

ALGÈBRE EFFECTIVE

PIERRE-GUY PLAMONDON

22 octobre 2025

Ces notes sont issues d'un cours de deuxième année de Master donné à l'Université de Versailles Saint-Quentin de 2020 à 2025. Notre objectif dans ce cours est de présenter les bases de Gröbner tant théoriquement que pratiquement, et d'en voir quelques applications.

Chaque exercice apparaît dans le texte à l'endroit où il m'a semblé le plus naturel de l'inclure.

Mes notes sont influencées par celles de Nicolas Perrin, qui était responsable de ce cours avant moi, et par Luca de Feo et Christina Boura, qui ont élaboré et maintenu une liste d'exercices à effectuer avec Sage.

Si vous trouvez des erreurs ou des fautes de frappe, n'hésitez pas à m'en informer en m'écrivant à l'adresse `pierre-guy.plamondon@uvsq.fr`.

TABLE DES MATIÈRES

1. Anneaux de polynômes et noethérianité	1
2. Division multivariée	3
3. Bases de Gröbner	7
4. Algorithme de Buchberger	8
Références	11

1. ANNEAUX DE POLYNÔMES ET NOETHÉRIANITÉ

On suppose connue la théorie élémentaire des anneaux, ainsi que les objets principaux de cette théorie : idéaux, anneaux quotients, sous-anneaux, morphismes d'anneaux, corps, etc. Dans ces notes, les anneaux sont tous unitaires et ne sont pas nécessairement commutatifs. Les corps sont tous commutatifs.

Définition 1.1. Un idéal (à gauche, à droite ou bilatère) I d'un anneau A est *finiment engendré* (ou *de type fini*) s'il existe des éléments a_1, \dots, a_n de A tels que I soit engendré par a_1, \dots, a_n .

Notation 1.2. On note $\langle a_1, \dots, a_n \rangle$ l'idéal (à gauche, à droite ou bilatère, selon le contexte) engendré par a_1, \dots, a_n . Si E est une partie de A , on note $\langle E \rangle$ l'idéal engendré par E .

Définition 1.3. Un anneau est *noethérien* à gauche (ou à droite) si tous ses idéaux à gauche (ou à droite, respectivement) sont finiment engendrés. Pour un anneau commutatif, on dira *noethérien* au lieu de "noethérien à gauche (ou à droite)".

Exemples 1.4. (1) L'anneau \mathbb{Z} est noethérien.

(2) Plus généralement, tout anneau principal est noethérien.

(3) Pour un anneau R , l'anneau des polynômes $R[x_1, x_2, \dots]$ en une infinité de variables n'est pas noethérien.

Dans la littérature, les anneaux noethériens sont généralement plutôt définis en utilisant la caractérisation suivante.

Proposition 1.5. *Un anneau est noethérien à gauche (ou à droite) si et seulement si toute suite croissante d'idéaux à gauche (ou à droite) $I_0 \subset I_1 \subset \dots$ se stabilise (c'est-à-dire qu'il existe un entier $N \in \mathbb{N}$ tel que si $n \geq N$, alors $I_n = I_N$).*

Démonstration. On ne traitera que le cas "à gauche". Supposons d'abord que A est noethérien à gauche. Soit $I_0 \subset I_1 \subset \dots$ une suite croissante d'idéaux à gauche de A . Soit I leur union ; c'est un idéal de A . Comme A est noethérien, I est finiment engendré, disons par a_1, \dots, a_r . Chacun des a_i est contenu dans un certain I_{n_i} . Prenant N comme étant le maximum des n_i , on a que $a_1, \dots, a_r \in I_N$. En particulier, $I_N = I$, et la suite se stabilise.

Réciproquement, supposons que A n'est pas noethérien à gauche, et soit I un idéal à gauche de A qui n'est pas finiment engendré. Soit $a_0 \in I$. Pour chaque entier $m \geq 1$, soit $a_m \in I \setminus \langle a_0, \dots, a_{m-1} \rangle$. Un tel a_m existe, sans quoi I serait égal à $\langle a_0, \dots, a_{m-1} \rangle$ et donc finiment engendré. Alors la suite d'idéaux à gauche

$$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \dots$$

est strictement croissante, et ne se stabilise donc pas. □

Exercice 1.1. Soit A est un anneau noethérien à gauche, et soit E une partie non vide de A . Il existe une partie finie F de E telle que les idéaux à gauche $\langle E \rangle$ et $\langle F \rangle$ sont égaux.

Le résultat principal de cette section est le Théorème de la base de Hilbert. Il a été démontré par Hilbert dans [Hil90]. On peut trouver une traduction anglaise dans [Hil78]. La démonstration présentée ici n'est pas celle de Hilbert – elle est basée, par exemple, sur celle trouvée dans [Ass97, Chap. VI.2].

Théorème 1.6 (de la base de Hilbert). *Soit A un anneau noethérien à gauche (ou à droite). Alors l'anneau de polynômes $A[x]$ est aussi noethérien à gauche (ou à droite, respectivement).*

Démonstration. Soit I un idéal à gauche de $A[x]$. Il faut montrer que I est finiment engendré.

Pour chaque entier $n \in \mathbb{N}$, soit

$$I_n = \{a_n \in A \mid \exists a_0 + a_1x + \dots + a_nx^n \in I\}.$$

Alors I_n est un idéal de A . De plus, $I_n \subset I_{n+1}$, car si $\sum_{i=0}^n a_i x^i \in I$, alors on a que $x \sum_{i=0}^n a_i x^i \in I$.

Puisque A est noethérien à gauche, la suite $I_0 \subset I_1 \subset \dots$ se stabilise. Soit $N \in \mathbb{N}$ tel que $n \geq N$ entraîne que $I_n = I_N$.

Comme A est noethérien, les idéaux I_0, \dots, I_N sont finiment engendrés. Posons

$$\begin{aligned} I_0 &= \langle a_{0,1}, a_{0,2}, \dots, a_{0,r_0} \rangle \\ I_1 &= \langle a_{1,1}, a_{1,2}, \dots, a_{1,r_1} \rangle \\ &\dots \\ I_N &= \langle a_{N,1}, a_{N,2}, \dots, a_{N,r_N} \rangle. \end{aligned}$$

De plus, pour chaque $a_{i,j} \in I_i$, soit $f_{i,j} \in I$ un polynôme de degré au plus i dont le coefficient en degré i est $a_{i,j}$ (un tel polynôme existe par définition de I_i). Nous allons montrer que I est engendré par les $f_{i,j}$ et qu'il est donc de type fini. Soit $f \in I$ et soit d le degré de f . On montre par récurrence sur d que f est engendré par les $f_{i,j}$.

Si $d = 0$, alors $f \in A$, et donc $f \in I_0$. D'où $f = \sum_{j=1}^{r_0} \lambda_j a_{0,j}$, où les λ_j sont dans A . Or, chaque $a_{0,j}$ est égal à $f_{0,j}$. Donc f est engendré par les $f_{i,j}$.

Si $1 \leq d \leq N$, alors écrivons $f = bx^d + r$, avec $b \in A$ et $\deg(r) < d$. Alors $b \in I_d$, et on peut écrire $b = \sum_{j=1}^{r_d} \lambda_j a_{d,j}$, où les λ_j sont dans A . Soit $S = \sum_{j=1}^{r_d} \lambda_j f_{d,j}$. Alors S est de degré d et son coefficient directeur est b . Donc $f - S$ est de degré strictement inférieur à d , et par hypothèse de récurrence, il est engendré par les $f_{i,j}$. Comme S est aussi engendré par les $f_{i,j}$ par définition, on en déduit que f l'est aussi.

Si $d > N$, alors écrivons encore $f = bx^d + r$, avec $b \in A$ et $\deg(r) < d$. Alors $b \in I_d = I_N$, et on peut écrire $b = \sum_{j=1}^{r_N} \lambda_j a_{N,j}$, où les λ_j sont dans A . Soit $T = x^{d-N} \cdot \sum_{j=1}^{r_N} \lambda_j f_{N,j}$. Alors T est de degré d et son coefficient directeur est b . On montre alors comme au cas précédent que f est engendré par les $f_{i,j}$. □

Corollaire 1.7. *Si A est noethérien à gauche (ou à droite), alors l'anneau de polynômes $A[x_1, \dots, x_n]$ est noethérien à gauche (ou à droite) pour tout $n \geq 1$.*

Corollaire 1.8. *Si K est un corps, alors l'anneau $K[x_1, \dots, x_n]$ est noethérien pour tout $n \geq 1$.*

2. DIVISION MULTIVARIÉE

On fixe un corps K et un entier $n \geq 1$. Notre objectif est de généraliser la division euclidienne de l'anneau $K[x]$ à l'anneau $K[x_1, \dots, x_n]$. Pour ce faire, il nous faut un ordre permettant de définir le terme "de plus haut degré" d'un polynôme multivarié.

Notation 2.1. Si $\alpha \in \mathbb{N}^n$, on pose $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Définition 2.2. Un *ordre monomial* pour $K[x_1, \dots, x_n]$ est une relation $<$ sur l'ensemble $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ des monômes de $K[x_1, \dots, x_n]$ telle que

- (1) la relation $<$ définit un ordre total sur l'ensemble des monômes ;
- (2) si $x^\alpha \leq x^\beta$, alors pour tout $\gamma \in \mathbb{N}^n$, on a que $x^{\alpha+\gamma} \leq x^{\beta+\gamma}$;
- (3) pour tout $\alpha \in \mathbb{N}^n$, on a que $1 \leq x^\alpha$.

Remarque 2.3. (1) On écrira souvent $\alpha \leq \beta$ au lieu de $x^\alpha \leq x^\beta$. Autrement dit, on voit $<$ comme un ordre sur \mathbb{N}^n .

- (2) L'axiome (3) est équivalent à un autre axiome (3') (voir Proposition 2.9), qui est souvent utilisé dans la littérature à la place de (3) pour définir un ordre monomial.

Exemple 2.4. Dans $K[x]$, le seul ordre monomial est celui donné par la suite de relations $1 < x < x^2 < \dots$

Exemple 2.5 (Ordre lexicographique). On pose $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \dots >_{\text{lex}} x_n$, et pour tous $\alpha, \beta \in \mathbb{N}^n$, on pose

$$\begin{aligned} \alpha <_{\text{lex}} \beta &\Leftrightarrow \alpha_1 = \beta_1, \dots, \alpha_{r-1} = \beta_{r-1}, \alpha_r < \beta_r \text{ pour un certain } r; \\ &\Leftrightarrow \text{le coefficient le plus à gauche de } \beta - \alpha \text{ est non nul et positif.} \end{aligned}$$

Par exemple, pour $n = 3$, on a que $x_1^2 >_{\text{lex}} x_1x_2 >_{\text{lex}} x_2^2 >_{\text{lex}} x_3^2x_4x_5$. Il y a aussi une infinité de monômes m tels que $x_1 >_{\text{lex}} m >_{\text{lex}} 1$ (par exemple, x_2^r pour tout r).

Exemple 2.6 (Ordre lexicographique gradué). Pour tout vecteur $\alpha \in \mathbb{N}^n$, on pose $|\alpha| := \sum_{i=1}^n \alpha_i$. On définit $x_1 >_{\text{deglex}} x_2 >_{\text{deglex}} \dots >_{\text{deglex}} x_n$, et pour tous $\alpha, \beta \in \mathbb{N}^n$, on pose

$$\alpha <_{\text{deglex}} \beta \Leftrightarrow (|\alpha| < |\beta|) \text{ ou } (|\alpha| = |\beta| \text{ et } \alpha <_{\text{lex}} \beta).$$

Exemple 2.7. Plus généralement, si $<$ est un ordre monomial, on définit une version graduée de $<$ par

$$\alpha <^g \beta \Leftrightarrow (|\alpha| < |\beta|) \text{ ou } (|\alpha| = |\beta| \text{ et } \alpha < \beta).$$

Exemple 2.8 (Ordre lexicographique renversé gradué). On ordonne les variables par $x_1 >_{\text{degrevlex}} x_2 >_{\text{degrevlex}} \dots >_{\text{degrevlex}} x_n$, et pour tous $\alpha, \beta \in \mathbb{N}^n$, on pose

$$\begin{aligned} \alpha <_{\text{degrevlex}} \beta &\Leftrightarrow (|\alpha| < |\beta|) \text{ ou } (|\alpha| = |\beta| \text{ et } \alpha_n = \beta_n, \dots, \alpha_{r+1} = \beta_{r+1}, \alpha_r > \beta_r \text{ pour un certain } r); \\ &\Leftrightarrow (|\alpha| < |\beta|) \text{ ou } (|\alpha| = |\beta| \text{ et le coefficient non nul le plus à droite de } \beta - \alpha \text{ est négatif}). \end{aligned}$$

Exercice 2.1. Lorsque $n = 2$, les ordres **deglex** et **degrevlex** sont égaux.

Proposition 2.9. Soit $<$ une relation d'ordre sur \mathbb{N}^n satisfaisant aux conditions (1) et (2) de la Définition 2.2. Alors $<$ satisfait à (3) si et seulement si $<$ satisfait à

(3') l'ensemble \mathbb{N}^n muni de $<$ est bien ordonné (c'est-à-dire que tout sous-ensemble non vide de \mathbb{N}^n contient un élément minimal).

Pour démontrer cette proposition, il nous faut faire un détour par les idéaux monomiaux.

Définition 2.10. Un idéal monomial de $K[x_1, \dots, x_n]$ est un idéal engendré par un ensemble de monômes.

Proposition 2.11. Soient $m_1, \dots, m_r \in K[x_1, \dots, x_n]$ des monômes, et soit $I = \langle m_1, \dots, m_r \rangle$ l'idéal monomial qu'ils engendrent. Soit m un autre monôme. Alors $m \in I$ si et seulement si m est divisible par l'un des m_i .

Démonstration. Si m est divisible par l'un des m_i , alors m est bien sûr dans l'idéal I engendré par les m_i . Supposons donc que $m \in I$, et montrons que m est divisible par l'un des m_i .

Comme $m \in I$, il existe des polynômes f_1, \dots, f_r tels que $m = \sum_{i=1}^r f_i m_i$. Puisque m est un monôme, il existe $\alpha \in \mathbb{N}^n$ tel que $m = x^\alpha$. De même, on écrit $m_i = x^{\alpha_i}$ pour chaque i . Enfin, soit λ_i le coefficient devant $x^{\alpha - \alpha_i}$ dans f_i . Alors en étudiant le terme en degré α de la somme $\sum_{i=1}^r f_i m_i$, on obtient que

$$x^\alpha = m = \sum_{i=1}^r \lambda_i x^\alpha.$$

En particulier, au moins l'un des λ_i est non nul, ce qui entraîne que $\alpha - \alpha_i$ doit être dans \mathbb{N}^n . Autrement dit, m_i divise m . \square

Démonstration. (de la Proposition 2.9.) Supposons d'abord que (3') est vrai. Soit $F = \{\alpha \in \mathbb{N}^n \mid x^\alpha < 1\}$. Supposons que F est non vide, et soit $\beta \in F$. Alors (2) entraîne que

$$\dots < x^{3\beta} < x^{2\beta} < x^\beta < 1,$$

et donc $\{x^{m\beta} \mid m \in \mathbb{N}\}$ n'a pas d'élément minimal, contredisant (3'). D'où F est vide et (3) est vérifié.

Supposons maintenant que (3) est vrai. Soit F un ensemble non vide de monômes. Considérons l'idéal $\langle F \rangle$. Par le théorème de la base de Hilbert, il existe un sous-ensemble fini $E = \{m_1, \dots, m_r\}$ de F tel que $\langle E \rangle = \langle F \rangle$. On peut supposer que m_1 est l'élément minimal de E . Par la Proposition 2.11, chaque élément z de F est divisible par l'un des m_i ; en utilisant (3), cela entraîne que $m_i \leq z$. Comme $m_1 \leq m_i$, on en conclut que m_1 est un élément minimal pour F . Donc (3') est vrai. \square

Fixons maintenant un ordre monomial $<$ pour $K[x_1, \dots, x_n]$.

Définition 2.12. Soit $f = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha x^\alpha \in K[x_1, \dots, x_n]$ un polynôme non nul.

- (1) Le *multidegré* de f est $\text{mdeg}(f) = \max_{<} \{\alpha \in \mathbb{N}^n \mid \lambda_\alpha \neq 0\}$.
- (2) Le *coefficient dominant* (en anglais "leading coefficient") de f est $\text{LC}(f) = \lambda_{\text{mdeg}(f)}$.
- (3) Le *monôme dominant* (en anglais "leading monomial") de f est $\text{LM}(f) = x^{\text{mdeg}(f)}$.
- (4) Le *terme dominant* (en anglais "leading term") de f est $\text{LT}(f) = \text{LC}(f) \text{LM}(f)$.

Les propriétés suivantes sont immédiates.

Proposition 2.13. Soient $f, g \in K[x_1, \dots, x_n]$ deux polynômes non nuls. Alors

- (1) $\text{mdeg}(fg) = \text{mdeg}(f) + \text{mdeg}(g)$;
- (2) $\text{LT}(fg) = \text{LT}(f) \text{LT}(g)$; idem pour LC et LM ;
- (3) si $f + g \neq 0$, alors $\text{mdeg}(f + g) \leq \text{mdeg}(f) + \text{mdeg}(g)$;
- (4) si $\text{mdeg}(g) < \text{mdeg}(f)$, alors $f + g \neq 0$ et $\text{mdeg}(f + g) = \text{mdeg}(f)$.

Algorithme de division multivariée. Soit (f_1, \dots, f_r) un r -tuple de polynômes non nuls de $K[x_1, \dots, x_n]$. Soit $f \in K[x_1, \dots, x_n]$. L'algorithme trouve des polynômes $q_1, \dots, q_r, R \in K[x_1, \dots, x_n]$ tels que

- (1) $f = \sum_{i=1}^r q_i f_i + R$, et
- (2) $R = 0$ ou aucun des termes de R n'est divisible par $\text{LT}(f_1), \dots, \text{LT}(f_r)$.

Initialisation. On pose $f^{(0)} = f, q_1^{(0)} = q_1, \dots, q_r^{(0)} = q_r, R^{(0)} = 0$.

Condition d'arrêt à l'étape m . Si $f^{(m)} = 0$, alors poser $q_1 = q_1^{(m)}, \dots, q_r = q_r^{(m)}, R = R^{(m)}$ et terminer.

Étape $m \geq 1$.

— Si $\text{LT}(f_1)$ divise $\text{LT}(f^{(m-1)})$, effectuer

$$f^{(m)} \leftarrow f^{(m-1)} - \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_1)} f_1, \quad q_1^{(m)} \leftarrow q_1^{(m-1)} + \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_1)},$$

$$\text{Pour } i \neq 1, q_i^{(m)} \leftarrow q_i^{(m-1)}, \quad R^{(m)} \leftarrow R^{(m-1)}.$$

— Sinon, si $\text{LT}(f_2)$ divise $\text{LT}(f^{(m-1)})$, effectuer

$$f^{(m)} \leftarrow f^{(m-1)} - \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_2)} f_2, \quad q_2^{(m)} \leftarrow q_2^{(m-1)} + \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_2)},$$

$$\text{Pour } i \neq 2, q_i^{(m)} \leftarrow q_i^{(m-1)}, \quad R^{(m)} \leftarrow R^{(m-1)}.$$

— Sinon, si ...

— Sinon, si $\text{LT}(f_r)$ divise $\text{LT}(f^{(m-1)})$, effectuer

$$f^{(m)} \leftarrow f^{(m-1)} - \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_r)} f_r, \quad q_r^{(m)} \leftarrow q_r^{(m-1)} + \frac{\text{LT}(f^{(m-1)})}{\text{LT}(f_r)},$$

$$\text{Pour } i \neq r, q_i^{(m)} \leftarrow q_i^{(m-1)}, \quad R^{(m)} \leftarrow R^{(m-1)}.$$

— Sinon, effectuer

$$f^{(m)} \leftarrow f^{(m-1)} - \text{LT}(f^{(m-1)}), \quad R^{(m)} \leftarrow R^{(m-1)} + \text{LT}(f^{(m-1)}),$$

pour tout $i, q_i^{(m)} \leftarrow q_i^{(m-1)}$.

Théorème 2.14. *La procédure ci-dessus s'arrête toujours et détermine des polynômes $q_1, \dots, q_r, R \in K[x_1, \dots, x_n]$ tels que*

- (1) $f = \sum_{i=1}^r q_i f_i + R$, et
- (2) $R = 0$ ou aucun des termes de R n'est divisible par $\text{LT}(f_1), \dots, \text{LT}(f_r)$.

Démonstration. Pour montrer que la procédure s'arrête, on utilise le fait que l'ordre monomial $<$ est un bon ordre. Supposons en effet que la procédure ne s'arrête pas. Alors par construction, on a que

$$\dots < \text{LT}(f^{(2)}) < \text{LT}(f^{(1)}) < \text{LT}(f^{(0)}),$$

et donc que l'ensemble $\{\text{LT}(f^{(m)}) \mid m \in \mathbb{N}\}$ n'a pas d'élément minimal, une contradiction.

Pour montrer que l'algorithme renvoie bien des polynômes q_1, \dots, q_r, R satisfaisant à la condition (1), il suffit de montrer par récurrence sur m que l'égalité

$$f^{(m)} + \sum_{i=1}^r q_i^{(m)} f_i + R^{(m)} = f$$

est vérifiée. La condition (2) est satisfaite par construction de R . \square

Notation 2.15. Avec les hypothèses di-cessus, on écrit $\bar{f}^{f_1, \dots, f_r} := R$. Si $F = (f_1, \dots, f_r)$, on écrit aussi $\bar{f}^F := R$.

Remarque 2.16. — L'ordre des f_1, \dots, f_r est important ; les permuter donne lieu à des résultats différents.

- L'algorithme montre l'existence de q_1, \dots, q_r, R satisfaisant aux conditions (1) et (2), mais pas leur unicité. Il ne sont en effet pas uniques. Par exemple, pour l'ordre lexicographique, $f = x_1^2 + x_1x_2 + x_2^2, f_1 = x_1, f_2 = x_1 + x_2$, voici trois écritures de f satisfaisant à (1) et (2) :

$$\begin{aligned} f &= (x_1 + x_2)f_1 + 0 \cdot f_2 + x_2^2 \\ &= 0 \cdot f_1 + x_1f_2 + x_2^2 \\ &= x_1f_1 + x_2f_2 + 0. \end{aligned}$$

- Il est clair que $\bar{f}^F = 0$ entraîne que $f \in \langle F \rangle$, mais l'exemple ci-dessus montre que la réciproque n'est pas nécessairement vraie.
- Le résultat de l'algorithme dépend de l'ordre monomial $<$.

Exercice 2.2. Montrer que si $n = 1$, alors l'algorithme de division multivariée est l'algorithme de division euclidienne dans un anneau de polynômes en une seule variable.

3. BASES DE GRÖBNER

On fixe $K[x_1, \dots, x_n]$ et $<$ un ordre monomial. On rappelle qu'une des motivations du cours est de savoir déterminer si un polynôme f est dans un idéal donné $\langle F \rangle$, où $F = \{f_1, \dots, f_r\}$. On a vu plus haut qu'il se peut que $\bar{f}^F \neq 0$ même si $f \in \langle F \rangle$. On voit ce fait comme un défaut de F . Les F n'ayant pas ce défaut seront appelés des bases de Gröbner.

Définition 3.1 (Bases de Gröbner, première définition). Soit I un idéal de l'anneau $K[x_1, \dots, x_n]$ un idéal non nul. Une *base de Gröbner* de I est un ensemble fini $G \subset I$ tel que $I = \langle G \rangle$ et tel que pour tout $f \in K[x_1, \dots, x_n]$, on a que $f \in I$ si et seulement si $\bar{f}^G = 0$.

Par convention, l'ensemble vide est une base de Gröbner de l'idéal nul.

- Exemple 3.2.** (1) Si $0 \neq g \in K[x_1, \dots, x_n]$, alors $\{g\}$ est une base de Gröbner de $\langle g \rangle$.
- (2) Si m_1, \dots, m_r sont des monômes, alors ils forment une base de Gröbner de l'idéal monomial qu'ils engendrent.

Cette définition a l'inconvénient d'être difficile à vérifier : étant donné un sous-ensemble G de I , comment déterminer s'il s'agit d'une base de Gröbner de I ?

Analysons ce qu'il peut se passer. Comment un ensemble fini $G = \{g_1, \dots, g_r\}$ de générateur de I peut-il **ne pas** être une base de Gröbner de I , avec la définition ci-dessus ? Il faut et il suffit qu'il existe un $f \in I$ tel que $\bar{f}^G \neq 0$. Avec les notations de l'algorithme de division multivariée, cela signifie qu'il existe un $m \in \mathbb{N}$ tel que $\text{LT}(f^{(m)})$ n'est divisible par aucun des $\text{LT}(g_i)$; autrement dit (voir Proposition 2.11), $\text{LT}(f^{(m)}) \notin \langle \text{LT}(g_1), \dots, \text{LT}(g_r) \rangle$.

Ceci nous suggère une autre définition (équivalente) de base de Gröbner. D'abord une notation : si $E \subset K[x_1, \dots, x_n]$, alors $\text{LT}(E) := \{\text{LT}(f) \mid f \in E\}$.

Définition 3.3 (Bases de Gröbner, deuxième définition). Soit I un idéal de l'anneau $K[x_1, \dots, x_n]$ un idéal non nul. Une *base de Gröbner* de I est un ensemble fini $G \subset I$ tel que $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$.

Par convention, l'ensemble vide est une base de Gröbner de l'idéal nul.

Exercice 3.1. Montrer que les deux définitions de bases de Gröbner données ci-dessus sont équivalentes.

Remarque 3.4. (1) Une base de Gröbner de I pour un ordre monomial donné n'en est pas nécessairement une pour un autre ordre monomial.

(2) On ne suppose pas dans la définition que G engendre I ; c'est en fait une conséquence de la définition. En effet, la définition entraîne que si $f \in I$, alors $\bar{f}^G = 0$, ce qui entraîne que $f \in \langle G \rangle$.

(3) Si G est une base de Gröbner de I , alors tout sous-ensemble fini G' de I qui contient G est aussi une base de Gröbner de I ; en particulier, un idéal I non nul admet une infinité de bases de Gröbner (pour $<$ fixé). Nous verrons plus loin que la notion de base de Gröbner *réduite* sert à pallier à ce problème.

Un premier résultat théorique est celui d'existence.

Théorème 3.5. *Tout idéal I de $K[x_1, \dots, x_n]$ admet une base de Gröbner.*

Démonstration. On cherche $G \subset I$ fini tel que $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$. Par le théorème de la base de Hilbert, ce dernier idéal est engendré par un sous-ensemble fini H de $\text{LT}(I)$. Soient $h_1, \dots, h_r \in I$ tels que $H = \{\text{LT}(h_1), \dots, \text{LT}(h_r)\}$; par définition, H est une base de Gröbner de I . \square

Ce théorème d'existence ne nous indique pas comment calculer une base de Gröbner de I . Nous donnons un algorithme dans la section suivante.

4. ALGORITHME DE BUCHBERGER

Étant donné un idéal $I = \langle f_1, \dots, f_r \rangle$, comment calculer une base de Gröbner de I ? Comment savoir si f_1, \dots, f_r forment une base de Gröbner de I ?

On rappelle la définition : un sous-ensemble fini G de I en est une base de Gröbner lorsque $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$. Comment connaître $\text{LT}(I)$? Si on sait que $I = \langle f_1, \dots, f_r \rangle$, alors on sait déjà que $\text{LT}(f_1), \dots, \text{LT}(f_r) \in \text{LT}(I)$. Comment peut-on trouver d'autres éléments de $\text{LT}(I)$, c'est-à-dire d'autres termes dominants de polynômes dans I ?

(1) On peut multiplier f_i par un polynôme q : $\text{LT}(qf_i) = \text{LT}(q)\text{LT}(f_i) \in \text{LT}(I)$. Autrement dit, tout monôme divisible par l'un des $\text{LT}(f_i)$ est dans $\text{LT}(I)$.

(2) De façon moins évidente, on peut prendre des combinaisons linéaires de polynômes f_i et f_j de sorte qu'on en élimine les termes dominants, faisant apparaître un nouveau terme dominant. Ceci se comprend mieux sur un exemple : prenons l'ordre lexicographique, et posons $f_1 = x_2x_3 + x_4$ et $f_2 = x_1x_3 + x_4$. Alors $\text{LT}(f_1) = x_1x_3$ et $\text{LT}(f_2) = x_2x_3$. Mais alors

$$x_1f_1 - x_2f_2 = x_1x_4 - x_2x_4,$$

dont le terme dominant x_1x_4 n'est divisible ni par $\text{LT}(f_1)$ ni par $\text{LT}(f_2)$.

Ce dernier calcul justifie la notation suivante.

Définition 4.1. Soient $f, g \in K[x_1, \dots, x_n]$ non nuls. Le S -polynôme de f et g est

$$S(f, g) = \frac{\text{ppcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)}f - \frac{\text{ppcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)}g.$$

(On choisit toujours le ppcm dont le coefficient dominant est 1.)

Cette notation nous permet d'énoncer un critère pour déterminer si un ensemble est une base de Gröbner.

Théorème 4.2 (Critère de Buchberger). *Soit G un sous-ensemble fini de $K[x_1, \dots, x_n]$ et soit $I = \langle G \rangle$. Alors G est une base de Gröbner de I si et seulement si pour tous $g, h \in G$, on a que $\overline{S(g, h)}^G = 0$.*

La démonstration de ce théorème nécessite quelques résultats préliminaires sur les S -polynômes.

Lemme 4.3. *Soient $f, g \in K[x_1, \dots, x_n]$ non nuls.*

- (1) *Si m, m' sont des monômes non nuls et λ, λ' sont des scalaires non nuls tels que $\lambda m \text{LT}(f) = \lambda' m' \text{LT}(g)$, alors il existe un monôme m'' et un scalaire λ'' tels que*

$$\lambda m f - \lambda' m' g = \lambda'' m'' S(f, g).$$

De plus, $\text{mdeg}(m'' S(f, g)) < \max(\text{mdeg}(m f), \text{mdeg}(m' g))$.

- (2) *Soient f_1, \dots, f_r des polynômes non nuls. Si m_1, \dots, m_r sont des monômes non tous nuls et $\lambda_1, \dots, \lambda_r$ sont des scalaires non tous nuls tels que*

(a) *tous les $m_i f_i$ ont le même multidegré et*

(b) $\sum_{i=1}^r \lambda_i m_i \text{LT}(f_i) = 0$,

alors il existe des monômes m'_1, \dots, m'_{r-1} et des scalaires $\lambda'_1, \dots, \lambda'_{r-1}$ tels que

$$\sum_{i=1}^r \lambda_i m_i f_i = \sum_{i=1}^{r-1} \lambda'_i m'_i S(f_i, f_{i+1}).$$

De plus, $\max_i(\text{mdeg}(m'_i S(f_i, f_{i+1}))) < \max_i(\text{mdeg}(m_i f_i))$.

Démonstration. On montre (1) d'abord. Comme $\lambda m \text{LT}(f) = \lambda' m' \text{LT}(g)$, ce polynôme est un multiple commun de $\text{LM}(f)$ et de $\text{LM}(g)$ et est donc divisible par $\text{ppcm}(\text{LM}(f), \text{LM}(g))$. Il existe donc un monôme m'' et un scalaire λ'' tels que $\lambda m \text{LT}(f) = \lambda' m' \text{LT}(g) = \lambda'' m'' \text{ppcm}(\text{LM}(f), \text{LM}(g))$. D'où

$$\begin{aligned} \lambda m f - \lambda' m' g &= \lambda'' m'' \frac{\text{ppcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} f - \lambda'' m'' \frac{\text{ppcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} g \\ &= \lambda'' m'' S(f, g). \end{aligned}$$

L'inégalité sur les multidegrés s'explique en observant que, par hypothèse, les termes dominants de $\lambda m f$ et de $\lambda' m' g$ s'annulent quand on prend leur différence.

Montrons maintenant (2). Par l'hypothèse (b),

$$0 = \sum_{i=1}^r \lambda_i m_i \text{LT}(f_i) = \sum_{i=1}^r \lambda_i \text{LC}(f_i) m_i \text{LM}(f_i).$$

Aussi, par (a), on a que $m_i \text{LM}(f_i)$ ne dépend pas de i ; posons $H = m_i \text{LM}(f_i)$ pour tout i . Alors

$$0 = \sum_{i=1}^r \lambda_i \text{LC}(f_i) m_i \text{LM}(f_i) = \left(\sum_{i=1}^r \lambda_i \text{LC}(f_i) \right) H,$$

d'où $\sum_{i=1}^r \lambda_i \text{LC}(f_i) = 0$ dans K . Nous allons maintenant utiliser un résultat d'algèbre linéaire : si $\alpha_1, \dots, \alpha_r \in K$ et v_1, \dots, v_r sont des vecteurs dans un espace

vectorel tels que $\sum_{i=1}^r \alpha_i v_i$, alors il existe $\lambda'_1, \dots, \lambda'_{r-1} \in K$ tels que $\sum_{i=1}^r \alpha_i v_i = \sum_{i=1}^{r-1} \lambda'_i (v_i - v_{i+1})$. On applique ce résultat à $\alpha_i = \lambda_i \text{LC}(f_i)$ et $v_i = m_i \frac{f_i}{\text{LC}(f_i)}$; on a alors que

$$\begin{aligned} \sum_{i=1}^r \lambda_i \text{LC}(f_i) m_i \frac{f_i}{\text{LC}(f_i)} &= \sum_{i=1}^{r-1} \lambda'_i \left(m_i \frac{f_i}{\text{LC}(f_i)} - m_{i+1} \frac{f_{i+1}}{\text{LC}(f_{i+1})} \right) \\ &= \sum_{i=1}^{r-1} \left(\frac{\lambda'_i}{\text{LC}(f_i)} m_i f_i - \frac{\lambda'_i}{\text{LC}(f_{i+1})} m_{i+1} f_{i+1} \right). \end{aligned}$$

Or, la partie (1) du lemme s'applique à chaque terme de cette somme : il existe donc λ''_i et m''_i tels que $\left(\frac{\lambda'_i}{\text{LC}(f_i)} m_i f_i - \frac{\lambda'_i}{\text{LC}(f_{i+1})} m_{i+1} f_{i+1} \right) = \lambda''_i m''_i S(f_i, f_{i+1})$, et on a $\text{mdeg}(m''_i S(f_i, f_{i+1})) < \max(\text{mdeg}(m_i f_i, m_{i+1} f_{i+1}))$. Ceci termine la démonstration. \square

Démonstration. (du Théorème 4.2.) Une implication est claire : si G est une base de Gröbner, alors pour tous $g, h \in I$, comme $S(g, h) \in I$, on a bien que $\overline{S(g, h)}^G = 0$.

Montrons la réciproque. Supposons que pour tous $g, h \in G$, $\overline{S(g, h)}^G = 0$. Pour simplifier les notations, supposons que $G = \{g_1, \dots, g_r\}$. On doit montrer que, pour tout $f \in I$, $\text{LT}(f)$ est divisible par l'un des $\text{LT}(g_i)$.

Comme $f \in I = \langle g_1, \dots, g_r \rangle$, il existe des polynômes q_1, \dots, q_r tels que $f = \sum_{i=1}^r q_i g_i$. Soit $\mathbf{m} = \max_i(\text{mdeg}(q_i g_i))$. Forcément, $\text{mdeg}(f) \leq \mathbf{m}$. La preuve se fait par récurrence sur $\mathbf{m} - \text{mdeg}(f)$.

Cas 1 : $\text{mdeg} f = \mathbf{m}$. Alors il existe un i tel que $\text{mdeg}(f) = \text{mdeg}(q_i g_i)$, ce qui entraîne que $\text{LT}(f)$ est divisible par $\text{LT}(g_i)$.

Cas 2 : $\text{mdeg} f < \mathbf{m}$. Quitte à réordonner les g_i , on peut supposer que les s premiers $q_i g_i$ sont de multidegré maximal. Autrement dit, $1 \leq i \leq s$ si et seulement si $\text{mdeg}(q_i g_i) = \mathbf{m}$. Récrivons f :

$$f = \left(\sum_{i=1}^s \text{LT}(q_i) g_i \right) + \left(\sum_{i=1}^s (q_i - \text{LT}(q_i)) g_i + \sum_{i=s+1}^r q_i g_i \right).$$

La somme dans la deuxième parenthèse est constituée de termes de multidegrés strictement inférieurs à \mathbf{m} . La somme dans la première parenthèse satisfait aux conditions du Lemme 4.3 (2); donc il existe des scalaires $\lambda_1, \dots, \lambda_{s-1} \in K$ et des monômes m_1, \dots, m_{s-1} tels que

$$\sum_{i=1}^s \text{LT}(q_i) g_i = \sum_{j=1}^{s-1} \lambda_j m_j S(g_j, g_{j+1})$$

et $\max_j(\text{mdeg}(m_j S(g_j, g_{j+1}))) < \max_i(\text{mdeg}(\text{LT}(q_i) g_i)) = \mathbf{m}$.

Comme $\overline{S(g_j, g_{j+1})}^G = 0$ par hypothèse, on en déduit que $\overline{m_j S(g_j, g_{j+1})}^G = 0$. En appliquant l'algorithme de division multivariée, on peut donc écrire

$$m_j S(g_j, g_{j+1}) = \sum_{i=1}^r q_i^{(j)} g_i,$$

avec chaque terme de la somme de droite de multidegré au plus $\text{mdeg}(m_j S(g_j, g_{j+1})) < \mathbf{m}$. On récrit donc f :

$$f = \left(\sum_{j=1}^{s-1} \sum_{i=1}^r q_i^{(j)} g_i \right) + \left(\sum_{i=1}^s (q_i - \text{LT}(q_i)) g_i + \sum_{i=s+1}^r q_i g_i \right).$$

On a donc récrit f comme une combinaison linéaire des g_i dont chaque terme est de multidegré strictement inférieur à \mathbf{m} . On remplace $\sum_{i=1}^r q_i g_i$ par cette nouvelle expression de f ; la quantité $\mathbf{m} - \text{mdeg}(f)$ a strictement diminué. La preuve par récurrence sur cette différence est terminée. \square

Une conséquence immédiate du critère de Buchberger est un algorithme pour construire une base de Gröbner à partir d'un ensemble de générateurs d'un idéal.

Théorème 4.4 (Algorithme de Buchberger). *Soit G un sous-ensemble fini de $K[x_1, \dots, x_n]$ et soit $I = \langle G \rangle$. Posons $G^{(0)} = G$ et, pour tout $n \geq 0$,*

$$G^{(n+1)} = G^{(n)} \cup \{ \overline{S(f, g)}^{G^{(n)}} \mid f, g \in G^{(n)}, \overline{S(f, g)}^{G^{(n)}} \neq 0 \}.$$

Alors il existe $N \geq 0$ tel que $G^{(N+1)} = G^{(N)}$. Dans ce cas, $G^{(m)} = G^{(N)}$ pour tout $m \geq N$, et $G^{(N)}$ est une base de Gröbner de I .

Démonstration. Il est clair que s'il existe N tel que $G^{(N+1)} = G^{(N)}$, alors $G^{(m)} = G^{(N)}$ pour tout $m \geq N$. De plus, dans ce cas, le critère de Buchberger implique que $G^{(N)}$ est une base de Gröbner de I .

Supposons que $G^{(n+1)} \neq G^{(n)}$ pour tout $n \geq 0$. Alors il existe $f, g \in G^{(n)}$ tels que $\overline{S(f, g)}^{G^{(n)}} \neq 0$. Mais alors $\text{LT}(\overline{S(f, g)}^{G^{(n)}}) \notin \langle \text{LT}(G^{(n)}) \rangle$. Donc on a une inclusion stricte $\langle \text{LT}(G^{(n)}) \rangle \subsetneq \langle \text{LT}(G^{(n+1)}) \rangle$. On a donc une suite strictement croissante d'idéaux $(\langle \text{LT}(G^{(n)}) \rangle)$, contredisant la noéthérianité de l'anneau de polynômes. \square

RÉFÉRENCES

- [Ass97] Ibrahim Assem. *Algèbres et modules*. Enseignement des Mathématiques. Masson, Les presses de l'Université d'Ottawa, 1997.
- [Hil90] David Hilbert. Ueber die theorie der algebraischen formen. *Math. Ann.*, 36(4) :473–534, 1890.
- [Hil78] David Hilbert. *Hilbert's invariant theory papers*, volume VIII of *Lie Groups : History, Frontiers and Applications*. Math Sci Press, Brookline, MA, 1978. Translated from the German by Michael Ackerman, With comments by Robert Hermann.