Chapitre VI

L'algorithme de Burchberger et le calcul de bases de Gröbner pour un idéal

1. Ordre total sur $\mathbf{N}^n$, sous-ensembles de $\mathbf{N}^n$ et leurs frontières

1.1. Définitions. On dit qu'un sous-ensemble E de $\mathbf{N}^n$ est *saturé par translation positive* si $E \neq \emptyset$ et si, pour tout $\alpha \in E$ et tout $\beta \in \mathbf{N}^n$, $\alpha + \beta \in E$.

On appelle *frontière* de E tout sous-ensemble F de E tel que pour tout $\alpha \in E$, il existe $\alpha_0 \in F$ et $\beta \in \mathbf{N}^n$ tels que $\alpha = \alpha_0 + \beta$.

1.2. Proposition. *Soit E un sous-ensemble de $\mathbf{N}^n$ saturé par translation positive. Il existe une partie finie F de E qui est frontière de E.*

Démonstration. On effectue une récurrence sur n. La propriété est évidemment vraie si $n = 1$ (il suffit de prendre pour F l'ensemble ayant pour seul élément la borne inférieure de E). Supposons la propriété vraie pour $1 \leq n \leq m-1$, et montrons qu'elle l'est pour $n = m$. Soit E une partie de $\mathbf{N}^m$ saturée par translation positive. Notons $p : \mathbf{N}^m \to \mathbf{N}^{m-1}$ la projection de $\mathbf{N}^m$ sur ses $m-1$ premiers facteurs.

Afin d'éviter les confusions, nous désignerons par des lettres surlignées, comme par exemple $\overline{\alpha}$, les éléments de $\mathbf{N}^{m-1}$, et par des lettre non surlignées, comme par exemple α, les éléments de $\mathbf{N}^m$. Nous écrirons $\overline{\alpha} = (\alpha^1, \ldots, \alpha^{m-1})$, $\alpha = (\alpha^1, \ldots, \alpha^m)$, les α^i désignant les composantes de $\overline{\alpha}$ (dans ce cas $1 \leq i \leq m-1$) ou celles de α (dans ce cas $1 \leq i \leq m$).

Nous remarquons que $p(E)$ est un sous-ensemble de $\mathbf{N}^{m-1}$ saturé par translation positive. En effet, si $\overline{\alpha} = (\alpha^1, \ldots, \alpha^{m-1}) \in p(E)$ et $\overline{\beta} = (\beta^1, \ldots, \beta^{m-1}) \in \mathbf{N}^{m-1}$, il existe $\alpha^m \in \mathbf{N}$ tel que $\alpha = (\alpha^1, \ldots, \alpha^{m-1}, \alpha^m) \in E$, donc $(\alpha^1+\beta^1, \ldots, \alpha^{m-1}+\beta^{m-1}, \alpha^m+0) \in E$, et par suite $\overline{\alpha} + \overline{\beta} = (\alpha^1 + \beta^1, \ldots, \alpha^{m-1} + \beta^{m-1}) \in p(E)$. D'après l'hypothèse de récurrence, il existe une frontière finie de $p(E)$, formée par les éléments $\overline{b_1}, \ldots, \overline{b_q}$ de $p(E)$. Soient $b_i \in E$ tels que $p(b_i) = \overline{b_i}$, $1 \leq i \leq q$. Explicitons les composantes des b_i en écrivant $b_i = (b_i^1, \ldots, b_i^m)$, et soit $\beta^m = \sup_{1 \leq i \leq q}(b_i^m)$.

Pour tout $k \in \mathbf{N}$ vérifiant $0 \leq k < \beta^m$ et $E \cap (\mathbf{N}^{m-1} \times \{ k \}) \neq \emptyset$, $p\big(E \cap (\mathbf{N}^{m-1} \times \{ k \})\big)$ est une partie de $\mathbf{N}^{m-1}$ saturée par translation positive. D'après l'hypothèse de récurrence, $p\big(E \cap (\mathbf{N}^{m-1} \times \{ k \})\big)$ admet une frontière finie, formée par $r(k)$ éléments de $\mathbf{N}^{m-1}$, notés $\big(\overline{c_1}(k), \ldots, \overline{c_{r(k)}}(k)\big)$. Posons, pour chaque i, $1 \leq i \leq r(k)$, $c_i(k) = \big(\overline{c_i}(k), k\big)$. Les $c_i(k)$, $1 \leq i \leq r(k)$, sont des éléments de E tels que, pour tout $\alpha \in E \cap (\mathbf{N}^{m-1} \times \{ k \})$, il existe $i \in \{ 1, \ldots, r(k) \}$ et $\gamma = (\gamma^1, \ldots, \gamma^{m-1}, 0) \in \mathbf{N}^m$ tel que $\alpha = c_i(k) + \gamma$.

La famille de points de E formée par $b_1, \ldots, b_q$ et par les points $c_i(k)$, $0 \leq k \leq \beta^m$, $1 \leq i \leq r(k)$, est finie. Montrons que c'est une frontière de E. Soit $\alpha = (\alpha^1, \ldots, \alpha^m)$ un point de E. Si $\alpha^m < \beta^m$, il existe $i \in \{1, \ldots, r(\alpha^m)\}$ et $\gamma = (\gamma^1, \ldots, \gamma^{m-1}, 0) \in \mathbf{N}^m$ tel que $\alpha = c_i(\alpha^m) + \gamma$. Si $\alpha^m \geq \beta^m$, considérons le point $\underline{\alpha} = p(\alpha)$; il appartient à $p(E)$, donc il existe $j \in \{1, \ldots, q\}$ et $\overline{\gamma} \in \mathbf{N}^{m-1}$ tel que $\underline{\alpha} = p(\alpha) = c_i + \overline{\gamma}$; mais $\alpha^m \geq \beta^m \geq b_i^m$, donc $(\overline{\gamma}, \alpha^m - b_i^m) \in \mathbf{N}^m$ et $\alpha = c_i + (\overline{\gamma}, \alpha^m - b_i^m)$. □

1.3. Proposition. *Un sous-ensemble E de $\mathbf{N}^n$ saturé par translation positive possède une unique frontière de cardinal minimum, qu'on appelle son escalier.*

Démonstration. D'après la proposition précédente, E admet des frontières de cardinal fini; soit q la borne inférieure de leurs cardinaux; il existe au moins une frontière de E de cardinal q. Supposons qu'il en existe deux, $F = \{A_1, \ldots, A_q\}$ et $G = \{B_1, \ldots, B_q\}$. Nous avons

$$E = \bigcup_{i=1}^{q} (A_i + \mathbf{N}^n) = \bigcup_{j=1}^{q} (B_j + \mathbf{N}^n).$$

Pour chaque i ($1 \leq i \leq q$), $A_i \in E$, donc il existe $\sigma(i) \in \{1, \ldots, q\}$ tel que $A_i = B_{\sigma(i)} + \mathbf{N}^n$. L'application σ de $\{1, \ldots, q\}$ dans lui-même ainsi construite est surjective, car si ce n'était pas le cas, E admettrait pour frontière l'ensemble des $B_{\sigma(i)}$, de cardinal strictement inférieur à q. L'application σ est donc une permutation de $\{1, \ldots, q\}$. En échangeant les rôles des A_i et des B_j, on montre de même qu'il existe une autre permutation σ' de $\{1, \ldots, q\}$ telle que, pour tout $j \in \{1, \ldots, q\}$, $B_j \in A_{\sigma'(j)} + \mathbf{N}^n$. Par suite, pour tout $i \in \{1, \ldots, q\}$, $A_i + \mathbf{N}^n \subset A_{\sigma' \circ \sigma(i)} + \mathbf{N}^n$. Montrons que $\sigma' = \sigma^{-1}$. Si ce n'était pas le cas, il existerait un élément i de $\{1, \ldots q\}$ tel que $\sigma' \circ \sigma(i) \neq i$; mais alors l'ensemble des A_j, avec $j \in \{1, \ldots, q\}$, $j \neq i$, serait une frontière de E de cardinal $q - 1$, ce qui est impossible. Donc $\sigma' = \sigma^{-1}$, et par suite, pour tout $i \in \{1, \ldots, q\}$, $A_i = B_{\sigma(i)}$. □

1.4. Définition. Un ordre total sur $\mathbf{N}^n$ est dit *compatible avec l'addition* si les deux conditions suivantes sont satisfaites:

(i) pour tous α et $\beta \in \mathbf{N}^n$, avec $\beta \neq 0$, $\alpha < \alpha + \beta$;

(ii) pour tous α_1 et $\alpha_2 \in \mathbf{N}^n$ vérifiant $\alpha_1 < \alpha_2$, et tout $\beta \in \mathbf{N}^n$, $\alpha_1 + \beta < \alpha_2 + \beta$.

1.5. Exemple. Soit $L : x \mapsto L(x) = \sum_{i=1}^{n} l_i x^i$ une forme linéaire sur $\mathbf{R}^n$. On définit un ordre total sur $\mathbf{N}^n$ en posant

$$\alpha < \beta \quad \text{si} \quad \begin{cases} \text{ou bien } L(\alpha) < L(\beta), \\ \text{ou bien } L(\alpha = L(\beta) \text{ et il existe } s,\ 1 \leq s \leq n, \text{ tel que} \\ \qquad \alpha_j = \beta_j \text{ pour } j < s \text{ et } \alpha_s < \beta_s. \end{cases}$$

En particulier, si $L = 0$, l'ordre ainsi défini est appelé *ordre lexicographique*.

On peut vérifier que les relations d'ordre ainsi définies sont compatibles avec l'addition.

1.6. Proposition. *Dans $\mathbf{N}^n$, muni d'une relation d'ordre total compatible avec l'addition, il n'existe pas de suite infinie strictement décroissante* ($\alpha_0 > \alpha_1 > \cdots > \alpha_p > \alpha_{p+1} > \cdots$).

Démonstration. Supposons qu'une telle suite existe, et soit $E = \bigcup_{p\in\mathbf{N}} (\alpha_p + \mathbf{N}^n)$. Le sous-ensemble E de $\mathbf{N}^n$ est saturé par translation positive; d'après la proposition 1.2, il possède une frontière de cardinal fini $\{ A_1, \ldots, A_s \}$. Il existe donc un $i \in \{ 1, \ldots, s \}$ tel que $A_i + \mathbf{N}^n$ contienne tous les termes d'une suite infinie $(\alpha_{\sigma(p)}\,,\ p \in \mathbf{N})$, extraite de la suite $(\alpha_p\,,\ p \in \mathbf{N})$, $\sigma = \mathbf{N} \to \mathbf{N}$ désignant une application strictement croissante. On a donc, pour tout $p \in \mathbf{N}$, $A_i \leq \alpha_{\sigma(p)}$. Mais puisque $A_i \in E$, il existe $q \in \mathbf{N}$ tel que $A_i \in \alpha_q + \mathbf{N}^n$, et par suite $\alpha_q \leq \alpha_{\sigma(p)}$. Comme $\sigma(p)$ tend vers $+\infty$ avec p, on a pour p assez grand $\sigma(p) > q$, ce qui contredit l'hypothèse de stricte décroissance de la suite $(\alpha_p\,,\ p \in \mathbf{N})$. □

2. La division euclidienne pour les polynômes à plusieurs variables

2.1. Notations relatives aux polynômes. Soit $\mathbf{K}$ un corps. On note $\mathbf{K}[X_1, \ldots, X_n]$ l'algèbre des polynômes à n variables $X_1, \ldots, X_n$, à coefficients dans $\mathbf{K}$. Un polynôme f élément de $\mathbf{K}[X_1, \ldots, X_n]$ sera noté

$$f = \sum_{\alpha\in\mathbf{N}^n} f_\alpha X^\alpha\,,$$

les f_α, éléments de $\mathbf{K}$, étant les coefficients du polynôme. La somme figurant au membre de droite est une somme finie, car il n'y a qu'un nombre fini de valeurs de $\alpha \in \mathbf{N}^n$ pour lesquelles le coefficient f_α est non nul. On a noté, par convention,

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n\,, \qquad X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}\,.$$

On dit que $f_\alpha X^\alpha$ est le *monôme de multidegré* α du polynôme f.

2.2. Définition. On suppose qu'on a choisi sur $\mathbf{N}^n$ une relation d'ordre total compatible avec l'addition (1.4). Soit $f = \sum_\alpha f_\alpha X^\alpha$ un polynôme non nul à n variables $X_1, \ldots, X_n$, à coefficients dans un corps $\mathbf{K}$. On appelle *exposant privilégié* de f et on note $\exp(f)$ le plus grand $\alpha \in \mathbf{N}^n$ tel que $f_\alpha \neq 0$. On note $\mathrm{in}(f)$ le seul monôme de f qui correspond à l'exposant $\exp(f)$.

On vérifie aisément que

$$\exp(f.g) = \exp(f) + \exp(g)\,, \quad \mathrm{in}(f.g) = \mathrm{in}(f).\mathrm{in}(g)\,.$$

Dans tout ce qui suit, on suppose qu'une relation ordre total compatible avec l'addition a été choisie sur $\mathbf{N}^n$.

2.3. Partition de $\mathbf{N}^n$ associée à une famille finie ordonnée de polynômes.

Soit $(f_1, \ldots, f_s)$ une famille ordonnée de s polynômes à n variables $X_1, \ldots, X_n$, à coefficients dans le corps $\mathbf{K}$. On associe à cette donnée la partition de $\mathbf{N}^n$,

$$\mathbf{N}^n = \Delta_1 \cup \cdots \cup \Delta_s \cup \overline{\Delta}\,,$$

ainsi définie:

$$\Delta_1 = \exp(f_1) + \mathbf{N}^n\,, \quad \Delta_2 = \big(\exp(f_2) + \mathbf{N}^n\big)\backslash\Delta_1\,,$$

et, pour tout j, $2 \leq j \leq s$,

$$\Delta_j = \big(\exp(f_j) + \mathbf{N}^n\big)\backslash\big(\Delta_1 \cup \cdots \cup \Delta_{j-1}\big)\,,$$

et enfin

$$\overline{\Delta} = \mathbf{N}^n\backslash \bigcup_{i=1}^{s} \Delta_i\,.$$

2.4. Théorème. *Soit $(f_1,\ldots,f_s)$ une famille ordonnée de s polynômes éléments de $\mathbf{K}[X_1,\ldots,X_n]$, et $(\Delta_1,\ldots,\Delta_s,\overline{\Delta})$ la partition de $\mathbf{N}^n$ associée (2.3). Pour tout polynôme $f \in \mathbf{K}[X_1,\ldots,X_n]$, il existe une unique famille de $s+1$ polynômes $(h_1,\ldots,h_s,h)$, telle que*

(i) $f = h_1 f_1 + \cdots + h_s f_s + h$;

(ii) *pour chaque $i \in \{1,\ldots,s\}$, si $h_i(X) = \sum_\alpha h_{i\alpha} X^\alpha$, $h_{i\alpha} \neq 0$ implique $\exp(f_i)+\alpha \in \Delta_i$;*

(iii) *si $h(X) = \sum_\alpha h_\alpha X^\alpha$, $h_\alpha \neq 0$ implique $\alpha \in \overline{\Delta}$.*

On dit que h est le reste de la division euclidienne de f par $(f_1,\ldots,f_s)$.

Démonstration. Soit $f \in \mathbf{K}[X_1,\ldots,X_n]$, $\exp(f) = \alpha_0$, et $\mathrm{in}(f) = f_{\alpha_0} X^{\alpha_0}$.

Si $\alpha_0 \in \overline{\Delta}$, on pose

$$h^{(1)} = f_{\alpha_0} X^{\alpha_0}\,, \quad h_i^{(1)} = 0\,, \quad i \in \{1,\ldots,s\}\,,$$

puis

$$f^{(1)} = f - \sum_{i=1}^{s} h_i^{(1)} f_i - h^{(1)} = f - h^{(1)}\,.$$

On a

$$\exp(f^{(1)}) < \exp(f)\,.$$

Si $\alpha_0 \in \Delta_i$, on peut écrire $\alpha_0 = \exp(f_i) + \beta_0$, avec $\beta_0 \in \mathbf{N}^n$. On a

$$\mathrm{in}(f_i) = \mu_i X^{\exp(f_i)}\,.$$

On pose

$$h^{(1)} = 0\,, \quad h_j^{(1)} = \begin{cases} \dfrac{f_{\alpha_0}}{\mu_i} X^{\beta_0} & \text{si } j = i, \\ 0 & \text{si } j \neq i,\ 1 \leq j \leq s. \end{cases}$$

Puis on pose

$$f^{(1)} = f - \sum_{j=1}^{s} h_j^{(1)} f_j - h^{(1)} = f - h_i^{(1)} f_i\,.$$

On a

$$\mathrm{in}\big(h_i^{(1)} f_i\big) = \mathrm{in}(h_i^{(1)})\mathrm{in}(f_i) = f_{\alpha_0} X^{\alpha_0} = \mathrm{in}(f)\,,$$

de sorte que

$$\exp(f^{(1)}) < \exp(f)\,.$$

Si $f^{(1)} = 0$, on s'arrête. Sinon on recommence en remplaçant f par $f^{(1)}$, et ainsi de suite. Le processus s'arrête au bout d'un nombre fini d'étapes car sinon il existerait une suite infinie strictement décroissante d'indices éléments de $\mathbf{N}^n$, ce qui est impossible (1.6). Ceci démontre l'existence de la décomposition annoncée, et donne un algorithme pour la déterminer. Montrons son unicité. Supposons qu'on ait deux familles de polynômes $h_1, \ldots, h_s, h$ et $h'_1, \ldots, h'_s, h'$ vérifiant les conditions de l'énoncé. Par suite,

$$\sum_{i=1}^{s}(h_i - h'_i)f_i + (h - h') = 0\,.$$

Si $h - h' \neq 0$, chaque monôme de $h - h'$ a son exposant qui appartient à $\overline{\Delta}$. En particulier, $\exp(h - h') \in \overline{\Delta}$. D'après **(ii)**, $\exp\big((h_i - h'_i)f_i\big) \in \Delta_i$. Puisque $\Delta_i \cap \Delta_j = \emptyset$ pour $i \neq j$,

$$\exp\left(\sum_{i=1}^{s}(h_i - h'_i)f_i\right) = \sup_{1\leq i\leq s}\big(\exp\big((h_i - h'_i)f_i\big)\big)\,;$$

il existe donc un i_0 tel que

$$\exp\left(\sum_{i=1}^{s}(h_i - h'_i)f_i\right) \in \Delta_{i_0}\,,$$

ce qui est impossible puisque $\Delta_{i_0} \cap \overline{\Delta} = \emptyset$. On a donc $h - h' = 0$. Supposons maintenant $h_1 - h'_1 \neq 0$. On aurait alors

$$-(h_1 - h'_1)f_1 = \sum_{i=2}^{s}(h_i - h'_i)f_i\,,$$

et par le même raisonnement que ci-dessus

$$\exp\big((h_1 - h'_1)f_1 \in \Delta_1 \quad \text{et} \quad \exp\left(\sum_{i=2}^{s}(h_i - h'_i)f_i\right) \in \Delta_{i_0}\,,\ \text{avec } 2 \leq i_0 \leq s\,.$$

Comme $\Delta_1 \cap \Delta_{i_0} = \emptyset$, c'est impossible et $h_1 = h'_1$. De proche en proche on montre de même que $h'_i = h_i$, $1 \leq i \leq s$. D'où l'unicité. □

3. Bases de Gröbner d'un idéal et algorithme de Burchberger

3.1. Rappel. Soit $\mathbf{K}$ un corps, et $\mathbf{K}[X_1, \ldots, X_n]$ l'algèbre des polynômes à n variables à coefficients dans K. On appelle *idéal* de $\mathbf{K}[X_1, \ldots, X_n]$ un sous-espace vectoriel I de $\mathbf{K}[X_1, \ldots, X_n]$ tel que, pour tout $f \in I$ et tout $g \in \mathbf{K}[X_1, \ldots, X_n]$, on ait $fg \in I$.

Soit $(f_j\,,\ j \in J)$ une famille de polynômes éléments de $\mathbf{K}[X_1, \ldots, X_n]$, indexée par un ensemble d'indices J (qui peut être fini ou infini). On vérifie aisément que l'ensemble des polynômes de la forme

$$f = \sum_{j \in J} f_j\, h_j\,,$$

avec $h_j \in \mathbf{K}[X_1, \ldots, X_n]$, et $h_j = 0$ sauf pour un nombre fini de valeurs de l'indice j, est un idéal de $\mathbf{K}[X_1, \ldots, X_n]$. On dit que cet idéal est *engendré* par la famille $(f_j\,,\ j \in J)$, ou que cette famille constitue un *système de générateurs* de cet idéal.

Rappelons que pour $n = 1$, tout idéal I de l'algèbre $\mathbf{K}[X]$ des polynômes à une variable possède un système de générateurs comportant un seul élément. En effet, on voit aisément qu'il existe un élément non nul f de I de degré minimum. Soit g un élément quelconque de I. On sait que g peut s'écrire sous la forme

$$g = fq + r\,,$$

q et r étant deux polynômes (le quotient et le reste de la division euclidienne de g par f selon les puissances décroissantes de la variable), le degré de r (si celui-ci est non nul) étant strictement inférieur à celui de f. Mais g et fq sont éléments de I, donc, s'il est non nul, $r = g - fq$ est un élément de I de degré strictement inférieur à celui de f, ce qui est impossible. Donc $g = fq$, et par suite I est l'idéal engendré par f.

Pour $n > 1$, les idéaux de l'algèbre $\mathbf{K}[X_1, \ldots, X_n]$ des polynômes à n variables n'ont en général pas un générateur unique. On va voir cependant (3.6) qu'ils admettent toujours un système de générateurs comportant un nombre fini d'éléments.

Comme dans le paragraphe précédent, onsuppose qu'une relation d'ordre total compatible avec l'addition a été choisie sur $\mathbf{N}^n$.

3.2. Lemme. *Soit I un idéal de $\mathbf{K}[X_1, \ldots, X_n]$. Le sous-ensemble de $\mathbf{N}^n$, noté $\exp(I)$, formé par les exposants privilégiés $\exp(f)$ des polynômes f qui appartiennent à l'idéal I, est saturé par translation positive (1.1).*

Démonstration. Si $\alpha \in \exp(I)$, il existe $f \in I$ tel que $\alpha = \exp(f)$. Soit $\beta \in \mathbf{N}^n$. Comme I est un idéal, $X^\beta f$ appartient à I et $\exp(X^\beta f) = \alpha + \beta$ appartient à $\exp(I)$. □

3.3. Définition. On appelle *escalier* de l'idéal I, et on note $E(I)$, l'escalier de l'ensemble $\exp(I)$ (1.3).

3.4. Définition. On appelle *base de Gröbner* de l'idéal I, toute famille $(f_1, \ldots, f_s)$ de polynômes éléments de I telle que $\{\exp(f_1), \ldots, \exp(f_s)\}$ soit une frontière de $\exp(I)$.

On appelle *base de Gröbner minimale* de I une base de Gröbner de I telle que $\{\exp(f_1), \ldots, \exp(f_s)\}$ soit l'escalier de $\exp(I)$.

3.5. Proposition. *Une base de Gröbner $(f_1, \ldots, f_s)$ d'un idéal I est un système de générateurs de I.*

Démonstration. Soit $f \in I$. D'après le théorème 2.4, il existe une décomposition

$$f = \sum_{i=1}^{s} h_i f_i + h\,,$$

et si $h = \sum_\alpha c_\alpha X^\alpha$, $c_\alpha \neq 0$ implique $\alpha \in \overline{\Delta} = \mathbf{N}^n \backslash \bigcup_{i=1}^s \Delta_i$. Puisque $f \in I$ et $\sum_{i=1}^s h_i f_i \in I$, on a $h \in I$ et donc $\exp(h) \in \exp(I) = \bigcup_{i=1}^s \big(\exp(f_i + \mathbf{N}^n\big) = \bigcup_{i=1}^s \Delta_i$. Il y a donc contradiction, et $h = 0$. □

3.6. Corollaire. *L'anneau $\mathbf{K}[X_1, \ldots, X_n]$ est noethérien, c'est-à-dire que tout idéal de cet anneau possède un nombre fini de générateurs.*

3.7. Remarque. Une base de Gröbner minimale n'est pas forcément un système de générateurs minimal de l'idéal.

3.8. Notation. Une famille $(f_1, \ldots, f_s)$ de polynômes éléments de $\mathbf{K}[X_1, \ldots, X_n]$ étant donnée, il est commode de noter, pour tout polynôme $f \in \mathbf{K}[X_1, \ldots, X_n]$, $f\,R\,(f_1, \ldots, f_s)$ le reste de la division euclidienne de f par $f_1, \ldots, f_s$.

3.9. Proposition. *Soient $(f_1, \ldots, f_s)$ et $(f'_1, \ldots, f'_{s'})$ deux bases de Gröbner d'un idéal I. On a, pour tout polynôme f,*

$$f\,R\,(f_1, \ldots, f_s) = f\,R\,(f'_1, \ldots, f'_{s'})\,.$$

Démonstration. Soient $\Delta_1, \ldots, \Delta_s; \overline{\Delta}$ et $\Delta'_1, \ldots, \Delta'_{s'}; \overline{\Delta'}$ les partitions de $\mathbf{N}^n$ associées aux deux bases de Gröbner $(f_1, \ldots, f_s)$ et $(f'_1, \ldots, f'_{s'})$. On a

$$\exp(I) = \bigcup_{i=1}^{s} \big(\exp(f_i) + \mathbf{N}^n\big) = \bigcup_{j=1}^{s'} \big(\exp(f'_j) + \mathbf{N}^n\big)\,.$$

Donc $\overline{\Delta} = \overline{\Delta'}$. Écrivons

$$\begin{aligned} f &= \sum_{i=1}^{s} h_i f_i + f\,R\,(f_1, \ldots, f_s) \\ &= \sum_{j=1}^{s'} h'_j f'_j + f\,R\,(f'_1, \ldots, f'_{s'}) \end{aligned}$$

.

Posons $g = f\,R\,(f_1, \ldots, f_s) - f\,R\,(f'_1, \ldots, f'_{s'})$. Si $g \neq 0$, $\exp(g) \in \overline{\Delta}$. Or $g \in I$, donc $\exp(g) \in \exp(I) = \bigcup_{i=1}^s \Delta_i = \bigcup_{j=1}^{s'} \Delta'_j = \mathbf{N}^n \backslash \overline{\Delta}$. Il y a contradiction et $g = 0$. □

3.10. Théorème. *Une condition nécessaire et suffisante pour que $(f_1, \ldots, f_s)$ soit une base de Gröbner de l'idéal I est que pour tout $f \in I$, $f\,R\,(f_1, \ldots, f_s) = 0$.*

Démonstration. Soit $(f_1, \ldots, f_s)$ une base de Gröbner de I. Si $f \in I$, on a

$$f\,R\,(f_1, \ldots, f_s) = f - \sum_{i=1}^{s} h_i f_i \in I\,.$$

Mais $\exp\big(f\,R\,(f_1, \ldots, f_s)\big) \notin \exp(I)$, donc $f\,R\,(f_1, \ldots, f_s) = 0$.

Réciproquement, soit $(f_1, \ldots, f_s)$ une famille d'éléments de I telle que pour tout $f \in I$, $f\,R\,(f_1, \ldots, f_s) = 0$. Soit $f \in I$. Il existe $h_1, \ldots, h_s$ tels que

$$f = \sum_{i=1}^{s} h_i f_i\,.$$

On a

$$\exp(h_i f_i) = \exp(h_i) + \exp(f_i) \in \Delta_i\,.$$

Puisque $\Delta_i \cap \Delta_j = \emptyset$,

$$\exp\left(\sum_{i=1}^{s} h_i f_i\right) = \sup_{1 \le i \le s} \exp(h_i f_i)\,.$$

Il existe donc i_0 tel que $\exp(f) \in \Delta_{i_0} \subset \exp(f_{i_0} + \mathbf{N}^n$. On a ainsi montré que $\exp(I) = \bigcup_{i=1}^{s} \big(\exp(f_i) + \mathbf{N}^n$, donc que $(f_1, \ldots, f_s)$ est une base de Gröbner de I. □

3.11. Notation. Soient f et g deux polynômes éléments de $\mathbf{K}[X_1, \ldots, X_n]$. Soit $\exp(f) = \alpha = (\alpha_1, \ldots, \alpha_n)$, $\exp(g) = \beta = (\beta_1, \ldots, \beta_n)$. On pose, pour chaque i $(1 \le i \le n)$, $\gamma_i = \sup(\alpha_i, \beta_i)$, et $\gamma = (\gamma_1, \ldots, \gamma_n)$. Si $\mathrm{in}(f) = \lambda X^\alpha$ et $\mathrm{in}(g) = \nu X^\beta$, on pose

$$f\,s\,g = \nu X_1^{\gamma_1 - \alpha_1} \cdots X_n^{\gamma_n - \alpha_n} f - \lambda X_1^{\gamma_1 - \beta_1} \cdots X_n^{\gamma_n - \beta_n} g\,.$$

On a donc, si $f\,s\,g \neq 0$, $\exp(f\,s\,g) < \gamma$.

3.12. Théorème. *Une condition nécessaire et suffisante pour qu'un système de générateurs $(f_1, \ldots, f_s)$ d'un idéal I soit une base de Gröbner de cet idéal est que pour tous i et j vérifiant $1 \le i < j \le s$, on ait $(f_i\,s\,f_j)\,R\,(f_1, \ldots, f_s) = 0$.*

Démonstration. La condition est nécessaire d'après 3.10 puisque $f_i\,s\,f_j$ appartient à l'idéal I. Pour montrer qu'elle est suffisante, il suffit, toujours d'après 3.10, de vérifier que si cette condition est satisfaite, pour tout $f \in I$, on a $f\,R\,(f_1, \ldots, f_s) = 0$. Soit donc $f \in I$, et $g = f\,R\,(f_1, \ldots, f_s)$; supposons $g = \sum_\alpha g_\alpha X^\alpha \neq 0$. Si $g_\alpha \neq 0$, on a $\alpha \in \mathbf{N}^n \setminus \big(\bigcup_{i=1}^{s} \big(\exp(f_i) + \mathbf{N}^n\big)\big)$. D'autre part $g = f - \sum_{i=1}^{s} h_i f_i \in I$, donc il existe $H_1, \ldots, H_s$ tels que $g = \sum_{i=1}^{s} H_i f_i$. Notons $N = \sup_{1 \le i \le s} \exp(H_i f_i)$.

Supposons qu'il existe un seul i tel que $\exp(H_i f_i) = N$; on aurait donc $\exp(g) = N$; mais alors $\exp(g) = \exp(H_i) + \exp(f_i)$, et $\exp(g) \in \exp(f_i) + \mathbf{N}^n$, ce qui n'est pas possible. Il existe donc au moins deux valeurs i_0 et i_1 de l'indice, $i_0 \neq i_1$, telles que

$\exp(H_{i_0} f_{i_0}) = \exp(H_{i_1} f_{i_1}) = N$. On peut toujours supposer qu'il n'y a pas d'indice i vérifiant $i_0 < i < i_1$ tel que $\exp(H_i f_i) = N$. Posons

$$\begin{aligned} \mathrm{in}(f_{i_0}) = \lambda_0 X^\alpha\,,\ \mathrm{in}(H_{i_0}) = \nu_0 X^u\,,\\ \mathbf{rm}(f_{i_1}) = \lambda_1 X^\beta\,,\ \mathrm{in}(H_{i_1}) = \nu_1 X^v\,. \end{aligned}$$

On a $\alpha+u = \beta+v = N$. Soit $\gamma_i = \sup(\alpha_i, \beta_i)$, $i = 0$ ou 1. Posons $p = u-(\gamma-\alpha = v-(\gamma-\beta)$. Il vient

$$\begin{aligned} X^p f_{i_0}\, s\, f_{i_1} &= \lambda_1 X^u f_{i_0} - \lambda_0 X^v f_{i_1} \\ &= \frac{\lambda_1}{\nu_0}\mathrm{in}(H_{i_0}) f_{i_0} - \frac{\lambda_0}{\nu_1}\mathrm{in}(H_{i_1}) f_{i_1}\,. \end{aligned}$$

Écrivons

$$g = \mathrm{in}(H_{i_0}) f_{i_0} + \mathrm{in}(H_{i_1}) f_{i_1} + \big(H_{i_0} - \mathrm{in}(H_{i_0})\big) f_{i_0} + \big(H_{i_1} - \mathrm{in}(H_{i_1})\big) f_{i_1} + \sum_{j \notin \{\, i_0, i_1 \,\}} H_j f_j\,,$$

puis

$$\begin{aligned} g = \frac{\nu_0}{\lambda_1} X^p f_{i_0}\, s\, f_{i_1} + \left(1 + \frac{\lambda_0 \nu_0}{\lambda_1 \nu_1}\right) \mathrm{in}(H_{i_1} f_{i_1} \\ + \big(H_{i_0} - \mathrm{in}(H_{i_0})\big) f_{i_0} + \big(H_{i_1} - \mathrm{in}(H_{i_1})\big) f_{i_1} + \sum_{j \notin \{\, i_0, i_1 \,\}} H_j f_j\,. \end{aligned}$$

Observons que $\exp(X^p f_{i_0}\, s\, f_{i_1}) < p + \gamma = N$, et que $\exp\big(H_{i_0} - \mathrm{in}(H_{i_0}\big) < u$. On peut donc réécrire

$$g = \frac{\nu_0}{\lambda_1} X^p f_{i_0}\, s\, f_{i_1} + \sum_{j \neq i_0} H'_j f_j + H'_{i_0} f_{i_0}\,,$$

avec $\sup_{j \neq i_0} \exp(H'_j f_j) < N$ et $\exp(H'_{i_0} f_{i_0}) < N$. On réécrit ainsi de proche en proche

$$g = \sum_{i,j} \lambda_{ij} X^{q_{ij}} f_i\, s f_j + \sum_i \widetilde{H}_i f_i\,,$$

avec $\exp(\widetilde{H}_i f_i) < N$ et $\exp(X^{q_{ij}} f_i\, s\, f_j) < N$. Par hypothèse $f_i\, s\, f_j\, R\,(f_1, \ldots, f_s) = 0$, donc il existe des h^k_{ij} tels que $f_i\, s\, f_j = \sum_k h^k_{ij} f_k$, avec $\exp(h^k_{ij} f_k) \leq \exp(f_i\, s\, f_j)$. Alors $X^{q_{ij}} f_i\, s\, f_j = \sum_k X^{q_{ij}} h^k_{ij} f_k$, avec $\exp(X^{q_{ij}} h^k_{ij} f_k) \leq \exp(X^{q_{ij}} f_i\, s\, f_j) < N$. D'où une nouvelle expression

$$g = \sum_i \overline{H}_i f_i\,,$$

avec $N_2 = \sup_i \exp(\overline{H}_i f_i) < N_1 = N$.

On recommence alors et on détermine une suite infinie d'exposants $N_1 > N_2 > \cdots > N_p > N_{p+1} > \cdots$, ce qui est impossible d'après 1.6. On a donc $g = 0$. □

3.13. L'algorithme de Burchberger pour le calcul d'une base de Gröbner.

Le théorème 3.12 fonde l'algorithme qui suit dû à Burchberger. Connaissant un système de générateurs $(f_1, \ldots, f_s)$ d'un idéal I de $\mathbf{K}[X_1, \ldots, X_n]$, on souhaite construire une base de Gröbner de cet idéal. On calcule, pour chaque couple (i, j), $1 \leq i, j \leq s$, $i \neq j$,

$$f_i\, s\, f_j\, R\,(f_1, \ldots, f_s)\,.$$

Si pour tous i, j, ceci est nul, on a une base de Gröbner. Si pour au moins un couple (i,j), $f_i \, s \, f_j \, R\,(f_1, \ldots, f_s) \neq 0$, on pose $f_{s+1} = f_i \, s \, f_j \, R\,(f_1, \ldots, f_s)$. Observons que si $f_i \, s \, f_j \, R\,(f_1, \ldots, f_s) = 0$, alors $f_i \, s \, f_j \, R\,(f_1, \ldots, f_{s+1}) = 0$. Si pour tout (i,j), $1 \leq i \leq s+1$, $1 \leq j \leq s+1$, on a $f_i \, s \, f_j \, R\,(f_1, \ldots, f_{s+1}) = 0$, on s'arrête car on a une base de Gröbner. Sinon il existe i, j tels que $f_i \, s \, f_j \, R\,(f_1, \ldots, f_{s+1}) \neq 0$, et on pose $f_{s+2} = f_i \, s \, f_j \, R\,(f_1, \ldots, f_{s+1})$, et ainsi de suite.

Il reste à vérifier que ce procédé s'arrête. Supposons que cela ne soit pas le cas. Considérons $E = \bigcup\big(\exp(f_p) + \mathbf{N}^n\big)$. Soit $A_1, \ldots, A_p$ une frontière finie de E. Pour tout i, il existe $p(i)$ tel que $A_i \in \exp(f_{p(i)} + \mathbf{N}^N$. Soit $k = \sup_{1 \leq i \leq p} p(i)$. On a donc

$$E = \bigcup_{i=1}^{k} \big(\exp(f_i) + \mathbf{N}^n\big)\,.$$

Or $f_{k+1} \neq 0$ et il existe i, j tels que

$$f_{k+1} = f_i \, s \, f_j \, R\,(f_1, \ldots, f_k)\,.$$

On a $\exp(f_{k+1} \in \mathbf{N}^n \setminus \Big(\bigcup_{i=1}^{k} \big(\exp(f_i) + \mathbf{N}^n\Big)$. Or $\exp(f_{k+1} \in R$ et on a une contradiction.