

Bases de Gröbner II : Calcul et Géométrie¹

Résumé

L'une des applications principales des bases de Gröbner est en relation avec la géométrie, et l'appartenance au radical d'un idéal. Quant au calcul de ces bases, il est permis par un algorithme simple de Buchberger, dont la correction et la terminaison nécessitent un peu de travail.

1. Radicaux et Nullstellensatz

Dans tout ce qui suit, \mathbb{A} est un anneau commutatif unitaire et \mathbb{K} est un corps.

DÉFINITION 1. Soit \mathcal{I} un idéal de \mathbb{A} . Son radical :

$$\sqrt{\mathcal{I}} := \{f \in \mathbb{A} \mid \exists p \in \mathbb{N}, f^p \in \mathcal{I}\}$$

est un idéal de \mathbb{A} .

Cette définition vise à éliminer les multiplicités dans les polynômes sur lesquels on travaille. Par exemple, si $\mathbb{A} = \mathbb{K}[X]$ et $\mathcal{I} = \langle X^2 \rangle$, alors $\sqrt{\mathcal{I}} = \langle X \rangle$.

On se place maintenant définitivement dans le cas $\mathbb{A} = \mathbb{K}[X_1, \dots, X_n]$, cadre des bases de Gröbner. On notera \mathbf{X} pour X_1, \dots, X_n .

PROPOSITION 1 (Astuce de Rabinowitsch, 1929). Soient f, f_1, \dots, f_r des éléments de $\mathbb{K}[\mathbf{X}]$. On définit aussi :

$$\begin{aligned} \mathcal{I} &:= \langle f_1, \dots, f_r \rangle \subset \mathbb{K}[\mathbf{X}] \\ \tilde{\mathcal{I}} &:= \langle f_1, \dots, f_r, 1 - tf \rangle \subset \mathbb{K}[\mathbf{X}, t] \end{aligned}$$

Alors :

$$f \in \sqrt{\mathcal{I}} \Leftrightarrow \tilde{\mathcal{I}} = \langle 1 \rangle.$$

Ce résultat donne un algorithme pour le test d'appartenance au radical : le calcul d'une base de Gröbner de $\tilde{\mathcal{I}}$.

DÉMONSTRATION. $\boxed{\Rightarrow}$ Supposons que $f^p \in \mathcal{I}$. Alors $f^p \in \tilde{\mathcal{I}}$ donc $t^p f^p \in \tilde{\mathcal{I}}$. Or $1 - t^p f^p \in \tilde{\mathcal{I}}$ donc $1 \in \tilde{\mathcal{I}}$.

$\boxed{\Leftarrow}$ Si $1 \in \tilde{\mathcal{I}}$, alors il s'écrit

$$1 = g_1(\mathbf{X}, t)f_1(\mathbf{X}) + \dots + g_r(\mathbf{X}, t)f_r(\mathbf{X}) + g(\mathbf{X}, t)(1 - tf(\mathbf{X})).$$

En injectant $t = \frac{1}{f(\mathbf{X})}$, et en réduisant au même dénominateur, on obtient explicitement la décomposition de f^m en termes des f_i , où m est le maximum des degrés des g_i en t , ce qui montre $f \in \sqrt{\mathcal{I}}$. \square

On arrive au théorème fondamental de cette partie.

¹La première rédaction de ce chapitre est due à Sary Drappeau.

THÉORÈME 17 (Nullstellensatz de Hilbert). *On suppose que \mathbb{K} est algébriquement clos. Soient f, f_1, \dots, f_r des éléments de $\mathbb{K}[\mathbf{X}]$. Alors $f \in \sqrt{\langle f_1, \dots, f_r \rangle}$ si et seulement si f s'annule sur le lieu des zéros communs des f_i dans \mathbb{K}^n .*

Ainsi, la géométrie de la variété définie par les f_i est codée dans le radical de l'idéal qu'ils engendrent.

DÉMONSTRATION. $\boxed{\Rightarrow}$ Si $f^p = \sum g_i f_i$, et si $\mathbf{x} \in \mathbb{K}^n$ est un zéro commun aux f_i , alors $f^p(\mathbf{x})$ donc $f(\mathbf{x}) = 0$.

$\boxed{\Leftarrow}$ Soit f s'annulant en tous les zéros communs des f_i . D'après l'astuce de Rabinowitsch, il suffit de montrer que 1 est dans l'idéal engendré par $f_1, \dots, f_r, 1 - tf$. Tout d'abord, on observe que ces polynômes n'ont pas de zéros communs. En effet, s'il en existait un, disons $\mathbf{a} = (a_1, \dots, a_n)$, alors par hypothèse $f(\mathbf{a}) = 0$, donc $(1 - tf)(\mathbf{a}) = 1$, ce qui est contradictoire. La conclusion découle alors de la forme faible du Nullstellensatz ci-dessous. \square

PROPOSITION 2 (Nullstellensatz faible). *Si \mathbb{K} est algébriquement clos, et \mathcal{I} est un idéal strict de $\mathbb{K}[\mathbf{X}]$, alors $\exists \mathbf{a} = (a_1, \dots, a_n) \in \mathbb{K}^n$ tel que*

$$\forall f \in \mathcal{I}, \quad f(\mathbf{a}) = 0.$$

La preuve procède par récurrence, et pour $n \geq 2$ utilise un argument de projection pour se ramener à une variable de moins. Le lemme suivant permet d'assurer que cette projection se passe bien. (Notons que si \mathbb{K} est algébriquement clos, il est infini.)

LEMME 1 (Lemme de normalisation de Noether). *Supposons $n \geq 2$, et \mathbb{K} infini. Soit $f \in \mathbb{K}[\mathbf{X}]$ de degré $d > 0$. Alors il existe $(\lambda_1, \dots, \lambda_{n-1}) \in \mathbb{K}^{n-1}$ tels que le coefficient de X_n^d dans*

$$f(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

soit non nul.

DÉMONSTRATION. Posons

$$f(\mathbf{X}) = \sum_{i_1 + \dots + i_n \leq d} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

Puisque f est de degré d , le polynôme

$$g(\mathbf{X}) := \sum_{i_1 + \dots + i_n = d} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

est non nul.

Or le coefficient de X_n^d dans $f(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n)$ vaut précisément

$$\sum_{i_1 + \dots + i_n = d} a_{i_1, \dots, i_n} \lambda_1^{i_1} \cdots \lambda_{n-1}^{i_{n-1}}$$

Comme \mathbb{K} est infini, on est assuré de l'existence de scalaires $\lambda_1, \dots, \lambda_{n-1}$ qui lui donnent une valeur non nulle (encore par récurrence sur le nombre de variables : pour une variable, le nombre de racines est borné par le degré, ensuite on regarde le coefficient de tête, on prend un point où il ne s'annule pas et on conclut sur le polynôme en une variable ainsi obtenu). \square

DÉMONSTRATION (DU NULLSTELLENSATZ FAIBLE). On procède par récurrence sur n .

Le cas $n = 1$ est assuré par le fait que \mathbb{K} est algébriquement clos.

Si $n \geq 2$, on va projeter pour se ramener à une variable de moins. Soit $g \in \mathcal{I}$. D'après le lemme de normalisation, on peut supposer quitte à renormaliser g qu'il existe $\lambda_1, \dots, \lambda_{n-1}$ tels que $g(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n) = X_n^d + r(X_1, \dots, X_n)$, r étant de degré au plus $n - 1$ en X_n .

Alors en posant $\mathcal{J} := \{f(X_1 + \lambda_1 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n), f \in \mathcal{I}\}$, on obtient un autre idéal strict de $\mathbb{K}[\mathbf{X}]$. Donc, quitte à remplacer \mathcal{I} par \mathcal{J} , on suppose que $g(\mathbf{X}) = X_n^d + g_{d-1} X_n^{d-1} + \dots + g_0$, $g_i \in \mathbb{K}[X_1, \dots, X_{n-1}]$.

On pose alors $\mathcal{I}' = \mathcal{I} \cap \mathbb{K}[X_1, \dots, X_{n-1}]$. C'est un idéal strict de $\mathbb{K}[X_1, \dots, X_{n-1}]$. Par hypothèse de récurrence, il existe donc $\mathbf{a} = a_1, \dots, a_{n-1}$ qui annule tous les polynômes de \mathcal{I}' .

On pose alors $\mathcal{J} = \{f(\mathbf{a}, X_n), f \in \mathcal{I}\}$. C'est un idéal de $\mathbb{K}[X_n]$. S'il est strict alors il est engendré par un polynôme non constant en X_n , dont n'importe quelle racine a_n donne la réponse (\mathbf{a}, a_n) à la question. Si on suppose le contraire, alors $\exists f \in \mathcal{I}$ tel que $f(\mathbf{a}, X_n) = 1$. Ce polynôme peut s'écrire

$$f(\mathbf{X}) = f_0 + f_1 X_n + \dots + f_k X_n^k,$$

où les f_i sont dans $\mathbb{K}[X_1, \dots, X_{n-1}]$. L'hypothèse implique que $f_0(\mathbf{a}) = 1$ et $f_1(\mathbf{a}) = \dots = f_k(\mathbf{a}) = 0$.

Le résultant R de f et g par rapport à la variable X_n est à la fois un élément de $\mathbb{K}[X_1, \dots, X_{n-1}]$ et de $\langle f, g \rangle \subset \mathcal{I}$. Donc $R \in \mathcal{I}'$, ce qui implique $R(\mathbf{a}) = 0$. Pourtant, en évaluant la matrice de Sylvester de (f, g) en \mathbf{a} , on obtient des 1 sur la diagonale et des 0 au-dessus, ce qui entraîne $R(\mathbf{a}) = 1$, une contradiction. Donc \mathcal{J} est strict et la preuve est terminée. \square

2. Calcul effectif des bases de Gröbner

Nous allons maintenant voir comment mettre en place le calcul des bases de Gröbner, et enfin prouver leur existence.

2.1. S-polynômes. On se place dans $\mathbb{K}[X_1, \dots, X_n]$, et on fixe un ordre monomial.

DÉFINITION 2. Soient f et g deux polynômes. On appelle S-polynôme de f et g et on note $S(f, g)$ le polynôme suivant :

$$S(f, g) := (\text{LM}(f) \vee \text{LM}(g)) \left(\frac{f}{\text{LT}(f)} - \frac{g}{\text{LT}(g)} \right),$$

où l'on note $f \vee g$ le ppcm de f et g .

Par construction, $S(f, g)$ est un polynôme, et il appartient à $\langle f, g \rangle$. La notation S vient du mot *syzygie*, qui vient lui-même du grec ancien *suzugia* qui signifie « sous le même joug ».

La proposition suivante donne la clé de la construction de bases de Gröbner.

PROPOSITION 3. L'ensemble $G = \{g_1, \dots, g_m\}$ est une base de Gröbner de $\langle G \rangle$ si et seulement si

$$\forall 1 \leq i < j \leq m, \quad \overline{S(g_i, g_j)}^G = 0.$$

DÉMONSTRATION. Le sens direct est clair.

Soit $f \in \mathcal{I} := \langle G \rangle$. Il s'agit de montrer que $\text{LT}(f) \in \langle \text{LT}(G) \rangle$. Parmi toutes les décompositions

$$f = \sum h_i g_i,$$

on en choisit une qui minimise la quantité

$$\delta := \max_i \text{LM}(h_i g_i),$$

ce qui est possible puisqu'il n'y a pas de chaîne infinie décroissante. Il suffit de montrer que $\text{LM}(f) = \delta$. Soit $S := \{i \mid \text{LM}(h_i g_i) = \delta\}$ et quitte à renuméroter les h_i et les g_i , on peut supposer $S = \{1, \dots, k\}$ pour un certain k . La décomposition de f se réécrit

$$\begin{aligned} f &= \sum_{i \in S} h_i g_i + \sum_{i \notin S} h_i g_i \\ &= \sum_{i \in S} \text{LT}(h_i) g_i + \underbrace{\sum_{i \in S} (h_i - \text{LT}(h_i)) g_i + \sum_{i \notin S} h_i g_i}_{\text{chaque terme a un LM} < \delta} \end{aligned}$$

On note $\text{LT}(h_i) = c_i \mathbf{X}^{\alpha_i} = c_i X_1^{\alpha_{i1}} \cdots X_n^{\alpha_{in}}$ et on observe que $S(\mathbf{X}^{\alpha_i} g_i, \mathbf{X}^{\alpha_j} g_j)$ est un multiple de $S(g_i, g_j)$:

$$S(\mathbf{X}^{\alpha_i} g_i, \mathbf{X}^{\alpha_j} g_j) = \delta \left(\frac{\mathbf{X}^{\alpha_i} g_i}{\text{LC}(g_i) \delta} - \frac{\mathbf{X}^{\alpha_j} g_j}{\text{LC}(g_j) \delta} \right) = \frac{\mathbf{X}^{\alpha_i} g_i}{\text{LC}(g_i)} - \frac{\mathbf{X}^{\alpha_j} g_j}{\text{LC}(g_j)}.$$

Maintenant,

$$\begin{aligned} \sum_{i=1}^k c_i \mathbf{X}^{\alpha_i} g_i &= c_1 \text{LC}(g_1) S(\mathbf{X}^{\alpha_1} g_1, \mathbf{X}^{\alpha_2} g_2) \\ &\quad + (c_1 \text{LC}(g_1) + c_2 \text{LC}(g_2)) S(\mathbf{X}^{\alpha_3} g_3, \mathbf{X}^{\alpha_3} g_3) + \cdots \\ &\quad + (c_1 \text{LC}(g_1) + \cdots + c_{k-1} \text{LC}(g_{k-1})) S(\mathbf{X}^{\alpha_{k-1}} g_{k-1}, \mathbf{X}^{\alpha_k} g_k) \\ &\quad + (c_1 \text{LC}(g_1) + \cdots + c_k \text{LC}(g_k)) \frac{\mathbf{X}^{\alpha_k} g_k}{\text{LC}(g_k)}. \end{aligned}$$

Tous les termes de la somme sauf le dernier ont, par construction des S-polynômes, un monôme dominant strictement inférieur à δ et par hypothèse peuvent être réécrits par l'algorithme de division comme combinaison des g_i , dont le terme de tête n'atteint pas δ . Par minimalité de δ , le dernier terme doit donc avoir pour monôme δ et on a récrit f comme une somme avec un seul monôme égal à δ et tous les autres inférieurs, donc $\text{LM}(f) = \delta$. \square

2.2. L'algorithme de Buchberger. L'algorithme de Buchberger est donné en figure. Il se base sur des calcul de S-polynômes que l'on réduit puis que l'on ajoute à la base que l'on a déjà.

PREUVE DE L'ALGORITHME. À chaque étape de l'algorithme, l'idéal engendré par G est $\langle f_1, \dots, f_m \rangle$. L'inclusion provient de l'initialisation de G et ensuite G ne s'accroît que de S-polynômes d'éléments de G . Enfin, lorsque l'algorithme termine, tous les S-polynômes de G sont bien réduits à 0 par G , ce qui prouve qu'il s'agit d'une base de Gröbner. Le seul point délicat à prouver est donc la terminaison.

Algorithme 1 Algorithme de Buchberger**Entrées:** $f_1, \dots, f_m \in \mathbb{K}[\mathbf{X}]$, muni d'un ordre monomial.**Sorties:** Une base de Gröbner de l'idéal engendré par les f_i ,
pour l'ordre monomial donné. $G := \{f_1, \dots, f_m\}$ $S := \{S(f_i, f_j), i < j\}$ **tant que** $S \neq \emptyset$ **faire** Choisir un $p \in S$ $S := S \setminus \{p\}$ $g := \bar{p}^G$ **si** $g \neq 0$ **alors** $S := S \cup \{S(g, h), h \in G\}$ $G := G \cup \{g\}$ **fin si****fin tant que****renvoyer** G

À chaque étape, soit le cardinal de S décroît, $\langle \text{LT}(G) \rangle$ croît. Il suffit de montrer que la deuxième possibilité ne peut se produire qu'à un nombre fini d'étapes. L'union de tous ces idéaux $\langle \text{LT}(G) \rangle$ est un idéal. Le résultat est alors une conséquence du lemme de Dickson ci-dessous. \square

LEMME 2 (Lemme de Dickson). *Soit A un ensemble de multi-indices en n variables. Alors tout idéal monomial $\mathcal{I} = \langle \mathbf{X}^\alpha, \alpha \in A \rangle$ admet une base monomiale finie.*

DÉMONSTRATION. On procède par récurrence sur le nombre de variables. Pour $n = 1$, on a $\mathcal{I} = \langle X^\beta \rangle$ où $\beta = \min A$.

Supposons $n > 1$. On note $\mathbf{X} = X_1, \dots, X_{n-1}$ et $Y = X_n$. Posons

$$\mathcal{J} := \{\mathbf{X}^\alpha \mid \exists m, \mathbf{X}^\alpha Y^m \in \mathcal{I}\}$$

Où α est un multi-indice en $n - 1$ variables.

L'idéal $\langle \mathcal{J} \rangle$ est un idéal monomial de $\mathbb{K}[\mathbf{X}]$. Il admet donc une base finie notée $\mathbf{X}^{\alpha_1}, \dots, \mathbf{X}^{\alpha_s}$. Posons alors :

$$m_i := \min \{m \in \mathbb{N} \mid \mathbf{X}^{\alpha_i} Y^m \in \mathcal{I}\}, \quad m := \max_i m_i.$$

Ensuite, pour $k = 0, \dots, m - 1$, on considère les « tranches »

$$\mathcal{J}_k := \{\mathbf{X}^\alpha \mid \mathbf{X}^\alpha Y^k \in \mathcal{I}\}.$$

Chaque $\langle \mathcal{J}_k \rangle$ est un idéal monomial de $\mathbb{K}[\mathbf{X}]$, et admet par hypothèse de récurrence une base finie $\mathbf{X}^{\alpha_1^{(k)}}, \dots, \mathbf{X}^{\alpha_{s_k}^{(k)}}$.

Une base finie de \mathcal{I} est donc finalement donnée par

$$\{\mathbf{X}^{\alpha_j^{(k)}} Y^k \mid 0 \leq k < m, 1 \leq j \leq s_k\} \cup \{\mathbf{X}^{\alpha_1} Y^m, \dots, \mathbf{X}^{\alpha_s} Y^m\}.$$

 \square