Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Polynômes multivariés

1 Monômes

Etant donné un *ensemble fini* $\{X_1, \cdots, X_n\}$ d'*indéterminées*, on désignera par

$$\mathbb{F}_1[X_1, \cdots, X_n] = \{\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} / \alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n\}$$

le monoïde commutatif *libre* des monômes relativement aux indéterminées $X_1, \cdots, X_n$ caractérisé par la *propriété universelle* suivante : pour tout monoïde commutatif [1] R, toute application $\varphi : \{X_1, \cdots, X_n\} \longrightarrow R$ se prolonge en un unique homomorphisme $\Phi : \mathbb{F}_1[X_1, \cdots, X_n] \longrightarrow R$.
En particulier [2] $\mathbb{F}_1$ est le *monoïde unité* [3] $\{1\}$.
Le *degré* est l'unique homomorphisme

$$\deg : \mathbb{F}_1[X_1, \cdots, X_n] \longrightarrow \mathbb{N}$$

tel que $\deg(X_i) = 1$ pour $1 \leq i \leq n$ de sorte que $\deg(\mathbf{X}^\alpha) = |\alpha| = \sum_{i=1}^{n} \alpha_i$.
Le *multidegré* est l'unique homomorphisme

$$\mathrm{mdeg} : \mathbb{F}_1[X_1, \cdots, X_n] \longrightarrow \mathbb{N}^n$$

tel que $\mathrm{mdeg}(X_i) = (\delta_{i,j})_{1 \leq j \leq n}$ pour $1 \leq i \leq n$ de sorte que $\mathrm{mdeg}(\mathbf{X}^\alpha) = \alpha$. C'est un isomorphisme de monoïdes dont l'isomorphisme réciproque est :

$$\begin{array}{rcc} \mathbb{N}^n & \longrightarrow & \mathbb{F}_1[X_1, \cdots, X_n] \\ \alpha = (\alpha_1, \cdots, \alpha_n) & \longrightarrow & \mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \end{array}$$

Une partie $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ est un *idéal* si pour tout $M \in \mathbb{F}_1[X_1, \cdots, X_n]$ et tout $E \in \mathfrak{s}$ on a $M\,E \in \mathfrak{s}$.
En particulier si $\mathfrak{s}$ est un idéal de $\mathbb{F}_1[X_1, \cdots, X_n]$ on a $\mathfrak{s} = \mathbb{F}_1[X_1, \cdots, X_n]$ si et seulement si $1 \in \mathfrak{s}$.
Une partie $\mathfrak{b}$ d'un idéal $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ est un *système générateur* de $\mathfrak{s}$ si et seulement si $\mathfrak{s}$ est le plus petit idéal de $\mathbb{F}_1[X_1, \cdots, X_n]$ contenant $\mathfrak{b}$ *ie.* pour tout $E \in \mathfrak{s}$, il existe $B \in \mathfrak{b}$ tel que B *divise* E.

Proposition 1 (Dickson)
Tout idéal $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ possède un système générateur $\mathfrak{b}$ fini.

$\triangledown$ Pour $n = 1$, soit d le plus petit élément de $\{\deg(E)/E \in \mathfrak{s}\}$; $\mathfrak{b} = \{X_1^d\}$ est alors un système générateur de $\mathfrak{s}$.
Supposons, par hypothèse de récurrence, la propriété vraie pour $\mathbb{F}_1[X_1, \cdots, X_{n-1}]$ et considérons un idéal *non trivial* $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$.

1. par exemple le monoïde multiplicatif sous-jacent à une K-algèbre commutative unitaire R.
2. en appliquant la propriété universelle à un ensemble vide d'indéterminées.
3. avatar naïf du mythique *"corps à un élément"*.

L'ensemble $\mathfrak{s}'_\infty$ des $E' \in \mathbb{F}_1[X_1, \cdots, X_{n-1}]$ pour lesquels il existe $k \in \mathbb{N}$ tel que $E'X_n^k \in \mathfrak{s}$ est un idéal de $\mathbb{F}_1[X_1, \cdots, X_{n-1}]$ qui possède donc un système générateur fini $\mathfrak{b}'_\infty$. Il existe alors un entier d tel que $B'X_n^d \in \mathfrak{s}$ pour tout $B' \in \mathfrak{b}'_\infty$.
De même, pour $k \leq d-1$, l'ensemble $\mathfrak{s}'_k$ des $E' \in \mathbb{F}_1[X_1, \cdots, X_{n-1}]$ tels que $E'X_n^k \in \mathfrak{s}$ est un idéal de $\mathbb{F}_1[X_1, \cdots, X_{n-1}]$ qui possède un système générateur fini $\mathfrak{b}'_k$.
Alors l'ensemble :

$$\mathfrak{b} = \{B'X_n^d / B' \in \mathfrak{b}'_\infty\} \cup \bigcup_{k=0}^{d-1} \{B'X_n^k / B' \in \mathfrak{b}'_k\}$$

est un système générateur de $\mathfrak{s}$. Pour $E \in \mathfrak{s}$ on a $E = E'X_n^k$; si $k \geq d$ on a $E' \in \mathfrak{s}'_\infty$ et il existe $B' \in \mathfrak{b}'_\infty$ divisant E' de sorte que $B'X_n^d \in \mathfrak{b}$ divise E tandis que si $k \leq d-1$ on a $E' \in \mathfrak{s}'_k$ et il existe $B' \in \mathfrak{b}'_k$ divisant E' de sorte que $B'X_n^k \in \mathfrak{b}$ divise E. $\triangle$

La *relation de divisibilité* est une relation d'*ordre partiel* dans le monoïde $\mathbb{F}_1[X_1, \cdots, X_n]$; on a :
i) $1|M$ pour tout $M \in \mathbb{F}_1[X_1, \cdots, X_n]$.
ii) $M|N \Rightarrow MP|NP$ pour tout $M, N, P \in \mathbb{F}_1[X_1, \cdots, X_n]$.
Un système générateur $\mathfrak{b}$ d'un idéal $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ est *minimal* si pour tout $B \in \mathfrak{b}$, $\mathfrak{b} \setminus \{B\}$ n'est pas un système générateur de $\mathfrak{s}$.

Corollaire 1
Un système générateur $\mathfrak{b}$ d'un idéal $\mathfrak{s}$ est minimal si et seulement si ses éléments sont deux à deux incomparables pour la relation de divisibilité.

$\triangledown$ Soit $\mathfrak{b}$ un système générateur ; s'il existe $B, B' \in \mathfrak{b}$ avec $B|B'$ alors $\mathfrak{b} \setminus \{B'\}$ est encore un système générateur et $\mathfrak{b}$ n'est pas minimal.
Réciproquement supposons que $\mathfrak{b}$ n'est pas minimal ; il existe $B' \in \mathfrak{b}$ tel que $\mathfrak{b} \setminus \{B'\}$ soit un système générateur de sorte qu'il existe $B \in \mathfrak{b} \setminus \{B'\}$ avec $B|B'$ de sorte que $\mathfrak{b}$ contient des éléments comparables. $\triangle$

Corollaire 2
Tout idéal $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ possède un unique système générateur minimal $\mathfrak{b}$. Ce système générateur minimal $\mathfrak{b}$ est fini. Pour tout système générateur $\mathfrak{b}'$ de $\mathfrak{s}$ on a $\mathfrak{b} \subset \mathfrak{b}'$.

$\triangledown$ Tout d'abord soient $\mathfrak{b}'$ un *système générateur fini* de $\mathfrak{s}$ et $\mathfrak{b}$ l'ensemble (fini) des éléments minimaux (pour la relation de divisibilité) de $\mathfrak{b}'$; un élément $B' \in \mathfrak{b}' \setminus \mathfrak{b}$ n'est pas minimal donc il existe $B \in \mathfrak{b}' \setminus \{B'\}$ tel que $B|B'$; si $B \notin \mathfrak{b}$ on recommence. Finalement en un nombre fini d'étapes on obtient qu'il existe $B \in \mathfrak{b}$ tel que $B|B'$ et par conséquent $\mathfrak{b}$ est un système générateur de $\mathfrak{s}$ et comme les éléments de $\mathfrak{b}$ sont deux à deux incomparables ce système est minimal.
Considérons maitenant un système générateur *quelconque* $\mathfrak{b}'$ de $\mathfrak{s}$; pour $B \in \mathfrak{b}$ il existe donc $B' \in \mathfrak{b}'$ tel que $B'|B$ et il existe $\widetilde{B} \in \mathfrak{b}$ tel que $\widetilde{B}|B'$. Comme $\mathfrak{b}$ est minimal on a $\widetilde{B} = B$ d'où $B = B' \in \mathfrak{b}'$ et finalement $\mathfrak{b} \subset \mathfrak{b}'$. De plus si $\mathfrak{b}$ et $\mathfrak{b}'$ sont tous deux minimaux on a $\mathfrak{b} = \mathfrak{b}'$ $\triangle$

Une relation d'*ordre total* $\preceq$ sur le monoïde $\mathbb{F}_1[X_1, \cdots, X_n]$ est *monomiale*[4] si elle vérifie les conditions :
i) $1 \preceq M$ pour tout $M \in \mathbb{F}_1[X_1, \cdots, X_n]$.
ii) $M \preceq N \Rightarrow MP \preceq NP$ pour tout $M, N, P \in \mathbb{F}_1[X_1, \cdots, X_n]$.
En particulier une relation d'ordre monomiale est *plus fine*[5] que la relation d'ordre de divisibilité.

Proposition 2
L'ensemble $\mathbb{F}_1[X_1, \cdots, X_n]$ muni d'un ordre monomial $\preceq$ est bien ordonné.

4. ou *admissible*
5. si $M|N$ on a $N = MP$; comme $1 \preceq P$ on a $M \preceq MP = N$.

$\triangledown$ Considérons une partie non vide $\mathcal{S}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$. Compte tenu du lemme de Dickson, soit $\mathfrak{b}$ le système générateur *minimal* de l'idéal $\mathfrak{s}$ du monoïde $\mathbb{F}_1[X_1, \cdots, X_n]$. On a $\mathfrak{b} \subset \mathcal{S}$.
En particulier pour tout $S \in \mathcal{S}$ il existe $B \in \mathfrak{b}$ telle que $B|S$ de sorte que $B \preceq S$. Le plus petit élément de $\mathfrak{b}$ est alors le plus petit élément de $\mathcal{S}$. $\triangle$
Exemples d'ordres monomiaux :

* *ordre lexicographique pur :* $\mathbf{X}^\alpha \succ \mathbf{X}^\beta$ si et seulement si on a $\alpha_i > \beta_i$ où i est le plus petit indice tel que $\alpha_i \neq \beta_i$.
* *ordre gradué-lexicographique inversé :* $\mathbf{X}^\alpha \succ \mathbf{X}^\beta$ si et seulement si on a $|\alpha| > |\beta|$ ou bien $|\alpha| = |\beta|$ et $\alpha_i < \beta_i$ où i est le plus grand indice tel que $\alpha_i \neq \beta_i$.

Pour ces ordres on a $X_1 \succ \cdots \succ X_n$.

2 Polynômes

Soit K un corps ; on désigne par $K[X_1, \cdots, X_n]$ l'algèbre des polynômes à coefficients dans K relativement aux indéterminées $X_1, \cdots, X_n$. Elle est caractérisée par la *propriété universelle* suivante : pour toute K-algèbre R (associative, commutative et unitaire), toute application $\varphi : \{X_1, \cdots, X_n\} \longrightarrow R$ se prolonge de manière unique en un K-homomorphisme $\Phi : K[X_1, \cdots, X_n] \longrightarrow R$.
Alors [6] $K[X_1, \cdots, X_n]$ est un K-espace vectoriel de base l'ensemble $\mathbb{F}_1[X_1, \cdots, X_n]$ ce qui signifie qu'un polynôme $f \in K[X_1, \cdots, X_n]$ s'écrit de manière unique :

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathbf{X}^\alpha$$

où pour tout $\alpha \in \mathbb{N}^n$, $c_\alpha \in K$. Si $c_\alpha \neq 0$ on dira que le *monôme* $\mathbf{X}^\alpha$ *figure* dans f et que c_α est son *coefficient*[7]. On définit alors le degré total de f par :

$$\deg(f) = \max\{|\alpha| \,/\, c_\alpha \neq 0\}$$

On *fixe* alors un ordre *monomial* $\preceq$ sur $\mathbb{F}_1[X_1, \cdots, X_n]$.
Etant donné un polynôme *non nul* $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathbf{X}^\alpha \in K[X_1, \cdots, X_n]$, on *ordonne* f selon l'*ordre* $\preceq$ *décroissant* de ses monômes et on définit :

* $\Diamond$ le monôme dominant $\mathrm{lm}_\preceq(f)$ de f comme le plus grand élément pour l'ordre monomial $\preceq$ de l'ensemble des monômes figurant dans f (*ie.* des $\mathbf{X}^\alpha$ tels que $c_\alpha \neq 0$).
* $\Diamond$ le multi-degré $\mathrm{mdeg}_\preceq(f) \in \mathbb{N}^n$ de f comme le multidegré du monôme dominant $\mathrm{lm}_\preceq(f)$.
* $\Diamond$ le coefficient dominant $\mathrm{lc}_\preceq(f)$ de f comme le coefficient du terme dominant $\mathrm{lm}_\preceq(f)$.
* $\Diamond$ le terme dominant $\mathrm{lt}_\preceq(f)$ de f comme le terme $\mathrm{lc}_\preceq(f)\,\mathrm{lm}_\preceq(f)$. On a alors :

$$\mathrm{lt}_\preceq(fg) = \mathrm{lt}_\preceq(f)\mathrm{lt}_\preceq(g)$$

pour $f, g \in K[X_1, \cdots, X_n]$

Soit $\{g_1, \cdots, g_k\}$ un ensemble fini de polynôme de $K[X_1, \cdots, X_n]$, on dit que $f \in K[X_1, \cdots, X_n]$ est *réduit relativement à l'ensemble* [8] $\{g_1, \cdots, g_k\}$ si $f = 0$ ou si *aucun* monôme de f n'est divisible par le monôme dominant $\mathrm{lm}_\preceq(g_i)$ de l'un des g_i, $1 \leq i \leq k$.
L'algorithme de *division euclidienne* se généralise, au cas d'un dividende f et d'un *ensemble ordonné* de diviseurs *non nuls* $[g_1, \cdots, g_k]$; on calcule alors un ensemble ordonné de quotients $[q_1, \cdots, q_k]$ et un reste r tels que [9] :

6. on peut *imaginer* que l'on a "$K[X_1, \cdots, X_n] = \mathbb{F}_1[X_1, \cdots, X_n] \otimes_{\mathbb{F}_1} K$"
7. $c_\alpha \mathbf{X}^\alpha$ est un *terme* de f.
8. dans $K[X]$, f est réduit relativement à $\{g\}$ si $f = 0$ ou si $\deg(f) < \deg(g)$.
9. les quotients $q_1, \cdots, q_k$ et r ne sont pas nécessairement uniques, dépendent en général de l'ordre des diviseurs $g_1, \cdots, g_k$ et on peut avoir $f \in \langle g_1, \cdots, g_k \rangle$ et $r \neq 0$.

1. $f = q_1 g_1 + \cdots + q_k g_k + r$
2. r est *réduit* relativement à $\{g_1, \cdots, g_k\}$
3. $\mathrm{lm}_{\preceq}(q_i g_i) \preceq \mathrm{lm}_{\preceq}(f)$ pour tout $1 \leq i \leq k$ tel que $q_i \neq 0$.

Algorithme 1 (Division multivariée)

1. *entrée : le dividende f, la liste des diviseurs $[g_1, \cdots, g_k]$*
2. *initialisations : $f\_ := f, q_1 := 0, \cdots, q_k := 0, r := 0$*
3. *tant que $f\_ \neq 0$ boucle :*
   {
   s'il existe i, $1 \leq i \leq k$ tel que $\mathrm{lm}_{\preceq}(g_i)$ divise $\mathrm{lm}_{\preceq}(f\_)$ alors
   $T := \dfrac{\mathrm{lt}_{\preceq}(f\_)}{\mathrm{lt}_{\preceq}(g_i)}$
   $q_i := q_i + T$
   $f\_ := f\_ - T\, g_i$
   sinon
   $T := \mathrm{lt}_{\preceq}(f\_)$
   $r := r + T$
   $f\_ = f\_ - T$
   }
4. *sortie : les polynômes $q_1, \cdots, q_k$ et r.*

Proposition 3 (preuve de l'algorithme de division multivariée)

a. terminaison : L'algorithme de division se termine en un nombre fini d'étapes.

b. correction : Etant donnés $f \in A$ et $\boldsymbol{G} = [g_1, \cdots, g_k]$, l'algorithme de division renvoie des polynômes $q_1, \cdots, q_k$ et r tels que

$$f = q_1 g_1 + \cdots + q_k g_k + r$$

où r est $\boldsymbol{G}$-réduit et $\mathrm{lm}_{\preceq}(q_i g_i) \preceq \mathrm{lm}_{\preceq}(f)$ pour tout $1 \leq i \leq k$ tel que $q_i \neq 0$.

$\triangledown$

[terminaison] A l'initialisation de l'algorithme on a $\mathrm{lm}_{\preceq}(f\_) = \mathrm{lm}_{\preceq}(f)$. A chaque étape de la boucle on exécute l'une des affectations $f\_ := f\_ - \dfrac{\mathrm{lt}_{\preceq}(f\_)}{\mathrm{lt}_{\preceq}(g_i)} g_i$ ou $f\_ := f\_ - \mathrm{lt}_{\preceq}(f\_)$, mais on a $\mathrm{lm}_{\preceq}(f\_ - \dfrac{\mathrm{lt}_{\preceq}(f\_)}{\mathrm{lt}_{\preceq}(g_i)} g_i) \prec \mathrm{lm}_{\preceq}(f\_)$ ou bien $\mathrm{lm}_{\preceq}(f\_ - \mathrm{lt}_{\preceq}(f\_)) \prec \mathrm{lm}_{\preceq}(f\_)$. Ainsi la suite $(\mathrm{lm}_{\preceq}(f\_))_{f\_}$ est strictement décroissante et comme l'ensemble $\mathbb{F}_1[X_1, \cdots, X_n]$ muni de l'ordre $\preceq$ est bien-ordonné cette suite est nécessairement finie.

[correction] Montrons que l'expression $f\_ + \sum_{j=1}^{k} q_j g_j + r$ est un *invariant de boucle* de valeur f. C'est vrai lors de l'initialisation.

Si l'on exécute l'affectation $f\_ := f\_ - T g_i$ avec $T = \dfrac{\mathrm{lt}_{\preceq}(f\_)}{\mathrm{lt}_{\preceq}(g_i)}$ on a :

$$\underbrace{f\_ - T g_i}_{f\_} + \sum_{j \neq i} q_j g_j + (\underbrace{q_i + T}_{q_i}) g_i + r = f\_ + \sum_{j=1}^{k} q_j g_j + r = f$$

tandis que si l'on exécute l'affectation $f\_ := f\_ - T$ avec $T = \mathrm{lt}_{\preceq}(f\_)$ on a :

$$\underbrace{f\_ - T}_{f\_} + \sum_{j=1}^{k} q_j g_j + \underbrace{r + T}_{r} = f\_ + \sum_{j=1}^{k} q_j g_j + r = f$$

de sorte qu'à la sortie on a $\sum_{j=1}^{k} q_j g_j + r = f$.
A partir de la valeur initiale $r = 0$, on construit r en lui ajoutant des monômes qui ne sont divisibles par aucun des monômes dominants $\mathrm{lm}_{\preceq}(g_i),\ 1 \leq i \leq k$ de sorte que r est **G**-réduit.
Il reste à montrer que l'on a $\mathrm{lm}_{\preceq}(q_j g_j) \preceq \mathrm{lm}_{\preceq}(f)$ pour tout $1 \leq j \leq k$ tel que $q_j \neq 0$ ce qui est vrai à l'initialisation [10].
A chaque étape si l'on exécute l'affectation $f\_ := f\_ - T g_i$ avec $T = \dfrac{\mathrm{lt}_{\preceq}(f\_)}{\mathrm{lt}_{\preceq}(g_i)}$ les termes $q_j g_j,\ j \neq i$ sont inchangés tandis que $q_i g_i$ est remplacé par $(q_i + T) g_i$ et l'on a

$$\mathrm{lm}_{\preceq}(q_i g_i + T g_i) \preceq \max(\mathrm{lm}_{\preceq}(f), \mathrm{lm}_{\preceq}(f\_)) = \mathrm{lm}_{\preceq}(f)$$

tandis que si l'on exécute l'affectation $f\_ := f\_ - T$ avec $T = \mathrm{lt}_{\preceq}(f\_)$ tous les termes $q_j g_j$, $1 \leq j \leq k$ sont inchangés. $\triangle$

3 Idéaux de l'algèbre $K[X_1, \cdots, X_n]$

Lemme 1
Considérons un ordre monomial $\preceq$ sur $\mathbb{F}_1[X_1, \cdots, X_n]$; pour tout idéal I de $K[X_1, \cdots, X_n]$, $\mathrm{lm}_{\preceq}(I) = \{\mathrm{lm}_{\preceq}(f) \,/\, f \in I \setminus \{0\}\}$ est un idéal de $\mathbb{F}_1[X_1, \cdots, X_n]$.

$\triangledown$ Pour tout $M \in \mathbb{F}_1[X_1, \cdots, X_n]$ et tout $\mathrm{lm}_{\preceq}(f) \in \mathrm{lm}_{\preceq}(I)$ avec $f \in I$, $f \neq 0$, on a $M f \in I$ et par suite $M \mathrm{lm}_{\preceq}(f) = \mathrm{lm}_{\preceq}(M f) \in \mathrm{lm}_{\preceq}(I)$. $\triangle$
On a ainsi une application $I \longrightarrow \mathrm{lm}_{\preceq}(I)$ de l'ensemble des idéaux de $K[X_1, \cdots, X_n]$ dans l'ensemble des idéaux de $\mathbb{F}_1[X_1, \cdots, X_n]$.

Une partie finie $\mathbf{G} = \{g_1, \cdots, g_k\}$ de l'idéal I de la K-algèbre $K[X_1, \cdots, X_n]$ telle que l'ensemble $\mathrm{lm}_{\preceq}(\mathbf{G}) = \{\mathrm{lm}_{\preceq}(g_1), \cdots, \mathrm{lm}_{\preceq}(g_k)\}$ soit un système générateur de l'idéal $\mathrm{lm}_{\preceq}(I)$ du monoïde $\mathbb{F}_1[X_1, \cdots, X_n]$ est appelée une *base de Gröbner* de I.
Ainsi, une partie finie $\boldsymbol{G} = \{g_1, \cdots, g_k\}$ de I est une base de Gröbner de I si et seulement si pour tout $f \in I \setminus \{0\}$, il existe $g_j \in \boldsymbol{G}$ tel que $\mathrm{lm}_{\preceq}(g_j)$ divise $\mathrm{lm}_{\preceq}(f)$.

Lemme 2
Considérons un ordre monomial $\preceq$ sur $\mathbb{F}_1[X_1, \cdots, X_n]$; tout idéal I de $K[X_1, \cdots, X_n]$ possède une base de Gröbner $\boldsymbol{G}$ relativement à l'ordre $\preceq$.

$\triangledown$ En effet, d'après le lemme de Dickson, l'idéal $\mathrm{lm}_{\preceq}(I)$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ possède un système générateur fini. $\triangle$

Lemme 3
Soit $\boldsymbol{G} = \{g_1, \cdots, g_k\}$ une base de Grôbner d'un idéal I de $K[X_1, \cdots, X_n]$ relativement à un ordre monomial $\preceq$ sur $\mathbb{F}_1[X_1, \cdots, X_n]$; alors un monôme $M \in \mathbb{F}_1[X_1, \cdots, X_n]$ est réduit [11] relativement à $\boldsymbol{G}$ si et seulement si $M \in \mathbb{F}_1[X_1, \cdots, X_n] \setminus \mathrm{lm}_{\preceq}(I)$

10. on peut aussi remarquer que si à une étape on a $q_i = 0$, à l'étape suivante on a $q_i = T$ de sorte que $\mathrm{lm}_{\preceq}(q_i g_i) = \mathrm{lm}_{\preceq}(T g_i) = \mathrm{lm}_{\preceq}(f\_) \preceq \mathrm{lm}_{\preceq}(f)$
11. ou *monôme standard* ; ces monômes ne dépendent donc que de l'ordre $\preceq$.

$\triangledown$ On a $M \in \mathrm{lm}_{\preceq}(I)$ si et seulement s'il existe $g_j \in \mathbf{G}$ tel que $\mathrm{lm}_{\preceq}(g_j)|M$ c'est à dire si et seulement si M n'est pas réduit relativement à $\mathbf{G}$. $\triangle$

Proposition 4 (th de la base finie de Hilbert)
Soit $\boldsymbol{G} = \{g_1, \cdots, g_k\}$ une base de Gröbner de I, alors $\boldsymbol{G}$ est un système générateur[12] *de l'idéal I de la K-algèbre $K[X_1 \cdots, X_n]$.*
En particulier tout idéal I de $K[X_1 \cdots, X_n]$ possède un système générateur fini.

$\triangledown$ Soit $f \in I$; par la division multivariée on a :

$$f = q_1 g_1 + \cdots + q_k g_k + r$$

Supposons $r \neq 0$. D'une part on a $r \in I$ donc $\mathrm{lm}_{\preceq}(r) \in \mathrm{lm}_{\preceq}(I)$. D'autre part r est $\mathbf{G}$-réduit de sorte que $\mathrm{lm}_{\preceq}(r) \in \mathbb{F}_1[X_1, \cdots, X_n] \setminus \mathrm{lm}_{\preceq}(I)$. d'où une contradiction et $r = 0$. $\triangle$

Proposition 5 (th de Macaulay)
On considère une base de Grôbner $\boldsymbol{G} = \{g_1, \cdots, g_k\}$, relativement à un ordre monomial $\preceq$, d'un idéal I de $K[X_1, \cdots, X_n]$; le sous-K-espace vectoriel $\mathcal{R}$ des polynômes réduits relativement à $\boldsymbol{G}$ a pour base $\mathbb{F}_1[X_1, \cdots, X_n] \setminus \mathrm{lm}_{\preceq}(I)$. En particulier $\mathcal{R}$ ne dépend que de l'idéal I et de l'ordre monomial $\preceq$ et l'on a[13]

$$I \oplus \mathcal{R} = K[X_1, \cdots, X_n]$$

$\triangledown$ Soit $f \in I \cap \mathcal{R}$; si $f \neq 0$, on aurait $\mathrm{lm}_{\preceq}(f) \in \mathbb{F}_1[X_1, \cdots, X_n] \setminus \mathrm{lm}_{\preceq}(I)$ ce qui n'est pas puisque $\mathrm{lm}_{\preceq}(f) \in \mathrm{lm}_{\preceq}(I)$, donc $I \cap \mathcal{R} = \{0\}$.
Etant donné $f \in K[X_1, \cdots, X_n]$, la division multivariée de f par $g_1, \cdots, g_s$ montre l'existence de $q_1, \cdots, q_s, r \in K[X_1, \cdots, X_n]$ tel que $f = q_1 g_1 + \cdots + q_s g_s + r$ avec $r \in \mathcal{R}$.
$\triangle$
Ainsi l'application K-linéaire canonique :

$$\begin{array}{ccc} \mathcal{R} & \longrightarrow & K[X_1, \cdots, X_n]/I \\ f & \longrightarrow & \overline{f} \end{array}$$

est bijective. Pour tout $f \in K[X_1, \cdots, X_n]$ l'unique polynôme réduit $r \in \mathcal{R}$ tel que :

$$f \equiv r \bmod I$$

est appelé la forme normale de f relativement à I pour l'ordre $\preceq$.

On considère un ordre monomial $\preceq_{X,Y}$ sur $\mathbb{F}_1[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$; on note $\preceq_X$ (*resp.* $\preceq_Y$) l' ordre monomial *induit* sur $\mathbb{F}_1[X_1, \cdots, X_m]$ (*resp.* sur $\mathbb{F}_1[Y_1, \cdots, Y_n]$). On dit que $\prec_{X,Y}$ est un *ordre d'élimination* de $X_1, \cdots, X_m$ si la propriété suivante est vérifiée :

$$M.N \prec_{X,Y} M'.N' \Longleftrightarrow \left\{ \begin{array}{l} M \prec_X M' \\ \quad ou \\ M = M' \text{ et } N \prec_Y N' \end{array} \right.$$

où $M, M' \in \mathbb{F}_1[X_1, \cdots, X_m]$ et $N, N' \in \mathbb{F}_1[Y_1, \cdots, Y_n]$.
Par exemple l'ordre *lexicographique* est un ordre d'élimination tandis que l'ordre *gradué-lexicographique inversé* ne l'est pas.

---

12. *base* signifie *système générateur*, provient du mot allemand *Basis*
13. Ainsi dans la division multivariée $f = q_1 g_1 + \cdots + q_k g_k + r$, où $\{g_1, \cdots, g_k\}$ est une base de Grôbner, le reste $r \in \mathcal{R}$ et le polynôme $q_1 g_1 + \cdots + q_k g_k \in I$ sont uniques et ne dépendent que de l'ordre monomial $\preceq$ et non du choix d'une base de Gröbner relativement à cet ordre.

Lemme 4
Soit $\preceq X,Y$ un ordre d'élimination de $X_1,\cdots,X_m$; pour tout $f \in K[X_1,\cdots,X_m,Y_1,\cdots,Y_n]$ on a $f \in K[Y_1,\cdots,Y_n]$ si et seulement si $\mathrm{lm}_{\preceq X,Y}(f) \in K[Y_1,\cdots,Y_n]$.

$\triangledown$ Tout monôme de $\mathbb{F}_1[X_1,\cdots,X_m,Y_1,\cdots,Y_n]$ qui contient au moins l'une des indéterminées X_j est strictement supérieur à tout monôme $N \in \mathbb{F}_1[Y_1,\cdots,Y_n]$ contenant uniquement les indéterminées $Y_1,\cdots,Y_n$. $\triangle$

Proposition 6 (élimination)
Soit $\boldsymbol{G}$ une base de Gröbner d'un idéal I de $K[X_1,\cdots,X_m,Y_1,\cdots,Y_n]$ pour un ordre d'élimination $\preceq_{X,Y}$ de $X_1,\cdots,X_m$; alors $\boldsymbol{G} \cap K[Y_1,\cdots,Y_n]$ est une base de Gröbner de l'idéal $I \cap K[Y_1,\cdots,Y_n]$ de $K[Y_1,\cdots,Y_n]$ relativement à l'ordre monomial $\preceq_Y$.

$\triangledown$ Soit $f \in I \cap K[Y_1,\cdots,Y_n] \setminus \{0\}$; il existe $g \in \mathbf{G}$ tel que $\mathrm{lm}_{\prec X,Y}(g)$ divise $\mathrm{lm}_{\prec X,Y}(f)$ de sorte que $\mathrm{lm}_{\prec X,Y}(g) \in K[Y_1,\cdots,Y_n]$ et par suite $g \in K[Y_1,\cdots,Y_n]$. Ainsi $g \in \mathbf{G} \cap K[Y_1,\cdots,Y_n]$ et $\mathrm{lm}_{\prec Y}(g)$ divise $\mathrm{lm}_{\prec Y}(f)$. $\triangle$

4 Questions d'unicité

Une base de Gröbner $\mathbf{G}$ d'un idéal I de $K[X_1,\cdots,X_n]$, relativement à un ordre monomial $\preceq$, est *minimale* si pour tout $g \in \mathbf{G}$, $\mathbf{G} \setminus \{g\}$ n'est pas une base de Grôbner de I.

Lemme 5
Soit $\boldsymbol{G}$ une base de Gröbner, relativement à un ordre monomial $\preceq$, d'un idéal I de $K[X_1,\cdots,X_n]$, alors $\boldsymbol{G}$ est minimale si et seulement $\mathrm{lm}_{\preceq}(\boldsymbol{G}) = \{\mathrm{lm}_{\preceq}(g)/g \in \boldsymbol{G}\}$ est le système générateur minimal de l'idéal $\mathrm{lm}_{\preceq}(I)$ du monoïde $\mathbb{F}_1[X_1,\cdots,X_n]$.
De plus I de $K[X_1,\cdots,X_n]$ possède une base de Gröbner minimale.

$\triangle$ Soit $\mathbf{G}$ une base de Gröbner de I ; supposons qu'il existe $g \in \mathbf{G}$ tel que $\mathbf{G} \setminus \{g\}$ soit une base de Grôbner de I ; alors il existe $\tilde{g} \in \mathbf{G} \setminus \{g\}$ tel que $\mathrm{lm}(\tilde{g})$ divise $\mathrm{lm}(g)$ donc $\mathrm{lm}_{\preceq}(\mathbf{G})$ contient deux éléments comparables.
Réciproquement supposons que $\mathrm{lm}_{\preceq}(\mathbf{G})$ contienne deux éléments comparables, par exemple $\mathrm{lm}(\tilde{g})$ qui divise $\mathrm{lm}(g)$, alors $\mathbf{G} \setminus \{g\}$ est une base de Gröbner de I.
Soit $\mathfrak{b}$ l'unique système générateur *minimal* de $\mathrm{lm}_{\preceq}(I)$; si $\mathbf{G}$ est une base de Gröbner de I on a $\mathfrak{b} \subset \mathrm{lm}_{\preceq}(\mathbf{G})$. Pour chaque $M \in \mathfrak{b}$ soit $g_M \in \mathbf{G}$ tel que $\mathrm{lm}(g_M) = M$; $\mathbf{G}_{\min} = \{g_M/M \in \mathfrak{b}\}$ est alors une base de Gröbner minimale de I. $\triangledown$

Une base de Gröbner $\mathbf{G}$ d'un idéal I, relativement à un ordre monomial $\preceq$, est *réduite* si tout $g \in \mathbf{G}$ est unitaire [14] et réduit relativement à $\mathbf{G} \setminus \{g\}$. Une base réduite est évidemment minimale.

Proposition 7
Soit $\preceq$ un ordre monomial sur $\mathbb{F}_1[X_1,\cdots,X_n]$; tout idéal I de $K[X_1,\cdots,X_n]$ possède une unique base de Gröbner réduite $\boldsymbol{G}$ relativement à l'ordre $\preceq$.

$\triangle$ Montrons d'abord *l'unicité*. Soient $\mathbf{G}$ et $\mathbf{H}$ deux bases de Grôbner réduites de I ; puisqu'elles sont minimales on a :

$$\mathrm{lm}_{\preceq}(\mathbf{G}) = \mathrm{lm}_{\preceq}(\mathbf{H})$$

Supposons qu'il existe $g \in \mathbf{G} \setminus \mathbf{H}$; il existe $h \in \mathbf{H}$ tel que $\mathrm{lm}(g) = \mathrm{lm}(h)$ d'où $\mathrm{lt}(g) = \mathrm{lt}(h)$ puisque g et h sont unitaires.

14. lorsque $K = \mathrm{Frac}(A)$, avec A factoriel, on peut supposer que g est primitif plutôt qu'unitaire.

On a $g-h \in I \setminus \{0\}$ et il existe $g_1 \in \mathbf{G}$ tel que $\mathrm{lm}(g_1)$ divise $\mathrm{lm}(g-h)$. On a $g_1 \neq g$ puisque $\mathrm{lm}(g_1) \preceq \mathrm{lm}(g-h) \prec \mathrm{lm}(g)$ et $\mathrm{lm}(g_1)$ divise un monôme $N \prec \mathrm{lm}(h)$ figurant dans h puisque $\mathbf{G}$ est réduite.
Mais il existe $h_1 \in \mathbf{H}$ tel que $\mathrm{lm}(h_1) = \mathrm{lm}(g_1)$. On a $h_1 \neq h$; si on avait $h_1 = h$ on aurait $\mathrm{lm}(h_1) = \mathrm{lm}(h) = \mathrm{lm}(g_1) = \mathrm{lm}(g)$ or $\mathrm{lm}(g_1) \prec \mathrm{lm}(g)$. Ainsi $\mathrm{lm}(h_1)$ divise N ce qui contredit $\mathbf{H}$ réduite.
Il reste à établir *l'existence*. Soit $\mathbf{G}$ une base de Gröbner minimale de I dont tous les éléments sont unitaires ; on a $\mathrm{lm}_\preceq(\mathbf{G}) = \mathfrak{b}$ où $\mathfrak{b}$ est le système générateur *minimal* de $\mathrm{lm}_\preceq(I)$.
Pour $g \in \mathbf{G}$ soit $\widetilde{g}$ le reste de la division multivariée de g par $\mathbf{G} \setminus \{g\}$: on a donc :

$$g = \sum_{g' \in \mathbf{G} \setminus \{g\}} q_{g'} g' + \widetilde{g}$$

avec $\widetilde{g}$ réduit relativement à $\mathbf{G} \setminus \{g\}$ et $\mathrm{lm}(q_{g'} g') \preceq \mathrm{lm}(g)$ pour tout $g' \in \mathbf{G} \setminus \{g\}$. On a ainsi :

$$\mathrm{lm}(g) \preceq \max(\mathrm{lm}(\widetilde{g}), \mathrm{lm}(q_{g'} g')/g' \in \mathbf{G} \setminus \{g\}$$

S'il existait $g' \in \mathbf{G} \setminus \{g\}$ tel que $\mathrm{lm}(q_{g'} g') = \mathrm{lm}(g)$, on aurait que $\mathrm{lm}(g') | \mathrm{lm}(g)$ ce qui contredirait le fait que $\mathbf{G}$ est minimale. On a donc $\mathrm{lm}(q_{g'} g') \prec \mathrm{lm}(g)$ pour tout $g' \in \mathbf{G} \setminus \{g\}$ et finalement $\mathrm{lm}(\widetilde{g}) = \mathrm{lm}(g)$ de sorte que si on pose :

$$\widetilde{\mathbf{G}} = \mathbf{G} \setminus \{g\} \cup \{\widetilde{g}\}$$

on a $\mathrm{lm}_\preceq(\widetilde{\mathbf{G}}) = \mathfrak{b}$; $\widetilde{\mathbf{G}}$ est une base de Gröbner minimale de I avec $\widetilde{g}$ réduit relativement à $\widetilde{\mathbf{G}} \setminus \{\widetilde{g}\} = \mathbf{G} \setminus \{g\}$. De plus tout élément $g' \neq g$ de $\mathbf{G}$ qui était réduit relativement à $\mathbf{G} \setminus \{g'\}$, reste réduit relativement à $\widetilde{\mathbf{G}} \setminus \{g'\}$ puisque $\mathrm{lm}(\widetilde{g}) = \mathrm{lm}(g)$.
Ainsi $\{\widetilde{g}/g \in \mathbf{G}\}$ est une base de Gröbner réduite de I. $\triangledown$

5 Aspects effectifs

5.1 Le critère de Buchberger

Soient $f, g \in K[X_1, \cdots, X_n]$; le S-polynôme (polynôme de *syzygy*) associé est défini par :

$$\begin{aligned} S_\preceq(f,g) &= \frac{\mu}{\mathrm{lt}_\preceq(f)} f - \frac{\mu}{\mathrm{lt}_\preceq(g)} g \\ &= \frac{\mathrm{lm}_\preceq(g)}{\mathrm{lc}_\preceq(f)\delta} f - \frac{\mathrm{lm}_\preceq(f)}{\mathrm{lc}_\preceq(g)\delta} g \end{aligned}$$

où on a posé $\mu = \mathrm{ppcm}(\mathrm{lm}_\preceq(f), \mathrm{lm}_\preceq(g))$ et $\delta = \mathrm{pgcd}(\mathrm{lm}_\preceq(f), \mathrm{lm}_\preceq(g))$
de sorte que $\mu\,\delta = \mathrm{lm}_\preceq(f)\mathrm{lm}_\preceq(g)$ (avec $\mathrm{lt}(f) = \mathrm{lc}_\preceq(f)\mathrm{lm}_\preceq(f)$ et $\mathrm{lt}(g) = \mathrm{lc}_\preceq(g)\mathrm{lm}_\preceq(g)$).

Lemme 6
Soient $f, g \in K[X_1, \cdots, X_n]$; on a $\mathrm{lm}_\preceq(S_\preceq(f,g)) \prec \mu$.

$\triangledown$ Il suffit de remarquer que :

$$S_\preceq(f,g) = \frac{\mathrm{lm}_\preceq(g)}{\mathrm{lc}_\preceq(f)\delta}(f - \mathrm{lt}_\preceq(f)) - \frac{\mathrm{lm}_\preceq(f)}{\mathrm{lc}_\preceq(g)\delta}(g - \mathrm{lt}_\preceq(g))$$

et que $\mathrm{lm}_\preceq(f - \mathrm{lt}_\preceq(f)) \prec \mathrm{lm}_\preceq(f)$, $\mathrm{lm}_\preceq(g - \mathrm{lm}_\preceq(g)) \prec \mathrm{lm}_\preceq(g)$ $\triangle$

On considère la sous-algèbre de $K(X_1, \cdots, X_n)$

$$K[X_1^{\pm 1}, \cdots, X_n^{\pm 1}] = \{\frac{f}{M} \,/\, f \in K[X_1, \cdots, X_n], M \in \mathbb{F}_1[X_1, \cdots, X_n]\}$$

contenant $K[X_1, \cdots, X_n]$ et l'application K-bilinéaire :

$$\begin{array}{rcl} K^r \times K[X_1^{\pm 1}, \cdots, X_n^{\pm 1}]^r & \longrightarrow & K[X_1^{\pm 1}, \cdots, X_n^{\pm 1}] \\ (\underline{s} = (s_k)_{1 \leq k \leq r}, \underline{\varphi} = (\varphi_k)_{1 \leq k \leq r} & \longrightarrow & \langle \underline{s}, \underline{\varphi} \rangle = \sum_{k=1}^{r} s_k \varphi_k \end{array}$$

Lemme 7
Soient $\boldsymbol{F} = \{f_1, \cdots, f_r\} \subset K[X_1, \cdots, X_n] \setminus \{0\}$ *et* $a_i = \mathrm{lc}_{\preceq}(f_i)$ *pour* $1 \leq i \leq r$. *considérons :*

$$h = \sum_{1 \leq k \leq r} s_k M_k f_k$$

où $s_k \in K$, $M_k \in \mathbb{F}_1[X_1, \cdots, X_n]$, *avec* $\mathrm{lm}_{\preceq}(M_k f_k) = M$ *pour* $1 \leq k \leq r$. *Alors si* $\mathrm{lm}_{\preceq}(h) \prec M$, *on a :*

$$h = \sum_{1 \leq i < j \leq r} s_{i,j} M_{i,j} S_{\preceq}(f_i, f_j)$$

avec $s_{i,j} \in K$, $M_{i,j} \in \mathbb{F}_1[X_1, \cdots, X_n]$ *et* $\mathrm{lm}_{\preceq}(M_{i,j} S_{\preceq}(f_i, f_j)) \prec M$ *pour* $1 \leq i, j \leq r$.

$\triangledown$ On a $0 = \sum\limits_{1 \leq k \leq r} s_k \,\mathrm{lm}_{\preceq}(M_k f_k) = (\sum\limits_{1 \leq k \leq r} s_k a_k) M$ de sorte que $\underline{s} = (s_1, \cdots, s_r) \in \mathrm{Ker}(\phi)$ où ϕ est la forme K-linéaire sur K^r :

$$\phi : \underline{s} = (s_1, \cdots, s_r) \longrightarrow a_1 s_1 + \cdots a_r s_r$$

définie par $a_i = \phi(e_i) \neq 0$ pour $1 \leq i \leq r$ où $(e_i)_{1 \leq i \leq r}$ est la base canonique de K^r. Alors $\mathrm{Ker}(\phi)$ est un hyperplan de K^r et un *système générateur* de cet hyperplan est constitué par les vecteurs $\underline{\epsilon}_{i,j} = a_i^{-1} e_i - a_j^{-1} e_j$, pour $1 \leq i < j \leq r$.
On a donc $\underline{s} = \sum\limits_{1 \leq i < j \leq r} s_{i,j} \underline{\epsilon}_{i,j}$ avec $s_{i,j} \in K$. Posons :

$$\underline{\varphi} = (\frac{f_k}{\mathrm{lm}_{\preceq}(f_k)})_{1 \leq k \leq r} \in K[X_1^{\pm 1}, \cdots, X_n^{\pm 1}]^r$$

de sorte que :

$$h = \langle \underline{s}, M\underline{\varphi} \rangle = \sum_{1 \leq i < j \leq r} s_{i,j} \langle \underline{\epsilon}_{i,j}, M\underline{\varphi} \rangle$$

Pour $1 \leq i < j \leq r$ posons $\mu_{i,j} = \mathrm{ppcm}(\mathrm{lm}_{\preceq}(f_i), \mathrm{lm}_{\preceq}(f_j))$; comme $\mathrm{lm}_{\preceq}(f_i)$ et $\mathrm{lm}_{\preceq}(f_j)$ divisent M, $\mu_{i,j}$ divise M de sorte qu'il existe $M_{i,j} \in \mathbb{F}_1[X_1, \cdots, X_n]$ tel que

$$M = \mu_{i,j} M_{i,j}$$

d'où :

$$\begin{array}{rcl} h & = & \sum\limits_{1 \leq i < j \leq r} s_{i,j} \langle \underline{\epsilon}_{i,j}, \mu_{i,j} M_{i,j} \underline{\varphi} \rangle \\ & = & \sum\limits_{1 \leq i < j \leq r} s_{i,j} \langle a_i^{-1} e_i - a_j^{-1} e_j, \mu_{i,j} M_{i,j} \underline{\varphi} \rangle \\ & = & \sum\limits_{1 \leq i < j \leq r} s_{i,j} M_{i,j} \left(a_i^{-1} \langle e_i, \mu_{i,j} \underline{\varphi} \rangle - a_j^{-1} \langle e_j, \mu_{i,j} \underline{\varphi} \rangle \right) \\ & = & \sum\limits_{1 \leq i < j \leq r} s_{i,j} M_{i,j} \left(a_i^{-1} \mu_{i,j} \varphi_i - a_j^{-1} \mu_{i,j} \varphi_j \right) \\ & = & \sum\limits_{1 \leq i < j \leq r} s_{i,j} M_{i,j} S_{\preceq}(f_i, f_j) \end{array}$$

On a, d'après le lemme précédent :

$$\mathrm{lm}_{\preceq}(M_{i,j}S_{\preceq}(f_i,f_j)) \prec M_{i,j}\mu_{i,j} = M$$

$\triangle$

Tout d'abord notons que l'on a la caractérisation suivante des systèmes générateurs qui sont des bases de Gröbner :

Proposition 8
Un système générateur $\boldsymbol{G} = \{g_1, \cdots, g_s\}$ *d'un idéal* I *de* $K[X_1, \cdots, X_n]$ *est une base de Gröbner de* I *si et seulement si, pour tout* $f \in I$ *on a :*

$$f = \sum_{k=1}^{s} q_k\, g_k \text{ avec } \mathrm{lm}_{\preceq}(q_k\, g_k) \preceq \mathrm{lm}_{\preceq}(f) \text{ pour tout } k \text{ tel que } q_k \neq 0$$

$\nabla \Rightarrow$ Si $\mathbf{G}$ est une base de Gröbner de I, pour tout $f \in I$, le reste de la division multivariée de f par $\mathbf{G}$ est nul.
$\Leftarrow$ Soit $f \in I$; on a donc $f = \sum_{k=1}^{s} q_k\, g_k$ avec $\mathrm{lm}_{\preceq}(q_k\, g_k) \preceq \mathrm{lm}_{\preceq}(f)$ pour $1 \leq k \leq s$. Si l'on avait $\mathrm{lm}_{\preceq}(q_k\, g_k) \neq \mathrm{lm}_{\preceq}(f)$ pour tout $1 \leq k \leq s$ on aurait évidemment $\sum_{k=1}^{s} \mathrm{lm}_{\preceq}(q_k\, g_k) \prec \mathrm{lm}_{\preceq}(f)$. Ainsi il existe k tel que $\mathrm{lm}_{\preceq}(q_k\, g_k) = \mathrm{lm}_{\preceq}(f)$ *ie.* $\mathrm{lm}_{\preceq}(g_k)$ *divise* $\mathrm{lm}_{\preceq}(f)$. Ainsi $\mathbf{G}$ est une base de Gröbner de I. $\triangle$

Proposition 9 (Critère de Buchberger)
Un système générateur $\boldsymbol{G} = \{g_1, \cdots, g_s\}$ *d'un idéal* I *de* $K[X_1, \cdots, X_n]$ *est une base de Gröbner de* I *si et seulement si, pour tout* $i < j$ *on a :*

$$S_{\preceq}(g_i, g_j) = \sum_{k=1}^{s} q_{i,j,k} g_k \text{ avec } \mathrm{lm}_{\preceq}(q_{i,j,k}\, g_k) \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(g_i, g_j)) \text{ pour tout } i,j,k \text{ tel que } q_{i,j,k} \neq 0$$

$\nabla \Rightarrow$ On a $S_{\preceq}(g_i, g_j) \in I$ donc si $\mathbf{G}$ est une base de Gröbner de I, le reste de la division multivariée de $S_{\preceq}(g_i, g_j)$ par $\mathbf{G}$ est nul.
$\Leftarrow$ On considère $f \in I$. Puisque $\mathbf{G} = \{g_1, \cdots, g_s\}$ est un système générateur de I, on a une écriture $f = \sum_{i=1}^{s} h_i\, g_i$ avec $h_i \in K[X_1, \cdots, X_n]$ et comme $\mathbb{F}_1[X_1, \cdots, X_n]$ est *bien ordonné* par l'ordre monomiale $\preceq$ on peut supposer que $M = \max(\mathrm{lm}_{\preceq}(h_i g_i)/1 \leq i \leq s)$ *minimal.*
Supposons que $M \succ \mathrm{lm}_{\preceq}(f)$; on a alors :

$$f = \sum_{i=1}^{r} \mathrm{lm}_{\preceq}(h_i)\, g_i + \underbrace{\sum_{i=1}^{r} (h_i - \mathrm{lm}_{\preceq}(h_i))\, g_i + \sum_{i=r+1}^{s} h_i\, g_i}_{=F}$$

avec $\mathrm{lm}_{\preceq}(h_i g_i) = M$ pour tout $i,\ 1 \leq i \leq r$ et $\mathrm{lm}_{\preceq}(h_i g_i) \prec M$ pour tout $i,\ r+1 \leq i \leq s$.
Notons que l'on a $\mathrm{lm}_{\preceq}\left((h_i - \mathrm{lm}_{\preceq}(h_i))g_i\right) \prec M$ pour tout $i,\ 1 \leq i \leq r$ En utilisant le lemme précédent on obtient que :

$$f = \sum_{i,j=1}^{r} s_{i,j} M_{i,j}\, S_{\preceq}(g_i, g_j) + F$$

avec $s_{i,j} \in K$, $M_{i,j} \in \mathbb{F}_1[X_1, \cdots, X_n]$ et $\mathrm{lm}_{\preceq}(M_{i,j} S_{\preceq}(g_i, g_j)) \prec M$ pour $1 \leq i, j \leq r$.
Or par hypothèse on a :

$$S_{\preceq}(g_i, g_j) = \sum_{k=1}^{s} q_{i,j,k}\, g_k$$

avec $q_{i,j,k} \in K[X_1, \cdots, X_n]$ et $\mathrm{lm}_{\preceq}(q_{i,j,k}\, g_k) \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(g_i, g_j))$ pour tout i, j, k de sorte que :

$$f = \sum_{i,j=1}^{r} s_{i,j} M_{i,j} \, (\sum_{l=1}^{r} q_{i,j,l}\, g_l) + \sum_{k=1}^{r} (h_k - \mathrm{lm}_{\preceq}(h_k))\, g_k + \sum_{k=r+1}^{s} h_k\, g_k$$

avec $\mathrm{lm}_{\preceq}(M_{i,j} q_{i,j,k}\, g_k) \preceq \mathrm{lm}_{\preceq}(M_{i,j} S_{\preceq}(g_i, g_j)) \prec M$ d'où une contradiction avec la minimalité de M.
Ainsi on a $M \preceq \mathrm{lm}_{\preceq}(f)$ et le système générateur $g_1, \cdots, g_s$ est une base de Grôbner. $\triangle$

Corollaire 3
Un système générateur fini $\boldsymbol{G}$ *d'un idéal* I *de* $K[X_1, \cdots, X_n]$ *tel que les monômes dominants* $\mathrm{lm}_{\preceq}(g)$ *pour* $g \in \boldsymbol{G}$ *sont deux à deux premiers entre eux est une base de Gröbner de* I *pour l'ordre monomial* $\preceq$.

$\triangledown$ On peut évidemment supposer les polynômes unitaires. Soient $f, g \in \mathbf{G}$ avec $f \neq g$; on a :

$$\begin{aligned} S_{\preceq}(f,g) &= \mathrm{lm}_{\preceq}(g) f - \mathrm{lm}_{\preceq}(f) g \\ &= \mathrm{lm}_{\preceq}(g)(f - \mathrm{lm}_{\preceq}(f)) - \mathrm{lm}_{\preceq}(f)(g - \mathrm{lm}_{\preceq}(g)) \end{aligned}$$

Les monômes figurant dans la dernière expression sont deux à deux distincts car si l'on avait par exemple $\mathrm{lm}_{\preceq}(g)P = \mathrm{lm}_{\preceq}(f)M$ où P figure dans $f - \mathrm{lm}_{\preceq}(f)$ et M figure dans $g - \mathrm{lm}_{\preceq}(g)$, on aurait $\mathrm{lm}_{\preceq}(f)M$ multiple de $\mathrm{lm}_{\preceq}(f)$ et de $\mathrm{lm}_{\preceq}(g)$ donc du produit (puisque ces monômes sont premiers entre eux) de sorte que :

$$\mathrm{lm}_{\preceq}(f)\mathrm{lm}_{\preceq}(g) \preceq \mathrm{lm}_{\preceq}(f)M$$

et par suite :

$$\mathrm{lm}_{\preceq}(g) \preceq M$$

ce qui est contradictoire.
On a donc $\mathrm{lm}_{\preceq}(g)P \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(f,g))$ (*resp.* $\mathrm{lm}_{\preceq}(f)M \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(f,g))$) pour tout monôme P (*resp.* M) figurant dans $f - \mathrm{lm}_{\preceq}(f)$ (*resp.* $g - \mathrm{lm}_{\preceq}(g)$).
On a donc $\mathrm{lm}_{\preceq}((f - \mathrm{lm}_{\preceq}(f))g) \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(f,g))$ (*resp.* $\mathrm{lm}_{\preceq}((g - \mathrm{lm}_{\preceq}(g))f) \preceq \mathrm{lm}_{\preceq}(S_{\preceq}(f,g))$).
comme on a :

$$S_{\preceq}(f,g) = (f - \mathrm{lm}_{\preceq}(f))g - (g - \mathrm{lm}_{\preceq}(g))f$$

le critère de Buchberger est vérifié. $\triangle$

5.2 Algorithme de Buchberger

Tout d'abord une version sommaire de l'algorithme de Buchsberger qui permet de calculer une base de Gröbner d'un idéal I pour un ordre monomial $\preceq$ à partir d'un système générateur fini de l'idéal I.

Algorithme 2

1. *entrée :* $\boldsymbol{F} = \{f_1, \cdots, f_r\}$ *système générateur fini de* I
2. *initialisations :*
   (a) $\boldsymbol{G} := \boldsymbol{F}$
   (b) $\mathfrak{G} := \{\{f, g\} / f, g \in \boldsymbol{G}\}$
3. *boucle tant que :* $\mathfrak{G} \neq \emptyset$ *:*
   (a) *choisir* $\{f, g\} \in \mathfrak{G}$

(b) $\mathfrak{G} := \mathfrak{G} \setminus \{\{f,g\}\}$

(c) calculer le reste r *de la division multivariée de* $S_\preceq(f,g)$ *par* $\boldsymbol{G}$

(d) si $r \neq 0$ *alors :*

$\mathfrak{G} := \mathfrak{G} \cup \{\{r,h\}/h \in \boldsymbol{G}\}$

$\boldsymbol{G} := \boldsymbol{G} \cup \{r\}$

sortie : $\boldsymbol{G}$ *base de Gröbner de* I

Proposition 10
L'algorithme de Buchberger se termine et permet de calculer une base de Gröbner $\boldsymbol{G}$ *de* I *à partir d'un système générateur fini de* I*.*

$\triangledown$ *terminaison* : Soit $(\mathbf{G}_k)_k$ la suite des valeurs successives[15] de $\mathbf{G}$; si la boucle était infinie il existerait une suite strictement croissante d'entiers $(k_i)_i$ telle que $\mathbf{G}_{k_i} = \mathbf{G}_{k_{i-1}} \cup \{r_i\}$ avec r_i réduit[16] relativement à $\mathbf{G}_{k_{i-1}}$ et $r_i \neq 0$. En particulier, pour tout i, le monôme $\mathrm{lm}_\preceq(r_i)$ ne serait divisible par aucun des monômes $\mathrm{lm}_\preceq(r_j)$ avec $j < i$ ce qui n'est pas possible puisque le système générateur minimal[17] $\mathfrak{b}$ de l'idéal $\mathfrak{s}$ de $\mathbb{F}_1[X_1, \cdots, X_n]$ engendré par $\mathfrak{b}' = \{\mathrm{lm}_\preceq(r_i)\,/\,i \geq 0\}$ est fini et vérifie $\mathfrak{b} \subset \mathfrak{b}'$.
correction : On a $\mathbf{F} \subset \mathbf{G} \subset I$ de sorte que $\mathbf{G}$ est un système générateur de I. D'autre part, pour que $\mathfrak{G} = \emptyset$ il faut que pour tout $f, g \in \mathbf{G}$, $f \neq g$ le reste de la division multivariée de $S_\preceq(f,g)$ par $\mathbf{G}$ soit nul. Le critère de Buchberger montre alors que $\mathbf{G}$ est une base de Gröbner de I. $\triangle$

L'algorithme suivant permet de déterminer une base minimale à partir d'une base quelconque.

Algorithme 3

1. *entrée :* $\boldsymbol{G}$ *base de Gröbner de l'idéal* I *pour l'ordre* $\preceq$
2. *initialisation :* $\boldsymbol{G}_{min} := \emptyset$
3. *boucle pour :* $f \in \boldsymbol{G}$ *:*
   (a) soit $M := \mathrm{lm}_\preceq(f)$
   (b) s'il n'existe aucun $g \in \boldsymbol{G} \setminus \{f\}$ *tel que* $\mathrm{lm}_\preceq(g) | M$ *:*
   $\boldsymbol{G}_{min} := \boldsymbol{G}_{min} \cup \{f\}$
4. *sortie* $\boldsymbol{G}_{min}$ *base de Gröbner minimale de* I

Proposition 11
L'algorithme permet de calculer une base minimale $\boldsymbol{G}_{min}$ *de* I *à partir d'une base de Gröbner.*

$\triangledown$ *terminaison* : la boucle est énumérée par l'ensemble fini $\mathbf{G}$.
correction : $\mathrm{lm}_\preceq(\mathbf{G}_{min})$ est l'ensemble des éléments minimaux de $\mathrm{lm}_\preceq(\mathbf{G})$ qui est un système générateur de l'idéal $\mathrm{lm}_\preceq(I)$. Il en résulte que $\mathrm{lm}_\preceq(\mathbf{G}_{min})$ est le système générateur minimal de $\mathrm{lm}_\preceq(I)$ de sorte que $\mathbf{G}_{min}$ est une base de Gröbner minimale de I. $\triangle$

Ce dernier algorithme permet de déterminer la base réduite à partir d'une base minimale.

Algorithme 4

1. *entrée :* $\boldsymbol{G}_{min}$ *base de Gröbner minimale de* I*, pour l'ordre monomial* $\preceq$
2. *initialisation :* $\boldsymbol{G}_{red} := \emptyset$

15. on a $\mathbf{G}_0 = \mathbf{F}$.
16. *ie.* aucun des monômes figurant dans r_i divisible par l'un des monômes $\mathrm{lm}_\preceq(g)$ pour $g \in \mathbf{G}_{k_{i-1}}$.
17. qui est fini

3. *boucle pour* $g \in \boldsymbol{G}_{min}$ *:*
   (a) *calculer le reste* $\widetilde{g}$ *de la division multivariée de* g *par* $\boldsymbol{G}_{min} \setminus \{g\}$
   (b) *normaliser* $\widetilde{g}$ *en divisant par* $\mathrm{lc}_{\preceq}(\widetilde{g})$
   (c) $\boldsymbol{G}_{red} := \boldsymbol{G}_{red} \cup \{\widetilde{g}\}$
4. *sortie :* $\boldsymbol{G}_{red}$ *base de Gröbner réduite de* I

Proposition 12
L'algorithme permet de calculer une base de Gröbner réduite $\boldsymbol{G}_{red}$ *de* I *à partir d'une base minimale.*

$\triangledown$ *terminaison* : la boucle est énumérée par l'ensemble fini $\mathbf{G}_{min}$.
correction : pour tout $g \in g \in \mathbf{G}_{min}$ on a $\mathrm{lm}_{\preceq}(\widetilde{g}) = \mathrm{lm}_{\preceq}(g)$ de sorte que $\mathbf{G}_{red}$ est une base minimale et tout $\widetilde{g} \in \mathbf{G}_{red}$ est réduit relativement à $\mathbf{G}_{red} \setminus \{\widetilde{g}\}$. $\triangle$