COURS DE L'INSTITUT FOURIER

MONIQUE LEJEUNE-JALABERT

Chapitre 1 Algorithme de calcul de bases standards

Cours de l'institut Fourier, tome 19 (1984-1985), p. 33-52

<http://www.numdam.org/item?id=CIF_1984-1985__19__33_0>

Chapitre 1

ALGORITHME DE CALCUL DE BASES STANDARDS

1. Algorithme de division euclidienne

Nous cherchons à généraliser simultanément la notion de terme de plus haut degré dans 1 polynôme à 1 variable et celle de 1e variable figurant effectivement dans un polynôme de degré ≤ 1 qui nous ont permis de fabriquer l'algorithme de calcul du $PGCD$ de 2 polynômes à 1 variable et l'algorithme d'élimination de Gauss pour la résolution des systèmes linéaires. Autrement dit, étant donné $f \in k[X_1, \ldots, X_n]$ nous cherchons à définir la notion de "plus grand" monôme figurant dans f . Nous sommes donc amenés à munir $\mathbf{N}^n$ d'un ordre total. Bien sûr, il existe de nombreuses manières de le faire.

1.1. HYPOTHÈSE . — Dans toute la suite, nous supposerons que l'ordre total choisi sur $\mathbf{N}^n$ vérifie les conditions suivantes :

i) $\forall \alpha \in \mathbf{N}^n \ , \ \forall \beta \in \mathbf{N}^n \ , \ \beta \neq 0 \ , \ \alpha < \alpha + \beta$

ii) $\forall \alpha_i \in \mathbf{N}^n \ , \ i = 1,2 \ , \ \forall \beta \in \mathbf{N}^n,$

$$\alpha_1 < \alpha_2 \ \Leftrightarrow \alpha_1 + \beta < \alpha_2 + \beta.$$

1.1.1. NOTATIONS . — $\alpha \leq \beta$ signifiera que $\alpha < \beta$ ou $\alpha = \beta$.

1.1.2. EXEMPLES . — Voici quelques choix possibles :
soit $L = \sum_{i=1}^n c_i X_i \ , \ c_i \in \mathbf{R} \ , \ c_i \geq 0$ une forme linéaire sur $\mathbf{R}^n$.

1.1.2.1. $\alpha < \beta \ \Leftrightarrow$ ou bien $L(\alpha) < L(\beta)$

ou bien $L(\alpha) = L(\beta)$ et il existe $s \ , \ 1 \leq s \leq n$ tel que $\alpha_j = \beta_j \ , \ j < s$ et $\alpha_s < \beta_s$.

On départage les α tels que $L(\alpha) = L(\beta)$ par l'ordre lexicographique.

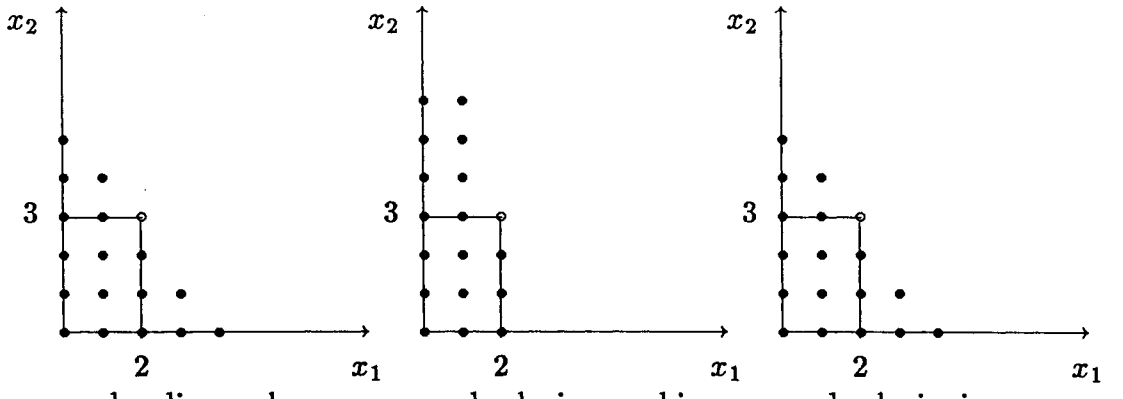
Si $L = \sum_{i=1}^n X_i$, on appelle l'ordre en question *l'ordre diagonal.*

Si $L = 0$, c'est *l'ordre lexicographique.*

1.1.2.2. $\alpha < \beta \ \Leftrightarrow$ ou bien $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$

ou bien $\sum \alpha_i = \sum \beta_i$ et il existe $s \ , \ 1 \leq s \leq n$ tel que $\alpha_j = \beta_j \ , \ j > s \ , \ \alpha_s > \beta_s$. Nous appellerons ici cet ordre, *ordre lexicographique inverse.*

1.1.2.3. Représentons dans ces 3 cas, lorsque $n = 2$, les α plus petits que l'exposant $(2,3)$.



1.2. DÉFINITION. — *On appelle exposant privilégié de* $f \in k[X_1, \ldots, X_n]$ $f \neq 0$, $f = \sum c_\alpha X^\alpha$ *et on note* $\exp f$ *le plus grand* α *tel que* $c_\alpha \neq 0$.

On appelle forme initiale de f , $f \neq 0$ *et on note* $\operatorname{in} f$ *le monôme* $c_\alpha X^\alpha$ *où* $\alpha = \exp f$.

1.3. REMARQUE. —

$$\exp fg = \exp f + \exp g$$
$$\operatorname{in} fg = \operatorname{in} f . \operatorname{in} g.$$

En effet, soit

$$f = \sum c_\alpha X^\alpha \quad , \quad f \neq 0$$
$$g = \sum c'_{\alpha'} X^{\alpha'} \quad , \quad g \neq 0.$$

Soit $\alpha_0 = \exp f$, $\alpha'_0 = \exp g$.

$$fg = \sum_\gamma \left(\sum_{\alpha+\alpha'=\gamma} c_\alpha c'_{\alpha'} \right) X^\gamma = \sum_\gamma d_\gamma X^\gamma.$$

Soit $\gamma_0 = \alpha_0 + \alpha'_0$, $d_{\gamma^0} = c_{\alpha^0} c'_{\alpha'_0} \neq 0$. En effet, si $\alpha + \alpha' = \alpha_0 + \alpha'_0$ et si $c_\alpha \neq 0$, $\alpha \leq \alpha_0$. Donc (ii), $\alpha + \alpha' = \alpha_0 + \alpha'_0 \leq \alpha_0 + \alpha'$ et (ii) $\alpha'_0 \leq \alpha'$. Si $c'_{\alpha'} \neq 0$, $\alpha' = \alpha'_0$ et $\alpha = \alpha_0$. Si maintenant $d_\gamma \neq 0$, il existe α , $c_\alpha \neq 0$ et $\alpha', c'_{\alpha'} \neq 0$ tels que $\alpha + \alpha' = \gamma$. Alors $\alpha \leq \alpha_0$, $\alpha' \leq \alpha'_0$. De (ii), on déduit :

$$\alpha + \alpha' \leq \alpha_0 + \alpha' \leq \alpha_0 + \alpha'_0 \quad , \quad \text{i.e.} \quad \gamma \leq \gamma_0.$$

1.4. EXEMPLE. — Soit

$$f = 3X_1^2 X_2^4 + 5X_1^3 X_2^3 + 7X_1^4 X_2 + 8X_1^5.$$

Pour l'ordre diagonal, $\exp f = (3,3)$ $\quad \text{in} f = 5X_1^3X_2^3$.
Pour l'ordre lexicographique, $\exp f = (5,0)$ $\quad \text{in} f = 8X_1^5$.

1.5. DÉFINITION. — *On appelle E-sous-ensemble de* $\mathbf{N}^n$, *tout sous-ensemble* E *de* $\mathbf{N}^n$ *tel que :*

$$\forall \alpha \in E \ , \ \forall \beta \in \mathbf{N}^n \ , \quad \alpha + \beta \in E.$$

On appelle frontière de E *tout sous-ensemble* F *de* E *tel que :*

$$\forall \alpha \in E \ , \ \exists \alpha_0 \in F \quad et \quad \beta \in \mathbf{N}^n \quad tel\ que \quad \alpha = \alpha_0 + \beta.$$

1.6. PROPOSITION. — *Si* E *est un E-sous-ensemble* $\neq \emptyset$ *de* $\mathbf{N}^n$, *il existe un ensemble fini* F *qui soit une frontière de* E .

Démonstration. — Par récurrence sur n . Si $n = 1$, c'est évident. Soit $p : \mathbf{N}^n \to \mathbf{N}^{n-1}$ la projection sur les $n-1$ premiers facteurs de $\mathbf{N}^n$. $p(E)$ est un E- sous-ensemble de $\mathbf{N}^{n-1} \neq \emptyset$. En effet, si $(\alpha_1, \ldots, \alpha_{n-1}) \in p(E)$ et $(\beta_1, \ldots, \beta_{n-1}) \in \mathbf{N}^{n-1}$, il existe $\alpha_n \in \mathbf{N}$ tel que $(\alpha_1, \ldots, \alpha_n) \in E$, $(\alpha_1 + \beta_1, \ldots, \alpha_{n-1} + \beta_{n-1}, \alpha_n + 0) \in E$ et $(\alpha_1 + \beta_1, \ldots, \alpha_{n-1} + \beta_{n-1}) \in p(E)$. Par hypothèse de récurrence, il existe $\tilde{\alpha}^1, \ldots, \tilde{\alpha}^q \in p(E)$, formant une frontiére de $p(E)$. Il existe donc $\alpha^1, \ldots, \alpha^q \in E$ tel que $p(\alpha^1), \ldots, p(\alpha^q)$ soit une frontière de $p(E)$.

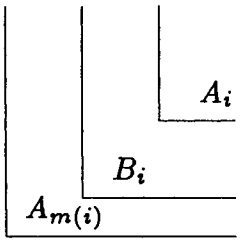
D'autre part, pour tout entier $a \geq 0$, $p(E \cap \mathbf{N}^{n-1} \times a)$ est un E-sous-ensemble de $\mathbf{N}^{n-1}$. Posons $\alpha^j = (\alpha_1^j, \ldots, \alpha_n^j)$ et $\bar{a} = \sup_{j=1\ldots q} \alpha_n^j$. Toujours par hypothèse de récurrence, pour tout $a \in \mathbf{N}$, $a < \bar{a}$, tel que $E \cap \mathbf{N}^{n-1} \times a \neq \emptyset$, il existe α_a^j , $1 \leq j \leq q_a$, tels que $\alpha_a^j \in E \cap \mathbf{N}^{n-1} \times a$ et tels que $\{p(\alpha_a^j)$, $1 \leq j \leq q_a\}$ soit une frontière de $p(E \cap \mathbf{N}^{n-1} \times a)$. Soit $F = (\alpha^1, \ldots, \alpha^q, \alpha_a^j$, $a \in \mathbf{N}$, $a < \bar{a}$, $1 \leq j \leq q_a)$. F est un ensemble fini et c'est une frontière de E .En effet, soit $\alpha = (\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in E$. Il existe i tel que $(\alpha_1, \ldots, \alpha_{n-1}) \in p(\alpha^i) + \mathbf{N}^{n-1}$. Ainsi $\alpha_k - \alpha_k^i \geq 0$, $k = 1 \ldots n-1$. Si $\alpha_n \geq \bar{a} = \sup_j \alpha_n^j$, $\alpha_n \geq \alpha_n^i$ et $\alpha \in \alpha^i + \mathbf{N}^n$. Si $\alpha_n < \bar{a}$, $(\alpha_1, \ldots, \alpha_{n-1}) \in p(E \cap \mathbf{N}^{n-1} \times \alpha_n)$. Il existe i' , $1 \leq i' \leq q_{\alpha_n}$ tel que $(\alpha_1, \ldots, \alpha_{n-1}) \in p(\alpha_{\alpha_n}^{i'}) + \mathbf{N}^{n-1}$ et $(\alpha_1, \ldots, \alpha_n) \in \alpha_{\alpha_n}^{i'} + \mathbf{N}^n$.

1.7. LEMME. — *Un E-sous-ensemble de* $\mathbf{N}^n$ *possède une unique frontière de cardinal minimum.*

Démonstration. — Supposons $E \neq \emptyset$ et soit $q = \inf \sharp$ frontière finie de E . Supposons qu'on ait 2 frontières de cardinal q , $F = (A_1, \ldots, A_q)$, $G = (B_1, \ldots, B_q)$. Par définition, on a $E = \cup_i A_i + \mathbf{N}^n = \cup_j B_j + \mathbf{N}^n$. $A_i \in E$, donc il existe $n(i)$ tel que $A_i \in B_{n(i)} + \mathbf{N}^n$. L'application n de $(1, \ldots, q)$ dans lui-même est certainement surjective car, sinon, $E = \cup_i A_i + \mathbf{N}^n \subset \cup_i B_{n(i)} + \mathbf{N}^n$ admettrait une frontière de cardinal $< q$. n est donc une permutation de $1 \ldots q$ et en réindexant au besoin les B_j , on peut supposer que $n(i) = i$.

On a donc $A_i \in B_i + \mathbf{N}^n$.

Mais il existe aussi $m(i)$ tel que $B_i \in A_{m(i)} + \mathbf{N}^n$ et



$A_i + \mathbf{N}^n \subset A_{m(i)} + \mathbf{N}^n$

Si donc $i \neq m(i)$, $F - A_i$ serait encore une frontière de E . C'est impossible. Donc $i = m(i)$ et $A_i = B_i$.

1.8. DÉFINITION. — *La frontière de cardinal minimal d'un E-sous-ensemble de $\mathbf{N}^n$ est appelé son escalier.*

1.9. PROPOSITION. — *Il n'existe pas de suite infinie $\{\alpha_p\}_{p\in\mathbf{N}}$ telle que* $\ldots < \alpha_{p+1} < \alpha_p < \ldots < \alpha_1 < \alpha_0$.

Démonstration. — Remarquons tout d'abord que l'hypothèse 1.1 n'entraîne pas forcément que $\{\alpha, \alpha < \alpha_0$ donné $\}$ soit toujours un ensemble fini (cf. ordre lexicographique). S'il existait une telle suite, soit $E = \cup_{p\in\mathbf{N}}\alpha_p + \mathbf{N}^n$. E est un E-sous- ensemble $\neq \emptyset$ de $\mathbf{N}^n$. Il possède donc une frontière finie $A_1, \ldots, A_s$. Il existe donc i tel que $A_i + \mathbf{N}^n$ contienne une sous-suite infinie extraite de $\{\alpha_p\}$. Soit $\alpha_{n(1)}, \ldots, \alpha_{n(p)}, \ldots$ une telle suite. D'après 1.1, i), $\forall p$, $A_i \leq \alpha_{n(p)}$. Mais $A_i \in E = \cup_p \alpha_p + \mathbf{N}^n$. Il existe donc p_0 tel que $A_i \in \alpha_{p_0} + \mathbf{N}^n$ et $\alpha_{p_0} \leq A_i$. On a donc $\forall p$, $\alpha_{p_0} \leq \alpha_{n(p)}$. Mais si p est assez grand pour que $p_0 < n(p)$, $\alpha_{n(p)} < \alpha_{p_0}$. Contradiction.

1.10. DÉFINITION ET NOTATION . — Soit k un corps commutatif. Etant donné $\{f_1, \ldots, f_s\}$ une suite de s polynômes tous $\neq 0$ dans $k[X_1, \ldots, X_n]$, on lui associe la partition suivante $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$ de $\mathbf{N}^n$:

$$\Delta_1 = \exp f_1 + \mathbf{N}^n, \ldots, \quad \Delta_i = \exp f_i + \mathbf{N}^n - \cup_{j<i}\Delta_i \ldots, \quad i = 1 \ldots s,$$
$$\overline{\Delta} = \mathbf{N}^n - \cup_{i=1\ldots s}\Delta_i.$$

Notez qu'il se peut qu'il existe $i \neq j$ tel que $\exp f_i = \exp f_j$ et que certains parmi les Δ_i $i = 2 \ldots s$ ou $\overline{\Delta}$ peuvent être $\emptyset$.

1.11. THÉORÈME DE DIVISION . — Soit k , $\{f_1, \ldots, f_s\} \in k[X_1, \ldots, X_n]$, $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$ comme en 1.10.

Pour tout $f \in k[X_1, \ldots, X_n]$, il existe $h_1, \ldots, h_s$ et $h \in k[X_1, \ldots, X_n]$ uniques tels que

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

ii) $$\forall i = 1 \ldots s \text{ ,si } h_i = \sum_\alpha c_\alpha^i X^\alpha \ , \ c_\alpha^i \neq 0 \Rightarrow \exp f_i + \alpha \in \Delta_i$$

iii) $$\text{si } h = \sum_{\alpha} c_\alpha X^\alpha \ , \ c_\alpha \neq 0 \Rightarrow \alpha \in \overline{\Delta}.$$

De plus, si $f \neq 0$ et $h \neq 0$, $\exp h \leq \exp f$ et si $f \neq 0$ et $h_i \neq 0$, $\exp h_i + \exp f_i \leq \exp f$.

$h_1, \ldots, h_s, h$ sont obtenus par l'algorithme suivant :

1.11.1. ALGORITHME DE DIVISION . — Si $f = 0$, on pose $h_1 = \ldots = h_s = h = 0$. Si $f \neq 0$, soit $\text{in } f = c_{\alpha_0} X^{\alpha_0}$.

Si $\alpha_0 \in \overline{\Delta}$, soit $h^{(1)} = c_{\alpha_0} X^{\alpha_0}$, $h_i^{(1)} = 0$, $i = 1 \ldots s$ et $f^{(1)} = f - \sum_i h_i^{(1)} f_i - h^{(1)} = f - h^{(1)}$, de sorte que $\exp h^{(1)} = \exp f$ et $\exp f^{(1)} < \exp f$, si $f^{(1)} \neq 0$.

Si $\alpha_0 \in \Delta_i$, soit $h_j^{(1)} = 0$ si $j \neq i$, $h^{(1)} = 0$. Ecrivons que :

$$\alpha_0 = \exp f_i + \beta_0 \ , \ \beta_0 \in \mathbf{N}^n$$
$$\text{in } f_i = \lambda_i X^{\exp f_i} \ , \ \lambda_i \in k \ , \ \lambda_i \neq 0$$

et posons

$$h_i^{(1)} = \frac{c_{\alpha_0}}{\lambda_i} X^{\beta_0}$$

et

$$f^{(1)} = f - \sum_j h_j^{(1)} f_j - h^{(1)} = f - h_i^{(1)} f_i.$$

On a

$$\text{in } h_i^{(1)} f_i = \text{in } h_i^{(1)} . \text{in } f_i = \frac{c_{\alpha_0}}{\lambda_i} X^{\beta_0} . \lambda_i X^{\exp f_i} = c_{\alpha_0} X^{\alpha_0} = \text{in } f,$$

de sorte que $\exp f^{(1)} < \exp f$, si $f^{(1)} \neq 0$.

Si $f^{(1)} = 0$, on s'arrête et $h_1^{(1)}, \ldots, h_s^{(1)}, h^{(1)}$ vérifient bien i), ii), iii). Si $f^{(1)} \neq 0$, on considère $\text{in } f^{(1)} = c_{\alpha_1} X^{\alpha_1}$ et on recommence avec $f^{(1)}$ les mêmes opérations que ci-dessus.

Ainsi de suite, on détermine $h^{(j)}, h_1^{(j)}, \ldots, h_s^{(j)}, f^{(j)}$ tels que :

1) $f^{(j)} = f^{(j-1)} - \sum_i h_i^{(j)} f_i - h^{(j)}$.

2) Si $h_i^{(j)} = \sum_\alpha c_{i\alpha}^{(j)} X^\alpha$, $c_{i\alpha}^{(j)} \neq 0 \Rightarrow \alpha + \exp f_i \in \Delta_i$.

3) Si $h^{(j)} = \sum_\alpha c_\alpha^{(j)} X^\alpha$, $c_\alpha^{(j)} \neq 0 \Rightarrow \alpha \in \overline{\Delta}$

et si $f^{(j-1)}$ et $f^{(j)} \neq 0$, $\exp f^{(j)} < \exp f^{(j-1)}$. De plus, toujours si $f^{(j-1)} \neq 0$ ou $h^{(j)} \neq 0$ et $\exp h^{(j)} = \exp f^{(j-1)}$, ou $h^{(j)} = 0$ et il existe $i(j)$ tel que $h_k^{(j)} = 0$ si $k \neq i(j)$, $h_{i(j)}^{(j)} \neq 0$ et $\exp h_{i(j)}^{(j)} + \exp f_{i(j)} = \exp f^{(j-1)}$.

Un tel processus s'arrête, sinon il existerait une suite infinie d'éléments de $\mathbf{N}^n$, $\alpha_n = \exp f^{(n)}$, strictement décroissante contrairement à 1.9.

Il existe donc n_0 tel que $f^{(n_0)} = 0$; en regroupant les identités obtenues et en posant :

$$h = \sum_{j=1,\ldots,n_0} h^{(j)} \ , \ h_i = \sum_{j=1,\ldots,n_o} h_i^{(j)} \ , \ i = 1, \ldots, s,$$

nous obtenons :

1) $f = \sum h_i f_i + h$.

2) Chacun des $h_i^{(j)}$ est ou 0 ou un monôme et si $h_i^{(j)} \neq 0$, $\exp h_i^{(j)} + \exp f_i \in \Delta_i$. Si $h_i \neq 0$, $\exp h_i$ coïncide avec l'un des $\exp h_i^{(j)}$ et $\exp h_i^{(j)} + \exp f_i = \exp f^{(j-1)} \leq \exp f$.

3) De même chacun des $h^{(j)}$ est 0 ou un monôme. h est donc écrit comme somme de monômes dont les exposants sont tous dans $\overline{\Delta}$. Enfin, si $h \neq 0$, il existe j tel que $h^{(j)} \neq 0$ et $\exp h = \exp h^{(j)} = \exp f^{(j-1)} \leq \exp f$.

L'existence est donc démontrée.

Il reste à prouver l'unicité. Supposons qu'on ait 2 solutions $h_1, \ldots, h_s, h$ et $h'_1, \ldots, h'_s, h'$ vérifiant i), ii) et iii). Il en résulterait que :

$$0 = \sum_i (h_i - h'_i) f_i + (h - h').$$

Si $h - h' \neq 0$, d'après iii) tout monôme X^α non trivial de h et h' vérifiant $\alpha \in \overline{\Delta}$, il en est de même pour $h - h'$ et en particulier $\exp(h - h') \in \overline{\Delta}$. D'après ii) tout monôme non trivial X^α figurant dans h_i et h'_i est tel que $\alpha + \exp f_i \in \Delta_i$, il en est de même pour $h_i - h'_i$ et en particulier $\exp(h_i - h'_i) f_i \in \Delta_i$.

Puisque $\Delta_i \cap \Delta_j = \emptyset$ si $i \neq j$, $\exp \sum_i (h_i - h'_i) f_i = \max_i \exp(h_i - h'_i) f_i$. Il existe donc $i_0 \in 1 \ldots s$ tel que $\exp \sum_i (h_i - h'_i) f_i \in \Delta_{i_0}$. C'est impossible puisque $\Delta_{i_0} \cap \overline{\Delta} = \emptyset$. On a donc $h - h' = 0$. Supposons maintenant que $h_1 - h'_1 \neq 0$. On a donc :

$$-(h_1 - h'_1) f_1 = \sum_{i \geq 2} (h_i - h'_i) f_i.$$

D'une part, $\exp(h_1 - h'_1) f_1 \in \Delta_1$, d'autre part le même raisonnement que ci-dessus montre qu'il existe $i_0 \in 2 \ldots s$ tel que $\exp \sum_{i \geq 2} (h_i - h'_i) f_i \in \Delta_{i_0}$. C'est impossible, puisque $\Delta_{i_0} \cap \Delta_1 = \emptyset$. On a donc $h_1 - h'_1 = 0$.

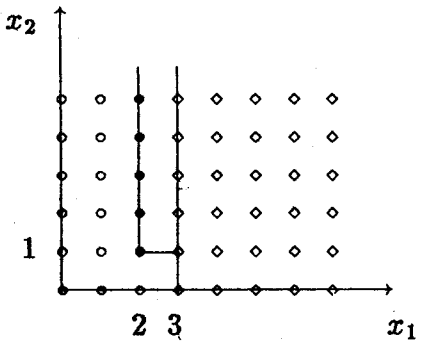
1.12. NOTATIONS ET EXEMPLE . — Le h obtenu dans 1.11 est appelé le reste de la division de f par $\{f_1, \ldots, f_s\}$ et noté $fR\{f_1, \ldots, f_s\}$.

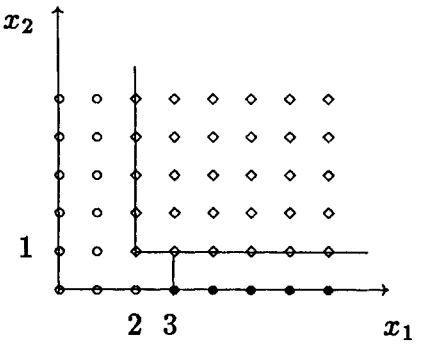
Il faut noter que l'ordre dans lequel on a écrit $f_1, \ldots, f_s$ est important comme le montre l'exemple suivant :

$n = 2$, l'ordre sur $\mathbf{N}^2$ est l'ordre lexicographique

$$f_1 = X_1^3 \ , \ f_2 = X_1^2 X_2 - X_2^3 \ , \ f = X_1^3 X_2.$$

On a $\text{in} f_1 = X_1^3$, $\text{in} f_2 = X_1^2 X_2$, $\text{inf} = X_1^3 X_2$.





◇ Δ_1

• Δ_2

○ $\overline{\Delta}$

partition associée à $\{f_1, f_2\}$
$f\ R\ \{f_1, f_2\} = 0$

partition associée à $\{f_2, f_1\}$
$f\ R\ \{f_2, f_1\} = X_1 X_2^3$

2. Base standard (ou de Gröbner) d'un idéal

Soit k un corps et $I \subset k[X_1, \ldots, X_n]$ un idéal $\neq (0)$.

2.1. DÉFINITIONS ET NOTATIONS . — $\exp I = \{\exp f\ ,\ f \in I\ ,\ f \neq 0\}$, $\exp I$ est un E-ensemble $\neq \emptyset$. Si $\alpha \in \exp I$, $\exists f \in I$, $f \neq 0$, $\alpha = \exp f$. Si $\gamma \in \mathbf{N}^n$, $\alpha + \gamma = \exp X^\gamma f$.

On appelle *escalier de* I et *on note* $E(I)$ l'escalier de $\exp I$ (définition 1.8).

On appelle *base standard* (ou de Gröbner) de I tout ensemble de polynômes $(f_1, \ldots, f_s)$ de I tel que $(\exp f_1, \ldots, \exp f_s)$ soit une frontière de I , autrement dit tel que :

$$\exp I = \bigcup_{i=1\ldots s} \exp f_i + \mathbf{N}^n.$$

On appelle *base standard minimale* une base standard de cardinal minimal, autrement dit telle que $(\exp f_1, \ldots, \exp f_s)$ soit l'escalier de $\exp I$.

2.2. REMARQUE . — Une base standard est un ensemble fini de polynômes et non pas une suite.

2.3. PROPOSITION. — *Une base standard* $(f_1, \ldots, f_s)$ *d'un idéal* $I \neq (0)$ *est un système de générateurs de* I.

Démonstration. — Ordonnons les éléments de la base standard par exemple en choisissant l'ordre fourni par l'indiciation et soit $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$ la partition de $\mathbf{N}^n$ associée à la suite $\{(f_1, \ldots, f_s)\}$ (1.10).

Soit $f \in I$. Du théorème de division (1.11), nous déduisons qu'il existe $h_1, \ldots, h_s$, $h \in k[X_1, \ldots, X_n]$ tels que :

$$f = \sum h_i f_i + h$$

et si $h = \sum c_\alpha X^\alpha$, $c_\alpha \neq 0 \Rightarrow \alpha \in \overline{\Delta}$.

Puisque $f \in I, h \in I$. Si $h \neq 0$, $\exp h \in \exp I = \cup_i \exp f_i + \mathbf{N}^n = \cup_i \Delta_i$. Or, $\exp h \in \overline{\Delta} = \mathbf{N}^n - \cup_i \Delta_i$. Il y a donc contradiction et $h = 0$.

2.3.1. COROLLAIRE. — *Tout idéal de* $k[X_1, \ldots, X_n]$ *peut être engendré par un nombre fini d'éléments.*

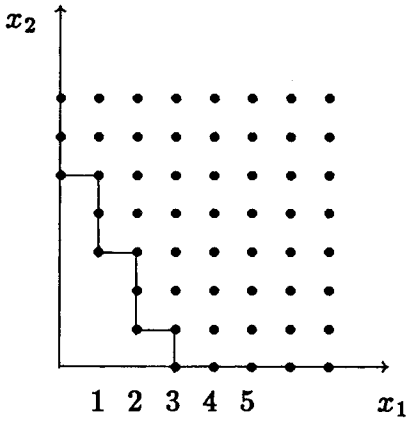
2.3.2. DÉFINITION. — *On dit qu'un anneau (commutatif, unitaire)* A *est noethérien si tout idéal de* A *peut être engendré par un nombre fini d'éléments.*

2.3.3. COROLLAIRE. — *$k[X_1,\dots,X_n]$ est un anneau noethérien.*

2.4. REMARQUES . — Si $(f_1,\dots,f_s)$ est un système de générateurs minimal de I, il se peut que $\exp I \neq \cup \exp f_i + \mathbf{N}^n$.

Une base standard minimale n'est pas nécessairement un système de générateurs minimal.

2.4.1. EXEMPLE . — Reprenons l'exemple de 1.12 : $f_1 = X_1^3$, $f_2 = X_1^2X_2 - X_2^3$, $I = (f_1, f_2)$.



Pour l'ordre lexicographique $\exp f_1 = X_1^3$, $\exp f_2 = X_1^2X_2$, $X_2f_1 - X_1f_2 = X_1X_2^3$. Donc $X_1X_2^3 \in I$ et $(1,3) \in \exp I$. Soit $f_3 = X_1X_2^3$, $X_1f_3 - X_2^2f_2 = X_2^5$. Donc $X_2^5 \in I$ et $(0,5) \in \exp I$. Soit $f_4 = X_2^5$. On démontrera plus tard que f_1, f_2, f_3, f_4 est une base standard minimale de I et que $E(I) = \{(3,0),(2,1),(1,3),(0,5)\}$. $\exp I \neq \cup_{i=1.2} \exp f_i + \mathbf{N}^2$. Une base standard minimale comporte 4 éléments, tandis que I peut être engendré par 2 générateurs.

2.5. REMARQUE . — Soit k' une extension de k , I' l'idéal engendré par I dans $k'[X_1,\dots,X_n]$. $E(I) = E(I')$. Toute base standard de I est une base standard de I' .

Démonstration. — Evidemment $E(I) \subset E(I')$. Soit $f' \in I' \neq 0$. Soit $(e_\alpha)_{\alpha\in\mathcal{A}}$ une base de k' sur k . Il existe $f_\alpha \in I$ tous nuls, sauf un nombre fini d'entre eux tels que :

$$f' = \sum_\alpha f_\alpha e_\alpha .$$

Soit $A = \max_{\alpha\in\mathcal{A}:f_\alpha\neq 0} \exp f_\alpha$. $A \in \exp I$ et $A = \exp f'$. En effet, si $\mathcal{A}' = \{\alpha \in \mathcal{A} \ , \ f_\alpha \neq 0 \ , \ \exp f_\alpha = A\}$ le monôme en X^A dans f' est $\sum_{\alpha\in\mathcal{A}'} \text{in}\, f_\alpha e_\alpha = (\sum_{\alpha\in\mathcal{A}'} \lambda_\alpha e_\alpha)X^A \neq 0$.

2.6. PROPOSITION. — *Soit $(f_1,\dots,f_s)$,$(f'_1,\dots,f'_{s'})$ 2 bases standard de I . On a :*

$$fR\{f_1,\dots,f_s\} = fR\{f'_1,\dots,f'_{s'}\}$$

(l'ordre choisi est celui induit par l'indiciation).

Démonstration. — Soit $A_i = \exp f_i$, $A'_i = \exp f'_i$. Soit $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$, $\Delta'_1, \ldots, \Delta'_{s'}, \overline{\Delta}'$ les partitions respectives de $\mathbf{N}^n$ associées aux suites $\{f_1, \ldots, f_s\}$; $\{f'_1, \ldots, f'_{s'}\}$. On a :

$$\exp I = \cup_i A_i + \mathbf{N}^n = \cup_i \Delta_i = \cup_i A'_i + \mathbf{N}^n = \cup_i \Delta'_i.$$

Il s'ensuit que $\overline{\Delta} = \overline{\Delta}'$.

Ecrivons la division de f par $\{f_1, \ldots, f_s\}$ et par $\{f'_1, \ldots, f'_{s'}\}$

$$f = \sum h_i f_i + fR\{f_1, \ldots, f_s\}$$
$$= \sum h'_i f'_i + fR\{f'_1, \ldots, f'_{s'}\}$$

et si $fR\{f_1, \ldots, f_s\} = \sum c_\alpha X^\alpha$, $c_\alpha \neq 0 \Rightarrow \alpha \in \overline{\Delta}$
et $fR\{f'_1, \ldots, f'_{s'}\} = \sum c'_\alpha X^\alpha$, $c'_\alpha \neq 0 \Rightarrow \alpha \in \overline{\Delta}' = \overline{\Delta}$.

Il en résulte que si $g = fR\{f_1, \ldots, f_s\} - fR\{f'_1, \ldots, f'_{s'}\} \neq 0$, $\exp g \in \overline{\Delta}$. Or, $g \in I$, $\exp g \in \exp I = \cup_i \Delta_i = \mathbf{N}^n - \overline{\Delta}$. Il y a contradiction. Donc $g = 0$.

2.7. REMARQUE - DÉFINITION . — Le reste de la division de f par une suite de polynômes dont l'ensemble sous-jacent est une base standard de I ne dépend pas de cette base standard, ni de l'ordre choisi sur ses éléments. On l'appelle le reste de la divison de f par I et on le note fRI . Il possède donc les propriétés :

1) si $fRI = \sum c_\alpha X^\alpha$, $c_\alpha \neq 0 \Rightarrow \alpha \notin \exp I$

2) si $fRI \neq 0$, $\exp fRI \leq \exp f$

3) $(fRI)RI = fRI$.

2.8. PROPOSITION . — *Les conditions suivantes sont équivalentes :*

i) $f \in I$

ii) $fRI = 0$

Démonstration. — Choisissant une base standard $(f_1, \ldots, f_s)$ de I et un ordre sur ses éléments, on a : $fRI = fR\{f_1, \ldots, f_s\} = f - \sum h_i f_i$ (1.11). Si donc $f \in I$, $fRI \in I$. Si $fRI \neq 0$, on a $\exp fRI \in \exp I$. Mais d'après 2.7. 1) $\exp fRI \notin \exp I$. Donc $fRI = 0$ et i) $\Rightarrow$ ii). Réciproquement, si $fRI = 0$, $f = \sum h_i f_i \in I$.

2.9. COROLLAIRE . — *Les classes modulo I des X^α , $\alpha \in \mathbf{N}^n - \exp I$ forment une k-base de $k[X_1, \ldots, X_n]/I$. En particulier, pour que $k[X_1, \ldots, X_n]/I$ soit un espace vectoriel de rang fini sur k , il faut et il suffit que cardinal $\mathbf{N}^n - \exp I < \infty$ et on a alors*

$$\mathrm{rg}_k k[X_1, \ldots, X_n]/I = \sharp \mathbf{N}^n - \exp I.$$

Démonstration. — Les classes modulo I des X^α , $\alpha \notin \exp I$ engendrent $k[X_1, \ldots, X_n]/I$ d'après 2.7.

Elles sont linéairement indépendantes. Si $f = \sum_{\alpha \notin \exp I} c_\alpha X^\alpha \in I$, $f = 0$ sinon $\exp f \in \exp I$ et $\exp f \notin \exp I$.

3. Algorithme de calcul d'une base standard

La question se pose maintenant de savoir comment, étant donné un système de générateurs d'un idéal I , construire une base standard de cet idéal. Nous allons tout d'abord donner un critère pour reconnaître qu'une suite de polynômes $\{f_1,\dots,f_s\}$ de I a pour ensemble sous-jacent une base standard de I .

3.1. PROPOSITION. — *Une condition nécessaire et suffisante pour que l'ensemble sous-jacent à une suite de polynômes $\{f_1,\dots,f_s\}$ de I soit une base standard de I est que pour tout $f \in I$, $fR\{f_1,\dots,f_s\} = 0$.*

Démonstration. — La condition est nécessaire. En effet, si $(f_1,\dots,f_s)$ est une base standard, $fR\{f_1,\dots,f_s\} = fRI = 0$ si $f \in I$ (2.8).

La condition est suffisante. Il s'agit de montrer que $\exp I = \cup_i \exp f_i + \mathbf{N}^n$.

Soit $f \in I$, $f \neq 0$. D'après 1.11, il existe $h_1,\dots,h_s \in k[X_1,\dots,X_n]$ tels que :

i) $f = \sum h_i f_i + fR\{f_1,\dots,f_s\} = \sum h_i f_i$

ii) $\forall i = 1\dots s$, si $h_i = \sum_\alpha c_\alpha^i X^\alpha$, $c_\alpha^i \neq 0 \Rightarrow \exp f_i + \alpha \in \Delta_i$ où $\Delta_1,\dots,\Delta_s,\overline{\Delta}$ est la partition de $\mathbf{N}^n$ associée à $f_1,\dots,f_s$. Il en résulte que $\exp h_i f_i = \exp h_i + \exp f_i \in \Delta_i$, $\forall i = 1\dots s$, et puisque $\Delta_i \cap \Delta_j = \emptyset$ si $i \neq j$, $\exp \sum h_i f_i = \max_{i=1\dots s} \exp h_i f_i$. Il existe donc i_0 tel que $\exp f \in \Delta_{i_0} \subset \exp f_{i_0} + \mathbf{N}^n$.

Cette proposition est insuffisante en pratique, car il faut tester une infinité de f . Nous allons voir qu'on peut se ramener à un nombre fini.

3.2. UNE CONSTRUCTION . — Soit $f,g \in k[X_1,\dots,X_n]$ tous deux $\neq 0$. Soit $\exp f = (\alpha_1,\dots,\alpha_n)$, $\exp g = (\beta_1,\dots,\beta_n)$. On pose : $\gamma_i = \sup(\alpha_i,\beta_i)$ $i = 1\dots n$ et $\gamma = (\gamma_1,\dots,\gamma_n)$. Si $\operatorname{in} f = \lambda X^\alpha$ et $\operatorname{in} g = \nu X^\beta$, $\lambda \neq 0$, $\nu \neq 0$, on pose :

$$fSg = \nu X_1^{\gamma_1-\alpha_1}\dots X_n^{\gamma_n-\alpha_n} f - \lambda X_1^{\gamma_1-\beta_1}\dots X_n^{\gamma_n-\beta_n} g$$

de sorte que $\exp fSg < \gamma$ si $fSg \neq 0$.

Il se peut que $\gamma = \alpha$. Ceci est le cas si $\alpha \in \beta + \mathbf{N}^n$, (de même $\gamma = \beta$). Il se peut aussi que $\gamma = \alpha + \beta$. C'est le cas si $\alpha_i \neq 0$ implique $\beta_i = 0$; $\operatorname{in} f$ et $\operatorname{in} g$ ne contiennent pas les mêmes variables.

3.3. THÉORÈME . — *Une condition nécessaire et suffisante pour qu'un système de générateurs $(f_1,\dots,f_s)$ d'un idéal $I \neq (0)$ soit une base standard de I est que, ordonnant les f_i selon leur indiciation, pour tout (i,j) , $i < j$, $f_i S f_j R\{f_1,\dots,f_s\} = 0$ (les $f_i, i = 1\dots s$ sont implicitement supposés tous $\neq 0$).*

Démonstration. — La condition est tout d'abord nécessaire d'après 3.1, puisque $f_i S f_j \in I$.

Montrons qu'elle est suffisante. Il suffit, d'après 3.1 de voir que pour tout $f \in I$, $fR\{f_1, \ldots, f_s\} = 0$.

Soit donc $f \in I$ et soit $g = fR\{f_1, \ldots, f_s\}$; si $g \neq 0$ et si $g = \sum c_\alpha X^\alpha$, on sait que $c_\alpha \neq 0 \Rightarrow \alpha \in \mathbf{N}^n - \cup_{i=1\ldots s} \exp f_i + \mathbf{N}^n$; d'autre part, il existe h_i , $i \in 1 \ldots s$ tels que $f = \sum h_i f_i + g$ et $g \in I$. Puisque $f_1, \ldots, f_s$ est un système de générateurs de I , il existe $H_1, \ldots, H_s \in k[X_1, \ldots, X_n]$ non tous nuls (sans contrainte a priori sur la position des monômes) tels que :

$$g = H_1 f_1 + \cdots + H_s f_s \, .$$

Soit

$$N = \max_{i, H_i \neq 0} \exp H_i f_i \, .$$

S'il existait un seul i tel que $\exp H_i f_i = N$, on aurait $\exp g = N$. En effet, soit i_0 l'indice en question. Tout exposant de monôme dans $H_i f_i$, $i \neq i_0$ est plus petit ou égal à $\exp H_i f_i$, lui-même plus petit que N , tout exposant de monôme dans $H_{i_0} f_{i_0}$ est plus petit que N s'il en est $\neq$. Mais alors, $\exp g = \exp H_{i_0} f_{i_0} = \exp H_{i_0} + \exp f_{i_0}$. Or $\exp g \notin \cup_i \exp f_i + \mathbf{N}^n$. C'est donc qu'il existe au moins $i \neq j$ tels que $\exp H_i f_i = \exp H_j f_j = N$. Soit $i_0 < i_1 < \cdots < i_t$, $t \geq 1$, ceux des indices i rangés dans l'ordre croissant tels que $\exp H_i f_i = N$.

Posons

$$\begin{aligned}
\operatorname{in} f_{i_0} &= \lambda_{i_0} X_1^{\alpha_1} \ldots X_n^{\alpha_n} \quad , \quad \lambda_{i_0} \in k \quad , \quad \lambda_{i_0} \neq 0 \\
\operatorname{in} f_{i_1} &= \lambda_{i_1} X_1^{\beta_1} \ldots X_n^{\beta_n} \quad , \quad \lambda_{i_1} \in k \quad , \quad \lambda_{i_1} \neq 0 \\
\operatorname{in} H_{i_0} &= \nu_{i_0} X_1^{u_1} \ldots X_n^{u_n} \quad , \quad \nu_{i_0} \in k \quad , \quad \nu_{i_0} \neq 0 \\
\operatorname{in} H_{i_1} &= \nu_{i_1} X_1^{v_1} \ldots X_n^{v_n} \quad , \quad \nu_{i_1} \in k \quad , \quad \nu_{i_1} \neq 0
\end{aligned}$$

On a $\alpha + u = \beta + v = N$. Soit $\gamma_i = \sup(\alpha_i, \beta_i), i = 1 \ldots n, \gamma = (\gamma_1, \ldots, \gamma_n)$. On vérifie que $u_i \geq \gamma_i - \alpha_i$ et $v_i \geq \gamma_i - \beta_i, i = 1 \ldots n$. (En effet ou $\alpha_i \geq \beta_i$, $\gamma_i = \alpha_i$ et $u_i \geq 0$, ou $\beta_i \geq \alpha_i$, $\gamma_i = \beta_i$ et $u_i = \beta_i - \alpha_i + v_i \geq \beta_i - \alpha_i$).

Posons alors $p_i = u_i - (\gamma_i - \alpha_i) = v_i - (\gamma_i - \beta_i)$, $p_i \in \mathbf{N}$. Par définition de $f_{i_0} S f_{i_1}$, on a :

$$\begin{aligned}
X_1^{p_1} \ldots X_n^{p_n} f_{i_0} S f_{i_1} &= \lambda_{i_1} X^u f_{i_0} - \lambda_{i_0} X^v f_{i_1} \\
(*) \qquad &= \lambda_{i_1} / \nu_{i_0} (\operatorname{in} H_{i_0}) f_{i_0} - \lambda_{i_0} / \nu_{i_1} (\operatorname{in} H_{i_1}) f_{i_1} \, .
\end{aligned}$$

Récrivant alors g :

$$\begin{aligned}
g = &(\operatorname{in} H_{i_0}) f_{i_0} + (\operatorname{in} H_{i_1}) f_{i_1} + (H_{i_0} - \operatorname{in} H_{i_0}) f_{i_0} + (H_{i_1} - \operatorname{in} H_{i_1}) f_{i_1} \\
&+ \sum_{j \geq 2} H_{i_j} f_{i_j} + \sum_{i \neq i_0, \ldots, i_t} H_i f_i
\end{aligned}$$

et tenant compte de (*), il vient :

$$\begin{aligned}
g = &\nu_{i_0} / \lambda_{i_1} X^p f_{i_0} S f_{i_1} + (1 + \lambda_{i_0} \nu_{i_0} / \lambda_{i_1} \nu_{i_1}) (\operatorname{in} H_{i_1}) f_{i_1} \\
&+ \sum_{j \geq 2} H_{i_j} f_{i_j} + (H_{i_0} - \operatorname{in} H_{i_0}) f_{i_0} + (H_{i_1} - \operatorname{in} H_{i_1}) f_{i_1} + \sum_{i \neq i_0 \ldots i_t} H_i f_i .
\end{aligned}$$

Posant

$$H'_{i_0} = H_{i_0} - \operatorname{in} H_{i_0}$$
$$H'_{i_1} = H_{i_1} + \lambda_{i_0}\nu_{i_0}/\lambda_{i_1}\nu_{i_1} \cdot \operatorname{in} H_{i_1}$$
$$H'_i = H_i \quad i \neq i_0, i_1$$

on a

$$\exp H'_{i_0} f_{i_0} < N \ , \quad \text{si} \quad H'_{i_0} \neq 0 \ ,$$
$$\exp H'_{i_1} f_{i_1} \leq N \ , \quad \text{si} \quad H'_{i_1} \neq 0 \ ,$$
$$\exp H'_{i_j} f_{i_j} = N \ , \quad j \geq 2 \ ,$$
$$\exp H'_i f_i < N \ , \quad i \neq i_0, \ldots, i_t \quad \text{si} \quad H'_i \neq 0 \ ,$$

et

$$g = \nu_{i_0}/\lambda_{i_1} X^p f_{i_0} S f_{i_1} + \sum H'_i f_i .$$

Finalement

$$\exp X^p f_{i_0} S f_{i_1} = p + \exp f_{i_0} S f_{i_1} < p + \gamma = N \ , \quad \text{si} \quad f_{i_0} S f_{i_1} \neq 0 \ .$$

Ou bien $H'_i = 0 \ , \ i = 1, \ldots, s$. Ou bien $N' = \max_{i, H'_i \neq 0} \exp H'_i f_i < N$. Ou bien $N' = N$ et dans ce cas, comme ci-dessus, il existe au moins $i' \neq j'$ tels que $\exp H'_{i'} f_{i'} = \exp H'_{j'} f_{j'} = N' = N$. Une suite de calculs semblables à celui que nous venons d'effectuer va nous fournir $q_{ij} \in \mathbf{N}^n$, $\lambda_{ij} \in k$, $i < j$, $i = i_0, \ldots, i_t$, $j = i_0, \ldots, i_t$, et $\tilde{H}_i \in k[X_1, \ldots, X_n]$, $i = 1, \ldots, s$ tels que :

$$g = \sum_{i<j, i=i_0 \ldots i_t, j=i_0 \ldots i_t} \lambda_{ij} X^{q_{ij}} f_i S f_j + \sum_i \tilde{H}_i f_i$$

et que

$$\exp X^{q_{ij}} f_i S f_j < N$$

et ou bien $\tilde{H}_i = 0, i = 1 \ldots s$ ou $\max_{i, \tilde{H}_i \neq 0} \exp \tilde{H}_i f_i < N$. Or, par hypothèse, $f_i S f_j R\{f_1, \ldots, f_s\} = 0$.

De 1.11, on déduit alors l'existence de $h^l_{ij} \in k[X_1, \ldots, X_n]$ tels que $f_i S f_j = \sum_l h^l_{ij} f_l$ et que si $h^l_{ij} \neq 0$, $\exp h^l_{ij} f_l \leq \exp f_i S f_j$. Alors $X^{q_{ij}} f_i S f_j = \sum_l X^{q_{ij}} h^l_{ij} f_l$ et si $h^l_{ij} \neq 0$, $\exp X^{q_{ij}} h^l_{ij} f_i \leq \exp X^{q_{ij}} f_i S f_j < N$.

On a donc finalement obtenu une nouvelle expression pour g

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

où $N_1 = \max_{i, \overline{H}_i \neq 0} \exp \overline{H}_i f_i < N$. On peut recommencer avec cette nouvelle expression pour g toute la séquence de calculs. Finalement, on détermine ainsi, si $g \neq 0$, une suite infinie $\{N_p\}_{p \in \mathbf{N}}$ telle que $\cdots N_{p+1} < N_p < \cdots < N_1 < N$. C'est impossible, d'après 1.9.

3.4. EXEMPLE . — Vérifions maintenant que dans l'exemple 2.4.1 f_1, f_2, f_3, f_4 est une base standard pour l'ordre lexicographique :

$$
\begin{array}{lll}
f_1Sf_2 = X_2f_1 - X_1f_2 = f_3\,, & f_3R\{f_1,f_2,f_3,f_4\} & = 0 \\
f_1Sf_3 = X_2^3f_1 - X_1^2f_3 = 0 & & \\
f_1Sf_4 = X_2^5f_1 - X_1^3f_4 = 0 & & \\
f_2Sf_3 = X_2^2f_2 - X_1f_3 = -f_4\,, & f_4R\{f_1,f_2,f_3,f_4\} & = 0 \\
f_2Sf_4 = X_2^4f_2 - X_1^2f_4 = -X_2^7\,, & X_2^7 = X_2^2f_4\,, (0,7) \in \Delta_4\,, & \\
f_3Sf_4 = X_2^2f_3 - X_1f_4 = 0\,, & \Delta_4 = \{(0,\alpha)\alpha \in \mathbf{N}, \alpha \geq 5\} & \\
 & X_2^7R\{f_1,f_2,f_3,f_4\} & = 0.
\end{array}
$$

Ceci va nous permettre d'obtenir un algorithme pour calculer une base standard d'un idéal I dont on s'est donné un système de générateurs $(f_1, \ldots, f_s)$.

3.5. ALGORITHME . — On ordonne les générateurs, par exemple en choisissant l'ordre provenant de l'indiciation. Si pour tout (i,j) , $i < j$, $f_iSf_jR\{f_1, \ldots, f_s\} = 0$, $(f_1, \ldots, f_s)$ est une base standard. Sinon, il existe au moins un couple i,j tel que $f_iSf_jR\{f_1, \ldots, f_s\} \neq 0$. Posons $f_{s+1} = f_iSf_jR\{f_1, \ldots, f_s\}$.

Remarquons que si $f_iSf_jR\{f_1, \ldots, f_s\} = 0$, alors $f_iSf_jR\{f_1, \ldots, f_{s+1}\} = 0$. En effet, la partition de $\mathbf{N}^n$ associée à $\{f_1, \ldots, f_s\}$ étant $\Delta_1, \ldots, \Delta_s, \overline{\Delta}$ la partition de $\mathbf{N}^n$ associée à $\{f_1, \ldots, f_{s+1}\}$ est $\Delta_1, \ldots, \Delta_s, \Delta_{s+1}, \overline{\Delta}'$. Si $gR\{f_1, \ldots, f_s\} = 0$ et si $g = \sum_{i=1\ldots s} h_if_i$ vérifient i), ii), iii) de 1.11 relativement à $\{f_1, \ldots, f_s\}$, $g = \sum_{i=1\ldots s} h_if_i + 0f_{s+1}$ vérifient i), ii), iii) de 1.11 relativement à $\{f_1, \ldots, f_s\}$ et d'après l'unicité $gR\{f_1, \ldots, f_{s+1}\} = 0$.

Si pour tout (i,j) , $i < j$, $i = 1 \ldots s+1$, $j = 1 \ldots s+1$, $f_iSf_jR\{f_1, \ldots, f_{s+1}\} = 0$, $(f_1, \ldots, f_{s+1})$ est une base standard de I . Sinon, il existe un couple (i,j) , $i < j$, $i = 1 \ldots s+1$, $j = 1 \ldots s+1$, tel que $f_iSf_jR\{f_1, \ldots, f_{s+1}\} \neq 0$. On pose $f_{s+2} = f_iSf_jR\{f_1, \ldots, f_{s+1}\}$ etc.

Ce processus de construction s'arrête certainement, sinon on construirait une suite $\{f_p\}_{p \in \mathbf{N}}$ d'éléments de I tous $\neq 0$.

Soit $F = \cup_p \exp f_p + \mathbf{N}^n$. F est un E-ensemble $\neq \emptyset$. Il possède donc une frontière finie $A_1, \ldots, A_r$ (1.6). $\forall i = 1 \ldots r$, il existe $p(i) \in \mathbf{N}$ tel que $A_i \in \exp f_{p(i)} + \mathbf{N}^n$. Soit $t = \sup_{i=1\ldots r} p(i)$. On a donc $F \subset \cup_{i=1\ldots t} \exp f_i + \mathbf{N}^n$ et l'inclusion opposée étant évidente, $F = \cup_{i=1\ldots t} \exp f_i + \mathbf{N}^n$. Or, $f_{t+1} \neq 0$ et il existe i,j , $i < j$, $i = 1 \ldots t$, $j = 1 \ldots t$ tel que $f_{t+1} = f_iSf_jR\{f_1, \ldots, f_t\}$. Donc, d'après 1.11, iii) $\exp f_{t+1} \in \mathbf{N}^n - \cup_{i=1\ldots t} \exp f_i + \mathbf{N}^n$. Or, $\exp f_{t+1} \in F$, d'où la contradiction.

3.6. REMARQUE . — Cette construction n'apporte aucune information sur les $\exp f_i$, $i \geq s+1$. $|\exp f_i|$ peut-il devenir très grand par rapport aux données initiales?

3.7. LEMME . — *Soit F un E-ensemble et $A_1, \ldots, A_t$ une frontière de F. Si $t > \sharp$ escalier de F (1.8), il existe j , $j \in 1 \ldots t$, tel que $A_1, \ldots, \widehat{A_j}, \ldots, A_t$ soit une frontière de F . ($\widehat{\ }$ sur A_j signifie qu'il a été oté).*

Démonstration. — F possède une frontière $B_1, \ldots, B_{t'}$ avec $t' < t$. On a donc :

$$F = \cup_{i=1\ldots t} A_i + \mathbf{N}^n = \cup_{i=1\ldots t'} B_i + \mathbf{N}^n$$

$\forall i = 1 \ldots t'$, $\exists \sigma(i) \in 1 \ldots t$ tel que $B_i \in A_{\sigma(i)} + \mathbf{N}^n$. Alors

$$F \subset \cup_{i=1\ldots t'} A_{\sigma(i)} + \mathbf{N}^n$$

et

$$F = \cup_{i=1\ldots t'} A_{\sigma(i)} + \mathbf{N}^n.$$

Il suffit de choisir $j \notin \mathrm{Im}\sigma$.

3.8. ALGORITHME . — $(f_1, \ldots f_t)$ étant une base standard de I , pour obtenir une base standard minimale, on procède comme suit :

Ou $\forall i = 1 \ldots, t$, $\exp f_i \notin \cup_{j \neq i} \exp f_j + \mathbf{N}^n$ et $f_1, \ldots, f_t$ est une base standard minimale (3.7).

Ou $\exists i_0 = 1 \ldots t$, tel que : $\exp f_{i_0} \in \cup_{j \neq i_0} \exp f_j + \mathbf{N}^n$. On a encore $E(I) = \cup_{j \neq i_0} \exp f_j + \mathbf{N}^n$. On supprime $f_{i_0} \ldots$ etc. Ce processus d'élimination s'arrête nécessairement.

4. Un énoncé d'élimination

Dans ce paragraphe, l'ordre total choisi sur $\mathbf{N}^n$ est *l'ordre lexicographique* (1.1.2.1).

4.1. LEMME. — *Soit* $f \in k[X_1, \ldots, X_n]$, $f \neq 0$. *Soit* $t \in \mathbf{N}$, $0 \leq t < n$. *Les conditions suivantes sont équivalentes :*

i) $f \in k[X_{t+1}, \ldots, X_n]$

ii) $\operatorname{in} f \in k[X_{t+1}, \ldots, X_n]$.

Démonstration. — i) $\Rightarrow$ ii) trivialement.

ii) $\Rightarrow$ i). Si $X_1^{\alpha_1} \ldots X_t^{\alpha_t} X_{t+1}^{\alpha_{t+1}} \ldots X_n^{\alpha_n}$ est un monôme figurant effectivement dans f ,$(\alpha_1, \ldots, \alpha_t, \alpha_{t+1}, \ldots, \alpha_n) \leq \exp f = (0, \ldots, 0, \beta_{t+1}, \ldots, \beta_n)$. Ceci entraîne que $\alpha_1 = \cdots = \alpha_t = 0$.

4.2. THÉORÈME . — *Soit* I *un idéal de* $k[X_1, \ldots, X_n] \neq (0)$. *Soit* $(f_1, \ldots, f_s)$ *une base standard de* I *pour l'ordre lexicographique. Soit* $t \in \mathbf{N}$, $0 \leq t < n$. *Soit* $J = \{i, i = 1 \ldots s, f_i \in k[X_{t+1}, \ldots, X_n]\}$. *Si* $J = \emptyset$, $I \cap k[X_{t+1}, \ldots, X_n] = (0)$. *Si* $J \neq \emptyset$, $(\ldots, f_i, \ldots)_{i \in J}$ *est une base standard de* $I \cap k[X_{t+1}, \ldots, X_n]$ *pour l'ordre lexicographique. En particulier, c'est un système de générateurs de* $I \cap k[X_{t+1}, \ldots, X_n]$ *(2.3).*

Démonstration. — Soit $f \in I \cap k[X_{t+1}, \ldots, X_n]$; si $f \neq 0$, $\operatorname{in} f \in k[X_{t+1}, \ldots, X_n]$. Divisons f par $\{f_1, \ldots, f_s\}$. $fR\{f_1, \ldots, f_s\} = fRI = 0$ (2.8) et il existe $h_1, \ldots, h_s \in k[X_1, \ldots, X_n]$ tels que :

$$f = \sum_i h_i f_i$$

et vérifiant ii) de 1.11.

Il en résulte qu'il existe $i \in 1 \ldots s$ tel que $\operatorname{in} f = \operatorname{in} h_i . \operatorname{in} f_i$. Par suite $\operatorname{in} h_i$, $\operatorname{in} f_i \in k[X_{t+1}, \ldots, X_n]$ et d'après 4.1, h_i et $f_i \in k[X_{t+1}, \ldots, X_n]$, de sorte que $i \in J$ et $J \neq \emptyset$. Si donc $J = \emptyset$, $I \cap k[X_{t+1}, \ldots, X_n]$ se réduit à 0 .

Si $J \neq \emptyset$, on a donc

$$\exp(I \cap k[X_{t+1}, \ldots, X_n]) \subset \cup_{i \in J} \exp f_i + \mathbf{N}^{n-t}.$$

L'autre inclusion étant évidente, $\exp I \cap k[X_{t+1}, \ldots, X_n] = \cup_{i \in J} \exp f_i + \mathbf{N}^{n-t}$ et par définition (2.1), $(f_i)_{i \in J}$ est une base standard de $I \cap k[X_{t+1}, \ldots, X_n]$ pour l'ordre lexicographique.

(Identifiant $0 \times \mathbf{N}^{n-t}$ à $\mathbf{N}^{n-t}$, l'ordre lexicographique de $\mathbf{N}^n$ induit sur $\mathbf{N}^{n-t}$ l'ordre lexicographique).

Exercice

k est un corps et I un idéal $\neq 0$ de $k[X_1, \ldots, X_n]$. Soit $(f_1, \ldots, f_s)$ des éléments tous $\neq 0$ de I . On dit que $(f_1, \ldots, f_s)$ est une base standard réduite de I si

1) $(f_1, \ldots, f_s)$ est une base standard de I;

2) $\forall i, i = 1 \ldots s$, $\text{in}\, f_i = X^{\exp f_i}$;

3) $\forall i, i = 1 \ldots s$, $f_i R\{f_1, \ldots, \widehat{f_i}, \ldots, f_s\} = f_i$;

(la notation $\widehat{f_i}$ signifie que f_i a été supprimé de la suite $\{f_1, \ldots, f_s\}$).

1) Montrer qu'une base standard réduite de I est une base standard de cardinal minimal de I . Soit t ce nombre.

2) Montrer que si $(f_1, \ldots, f_t), (f'_1, \ldots, f'_t)$ sont 2-bases standard réduites de I , il existe σ une permutation de $\{1 \ldots t\}$ telle que $f_i = f'_{\sigma(i)}, i = 1 \ldots t$. Pour ce faire, on montrera d'abord qu'il existe σ une permutation de $\{1, \ldots, t\}$ telle que $\text{in}\, f_i = \text{in}\, f'_{\sigma(i)}, i = 1 \ldots t$ .On considèrera ensuite la division de $f'_{\sigma(i)}$ par $\{f_1, \ldots, f_t\}$.

3) $(f_1, \ldots, f_t)$ étant une base standard de I telle que $\text{in}\, f_i = X^{\exp f_i}$, $i = 1 \ldots t$, soit $g_i = f_i R\{f_1, \ldots, \hat{f}_i, \ldots, f_t\}$, $i = 1 \ldots t$. Montrer que $(g_1, \ldots, g_t)$ est une base standard réduite de I .