CHAPITRE 2

CALCUL DANS UNE ALGÈBRE QUOTIENT

Sommaire

Dans ce chapitre, nous allons définir les notions de formes normales et de bases de Gröbner, puis donner quelques unes de leurs applications qui seront utiles par la suite. Pour une présentation détaillée, consulter [**AL94**], [**BWK93**], [**CLO92**], [**Eis94**].

2.1. Introduction

Soit f un polynôme d'une variable, de degré m et à coefficients dans $\mathbb{K}$. L'algorithme d'Euclide assure que tout $g \in \mathbb{K}[x]$ peut se réduire modulo f : il existe un unique $(q, r) \in \mathbb{K}[x]^2$ tel que $g = qf + r$, où le reste r est une combinaison linéaire des monômes $1, x, \ldots, x^{m-1}$. Cette réduction consiste à trouver un représentant canonique d'un élément quelconque de l'algèbre quotient $\mathbb{K}[x]/(f)$. C'est la clé de l'étude de certains problèmes effectifs, tels que le calcul du pgcd et ppcm de polynômes, le problème de l'appartenance d'un polynôme à un idéal $I = (f_1, \ldots, f_s)$ de $\mathbb{K}[x]$, le calcul d'une base de l'espace vectoriel $\mathcal{A} = \mathbb{K}[x]/I$, le calcul des représentants canoniques des éléments de $\mathcal{A}$, ...

Pour étudier des problèmes de même nature dans le cas multivariable, nous avons besoin d'une généralisation de l'algorithme d'Euclide :

> *Étant donnés* $f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$, *comment peut-on réduire* $g \in \mathbb{K}[\mathbf{x}]$ *modulo* $f_1, \ldots, f_s$ *? C'est-à-dire, trouver des polynômes* $q_1, \ldots, q_s, r$ *tels que* $g = q_1 f_1 + \cdots + q_s f_s + r$, *où* r *est « le représentant canonique » de* g *modulo l'idéal* $(f_1, \ldots, f_s)$.

La théorie des bases de Gröbner permet de répondre à cette question, comme nous le verrons par la suite.

2.2. Réduction des polynômes

L'algorithmique dans une algèbre quotient s'appuie sur la réduction des polynômes nécessaire au calcul des « représentants canoniques » des éléments de celle-ci. Le but de cette section est l'étude de cette réduction.

Tout polynôme peut être vu comme une somme de composantes « ordonnées » dont la plus grande sera appelée le « terme dominant ». Ceci correspond à une décomposition de $\mathbb{K}[\mathbf{x}]$ en somme directe de sous-espaces vectoriels :

$$\mathbb{K}[\mathbf{x}] = \oplus_{\gamma \in \Gamma} \mathbb{K}[\mathbf{x}]_{[\gamma]},$$

où Γ est un ensemble ordonné et $\mathbb{K}[\mathbf{x}]_{[\gamma]}$ le sous-espace vectoriel de $\mathbb{K}[\mathbf{x}]$ engendré par les composantes d'indice γ. Donc pour tout $p \in \mathbb{K}[\mathbf{x}]$ non nul, il existe des composantes non nulles uniques $p_{[\gamma_i]} \in \mathbb{K}[\mathbf{x}]_{[\gamma_i]}, i = 1, \ldots, s$, telles que

$$p = p_{[\gamma_1]} + \cdots + p_{[\gamma_s]}.$$

Par exemple la décomposition d'un polynôme en composantes homogènes correspond à $\Gamma = \mathbb{N}$, muni de son ordre naturel, qui indexe le degré. Le polynôme $p = x_1^2 - x_2^2 + 2\,x_1 - 2\,x_2 - 1$ se décompose alors en la somme des termes

$$x_1^2 - x_2^2 \in \mathbb{K}[\mathbf{x}]_{[2]}, \quad 2\,x_1 - 2\,x_2 \in \mathbb{K}[\mathbf{x}]_{[1]}, \quad -1 \in \mathbb{K}[\mathbf{x}]_{[0]}.$$

Si $\Gamma = \mathbb{N}^2$ est ordonné suivant l'*ordre lexicographique* (i.e. l'ordre du dictionnaire) pour lequel $x_2 > x_1$. Les composantes de p, de la plus grande à la plus petite, sont

$$-x_2^2 \in \mathbb{K}[\mathbf{x}]_{[0,2]}, -2\,x_2 \in \mathbb{K}[\mathbf{x}]_{[0,1]}, x_1^2 \in \mathbb{K}[\mathbf{x}]_{[2,0]}, 2\,x_1 \in \mathbb{K}[\mathbf{x}]_{[1,0]}, -1 \in \mathbb{K}[\mathbf{x}]_{[0,0]}.$$

Nous verrons, plus loin, d'autres décompositions de $\mathbb{K}[\mathbf{x}]$.

***Définition* 2.1.** *Pour tout élément p non nul de $\mathbb{K}[\mathbf{x}]$,*
- $\mathtt{m}(p)$ *est le plus grand indice $\gamma \in \Gamma$ tel que $p_{[\gamma]} \neq 0$. Il est appelé le Γ-degré de p.*
- $\mathtt{t}(p)$ *désigne la composante de p de plus grand indice $\gamma \in \Gamma$ tel que $p_{[\gamma]} \neq 0$. Elle est appelée le terme dominant de p.*
- *Si $p \in \mathbb{K}[\mathbf{x}]_{[\gamma]}$, nous dirons que p est Γ-homogène de Γ-degré γ.*

Pour le polynôme $p = x_1^2 - x_2^2 + 2\,x_1 - 2\,x_2 - 1$,
– dans le cas $\Gamma = \mathbb{N}$ qui indexe le degré, $\mathtt{t}(p) = x_1^2 - x_2^2, \mathtt{m}(p) = 2$,
– dans le cas $\Gamma = \mathbb{N}^2$ muni de l'ordre lexicographique avec $x_2 > x_1$, $\mathtt{t}(p) = -x_2^2$ et $\mathtt{m}(p) = (0, 2)$.

***Définition* 2.2.** *Soient $a, b_1, \ldots, b_s \in \mathbb{K}[\mathbf{x}]$. Nous dirons que a se réduit par $b_1, \ldots, b_s$ s'il existe des éléments Γ-homogènes $q_1, \ldots, q_s$ de $\mathbb{K}[\mathbf{x}]$ tels que $\mathtt{t}(a) = \sum_{i=1}^s q_i\,\mathtt{t}(b_i)$. La réduction de a par $b_1, \ldots, b_s$ est alors $a - \sum_{i=1}^s q_i\,b_i$.*

Remarquons que $\mathtt{t}\big(a - \sum_{i=1}^s q_i\,b_i\big) < \mathtt{t}(a)$. Nous pouvons de nouveau réduire $a - \sum_{i=1}^s q_i\,b_i$ par $b_1, \ldots, b_s$, et ainsi de suite. Pour pouvoir réitérer la réduction un nombre fini de fois et obtenir un polynôme que l'on ne peut plus réduire par $b_1, \ldots, b_s$, et calculer facilement les q_i nous imposons les hypothèses suivantes :

***Hypothèse* 2.3.**
- Γ *est un monoïde additif muni d'un bon ordre (i.e. tout sous-ensemble de Γ admet un plus petit élément),*
- *Pour tout $(\alpha, \beta, \gamma) \in \Gamma^3, \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$,*
- *Si $f \in \mathbb{K}[\mathbf{x}]_{[\alpha]}$ et $g \in \mathbb{K}[\mathbf{x}]_{[\beta]}$, alors $f\,g \in \mathbb{K}[\mathbf{x}]_{[\alpha+\beta]}$.*
- *Pour tout $\gamma \in \Gamma$, l'espace vectoriel $\mathbb{K}[\mathbf{x}]_{[\gamma]}$ est de dimension finie.*

Nous dirons dans ce cas que Γ est une *graduation effective*.

Dans le cas de la graduation par le degré, où $\Gamma = \mathbb{N}$ est muni de son ordre naturel, ces hypothèses sont vérifiées. Les quotients q_i dans la réduction de a par $b_1, \ldots, b_s$ sont Γ-homogènes de Γ-degrés $\mathtt{m}(a) - \mathtt{m}(b_i)$.

Si $\Gamma = \mathbb{N}^n$ est muni de l'ordre lexicographique, les hypothèses 2.3 sont aussi vérifiées. Les *termes dominants* sont des termes monomiaux et tester si $\mathtt{t}(a) = \sum_{i=1}^{s} q_i\, \mathtt{t}(b_i)$ revient simplement à vérifier si $\mathtt{t}(a)$ est divisible par l'un des $\mathtt{t}(b_i)$. Si c'est le cas q_i est un monôme et $q_j = 0$ pour $j \neq i$. Une telle graduation peut être definie par un ordre monomial, permettant de choisir le plus grand monôme :

***Définition* 2.4.** *Un ordre monomial est un ordre total $>$ sur les monômes de $\mathbb{K}[x]$ tel que tout monôme non constant $m > 1$ et si m_0, m_1, m_2 sont des monômes, on a $m_0 < m_1 \Rightarrow m_0\, m_2 < m_1\, m_2$.*

Dans le cas général d'une graduation effective, si $\{m_{i,1}, \ldots, m_{i,k_i}\}$ est une base de l'espace vectoriel $\mathbb{K}[\mathbf{x}]_{[\mathtt{m}(a)-\mathtt{m}(b_i)]}$ (qui est réduit à $\{0\}$ si $\mathtt{m}(a) < \mathtt{m}(b_i)\big)$, Réduire a par $b_1, \ldots, b_s$ revient à résoudre le système linéaire

$$\mathtt{t}(a) - \sum_{i=1}^{s} \sum_{j=1}^{k_i} \lambda_{i,j}\, m_{i,j}\, \mathtt{t}(b_i) = 0$$

dans lequel les inconnues sont les scalires $\lambda_{i,j}$.

Dans le cas simple de la réduction par un polynôme, il suffit de tester la divisibilité des termes dominants : une réduction de $p = x_1^2 - x_2^2 + 2\,x_1 - 2\,x_2 - 1$ par $x_1 + x_2 - 1$, pour $\Gamma = \mathbb{N}$, donne

$$x_1^2 - x_2^2 + 2\,x_1 - 2\,x_2 - 1 - (x_1 - x_2)(x_1 + x_2 - 1) = 3\,x_1 - 3\,x_2 - 1.$$

Nous allons décrire l'algorithme de division dans $\mathbb{K}[\mathbf{x}]$ qui généralise celui d'Euclide à une seule variable. Il consiste à itérer la réduction décrite ci-dessus, jusqu'à obtenir un polynôme que l'on ne peut plus réduire.

***Définition* 2.5.** *Soient Γ une graduation effective et $r, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$. Le polynôme r est dit réduit par rapport à $\{f_1, \ldots, f_s\}$ si aucune composante Γ-homogène non nulle de r ne peut être réduite par $f_1, \ldots, f_s$.*

***Algorithme* 2.6.** DIVISION MULTIVARIABLE.

ENTRÉE : Γ une graduation effective, $f, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$.
  $r := f$; $q_i := 0$, $i = 1, \ldots, s$.
  Tant qu'une des composantes Γ-homogènes non nulles $r_{[\gamma]}$ de r se décompose en $r_{[\gamma]} = \sum_{i=1}^{s} m_i\, \mathtt{t}(f_i)$, calculer
    -- $r := r - \sum_{i=1}^{s} m_i f_i$,
    -- $q_i := q_i + m_i$, $i = 1, \ldots, s$.
SORTIE : Des éléments $q_1, \ldots, q_s, r$ de $\mathbb{K}[\mathbf{x}]$ qui vérifient
    i) $f = q_1 f_1 + \cdots + q_s f_s + r$,
    ii) r est réduit par rapport à $\{f_1, \ldots, f_s\}$.

Cet algorithme s'arrête après un nombre fini d'étapes. Sinon, il serait possible de construire une suite infinie strictement décroissante d'éléments de Γ, à partir des termes dominants des restes intermédiaires, ce qui contredirait l'hypothèse de bon ordre faite sur Γ.

Contrairement à l'algorithme d'Euclide, les quotients $q_1, \ldots, q_s$ et le reste r ne sont pas uniques. Ils le sont si un ordre de division dans la liste $\{f_1, \ldots, f_s\}$ est imposé. Dans le cas d'une seule variable, le polynôme f appartient à l'idéal $(f_1, \ldots, f_s)$ si, et seulement si, le reste r de la division de f par le pgcd de $f_1, \ldots, f_s$ est nul, ce qui n'est pas vrai pour cet algorithme multivariable comme le montre l'exemple suivant :

***Exemple* 2.7.** *Munissons $\mathbb{K}[x, y]$ de la graduation par le degré. Si $f_1 = x^3 + xy - 1$ et $f_2 = x^2 + y$, alors $1 = x\, f_2 - f_1 \in (f_1, f_2)$. Le polynôme constant 1 est réduit par rapport à $\{f_1, f_2\}$, donc l'algorithme de division de 1 par $\{f_1, f_2\}$ produit $q_1 = q_2 = 0$ et $r = 1$.*

Dans cet exemple, $\big(\mathtt{t}(f_1), \mathtt{t}(f_2)\big) = (x^2)$ est contenu strictement dans l'idéal engendré par $\{\mathtt{t}(f) : f \in (f_1, f_2)\}$ qui est égal à $\mathbb{K}[\mathbf{x}]$. Dans ce cas, on dit que f_1 et f_2 ne forment pas un « bon système de générateurs » de l'idéal (f_1, f_2) ; car en partant de $f \in (f_1, f_2)$, l'algorithme de division de f par $\{f_1, f_2\}$ s'arrête sans réduire f à 0. D'où la définition suivante :

***Définition* 2.8.** *Soient Γ une graduation effective, I un idéal de $\mathbb{K}[\mathbf{x}]$ et $\mathtt{t}(I)$ l'idéal engendré par $\{\mathtt{t}(p) : p \in I\}$. Nous dirons que $G = \{g_1, \ldots, g_t\}$ est une Γ-base de I si*

i) $g_1, \ldots, g_t \in I$,

ii) $\mathtt{t}(g_1), \ldots, \mathtt{t}(g_t)$ engendrent $\mathtt{t}(I)$.

Pour simplifier la présentation, nous considérons seulement des Γ-bases finies, bien que la définition s'étende au cas infini. L'existence d'une Γ-base finie est une conséquence du fait que $\mathbb{K}[\mathbf{x}]$ est noethérien (théorème 1.3). Une première propriété de ces Γ-bases est la suivante :

***Proposition* 2.9.** *Tout polynôme p de I se réduit à 0 par une Γ-base de I.*

Démonstration. Si $p \in I \setminus \{0\}$ et $G = \{g_1, \ldots, g_t\}$ est une Γ-base de I, $\mathtt{t}(p) \in \big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_t)\big)$. Il existe alors des éléments Γ-homogènes $h_1, \ldots, h_t$ de $\mathbb{K}[\mathbf{x}]$ tels que $\mathtt{t}(p) = \sum_{i=1}^{t} h_i \mathtt{t}(g_i)$. Le polynôme p se réduit par G en $q = p - \sum_{i=1}^{s} h_i g_i \in I$, avec $\mathtt{m}(q) < \mathtt{m}(p)$. Comme Γ est muni d'un bon ordre, en itérant la réduction par G nous obtenons 0 comme reste. Sinon, la partie des termes dominants des restes successifs n'aurait pas de plus petit élément. Ainsi, tout polynôme de I se réduit à 0 par une Γ-base. □

Nous déduisons le corollaire suivant :

***Corollaire* 2.10.** *Une* Γ*-base de l'idéal* I *est un système de générateurs de* I*.*

Démonstration. La réduction à 0 de tout élément $p \in I$ par une Γ-base $G = \{g_1, \ldots, g_t\}$ implique une décomposition de la forme $p = \sum_{i=1}^{t} h_i\, g_i$, avec $h_i \in \mathbb{K}[\mathbf{x}]$. Le système G engendre bien l'idéal I. □

Ceci permet de définir la notion de forme normale :

***Proposition* 2.11.** *Le reste* r *de la division de* $f \in \mathbb{K}[\mathbf{x}]$ *par une* Γ*-base* G *de* I *est unique. Il est appelé la forme normale de* f *par rapport à* G*, et noté* $\mathtt{N}_G(f)$*.*

Démonstration. Soient r_1 et r_2 deux restes de la division de f par G. Comme $r_1 - r_2$ est réduit par rapport à G et $r_1 - r_2 \in I$, $r_1 - r_2 = 0$. □

Une Γ-base permet de travailler effectivement dans une algèbre quotient :

***Proposition* 2.12.** *Soit* G *une* Γ*-base de* I*. L'espace vectoriel* $\mathbb{K}[\mathbf{x}]/I$ *est isomorphe à l'espace vectoriel des polynômes réduits par rapport à* G*.*

Démonstration. Soit E l'espace vectoriel des polynômes réduits par rapport à $G = \{g_1, \ldots, g_t\}$. En appliquant l'algorithme 2.6, tout $f \in \mathbb{K}[\mathbf{x}]$ se réduit par G en un élément de E. Il existe alors des polynômes $q_i \in \mathbb{K}[\mathbf{x}]$, et $r \in E$ tels que $f = \sum_{i=1}^{t} q_i\, g_i + r$. Par conséquent, $f \equiv r$ dans $\mathbb{K}[\mathbf{x}]/I$ et $\{\overline{a} : a \in E\}$ engendre bien $\mathbb{K}[\mathbf{x}]/I$.

D'après la proposition 2.9, $I \cap E = \{0\}$, donc $\mathbb{K}[\mathbf{x}]/I$ est isomorphe à E. □

Nous allons décrire un critère effectif pour tester si un ensemble est une Γ-base d'un idéal I qui est la clé de voûte de l'algorithmique dans $\mathbb{K}[\mathbf{x}]/I$. La définition qui suit est nécessaire à la description de ce critère.

***Définition* 2.13.** *Soient* $g_1, \ldots, g_s \in \mathbb{K}[\mathbf{x}]$*. Le* premier module des syzygies (ou des relations) *de* $g_1, \ldots, g_s$ *est l'ensemble*

$$\mathrm{Syz}(g_1, \ldots, g_s) = \{(h_1, \ldots, h_s) \in \mathbb{K}[\mathbf{x}]^s : \sum_{i=1}^{s} h_i\, g_i = 0\}.$$

Cet ensemble est un $\mathbb{K}[\mathbf{x}]$-module engendré par un nombre fini d'éléments (voir exercice 2.19).

Si $g_i \in \mathbb{K}[\mathbf{x}]_{[\gamma_i]}, i = 1, \ldots, s$, alors $\mathrm{Syz}(g_1, \ldots, g_s)$ est engendré par des éléments de la forme $(h_1, \ldots, h_s)$, où h_i est Γ-homogène et il existe $\gamma \in \Gamma$, tel que pour tout i, $h_i g_i \in \mathbb{K}[\mathbf{x}]_\gamma$. Nous dirons dans ce cas que $(h_1, \ldots, h_s)$ est Γ-homogène.

***Théorème* 2.14.** *Soit $G = \{g_1, \ldots, g_s\}$ un ensemble de générateurs de l'idéal I. Alors G est une Γ-base de I si, et seulement si, pour tout $(h_1, \ldots, h_s)$ Γ-homogène de $\mathrm{Syz}\big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$, le polynôme $h_1 g_1 + \cdots + h_s g_s$ se réduit à 0 par $g_1, \ldots, g_s$.*

Démonstration. Si G est une Γ-base de I, d'après la proposition 2.9, tout polynôme de I se réduit à 0 par G. En particulier, tout élément de la forme $h_1 g_1 + \cdots + h_s g_s$, avec $(h_1, \ldots, h_s) \in \mathrm{Syz}\big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$. Réciproquement, si $\{\mathbf{h}_u = (\mathbf{h}_{u,1}, \ldots, \mathbf{h}_{u,n})\}_{u \in U}$ est un système de générateurs Γ-homogènes de $\mathrm{Syz}\big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$ tel que pour tout $u \in U$, l'élément $\mathbf{h}_{u,1}\, g_1 + \cdots + \mathbf{h}_{u,s}\, g_s$ se réduit à 0 par G, montrons que G est une Γ-base de I.

Soit $p \in I$. L'élément p se décompose sous la forme

$$p = \sum_{i=1}^{s} q_i g_i \quad , \quad q_i \in \mathbb{K}[\mathbf{x}]. \tag{2.1}$$

Il faut prouver que $\mathtt{t}(p) \in \big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$. Notons

$$\gamma = \max\{\mathtt{m}(q_i g_i) : q_i \neq 0\} = \max\{\mathtt{m}(q_i) + \mathtt{m}(g_i) : q_i \neq 0\} \in \Gamma$$

et S_γ l'ensemble des indices $i \in \{1, \ldots, s\}$ tel que $\mathtt{m}(q_i\, g_i) = \gamma$. Comme Γ est muni d'un bon ordre, supposons que pour la décomposition (2.1) de p, γ soit le plus petit possible.

Par construction, nous avons $\mathtt{m}(p) \leq \gamma$. Nous allons montrer que $\mathtt{m}(p) = \gamma$, par suite $\mathtt{t}(p) = \sum_{i \in S_\gamma} \mathtt{t}(q_i)\mathtt{t}(g_i)$, et donc $\mathtt{t}(p) \in \big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$.

Sinon, $\mathtt{m}(p) < \gamma$, c'est-à-dire

$$\sum_{i \in S_\gamma} \mathtt{t}(q_i)\, \mathtt{t}(g_i) = 0,$$

ou encore $\sum_{i=1}^{s} h_i\, \mathtt{t}(g_i) = 0$, avec $h_i = \mathtt{t}(q_i)$ si $i \in S_\gamma$ et $h_i = 0$ si $i \notin S_\gamma$.

Le vecteur $\mathbf{h} = (h_1, \ldots, h_s)$ est un élément de $\mathrm{Syz}\big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$ pour lequel $\mathtt{m}(h_i g_i) = \gamma$ pour $i \in S_\gamma$. Comme $\{\mathbf{h}_u\}_{u \in U}$ engendre $\mathrm{Syz}\big(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s)\big)$, il existe des polynômes $m_u \in \mathbb{K}[\mathbf{x}]$ qui vérifient $\mathbf{h} = \sum_{u \in U} m_u\, \mathbf{h}_u$. Nous avons

$$\sum_{i=1}^{s} h_i\, g_i = \sum_{i=1}^{s} \sum_{u \in U} m_u\, \mathbf{h}_{u,i}\, g_i.$$

D'après l'hypothèse, pour tout $u \in U$, $\mathbf{h}_{u,1}\, g_1 + \cdots + \mathbf{h}_{u,s}\, g_s$ se réduit à 0 par G, donc nous pouvons aussi réduire $m_u(\mathbf{h}_{u,1}\, g_1 + \cdots + \mathbf{h}_{u,s}\, g_s)$ à 0. Ainsi,

$$m_u \sum_{i=1}^{s} \mathbf{h}_{u,i}\, g_i = \sum_{i=1}^{s} q_{i,u}\, g_i \ ,$$

avec $q_{i,u} = m_u \mathbf{h}_{u,i}$ et $\mathtt{m}(q_{i,u}\, g_i) \leq \mathtt{m}(m_u(\mathbf{h}_{u,1}\, g_1 + \cdots + \mathbf{h}_{u,s}\, g_s)\big) < \gamma$. Par conséquent,

$$\sum_{i=1}^{s} h_i\, g_i = \sum_{i=1}^{s}\sum_{u\in U} m_u\, \mathbf{h}_{u,i}\, g_i = \sum_{i=1}^{s}\big(\sum_{u\in U} q_{i,u}\big)\, g_i = \sum_{i=1}^{s} \tilde{h_i}\, g_i\ , \tag{2.2}$$

où $\tilde{h_i} = \sum_{u\in U} q_{i,u}$ et $\mathtt{m}(\tilde{h_i} g_i) \leq \max_u \mathtt{m}(q_{i,u}\, g_i) < \gamma$. En utilisant (2.2), p se réécrit sous la forme

$$p = \sum_{i=1}^{s} q_i\, g_i = \sum_{i=1}^{s} h_i\, g_i + \sum_{i=1}^{s}(q_i - h_i)\, g_i = \sum_{i=1}^{s}(\tilde{h_i} + q_i - h_i)\, g_i.$$

Dans cette nouvelle décomposition de p, nous avons

$$\mathtt{m}\big((\tilde{h_i} + q_i - h_i)\, g_i\big) \leq \max\big(\mathtt{m}(\tilde{h_i}\, g_i), \mathtt{m}((q_i - h_i)\, g_i)\big) < \gamma.$$

Ceci contredit l'hypothèse faite sur la décomposition (2.1) de p pour laquelle γ est le plus petit possible. □

2.3. Ordres monomiaux

Nous allons considérer dans cette section la réduction par une Γ-base dans le cas où $\Gamma = \mathbb{N}^n$. Les hypothèses 2.3 faites sur Γ donnent la notion d'ordre monomial que nous allons rappeler.

***Définition* 2.15.** *Un ordre monomial est un ordre total $<$ sur l'ensemble des monômes de $\mathbb{K}[\mathbf{x}]$ (ou de façon équivalente sur $\mathbb{N}^n$) qui satisfait*

i) $\forall \alpha \neq 0,\ 1 < \mathbf{x}^\alpha$,

ii) $\forall (\alpha, \beta, \gamma) \in (\mathbb{N}^n)^3,\ \mathbf{x}^\alpha < \mathbf{x}^\beta \Longrightarrow \mathbf{x}^{\alpha+\gamma} < \mathbf{x}^{\beta+\gamma}$.

Le point *i)* de cette définition implique que l'ordre monomial est un bon ordre (voir proposition 2.21).

***Exemple* 2.16.** *Voici quelques ordres totaux sur l'ensemble des monômes de $\mathbb{K}[\mathbf{x}]$. Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n)$ des éléments de $\mathbb{N}^n$.*

i) Ordre lexicographique $<_l$ avec $x_n <_l \cdots <_l x_1$:

$$\mathbf{x}^\alpha <_l \mathbf{x}^\beta \iff \exists\ k \in \{1, \ldots, n\}\ :\ \forall\ j < k\ ,\ \alpha_j = \beta_j \ \text{ et } \ \alpha_k < \beta_k.$$

ii) Ordre gradué lexicographique $<_{gl}$ avec $x_n <_{gl} \cdots <_{gl} x_1$:

$$\mathbf{x}^\alpha <_{gl} \mathbf{x}^\beta \iff |\alpha| < |\beta| \ \text{ ou } \ (|\alpha| = |\beta| \text{ et } \mathbf{x}^\alpha <_l \mathbf{x}^\beta).$$

iii) Ordre lexicographique inverse $<_{li}$ avec $x_n <_{li} \cdots <_{li} x_1$:

$$\mathbf{x}^\alpha <_{li} \mathbf{x}^\beta \iff \exists\ k \in \{1, \ldots, n\} :\ \forall j > k\ ,\ \alpha_j = \beta_j \ \text{ et } \ \alpha_k > \beta_k.$$

iv) Ordre gradué lexicographique inverse $<_{gli}$ avec $x_n <_{gli} \cdots <_{gli} x_1$,

$$\mathbf{x}^\alpha <_{gli} \mathbf{x}^\beta \iff |\alpha| < |\beta| \text{ ou } (|\alpha| = |\beta| \text{ et } \mathbf{x}^\alpha <_{li} \mathbf{x}^\beta).$$

Les ordres $<_l, <_{gl}, <_{gli}$ sont monomiaux, tandis que $<_{li}$ ne l'est pas, car pour tout $\alpha \neq 0$, $\mathbf{x}^\alpha <_{li} 1$.

Les monômes de degré au plus 2 sont rangés comme suit :
Pour l'ordre lexicographique $x > y > z$,

$$x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1.$$

Pour l'ordre gradué lexicographique $x > y > z$,

$$x^2 > xy > xz > y^2 > yz > z^2 > x > y > z > 1.$$

Pour l'ordre gradué lexicographique inverse $x > y > z$,

$$x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1.$$

***Définition* 2.17.** *Soit $<$ un ordre monomial. Alors tout polynôme f non nul s'écrit de manière unique sous la forme $f = a_0\mathbf{x}^{\alpha_0} + \cdots + a_d\mathbf{x}^{\alpha_d}$, où $a_0, \ldots, a_d$ sont des coefficients non nuls et $\alpha_0 > \cdots > \alpha_d$. Dans ce cas, a_0 est appelé le* coefficient dominant de f, $\mathbf{x}^{\alpha_0}$ le *monôme dominant de f*, $a_0\mathbf{x}^{\alpha_0}$ *le* terme dominant de f. Ils sont notés respectivement $\mathtt{c}_<(f)$, $\mathtt{m}_<(f)$, $\mathtt{t}_<(f)$ ou simplement $\mathtt{c}(f)$, $\mathtt{m}(f)$, $\mathtt{t}(f)$ s'il n'y a pas de confusion. Si $f = 0$, on définit $\mathtt{c}(0) = \mathtt{m}(0) = \mathtt{t}(0) = 0$.

Dans la section 2.2, $\mathtt{m}(f)$ désignait l'exposant de $\mathtt{m}_<(f)$. Comme l'ensemble des monômes de $\mathbb{K}[\mathbf{x}]$ est en bijection avec les multi-indices de $\mathbb{N}^n$, il n'y a pas d'ambiguïté dans ces deux notations.

Pour l'ordre lexicographique $x > y$, $\mathtt{m}(x^2 - x\,y^2 + x) = x^2$, et pour l'ordre gradué lexicographique $x > y$, $\mathtt{m}(x^2 - x\,y^2 + x) = x\,y^2$. Donc $\mathtt{c}(f)$, $\mathtt{m}(f)$ et $\mathtt{t}(f)$ dépendent de l'ordre monomial choisi.

***Définition* 2.18.** *Soit $w = (w_1, \ldots, w_n) \in \mathbb{Z}^n$. Si $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, on appelle w-degré de α, l'entier $w(\alpha) = w_1\alpha_1 + \cdots + w_n\alpha_n$.*

***Remarque* 2.19.** Considérons des n-uplets d'entiers $\mathbf{w} = (w_1, \ldots, w_s) \in (\mathbb{Z}^n)^s$ et définissons l'ordre $<_{\mathbf{w}}$,

$$\mathbf{x}^\alpha <_{\mathbf{w}} \mathbf{x}^\beta \iff \big(w_1(\alpha), \ldots, w_s(\alpha)\big) <_l \big(w_1(\beta), \ldots, w_s(\beta)\big),$$

où $<_l$ est l'ordre lexicographique sur $\mathbb{Z}^s$ (défini de la même façon que sur $\mathbb{N}^s$). On peut montrer que tous les ordres monomiaux sont de la forme $<_{\mathbf{w}}$, pour un certain $\mathbf{w} = (w_1, \ldots, w_s) \in (\mathbb{Z}^n)^s$ (voir [**Rob86**]). Ainsi, on peut définir

i) $<_l$ par $\mathbf{w} = \big((1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\big) \in (\mathbb{N}^n)^n$,

ii) $<_{gl}$ par $\mathbf{w} = \big((1, \ldots, 1), (1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1, 0)\big) \in (\mathbb{N}^n)^n$,

iii) $<_{gli}$ par $\mathbf{w} = \big((1, \ldots, 1), (0, \ldots, 0, -1), \ldots, (0, -1, 0, \ldots, 0)\big) \in (\mathbb{Z}^n)^n$.

Cette représentation est utilisée dans les logiciels de calcul des bases de Gröbner pour paramétrer les ordres monomiaux.

2.4. Idéaux monomiaux

Dans un premier temps, nous allons nous intéresser aux *idéaux monomiaux* (i.e. engendrés par des monômes), dont la manipulation est très simple (voir exercices 2.6, 2.7, 2.8, 2.20). Et nous verrons comment ils interviennent dans l'étude des idéaux quelconques de $\mathbb{K}[\mathbf{x}]$.

Si A est une partie (éventuellement infinie) de $\mathbb{N}^n$, $\mathbf{x}^A$ désigne l'ensemble $\{\mathbf{x}^\alpha : \alpha \in A\}$ et $(\mathbf{x}^A)$ l'idéal qu'il engendre. Il est facile de vérifier :

i) Un monôme $\mathbf{x}^\beta \in (\mathbf{x}^A)$ si, et seulement si, $\mathbf{x}^\beta$ est divisible par un $\mathbf{x}^\alpha$, avec $\alpha \in A$ (i.e. il existe $\gamma \in \mathbb{N}^n$ tel que $\beta = \alpha + \gamma$).

ii) Un polynôme $f \in (\mathbf{x}^A)$ si, et seulement si, chaque monôme de f est divisible par un $\mathbf{x}^\alpha$, avec $\alpha \in A$.

Notons que l'idéal engendré par tous les monômes situés dans la partie sombre ci-dessous est l'idéal monomial (xy^3, x^4y^2, x^7) de $\mathbb{K}[x, y]$.
Plus généralement, nous avons le lemme suivant :

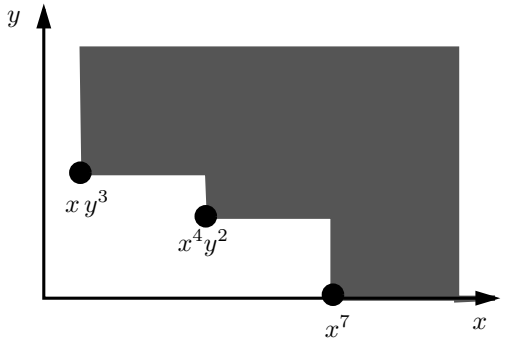

FIGURE 2.1. Un idéal monomial.

***Lemme* 2.20.** *(lemme de Dickson) Tout idéal monomial $I = (\mathbf{x}^A)$ est engendré par un nombre fini d'éléments $\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s}$ de $\mathbf{x}^A$.*

Démonstration. Ce lemme découle du fait que l'anneau $\mathbb{K}[\mathbf{x}]$ est noethérien (théorème 1.3). Mais nous allons donner ici une autre preuve de ce résultat. Nous procédons par récurrence sur le nombre de variables n. Si $n = 1$, $I = (x^\alpha)$, où α est le plus petit élément de A.

Supposons le lemme vrai pour les idéaux de $\mathbb{K}[x_1, \ldots, x_{n-1}]$ et soit $I = (\mathbf{x}^A)$ un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. Notons $\tilde{\mathbf{x}}$ les $n-1$ premières variables $x_1, \ldots, x_{n-1}$ et B la projection de A sur les $n-1$ premières coordonnées de $\mathbb{N}^n$. Par l'hypothèse de récurrence, l'idéal $\tilde{I} = (\tilde{\mathbf{x}}^B)$ est engendré par un nombre fini de monômes : $I = (\tilde{\mathbf{x}}^{\beta_1}, \ldots, \tilde{\mathbf{x}}^{\beta_t})$, avec $\beta_i \in B$.

Fixons $i \in \{1, \ldots, t\}$ et notons I_i l'idéal de $\mathbb{K}[x_n]$ engendré par l'ensemble

$$\{x_n^a : \tilde{\mathbf{x}}^{\beta_i} x_n^a \in I\}.$$

D'après le premier pas de récurrence, $I_i = (x_n^{d_i})$, avec $d_i \in \mathbb{N}$.

Posons $d = \max(d_1, \ldots, d_t)$. Pour tout $k \in \{0, \ldots, d\}$, soit J_k l'idéal de $\mathbb{K}[x_1, \ldots, x_{n-1}]$ engendré par $\{\tilde{\mathbf{x}}^\beta : \tilde{\mathbf{x}}^\beta x_n^k \in I\}$. Cet idéal est engendré par un nombre fini d'éléments $\tilde{\mathbf{x}}^{\beta_{k,1}}, \ldots, \tilde{\mathbf{x}}^{\beta_{k,s_k}}$. Les monômes

$$\tilde{\mathbf{x}}^{\beta_i} x_n^{d_i} \ , \ i = 1, \ldots, t \ \text{ et } \ \tilde{\mathbf{x}}^{\beta_{k,j}} x_n^k \ , \ \ k = 0, \ldots, d \ \ , \ \ j = 1, \ldots, s_k \ ,$$

engendrent I. En effet, tout monôme $\mathbf{x}^\alpha = \tilde{\mathbf{x}}^\beta x_n^e \in I$ est divisible par un $\tilde{\mathbf{x}}^{\beta_i} x_n^e, i = 1, \ldots, t$.

Si $e \geq d$, $\mathbf{x}^\alpha$ est divisible par $\tilde{\mathbf{x}}^{\beta_i} x_n^{d_i}$.

Si $e < d$, $\mathbf{x}^\alpha$ est divisible par un $\tilde{\mathbf{x}}^{\beta_{e,j}} x_n^e, j = 1, \ldots, s_e$. □

Une conséquence importante du lemme de Dickson est le résultat suivant :

***Proposition* 2.21.** *Un ordre monomial est un bon ordre (i.e. tout ensemble de monômes de* $\mathbb{K}[\mathbf{x}]$ *admet un plus petit élément).*

Démonstration. Soit $\mathbf{x}^A$ un ensemble de monômes. D'après le lemme 2.20, l'idéal $(\mathbf{x}^A) = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s})$, où $\alpha_1, \ldots, \alpha_s \in A$. Si $\alpha \in A$, il existe i tel que $\mathbf{x}^\alpha \geq \mathbf{x}^{\alpha_i}$. Par conséquent, le plus petit élément de $\{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s}\}$ est aussi celui de $\mathbf{x}^A$. □

La réciproque de la proposition 2.21 est aussi vraie (voir exercice 2.3). La notion de Γ-base dans le contexte d'un ordre monomial conduit à la notion de base de Gröbner :

***Définition* 2.22.** *Une partie* $\{g_1, \ldots, g_t\}$ *de l'idéal* I *est une* base de Gröbner *si* $\mathtt{m}(I) = \big(\mathtt{m}(g_1), \ldots, \mathtt{m}(g_t)\big)$, *où* $\mathtt{m}(I)$ *désigne l'idéal monomial engendré par* $\{\mathtt{m}(p) : p \in I\}$.

L'existence d'une base de Gröbner de I est assurée par le lemme de Dickon : l'idéal $\mathtt{m}(I)$ est engendré par un nombre fini de monômes $\mathtt{m}(g_1), \ldots, \mathtt{m}(g_t)$, et les éléments $g_1, \ldots, g_t$ de I forment bien une base de Gröbner.

***Remarque* 2.23.** Nous allons donner une autre preuve du théorème 1.3 : l'anneau $\mathbb{K}[\mathbf{x}]$ est noethérien. En effet, si I est un idéal de $\mathbb{K}[\mathbf{x}]$, d'après le lemme de Dickson, il existe $g_1, \ldots, g_t \in I$ tels que $\mathtt{m}(I) = \big(\mathtt{m}(g_1), \ldots, \mathtt{m}(g_t)\big)$. D'après le corollaire 2.10, la base de Gröbner $\{g_1, \ldots, g_t\}$ de I est, en particulier, un système de générateurs de I.

La proposition 2.12 se traduit dans le cas d'un ordre monomial de la façon suivante :

***Proposition* 2.24.** *Soit* G *une base de Gröbner pour un ordre monomial* $<$. *Une base de l'espace vectoriel quotient* $\mathbb{K}[\mathbf{x}]/I$ *est donnée par les monômes qui n'appartiennent pas à l'idéal monomial* $\mathtt{m}(G)$ *engendré par* $\{\mathtt{m}(g) : g \in G\}$.

2.5. Algorithme de construction d'une base de Gröbner

Nous allons maintenant voir comment construire une base de Gröbner de $I = (f_1, \ldots, f_s)$. Pour cela nous introduisons la définition suivante :

***Définition* 2.25.** *Soit* $(f, g) \in (\mathbb{K}[\mathbf{x}] \setminus \{0\})^2$. *Le* S-polynôme de f et g est

$$S(f,g) = \mathrm{ppcm}\big(\mathtt{m}(f), \mathtt{m}(g)\big)\left(\frac{f}{\mathtt{t}(f)} - \frac{g}{\mathtt{t}(g)}\right) \in \mathbb{K}[\mathbf{x}].$$

Notons que le polynôme $S(f, g)$ appartient à l'idéal engendré par f et g, et que $\mathtt{m}\big(S(f,\, g)\big) < \mathrm{ppcm}\big(\mathtt{m}(f), \mathtt{m}(g)\big)$.

***Théorème* 2.26.** *(théorème de Buchberger) Le système de générateurs* $G = \{g_1, \ldots, g_s\}$ *de l'idéal* I *est une base de Gröbner si, et seulement si, pour tout* $(i, j) \in \{1, \ldots, s\}^2$, *le reste de la division de* $S(g_i, g_j)$ *par* G *est nul.*

Démonstration. Un système de générateurs de $\mathrm{Syz}(\mathtt{t}(g_1), \ldots, \mathtt{t}(g_s))$ est formé des vecteurs de polynômes

$$\mathbf{h}_{i,j} = \left(0, \ldots, 0, \frac{\mathrm{ppcm}\big(\mathtt{m}(g_i), \mathtt{m}(g_j)\big)}{\mathtt{t}(g_i)}, 0, \ldots, 0, -\frac{\mathrm{ppcm}\big(\mathtt{m}(g_i), \mathtt{m}(g_j)\big)}{\mathtt{t}(g_j)}, 0, \ldots, 0\right)$$

pour $i < j$ (voir exercice 2.20). D'après le théorème 2.14, G est une base de Gröbner de I si, et seulement si, $S(g_i, g_j)$ se réduit à 0 par G. □

Une conséquence importante du théorème 2.26 est *l'algorithme de Buchberger* qui permet de construire une base de Gröbner d'un idéal I.

***Algorithme* 2.27.** Algorithme de Buchberger.

Entrée : Un ordre monomial $<$ et des polynômes $f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$.
$G := \{f_1, \ldots, f_s\}$,
$S := \{r_{ij} =$ reste de la division de $S(f_i, f_j)$ par G, pour $i, j = 1, \ldots, s\}$.
Tant que $S \neq \{0\}$, pour tout $r \neq 0$ dans S,
-- $S := S \cup \{$ reste la division de $S(r, g)$, pour $g \in G$ $\}$,
-- $G := G \cup \{r\}$,
Sortie : Un base de Gröbner de $I = (f_1, \ldots, f_s)$ pour l'ordre monomial $<$.

Cet algorithme s'arrête après un nombre fini d'étapes, car d'après le lemme de Dickson, la suite croissante d'idéaux monomiaux $\mathtt{m}(G)$ qui interviennent dans cette construction est stationnaire.

L'algorithme de Buchberger produit beaucoup d'éléments inutiles de G. C'est pour cela que l'on introduit la définition suivante :

***Définition* 2.28.** *Une base de Gröbner G est dite réduite si*
i) $\forall g \in G$, $\mathtt{c}(g) = 1$,
ii) $\forall g \in G$, *g est réduit par rapport à* $G \setminus \{g\}$.

***Théorème* 2.29.** *Tout idéal admet une unique base de Gröbner réduite.*

Pour la preuve de ce résultat, voir l'exercice 2.11. C'est cette base de Gröbner réduite qui est calculée par les systèmes de calcul formel (Maple, Macaulay, Mathematica, Gb, CoCoA, Singular, ...). L'algorithme 2.27 n'y est pas implémenter tel que nous l'avons décrit. Des optimisations importantes sur la construction des ensembles S, le choix des éléments dans ces ensembles, ... y ont été apportées [**Fau99, Fau02**], ou pour des calculs de formes normales plus générales [**Tré02**].

2.6. Quelques applications des bases de Gröbner

Dans cette section, nous donnons quelques exemples de questions que l'on peut résoudre par des techniques de bases de Gröbner. D'autres applications sont données en exercices et dans les chapitres suivants.

Soit G une base de Gröbner de l'idéal $I = (f_1, \ldots, f_s)$ de $\mathbb{K}[\mathbf{x}]$.

2.6.1. Appartenance d'un polynôme à un idéal. — Comment peut-on tester l'appartenance d'un polynôme f à I ?

D'après la proposition 2.9, $f \in I$ si, et seulement si, $\mathtt{N}_G(f) = 0$. Donc

$$f \in I \Longleftrightarrow f \text{ se réduit à zéro par } G.$$

***Remarque* 2.30.** Une question intéressante, sous-jacente au problème de l'appartenance d'un polynôme f à l'idéal I, est celle de la représentation : si $f \in I$, déterminer des polynômes $q_1, \ldots, q_s$ tels que

$$f = q_1 f_1 + \cdots + q_s f_s.$$

Pour cela, on peut diviser f par $G = \{g_1, \ldots, g_t\}$, puis exprimer chaque g_i en fonction de $f_1, \ldots, f_s$, en utilisant les calculs effectués lors de la construction de G par l'algorithme de Buchberger. En fait, dans ce problème, on cherche des q_i ayant les plus petits degrés possibles. En général, une borne doublement exponentielle en le nombre de variables n (i.e. de la forme d^{2^n}, où $d = \max(\deg f, \deg f_1, \ldots, \deg f_s)$) est inévitable pour les degrés des q_i (voir [**MM82**], [**Dem87**]). Par conséquent, les éléments de G peuvent avoir de très grands degrés. En effet, une base de Gröbner réduite d'un idéal engendré par peu de polynômes ayant des petits degrés et coefficients peut contenir beaucoup d'éléments de degrés et coefficients très grands.

On utilise néanmoins ces techniques de bases de Gröbner car les problèmes pratiques ont souvent des propriétés particulières qui rendent les calculs beaucoup plus raisonnables ([**Mou96**], [**Mou93**], [**Rou95**], [**FMR98**], [**FJ03**],

[**FK99**], [**KL99**]). De même lorsque les données vérifient des hypothèses géométriques : par exemple, le problème de la représentation polynomiale, lorsque la variété algébrique définie par $f_1, \ldots, f_s$ est vide ou une intersection complète se résout avec des bornes simplement exponentielles en n (i.e. de la forme d^n) pour les degrés et aussi pour les coefficients de $q_1, \ldots, q_s$ (voir [**Bro87**], [**CGH88**], [**Kol88**], [**BY90**], [**BY91**], [**Phi91**], [**Amo90**], [**Elk93**], [**Elk94**], [**KP96**], [**KPS01**]).

2.6.2. Appartenance d'un polynôme au radical d'un idéal. — Comment peut-on tester l'appartenance d'un polynôme f à $\sqrt{I}$?

Si u est une nouvelle variable, le polynôme $f \in \sqrt{I}$ si, et seulement si, 1 appartient à l'idéal $I + (1 - u\,f)$ de $\mathbb{K}[\mathbf{x}, u]$ (l'anneau des polynômes en $x_1, \ldots, x_n, u$ à coefficients dans $\mathbb{K}$). Donc, si $\tilde{G}$ est une base de Gröbner de $I + (1 - u\,f)$, alors

$$f \in \sqrt{I} \Longleftrightarrow \tilde{G} \text{ contient une constante non nulle.}$$

2.6.3. Système polynomial sans solution. — Comment peut-on savoir si la variété algébrique $\mathcal{Z}(I) = \{a \in \overline{\mathbb{K}}^n : f(a) = 0, \forall f \in I\}$ est vide ?

D'après le théorème 1.17, $\mathcal{Z}(I)$ est vide si, et seulement si, $1 \in I$. Alors

$$\mathcal{Z}(I) = \emptyset \Longleftrightarrow G \text{ contient une constante non nulle.}$$

2.6.4. Idéaux d'élimination et résolution polynomiale. — Soit r un entier de $\{1, \ldots, n-1\}$. L'idéal $I_r = I \cap \mathbb{K}[x_1, \ldots, x_r]$ formé des éléments de I qui ne dépendent pas des variables $x_{r+1}, \ldots, x_n$, est appelé *idéal d'élimination* d'indice r. Ces idéaux jouent un rôle important dans la résolution des systèmes polynomiaux.

Étant donné un ordre monomial sur $\mathbb{K}[\mathbf{x}]$ pour lequel les monômes en les variables $x_{r+1}, \ldots, x_n$ sont plus grands que ceux en $x_1, \ldots, x_r$ (par exemple l'ordre lexicographique avec $x_1 < \cdots < x_n$). Un tel ordre est appelé un *ordre d'élimination* avec $(x_{r+1}, \ldots, x_n)$ plus grand que $(x_1, \ldots, x_r)$. Si G est une base de Gröbner de I pour cet ordre, alors $G \cap \mathbb{K}[x_1, \ldots, x_r]$ est une base de Gröbner de I_r (voir exercice 2.13). En particulier, d'après la proposition 2.10, $G \cap \mathbb{K}[x_1, \ldots, x_r]$ est un système de générateurs de I_r. Ceci fournit un procédé de résolution polynomiale par induction.

D'autres exemples d'applications des idéaux d'élimination sont donnés en exercices (2.15, 2.16, 2.17).

2.7. Bases de Gröbner des sous-modules de $\mathbb{K}[\mathbf{x}]^m$

Dans cette section, nous introduisons brièvement la théorie des bases de Gröbner des sous-modules de $\mathbb{K}[\mathbf{x}]^m$, qui généralise celle des idéaux de $\mathbb{K}[\mathbf{x}]$.

Notons $\{e_1, \ldots, e_m\}$ la base canonique du $\mathbb{K}[\mathbf{x}]$-module $\mathbb{K}[\mathbf{x}]^m$.

***Définition* 2.31.**
i) Un monôme *de $\mathbb{K}[\mathbf{x}]^m$ est un élément de la forme $\mathbf{x}^\alpha e_i$.*
ii) Un monôme $\mathbf{x}^\alpha e_i$ divise un autre monôme $\mathbf{x}^\beta e_j$ si $i = j$ et $\mathbf{x}^\alpha$ divise $\mathbf{x}^\beta$ dans $\mathbb{K}[\mathbf{x}]$.
iii) Un polynôme de $\mathbb{K}[\mathbf{x}]^m$ est une combinaison linéaire, à coefficients dans $\mathbb{K}$, de monômes de $\mathbb{K}[\mathbf{x}]^m$.

***Définition* 2.32.** *Un* ordre monomial *sur $\mathbb{K}[\mathbf{x}]^m$ est un ordre total $<$ sur l'ensemble des monômes de $\mathbb{K}[\mathbf{x}]^m$ qui satisfait*
i) Si X est un monôme de $\mathbb{K}[\mathbf{x}]^m$ et $\alpha \neq 0$, alors $X < \mathbf{x}^\alpha X$.
ii) Si X et Y sont deux monômes de $\mathbb{K}[\mathbf{x}]^m$ tels que $X < Y$, alors $\mathbf{x}^\alpha X < \mathbf{x}^\alpha Y$ pour tout $\alpha \in \mathbb{N}^n$.

Si $m = 1$, la définition 2.32 coïncide avec la définition 2.15.

***Exemple* 2.33.** *Ordres monomiaux sur $\mathbb{K}[\mathbf{x}]^m$: soit $<$ un ordre monomial sur $\mathbb{K}[\mathbf{x}]$.*
i) $\mathbf{x}^\alpha e_i < \mathbf{x}^\beta e_j \iff \mathbf{x}^\alpha < \mathbf{x}^\beta$ ou ($\mathbf{x}^\alpha = \mathbf{x}^\beta$ et $i < j$).
ii) $\mathbf{x}^\alpha e_i < \mathbf{x}^\beta e_j \iff i < j$ ou ($i = j$ et $\mathbf{x}^\alpha < \mathbf{x}^\beta$).

De la même façon que dans le cas $m = 1$, nous pouvons ordonner les termes d'un polynôme de $\mathbb{K}[\mathbf{x}]^m$, décrire l'algorithme de division dans $\mathbb{K}[\mathbf{x}]^m$, définir les bases de Gröbner pour les sous-modules de $\mathbb{K}[\mathbf{x}]^m$, généraliser l'algorithme de Buchberger pour la construction de ces bases de Gröbner, ... (voir exercice 2.19).

2.7.1. Relations entre polynômes. — Étant donnés $f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]$. Comment peut-on trouver un ensemble de générateurs du $\mathbb{K}[\mathbf{x}]$-module

$$\mathrm{Syz}(f_1, \ldots, f_s) = \{(h_1, \ldots, h_s) \in \mathbb{K}[\mathbf{x}]^s : h_1 f_1 + \cdots + h_s f_s = 0\} \ ?$$

Soient $z, e_1, \ldots, e_s$ des nouvelles variables (ici les vecteurs $e_1, \ldots, e_s$ de la base canonique du $\mathbb{K}[\mathbf{x}]$-module $\mathbb{K}[\mathbf{x}]^s$ sont considérés comme des variables). Si $(h_1, \ldots, h_s) \in \mathrm{Syz}(f_1, \ldots, f_s)$, alors

$$\sum_{i=1}^{s} h_i e_i = \sum_{i=1}^{s} h_i (e_i - z\, f_i) + z \sum_{i=1}^{s} h_i f_i = \sum_{i=1}^{s} h_i (e_i - z\, f_i). \tag{2.3}$$

Notons $\tilde{G}$ une base de Gröbner de l'idéal $J = (e_1 - z\, f_1, \ldots, e_s - z\, f_s)$ pour un ordre d'élimination pour lequel z est plus grand que $(x_1, \ldots, x_n, e_1, \ldots, e_s)$.

D'après (2.3), $\tilde{G}$ contient des éléments indépendants de z qui sont de la forme

$$a_1e_1 + \cdots + a_se_s \ , \ a_i \in \mathbb{K}[\mathbf{x}].$$

L'ensemble G de ces polynômes engendre le module $\mathrm{Syz}(f_1, \ldots, f_s)$. En effet, soit $a_1e_1 + \cdots + a_se_s \in G$. Comme les éléments de J s'annulent si on substitue e_i par f_i et z par 1, $a_1f_1 + \cdots + a_sf_s = 0$, donc $G \subset \mathrm{Syz}(f_1, \ldots, f_s)$. Inversement, soit $(h_1, \ldots, h_s) \in \mathrm{Syz}(f_1, \ldots, f_s)$. D'après (2.3), $\sum_{i=1}^{s} h_ie_i \in J$. Donc le polynôme $h_1e_1 + \cdots + h_se_s$ se réduit à 0 par $\tilde{G}$, mais aussi par G car il ne contient pas z. Ceci montre que G est bien un système de générateurs de $\mathrm{Syz}(f_1, \ldots, f_s)$.

2.8. Exercices

***Exercice* 2.1. Caractéristiques de certains ordres monomiaux.**
Supposons $x_1 > \cdots > x_n$. Soient $f \in \mathbb{K}[\mathbf{x}]$ et $s \in \{1, \ldots, n\}$. Montrer :

1. Si $\mathtt{m}_l(f) \in \mathbb{K}[x_s, \ldots, x_n]$, alors $f \in \mathbb{K}[x_s, \ldots, x_n]$.
2. Si f est homogène et $\mathtt{m}_{gl}(f) \in \mathbb{K}[x_s, \ldots, x_n]$, alors $f \in \mathbb{K}[x_s, \ldots, x_n]$.
3. Si f est homogène et $\mathtt{m}_{gli}(f) \in (x_s, \ldots, x_n)$, alors $f \in (x_s, \ldots, x_n)$.

***Exercice* 2.2.** Montrer que $<_{gl}$ et $<_{gli}$ coïncident sur $\mathbb{K}[x, y]$ et diffèrent sur $\mathbb{K}[x, y, z]$.

***Exercice* 2.3.** Soit $<$ un ordre total sur l'ensemble des monômes de $\mathbb{K}[\mathbf{x}]$ compatible avec la multiplication par les monômes (i.e. $<$ vérifie ii) de la définition 2.15). Montrer que $<$ est monomial si, et seulement si, $<$ est un bon ordre.

***Exercice* 2.4.** Soit $<$ un ordre monomial. Montrer que $<_g$ défini par

$$\mathbf{x}^\alpha <_g \mathbf{x}^\beta \Longleftrightarrow |\alpha| < |\beta| \ \text{ ou } \ (|\alpha| = |\beta| \ \text{ et } \ \mathbf{x}^\alpha < \mathbf{x}^\beta)$$

est aussi un ordre monomial.

***Exercice* 2.5.** Soit $A = \{(\alpha, \beta) \in \mathbb{N}^2 : 5\beta = \alpha^2 - 6\alpha + 20\}$.

1. Montrer que l'ensemble A est infini.
2. Trouver un sous-ensemble fini minimal B de A tel que $(\mathbf{x}^A) = (\mathbf{x}^B)$.

***Exercice* 2.6. Intersection des idéaux monomiaux de $\mathbb{K}[\mathbf{x}]$.**

1. Soient m_1 et m_2 deux monômes de $\mathbb{K}[\mathbf{x}]$. Déterminer $(m_1) \cap (m_2)$.
2. Soient I_1, I_2, I_3 des idéaux monomiaux de $\mathbb{K}[\mathbf{x}]$. Montrer que
$$(I_1 + I_2) \cap I_3 = (I_1 \cap I_3) + (I_2 \cap I_3).$$
3. En déduire l'intersection de deux idéaux monomiaux.
4. Calculer $(x^3, xyz^2, y^2z, z^3) \cap (z^2, xy^2z)$ dans $\mathbb{K}[x, y, z]$.

***Exercice* 2.7. Quotient des idéaux monomiaux de $\mathbb{K}[\mathbf{x}]$.**

1. Soient m_1 et m_2 deux monômes de $\mathbb{K}[\mathbf{x}]$. Montrer que
$$(m_1) : (m_2) = \{f \in \mathbb{K}[\mathbf{x}] : (m_2)f \subset (m_1)\} = \left(\frac{m_1}{\mathrm{pgcd}(m_1, m_2)}\right).$$

2. Soient I_1, I_2, I_3 des idéaux de $\mathbb{K}[\mathbf{x}]$. Montrer que
$$I_1 : (I_2 + I_3) = (I_1 : I_2) \cap (I_1 : I_3).$$
3. Soient $m, m_1, \ldots, m_s$ des monômes. Montrer que
$$(m_1, \ldots, m_s) : (m) = (m_1) : (m) + \cdots + (m_s) : (m).$$
4. Si I_1 et I_2 sont deux idéaux monomiaux, déterminer $I_1 : I_2$.
5. Calculer $(x^3, xyz^2, y^2z, z^3) : (z^2, xy^2z)$ dans $\mathbb{K}[x, y, z]$.

***Exercice* 2.8.** Déterminer le radical d'un idéal monomial de $\mathbb{K}[\mathbf{x}]$.

***Exercice* 2.9.** Soit I un idéal monomial de $\mathbb{K}[\mathbf{x}]$.

1. Montrer que le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/I$ est de dimension finie si, et seulement si, pour tout $i \in \{1, \ldots, n\}$, il existe $j \in \mathbb{N}$ tel que ${x_i}^j \in I$.
2. Supposons qu'un système minimal de générateurs de I contient les monômes ${x_1}^{d_1}, \ldots, {x_n}^{d_n}$. Trouver une borne inférieure et une borne supérieure pour la dimension du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/I$.

***Exercice* 2.10.** Soient $f_1 = x^2y + z$ et $f_2 = xz + y$.

1. Calculer une base de Gröbner de (f_1, f_2) pour l'ordre lexicographique $x > y > z$.
2. Montrer que $f = x^2z^3 - xy^2 - zy^2 + z^2 \in (f_1, f_2)$.
3. Déterminer des polynômes q_1 et q_2 tels que $f = q_1 f_1 + q_2 f_2$.

***Exercice* 2.11.** Une base de Gröbner G est dite minimale si
$$\forall\, g \in G\ ,\ \mathtt{m}(g) \notin \mathtt{m}(G \setminus \{g\}).$$
1. Comment peut-on trouver une base de Gröbner minimale de l'idéal I engendré par $f_1, \ldots, f_s$, à partir de celle obtenue par l'algorithme de Buchberger ?
2. Est-ce que l'idéal I admet une seule base de Gröbner minimale ?
3. Que peut-on dire du nombre d'éléments dans les différentes bases de Gröbner minimales de I ?
4. Montrer que tout idéal admet une seule base de Gröbner réduite.

***Exercice* 2.12.** Soient I un idéal de $\mathbb{K}[\mathbf{x}]$ et G une partie finie de I. Montrer que G est une base de Gröbner de I si, et seulement si, pour tout $f \in I$, le reste de la division de f par G est nul.

***Exercice* 2.13.** Soit I un idéal de $\mathbb{K}[\mathbf{x}]$. Pour $r \in \{1, \ldots, n\}$, $I_r = I \cap \mathbb{K}[x_1, \ldots, x_r]$.

1. Montrer que si G est une base de Gröbner de I pour l'ordre lexicographique $x_n > \cdots > x_1$, alors $G \cap \mathbb{K}[x_1, \ldots, x_r]$ est une base de Gröbner de I_r.
2. En déduire un algorithme pour la résolution des systèmes polynomiaux.
3. Qu'est ce que l'on obtient si l'on applique cet algorithme à un système linéaire ?

***Exercice* 2.14.** Considérons les éléments suivants de $\mathbb{K}[x]$

$$f_1 = {x_1}^d\ ,\ f_2 = x_1 - {x_2}^d\ ,\ \ldots\ ,\ f_{n-1} = x_{n-2} - {x_{n-1}}^d\ ,\ f_n = 1 - x_{n-1}{x_n}^{d-1}.$$

1. Montrer que $1 \in (f_1, \ldots, f_n)$.
2. Si $g_1, \ldots, g_n$ sont des polynômes tels que $1 = g_1 f_1 + \cdots + g_n f_n$, montrer que $\max \deg g_i \geq d^n - d^{n-1}$.
3. Déterminer $g_1, \ldots, g_n \in \mathbb{K}[\mathbf{x}]$ qui vérifient

$$1 = g_1 f_1 + \cdots + g_n f_n \quad , \quad \text{avec} \quad \max \deg g_i = d^n - d^{n-1}.$$

***Exercice* 2.15. Intersection des idéaux de $\mathbb{K}[\mathbf{x}]$.**
Soient $I = (f_1, \ldots, f_s)$ et $J = (h_1, \ldots, h_l)$ deux idéaux de $\mathbb{K}[\mathbf{x}]$.

1. Si u est une nouvelle variable, montrer que

$$I \cap J = \big(uf_1, \ldots, uf_s, (1-u)h_1, \ldots, (1-u)h_l\big) \cap \mathbb{K}[\mathbf{x}].$$

2. En déduire un algorithme pour déterminer des générateurs de $I \cap J$.

***Exercice* 2.16. Représentation implicite d'une variété algébrique.**

1. Soient $p_1, \ldots, p_n, q_1, \ldots, q_n \in \mathbb{K}[\mathbf{y}] = \mathbb{K}[y_1, \ldots, y_m]$. Si le corps $\mathbb{K}$ est infini, montrer que la plus petite variété algébrique de $\mathbb{K}^n$ contenant l'ensemble

$$\left\{ \left(\frac{p_1(y)}{q_1(y)}, \ldots, \frac{p_n(y)}{q_n(y)} \right) : y \in \mathbb{K}^m \text{ et } q_1 \ldots q_n(y) \neq 0 \right\}$$

est $\mathcal{Z}(J \cap \mathbb{K}[\mathbf{x}])$, où J est l'idéal de $\mathbb{K}[\mathbf{x}, \mathbf{y}, u]$ engendré par les polynômes

$$x_1 q_1(\mathbf{y}) - p_1(\mathbf{y}) \quad , \quad \ldots \quad , \quad x_n q_n(\mathbf{y}) - p_n(\mathbf{y}) \ , \ 1 - u q_1(\mathbf{y}) \ldots q_n(\mathbf{y}).$$

2. Montrer que la variété $\mathcal{Z}(J \cap \mathbb{K}[\mathbf{x}])$ est irréductible.
3. En déduire un algorithme pour passer d'une représentation paramétrée

$$\begin{cases} x_1 = \dfrac{f_1(t_1, \ldots, t_s)}{d_1(t_1, \ldots, t_s)} \\ \qquad \vdots \\ x_n = \dfrac{f_n(t_1, \ldots, t_s)}{d_n(t_1, \ldots, t_s)} \end{cases}$$

(les $f_i, d_i, i = 1, \ldots, n$, sont des polynômes) d'une variété algébrique V de $\mathbb{K}^n$ à une représentation implicite (i.e. $V = \mathcal{Z}(g_1, \ldots, g_t)$, avec $g_1, \ldots, g_t \in \mathbb{K}[\mathbf{x}]$).

***Exercice* 2.17. Saturé d'un idéal par un autre idéal.**
Soient I et $J = (g_1, \ldots, g_t)$ deux idéaux de $\mathbb{K}[\mathbf{x}]$. L'idéal saturé de I par J est

$$(I : J^*) = \cup_{i \in \mathbb{N}} (I : J^i) = \{ f \in \mathbb{K}[\mathbf{x}] : \text{ il existe } m \in \mathbb{N}, \ f\, J^m \subset I \}.$$

Il décrit la variété définie par I « en dehors » de celle définie par J.

1. Soient $u_1, \ldots, u_t$ des nouvelles variables, et K l'idéal de $\mathbb{K}[\mathbf{x}, u_1, \ldots, u_t]$ engendré par les éléments de I et les polynômes $1 - u_1 g_1, \ldots, 1 - u_t g_t$. Montrer que l'idéal d'élimination $K \cap \mathbb{K}[\mathbf{x}] = (I : J^*)$.
2. En déduire un algorithme pour déterminer le saturé de I par J.

***Exercice* 2.18. Quotient des idéaux de $\mathbb{K}[\mathbf{x}]$.**
Soient I et $J = (h_1, \ldots, h_t)$ deux idéaux de $\mathbb{K}[\mathbf{x}]$.

1. Si $I \cap (h_i) = (g_1, \ldots, g_r)$, montrer que $I : (h_i) = \left(\frac{g_1}{h_i}, \ldots, \frac{g_r}{h_i}\right)$.
2. Montrer que $I : J = \bigcap_{i=1}^{t} \big(I : (h_i)\big)$.
3. En déduire un algorithme pour calculer $I : J$.

***Exercice* 2.19. Bases de Gröbner des sous-modules de $\mathbb{K}[\mathbf{x}]^m$.**

1. Soient $f, f_1, \ldots, f_s \in \mathbb{K}[\mathbf{x}]^m$. Écrire l'algorithme de division de f par la famille $\{f_1, \ldots, f_s\}$.
2. Formuler la définition d'une base de Gröbner d'un sous-module de $\mathbb{K}[\mathbf{x}]^m$.
3. Généraliser l'algorithme de Buchberger aux sous-modules de $\mathbb{K}[\mathbf{x}]^m$.
4. Soit M un sous-module de $\mathbb{K}[\mathbf{x}]^m$. Comment peut-on trouver une base du module quotient $\mathbb{K}[\mathbf{x}]^m/M$?
5. Montrer que $\mathbb{K}[\mathbf{x}]^m$ est un *module noethérien* (i.e. tout sous-module de $\mathbb{K}[\mathbf{x}]^m$ est engendré par un nombre fini d'éléments).
6. Comment peut-on tester si un élément f de $\mathbb{K}[\mathbf{x}]^m$ appartient au sous-module engendré par $f_1, \ldots, f_s$?

***Exercice* 2.20. Module des relations de monômes de $\mathbb{K}[\mathbf{x}]$.**

Soient $m_1, \ldots, m_s$ des monômes de $\mathbb{K}[\mathbf{x}]$. Montrer que $\mathrm{Syz}(m_1, \ldots, m_s)$ est engendré par les relations élémentaires

$$\frac{\mathrm{ppcm}(m_i, m_j)}{m_i} e_i - \frac{\mathrm{ppcm}(m_i, m_j)}{m_j} e_j \quad , \qquad 1 \le i < j \le s,$$

où $(e_1, \ldots, e_s)$ est la base canonique de $\mathbb{K}[\mathbf{x}]^s$

***Exercice* 2.21. Module des relations de polynômes de $\mathbb{K}[\mathbf{x}]$.**

Soient $f_1, \ldots, f_s$ des polynômes de $\mathbb{K}[\mathbf{x}]$. Notons $(e_1, \ldots, e_s)$ la base canonique du $\mathbb{K}[\mathbf{x}]$-module $\mathbb{K}[\mathbf{x}]^s$.

1. Si $\{f_1, \ldots, f_s\}$ est une base de Gröbner, montrer que $\mathrm{Syz}(f_1, \ldots, f_s)$ est engendré par

$$\sigma_{ij} = \mathrm{ppcm}\big(\mathtt{m}(f_i), \mathtt{m}(f_j)\big) \left(\frac{e_i}{\mathtt{t}(f_i)} - \frac{e_j}{\mathtt{t}(f_j)}\right) - \sum_{k=1}^{s} q_{ij,k} e_k \ , \ 1 \le i < j \le s,$$

   où les $q_{ij,k}$ sont les quotients de la division de $S(f_i, f_j)$ par $\{f_1, \ldots, f_s\}$.
2. Soit $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de $(f_1, \ldots, f_s)$. Notons par f et g les vecteurs de composantes $f_1, \ldots, f_s$ et $g_1, \ldots, g_t$, M la matrice obtenue par la division de chaque f_i par G et qui satisfait $f = gM$, N la matrice obtenue lors de la construction de G par l'algorithme de Buchberger et qui vérifie $g = fN$.
   i) Si $\sigma_1, \ldots, \sigma_r$ sont des générateurs de $\mathrm{Syz}(g_1, \ldots, g_t)$, montrer que les $N\sigma_i$ sont des éléments de $\mathrm{Syz}(f_1, \ldots, f_s)$.
   ii) Montrer que les colonnes $l_1, \ldots, l_m$ de la matrice $\mathbb{I} - NM$ appartiennent à $\mathrm{Syz}(f_1, \ldots, f_s)$.
   iii) Montrer que le premier module des syzygies $\mathrm{Syz}(f_1, \ldots, f_s)$ est engendré par $N\sigma_1, \ldots, N\sigma_r, l_1, \ldots, l_m$.

***Exercice* 2.22. Autre méthode d'intersection des idéaux de $\mathbb{K}[\mathbf{x}]$.**

Soient $I = (f_1, \ldots, f_s)$ et $J = (h_1, \ldots, h_l)$ deux idéaux de $\mathbb{K}[\mathbf{x}]$. Notons

$$\mathbf{1} = (1,1)\ ,\ F_1 = (f_1, 0)\ , \ldots,\ F_s = (f_s, 0)\ ,\ H_1 = (0, h_1)\ , \ldots,\ H_l = (0, h_l),$$

$$\pi_1 : (g_1, \ldots, g_{s+l+1}) \in \mathbb{K}[\mathbf{x}]^{s+l+1} \quad \mapsto \quad g_1 \in \mathbb{K}[\mathbf{x}].$$

1. Montrer que $I \cap J = \pi_1\big(\mathrm{Syz}(\mathbf{1}, F_1, \ldots, F_s, H_1, \ldots, H_l)\big)$.
2. Montrer que si le $\mathbb{K}[\mathbf{x}]$-module $\mathrm{Syz}(\mathbf{1}, F_1, \ldots, F_s, H_1, \ldots, H_l)$ est engendré par $G_1, \ldots, G_r$, alors l'idéal $I \cap J = \big(\pi_1(G_1), \ldots, \pi_1(G_r)\big)$.
3. En déduire un algorithme pour calculer l'intersection des idéaux de $\mathbb{K}[\mathbf{x}]$.

***Exercice* 2.23.** Soient

$$\begin{aligned} f_0 &= 2\,x - 4\,xy + 4\,xy^2 - 2\,x^2 + 4\,x^2y - 4\,x^2y^2 + 2\,y - 2\,y^2 \\ f_1 &= 4\,xy - 4\,xy^2 \\ f_2 &= 2\,y - 2\,y^2 - 8\,xy + 10\,xy^2 + 8\,x^2y - 10\,x^2y^2 \\ f_3 &= 2\,xy^2 - 2\,x^2y^2. \end{aligned}$$

1. Décrire l'algèbre $\mathbb{Q}[\frac{f_1}{f_0}, \frac{f_2}{f_0}, \frac{f_3}{f_0}]$, comme une algèbre quotient.
2. Tracer la variété associée à ce quotient, déterminer ses points singuliers, montrer qu'elle contient quatres droites.

***Exercice* 2.24. Optimisation combinatoire.**

Le but de cet exercice est de résoudre le problème suivant : un chef d'une entreprise de 50 salariés (32 ouvriers, 13 techniciens, 5 commerciaux) souhaite minimiser sa masse salariale. Les employés se répartissent sur 3 sites : le premier (19 ouvriers, 8 techniciens, 2 commerciaux), le deuxième (8 ouvriers, 3 techniciens, 2 commerciaux) et le troisième (5 ouvriers, 2 techniciens, 1 commercial).

Supposons que le salaire perçu par chaque catégorie d'employés est le même sur les différents sites et que chaque salaire correspond à un nombre entier de points. Comment minimiser la masse salariale de cet entreprise sachant que pour la rentabilité de chaque site, les salaires sur le premier (respectivement deuxième, troisième) ne doivent pas dépasser 99 (respectivement 66, 35) points ?

Donc si A désigne le salaire d'un ouvrier, B celui d'un technicien et C celui d'un commercial, le problème est de minimiser $32A + 13B + 5C$ sous les contraintes en inégalités

$$19A + 8B + 2C \leq 99\ \ ,\ \ 8A + 3B + 2C \leq 66\ \ ,\ \ 5A + 2B + C \leq 35.$$

1. Quitte à introduire des nouvelles variables A_i, montrer que le problème générale se ramène à optimiser une forme linéaire

$$l : (A_1, \ldots, A_n) \in \mathbb{Z}^n \mapsto \alpha_1 A_1 + \cdots + \alpha_n A_n$$

sous les contraintes d'égalités

$$\gamma_{1,1}A_1 + \cdots + \gamma_{1,n}A_n = \beta_1\ \ ,\ \ \ldots\ \ ,\ \ \gamma_{m,1}A_1 + \cdots + \gamma_{m,n}A_n = \beta_m\ , \tag{2.4}$$

où les entiers $\alpha_j, \lambda_{i,j}$ et β_i sont donnés.

2. Supposons ici que les $\gamma_{i,j}$ et β_i soient positifs et considérons l'homomorphisme d'algèbres
$$\phi : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[y_1, \ldots, y_m]$$
défini par $\phi(x_i) = y_1^{\gamma_{1,i}} \ldots y_m^{\gamma_{m,i}}$. A quelle condition le n-uplet $(A_1, \ldots, A_n) \in \mathbb{N}^n$ vérifie les contraintes (2.4) ?
3. Soient $f_1, \ldots, f_n \in \mathbb{K}[y_1, \ldots, y_m]$, et G une base de Gröbner de l'idéal $I = (f_1 - x_1, \ldots, f_n - x_n)$ de $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ pour un ordre d'élimination pour lequel les monômes en $y_1, \ldots, y_m$ sont plus grands que ceux en $x_1, \ldots, x_n$. Pour tout $f \in \mathbb{K}[y_1, \ldots, y_m]$. Montrer que
   i) $f \in \mathbb{K}[f_1, \ldots, f_n]$ si, et seulement si, $\mathtt{N}_G(f) \in \mathbb{K}[x_1, \ldots, x_n]$ (ceci est un test d'appartenance au sous-anneau de $\mathbb{K}[y_1, \ldots, y_m]$ engendré par $f_1, \ldots, f_n$).
   ii) Si $f \in \mathbb{K}[f_1, \ldots, f_n]$, alors $f = N_G(f)(f_1, \ldots, f_n)$.
   iii) Si $f \in \mathbb{K}[f_1, \ldots, f_n]$ et $f_1, \ldots, f_n$ sont des monômes, alors $N_G(f)$ est aussi un monôme.

   Si $f_i = y_1^{\gamma_{1,i}} \ldots y_m^{\gamma_{m,i}}, i = 1, \ldots, n$, d'après iii), l'identité (2.4) est vérifiée si, et seulement si, $y_1^{\beta_1} \ldots y_m^{\beta_m} \in \mathrm{im}(\phi) = \mathbb{K}[f_1, \ldots, f_n]$.
4. Montrer que si $f = y_1^{\beta_1} \ldots y_m^{\beta_m} \in \mathbb{K}[f_1, \ldots, f_n]$, alors l'exposant du monôme $N_G(f) \in \mathbb{K}[x_1, \ldots, x_m]$ est un minimum de l'application l sous les contraintes (2.4).
5. Quelle est la solution de ce problème de minimisation de la masse salariale ?
6. Montrer que le cas $\gamma_{i,j}, \beta_k \in \mathbb{Z}$ peut se traiter de la même façon en rajoutant une nouvelle variable z et le polynôme $zy_1 \ldots y_m - 1$ à l'idéal I.