 \neq g_q$. Soit I l'idéal engendré par f et g et I_1 son premier idéal d'élimination. Soit $c = (c_2, \dots, c_n) \in Z(I_1)$. Comme $\mathrm{Res}_{X_1}(f, g) \in I_1$ alors $\mathrm{Res}_{X_1}(f, g)$.
Montrons que soit $f_p(c) = g_q(c) = 0$ soit il existe $c_1 \in k$ tel que $(c_1, \dots, c_n) \in Z(I)$.
Supposons que $f_p(c) \neq 0$. Alors, d'après les propriétés du résultant (c.f. lemme 4.7) et du théorème 4.9, on a : $\mathrm{Res}(f(X_1, c), g(X_1, c)) = ((-1)^p f_p(c))^{\deg(f(X_1,c))-q} \mathrm{Res}_{p,q}(f(X_1, c), g(X_1, c)) = \mathrm{Res}_{X_1}(f, g)(c) = 0$. Ce qui permet de conclure que $f(X_1, c)$ et $g(X_1, c)$ ont une racine commune c_1(grâce au théorème 4.8) et donc $(c_1, \dots, c_n) \in Z(I)$. On obtient la même chose en supposant $g_q(c) \neq 0$. □

On obtient le corollaire suivant en supposant que un g_i constant (non nul) et que donc $Z(g_1, \dots, g_s) = \emptyset$.

Corollaire 4.12. *Soit $I = \langle f_1, \dots, f_s \rangle$ un idéal de $\mathbb{C}[X_1, \dots, X_n]$ et supposons qu'il existe $i \in [\![1, n]\!]$ tel que f_i s'écrit de la forme : $f_i = cX_1^N$ +termes de degré $< N$ en X_1*
où $N > 0$ et $c \in \mathbb{C} \setminus \{0\}$. Si I_1 est le premier idéal d'élimination de I et $(a_2, \dots, a_n) \in Z(I_1)$ alors il existe $a_1 \in \mathbb{C}$ tel que $(a_1, \dots, a_n) \in Z(I)$

On va commencer par donner un contre-exemple montrant que toutes les hypothèses sont nécessaires.

Exemple 4.13. Soit S_1 le système $\begin{cases} x^2 = y \\ x^2 = z \end{cases}$ et son ensemble de solutions $Z(X^2 - Y, X^2 - Z)$. Notons $I = \langle X - Y, X - Z \rangle$ et I_1 son premier idéal d'élimination.
On peut calculer une base de Gröbner de $I : I = \left\langle X^2 - Z, Y - Z \right\rangle$ d'où $I_1 =< Y - Z >$. Et donc $Z(I_1) = \{(c, c) | c \in k\}$
On peut remarquer que les termes dominants de $X^2 - Y$ et $X^2 - Z$ ne s'annulent pas. D'où, d'après le théorème d'extension, on peut étendre toutes les solutions partielles dans $\mathbb{C}$.
Si on travaille dans $\mathbb{R}$, on peut étendre la solution (c, c) en une solution de S_1 si, et seulement si $c \geq 0$ car les solutions de S_1 ont leur deuxième et troisième coordonnées positives.
Soit S_2 le système $\begin{cases} xy = 1 \\ xz = 1 \end{cases}$ et $I = \langle XY - 1, XZ - 1 \rangle$.
On peut calculer une base de Gröbner de $I : I = \langle XZ - 1, Y - Z \rangle$ d'où $I_1 =< Y - Z >$. On en déduit que $Z(I_1) = \{(c, c) | c \in \mathbb{C}\}$
On peut étendre toutes les solutions partielles sauf la solution $(0, 0)$ (car $0x = 1$ n'a pas de solutions) où les termes dominants de $XY - 1$ et $XZ - 1$ en X s'annulent

On va maintenant finir d'étudier notre exemple (celui de 2.12).

Exemple 4.14. On a $I_1 = \left\langle Y^2 + 2Z^2 - 5, Z^4 - 7/2Z^2 + 3 \right\rangle$ et $I_2 = \left\langle Z^4 - 7/2Z^2 + 3 \right\rangle$.
On a $Z(I_2) = Z(\left\langle Z^4 - 7/2Z^2 + 3 \right\rangle) = \{\pm\sqrt{2}, \pm\sqrt{3/2}\}$. Puis, comme le terme dominant de g est constant alors on peut utiliser le théorème d'extension pour montrer que $Z(I_1) = \{(\pm 1, \pm\sqrt{2}), (\pm\sqrt{2}, \pm\sqrt{3/2})\}$ puis de la même façon, on a que $Z(I) = \{\pm(1, 1, \pm\sqrt{2}), \pm(1/\sqrt{2}, \sqrt{2}, \pm\sqrt{2})\}$

Ces deux théorèmes permettent de répondre à la troisième question de l'introduction.

4.5 Géométrie de l'élimination

Nous allons, dans cette sous-section, donner une interprétation géométrique aux théorèmes d'élimination et d'extension. On va commencer par donner quelques résultats de géométrie.

4.5.1 Résultats préliminaires

Définition 4.15. Soit $f_1, \ldots, f_s$ des polynômes de $k[X_1, \ldots, X_n]$.
On appelle variété affine définie par $f_1, \ldots, f_s$ l'ensemble définie précédemment $Z(f_1, \ldots, f_s) := \{(a_1, \ldots, a_n) \in k^n | \forall i \in [\![1, n]\!], f_i(a_1, \ldots, a_n) = 0\}$.

Exemple 4.16. Dans $\mathbb{R}^2$, le cercle ($= Z(X^2 + Y^2 - R^2)$ où $R \in \mathbb{R}$), la parabole ($= Z(2pX^2 - Y)$ où $p \in \mathbb{R}$) et plus généralement, les coniques sont des variétés affines.
Les sous-espaces affines de k^n sont aussi des variétés affines.

Lemme 4.17. *: Si $V, W \subset k^n$ sont des variétés affines alors $V \cap W$ aussi.*

Démonstration. Supposons que $V = Z(f_1, \ldots, f_s)$ et $W = Z(g_1, \ldots, g_r)$. Alors $V \cap W = Z(f_1, \ldots, f_s, g_1, \ldots, g_r)$.
En effet,$x \in V \cap W$ si, et seulement si, pour tous i, j, $f_i(x) = g_j(x) = 0$, c'est-à-dire si, et seulement si, $x \in Z(f_1, \ldots, f_s, g_1, \ldots, g_r)$. □

Proposition 4.18. *Si $\{f_1, \ldots, f_s\}$ et $\{g_1, \ldots, g_r\}$ sont des bases d'un même idéal I de $k[X_1, \ldots, X_n]$ alors $Z(f_1, \ldots, f_s) = Z(g_1, \ldots, g_r)$*

Démonstration. Comme $\{f_1, \ldots, f_s\}$ et $\{g_1, \ldots, g_r\}$ sont des bases d'un même idéal alors on peut écrire les g_j sous la forme $\sum_{i=1}^{s} h_{i,j} f_i$. De ce fait, si $x \in Z(f_1, \ldots, f_s)$ alors pour tout i, $f_i(x) = 0$ et donc $g_j(x) = \sum_{i=1}^{s} h_{i,j}(x) f_i(x) = 0$.
Et donc $x \in Z(g_1, \ldots, g_r)$.
Par symétrie de rôles, on obtient l'inclusion réciproque. □

De la même façon, on peut montrer que $Z(f_1, \ldots, f_s) = Z(\langle f_1, \ldots, f_s \rangle)$.

On va, dans la suite, considérer des projections de variété affine comme l'analogue géométrique de l'élimination des variables.

Définition 4.19. Soit π_p la projection $\mathbb{C}^n \to \mathbb{C}^{n-p}$ définie par : $\forall (a_1, \ldots, a_n) \in \mathbb{C}^n, \pi_p(a_1, \ldots, a_n) = (a_{p+1}, \ldots, a_n)$.

4.5.2 Géométrie de l'élimination

Soit $V = Z(f_1, \ldots, f_s) \subset \mathbb{C}^n$

Lemme 4.20. *Soit I_p le pème idéal d'élimination de l'idéal $\langle f_1, \ldots, f_s \rangle$ de $\mathbb{C}[X_1, \ldots, X_n]$.*
Alors, dans $\mathbb{C}^{n-p}$, $\pi_p(V) \subset Z(I_p)$.

Démonstration. Pour montrer cette inclusion, il faut montrer que $\forall a \in \pi_p(V), \forall f \in I_p, f(a) = 0$.
Soient $a = (a_{p+1}, \ldots, a_n) \in \pi_p(V)$ et $f \in I_p$.
Comme π_p est surjective alors il existe un $a' = (a_1, \ldots, a_n) \in V$ tel que $\pi_p(a) = a'$. Alors $f(a') = 0$ (car $f \in \langle f_1, \ldots, f_s \rangle$). Or comme f ne dépend que de $X_{p+1}, \ldots, X_n$ alors $f(a) = f(a') = 0$.

□

Théorème 4.21. *Soit g_i défini dans le théorème d'extension et I_1 le premier idéal d'élimination de $\langle f_1, \ldots, f_s \rangle$. On a alors l'égalité, dans $\mathbb{C}^{n-1}$,*
$Z(I_1) = \pi(V) \cup (Z(g_1, \ldots, g_s) \cap Z(I_1))$

Démonstration. $\supset$: c.f. Lemme 4.20
$\subset$: Soit $a := (a_2, \ldots, a_n) \in Z(I_1)$. Alors si $a \notin Z(g_1, \ldots, g_s)$, on a, d'après le théorème d'extension, l'existence d'un $a_1 \in \mathbb{C}$ tel que $(a_1, \ldots, a_n) \in V$ et donc $a \in \pi_1(V)$.
Sinon $a \in \langle g_1, \ldots, g_s \rangle$ et donc dans $Z(g_1, \ldots, g_s) \cap Z(I_1)$ □

En d'autres termes, d'après le théorème d'extension, une solution partielle de $Z(I_1)$ peut soit être étendue en une solution de $Z(I)$ (*i.e.* appartient à $\pi(V)$) soit est un zéro commun des g_i.
On a, de la même façon que pour le théorème d'extension, le corollaire suivant :

Corollaire 4.22. *Supposons qu'il existe $i \in [\![1, n]\!]$ tel que f_i s'écrit de la forme :*
$f_i = cX_1^N +$termes de degré $< N$ en X_1 où $N > 0$ et $c \in \mathbb{C} \setminus \{0\}$.
Alors $\pi(V) = Z(I_1)$.

Le théorème suivant décrit de manière plus précise le lien entre les projections de variété et les zéros de ses idéaux d'élimination et va nous permettre d'étudier les ensembles paramétrés.

Théorème 4.23 (de fermeture)**.** *Soit $V = Z(f_1, \dots, f_s) \subset \mathbb{C}^n$ et soit I_p le pème idéal d'élimination de $\langle f_1, \dots, f_s \rangle$. Alors*

1. *$Z(I_p)$ est la plus petite (au sens de l'inclusion) variété contenant $\pi_p(V)$*
2. *Si $V \neq \emptyset$, alors il existe une variété affine $W \subsetneqq Z(I_p)$ telle que $Z(I_p) \setminus W \subset \pi_p(V)$*

5 Implicitation

Nous allons maintenant étudier le dernier problème que l'on s'est posé : l'implicitation.

Soit S l'ensemble paramétré par le système suivant : $\begin{cases} x_1 = f_1(t_1, \dots, t_m) \\ \vdots \qquad\qquad\qquad\qquad (t_1, \dots, t_m) \in k^m \ (\dagger) \\ x_n = f_n(t_1, \dots, t_m) \end{cases}$

où $f_i \in k[T_1, \dots, T_m]$.

On peut tout d'abord remarquer que S est l'image de k^m par la fonction $F = (f_1, \dots, f_n) : k^m \to k^n$. S n'est pas nécessairement une variété affine (*c.f.* exemple 5.2). Le système (†) peut définir tout de même une variété $V := Z(X_1 - f_1, \dots, X_n - f_n) \subset k^{n+m}$.

On a donc $V = \{(t_1, \dots, t_n, x_1, \dots, x_m) \in k^{n+m} | \forall i \in [\![1, m]\!], x_i - f_i(t_1, \dots, t_n) = 0\}$

D'où, $V = \{(t_1, \dots, t_n, f_1(t_1, \dots, t_n), \dots, f_m(t_1, \dots, t_n)) \in k^{n+m} | (t_1, \dots, t_m) \in k^m\}$. Autrement dit, V est le graphe de F.

De plus, on peut remarquer que V est l'image de l'application $\begin{array}{rccc} i & : & k^m & \to & k^{n+m} \\ & & (t_1, \dots, t_m) & \mapsto & (t_1, \dots, t_n, f_1(t_1, \dots, t_n), \dots, f_m(t_1, \dots, t_n)) \end{array}$

On a donc $\pi_m(V) = F(k^m)$ où $\pi_m : k^{n+m} \to k^n$ est une projection définie de manière analogue à 4.19.

Autrement dit, l'image d'une paramétrisation est la projection de son graphe. En comparant ce résultat avec le théorème de fermeture, on peut trouver la plus petite variété contenant $F(k^m)$.

Théorème 5.1. *Supposons que k est un sous-corps de $\mathbb{C}$.*
Soit $F : k^m \to k^n$ une fonction déterminée par la paramétrisation polynomiale (†).
Soit I l'idéal $\langle X_1 - f_1, \dots, X_n - f_n \rangle \subset k[T_1, \dots, T_m, X_1, \dots, X_n]$ et I_m son m ème idéal d'élimination. Alors $Z(I_m)$ est la plus petite variété de k^n contenant $F(k^m)$.

Démonstration. Si $k = \mathbb{C}$ alors, d'après le théorème de fermeture, $Z(I_m)$ est la plus petite variété contenant $\pi_m(V) = F(k^m)$.

Si k est un sous-corps strict de $\mathbb{C}$ alors on ne peut pas utiliser le théorème de fermeture immédiatement.

Posons $Z_k(I) := \{x \in k^n | \forall f \in I, f(x) = 0\} \subset Z_{\mathbb{C}}(I) := \{x \in \mathbb{C}^n | \forall f \in I, f(x) = 0\}$.

On cherche à montrer que $Z_k(I_m)$ est la plus petite variété de k^n contenant $F(k^m)$.

Remarquons, tout d'abord, que $F(k^m) = \pi_m(V) \subset Z_k(I_m)$ (*c.f.* lemme 4.20).

Ensuite, considérons une variété $V_k := Z_k(g_1, \dots, g_s)$ contenant $F(k^m)$ et montrons que $Z_k(I_m) \subset V_k$.

Soit $i \in [\![1, s]\!]$. Alors g_i s'annule sur V_k(par définition) et en particulier sur $F(k^m)$. D'où $g_i \circ F$ s'annule sur k^m.

Comme $g_i \circ F \in k[T_1, \dots, T_m]$ et que k est infini, alors $g_i \circ F$ est le polynôme nul.

On en déduit que $g_i \circ F$ s'annule sur $\mathbb{C}^m$ ou encore que g_i s'annule sur $F(\mathbb{C}^m)$.

D'où $F(\mathbb{C}^m) \subset V_{\mathbb{C}}$. D'après ce que l'on a montré pour le cas $k = \mathbb{C}$, on a $Z_{\mathbb{C}}(I_m) \subset V_{\mathbb{C}}$. En intersectant par k^n à gauche et à droite de l'inclusion, on obtient $Z_k(I_m) \subset V_k$. □

Exemple 5.2. On appelle parapluie de Withney l'ensemble Γ_k paramétré par $\begin{cases} x = uv \\ y = u \\ z = v^2 \end{cases}$ pour $u, v \in k^2$. On note par F la fonction $(u, v) \mapsto (x, y, z)$.

En appliquant le théorème précédent, on obtient que $V_k := Z(X^2 - Y^2 Z) \subset k^3$ est la plus petite variété contenant Γ_k.

Examinons maintenant s'il y a une égalité :

— Supposons que $k = \mathbb{R}$ et considérons la variété $G_a := \{z = a\} \cap V_{\mathbb{R}}$ pour $a \in \mathbb{R}$. Si $a < 0$ alors l'équation $x^2 - ay^2 = 0$ a pour unique solution $(0, 0)$. De ce fait, $G_a = \{(0, 0, a)\}$. Cependant ce point n'appartient pas à

$\Gamma_{\mathbb{R}}$ car $z \geq 0$.
Si $a \geq 0$ alors, on a l'équivalence : $x^2 - ay^2 = 0 \Leftrightarrow x = \pm\sqrt{a}y$ et donc $G_a = \{(\pm\sqrt{a}y, y, a) | y \in \mathbb{R}\} = \{F(y, \pm\sqrt{a}) | y \in \mathbb{R}\} \subset \Gamma_{\mathbb{R}}$. On en conclut que $V_{\mathbb{R}} = \Gamma_{\mathbb{R}} \cup \{(0, 0, a) | a < 0\}$. De ce fait, $\Gamma_{\mathbb{R}}$ n'est pas une variété.

— Si $k = \mathbb{C}$, la situation est différente :
Soient $a \in \mathbb{C}$, α tel que $\alpha^2 = a$ et $G_a := \{z = a\} \cap V_{\mathbb{C}}$. On a l'équivalence suivante : $x^2 - ay^2 = 0 \Leftrightarrow x = \pm\alpha y$.
De ce fait, $G_a = \{F(y, \pm\alpha) | y \in k\} \subset \Gamma$.

On en déduit que les restrictions à un sous-corps ne préserve pas les égalités entre ensemble décrit par des équations paramétriques et variété associée.

De la même façon, on peut étudier le cas où l'ensemble est paramétré par des fractions rationnelles i.e. pour
$\begin{cases} x_1 = \frac{f_1(t_1,\dots,t_m)}{g_1(t_1,\dots,t_m)} \\ \vdots \qquad\qquad (t_1, \dots, t_m) \in k^m \setminus Z(g_1 \dots g_n) \ (\ddagger) \\ x_n = \frac{f_n(t_1,\dots,t_m)}{g_n(t_1,\dots,t_m)} \end{cases}$
où $f_i, g_i \in k[T_1, \dots, T_m]$.
Alors l'analogue du théorème 5.1 pour le système $(\ddagger)$ est :

Théorème 5.3. *Supposons que k est un sous-corps de $\mathbb{C}$.*
Soit $F : k^m \setminus Z(g_1 \dots g_n) \to k^n$ une fonction déterminée par la paramétrisation rationnelle $(\ddagger)$.
Soit I l'idéal $\langle g_1 X_1 - f_1, \dots, g_n X_n - f_n, 1 - g_1 \dots g_n Y \rangle \subset k[Y, T_1, \dots, T_m, X_1, \dots, X_n]$ et I_{m+1} son $m+1$ ème idéal d'élimination. Alors $Z(I_{m+1})$ est la plus petite variété de k^n contenant $F(k^m \setminus Z(g_1 \dots g_n))$.

Cet énoncé appelle quelques remarques :
Tout d'abord, on a ôté $Z(g_1 \dots g_n)$ du domaine de définition car c'est l'ensemble des points x pour lesquels au moins un $g_i(x)$ s'annule. Ensuite, on a dû ajouter le polynôme $1 - g_1 \dots g_n Y$ pour garder l'information que les g_i ne doivent pas s'annuler dans l'idéal après avoir "chassé" les dénominateurs. En effet, on voit que cela est nécessaire grâce à l'exemple suivant : $\begin{cases} x = \frac{u^2}{v} \\ y = \frac{v^2}{u} \\ z = u \end{cases}$ et $I = \langle VX - U^2, UY - V^2, Z - U \rangle$.
Lorqu'on calcule la base de Gröbner de I, on obtient $\{U - Z, V^2 - YZ, VX - Z^2, VZ^2 - XYZ, X^2YZ - Z^4\}$ et donc $Z(I_2) = Z(X^2YZ - Z^4) = Z(X^2Y - Z^3) \cup Z(Z)$, c'est-à-dire $Z(I_2)$ n'est pas la plus petite variété contenant $F((k^*)^2)$.
On va finir par un exemple d'utilisation du théorème 5.3 :

Exemple 5.4 (Folium de Descartes)**.** $(S) \begin{cases} x = \frac{3t}{1+t^3} \\ y = \frac{3t^2}{1+t^3} \end{cases}$
En calculant l'idéal d'élimination, on obtient que la variété associée est $V = Z(X^3 - 3XY + Y^3)$. En considérant les points d'intersection de V avec les droites $\mathscr{D}_t$ d'équation $y = tx$, $t \in \mathbb{R} \setminus \{-1\}$: $(0, 0)$, $(\frac{3t}{1+t^3}, \frac{3t^2}{1+t^3})$, on montre l'égalité entre la variété V et S.

Références

[1] Pierre Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres).* École Polytechnique, 2011.

[2] Donal O'Shea David Cox, John Little. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer New York, 1992.

[3] J.P. Ramis, X. Buff, A. Warusfel, E. Halberstadt, and F. Moulin. *Mathématiques : Tout-en-un pour la Licence niveau L2.* Dunod, 2014.

[4] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, 2003.