Méthodes Algébriques Effectives.

Mireille Martin-Deschamps

Chapitre 0

Introduction

En géométrie algébrique et en algèbre commutative, les résultats sont généralement formulés d'une manière qu'on qualifie de non-effective. Ainsi, un théorème fondamental dit que tout idéal d'un anneau de polynômes sur un corps est de type fini, mais ce résultat ne dit rien sur la manière effective de déterminer un ensemble fini de générateurs d'un idéal donné.
Voici des exemples de questions effectives :
– étant donnés deux idéaux $(f_1, \ldots, f_r)$ et $(g_1, \ldots, g_s)$, déterminer leur intersection ;
– savoir si un polynôme donné appartient à un idéal donné ;
– trouver toutes les relations entre des polynômes donnés.
Le but de ce cours est de donner des résultats et des techniques permettant de répondre à ce type de questions concernant des anneaux de polynômes.
L'idée fondamentale est la suivante : lorsqu'on considère des idéaux monomiaux, c'est-à-dire engendrés par des monômes, la plupart des problèmes sont beaucoup plus faciles à résoudre. Nous commencerons donc par l'étude des idéaux monomiaux, puis nous verrons comment, grâce à la notion d'ordre monomial et aux bases de Gröbner on peut se ramener dans le cas général à faire des calculs sur des monômes.
Pour suivre ce cours, il faut posséder au minimum les connaissances suivantes :
– Notions de base d'algèbre commutative.
– Anneaux noethériens
– Propriétés des anneaux de polynômes sur un corps.
– Variétés algébriques affines.

0.1 Plan du cours

1 Idéaux homogènes. Idéaux monomiaux. Fonctions de Hilbert.

2 Ordres monomiaux. Idéaux initiaux.

3 Algorithme de division euclidienne. Existence et unicité.

4 Bases de Gröbner d'un idéal. Propriétés et construction. Algorithme de Buchberger.

5 Applications :
- Elimination.
- Solutions des systèmes algébriques (sur un corps algébriquement clos).

- Intersection d'idéaux.
- Suites régulières.
- Clôture projective et idéal à l'infini.
- Construction d'une famille plate reliant une k-algèbre de type fini à la k-algèbre définie par l'idéal initial.

6 Idéaux initiaux génériques. Idéaux monomiaux Borel-fixes. Théorème de Galligo.

7 Conditions de croissance des idéaux (Macaulay).

0.2 Références

Aroca J.M., Hironaka H., Vicente J.L., The theory of maximal contact. Memorias de Matematica del Instituto Jorge Juan, 1975.
Bayer D.A. The division algorithm and the Hilbert scheme, Thesis, 1982, Harvard University.
Cox D., Little J., O'Shea D., Using Algebraic Geometry. Graduate texts in Mathematics, Springer 1998.
Eisenbud D., Commutative Algebra with a view toward Algebraic Geometry. Graduate texts in Mathematics, Springer 1995.
Green M., Generic Initial Ideals. Six lectures on Commutative Algebra. Progress in Mathematics, Birkhäuser 1998.
Hironaka H. Resolution of singularities of an algebraic variety over a field of char. 0, Annals of Maths 79 (1964) 109-326.
Lejeune-Jalabert M., Effectivité de calculs polynomiaux, Cours de DEA 1984-85, Institut Fourier.
Stanley R.P., Hilbert Functions of Graded Algebras, Advances in Maths 28 (1978) 57-83.

0.3 Notations

On désigne par k un corps commutatif, qui sera souvent algébriquement clos, et dont les éléments sont appelés *scalaires*, par n un entier ≥ 1 et par $S = k[X_1, \ldots, X_n]$ l'anneau des polynômes à n indéterminées à coefficients dans k. On rappelle que cet anneau est noethérien.

Définitions 0.3.1. Soit $\alpha \in \mathbb{N}^n$ le multi-indice $\alpha = (\alpha_1, \ldots, \alpha_n)$. On lui associe le polynôme $X^\alpha = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. Un *monôme* de S est un polynôme de la forme X^α, et α est son *exposant*.
Un *terme* de S est un polynôme égal au produit d'un scalaire de k par un monôme, qui lui est dit associé. Par abus de notation (qui sera justifié au chapitre 2), on appellera exposant d'un terme non nul l'exposant du monôme associé.

Remarque 0.3.1. On identifiera souvent monômes et multi-indices. Un monôme n'est jamais nul, un terme peut l'être.

Remarque 0.3.2. On ne reviendra pas ici sur les notions de divisibilité. Si m et m' sont deux monômes, d'exposants α et α', le pgcd (resp. ppcm) de m et m' est un monôme, d'exposant $\alpha \wedge \alpha' := \inf(\alpha, \alpha')$ (resp. $\alpha \vee \alpha' := \sup(\alpha, \alpha')$), l'inf et le sup étant pris pour l'ordre produit de $\mathbb{N}^n$.

Définitions 0.3.2. Fixons des entiers $a_1, \ldots, a_n$ strictement positifs. Le *degré pondéré* d'un terme non nul $\lambda X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ ($\lambda \neq 0$) est le nombre $\sum_{i=1}^n \alpha_i a_i$; ainsi le monôme (ou, par abus de langage, l'indéterminée) X_i est de degré pondéré a_i. Lorsque les entiers a_i sont tous égaux à 1, on parlera simplement de degré.
Soit $d \in \mathbb{Z}$. La *composante homogène de degré pondéré* d d'un polynôme f, notée $\pi_d(f)$, est égale à la somme de ses termes non nuls de degré pondéré d s'il en a, et à 0 sinon. Le *degré pondéré* d'un polynôme non nul f est le plus grand des degrés de ses termes non nuls. Un polynôme est dit *homogène* si tous ses termes non nuls ont même degré pondéré ou s'il est nul.
Pour $d \in \mathbb{N}$, on note S_d l'espace vectoriel réunion de 0 et des polynômes homogènes non nuls de degré pondéré d. Par convention on posera $S_d = \{0\}$ pour $d < 0$.

Lemme 0.3.3. *Soient $d \in \mathbb{N}$, f et g deux polynômes. On a :*
– $\pi_d(f+g) = \pi_d(f) + \pi_d(g)$;
– $\pi_d(fg) = \sum_{i+j=d} \pi_i(f)\pi_j(g)$.

Remarque 0.3.4. On a un isomorphisme de groupes abéliens $S \simeq \oplus_{d\in\mathbb{N}} S_d$ qui est compatible avec le produit au sens suivant : $S_d S_{d'} \subseteq S_{d+d'}$ pour $d, d' \geqslant 0$, autrement dit S est un anneau gradué.

Chapitre 1

Idéaux monomiaux. Fonctions de Hilbert

1.1 Idéaux homogènes. Idéaux monomiaux

Définition 1.1.1. Un idéal de S est *homogène* (resp. *monomial*) s'il est engendré par des polynômes homogènes (resp. par des monômes) (qui peuvent être choisis en nombre fini).

Lemme 1.1.2. *Soit I un idéal de S. Les propriétés suivantes sont équivalentes :*
i) I est homogène,
ii) un polynôme f appartient à I si et seulement si toutes ses composantes homogènes appartiennent à I.

Démonstration. Le résultat est immédiat si l'idéal I est nul, ce qu'on va exclure pour la suite.
$i) \Rightarrow ii)$: on note $I = (f_1, \dots, f_r)$, où pour tout $i \in [1, r]$, f_i est homogène de degré d_i.
Un polynôme étant la somme de ses composantes homogènes, il est dans I si ses composantes homogènes le sont.
Inversement soient $f = \sum_{i=1}^{r} f_i g_i$ un élément de I et $\pi_d(f)$ sa composante homogène de degré pondéré d. On a :

$$\pi_d(f) = \sum_{i=1}^{r} f_i \pi_{d-d_i}(g_i) \in I.$$

$ii) \Rightarrow i)$: soient $f_1, \dots, f_r$ des générateurs de I. Pour tout $i \in [1, r]$ et pour tout $d \in \mathbb{N}$, la composante homogène $\pi_d(f_i)$ appartient à I. On a donc les inclusions d'idéaux :

$$I = (f_1, \dots, f_r) \subseteq \sum_{d \in \mathbb{N}} (\pi_d(f_1), \dots, \pi_d(f_r)) = (\pi_d(f_i))_{i \in [1,r], d \in \mathbb{N}} \subseteq I$$

et l'idéal I est engendré par les $\pi_d(f_i)$ donc est homogène. □

Définition 1.1.3. Si I est un idéal homogène de S, on note I_d l'intersection $I \cap S_d$, qui est un sous-espace vectoriel de S_d. On dit que I_d est la *composante homogène de degré pondéré d* de I.

Corollaire 1.1.4. *Soient I un idéal homogène de S, et I_d sa composante homogène de degré pondéré d. Alors on a un isomorphisme d'espaces vectoriels : $\oplus_{d\in\mathbb{N}} I_d \simeq I$ et un isomorphisme de groupes abéliens : $\oplus_{d\in\mathbb{N}} S_d/I_d \simeq S/I$ qui fait de S/I un anneau gradué.*

Démonstration. L'injection canonique $S_d \hookrightarrow S$ se prolonge en une injection des quotients $S_d/I_d \hookrightarrow S/I$, d'où un homomorphisme de groupes abéliens $\oplus S_d/I_d \to S/I$ défini de la manière suivante (qui montre que c'est un homomorphisme de groupes) :
un élément de $\oplus S_d/I_d$ correspond à la donnée pour tout d de la classe d'équivalence dans S_d/I_d d'un polynôme homogène f_d de degré pondéré d, un nombre fini seulement de ces f_d étant non nuls ; son image dans S/I est la classe de la somme $\sum f_d$.
Supposons que cette image soit nulle. On a donc $\sum f_d \in I$ et d'après 1.1.2, $f_d \in I$ pour tout d, d'où l'injectivité.
La surjectivité est immédiate.
De même on construit un homomorphisme de groupes abéliens $\oplus I_d \to I$ et on vérifie facilement que c'est un homomorphisme d'espaces vectoriels. L'injectivité résulte du fait que c'est la restriction à $\oplus I_d$ de l'isomorphisme $\oplus S_d \simeq S$. La surjectivité est une conséquence de 1.1.2. □

Remarque 1.1.5. Si I est un idéal quelconque de S, $I_d = I \cap S_d$ est bien sûr toujours un sous-espace vectoriel de S_d, mais il donne peu d'informations sur I. Par exemple, si I est monogène, engendré par un polynôme non homogène, I_d est toujours l'espace vectoriel nul.

Lemme 1.1.6. *Soit I un idéal de S. Les propriétés suivantes sont équivalentes :*
i) I est monomial ,
ii) un polynôme f appartient à I si et seulement si tous ses termes appartiennent à I.

Démonstration. Le résultat est immédiat si l'idéal I est nul, ce qu'on va exclure pour la suite.
i) $\Rightarrow$ *ii)* : on note $I = (m_1, \ldots, m_r)$, où pour tout $i \in [1, r]$, m_i est un monôme. Un polynôme étant la somme de ses termes, il est dans I si ceux-ci le sont.
Inversement soient $f = \sum_{i=1}^{r} m_i g_i$ un élément de I. Tout terme non nul de f associé à un monôme m est la somme des termes non nuls des $m_i g_i$ associés à m, donc est divisible par au moins un des m_i.
ii) $\Rightarrow$ *i)* : la preuve est analogue à celle donnée en 1.1.2.

□

Remarque 1.1.7. On a montré dans la démonstration de 1.1.6 que si I est un idéal monomial de S engendré par des monômes $m_1, \ldots, m_r$, un monôme m appartient à I si et seulement si il est divisible par l'un des m_i.

Proposition 1.1.8. *Soient $(m_1, \ldots, m_r)$ et $(m'_1, \ldots, m'_s)$ deux systèmes de générateurs minimaux d'un idéal monomial I. Alors $r = s$ et quitte à renuméroter, on peut supposer qu'on a $m_i = m'_i$ pour tout $i \in [1, s]$.*

Démonstration. Supposons $r \leq s$. Pour tout $i \in [1, r]$, il existe $\lambda(i) \in [1, s]$ tel que $m'_{\lambda(i)}$ divise m_j. On définit ainsi une application λ de l'ensemble $\{1, \ldots, r\}$ dans l'ensemble $\{1, \ldots, s\}$ et on a :

$$I \subseteq (m'_{\lambda(1)}, \ldots, m'_{\lambda(r)}) \subseteq I$$

à cause de la minimalité du système de générateurs $(m'_1, \ldots, m'_s)$, l'application λ est surjective, donc $r = s$ et λ est bijective. Quitte à renuméroter les indices, on peut supposer que λ est l'identité : pour tout $i \in [1, r]$, m'_i divise m_i.
De même, pour tout i, il existe $\mu(i)$ tel que m_i divise $m'_{\mu(i)}$. Alors m_i divise $m'_{\mu(i)}$ qui divise $m_{\mu(i)}$. A cause de la minimalité du système de générateurs, on a $m_i = m_{\mu(i)=m'_{\mu(i)}}$, donc μ est l'identité.

□

Notation 1.1.9. Soit I un idéal monomial non nul. On note $\exp I$ l'ensemble des exposants des monômes de I.

Remarque 1.1.10. L'ensemble $\exp I$ possède la propriété suivante :

$$\forall \alpha \in \exp I, \forall \beta \in \mathbb{N}^n, \alpha + \beta \in \exp I$$

qu'on peut encore écrire $\exp I + \mathbb{N}^n \subseteq \exp I$, ou $\exp I + \mathbb{N}^n = \exp I$.

Proposition 1.1.11. *L'application qui à un idéal monomial non nul I associe l'ensemble $\exp I$ est une bijection de l'ensemble des idéaux monomiaux non nuls sur l'ensemble des sous-ensembles non vides $\mathcal{E}$ de $\mathbb{N}^n$ vérifiant $\mathcal{E} + \mathbb{N}^n = \mathcal{E}$.*

Démonstration. Soient I et I' deux idéaux monomiaux non nuls tels que $\exp I = \exp I'$. Puisque I et I' sont engendrés par leurs monômes, ils sont égaux.
Soient $\mathcal{E}$ un sous-ensemble de $\mathbb{N}^n$ vérifiant $\mathcal{E}+\mathbb{N}^n = \mathcal{E}$, et I l'idéal (monomial) engendré par les monômes m dont l'exposant appartient à $\mathcal{E}$. Soit m' un monôme de I. Il est divisible par un monôme m dont l'exposant appartient à $\mathcal{E}$, et donc son exposant appartient à $\mathcal{E}$. Donc $\exp I = \mathcal{E}$. □

Remarque 1.1.12. Soient I un idéal monomial, $\exp I$ son ensemble d'exposants et $(m_1, \ldots, m_r)$ un système de générateurs de I . Alors l'ensemble $\{\exp m_1, \ldots, \exp m_r\}$ est une frontière finie de $\exp I$, c'est-à-dire que $\exp I$ est réunion des sous-ensembles en nombre fini $\exp m_i + \mathbb{N}^n$.
Si $(m_1, \ldots, m_r)$ est un système minimal de générateurs, la frontière correspondante (qui est de cardinal minimum) est appelée escalier de $\exp I$.

Dans le cas des idéaux monomiaux, les problèmes du type de ceux qu'on a cités dans l'introduction sont faciles à résoudre, grâce en particulier à 1.1.6 et 1.1.7.

Proposition 1.1.13. *i) Soient I et I' deux idéaux monomiaux. L'idéal $I \cap I'$ est monomial.*

ii) Soient I un idéal monomial et m un monôme. L'idéal $(I : m) = \{ f \in S \mid mf \in I \}$ est monomial.

iii) Soient I un idéal monomial et $n' \leqslant n$ un entier. On considère $S' = k[X_1, \ldots, X_{n'}]$ comme un sous-anneau de S. L'idéal intersection $I' = I \cap S'$ est monomial.

Démonstration. On exclut le cas où les idéaux considérés sont nuls.
Dans chaque cas la démarche est la même : on utilise 1.1.6 pour montrer que l'idéal considéré est monomial, puis on détermine les monômes de cet idéal. Soit f un polynôme.

i) f appartient à $I \cap I'$ si et seulement si il appartient à I et à I', donc si et seulement si tous ses termes appartiennent à I et à I', c'est-à-dire à $I \cap I'$.
On note $I = (m_1, \ldots, m_r)$ et $I' = (m'_1, \ldots, m'_s)$ où pour tout $i \in [1, r]$ et $j \in [1, s]$, m_i et m'_j sont des monômes. Un monôme appartient à $I \cap I'$ si et seulement s'il est divisible par l'un des m_i et l'un des m'_j, ou encore par le ppcm de m_i et m'_j. Donc $I \cap I'$ est engendré par les rs monômes : $\operatorname{ppcm}(m_i, m'_j)$.

ii) f appartient à $(I : m)$ si et seulement si mf appartient à I, donc si et seulement si tous les termes de mf appartiennent à I, c'est-à-dire tous les termes de f appartiennent à $(I : m)$.
On note $I = (m_1, \ldots, m_r)$; si f est un monôme, mf appartient à I si et seulement s'il est divisible par l'un des m_i. Soit d_i le pgcd de m et m_i. On a $m_i = m'_i d_i$ et $m = m' d_i$ avec m' et m'_i sans facteur commun. Alors

$$m_i \text{ divise } mf \Leftrightarrow m'_i \text{ divise } m'f \Leftrightarrow m'_i \text{ divise } f.$$

Donc $(I : m)$ est engendré par les r monômes $m'_i = m_i / \operatorname{pgcd}(m, m_i)$.

iii) f appartient à $I' = I \cap S'$ si et seulement il est dans S', ce qui signifie qu'il ne dépend que des n' premières variables et qu'il appartient à I, donc si et seulement si tous ses termes (qui sont aussi dans S') appartiennent à I, c'est-à-dire tous ses termes appartiennent à I'.
On note $I = (m_1, \ldots, m_r)$; si f est un monôme de S', il appartient à I' si et seulement s'il est divisible par l'un des m_i, qui est alors aussi dans S'. Donc I' est engendré par les monômes parmi $m_1, \ldots, m_r$ qui ne dépendent que des n' premières variables s'il en existe, et est nul sinon.

□

Remarque 1.1.14. Soient $I = (m_1, \ldots, m_r)$, $I' = (m'_1, \ldots, m'_s)$ où pour tout $i \in [1, r]$ et $j \in [1, s]$, m_i et m'_j sont des monômes premiers entre eux. Alors les idéaux (monomiaux) $I \cap I'$ et II' sont égaux puisque $\operatorname{ppcm}(m_i, m'_j) = m_i m'_j$.

1.2 Fonctions de Hilbert

Dans tout ce paragraphe, l'anneau de polynômes S est muni du degré habituel (le degré de chaque indéterminée est égal à 1).
Quand on travaille avec des sous-variétés de l'espace projectif, on considère des idéaux homogènes. Pour un tel idéal I, on a vu en 1.1.4 qu'on a un isomorphisme d'espaces vectoriels : $\oplus I_d \simeq I$. On s'intéresse souvent aux dimensions des composantes homogènes

I_d. Si I est l'idéal des fonctions nulles sur une sous-variété projective X, la dimension de I_d représente le nombre d'hypersurfaces indépendantes de degré d contenant X. C'est ce qu'on appelle la postulation de X.
Une notion équivalente est celle de fonction de Hilbert :

Définition 1.2.1. Soit I un idéal homogène de S. La fonction de Hilbert de l'anneau (gradué, cf. 1.1.4) est la fonction $h_{S/I}$ de $\mathbb{Z}$ dans $\mathbb{N}$ définie par $h_{S/I}(d) = \dim S_d/I_d$.

Dans le cas des idéaux monomiaux, la fonction de Hilbert est facile à calculer. On va commencer par le cas où I est l'idéal nul.

Proposition 1.2.2. *La fonction de Hilbert h_S de l'anneau $S = k[X_1, \ldots, X_n]$ est nulle pour $d < 0$ et est définie par $h_S(d) = \binom{n+d-1}{d} = \binom{n+d-1}{n-1}$ pour $d \geqslant 0$. En particulier, elle est polynomiale en d pour $d \geqslant 0$.*

Démonstration. On peut la faire par récurrence sur n :
– pour $n = 1$, c'est immédiat.
– Pour $n > 1$, on considère le quotient $S' = S/(X_n) \simeq k[X_1, \ldots, X_{n-1}]$. On a un isomorphisme d'espaces vectoriels $S'_d \simeq S_d/X_n S_{d-1}$ donc on a :

$$h_S(d) = h_S(d-1) + h_{S'}(d) = h_S(1) + h_{S'}(2) + \cdots h_{S'}(d).$$

Par hypothèse de récurrence, on a $h_{S'}(d) = \binom{n+d-2}{n-2}$, donc :

$$h_S(d) = 1 + \binom{n-1}{n-2} + \cdots + \binom{n+d-2}{n-2} = \binom{n+d-1}{n-1}.$$

Il y a une autre démonstration, plus élégante : un monôme de degré d en n variables peut être vu comme une suite de $n+d-1$ signes, dont $(n-1)$ sont les signes de multiplication, et d sont des variables. Par exemple, si $n = 4$, le monôme $X_1X_2^2X_4$ correspond à la suite

$$X_1, \times, X_2, X_2, \times, \times, X_4.$$

Alors se donner un monôme de degré d en n variables revient à choisir $(n-1)$ éléments dans un ensemble de cardinal $n+d-1$. □

Proposition 1.2.3. *Soit I un idéal monomial. La fonction de Hilbert $h_{S/I}$ est polynomiale pour $d \gg 0$, c'est-à-dire qu'il existe un polynôme $P \in \mathbb{Q}[t]$, un entier d_0 tels qu'on ait $h_{S/I}(d) = P(d)$ pour $d \geqslant d_0$.*

Démonstration. On suppose l'idéal I non nul et différent de S, soit $I = (m_1, \ldots, m_r)$. On va faire la démonstration par récurrence sur l'entier $N = \sum_{i=1}^{r} \deg m_i$.
– Si tous les m_i sont de degré 1 (ce qui est le cas si $N = 1$), S/I est encore un anneau de polynômes et le résultat est vrai d'après 1.2.2.

– Sinon, on peut supposer que le degré de m_1 est > 1, donc que m_1 a un diviseur m de degré δ avec $1 \leqslant \delta < \deg m_1$.
Considérons les idéaux (monomiaux) $I' = I + (m)$ et $J = (I : m)$.
On a

$$I' = (m, m_2, \ldots, m_r) \quad \text{et} \quad \deg m + \sum_{i=2}^{r} \deg m_i < N.$$

Si on pose $m'_i = m_i / \operatorname{pgcd}(m, m_i)$, on a vu dans la démonstration de 1.1.13, ii), qu'on a $J = (m'_1, \ldots, m'_r)$. On a, pour tout i, $\deg m'_i \leqslant \deg m_i$. De plus pour $i = 1$ on a $m'_1 = m_1/m$ donc

$$\deg m'_1 < \deg m_1 \quad \text{et} \quad \sum_{i=1}^{r} \deg m'_i < N.$$

On peut donc appliquer l'hypothèse de récurrence à I' et à J : $h_{S/I'}$ et $h_{S/J}$ sont polynomiales pour $d \gg 0$.
Considérons l'application linéaire : $S_{d-\delta} \to I'_d/I_d$ qui à f associe la classe de mf. Son noyau est formé des polynômes homogènes f tels que fm appartienne à I, c'est-à-dire est égal à $J_{d-\delta}$. On a donc :

$$h_{S/J}(d-\delta) = \dim I'_d/I_d = h_{S/I}(d) - h_{S/I'}(d)$$

$$h_{S/I}(d) = h_{S/I'}(d) + h_{S/J}(d-\delta)$$

et $h_{S/I}$ est polynomiale pour $d \gg 0$.

□

Exemple 1.2.4. On suppose $n = 4$ et $I = (X_1X_3, X_1X_4, X_2X_4)$. On va utiliser le procédé précédent (deux fois) pour calculer la fonction $h_{S/I}$.
– On choisit $m = X_1$. On a alors $I' = I + (X_1) = (X_1, X_2X_4)$ et $J = (I : X_1) = (X_3, X_4)$, d'où :

$$h_{S/I}(d) = h_{S/I'}(d) + h_{S/J}(d-1).$$

– On choisit $m' = X_2$. On a alors $I'' = I' + (X_2) = (X_1, X_2)$ et $J' = (I' : X_2) = (X_1, X_4)$, d'où :

$$h_{S/I'}(d) = h_{S/I''}(d) + h_{S/J'}(d-1)$$

$$h_{S/I}(d) = h_{S/I''}(d) + h_{S/J}(d-1) + h_{S/J'}(d-1).$$

Les anneaux S/I'', S/J, S/J' sont des anneaux de polynômes à 2 variables et ont la même fonction de Hilbert $h(d) = d + 1$ pour $d \geqslant -1$. On a donc :

$$h_{S/I}(d) = h(d) + 2h(d-1) = 3d + 1 \quad \text{pour } d \geqslant 0.$$

Ce procédé est efficace et donne facilement un algorithme. Cependant il est parfois plus rapide de faire le calcul directement grâce au résultat suivant :

Proposition 1.2.5. *Soit I un idéal. L'ensemble $\mathcal{M}$ des monômes qui ne sont pas dans I (plus précisément leurs images dans S/I) est un système de générateurs de S/I. Si I est monomial, $\mathcal{M}$ une base de S/I.*

Démonstration. $\mathcal{M}$ est vide si et seulement si $I = S$ donc $S/I = (0)$.
Sinon, les images des monômes forment un système de générateurs de S/I. Ceux qui sont dans I ont une classe nulle dans S/I, donc $\mathcal{M}$ engendre S/I.
Soient $m_1, \ldots, m_r$ des monômes deux à deux distincts non dans I et supposons qu'il existe des scalaires non nuls $\lambda_1, \ldots, \lambda_r$ tels que $\sum \lambda_i m_i$ soit nul dans S/I, autrement dit tels que $\sum \lambda_i m_i$ appartienne à I. Si I est monomial, on en déduit que pour tout i, m_i appartient à I, d'où une contradiction. □

Exemple 1.2.6. On reprend l'exemple 1.2.4 : $n = 4$ et $I = (X_1X_3, X_1X_4, X_2X_4)$. Soit $m = X_1^{\alpha_1}X_2^{\alpha_2}X_3^{\alpha_3}X_4^{\alpha_4}$ un monôme. On a les équivalences :

$$m \in I \Leftrightarrow \begin{cases} \alpha_1 \geqslant 1 \text{ et } \alpha_3 \geqslant 1 \\ \quad \text{ou} \\ \alpha_1 \geqslant 1 \text{ et } \alpha_4 \geqslant 1 \\ \quad \text{ou} \\ \alpha_2 \geqslant 1 \text{ et } \alpha_4 \geqslant 1 \end{cases} \quad , \qquad m \notin I \Leftrightarrow \alpha_1\alpha_3 = \alpha_1\alpha_4 = \alpha_2\alpha_4 = 0.$$

Soit $\mathcal{M}_1$ (resp. $\mathcal{M}_2$, resp. $\mathcal{M}_3$) l'ensemble des monômes m tels que $\alpha_1 = \alpha_2 = 0$ (resp. $\alpha_1 = \alpha_4 = 0$, resp. $\alpha_3 = \alpha_4 = 0$). On a $\mathcal{M}_d = \mathcal{M}_{1,d} \cup \mathcal{M}_{2,d} \cup \mathcal{M}_{3,d}$ donc

$$\#\mathcal{M}_d = \sum_i \#\mathcal{M}_{i,d} - \sum_{i \neq j} \#(\mathcal{M}_{i,d} \cap \mathcal{M}_{j,d}) + \#(\mathcal{M}_{1,d} \cap \mathcal{M}_{2,d} \cap \mathcal{M}_{3,d}).$$

On a pour tout $d \geqslant 0$, $\#\mathcal{M}_{i,d} = d + 1$. De plus, $\mathcal{M}_{1,d} \cap \mathcal{M}_{2,d}$ (resp. $\mathcal{M}_{2,d} \cap \mathcal{M}_{3,d}$) est un espace vectoriel de dimension 1, engendré par X_3^d (resp. X_2^d) et $\mathcal{M}_{1,d} \cap \mathcal{M}_{3,d}$ est nul. On a donc $\#\mathcal{M}_d = 3(d + 1) - 2 = 3d + 1$.

Chapitre 2

Ordres monomiaux. Idéaux initiaux

2.1 Préliminaires

On a vu que lorsqu'un idéal I est monomial, les monômes qui ne sont pas dans I forment une base du quotient S/I, ce qui permet de calculer sa fonction de Hilbert. Lorsque l'idéal n'est pas monomial, ils forment encore un système de générateurs, donc on peut en principe en extraire une base. Comment faire ?
Soit f un polynôme. Peut-on savoir s'il appartient à I ? Là encore, si I est monomial et si on a un système de générateurs, il y a un moyen de résoudre le problème : on vérifie que les termes de f sont divisibles par un des générateurs de I.
C'est pour résoudre ces problèmes, et bien d'autres, qu'on introduit la notion d'ordre sur les monômes.

Remarque 2.1.1. Il y a deux cas où on sait également résoudre le problème d'appartenance d'un polynôme à un idéal :
- Si $n = 1$, alors I est monogène, engendré par un polynôme g. On fait la division euclidienne de f par g et on calcule le reste. Alors f est dans $I = (g)$ si et seulement si ce reste est nul.
- Si I est engendré par des polynômes de degré 1, l'algorithme de Gauss permet de construire un système de générateurs de I sous forme réduite échelonnée :

  $$f_1 = X_{i_1} - f'_1, \ldots, f_r = X_{i_r} - f'_r$$

  avec $i_1 < i_2 < \cdots < i_r$ et où f'_j ne dépend pas des variables X_{i_k} avec $1 \leqslant k \leqslant r$.
  On peut le voir aussi sous forme matricielle par blocs. Si $i_1 = 1$, la matrice des f_i est de la forme :

  $$\begin{pmatrix} A_{1,1} & A_{1,2} & \ldots & A_{1,r} \\ 0 & A_{2,2} & \ldots & A_{2,r} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & A_{r,r} \end{pmatrix}$$

  où chaque $A_{i,i}$ est un bloc d'une ligne commençant par 1 et pour $i \neq j$ chaque $A_{i,j}$ est un bloc d'une ligne commençant par 0.

Si $i_1 > 1$ c'est une matrice similaire, où on rajoute des premières colonnes formées de 0. Alors f peut s'écrire $f = (X_{i_1} - f'_1)g_1 + \cdots + (X_{i_r} - f'_r)g_r + f'$ où f' est obtenu en remplaçant X_{i_j} par f'_j pour $j \in [1, r]$, et ne dépend que des autres variables. Donc f appartient à I si et seulement si $f' = 0$.

Dans le premier cas, on a utilisé l'algorithme de division euclidienne, basé sur l'ordre total donné par le degré, dans le deuxième cas, on a utilisé l'algorithme de Gauss, basé sur l'ordre des variables : $X_1 > X_2 > \cdots > X_n$.

2.2 Ordres monomiaux

Définition 2.2.1. Un *ordre monomial* sur S est un ordre total sur les monômes qui vérifie la propriété suivante pour tous monômes m, m_1, m_2 (en notant $>$ l'ordre) :

$$m_1 > m_2\,,\, m \neq 1 \Rightarrow mm_1 > mm_2 > m_2.$$

Remarque 2.2.2. La deuxième inégalité : $mm_2 > m_2$ si $m \neq 1$, montre qu'un tel ordre est compatible avec la divisibilité. En particulier tout monôme $m \neq 1$ est > 1 et 1 est le plus petit des monômes.

On peut exprimer la propriété avec les exposants au lieu des monômes. Pour tous exposants α_1, α_2, β :

$$\alpha_1 > \alpha_2\,,\, \beta \neq 0 \Rightarrow \alpha_1 + \beta > \alpha_2 + \beta > \alpha_2.$$

La définition ne dit rien sur l'ordre entre les indéterminées et il faut faire un choix. Dans la pratique on prendra toujours $X_1 > X_2 > \cdots > X_n$.

Remarque 2.2.3. On étend la notation aux termes non nuls. Soient m_1 et m_2 deux monômes, λ_1 et λ_2 deux scalaires non nuls. Si $m_1 > m_2$ (resp. $m_1 \geqslant m_2$) on dira que $\lambda_1 m_1 > \lambda_2 m_2$ (resp. $\lambda_1 m_1 \geqslant \lambda_2 m_2$). C'est un abus de notation car ce n'est pas un ordre puisque ce n'est pas antisymétrique. En particulier le sup de deux termes $\lambda_1 m_1$ et $\lambda_2 m_2$ n'existe pas si $m_1 = m_2$ et $\lambda_1 \neq \lambda_2$.

Remarque 2.2.4. Par ailleurs, on sera aussi amené à considérer l'ordre produit sur $\mathbb{N}^n$, qui n'est pas un ordre total si $n > 1$.

Exemple 2.2.5. Les trois ordres monomiaux les plus utilisés sont les suivants. Soient $\alpha = (\alpha_1, \ldots, \alpha_n)$ et $\beta = (\beta_1, \ldots, \beta_n$ deux exposants. On définit :

– l'ordre lexicographique (noté lex) :

$$\alpha < \beta \Leftrightarrow \exists\, s \in [1, n] \text{ tel que } \alpha_i = \beta_i \text{ pour } i < s \text{ et } \alpha_s < \beta_s,$$

– l'ordre lexicographique homogène (noté hlex) :

$$\alpha < \beta \Leftrightarrow \begin{cases} \deg \alpha < \deg \beta \\ \quad \text{ou} \\ \deg \alpha = \deg \beta \text{ et } \exists\, s \in [1, n] \text{ tel que } \alpha_i = \beta_i \text{ pour } i < s \text{ et } \alpha_s < \beta_s, \end{cases}$$

c'est-à-dire que lex et hlex coïncident sur les monômes de même degré ;

– l'ordre lexicographique inverse (noté revlex) :

$$\alpha < \beta \Leftrightarrow \begin{cases} \deg \alpha < \deg \beta \\ \quad \text{ou} \\ \deg \alpha = \deg \beta \text{ et } \exists\, s \in [1,n] \text{ tel que } \alpha_i = \beta_i \text{ pour } i > s \text{ et } \alpha_s > \beta_s. \end{cases}$$

Sur les monômes de même degré, c'est l'inverse de l'ordre obtenu en renversant l'ordre des variables et en utilisant l'ordre lexicographique.

Pour tous ces ordres, on a bien $X_1 > X_2 > \cdots > X_n$. Les deux derniers raffinent l'ordre défini par le degré. On dit aussi qu'ils sont compatibles avec le degré.

Exemples 2.2.6. Si $n = 1$, il y a un seul ordre possible, donné par le degré : $X^d > X^{d'}$ si $d > d'$.

Si $n = 2$, si on choisit $X_1 > X_2$, on a obligatoirement $X_1^d > X_1^{d-1}X_2 > \cdots > X_2^d$, donc on n'a pas le choix pour les monômes de même degré. Les deux ordres hlex et revlex sont identiques, mais ils diffèrent de l'ordre lex. Par exemple, les exposants $\alpha = (\alpha_1, \alpha_2)$ inférieurs à $(2, 3)$ sont les suivants :

– pour l'ordre lexicographique : $\alpha_1 < 2$ ou $\alpha_1 = 2$, $\alpha_2 < 3$. En particulier il y en a une infinité.
– pour l'ordre lexicographique inverse : $\alpha_1 + \alpha_2 < 5$ ou $\alpha_1 + \alpha_2 = 5$ et $\alpha_2 > 3$. Il y en a un nombre fini (17 exactement).

Si $n = 3$, regardons par exemple les formes quadratiques. On a obligatoirement :

$$X_1^2 > X_1X_2 > X_1X_3 \quad X_2^2 > X_2X_3 > X_3^2$$

mais rien n'est imposé entre X_1X_3 et X_2^2. On a pour hlex, $X_1X_3 > X_2^2$ et pour revlex, $X_1X_3 < X_2^2$.

L'exemple ci-dessus montre qu'il peut exister une infinité de monômes plus petits qu'un monôme donné. Cependant on a un résultat de finitude :

Proposition 2.2.7. *Tout sous-ensemble $\mathcal{M}$ non vide de monômes a un plus petit élément. En particulier, il n'existe pas de suite décroissante infinie.*

Démonstration. Soit I l'idéal (monomial) engendré par les éléments de $\mathcal{M}$. On peut extraire de $\mathcal{M}$ un nombre fini de générateurs de I, qu'on peut supposer rangés par ordre croissant : $m_1 < \cdots < m_r$. Tout élément de l'idéal est divisible par l'un des m_i, donc est plus grand que m_1. □

2.3 Termes initiaux. Idéaux initiaux

Définition 2.3.1. Soit f un polynôme non nul et $>$ un ordre monomial sur S. Le *terme initial* de f, notée $\text{in}_> f$, est le terme correspondant au plus grand monôme qui apparaît dans f. L'exposant correspondant est l'*exposant* de f et noté $\exp_> f$. Lorsqu'il n'y a pas de confusion possible sur l'ordre, on ne le met pas en indice.

Exemple 2.3.2. Supposons $n = 2$ et soit $f = X_1^2X_2^3 - X_1^2X_2^2 + 2X_1^4 + 3X_1^3$. On a :
– Pour l'ordre lex, $\text{in}_{lex}\, f = 2X_1^4$, $\exp_{lex} f = (4, 0)$.
– Pour les ordres hlex et revlex, $\text{in}_{hlex}\, f = X_1^2X_2^3$, $\exp_{hlex} f = (2, 3)$.

Grâce à la notion d'ordre et à 2.2.7, nous pourrons utiliser dans les démonstrations un procédé de récurrence qui sera très utile. On peut le formaliser de la manière suivante :

Corollaire 2.3.3. *Soit $P(f)$ une propriété qui peut être satisfaite par des éléments non nuls de S. Si $P(1)$ est vrai, et si on a la condition suivante :*
"$f \neq 0$ donné ; si $P(f')$ est vrai pour tout $f' \neq 0$ vérifiant $exp\, f' < exp\, f$, alors $P(f)$ est vrai"
alors $P(f)$ est vrai pour tout $f \in S$ non nul.

Démonstration. Considérons l'ensemble $\mathcal{M}$ des f non nuls de S qui ne vérifient pas $P(f)$. S'il n'est pas vide il a un plus petit élément f_0. L'ensemble des $f' \neq 0$ vérifiant $\exp f' < \exp f$ n'est pas vide, puisqu'il contient 1, ce qui donne une contradiction. □

Nous allons voir que ces ordres ont des propriétés spécifiques.

Proposition 2.3.4. *Soient $2 \leqslant n' \leqslant n$ et f un polynôme non nul.*
i) Considérons $S' = k[X_{n'}, \ldots, X_n]$ comme sous-anneau de S. Si $in_{lex}\, f$ appartient à S', alors f appartient à S'.
ii) Supposons f homogène. Si $in_{revlex}\, f$ appartient à l'idéal $(X_{n'}, \ldots, X_n)$, alors f appartient à $(X_{n'}, \ldots, X_n)$.

Démonstration. i) Tout monôme faisant intervenir l'une des variables $X_1, \ldots, X_{n'-1}$ est plus grand pour l'ordre lexicographique que tout monôme de S', d'où le résultat.
ii) On peut écrire de manière unique $f = f_1 + f_2$ où f_1 est dans l'idéal $(X_{n'}, \ldots, X_n)$ et f_2 appartient à $k[X_1, \ldots, X_{n'-1}]$. De plus, f appartient à $(X_{n'}, \ldots, X_n)$ si et seulement si f_2 est nul.
Soit m un monôme de $k[X_1, \ldots, X_{n'-1}]$ de degré d, m' un monôme de degré $d - 1$ et $i \in [n', n]$ un entier. Alors pour l'ordre lexicographique inverse on a $m > m'X_i$. Donc tout terme non nul de f_2 est plus grand que tout terme non nul de f_1. Si $\text{in}_{revlex}\, f$ appartient à $(X_{n'}, \ldots, X_n)$, f_2 ne peut avoir de terme non nul.

□

La notion de terme initial, comme celle de degré, se comporte bien vis-à-vis du produit, moins bien vis-à-vis de la somme.

Proposition 2.3.5. *Soient f et g deux polynômes non nuls, et un ordre monomial sur S.*
i) On a $in\, fg = in\, f\, in\, g$, $exp\ fg = exp f + exp\, g$.
ii) Si $f + g \neq 0$, on a $exp(f + g) \leqslant \sup(exp\, f, exp\, g)$ avec égalité si et seulement si $in\, f + in\, g \neq 0$, en particulier égalité si $exp\, f \neq exp\, g$.

Démonstration. On écrit $f = \text{in}\, f + f'$, $g = \text{in}\, g + g'$ et tout terme non nul de f' (resp.g') est $< \text{in}\, f$ (resp. $< \text{in}\, g$). On a :

i) $fg = \operatorname{in} f \operatorname{in} g + f' \operatorname{in} g + g' \operatorname{in} f + f'g'$ et le plus grand terme non nul est $\operatorname{in} f \operatorname{in} g$.
ii) $f + g = \operatorname{in} f + \operatorname{in} g + f' + g'$. Si $\operatorname{in} f + \operatorname{in} g \neq 0$, le plus grand monôme qui apparaît dans $f + g$ est le sup des monômes associés aux termes $\operatorname{in} f$ et $\operatorname{in} g$ et on a $\exp(f + g) = \sup(\exp f, \exp g)$.
Si $\operatorname{in} f + \operatorname{in} g = 0$, le plus grand monôme qui apparaît dans $f + g$ est un monôme de f' ou g', donc on a $\exp(f + g) < \sup(\exp f, \exp g)$.

□

Remarque 2.3.6. Cela n'a pas de sens d'écrire $\operatorname{in}(f + g) = \sup(\operatorname{in} f, \operatorname{in} g)$ dans le cas où $\operatorname{in} f + \operatorname{in} g \neq 0$ puisqu'on a vu que le sup n'existe pas toujours. Supposons en effet qu'on ait $\operatorname{in} f = \lambda m$ et $\operatorname{in} g = \mu m$ avec $\lambda + \mu \neq 0$. On a alors $\operatorname{in}(f + g) = (\lambda + \mu)m$.

Corollaire 2.3.7. *Soient $f_1, \ldots, f_r$ des polynômes non nuls. On a $\exp(\sum f_i) \leqslant \sup \exp f_i$. De plus, si $\sum f_i = 0$ ou si $\sum f_i \neq 0$ et $\exp(\sum f_i) < \sup \exp f_i$, il existe deux indices $i \neq j$ tels qu'on ait $\exp f_i = \exp f_j$.*

Définition 2.3.8. Soit I un idéal non nul. L'*idéal initial* de I, noté $\operatorname{in} I$, est l'idéal engendré par les termes initiaux des éléments non nuls de I.

Remarque 2.3.9. Tout monôme de $\operatorname{in} I$ est divisible par un terme $\operatorname{in} f$ où $f \in I$, donc est lui-même de la forme $\operatorname{in} f'$ où $f' \in I$. L'ensemble des monômes de $\operatorname{in} I$ est donc l'ensemble des termes initiaux des éléments non nuls de I.

Proposition 2.3.10. *Soient I et I' deux idéaux et un ordre monomial fixé sur S. On a les propriétés suivantes :*
– *Si I est monomial, $I = \operatorname{in} I$.*
– *Si $I' \subseteq I$ et $\operatorname{in} I = \operatorname{in} I'$, alors $I = I'$.*

Démonstration. i) Si I est monomial, $I = (m_1, \ldots, m_r)$ où les m_i sont des monômes. Puisque $\operatorname{in} m_i = m_i$, I est contenu dans $\operatorname{in} I$. De plus, pour tout f non nul appartenant à I, tous ses termes non nuls appartiennent à I, en particulier $\operatorname{in} f$ appartient à I, donc $\operatorname{in} I$ est contenu dans I.
ii) Si $I \neq I'$, on considère l'ensemble $\mathcal{M}$ des monômes $\operatorname{in} f$ pour $f \in I$ et $f \notin I'$. D'après 2.2.7, il a un plus petit élément $\operatorname{in} f_0$ qui appartient à $\operatorname{in} I = \operatorname{in} I'$. Autrement dit, il existe g dans I' tel qu'on ait $\operatorname{in} f_0 = \operatorname{in} g$. En utilisant 2.3.5, on en déduit qu'on a $\operatorname{in}(f_0 - g) < \operatorname{in} f$. D'autre part, $f_0 - g$ appartient à I, donc $\operatorname{in}(f_0 - g)$ appartient à $\operatorname{in} I$, et à cause de la minimalité de $\operatorname{in} f_0$, $(f_0 - g)$ appartient à I', d'où une contradiction.

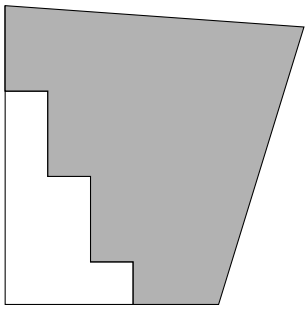
□

Notation 2.3.11. On note $\exp I$ l'ensemble des exposants des éléments non nuls de I.
Cette notation coïncide avec 1.1.9 lorsque l'idéal est monomial, et on a $\exp I = \exp \operatorname{in} I$.

Exemple 2.3.12. Supposons $n = 2$ et $I = (X_1^3, X_1^2X_2 - X_2^3)$ et choisissons l'ordre lexicographique. On a :

$$\operatorname{in} X_1^3 = X_1^3 \quad \operatorname{in}(X_1^2X_2 - X_2^3) = X_1^2X_2.$$

De plus, $X_1^3X_2 - X_1(X_1^2X_2 - X_2^3) = X_1X_2^3 \in I$, et $\operatorname{in} X_1X_2^3 = X_1X_2^3$. L'idéal $\operatorname{in} I$ contient donc X_1^3, $X_1^2X_2$ et $X_1X_2^3$. En fait on verra plus loin (cf. 4.2.9) qu'on a $\operatorname{in} I = (X_1^3, X_1^2X_2, X_1X_2^3, X_2^5)$ et que $\exp I$ est le domaine grisé suivant de $\mathbb{N}^2$:



Remarque 2.3.13. On a vu sur cet exemple qu'il ne suffit pas de connaître des générateurs de I pour déterminer $\operatorname{in} I$. Nous verrons au chapitre 4 comment on résoud ce problème.

Proposition 2.3.14. *Soit I un idéal homogène de S. L'idéal initial de I est engendré par les termes initiaux des polynômes homogènes de I.*

Démonstration. Soit I' l'idéal engendré par les termes initiaux des polynômes homogènes de I. On a bien sûr $I' \subseteq \operatorname{in} I$.
Inversement soit f un élément non nul de I, et $f = f_d + f_{d-1} + \cdots + f_0$ sa décomposition en composantes homogènes. Puisque I est homogène, toutes ces composantes appartiennent à I. De plus, pour $i \neq j$, les termes non nuls de f_i et f_j sont distincts, et en particulier les termes initiaux s'ils existent $\operatorname{in} f_i$ et $\operatorname{in} f_j$ sont distincts, donc il existe i tel que $\operatorname{in} f = \operatorname{in} f_i \in I'$. □

2.4 Polynômes symétriques

Nous allons donner une première application des ordres monomiaux, qui est une preuve assez simple du théorème des fonctions symétriques.
On rappelle que le groupe symétrique d'ordre n, noté $\mathfrak{S}_n$, est le groupe des permutations d'un ensemble fini à n éléments. Il agit sur $S = k[X_1, \ldots, X_n]$ de la manière suivante : soient $f \in S$ et $\sigma \in \mathfrak{S}_n$, on pose $f^\sigma = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

Définition 2.4.1. On polynôme f est symétrique s'il est invariant sous l'action de $\mathfrak{S}_n$ c'est-à-dire si on a $f^\sigma = f$ pour tout $\sigma \in \mathfrak{S}_n$.
On note $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ l'ensemble des polynômes symétriques.

Exemple 2.4.2. Pour $k \in [1, n]$, on définit des polynômes symétriques particuliers Σ_k qui sont les fonctions symétriques élémentaires en $X_1, \ldots, X_n$, par l'égalité de polynômes de $k[X, X_1, \ldots, X_n]$:

$$\prod_{i=1}^{n}(X + X_i) = X^n + \sum_{k=1}^{n} \Sigma_k X^{n-k}$$

Par exemple, pour $n = 3$ les trois fonctions symétriques élémentaires sont :

$$\Sigma_1 = X_1 + X_2 + X_3 \quad \Sigma_2 = X_1X_2 + X_2X_3 + X_3X_1 \quad \Sigma_3 = X_1X_2X_3.$$

Théorème 2.4.3. *L'homomorphisme de k-algèbres de $k[T_1, \ldots, T_n]$ dans S qui à T_k associe Σ_k est un isomorphisme sur $k[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, autrement dit, tout polynôme symétrique f s'écrit de manière unique sous la forme $g(\Sigma_1, \ldots, \Sigma_n)$.*

Démonstration. Fixons l'ordre lexicographique homogène sur S. On a alors

$$\operatorname{in} \Sigma_k = X_1 \ldots X_k$$

donc

$$\operatorname{in} \Sigma_1^{j_1} \ldots \Sigma_n^{j_n} = X_1^{j_1+\cdots+j_n} X_2^{j_2+\cdots+j_n} \ldots X_n^{j_n}.$$

Définissons une application ϕ de $\mathbb{N}^n$ dans lui-même par

$$\phi(j_1, \ldots, j_n) = (j_1 + \cdots + j_n, j_2 + \cdots + j_n, \ldots, j_n)$$

Elle est injective et son image est formée des suites décroissantes $(i_1, \ldots, i_n)$. On en déduit deux propriétés :

1) pour $j = (j_1, \ldots, j_n) \neq j' = (j'_1, \ldots, j'_n)$, $\Sigma_1^{j_1} \ldots \Sigma_n^{j_n}$ et $\Sigma_1^{'j_1} \ldots \Sigma_n^{'j_n}$ ont des exposants différents.
2) pour toute suite décroissante $(i_1, \ldots, i_n)$, $X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ est le terme initial de $\Sigma_1^{j_1} \ldots \Sigma_n^{j_n}$, avec $\phi(j_1, \ldots, j_n) = (i_1, \ldots, i_n)$.

Démontrons maintenant le théorème. Il est clair qu'on a défini un homomorphisme de k-algèbres.

Soit alors $g \in k[T_1, \ldots, T_n]$ tel que $g(\Sigma_1, \ldots, \Sigma_n) = 0$. On peut écrire $g = \sum \lambda_j T^j$, où j est un multi-indice, et on a $\sum \lambda_j \Sigma_1^{j_1} \ldots \Sigma_n^{j_n} = 0$. On en déduit, d'après 2.3.7, qu'il existe j et j' avec $j \neq j'$ tels que les exposants de $\Sigma_1^{j_1} \ldots \Sigma_n^{j_n}$ et $\Sigma_1^{'j_1} \ldots \Sigma_n^{'j_n}$ soient égaux, ce qui donne une contradiction.

Soient f un polynôme symétrique non nul et $\operatorname{in} f = \lambda X_1^{i_1} \ldots X_n^{i_n}$. Supposons qu'il existe k tel que $i_{k+1} > i_k$. Puisque f est symétrique, il contient également le terme obtenu en échangeant k et $k + 1$, qui est :

$$\lambda X_1^{i_1} \ldots X_{k-1}^{i_{k-1}} X_k^{i_{k+1}} X_{k+1}^{i_k} \ldots X_n^{i_n}$$

Donc la suite $(i_1, \ldots, i_n)$ est décroissante et il existe un élément g de $k[T_1, \ldots, T_n]$ tel que $\operatorname{in}(g(\Sigma_1, \ldots, \Sigma_n)) = \operatorname{in} f$. Si le polynôme symétrique $f' = f - g(\Sigma_1, \ldots, \Sigma_n)$ n'est pas nul, on a $\operatorname{in} f' < \operatorname{in} f$. On recommence, et le processus s'arrête car pour l'ordre choisi (hlex) l'ensemble des monômes inférieurs à un monôme donné est fini. □

Remarque 2.4.4. Le procédé de démonstration utilisé ci-dessus est différent du procédé de récurrence défini en 2.3.3.

Chapitre 3

Algorithme de division euclidienne

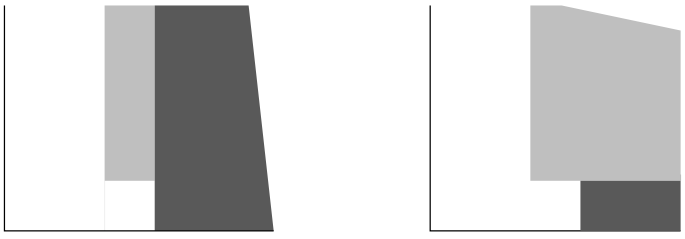
La division d'un polynôme par une suite de polynômes que nous allons donner dans ce court chapitre est due à Hironaka. Elle est plus précise que les définitions rencontrées le plus souvent dans la littérature, et a un avantage, l'unicité du résultat, qui se révèlera très utile dans les démonstrations.
On se donne un ordre monomial sur S.

3.1 Partition de $\mathbb{N}^n$ associée à une suite de polynômes

Notation 3.1.1. A une suite $\{f_1, \ldots, f_s\}$ de polynômes non nuls de S on associe une partition de l'ensemble $\mathbb{N}^n$ des exposants :
– $\Delta_1 = \exp f_1 + \mathbb{N}^n$
– pour $1 < i \leqslant s$, $\Delta_i = (\exp f_i + \mathbb{N}^n) \setminus \cup_{j<i} \Delta_j$
– $\bar{\Delta} = \mathbb{N}^n \setminus \cup_{i=1}^{s} \Delta_i$.

Remarque 3.1.2. Δ_1 correspond aux monômes divisibles par in f_1, Δ_i correspond aux monômes qui sont divisibles par in f_i, mais qui ne sont divisibles par aucun des in f_j pour $j < i$, et $\bar{\Delta}$ correspond aux monômes qui ne sont divisibles par aucun des in f_i.

Exemples 3.1.3. On choisit $n = 2$, $s = 2$, $f_1 = X_1^3$, $f_2 = X_1^2 X_2 - X_2^3$ et l'ordre lexicographique.
Alors $\exp f_1 = (3, 0)$ et $\exp f_2 = (2, 1)$. La partition de $\mathbb{N}^2$ en trois sous-ensembles Δ_1, Δ_2 et $\bar{\Delta}$ est représentée par le graphique de gauche suivant ($\bar{\Delta}$ est blanc, Δ_2 est gris clair et Δ_1 gris foncé) :



Le graphique de droite représente la partition de $\mathbb{N}^2$ en trois sous-ensembles Δ_1, Δ_2 et $\bar{\Delta}$ quand on échange les polynômes : $f_1 = X_1^2X_2 - X_2^3$, $f_2 = X_1^3$.

3.2 Division euclidienne par une suite de polynômes

Théorème 3.2.1. *Soit f un élément de S. Avec les notations ci-dessus, il existe $h_1, \ldots, h_s, h$ uniques tels qu'on ait :*
i) $f = h_1f_1 + \cdots + h_sf_s + h$,
ii) tous les termes non nuls de $h_i \operatorname{in} f_i$ ont un exposant dans Δ_i,
iii) tous les termes non nuls de h ont un exposant dans $\bar{\Delta}$.
De plus, si f et h sont non nuls, on a $\exp h \leqslant \exp f$, et si f, f_i et h_i sont non nuls, on a $\exp f_ih_i \leqslant \exp f$.

Remarques 3.2.2.
1. La condition ii) signifie que les monômes de $h_i \operatorname{in} f_i$ ne sont divisibles par aucun des $\operatorname{in} f_j$ pour $j < i$. Elle est vide pour $i = 1$. La condition iii) signifie que les monômes de h ne sont divisibles par aucun des $\operatorname{in} f_i$.
2. Pour $n = s = 1$, la partition de $\mathbb{N}$ est formée de deux sous-ensembles, Δ_1 est l'intervalle $[d_1, +\infty]$, où d_1 est le degré de f_1, et $\bar{\Delta}$ l'intervalle $[0, d_1[$. La condition ii) est vide et la condition iii) signifie que le degré de h est $< d_1$. On retrouve la division euclidienne.

Démonstration. Soit f un élément de S. Les propriétés sont évidemment vérifiées pour $f = 0$. On peut dons supposer $f \neq 0$. Nous allons montrer par récurrence (2.3.3) l'existence de $h_1, \ldots, h_s, h$ vérifiant toutes les propriétés de l'énoncé.
Si $f = 1$ et si pour tout i, $f_i \neq 1$, on vérifie que $h_i = 0$ et $h = 1$ conviennent.
Si $f = 1$ et s'il existe i_0 tel que $f_{i_0} = 1$ et $f_i \neq 1$ pour tout $i < i_0$, on vérifie que $h_{i_0} = 1$, $h_i = 0$ pour $i \neq i_0$ et $h = 0$ conviennent.
Supposons $f \neq 0$, et les propriétés vraies pour tout $f' \in S$ non nul avec $\exp f' < \exp f$.
Posons $\operatorname{in} f = \lambda X^\alpha$ où $\alpha \in \mathbb{N}^n$. Deux cas sont possibles :
– si $\alpha \in \bar{\Delta}$ posons $f' = f - \operatorname{in} f$. Si $f' \neq 0$, on a $\exp f' < \exp f$ donc il existe $h_1, \ldots, h_s, h$ vérifiant les propriétés i), ii) iii) et

$$f' = h_1f_1 + \cdots + h_sf_s + h.$$

On a alors

$$f = h_1f_1 + \cdots + h_sf_s + (h + \operatorname{in} f)$$

et il faut vérifier que les monômes de $h + \operatorname{in} f$ sont dans $\bar{\Delta}$, ce qui est vrai pour les monômes de h et pour $\operatorname{in} f$.
De plus, si $h + \operatorname{in} f \neq 0$, $\exp(h + \operatorname{in} f)$ est soit l'exposant d'un terme non nul de h, soit $\exp f$. Dans le premier cas, par l'hypothèse de récurrence, il est $\leqslant \exp f'$, donc dans tous les cas il est $\leqslant \exp f$ (il peut lui être égal, par exemple si $h = 0$).
Si $h_i \neq 0$, par l'hypothèse de récurrence, on a $\exp h_if_i \leqslant \exp f' < \exp f$.
Si $f' = 0$, on a $f = \operatorname{in} f$, qui est un monôme de $\bar{\Delta}$ et les conditions supplémentaires sont encore vérifiées..

– si il existe i tel que $\alpha \in \Delta_i$, on a $\alpha = \exp f_i + \alpha'$, où $\alpha' \in \mathbb{N}^n$. Posons

$$\text{in}\, f_i = \mu X^\beta \quad \text{et} \quad f' = f - \frac{\lambda}{\mu} X^{\alpha'} f_i.$$

Si $f' \neq 0$, puisque $\text{in}\, f = \frac{\lambda}{\mu} X^{\alpha'} \text{in}\, f_i$, on a $\exp f' < \exp f$ donc il existe $h_1, \ldots, h_s, h$ vérifiant les propriétés i), ii) iii) et

$$f' = h_1 f_1 + \cdots + h_s f_s + h.$$

On a alors

$$f = h_1 f_1 + \cdots + (h_i + \frac{\lambda}{\mu} X^{\alpha'}) f_i + \cdots + h_s f_s + h$$

et il suffit de vérifier que les monômes de $(h_i + \frac{\lambda}{\mu} X^{\alpha'})\text{in}\, f_i$ sont dans Δ_i, ce qui est vrai pour les monômes de $h_i \text{in}\, f_i$ et pour $X^{\alpha'} \text{in}\, f_i$.
De plus, si $h \neq 0$, par l'hypothèse de récurrence l'exposant d'un terme non nul de h est $\leqslant \exp f' < \exp f$.
Si $h_i + \frac{\lambda}{\mu} X^{\alpha'} \neq 0$, son exposant est égal soit à $\exp h_i f_i$, soit à $\exp f$, donc il est toujours $\leqslant \exp f$.
Si $f' = 0$, on a $f = \frac{\lambda}{\mu} X^{\alpha'} f_i$, qui donne encore le résultat.

Montrons l'unicité. Supposons qu'on ait deux écritures, donc qu'on ait

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

où $h_1, \ldots, h_s, h$ d'une part, $h'_1, \ldots, h'_s, h'$ d'autre part, vérifient les propriétés i), ii) iii).
Si $(h_i - h'_i) \neq 0$, $\exp (h_i - h'_i) f_i = \exp ((h_i - h'_i)\text{in}\, f_i)$. Cet exposant est celui d'un terme non nul de $h_i \text{in}\, f_i$ ou de $h'_i \text{in}\, f_i$ et est dans Δ_i. En particulier pour $i \neq j$, $(h_i - h'_i) f_i$ et $(h_j - h'_j) f_j$ ont des exposants distincts, donc on a :

$$\exp \sum_{i=1}^{s} (h_i - h'_i) f_i = \sup \exp (h_i - h'_i) f_i \in \bigcup_{i=1}^{s} \Delta_i$$

si les $h_i - h'_i$ ne sont pas tous nuls.
D'autre part, si $h - h'$ n'est pas nul, son exposant est celui d'un terme de h ou de h', donc est dans $\bar{\Delta}$.
On en conclut que $h = h'$ et pour tout i, $h_i = h'_i$.

□

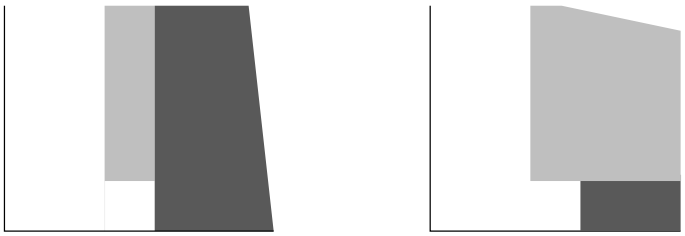
Remarques 3.2.3.

1. On a donné l'algorithme en même temps que la preuve de l'existence.
2. Avec les notations de l'énoncé on remarque, comme dans la preuve de l'unicité, que si $h_i \neq 0$, l'exposant de $h_i f_i$ est dans Δ_i, donc les exposants des $h_i f_i$ sont 2 à 2 distincts. On a donc, si l'un au moins des h_i est non nul :

$$\exp \sum_{i=1}^{s} h_i f_i = \sup \exp h_i f_i \in \bigcup_{i=1}^{s} \Delta_i.$$

L'exemple qui suit montre que l'ordre des polynômes $f_1, \ldots, f_s$ est important. On fait la division par une *suite* et non un *ensemble* de polynômes.

Exemples 3.2.4. On choisit $n = 2$, $s = 2$, $f = X_1^3X_2$, $f_1 = X_1^3$, $f_2 = X_1^2X_2 - X_2^3$ et l'ordre lexicographique. On a vu que la partition associée à la suite f_1, f_2 est représentée à gauche sur le graphique suivant :



On a $\exp f = (3, 1) \in \Delta_1$. Suivant l'algorithme, on pose $f' = f - X_2f_1 = 0$ et le résultat de la division est $f = X_2f_1$.
On choisit maintenant $n = 2$, $s = 2$, $f = X_1^3X_2$, l'ordre lexicographique et on échange les polynômes : $f_1 = X_1^2X_2 - X_2^3$, $f_2 = X_1^3$. La partition associée à la suite f_1, f_2 est alors représentée à droite sur le graphique précédent.
On a $\exp f = (3, 1) \in \Delta_1$. Suivant l'algorithme, on pose $f' = f - X_1f_1 = X_1X_2^3$.
On a $\exp f' = (1, 3) \in \bar{\Delta}$. On pose $f'' = f' - \operatorname{in} f' = 0$ et le résultat de la division est $f = X_1f_1 + X_1X_2^3$.

Définition 3.2.5. Soient $\{f_1, \ldots, f_s\}$ une suite de polynômes non nuls et f un polynôme. Avec les notations de l'énoncé 3.2.1, on a $f = h_1f_1 + \cdots + h_sf_s + h$ et h est appelé le *reste* de la division par la suite $\{f_1, \ldots, f_s\}$ et noté $f\,\mathcal{R}\{f_1, \ldots, f_s\}$. Ses propriétés sont détaillées dans la proposition suivante :

Proposition 3.2.6. *Soient $\{f_1, \ldots, f_s\}$ une suite de polynômes non nuls, f et g deux polynômes et λ un scalaire. Alors on a :*
i) $(f + g)\,\mathcal{R}\{f_1, \ldots, f_s\} = f\,\mathcal{R}\{f_1, \ldots, f_s\} + g\,\mathcal{R}\{f_1, \ldots, f_s\}$.
ii) $(\lambda f)\,\mathcal{R}\{f_1, \ldots, f_s\} = \lambda(f\,\mathcal{R}\{f_1, \ldots, f_s\})$.
iii) Si $f\,\mathcal{R}\{f_1, \ldots, f_s\} = 0$, alors f appartient à l'idéal engendré par $f_1, \ldots, f_s$.

Démonstration. Les propriétés i) et ii) sont des conséquences de l'unicité du reste, iii) est immédiate. □

Remarque 3.2.7. On voit sur l'exemple 3.2.4 que la réciproque de iii) est fausse : $f = X_1^3X_2$ appartient à l'idéal engendré par $X_1^2X_2 - X_2^3$ et X_1^3 mais le reste de la division de f par la suite (dans cet ordre) $X_1^2X_2 - X_2^3$ est égal à $X_1X_2^3$.

Remarque 3.2.8. Soient $\{f_1, \ldots, f_s\}$ une suite de polynômes non nuls homogènes et f un polynôme homogène. Alors pour des raisons d'unicité les polynômes h_1,..., h_s, h qui interviennent dans le résultat de la division de f par la suite $\{f_1, \ldots, f_s\}$:

$$f = h_1f_1 + \cdots + h_sf_s + h$$

sont tous homogènes.

Chapitre 4

Bases de Gröbner d'un idéal

Dans tout ce chapitre, un ordre monomial est donné sur S.

4.1 Définition des bases de Gröbner

Définition 4.1.1. Soit I un idéal non nul de S et $(f_1, \ldots, f_s)$ un ensemble de polynômes non nuls. On dit que $(f_1, \ldots, f_s)$ est une *base standard* ou une *base de Gröbner* de I si c'est un système de générateurs de I et si $(\operatorname{in} f_1, \ldots, \operatorname{in} f_s)$ est un système de générateurs de $\operatorname{in} I$.
Elle est *minimale* si elle est de cardinal minimum.

Remarque 4.1.2. Il n'y a pas d'ordre sur les polynômes $f_1, \ldots, f_s$. C'est un ensemble et non une suite.

On peut remplacer dans la définition "système de générateurs de I" par "éléments de I" :

Lemme 4.1.3. *Soient I un idéal non nul de S et $(f_1, \ldots, f_s)$ un ensemble de polynômes non nuls de I tels que $(\operatorname{in} f_1, \ldots, \operatorname{in} f_s)$ soit un système de générateurs de $\operatorname{in} I$. Alors ils forment une base de Gröbner de I.*

Démonstration. En effet, soit I' l'idéal engendré par $f_1, \ldots, f_s$. On a

$$I' \subseteq I \quad (\operatorname{in} f_1, \cdots, \operatorname{in} f_s) \subseteq \operatorname{in} I' \subseteq \operatorname{in} I$$

donc $\operatorname{in} I' = \operatorname{in} I$. D'après 2.3.10, on a $I = I'$. □

Exemple 4.1.4. Supposons $n = 2$ et $I = (X_1^3, X_1^2X_2 - X_2^3)$ et choisissons l'ordre lexicographique. On a vu que I contient le polynôme $X_1X_2^3$. Or on a :

$$\operatorname{in} X_1^3 = X_1^3 \quad , \quad \operatorname{in}(X_1^2X_2 - X_2^3) = X_1^2X_2 \quad , \quad \operatorname{in} X_1^3X_2 = X_1X_2^3$$

donc $\operatorname{in} I$ n'est pas égal à $(\operatorname{in} X_1^3, \operatorname{in}(X_1^2X_2 - X_2^3))$. Le système de générateurs donné $(X_1^3, X_1^2X_2 - X_2^3)$ de I n'est pas une base de Gröbner de I.

Proposition 4.1.5. *Tout idéal de S possède une base de Gröbner.*

Démonstration. L'ensemble des $\operatorname{in} f$ pour $f \in I$ est un système de générateurs de $\operatorname{in} I$. On peut donc en extraire un sous-ensemble fini de générateurs $(\operatorname{in} f_1, \ldots, \operatorname{in} f_s)$ et d'après 4.1.3, $(f_1, \ldots, f_s)$ est une base de Gröbner de I.

□

Remarque 4.1.6. D'après **??**, $(f_1, \ldots, f_s)$ est une base de Gröbner de I si et seulement si l'ensemble fini $\{\exp f_1, \ldots, \exp f_s\}$ est une frontière de l'ensemble $\exp I$, c'est-à-dire que $\exp I$ est réunion des sous-ensembles $\exp f_i + \mathbb{N}^n$.

Avant de voir comment on construit une base de Gröbner, nous allons en donner des propriétés.

Proposition 4.1.7. *Soit I un idéal non nul de S.*
i) De toute base de Gröbner de I on peut extraire une base minimale, qui correspond à un escalier de $\exp I$.
ii) Deux bases de Gröbner minimales de I ont même cardinal.
iii) Soient $(f_1, \ldots, f_s)$ et $(g_1, \ldots, g_s)$ deux bases de Gröbner minimales de I. Quitte à renuméroter, on peut supposer qu'on a $\exp f_i = \exp g_i$ pour tout $i \in [1, s]$.

Démonstration. Une base de Gröbner de I correspond à un système de générateurs monomiaux de $\operatorname{in} I$. Elle est minimale si et seulement si le système de générateurs l'est. D'où les propriétés pour les bases de Gröbner , sachant qu'elles sont vraies pour les générateurs monomiaux ([**?**]).

□

Proposition 4.1.8. *Soient I un idéal et $(f_1, \ldots, f_s)$ et $(g_1, \ldots, g_t)$ deux bases de Gröbner de I. Pour tout $f \in S$, le reste de la division de f par la suite $\{f_1, \ldots, f_s\}$ est égal au reste de la division de f par la suite $\{g_1, \cdots, g_t\}$.*

Démonstration. On note $\Delta_1, \ldots, \Delta_s, \bar{\Delta}$ et $\Delta'_1, \ldots, \Delta'_s, \bar{\Delta}'$ les éléments des partitions de $\mathbb{N}^n$ correspondant aux deux suites. Puisque ce sont des bases de Gröbner, on a $\exp I = \cup_{i=1}^{s} \Delta_i = \cup_{j=1}^{t} \Delta'_j$, donc les complémentaires $\bar{\Delta}$ et $\bar{\Delta}'$ sont égaux.
Ecrivons le résultat des divisions par les deux suites :

$$f = \sum_{i=1}^{s} h_i f_i + h = \sum_{j=1}^{t} h'_j g_j + h'$$

$$h - h' = \sum_{j=1}^{t} h'_j g_j - \sum_{i=1}^{s} h_i f_i \in I.$$

Si $h - h'$ n'est pas nul, son exposant est l'exposant d'un terme non nul de h ou de h', donc il est à la fois dans $\exp I$ et dans $\bar{\Delta}$ d'où une contradiction.

□

Définition 4.1.9. Soient I un idéal et $(f_1, \ldots, f_s)$ une base de Gröbner de I. Le reste de la division de f par la suite $\{f_1, \ldots, f_s\}$, qui ne dépend pas de la base (et donc pas de l'ordre) est appelé *reste de la division de f par I* et on le note $f\mathcal{R}I$.

Remarque 4.1.10. Aucun monôme de $f\mathcal{R}I$ n'est dans $\operatorname{in} I$.

Corollaire 4.1.11. *Soient I un idéal et f un élément de S. Alors f appartient à I si et seulement si $f\mathcal{R}I = 0$.*

Démonstration. Choisissons une base de Gröbner $(f_1, \ldots, f_s)$ de I et effectuons la division. On a $f = \sum_{i=1}^{s} h_i f_i + f\mathcal{R}I$.
Si $f \in I$, $f - \sum_{i=1}^{s} h_i f_i = f\mathcal{R}I \in I$ et si ce reste est non nul son terme initial est dans $\operatorname{in} I$ ce qui contredit 4.1.10. □

Nous pouvons maintenant généraliser le résultat que nous avons vu pour les idéaux monomiaux en 1.2.5 et donner une base de l'anneau quotient :

Corollaire 4.1.12. *Soit I un idéal de S. L'ensemble $\mathcal{M}$ des monômes qui ne sont pas dans $\operatorname{in} I$ (plus précisément leurs images dans S/I) forment une base de S/I.*

Démonstration. Montrons que leurs images dans S/I sont indépendantes.
Soient $m_1, \ldots, m_r$ des monômes deux à deux distincts non dans $\operatorname{in} I$ et supposons qu'il existe des scalaires non nuls $\lambda_1, \ldots, \lambda_r$ tels que $\sum \lambda_i m_i$ soit nul dans S/I, autrement dit tels que $\sum \lambda_i m_i$ appartienne à I. Son terme initial est un multiple de l'un des m_i et est dans $\operatorname{in} I$, d'où une contradiction.
Il reste à montrer qu'ils engendrent S/I : soit $f \in S$. Alors $f - f\mathcal{R}I \in I$ et f et $f\mathcal{R}I$ ont la même image dans R/I. D'où le résultat puisque les monômes de $f\mathcal{R}I$ ne sont pas dans $\operatorname{in} I$. □

4.2 Caractérisation et construction des bases de Gröbner

Nous allons maintenant donner une caractérisation des bases de Gröbner, puis un procédé de construction qui en résulte.

Proposition 4.2.1. *Soient I un idéal non nul de S et $\{f_1, \ldots, f_s\}$ une suite de polynômes non nuls de I . Alors l'ensemble $(f_1, \ldots, f_s)$ est une base de Gröbner de I si et seulement si pour tout $f \in I$, le reste $f\mathcal{R}\{f_1, \ldots, f_s\}$ est nul.*

Démonstration. Soit f un élément de I. On a vu en 4.1.11 que si $(f_1, \ldots, f_s)$ est une base de Gröbner de I, $f\mathcal{R}\{f_1, \ldots, f_s\} = f\mathcal{R}I = 0$.
Inversement, supposons que $\forall f \in I$, $f\mathcal{R}\{f_1, \ldots, f_s\} = 0$ et montrons qu'on a $\exp I = \bigcup_i \exp f_i + \mathbb{N}^n$.
Soit $\Delta_1, \ldots, \Delta_s, \bar{\Delta}$ la partition de $\mathbb{N}^n$ associée à la suite. On a $\bigcup_i \exp f_i + \mathbb{N}^n = \bigcup_i \Delta_i$.
Ecrivons le résultat de la division de f par la suite $\{f_1, \ldots, f_s\}$:

$$f = \sum_i h_i f_i + f\mathcal{R}\{f_1, \ldots, f_s\} = \sum_i h_i f_i$$

et on a vu en 3.2.3.2 que l'exposant $\exp \sum_i h_i f_i = \exp f$ appartient à la réunion des Δ_i. Donc $\exp I = \bigcup_i \Delta_i$.

□

Ce critère n'est pas encore satisfaisant puisqu'il demande une infinité de vérifications. Nous allons voir qu'on peut se limiter à un nombre fini. Pour celà, nous devons d'abord introduire une nouvelle notion.

Définition 4.2.2. Soient f et g deux polynômes non nuls. Si on a :

$$\operatorname{in} f = \lambda X^\alpha \quad \operatorname{in} g = \mu X^\beta \quad \gamma = \alpha \vee \beta$$

(qui est le sup de α et β au sens de l'ordre produit sur $\mathbb{N}^n$), on définit le *S-polynôme de f et g* noté $S(f,g)$ par :

$$S(f,g) = \mu X^{\gamma-\alpha} f - \lambda X^{\gamma-\beta} g.$$

Remarque 4.2.3. En un certain sens, c'est la "plus petite combinaison" de f et g qui permet de simplifier les termes initiaux. On a $\operatorname{in} \mu X^{\gamma-\alpha} f = \operatorname{in} \lambda X^{\gamma-\beta} g$, et si $S(f,g)$ n'est pas nul, $\exp S(f,g) < \gamma = \exp X^{\gamma-\alpha} f = \exp X^{\gamma-\beta} g$.

Exemple 4.2.4. On choisit $n = 2$, $f = X_1^3$, $g = X_1^2 X_2 - X_2^3$ et l'ordre lexicographique. On a

$$S(f,g) = X_2 f - X_1 g = X_1 X_2^3.$$

Les propriétés du S-polynôme sont décrites dans la proposition suivante :

Proposition 4.2.5. *Soient f et g des polynômes, m un monôme, λ un scalaire, tous non nuls. On a les propriétés suivantes :*
i) si f et g sont des termes, $S(f,g) = 0$;
ii) $S(mf, mg) = mS(f,g)$, $S(\lambda f, g) = \lambda S(f,g)$;
iii) si $\exp f = \exp g$, $S(f,g)$ est une combinaison linéaire de f et g ; si de plus $S(f,g)$ n'est pas nul, on a $\exp S(f,g) < \exp f$.

Démonstration. ii) est une conséquence du fait que $\operatorname{in} mf = m \operatorname{in} f$, $\operatorname{in} mg = m \operatorname{in} g$ et $\sup(\alpha + \exp m, \beta + \exp m) = \sup(\alpha, \beta) + \exp m$.
Les autres propriétés sont immédiates. □

Le résultat suivant, qui justifie d'une certaine manière l'introduction des S-polynômes, est plus technique et sera utile dans la preuve du théorème :

Lemme 4.2.6. *Soient $f_1, \ldots, f_s$ des polynômes non nuls ayant tous le même exposant α et $\lambda_1, \ldots \lambda_s$ des scalaires non nuls. Si on a $\sum_i \lambda_i f_i = 0$ ou $\sum_i \lambda_i f_i \neq 0$ et $\exp \sum_i \lambda_i f_i < \alpha$, il existe des scalaires $\mu_{j,k}$, $j,k \in [1,s]$ tels qu'on ait :*

$$\sum_i \lambda_i f_i = \sum_{j,k} \mu_{j,k} S(f_j, f_k).$$

Démonstration. Posons in $f_i = a_i X^\alpha$ et $g_i = f_i/a_i$. Dans les deux cas, on a $\sum_i \lambda_i a_i = 0$.

$$\begin{aligned}\sum_i \lambda_i f_i &= \sum_i \lambda_i a_i g_i \\ &= \lambda_1 a_1 (g_1 - g_2) + (\lambda_1 a_1 + \lambda_2 a_2)(g_2 - g_3) + \cdots + (\lambda_1 a_1 + \cdots + \lambda_{s-1} a_{s-1})(g_{s-1} - g_s) \\ &= \frac{\lambda_1 a_1}{a_1 a_2} S(f_1, f_2) + \frac{\lambda_1 a_1 + \lambda_2 a_2}{a_2 a_3} S(f_2, f_3) + \cdots + \frac{\lambda_1 a_1 + \cdots + \lambda_{s-1} a_{s-1}}{a_{s-1} a_s} S(f_{s-1}, f_s)\end{aligned}$$

□

Théorème 4.2.7. *Soient I un idéal non nul de S et $\{f_1, \ldots, f_s\}$ une suite de polynômes non nuls de I qui forment un système de générateurs de I . Alors l'ensemble $(f_1, \ldots, f_s)$ est une base de Gröbner de I si et seulement si pour tous $i, j \in [1, s]$, $\operatorname{in} f_i$ et $\operatorname{in} f_j$ sont premiers entre eux ou le reste $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\}$ est nul.*

Démonstration. La condition est nécessaire : $S(f_i, f_j)$ appartient à l'idéal (f_i, f_j), donc à I, et puisque $(f_1, \ldots, f_s)$ est une base de Gröbner de I, $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\} = S(f_i, f_j)\mathcal{R}I = 0$ (4.1.11).
Avant de montrer que la condition est suffisante, nous avons besoin d'un lemme qui sera montré plus loin :

Lemme 4.2.8. *Soient $f_1, \ldots, f_s$ des polynômes non nuls tels que pour tous $i, j \in [1, s]$, $i \neq j$, $\operatorname{in} f_i$ et $\operatorname{in} f_j$ sont premiers entre eux, ou le reste $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\}$ est nul. Alors pour tous $i, j \in [1, s]$, $i \neq j$, il existe des polynômes $h_{i,j,k}$, $k \in [1, s]$, vérifiant $S(f_i, f_j) = \sum_k h_{i,j,k} f_k$ et si $h_{i,j,k} \neq 0$, $\exp h_{i,j,k} f_k < \exp f_i \vee \exp f_j$.*

Soit $f \in I$. Soit $\Delta_1, \ldots, \Delta_s, \bar{\Delta}$ la partition de $\mathbb{N}^n$ associée à la suite. Ecrivons le résultat de la division de f par la suite $\{f_1, \ldots, f_s\}$:

$$f = \sum_i h_i f_i + f\mathcal{R}\{f_1, \ldots, f_s\}.$$

Il faut montrer que $h = f\mathcal{R}\{f_1, \ldots, f_s\}$ est nul.
S'il ne l'est pas, tous ses monômes sont dans $\bar{\Delta}$. De plus, puisque $h = f - \sum_i h_i f_i$, $h \in I$. On peut donc écrire $h = \sum_i k_i f_i$ où les k_i ne sont pas nuls et supposer que dans cette écriture $\alpha = \sup(\exp k_i f_i)$ est minimum (puisqu'un sous-ensemble d'exposants a un élément minimum, cf. 2.2.7).
Par définition, α appartient à la réunion des $\exp f_i + \mathbb{N}^n$ qui est aussi la réunion des Δ_i. Puisque $\exp h$ appartient à $\bar{\Delta}$, l'inégalité $\exp h \leqslant \sup(\exp k_i f_i) = \alpha$ ne peut être une égalité. On a donc $\exp h < \alpha$.
Soit L l'ensemble des indices $i \in [1, s]$ vérifiant $\exp k_i f_i = \alpha$. Les termes d'exposant α des $k_i f_i$ s'annulent dans la somme, c'est-à-dire $\sum_{i \in L} \operatorname{in} k_i \operatorname{in} f_i = 0$.
Pour $i \in L$ posons :

$$\operatorname{in} f_i = a_i X^{\alpha_i}, \quad \operatorname{in} k_i = b_i X^{\alpha - \alpha_i}, \quad k_i = \operatorname{in} k_i + k_i' \text{ avec } \exp k_i' < \alpha - \alpha_i \text{ ou } k_i' = 0$$

$$h = \sum_{i \in L} \operatorname{in} k_i f_i + \sum_{i \in L} k_i' f_i + \sum_{i \notin L} k_i f_i$$

et les deux derniers termes de la somme ne contiennent pas de monômes d'exposant α. Donc l'exposant de la somme $\sum_{i\in L} \operatorname{in} k_i f_i$ est plus petit que α. On peut appliquer 4.2.6, et il existe des scalaires $\lambda_{i,j}$ tels qu'on ait :

$$\begin{aligned}\sum_{i\in L} \operatorname{in} k_i f_i &= \sum_{i,j\in L} \lambda_{i,j} S(\operatorname{in} k_i f_i, \operatorname{in} k_j f_j) \\ &= \sum_{i,j\in L} \lambda_{i,j} b_i b_j S(X^{\alpha-\alpha_i} f_i, X^{\alpha-\alpha_j} f_j)\end{aligned}$$

Calculons ce S-polynôme. On a :

$$S(f_i, f_j) = a_j X^{\gamma_{i,j}-\alpha_i} f_i - a_i X^{\gamma_{i,j}-\alpha_j} f_j$$

où $\gamma_{i,j} = \alpha_i \vee \alpha_j$ est le sup de α_i et α_j pour l'ordre produit de $\mathbb{N}^n$.

$$\begin{aligned}S(X^{\alpha-\alpha_i} f_i, X^{\alpha-\alpha_j} f_j) &= a_j X^{\alpha-\alpha_i} f_i - a_i X^{\alpha-\alpha_j} f_j \\ &= X^{\alpha-\gamma_{i,j}} S(f_i, f_j)\end{aligned}$$

D'après 4.2.8, il existe des polynômes $h_{i,j,k}$, $k \in [1, s]$, vérifiant $S(f_i, f_j) = \sum_k h_{i,j,k} f_k$ et si $h_{i,j,k} \neq 0$, $\exp h_{i,j,k} f_k < \gamma_{i,j}$.
On a donc

$$\begin{aligned}\sum_{i\in L} \operatorname{in} k_i f_i &= \sum_{i,j\in L} \lambda_{i,j} b_i b_j S(X^{\alpha-\alpha_i} f_i, X^{\alpha-\alpha_j} f_j) \\ &= \sum_{i,j\in L} \lambda_{i,j} b_i b_j X^{\alpha-\gamma_{i,j}} S(f_i, f_j) \\ &= \sum_{i,j\in L} \lambda_{i,j} b_i b_j X^{\alpha-\gamma_{i,j}} \sum_k h_{i,j,k} f_k \\ &= \sum_k f_k \sum_{i,j\in L} \lambda_{i,j} b_i b_j X^{\alpha-\gamma_{i,j}} h_{i,j,k} = \sum_k f_k g_k\end{aligned}$$

où on a $\exp f_k g_k = \exp f_k X^{\alpha-\gamma_{i,j}} h_{i,j,k} < \alpha$. On a donc

$$h = \sum_k f_k g_k + \sum_{i\in L} k'_i f_i + \sum_{i\notin L} k_i f_i = \sum_i K_i f_i$$

avec $K_i = g_i + k'_i$ si $i \in L$, $K_i = g_i + k_i$ si $i \notin L$. Alors on a $\sup(\exp K_i f_i) < \alpha$ d'où une contradiction et $h = 0$.

□

Démonstration. (du lemme) Ecrivons le résultat de la division de $S(f_i, f_j)$ par la suite $\{f_1, \ldots, f_s\}$:

$$S(f_i, f_j) = \sum_k h_{i,j,k} f_k + S(f_i, f_j) \mathcal{R}\{f_1, \ldots, f_s\}$$

et si $h_{i,j,k} \neq 0$, on sait que $\exp h_{i,j,k} f_k \leqslant \exp S(f_i, f_j) < \exp f_i \vee \exp f_j$.
Donc si le reste $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\}$ est nul, on a le résultat.

Si maintenant $\operatorname{in} f_i$ et $\operatorname{in} f_j$ sont premiers entre eux, $\exp f_i \vee \exp f_j = \exp f_i + \exp f_j$. Ecrivons :

$$f_i = \operatorname{in} f_i + f_i' \quad f_j = \operatorname{in} f_j + f'j$$

$$\begin{aligned} S(f_i, f_j) &= (\operatorname{in} f_j) f_i - (\operatorname{in} f_i) f_j \\ &= (f_j - f_j') f_i - (f_i - f_i') f_j \\ &= f_i' f_j - f_j' f_i \end{aligned}$$

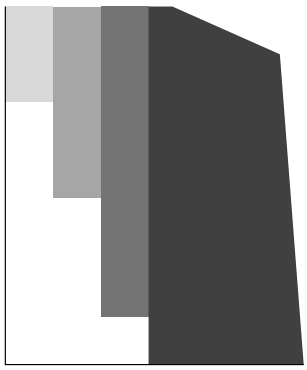
Il faut montrer alors que si f_i' et f_j' sont non nuls, $\exp f_i' f_j$ et $\exp f_j' f_i$ sont inférieurs à $\exp f_i \vee \exp f_j = \exp f_i + \exp f_j$ ce qui est immédiat.

□

Exemple 4.2.9. On choisit $n = 2$, $f_1 = X_1^3$, $f_2 = X_1^2 X_2 - X_2^3$, $f_3 = X_1 X_2^3$, $f_4 = X_2^5$, $I = (f_1, f_2, f_3, f_4)$ et l'ordre lexicographique.
On a :

$$\operatorname{in} f_1 = X_1^3 \quad \operatorname{in} f_2 = X_1^2 X_2 \quad \operatorname{in} f_3 = X_1 X_2^3 \quad \operatorname{in} f_4 = X_2^5.$$

La partition associée à la suite $\{f_1, f_2, f_3, f_4\}$ est la suivante (les Δ_i sont représentés par ordre de gris décroissant) :



$$S(f_1, f_2) = f_3 \quad S(f_2, f_3) = -f_4 \quad S(f_2, f_4) = -X_2^2 f_4$$

Puisque $\exp f_3 \in \Delta_3$, $\exp f_4 \in \Delta_4$ et $\exp X_2^2 f_4 \in \Delta_4$, ces trois égalités sont les résultats des divisions par la suite $\{f_1, f_2, f_3, f_4\}$ de $S(f_1, f_2)$, $S(f_2, f_3)$ et $S(f_2, f_4)$, et les restes sont nuls.
De plus $S(f_1, f_3) = S(f_1, f_4) = S(f_3, f_4) = 0$ puisque ce sont des monômes. Donc (f_1, f_2, f_3, f_4) est une base de Gröbner de I.

4.2.1 Algorithme de Buchberger

Le théorème va nous permettre de voir maintenant comment, à partir d'un système de générateurs d'un idéal I, on peut construire une base de Gröbner de cet idéal.
Soit donc $I = (f_1, \ldots, f_s)$ un idéal engendré par des polynômes non nuls.
Soit $\Delta_1, \ldots, \Delta_s, \bar{\Delta}$ la partition de $\mathbb{N}^n$ associée à la suite $\{f_1, \ldots, f_s\}$.

Si $(f_1, \ldots, f_s)$ n'est pas une base de Gröbner de I, choisissons les deux indices $i < j$ tels que $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\} \neq 0$ et tels que $i+j$ soit minimum pour cette propriété. Puisque $S(f_i, f_j) \in I$, ce reste est dans I. Posons $f_{s+1} = S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s\}$.

Lemme 4.2.10. *Soit f un polynôme. Avec les notations précédentes, si on a $f\mathcal{R}\{f_1, \ldots, f_s\} = 0$, alors $f\mathcal{R}\{f_1, \ldots, f_s, f_{s+1}\} = 0$.*

Démonstration. A la suite $\{f_1, \ldots, f_s, f_{s+1}\}$ on associe la partition $\Delta_1, \ldots, \Delta_s, \Delta_{s+1}, \bar{\Delta}'$ et $\bar{\Delta} = \Delta_{s+1} \cup \bar{\Delta}'$.
Si $f = \sum_{i=1}^{s} h_i f_i$, où tous les termes non nuls de $h_i \text{in}\, f_i$ ont un exposant dans Δ_i, c'est aussi le résultat de la division de f par la suite $\{f_1, \ldots, f_s, f_{s+1}\}$.
□

On remarque que puisque $\exp f_{s+1} \in \bar{\Delta}$, Δ_{s+1} n'est pas vide et contient $\exp f_{s+1}$, donc $f_{s+1}\mathcal{R}\{f_1, \ldots, f_s, f_{s+1}\} = 0$.
Si $(f_1, \ldots, f_s, f_{s+1})$ n'est pas une base de Gröbner de I, il existe deux indices $1 \leqslant i < j \leqslant s+1$ tels que $S(f_i, f_j)\mathcal{R}\{f_1, \ldots, f_s, f_{s+1}\} \neq 0$ et on recommence.

Proposition 4.2.11. *Le processus décrit ci-dessus s'arrête.*

Démonstration. On a vu que $\exp f_{s+1} \in \bar{\Delta}$ donc on a une inclusion stricte d'idéaux :

$$(\text{in}\, f_1, \ldots, \text{in}\, f_s) \subset (\text{in}\, f_1, \ldots, \text{in}\, f_s, \text{in}\, f_{s+1}) \subseteq \text{in}\, I$$

On ne peut avoir une suite infinie strictement croissante d'idéaux contenus dans l'idéal $\text{in}\, I$ car S est noethérien, d'où le résultat. □

Exemple 4.2.12. On choisit $n = 3$, $f_1 = X_1^2$, $f_2 = X_1X_2$, $f_3 = X_1X_3 + X_3^2$, $I = (f_1, f_2, f_3)$ et l'ordre lexicographique inverse. On a :

$$\text{in}\, f_1 = X_1^2 \quad \text{in}\, f_2 = X_1X_2 \quad \text{in}\, f_3 = X_1X_3$$

$$S(f_1, f_3) = X_3f_1 - X_1f_3 = -X_1X_3^2 = -X_3f_3 + X_3^3$$

et on a $S(f_1, f_3)\mathcal{R}\{f_1, f_2, f_3\} = X_3^3$. On pose donc $f_4 = X_3^3$.

$$S(f_2, f_3) = X_3f_2 - X_2f_3 = -X_2X_3^2$$

et on a $S(f_2, f_3)\mathcal{R}\{f_1, f_2, f_3\} = -X_2X_3^2$ On pose $f_5 = X_2X_3^2$.

$$S(f_3, f_4) = X_3^2f_3 - X_1f_4 = X_3^4 = X_3f_4$$

$$S(f_3, f_5) = X_2X_3f_3 - X_1f_5 = X_2X_3^3 = X_2f_4$$

et les restes de la division de $S(f_3, f_4)$ et $S(f_3, f_5)$ par la suite $\{f_1, f_2, f_3, f_4\}$ sont nuls.
Les autres $S(f_i, f_j)$ sont nuls car ils concernent des couples de monômes, donc toutes les conditions sont vérifiées et $(f_1, f_2, f_3, f_4, f_5)$ est une base de Gröbner.

Exemple 4.2.13. $n = 4$. On veut savoir si le polynôme

$$f = X_1^2X_2^2 + X_2^4 - X_1^3X_3 - X_2X_3^3 + X_2^2X_3X_4$$

appartient à l'idéal

$$I = (X_1X_3 - X_2^2, X_1X_4 - X_2X_3, X_2X_4 - X_3^2) = (f_1, f_2, f_3).$$

On considère l'ordre revlex et on regarde si le système de générateurs donné, qu'on note f_1, f_2, f_3, est une base de Gröbner.
On a

$$\operatorname{in} f_1 = -X_2^2 \quad \operatorname{in} f_2 = -X_2X_3 \quad \operatorname{in} f_3 = -X_3^2$$

et on remarque que $\operatorname{in} f_1$ et $\operatorname{in} f_3$ sont premiers entre eux.

$$S(f_1, f_2) = -X_3f_1 + X_2f_2 = X_1f_3$$
$$S(f_2, f_3) = -X_3f_2 + X_2f_3 = -X_4f_1$$

et on vérifie que ce sont bien les résultats des divisions par la suite $\{f_1, f_2, f_3\}$. On effectue alors la division de f :

$$f = -(X_1^2 + X_2^2 + X_1X_3 + X_3X_4)f_1 - X_1^2f_3 + X_3^2f_2 + X_1^2X_2X_4$$

Donc f n'appartient pas à I et on a obtenu ses coordonnées dans une base de S/I.

Définition 4.2.14. Soient I un idéal non nul de S et $(f_1, \dots, f_s)$ une base de Gröbner de I. On dit qu'elle est *réduite* si elle vérifie les deux propriétés suivantes pour tout $i \in [1, s]$:
i) $\operatorname{in} f_i = X^{\exp f_i}$
ii) $f_i = f_i\mathcal{R}\{f_1, \dots, \hat{f}_i, \dots f_s\}$.

Remarque 4.2.15. La notation $\hat{f}_i$ signifie qu'on a enlevé f_i à la suite $\{f_1, \dots, f_s\}$. La condition ii) signifie que tous les monômes de f_i sont dans le complémentaire de $\cup_{i\neq j}\exp f_i + \mathbb{N}^n$, c'est-à-dire que si $i \neq j$, $\operatorname{in} f_j$ ne divise aucun terme non nul de f_i.

Proposition 4.2.16. *Une base de Gröbner réduite est minimale, et unique à permutation près. De plus, il existe de telles bases.*

Démonstration. Soit $(f_1, \dots, f_s)$ une base de Gröbner réduite de I. Si elle n'est pas minimale, on peut en extraire une base plus petite (cf. 4.1.5), et on peut supposer, quitte à renuméroter les f_i, que $\exp I = \bigcup_{i<s} \exp f_i + \mathbb{N}^n$. Alors en particulier $\operatorname{in} f_s$ est divisible par l'un des $\operatorname{in} f_i$ pour $i < s$ ce qui contredit la propriété ii).
Soient $(f_1, \dots, f_s)$ et $(g_1, \dots, g_s)$ deux bases de Gröbner réduites. On a vu en **??** qu'on peut supposer $\exp f_i = \exp g_i$ pour tout $i \in [1, s]$. En utilisant la propriété i), on en déduit qu'on a aussi $\operatorname{in} f_i = \operatorname{in} g_i$.
Effectuons la division de g_1 par la suite $\{f_1, \dots, f_s\}$ (à laquelle on associe la partition $\Delta_1, \dots, \Delta_s, \Delta_s, \bar{\Delta}$) :

$$g_1 = \sum_{i=1}^{s} h_if_i \quad \text{d'où} \quad g_1 - h_1f_1 = \sum_{i=2}^{s} h_if_i$$

On sait que le terme initial de $\sum_{i=2}^{s} h_i f_i$ a son exposant dans l'un des Δ_i avec $i > 1$.
Si $h_1 \neq 1$ on a $\exp g_1 = \exp f_1 < \exp h_1 f_1$, donc le terme initial de $g_1 - h_1 f_1$ est égal à $\operatorname{in} h_1 \operatorname{in} f_1$ et son exposant est dans Δ_1, ce qui donne une contradiction.
On a donc $h_1 = 1$. Si $f_1 - g_1 \neq 0$, son terme initial est un terme de f_1 ou de g_1 et il ne peut être divisible par l'un des $\operatorname{in} f_i = \operatorname{in} g_i$ avec $i > 1$. Donc $f_1 = g_1$.
En changeant l'ordre de la suite $\{f_1, \ldots, f_s\}$, on en déduit qu'on a $f_i = g_i$ pour tout $i \in [1, s]$.
Montrons maintenant l'existence. On se donne une base de Gröbner minimale $(f_1, \ldots, f_s)$ et quitte à multiplier les f_i par des scalaires non nuls, on peut supposer que la condition $\operatorname{in} f_i = X^{\exp f_i}$ est réalisée.
On pose $g_i = f_i \mathcal{R}\{f_1, \ldots, \hat{f}_i, \ldots f_s\}$ et on va montrer que $(g_1, \ldots, g_s)$ est une base de Gröbner réduite.
On a donc $f_i = \sum_{j \neq i} h_{i,j} f_j + g_i$, g_i n'est pas nul puisque la base est minimale, et aucun terme non nul de g_i n'est divisible par un des $\operatorname{in} f_j$ pour $i \neq j$.
On sait que $\exp \sum_{j \neq i} h_{i,j} f_j$ est égal à l'un des $\exp h_{i,j} f_j$, soit $h_{i,j_0} f_{j_0}$.
Si

$$\exp g_i < \exp \sum_{j \neq i} h_{i,j} f_j = \exp h_{i,j_0} f_{j_0} = \exp h_{i,j_0} + \exp f_{j_0}$$

alors $\exp f_i = \exp \sum_{j \neq i} h_{i,j} f_j = \exp h_{i,j_0} + \exp f_{j_0}$ et la base n'est pas minimale.
Si

$$\exp g_i = \exp \sum_{j \neq i} h_{i,j} f_j = \exp h_{i,j_0} f_{j_0} = \exp h_{i,j_0} + \exp f_{j_0}$$

$\operatorname{in} g_i$ est divisible par $\operatorname{in} f_{j_0}$.
Donc $\exp g_i > \exp \sum_{j \neq i} h_{i,j} f_j$,

$$\exp f_i = \sup(\exp g_i, \exp (\sum_{j \neq i} h_{i,j} f_j) = \exp g_i$$

et $\operatorname{in} f_i = \operatorname{in} g_i$.
Alors puisque $\exp I = \bigcup_i \exp f_i + \mathbb{N}^n = \bigcup_i \exp g_i + \mathbb{N}^n$, $(g_1, \ldots, g_s)$ est une base de Gröbner de I.
Pour montrer qu'elle est réduite il reste à vérifier la condition ii) : si $i \neq j$, $\operatorname{in} g_j = \operatorname{in} f_j$ ne divise aucun terme non nul de g_i, mais celà découle des propriétés du reste de la division.
□

Remarque 4.2.17. Soit I un idéal homogène de S. Il possède une base de Gröbner formée de polynômes homogènes. De plus, on peut la supposer minimale ou encore réduite. En effet, $\operatorname{in} I$ est engendré par les $\operatorname{in} f$ où f est homogène et appartient à I. On en extrait un système fini de générateurs, qui est une base de Gröbner d'après 4.1.3. En utilisant le procédé de réduction de la base décrit dans la preuve de 4.2.16 on obtient à chaque étape des polynômes homogènes.

Remarque 4.2.18. Soit J un idéal monômial de S, engendré par des monômes $m_1, \ldots, m_r$. Alors $(m_1, \ldots, m_r)$ est une base de Gröbner de J, réduite si et seulement s'ils forment un système minimal de générateurs de J.

Chapitre 5

Applications

Dans ce chapitre nous donnons des applications des bases de Gröbner, qui répondent à des questions posées dans l'introduction. Nous verrons que le choix de l'ordre n'est pas indifférent, nous choisirons tel ou tel ordre suivant le problème traité.

5.1 Elimination

Soit I un idéal non nul de S. On a vu (cf. 4.1.12) qu'une base de l'espace vectoriel S/I est formée des monômes qui ne sont pas dans l'idéal initial $\operatorname{in} I$. On en déduit immédiatement le résultat suivant :

Proposition 5.1.1. *Soit I un idéal non nul de S. Pour que S/I soit un espace vectoriel de dimension finie, il faut et il suffit que le cardinal de $\mathbb{N}^n \setminus \exp I$ soit fini et la dimension de S/I est alors égale à ce cardinal.*

Démonstration. Pour tout f non nul dans S, on a $\exp f = \exp \operatorname{in} f$, et on en déduit qu'on a :

$$\exp I = \{\exp f \mid f \in I\} = \{\exp m \mid m \in \operatorname{in} I\}$$

d'où le résultat.

□

Nous allons utiliser ce résultat pour calculer le nombre de solutions d'un système algébrique (s'il est fini). Auparavant nous avons besoin d'un résultat d'élimination qui utilise la propriété de l'ordre lexicographique vue en 2.3.4.

Proposition 5.1.2. *Soient $n' \leqslant n$ et I un idéal non nul de S. On considère $S' = k[X_{n'}, \ldots, X_n]$ comme sous-anneau de S et on fixe l'ordre lexicographique sur S et S'.*
Soit $(f_1, \ldots, f_s)$ une base de Gröbner de I et soit J l'ensemble des entiers $i \in [1, s]$ tels que f_i appartienne à S'.
Si J est vide, $I \cap S'$ est nul. Sinon, $I \cap S'$ a une base de Gröbner formée des f_i tels que $i \in J$ et $\operatorname{in}(I \cap S') = \operatorname{in} I \cap S'$.

Démonstration. Soit $I' = I \cap S'$ et $f \in I'$. Effectuons la division de f par la suite $\{f_1, \ldots, f_s\}$: $f = \sum h_i f_i$. On sait que si f n'est pas nul, son terme initial est celui d'un des $h_i f_i$: il existe i_0 tel qu'on ait $\operatorname{in} f = \operatorname{in} h_{i_0} \operatorname{in} f_{i_0}$.
Or puisque f appartient à S', il en est de même de $\operatorname{in} f$, donc $\operatorname{in} f_{i_0} \in S'$ et $f_{i_0} \in S'$ (cf.2.3.4). En particulier J n'est pas vide. On a montré aussi les inclusions :

$$\exp I' \subseteq \bigcup_{i \in J} \exp f_i + N^{n-n'+1} \subseteq \exp I'$$

d'où l'égalité et les f_i tels que $i \in J$ forment une base de Gröbner de I'.
On en déduit immédiatement l'égalité $\operatorname{in} I' = \operatorname{in} I \cap S'$.

□

Remarque 5.1.3. Géométriquement, si I est l'idéal d'une sous-variété V de l'espace affine $\mathbb{A}^n$, $I \cap S'$ définit l'adhérence de la projection de V sur l'espace affine des dernières coordonnées $X_{n'}, \ldots, X_n$.

Exemple 5.1.4. On choisit $n = 4$, $I = (X_1X_3, X_2X_4, X_1 + X_2 - 1)$ et on veut calculer $I \cap k[X_3, X_4]$. Notons f_1, f_2 et f_3 les générateurs.
On a

$$\operatorname{in} f_1 = X_1X_3 \quad \operatorname{in} f_2 = X_2X_4 \quad \operatorname{in} f_3 = X_1$$

et
On a :

$$S(f_1, f_3) = f_1 - X_3 f_3 = X_3 - X_2X_3 = f_4$$
$$S(f_1, f_4) = X_2 f_1 - X_1 f_4 = X_1X_3 = f_1$$
$$S(f_2, f_4) = X_3 f_2 - X_4 f_4 = X_3X_4 = f_5$$
$$S(f_5, f_4) = X_4 f_4 - + X_2 f_5 = X_3X_4 = f_5$$

et on vérifie que ce sont bien les résultats des divisions par la suite $\{f_1, f_2, f_3, f_4, f_5\}$. Alors $(f_1, \ldots, f_5)$ est une base de Gröbner de I donc $I \cap k[X_3, X_4] = (X_3X_4)$.

Remarque 5.1.5. Cette méthode a l'avantage d'être systématique mais en l'occurrence elle est un peu lourde. Le calcul est plus rapide directement. En effet, soit f un polynôme indépendant de X_1 et X_2 qu'on peut écrire :

$$f = \alpha X_1X_3 + \beta X_2X_4 + \gamma(X_1 + X_2 - 1)$$

où α, β et γ sont des polynômes. En faisant $X_1 = 1$, $X_2 = 0$, ce qui laisse f inchangé, on obtient $f = \alpha(1, 0, X_3, X_4)X_3$ donc f est divisible par X_3.
De même, en faisant $X_1 = 0$, $X_2 = 1$, on montre que f est divisible par X_4. Donc f est divisible par X_3X_4 et $I \cap k[X_3, X_4] \subseteq (X_3X_4)$.
D'autre part on a :

$$X_3X_4 = X_1X_3X_4 + X_2X_3X_4 - X_3X_4(X_1 + X_2 - 1)$$

et $(X_3X_4) \subseteq I$ d'où le résultat.

Exemple 5.1.6. On choisit $n = 4$, $I = (X_1X_3 - X_2^2, X_1X_4 - X_2X_3, X_2X_4 - X_3^2)$ et on veut calculer $I' = I \cap k[X_2, X_3, X_4]$ et $I'' = I \cap k[X_1, X_3, X_4]$. Notons f_1, f_2 et f_3 les générateurs.
On a

$$\text{in}\, f_1 = X_1X_3 \quad \text{in}\, f_2 = X_1X_4 \quad \text{in}\, f_3 = X_2X_4$$

et

$$S(f_1, f_2) = X_4f_1 - X_3f_2 = X_2X_3^2 - X_2^2X_4 = -X_2^2f_3$$
$$S(f_2, f_3) = X_2f_2 - X_1f_3 = -X_1X_2^2 - X_2^2X_3 = X_3f_1$$

et on vérifie que ce sont bien les résultats des divisions par la suite $\{f_1, f_2, f_3\}$.
Donc (f_1, f_2, f_3) est une base de Gröbner de I et $I' = (X_2X_4 - X_3^2)$.
Pour calculer I'' il faut échanger X_1 et X_2. On pose $Y_1 = X_2$, $Y_2 = X_1$, $Y_3 = X_3$, $Y_4 = X_4$.
On a $I = (Y_1^2 - Y_2Y_3, Y_2Y_4 - Y_1Y_3, Y_1Y_4 - Y_3^2)$ et

$$\text{in}\, f_1 = Y_12 \quad \text{in}\, f_2 = -Y_1Y_3 \quad \text{in}\, f_3 = Y_1Y_4$$

$$S(f_1, f_2) = Y_3f_1 - Y_1f_3 = Y_1Y_2Y_4 - Y_2Y_3^2 = -Y_2f_3$$
$$S(f_1, f_3) = Y_4f_1 - Y_1f_3 = Y_1Y_3^2 - Y_1Y_2Y_4 = -Y_3f_2$$
$$S(f_2, f_3) = -Y_4f_2 - Y_3f_3 = Y_3^3 - Y_2Y_4^2 = f_4$$
$$S(f_2, f_4) = Y_3^2f_2 - Y_1f_4 = Y_1Y_2Y_4^2 - Y_2Y_3^2Y_4 = Y_2Y_4f_3$$

Alors (f_1, f_2, f_3, f_4) est une base de Gröbner de I et $I'' = (Y_3^3 - Y_2Y_4^2) = (X_3^3 - X_1X_4^2)$.

Proposition 5.1.7. *On suppose k algébriquement clos. Soit $I = (f_1, \ldots, f_s)$ un idéal de S. Si $1 \leq \dim S/I < +\infty$, le système d'équations $f_1 = 0, \ldots f_s = 0$ possède un nombre fini N de solutions et on a $1 \leq N \leq \dim S/I$.*

Démonstration. La démonstration de la finitude se fait par récurrence sur n.
– Pour $n = 1$, I est engendré par un polynôme f de degré d qui a au plus d racines ; le quotient $k[X]/(f)$ a pour base $1, X, \ldots, X^{d-1}$, d'où le résultat.
– Supposons $n > 1$. Les solutions du système d'équations $f_1 = 0, \ldots, f_s = 0$ sont les "zéros de I" et ne dépendent pas du système de générateurs. On peut donc supposer que $(f_1, \ldots, f_s)$ est une base de Gröbner minimale de I pour l'ordre *lex*.
Puisque la dimension de S/I est finie, l'ensemble $\mathbb{N}^n \setminus \exp I$ l'est aussi et l'intersection de $\exp I$ avec le dernier axe de coordonnées de $\mathbb{N}^n$ est un segment $[\alpha, +\infty]$ avec

$$\alpha = \inf\{d \mid (0, \ldots, 0, d) \in \exp I\}.$$

On remarque que $\alpha \neq 0$, sinon I contient 1 et la dimension de S/I est égale à 0 ce qu'on a exclus.
On a :

$$(0, \ldots, 0, \alpha) \in \exp I = \cup_i \exp f_i + \mathbb{N}^n \Rightarrow \exists i_0,\ (0, \ldots, 0, \alpha) \in \exp f_{i_0} + \mathbb{N}^n$$

On a donc nécessairement $\exp f_{i_0} = (0, \ldots, 0, \beta)$ avec $\beta \leqslant \alpha$ et puisque $\exp f_{i_0} \in \exp I$, $\beta = \alpha$.

Puisque in $f_{i_0} \in k[X_n]$, $f_{i_0} \in k[X_n]$ (cf.2.3.4). De plus s'il existe $j \neq i_0$ tel que $f_j \in k[X_n]$, on a encore $\exp f_j = (0, \ldots, 0, \gamma)$ avec $\gamma \geqslant \alpha$ et la base n'est pas minimale.
D'après 5.1.2 on a donc $I \cap k[X_n] = (f_{i_0})k[X_n]$.
Si $\xi = (\xi_1, \ldots, \xi_n)$ est un zéro de l'idéal I, ξ_n est une racine de f_{i_0}.
Inversement, soit ξ_n une racine de f_{i_0}. On considère l'homomorphisme de k-algèbres :

$$\Phi : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_{n-1}]$$

défini par $\Phi(X_i) = X_i$ pour $1 \leqslant i \leqslant n-1$ et $\Phi(X_n) = \xi_n$. Soit I_n l'image de I par Φ, qui est l'idéal engendré par les $f_i(X_1, \ldots, X_{n-1}, \xi_n)$.
On vérifie que Φ induit un homomorphisme surjectif :

$$\bar{\Phi} : k[X_1, \ldots, X_n]/I \to k[X_1, \ldots, X_{n-1}]/I_n$$

donc la dimension de $k[X_1, \ldots, X_{n-1}]/I_n$ est finie.
Si elle est nulle, I_n contient 1, et il existe $h \in I$ tel que $h-1$ soit divisible par $X_n - \xi_n$: $h - 1 = (X_n - \xi_n)h'$. De plus, puisque ξ_n est une racine de f_{i_0} on a : $f_{i_0} = (X_n - \xi_n)f'$. On en déduit :

$$(h-1)f' = (X_n - \xi_n)h'f' = h'f_{i_0} \quad \text{ou encore} \quad f' = hf' + h'f_{i_0}$$

et donc $f' \in I \cap k[X_n] = (f_{i_0})k[X_n]$ ce qui est impossible pour des raisons de degré.
On peut donc appliquer l'hypothèse de récurrence à I_n qui admet un nombre fini de zéros. Ceci étant vrai pour chaque ξ_n racine de f_{i_0}, c'est encore vrai pour I.

Nous allons maintenant majorer le nombre de solutions. Soient $\xi_1, \ldots, \xi_N$ les solutions du système, avec $\xi_j = (\xi_{j,1}, \ldots, \xi_{j,n}) \in k^n$. L'homomorphisme de k-espaces vectoriels :

$$\Theta : k[X_1, \ldots, X_n] \to k^N$$

défini par $\Theta(f) = (f(\xi_1), \ldots, f(\xi_n))$ est nul sur I donc se factorise par S/I. La dimension de S/I est donc supérieure ou égale à celle de l'image de Θ. On aura terminé en montrant que Θ est surjectif.
Nous allons montrer par exemple que l'élément $(1, 0, \ldots, 0)$ de k^N est dans l'image.
Pour tout $j > 1$, puisque $\xi_j \neq \xi_1$, il existe i_j tel que $\xi_{j,i_j} \neq \xi_{1,i_j}$. Posons

$$f = \lambda(X_{i_2} - \xi_{2,i_2}) \ldots (X_{i_n} - \xi_{n,i_n})$$

il vérifie $f(\xi_1) \neq 0$, $f(\xi_2) = \cdots, f(\xi_n) = 0$ et en posant $\lambda = 1/f(\xi_1)$ on a bien $\Theta(f) = (1, 0, \ldots, 0)$. □

Remarque 5.1.8. Il peut bien sûr arriver que le nombre de solutions soit différent de la dimension de S/I, par exemple pour $n = 1$ si on prend un idéal engendré par un polynôme avec des racines multiples.

Exemple 5.1.9. On choisit $n = 2$ et on cherche les solutions du système donné par

$$f_1 = X_1^2 + X_1X_2 + 2X_1 + X_2 - 1 = 0 \quad f_2 = X_1^2 - X_2^2 + 3X_1 + 2X_2 - 1 = 0$$

On commence par regarder si (f_1, f_2) est une base de Gröbner.
On a $\operatorname{in} f_1 = \operatorname{in} f_2 = X_1^2$ et

$$\begin{aligned}
S(f_1, f_2) &= f_1 - f_2 = X_1X_2 - X_1 + X_2^2 - X_2 = f_3 \\
S(f_1, f_3) &= X_2 f_1 - X_1 f_3 = X_1^2 + 3X_1X_2 + X_2^2 - X_2 \\
&= f_1 + 2f_3 - X_2^2 + 1 = f_1 + 2f_3 + f_4 \\
S(f_2, f_3) &= X_2 f_2 - X_1 f_3 = X_1^2 - X_1X_2^2 + 4X_1X_2 - X_2^3 + 2X_2^2 \\
&= f_1 - (X_2 - 2)f_3 + f_4 \\
S(f_3, f_4) &= -X_2 f_3 - X_1 f_4 = f_3 + X_2 f_4
\end{aligned}$$

On a donc $I \cap k[X_2] = (f_4)k[X_2]$, ses racines sont 1 et -1 et les solutions du système sont de la forme $(\xi, 1)$ et $(\xi, -1)$.
On remplace d'abord X_2 par 1 : l'idéal à étudier est $I' = (X_1^2 + 3X_1)$ et les zéros sont 0 et -3.
On remplace ensuite X_2 par -1 : l'idéal à étudier est $I'' = (X_1^2 + X_1 - 2, X_1^2 + 3X_1 - 4) = (X_1 - 1)$ et le seul zéro est 1.
Les solutions du système sont donc $(0, 1)$, $(-3, 1)$ et $(1, -1)$.

L'élimination permet aussi de calculer les équations satisfaites par des éléments d'un anneau affine. Géométriquement, celà revient à décrire l'adhérence de l'image d'un ensemble algébrique par un morphisme. On est dans la situation suivante. Soient $R = k[Y_1, \ldots, Y_s]$ et J un idéal de R. Un homomorphisme de k-algèbres $\varphi : S \to R/J$ est défini par la donnée de n éléments $F_1, \ldots, F_n$ de R (ou plus précisément par la donnée de leurs classes $\bar{F}_1 = \varphi(X_1), \ldots, \bar{F}_n = \varphi(X_n)$ dans R/J) et on souhaite calculer le noyau de φ.

Proposition 5.1.10. *En gardant les notations précédentes, on considère l'anneau $T = k[X_1, \ldots, X_n, Y_1, \ldots, Y_s]$, qui contient S et R comme sous-anneaux, et I l'idéal de T engendré par J et les polynômes $F_1 - X_1, \ldots, F_n - X_n$. Le noyau de φ est l'intersection $I \cap S$.*

Démonstration. Soit l'homomorphisme de R-algèbres $\psi : T \to R/J$ défini par $\psi(X_i) = \bar{F}_i$. Alors le noyau de ψ est l'intersection de S et du noyau de φ.
Soit $P \in T$. On peut l'écrire $P = \sum_i (X_i - F_i)P_i + Q$, où Q ne dépend plus des X_i, donc $Q \in R$. De plus, l'image $\psi(P)$ est égale à la classe de Q dans R/J. Donc si P est dans le noyau de ψ, Q appartient à J et P appartient à I.
Inversement il suffit de voir que des générateurs de I sont dans le noyau de ψ. On peut prendre les polynômes $(X_i - F_i)$ et des générateurs de J dans R. Il sont bien dans le noyau de ψ, qui est donc égal à I, d'où le résultat.

□

Remarque 5.1.11. Dans la pratique, on prendra sur T l'ordre lexicographique avec

$$Y_1 > \cdots > Y_s > X_1 > \cdots > X_n$$

on calculera une base de Gröbner de I à partir d'une base de Gröbner de J et des $F_i - X_i$.

Remarque 5.1.12. Pour $n \leqslant s$ et $F_1 = Y_{n-s+1}, \ldots, F_n = Y_s$, on retrouve le cas de la projection.

5.2 Intersection d'idéaux

Proposition 5.2.1. *Soient I_1, ..., I_m des idéaux de S. On considère l'anneau $T = k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, qui contient S comme sous-anneau, et I l'idéal de T engendré par $Y_1 I_1$, ..., $Y_m I_m$ et le polynôme $1 - \sum_{i=1}^{m} Y_i$. Alors on a : $I_1 \cap \cdots \cap I_m = I \cap S$.*

Démonstration. On se donne pour tout i un système de générateurs $(f_{i,1}, \ldots, f_{i,s_i})$ de l'idéal I_i de S. Soit $f \in I \cap S$, donc ne dépendant que des variables X_1, ..., X_n. On peut l'écrire :

$$f = \sum_{i,j} f_{i,j} g_{i,j} Y_i + g(1 - \sum_i Y_i)$$

où $g_{i,j}$ et g sont des éléments de T.
En faisant $Y_k = 0$ pour $k \neq i$ et $Y_i = 1$, on obtient :

$$f = \sum_j f_{i,j} g_{i,j}(X_1, \ldots, X_n, 0, \ldots, 1, \ldots, 0)$$

et donc f appartient à I_i pour tout i.
Inversement, soit f un élément de l'intersection des idéaux I_i. On peut l'écrire :

$$f = \sum_i f Y_i + f(1 - \sum_i Y_i)$$

et il est bien dans l'idéal I.

□

Remarque 5.2.2. Dans la pratique, on prendra sur T l'ordre lexicographique avec

$$Y_1 > \cdots > Y_m > X_1 > \cdots > X_n$$

et on calculera une base de Gröbner de I.

5.3 Suites régulières

Définition 5.3.1. Soient $I = (f_1, \ldots, f_r)$ un idéal non nul de S. On dit que le système de générateurs $f_1, \ldots, f_r$ est *minimal* si pour tout $i \in [1, r]$, l'idéal engendré par les f_j, $j \in [1, r]$, $j \neq i$, est différent de I.

Définitions 5.3.1. Soient A un anneau et a un élément de A. On dit que a est *diviseur de zéro dans A* s'il existe $b \neq 0$ appartenant à A tel qu'on ait $ab = 0$. Sinon, on dit que a est *non-diviseur de zéro dans A*.
Soient A un anneau et $a_1, \ldots, a_s$ $(s \geq 1)$ une suite d'éléments de A. On dit que c'est une *A-suite régulière* (ou une *suite régulière de A*) si l'idéal $(a_1, \ldots, a_s)$ n'est pas égal à S, si a_1 est non-diviseur de zéro et si pour tout entier $i \in [1, s-1]$ l'image de a_{i+1} dans le quotient $A/(a_1, \ldots, a_i)$ est non-diviseur de zéro.
Soient A un anneau, I un idéal de A et $a_1, \ldots, a_s$ $(s \geq 1)$ une suite d'éléments de A. On dit que $a_1, \ldots, a_s$ est une suite régulière modulo I si les images de $a_1, \ldots, a_s$ dans S/I forment une suite régulière de S/I.

Remarques 5.3.2. On peut encore dire que a est non-diviseur de zéro dans A si et seulement si $((0) : a) = (0)$.
De même, la suite $a_1, \ldots, a_s$ est régulière si et seulement si $((0) : a_1) = (0)$ et pour tout $i \in [1, s-1]$, $((a_1, \ldots, a_i) : a_{i+1}) = (a_1, \ldots, a_i)$.
Enfin, la suite $a_1, \ldots, a_s$ est régulière modulo I si et seulement si $(I : a_1) = I$ et pour tout $i \in [1, s-1]$, $(((a_1, \ldots, a_i) + I) : a_{i+1}) = ((a_1, \ldots, a_i) + I)$.
L'ordre des éléments de la suite est important.

Nous allons voir que dans le cas où l'idéal I est monomial, il est facile de caractériser les suites régulières de monômes modulo I.

Proposition 5.3.3. *Soit J un idéal monomial de S différent de S et $m_1, \ldots, m_r$ ($r \geq 1$) des monômes qui forment un système minimal de générateurs de J. Soient $m'_1, \ldots, m'_s$ ($s \geq 1$) une suite de monômes de S. Ils forment une suite régulière modulo J si et seulement si pour tout i, j, k avec $i, j \in [1, s]$, $k \in [1, r]$, $i \neq j$, m'_i est premier avec m'_j et m_k.*

Démonstration. Soit $m'_1, \ldots, m'_s$ une suite de monômes régulière modulo J.
Soient i et j, $i < j$, les plus petits indices, s'ils existent, tels que m'_i et m'_j ne soient pas premiers entre eux. Posons $m'_i = dM'_i$ et $m'_j = dM'_j$ avec M'_i et M'_j premiers entre eux. On a $M'_i m'_j = M'_j m'_i$.
Puisque m'_j n'est pas diviseur de zéro dans $S/(m_1, \ldots, m_r, m'_1, \ldots, m'_{j-1})$, M'_i est divisible par l'un des $m_1, \ldots, m_r, m'_1, \ldots, m'_{j-1}$. On a plusieurs possibilités :
– si M'_i est divisible par l'un des $m_1, \ldots, m_r$, M'_i appartient à J, et m'_i appartient à J, ce qui contredit la régularité de la suite.
– si M'_i est divisible par $m'_{k'}$ avec $k' \leq j-1$, $k' \neq i$, $m'_{k'}$ et m'_i ne sont pas premiers entre eux, ce qui contredit la minimalité de i, j.
– si M'_i est divisible par m'_i, d est égal à 1, et m'_i et m'_j sont premiers entre eux.
Soitmaintenant i le plus petit indice, s'il existe, tel qu'il existe m_k non premier avec m'_i. Posons $m'_i = dM'_i$ et $m_k = dM_k$ avec M'_i et M_k premiers entre eux. On a $M'_i m_k = M_k m'_i$. Comme ci-dessus, on en déduit que M_k est divisible par l'un des $m_1, \ldots, m_r, m'_1, \ldots, m'_{i-1}$. D'où les différentes possibilités :
– si M_k est divisible par m_k, d est égal à 1, et m'_i et m_k sont premiers entre eux.
– si M_k est divisible par $m_{k'}$ avec $k' \neq k$, le système de générateurs n'est pas minimum.
– si M_k est divisible par $m'_{k'}$ avec $k' \leq i-1$, $m'_{k'}$ et m_k ne sont pas premiers entre eux, ce qui contredit la minimalité de i.
Inversement supposons que pour tout i, j, k avec $i, j \in [1, s]$, $k \in [1, r]$, $i \neq j$, m'_i soit premier avec m'_j et m_k. Soit alors a tel que $am'_i \in (m_1, \ldots, m_r, m'_1, \ldots, m'_{i-1})$, et $a \notin (m_1, \ldots, m_r, m'_1, \ldots, m'_{i-1})$. Tout monôme parmi $m_1, \ldots, m_r, m'_1, \ldots, m'_{i-1}$ est premier avec m'_i donc s'il divise am'_i il divise a, donc m'_i n'est pas diviseur de zéro dans $S/(m_1, \ldots, m_r, m'_1, \ldots, m'_{i-1})$.
On montre de la même manière que m'_1 n'est pas diviseur de zéro dans $S/(m_1, \ldots, m_r)$. □

Lemme 5.3.4. *Soient I un idéal de S et g un élément non nul de S. Si $in\, g$ est non-diviseur de zéro dans $S/in\, I$, alors g est non-diviseur de zéro dans S/I et on a $in\,(I+(g)) = in\, I + (in\, g)$.*

Démonstration. Considérons s'il est non vide l'ensemble des exposants des éléments f de S, tels que $f \notin I$ et $fg \in I$ et soit f_0 dont l'exposant est minimum dans cet ensemble. Alors $\operatorname{in} f_0 \operatorname{in} g \in \operatorname{in} I$, donc $\operatorname{in} f_0 \in \operatorname{in} I$.
Il existe $f \in I$ tel que $\operatorname{in} f = \operatorname{in} f_0$. Soit $f_1 = f_0 - f$. Si $f_1 \neq 0$ on a $\exp f_1 < \exp f_0$. De plus $f_1 g = f_0 g - fg \in I$ ce qui donne une contradiction avec la minimalité de $\exp f_0$.
De même, si $f_1 = 0$ $f_0 = f \in I$ et on a une contradiction.
Puisque $I \subseteq I + (g)$ et $g \in I + (g)$, on a $\operatorname{in} I \subseteq \operatorname{in}(I + (g))$ et $\operatorname{in} g \in \operatorname{in} I + (g))$ d'où l'inclusion $\operatorname{in} I + (\operatorname{in} g) \subseteq \operatorname{in}(I + (g))$.
Soit maintenant f_0 appartenant à $I + (g)$ tel que $\operatorname{in} f_0$ n'appartienne pas à $\operatorname{in} I + (\operatorname{in} g)$. On peut écrire $f_0 = f_1 - gh$, avec $f_1 \in I$. On peut supposer que f_1 a un exposant minimum.
- si $\operatorname{in} f_1 - \operatorname{in} gh \neq 0$, alors $\exp f_0 = sup(\exp f_1, \exp gh)$ et $\operatorname{in} f_0 \in \operatorname{in} I + (\operatorname{in} g)$, ce qui est contraire à l'hypothèse.
- sinon, $\operatorname{in} g \operatorname{in} h = \operatorname{in} f_1$. Puisque $\operatorname{in} g$ est non-diviseur de zéro dans $S/\operatorname{in} I$, alors $\operatorname{in} h$ appartient à $\operatorname{in} I$, donc il existe $h' \in I$ tel que $\operatorname{in} h = \operatorname{in} h'$. Posons $h_1 = h - h'$.
  On a $f_0 = f_1 - gh' - gh_1 = f_2 - gh_1$ et puisque $\operatorname{in} f_1 = \operatorname{in} gh'$, $\exp f_2 < \exp f_1$ ce qui contredit la minimalité de $\exp f_1$.

□

Proposition 5.3.5. *Soient I un idéal de S et $g_1, \ldots, g_s$ une suite d'éléments de S. Si $in\, g_1, \ldots, in\, g_s$ forment une suite régulière modulo $in\, I$, $g_1, \ldots, g_s$ forment une suite régulière modulo I et on a $in(I + (g_1, \ldots, g_s)) = in\, I + (in\, g_1, \ldots, in\, g_s)$.*

Démonstration. Elle se fait par récurrence sur s.
Pour $s = 1$, c'est le résultat précédent.
Pour $s > 1$, posons $I' = I + (g_1, \ldots, g_{s-1})$. Par hypothèse de récurrence $g_1, \ldots, g_{s-1}$ est une suite régulière modulo I et on a $\operatorname{in} I' = \operatorname{in} I + (\operatorname{in} g_1, \ldots, \operatorname{in} g_{s-1})$.
Alors, $\operatorname{in} g_s$ est non-diviseur de zéro dans $S/\operatorname{in} I + (\operatorname{in} g_1, \ldots, \operatorname{in} g_{s-1}) = S/\operatorname{in} I'$, donc g_s est non diviseur de zéro dans S/I' et la suite $g_1, \ldots, g_s$ est régulière modulo I. De plus, $\operatorname{in}(I' + (g_s)) = \operatorname{in} I' + (\operatorname{in} g_s) = \operatorname{in} I + (\operatorname{in} g_1, \ldots, \operatorname{in} g_{s-1})$.

□

Dans un cas particulier cette proposition admet une réciproque. Auparavant nous avons besoin d'un résultat qui utilise la propriété de l'ordre lexicographique inverse vue en 2.3.4.

Proposition 5.3.6. *Soient $n' \leqslant n$ et I un idéal homogène non nul de S. On fixe l'ordre lexicographique inverse sur S.*
Soit $(f_1, \ldots, f_s)$ une base de Gröbner de I. Alors $(f_1, \ldots, f_s, X_{n'}, \ldots, X_n)$ est une base de Gröbner de $I + (X_{n'}, \ldots, X_n)$. De plus on a $in(I + (X_{n'}, \ldots, X_n)) = in\, I + (X_{n'}, \ldots, X_n)$.

Démonstration. Soient f et g deux polynômes n'appartenant pas à l'idéal $(X_{n'}, \ldots, X_n)$. Si $f - g \in (X_{n'}, \ldots, X_n)$, on a $\operatorname{in} f = \operatorname{in} g$.
Soit alors $f \in I + (X_{n'}, \ldots, X_n)$. Si $f \in (X_{n'}, \ldots, X_n)$, $\operatorname{in} f \in (X_{n'}, \ldots, X_n)$. Sinon, il existe $g \in I$ tel que $f - g \in (X_{n'}, \ldots, X_n)$. D'après ce qui précède on a $\operatorname{in} f = \operatorname{in} g$. D'où l'inclusion $\operatorname{in}(I + (X_{n'}, \ldots, X_n)) \subseteq \operatorname{in} I + (X_{n'}, \ldots, X_n)$.
On en déduit immédiatement l'assertion sur les bases de Gröbner.

□

Proposition 5.3.7. *L'ordre est maintenant l'ordre lexicographique inverse. Soient I un idéal homogène et $n' \leq n$. La suite $X_n, \ldots, X_{n'}$ est une suite régulière modulo I si et seulement si elle est régulière modulo $\operatorname{in} I$.*

Démonstration. Soit m un monôme tel que $mX_{n'} \in \operatorname{in} I + (X_n, \ldots, X_{n'+1})$.
On a vu en 5.3.6 qu'on a $\operatorname{in} I + (X_n, \ldots, X_{n'-1}) = \operatorname{in}(I + (X_n, \ldots, X_{n'-1}))$ donc il existe $f \in I + (X_n, \ldots, X_{n'+1})$ tels qu'on ait $\operatorname{in} f = mX_{n'}$.
De plus, puisque $\operatorname{in} f \in (X_n, \ldots, X_{n'})$ on a $f \in (X_n, \ldots, X_{n'})$. On peut écrire $f = X_{n'}f_1 + f_2$ avec $f_2 \in (X_n, \ldots, X_{n'+1})$. Alors $X_{n'}f_1 \in I + (X_n, \ldots, X_{n'+1})$. Puisque la suite $X_n, \ldots, X_{n'}$ est régulière modulo I, on en déduit que $f_1 \in I + (X_n, \ldots, X_{n'+1})$. Quitte à modifier f_1 et f_2, on peut donc supposer que $f_1 \in I$.
– Si $f_1 \notin (X_n, \ldots, X_{n'+1})$, $X_{n'}f_1$ a un terme non nul ne dépendant que des premières coordonnées $X_1, \ldots, X_{n'}$, qui est plus grand que tout terme non nul de f_2. On a donc $\in f = X_{n'} \operatorname{in} f_1$ donc $m = \operatorname{in} f_1 \in\in I$.
– Si $f_1 \in (X_n, \ldots, X_{n'+1})$, on a $mX_{n'} = \operatorname{in} f \in (X_n, \ldots, X_{n'+1})$ donc $m \in (X_n, \ldots, X_{n'+1})$.
Dans les deux cas on a donc $m \in \operatorname{in} I + (X_n, \ldots, X_{n'+1})$. □

Remarque 5.3.8. On fera attention à l'ordre dans l'énoncé de 5.3.7.

5.4 Cas homogène

Proposition 5.4.1. *Soit I un idéal homogène de S et $\operatorname{in} I$ son idéal initial. Les fonctions de Hilbert (cf. 1.2.1) des anneaux S/I et $S/\operatorname{in} I$ sont égales.*

Démonstration. On a vu en 1.1.4 qu'on a un isomorphisme d'espaces vectoriels :
$\oplus_{d\in\mathbb{N}} S_d/I_d \simeq S/I$ et aussi (4.1.12) qu'une base de S/I est formée des monômes qui ne sont pas dans $\operatorname{in} I$. Il en est donc de même de S_d/I_d.
On peut également appliquer ce résultat à l'idéal monomial $\operatorname{in} I$, qui est égal à son idéal initial. Donc les monômes de degré d qui ne sont pas dans $\operatorname{in} I$ forment une base à la fois de S_d/I_d et de $S_d/\operatorname{in} I_d$. □

Ceci nous permet de généraliser à tous les idéaux homogènes le résultat vu pour les idéaux monomiaux :

Corollaire 5.4.2. *Soit I un idéal homogène de S. La fonction de Hilbert $h_{S/I}$ est polynomiale pour $d \gg 0$.*

Exemple 5.4.3. On choisit $n = 4$, $I = (X_1X_3 - X_2^2, X_1X_4 - X_2X_3, X_2X_4 - X_3^2)$. Notons f_1, f_2 et f_3 les générateurs.
Si on choisit l'ordre lexicographique, on a vu en 5.1.6 qu'on a :

$$\operatorname{in} f_1 = X_1X_3 \quad \operatorname{in} f_2 = X_1X_4 \quad \operatorname{in} f_3 = X_2X_4$$

que f_1, f_2, f_3 est une base de Gröbner de I et que $\operatorname{in} I = (X_1X_3, X_1X_4, X_2X_4)$. La fonction de Hilbert de $S/\operatorname{in} I$ a été calculée en 1.2.4 et on a : $h_{S/I}(d) = 3d + 1$ pour $d \geqslant 0$.

On aurait aussi pu mettre l'ordre lexicographique inverse. On a alors

$$\text{in}\, f_1 = X_2^2 \quad \text{in}\, f_2 = X_2X_3 \quad \text{in}\, f_3 = X_3^2$$

On vérifie que f_1, f_2, f_3 est une base de Gröbner de I et donc on a $\text{in}\, I = (X_2^2, X_2X_3, X_3^2)$.
On a immédiatement $h_{S/I}(0) = 1$, $h_{S/I}(1) = 4$.
Soit $m = X_1^{\alpha_1}X_2^{\alpha_2}X_3^{\alpha_3}X_4^{\alpha_4}$ un monôme de degré $d > 1$. Il appartient à I si et seulement si $\alpha_2 + \alpha_3 \geq 2$. Une base des monômes de degré d qui ne sont pas dans $\text{in}\, I$ est constituée :
– des monômes vérifiant $\alpha_2 = \alpha_3 = 0$, il y en a $d + 1$ linéairement indépendants ;
– des monômes vérifiant $\alpha_2 = 1$, $\alpha_3 = 0$, il y en a d linéairement indépendants ;
– des monômes vérifiant $\alpha_2 = 0$, $\alpha_3 = 1$, il y en a d linéairement indépendants.
ce qui redonne $h_{S/I}(d) = 3d + 1$.

5.5 Homogénéisation et déshomogénéisation

Dans tout ce paragraphe, on se place dans le cadre général du degré pondéré (cf. chapitre 1). Le degré pondéré de X_i est a_i. On considère S comme sous-anneau de l'anneau $S[t] = k[X_1, \ldots, X_n, t]$ sur lequel on met le degré pondéré défini par $\deg X_i = a_i$ et $\deg t = 1$.

Définition 5.5.1. Soit f un élément non nul de S et d son degré pondéré. L'*homogénéisé* de f est le polynôme $\tilde{f}$ de $S[t]$ homogène de degré d défini par :

$$\tilde{f} = t^d f(X_1/t^{a_1}, \ldots, X_n/t^{a_n}).$$

Soit F un élément non nul de $S[t]$ homogène de degré pondéré d. Le *déshomogénéisé* de F est le polynôme $F(X_1, \ldots, X_n, 1)$ de S.
On convient que l'homogénéisé et le déshomogénéisé de 0 sont tous deux nuls.

Exemple 5.5.2. On choisit $n = 2$, $a_1 = 3$, $a_2 = 1$, $f = X_1^5 + X_1^2X_2^4$, $\tilde{f} = X_1^5 + t^5X_1^2X_2^4$.

Remarque 5.5.3. Si on écrit f en faisant apparaitre ses composantes homogènes :

$$f = f_d + f_{d-1} + \cdots + f_0 \quad \text{avec} \quad f_d \neq 0$$

on a : $\tilde{f} = f_d + tf_{d-1} + \cdots + t^d f_0$.

Les opérations d'homogénéisation et de déshomogénéisation ont les propriétés suivantes :

Lemme 5.5.4. *i) pour tout $f \in S$ on a $\tilde{f}(X_1, \ldots, X_n, 1) = f$,*
ii) pour tout $F \in S[t]$ homogène il existe N tel que $t^N F(X_1, \ldots, X_n, 1)\tilde{} = F$,
iii) pour tous $f \in S$ et $g \in S$ on a $\widetilde{fg} = \tilde{f}\tilde{g}$.
iv) Soient $f_1, \ldots, f_s$ des éléments de S ; il existe $(n_1, \ldots, n_s) \in \mathbb{Z}^n$ tels qu'on ait : $(\sum f_i)\tilde{} = \sum t^{n_i}\tilde{f}_i$. De plus, si $\deg(\sum f_i) = \sup deg f_i$, alors les n_i sont positifs.

Démonstration. i) et iii) sont immédiats.
ii) écrivons $F = t^N G$ où G est de degré d et n'est pas divisible par t. On a $G = \sum_{i=0}^{d} G_i t^i$ avec G_i appartenant à S et homogène de degré $d - i$.
Alors si on pose $f = F(X_1, \ldots, X_n, 1) = G(X_1, \ldots, X_n, 1) = \sum_{i=0}^{d} G_i$, les G_i sont les composantes homogènes de f.
On en déduit $\tilde{f} = G$ et $F = t^N F(X_1, \ldots, X_n, 1)\tilde{)}$.
iv) Posons $d_i = \deg f_i$. Si $f = \sum f_i$ est de degré d on a :

$$\tilde{f} = t^d f(X_1/t^{a_1}, \ldots, X_n/t^{a_n}) = t^d \sum f_i(X_1/t^{a_1}, \ldots, X_n/t^{a_n}) = \sum t^{d-d_i} \tilde{f}_i$$

où $d - d_i \in \mathbb{Z}$ et si $d = \sup d_i$, $d - d_i \in \mathbb{N}$.

□

Notation 5.5.5. Pour tout $f \in S$ non nul, on pose $f_\infty = \tilde{f}(X_1, \ldots, X_n, 0)$ qui est la composante homogène de plus haut degré de f. On posera aussi $0_\infty = 0$.

Définition 5.5.6. Soit I un idéal de S. L'homogénéisé de I, noté $\tilde{I}$ est l'idéal de $S[t]$ engendré par les homogénéisés des éléments de I.
L'idéal "à l'infini" de $\tilde{I}$ est $I_\infty = \tilde{I} + (t)$, qu'on peut considérer comme un idéal de S.
Les deux idéaux $\tilde{I}$ et I_∞ sont homogènes.

Proposition 5.5.7. *Soient I un idéal de S et F un polynôme homogène de $S[t]$. Les propriétés suivantes sont équivalentes :*
i) $F \in \tilde{I}$,
ii) $F(X_1, \ldots, X_n, 1) \in I$,
iii) il existe $f \in I$ et $N \in \mathbb{N}$ tels que $F = t^N \tilde{f}$.

Démonstration. i) $\Rightarrow$ ii) Soit $F \in \tilde{I}$ homogène. On peut écrire $F = \sum \tilde{f}_i G_i$ où les f_i (en nombre fini) sont des éléments de I et les G_i des polynômes homogènes de $S[t]$. On a alors :

$$\begin{aligned} F(X_1, \ldots, X_n, 1) &= \sum \tilde{f}_i(X_1, \ldots, X_n, 1) G_i(X_1, \ldots, X_n, 1) \\ &= \sum f_i(X_1, \ldots, X_n) G_i(X_1, \ldots, X_n, 1) \end{aligned}$$

et $F(X_1, \ldots, X_n, 1) \in I$.
ii) $\Rightarrow$ iii) On a pour tout F homogène $F = t^N F(X_1, \ldots, X_n, 1)\tilde{)}$ d'où le résultat si $F(X_1, \ldots, X_n, 1) \in I$.
iii) $\Rightarrow$ i) est immédiat puisque $\tilde{f}$ appartient à $\tilde{I}$ si $f \in I$. □

Proposition 5.5.8. *Soient I un idéal de S et F un polynôme homogène de $S[t]$. Les propriétés suivantes sont équivalentes :*
i) $F \in I_\infty$,
ii) il existe $f \in I$ tel que $F - f_\infty$ soit divisible par t.

Démonstration. $i) \Rightarrow ii)$ On a $I_\infty = \tilde{I} + (t)$ donc d'après 5.5.7 il existe $f \in I$, $N \in \mathbb{N}$ et $F' \in S[t]$ tels qu'on ait $F = t^N \tilde{f} + tF'$. Si $N > 0$, on a $F \in (t)$. Si $N = 0$ on a :

$$F - f_\infty = \tilde{f} - f_\infty + tF' \in (t).$$

$ii) \Rightarrow i)$ est analogue. □

Proposition 5.5.9. *Soient $I = (f_1, \ldots, f_s)$ un idéal de S et I' l'idéal de $S[t]$ engendré par $(\tilde{f_1}, \ldots, \tilde{f_s})$. Alors on a :*

$$\tilde{I} = (I' : t^\infty) := \{F \in S[t] \mid \exists m \in \mathbb{N},\ t^m F \in I'\} \quad \textit{et} \quad \tilde{I} = (\tilde{I} : t^\infty)$$

Démonstration. On a évidemment $I' \subseteq \tilde{I}$ donc $(I' : t^\infty) \subseteq (\tilde{I} : t^\infty)$.
Soit $f \in I$. On peut écrire $f = \sum f_i g_i$ et il existe des $n_i \in \mathbb{Z}$ tels que $\tilde{f} = \sum t^{n_i} \tilde{f_i} \tilde{g_i}$. Pour $N \gg 0$, on a $N + n_i \in \mathbb{N}$ pour tout i donc $t^N \tilde{f} \in I'$. D'où l'inclusion

$$\tilde{I} \subseteq (I' : t^\infty) \subseteq (\tilde{I} : t^\infty).$$

Inversement soit F homogène dans $(\tilde{I} : t^\infty)$. Il existe donc N tel que $t^N F \in \tilde{I}$. D'après 5.5.7, on a $1^N F(X_1, \ldots, X_n, 1) \in I$ et $F \in \tilde{I}$. Donc $\tilde{I}$ et $(\tilde{I} : t^\infty)$ qui ont les mêmes éléments homogènes sont égaux. □

Remarque 5.5.10. Il peut bien sûr arriver que I' et $\tilde{I}$ soient différents. Considérons l'idéal $I = (X_1^4 + X_2^2, 1 + X_1^3 X_2)$ de $S = k[X_1, X_2]$ muni du degré habituel.
Alors $I' = (X_1^4 + t^2 X_2^2, t^4 + X_1^3 X_2)$.
Soient

$$f = X_2(X_1^4 + X_2^2) - X_1(1 + X_1^3 X_2) = X_2^3 - X_1 \quad \tilde{f} = X_2^3 - t^2 X_1.$$

Si $\tilde{f} \in I'$, il existe deux polynômes A et B de $S[t]$ tels qu'on ait :

$$X_2^3 - t^2 X_1 = A(X_1^4 + t^2 X_2^2) + B(t^4 + X_1^3 X_2).$$

En égalisant les coefficients de X_1, considérés comme des polynômes en X_2 et t, on obtient que t^2 appartient à l'idéal $(t^2 X_1^2, t^4)$, d'où une contradiction.

Cependant il y a un cas où on sait que I' et $\tilde{I}$ sont égaux, c'est-à-dire que $\tilde{I}$ est engendré par $(\tilde{f_1}, \ldots, \tilde{f_s})$.

Proposition 5.5.11. *Un ordre monomial étant choisi sur S, on met sur les monômes de $S[t]$ l'ordre défini de la manière suivante : soient m et m' deux monômes de S, d et d' deux entiers, on dit que $mt^d > mt^{d'}$ si $m > m'$ ou $m = m'$ et $d > d'$. C'est un ordre monomial qui étend celui de S.*

Remarque 5.5.12. Soit $f \in S$ non nul qu'on écrit en faisant apparaitre ses composantes homogènes :
$f = f_d + f_{d-1} + \cdots + f_0$ avec $f_d \neq 0$. On a $\tilde{f} = f_d + t f_{d-1} + \cdots + t^d f_0$ et $f_\infty = f_d$.
Si f et son terme initial $\operatorname{in} f$ ont même degré, alors on a $\operatorname{in} f = \operatorname{in} \tilde{f} = \operatorname{in} f_\infty$. C'est vrai en particulier si l'ordre monomial de S est compatible avec le degré, c'est-à-dire que pour tous monômes m et m', si $\deg m > \deg m'$, alors $m > m'$.

Proposition 5.5.13. *On choisit un ordre monomial sur S et on l'étend à $S[t]$ comme ci-dessus. Soient I un idéal de S et $(f_1, \dots, f_s)$ une base de Gröbner de I. Si pour tout $i \in [1, s]$, f_i et son terme initial $\operatorname{in} f_i$ ont même degré, alors :*
i) $\operatorname{in}\tilde{I}$ est l'idéal de $S[t]$ engendré par $\operatorname{in} I$ et $(\tilde{f}_1, \dots, \tilde{f}_s)$ est une base de Gröbner de $\tilde{I}$.
ii) Si de plus l'ordre est compatible avec le degré $\operatorname{in} I_\infty = \operatorname{in} I + (t)$ et $(f_{1,\infty}, \dots, \tilde{f}_{s,\infty}, t)$ est une base de Gröbner de I_∞.

Démonstration. On a $\operatorname{in} f_i = \operatorname{in} \tilde{f}_i$ donc $\operatorname{in} f_i \in \operatorname{in} \tilde{I}$.
Puisque $\tilde{I}$ est homogène, son idéal initial est engendré par les termes initiaux de ses éléments homogènes. Un tel polynôme homogène est de la forme $t^N \tilde{f}$ avec $f \in I$. Donc l'idéal initial $\operatorname{in}\tilde{I}$ est engendré par les $t^N \operatorname{in} \tilde{f}$, ou encore par les $\operatorname{in} \tilde{f}$ avec $f \in I$.
Soit $f \in I$ non nul. Puisque $(f_1, \dots, f_s)$ est une base de Gröbner de I, on peut écrire $f = \sum h_i f_i$ où pour tout $i \in [1, s]$ les monômes de $h_i \operatorname{in} f_i$ ne sont divisibles par aucun des $\operatorname{in} f_j$ pour $j < i$. Soit $\delta = \sup \deg h_i f_i$.
Si le degré de f est $< \delta$, la somme des composantes homogènes de degré δ des $h_i f_i$ est nulle, donc on a, en notant d_i le degré commun de f_i et $\operatorname{in} f_i$:

$$\sum \pi_{\delta - d_i}(h_i)\pi_{d_i}(f_i) = 0$$

où les $\pi_{\delta-d_i}(h_i)$ ne sont pas tout nuls. Il existe donc (cf. 2.3.7) $i \neq j$ tels que

$$\exp\left(\pi_{\delta-d_i}(h_i)\pi_{d_i}(f_i)\right) = \exp\left(\pi_{\delta-d_j}(h_j)\pi_{d_j}(f_j)\right)$$

$$\exp \pi_{\delta-d_i}(h_i) + \exp \pi_{d_i}(f_i) = \exp \pi_{\delta-d_j}(h_j) + \exp \pi_{d_j}(f_j)$$

Puisque f_i et $\operatorname{in} f_i$ ont même degré d_i, $\operatorname{in} f_i$ est un monôme de la composante homogène de degré d_i de f_i, donc $\exp \pi_{d_i}(f_i) = \exp(f_i)$. D'autre part, $\exp \pi_{\delta-d_i}(h_i)$ est l'exposant d'un monôme non nul m de h_i. Pour ce monôme, $m \operatorname{in} f_i$ est divisible par $\operatorname{in} f_j$ ce qui donne une contradiction.
Le degré de f est donc égal à δ. Alors, $\tilde{f} = \sum t^{n_i} \tilde{h}_i \tilde{f}_i$ avec $n_i \in \mathbb{N}$ pour tout i (cf.5.5.4). De plus, puisque les exposants des $h_i f_i$ (pour l'ordre sur S) sont tous distincts, il en est de même des exposants des $t^{n_i}\tilde{h}_i\tilde{f}_i$ (pour l'ordre sur $S[t]$) donc le terme initial de $\tilde{f}$ est égal à l'un des $t^{n_i} \operatorname{in} h_i \operatorname{in} f_i$.
L'idéal $\operatorname{in}\tilde{I}$ est donc engendré par $(\operatorname{in} f_1, \dots, \operatorname{in} f_s)$ et $(\tilde{f}_1, \dots, \tilde{f}_s)$ est une base de Gröbner de $\tilde{I}$. Supposons maintenant l'ordre compatible avec le degré. Soit encore $f \in I$ non nul. Puisque $\operatorname{in} f = \operatorname{in} f_\infty$, $\operatorname{in} f \in I_\infty$ et $\operatorname{in} I + (t) \subseteq \operatorname{in} I_\infty$.
Inversement soit $F \in I_\infty$ homogène. D'après 5.5.8 il existe $f \in I$ et F' tels qu'on ait $F = f_\infty + tF'$. Le terme initial $\operatorname{in} F$ est soit un terme de tF', et dans ce cas il est divisible par t, soit le terme initial $\operatorname{in} f_\infty = \operatorname{in} f$ de f_∞.
Alors $\operatorname{in} I_\infty = \operatorname{in} I + (t) = (\operatorname{in} f_{1,\infty}, \dots, \operatorname{in} f_{s,\infty}, t)$ et $(f_{1,\infty}, \dots, \tilde{f}_{s,\infty}, t)$ est une base de Gröbner de I_∞.

□

Clôture projective et idéal à l'infini

La situation est la suivante : on considère $\mathbb{A}^n$ l'espace affine de dimension n plongé dans l'espace projectif $\mathbb{P}^n$, une sous-variété fermée V de $\mathbb{A}^n$ définie par un idéal I de S, et on veut déterminer la clôture algébrique $\widetilde{V}$ de V dans $\mathbb{P}^n$, ainsi que l'intersection V_∞ de $\widetilde{V}$ avec l'hyperplan à l'infini de $\mathbb{P}^n$. Alors si on met sur S le degré habituel (les degrés des indéterminées $X_1, \ldots, X_n$ sont tous égaux à 1), $\widetilde{V}$ (resp. V_∞) est définie par l'idéal homogène $\tilde{I}$ (resp. I_∞). On a donc montré :

Proposition 5.5.14. *On choisit sur S un ordre compatible avec le degré (par exemple hlex ou revlex). Soient I un idéal de S, $\tilde{I}$ l'homogénéisé de I et $I_\infty = \tilde{I} + (t)$. Soit $(f_1, \ldots, f_s)$ une base de Gröbner de I. On a :*
– *$in\,\tilde{I} = (in\,I)S[t]$ et $(\tilde{f}_1, \ldots, \tilde{f}_s)$ est une base de Gröbner de $\tilde{I}$,*
– *$in\,I_\infty = in\,I + (t)$ et $(f_{1,\infty}, \ldots, \tilde{f}_{s,\infty}, t)$ est une base de Gröbner de I_∞.*

Exemple 5.5.15. On choisit $n = 3$ et $I = (X_2 - X_1^2, X_3 - X_1^3)$ qui est l'idéal de la "cubique gauche" affine C, paramétrée par $X_2 = X_1^2$, $X_3 = X_1^3$. Désignons par f_1 et f_2 les deux équations.
On a

$$\tilde{f}_1 = X_2 t - X_1^2 \quad \tilde{f}_2 = X_3 t - X_1^3 \quad f_{1,\infty} = -X_1^2 \quad f_{2,\infty} = -X_1^3.$$

On voit que la variété projective définie par l'idéal $(\tilde{f}_1, \tilde{f}_2)$ contient un plan d'idéal (X_1, t) donc n'est pas la clôture projective de C.
Choisissons l'ordre lexicographique homogène. On a :

$$S(f_1, f_2) = f_2 - X_1 f_1 = X_3 - X_1 X_2 = f_3$$

$$S(f_1, f_3) = X_1 f_3 - X_2 f_1 = X_1 X_3 - X_2^2 = f_4$$

$$S(f_2, f_3) = X_1^2 f_3 - X_2 f_2 = X_1^2 X_3 - X_2 X_3 = -X_3 f_1.$$

On vérifie que (f_1, f_2, f_3, f_4) est une base de Gröbner de I et (f_1, f_3, f_4) une base de Gröbner minimale.
On a :

$$\tilde{f}_3 = X_3 t - X_1 X_2 \quad \tilde{f}_4 = X_1 X_3 - X_2^2 \quad f_{3,\infty} = -X_1 X_2 \quad f_{4,\infty} = f_4 = X_1 X_3 - X_2^2.$$

La variété projective $\tilde{C}$ est donc définie par l'idéal $(\tilde{f}_1, \tilde{f}_3, \tilde{f}_4)$. Elle coupe le plan à l'infini suivant la variété C_∞ définie par l'idéal $(X_1^2, X_1 X_2, X_1 X_3 - X_2^2)$ et cette variété est portée par le point $X_1 = X_2 = 0$.

5.6 Construction d'une famille plate

Dans les applications que nous venons de voir, nous avons montré des propriétés d'un idéal en les déduisant de celles de son idéal initial. Cela vient du fait que ces idéaux sont proches algébriquement, en un sens que nous allons préciser dans ce paragraphe. Commençons par un exemple.

Exemple 5.6.1. Dans le plan projectif, l'idéal $(X_1X_3-X_2^2)$ (ou l'équation $X_1X_3-X_2^2=0$) définit une conique. Introduisons un paramètre t et regardons la "famille de courbes" définie par le polynôme $tX_1X_3-(1-t)X_2^2$:
– Pour $t\neq 0$ et $t\neq 1$, c'est une conique lisse.
– Pour $t=0$, c'est une droite double.
– Pour $t=1$, c'est la réunion de deux droites.
D'autre part, pour l'ordre lexicographique on a $\operatorname{in}(X_1X_3-X_2^2)=X_1X_3$ (qui définit la réunion de deux droites) et pour l'ordre lexicographique inverse on a $\operatorname{in}(X_1X_3-X_2^2)=-X_2^2$ (qui définit une droite double).

Nous allons montrer que c'est un résultat général :

Théorème 5.6.2. *On fixe un ordre monomial sur S. Soit I un idéal de S. Il existe une famille plate sur $k[t]$ dont la fibre pour $t\neq 0$ est isomorphe à S/I et la fibre pour $t=0$ isomorphe à $S/\operatorname{in} I$.*

Commentaire 5.6.3. L'énoncé du théorème signifie qu'il existe un idéal J de $S[t]$ tel que $S[t]/J$ soit *plat* sur $k[t]$ et qu'on ait des isomorphismes de k-algèbres :

$$S/J_\lambda \simeq S/I \quad \text{pour } \lambda\neq 0 \text{ et} \quad S/J_0\simeq S/\operatorname{in} I$$

où J_λ (resp. J_0) est l'idéal obtenu en remplaçant t par λ (resp. par 0) dans les équations d'un système de générateurs de J.

Rappel 5.6.4. On dit que $S[t]/J$ est *plat* sur $k[t]$ si pour tout $\lambda\in k$, $t-\lambda$ n'est pas diviseur de zéro dans $S[t]/J$, ou encore si :

$$\forall\lambda\in k,\forall F\in S[t],\ (t-\lambda)F\in J\Rightarrow F\in J.$$

La notion algébrique de platitude correspond à la notion topologique de continuité.

Exemple 5.6.5. $k[t,X_1,X_2,X_3]/(tX_1X_3-(1-t)X_2^2)$ est plat sur $k[t]$.
En effet, soient $F\in S[t]$, $G\in S[t]$ et $\lambda\in k$ tels qu'on ait :

$$(t-\lambda)F=(tX_1X_3-(1-t)X_2^2)G.$$

Si on fait $t=\lambda$ on obtient :

$$(\lambda X_1X_3-(1-\lambda)X_2^2)G(\lambda,X_1,X_2,X_3)=0.$$

Quel que soit λ, le polynôme (de S) $\lambda X_1X_3-(1-\lambda)X_2^2$ n'est pas nul , donc on a $G(\lambda,X_1,X_2,X_3)=0$ et G est divisible par $t-\lambda$, $G=(t-\lambda)G'$. On a donc :

$$F=(tX_1X_3-(1-t)X_2^2)G'.$$

Exemple 5.6.6. $k[t, X_1, X_2, X_3]/(X_1^3, X_1^2X_2 - tX_2^3)$ n'est pas plat sur $k[t]$.
Soit $F = X_1X_2^3$. On a :

$$tF = X_1^3X_2 - X_1(X_1^2X_2 - tX_2^3) \in (X_1^3, X_1^2X_2 - tX_2^3).$$

Supposons qu'il existe G et H tels qu'on ait :

$$F = X_1X_2^3 = X_1^3G + (X_1^2X_2 - tX_2^3)H$$

et faisons $t = 0$. On en déduit :

$$X_1X_2^3 = X_1^3G(0, X_1, X_2, X_3) + X_1^2X_2H(0, X_1, X_2, X_3)$$

et X_1^2 divise $X_1X_2^3$ d'où une contradiction. Donc t est diviseur de zéro dans le quotient $k[t, X_1, X_2, X_3]/(X_1^3, X_1^2X_2 - tX_2^3)$.

Pour démontrer le théorème nous aurons besoin d'un résultat technique préalable :

Lemme 5.6.7. *Soit U un ensemble fini d'exposants de $\mathbb{N}^n$. Il existe des entiers strictement positifs $a_1, \ldots, a_n$ tels qu'on ait :*

$$\forall \alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n) \in U \quad \alpha > \beta \Rightarrow \sum_{i=1}^{n} a_i\alpha_i > \sum_{i=1}^{n} a_i\beta_i$$

Démonstration. On considère $B = \{\alpha - \beta \mid \alpha > \beta\} \subseteq \mathbb{Z}^n$, qui est le cône positif associé à l'ordre monomial, et les deux ensembles :

$$B_U = \{\alpha - \beta \mid \alpha, \beta \in U, \alpha > \beta\} \subseteq B$$

$$B'_U = B_U \cup (1, 0, \ldots, 0) \cup (0, 1, 0, \ldots, 0) \cdots \cup (0, \ldots, 0, 1).$$

Puisque pour tout $i \in [1, n]$, $X_i > 1$, on a $\exp X_i > \exp 1 = (0, \ldots, 0)$ donc les n éléments $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0) \ldots, (0, \ldots, 0, 1)$ sont dans B et B'_U est aussi contenu dans B.
Montrons que l'enveloppe convexe de B'_U dans $\mathbb{Q}^n$ ne contient pas 0. Sinon, il existe une relation :

$$\sum_{j=1}^{r} q_jb_j = 0 \quad \text{avec} \quad b_j \in B'_U, q_j \in \mathbb{Q}_+, \quad \text{et} \quad \sum q_j = 1$$

ou encore, quitte à supprimer les dénominateurs, il existe des entiers positifs m_j non nuls avec $\sum_{j=1}^{r} m_jb_j = 0$. Quitte à autoriser des répétitions, on peut supposer $m_j = 1$ pour tout j.
Posons $b_j = \alpha_j - \beta_j$. On a donc $\sum(\alpha_j - \beta_j) = 0$ et on peut écrire :

$$\begin{aligned}
\gamma_1 &= \beta_1 + \cdots + \beta_r \\
\gamma_2 &= \alpha_1 + \beta_2 + \cdots + \beta_r = \gamma_1 + (\alpha_1 - \beta_1) \\
&\cdots\cdots\cdots\cdots \\
\gamma_{r+1} &= \alpha_1 + \cdots + \alpha_r = \gamma_r + (\alpha_r - \beta_r)
\end{aligned}$$

Puisque pour tout i, $\alpha_i - \beta_i > 0$, on a :

$$\gamma_1 < \gamma_2 < \cdots < \gamma_{r+1} = \gamma_1$$

d'où une contradiction.
Puisque l'enveloppe convexe de B'_U dans $\mathbb{Q}^n$ ne contient pas 0, on peut séparer B'_U de 0 par un hyperplan, donc il existe des entiers $a_1, \ldots, a_n$ tels qu'on ait $\sum_i a_i b_i > 0$ pour tout $b \in B'_U$. Celà donne en particulier :

$$\forall \alpha,\, \beta \in U \quad \alpha > \beta \Rightarrow \sum_{i=1}^{n} a_i \alpha_i > \sum_{i=1}^{n} a_i \beta_i$$

et pour tout $i \in [1, n]$, $a_i > 0$. □

Exemples 5.6.8. On choisit $n = 2$ et l'ordre lexicographique. On considère l'ensemble ordonné de monômes :

$$X_1^5 > X_1^4 X_2 > X_1^3 X_2^3 > X_1^2 X_2^4$$

et on cherche a_1 et a_2 strictement positifs vérifiant :

$$5a_1 > 4a_1 + a_2 > 3a_1 + 3a_2 > 2a_1 + 4a_2.$$

Les conditions se réduisent à $a_1 > 2a_2$ et par exemple $(a_1, a_2) = (3, 1)$ convient.
On choisit $n = 2$ et l'ordre lexicographique homogène. On considère l'ensemble ordonné de monômes :

$$X_1^3 X_2^3 > X_1^2 X_2^4 > X_1^5 > X_1^4 X_2$$

et on cherche a_1 et a_2 strictement positifs vérifiant :

$$3a_1 + 3a_2 > 2a_1 + 4a_2 > 5a_1 > 4a_1 + a_2.$$

Les conditions se réduisent à $a_2 < a_1 < \frac{4}{3} a_2$ et par exemple $(a_1, a_2) = (7, 6)$ convient.

Démonstration. (du théorème). On se donne une base de Gröbner $(f_1, \ldots, f_s)$ de I. On considère U l'ensemble (fini) des exposants des monômes des f_i, et on choisit $a_1, \ldots, a_n$ vérifiant les conditions de 5.6.7. Pour le degré pondéré défini par $a_1, \ldots, a_n$, les monômes des f_i ont donc des degrés tous distincts, et pour tout $i \in [1, s]$ le monôme de plus haut degré de f_i est $\operatorname{in} f_i$.
On étend l'ordre monomial à $S[t]$ comme en 5.5.11 et on homogénéise. Les conditions de 5.5.13 sont remplies et on en déduit que $(\tilde{f}_1, \ldots, \tilde{f}_s)$ est une base de Gröbner de $\tilde{I}$. De plus on a, pour tout $i \in [1, s]$, $\tilde{f}_i(X_1, \ldots, X_n, 0) = \operatorname{in} f_i$.
Nous allons monter que $S[t]/\tilde{I}$ est la famille plate cherchée.
L'idéal $\tilde{I}_\lambda$ (resp. $\tilde{I}_0$) est l'idéal obtenu en remplaçant t par λ (resp. par 0) dans les $\tilde{f}_i$, donc il est immédiat que $\tilde{I}_0$ est l'idéal $\operatorname{in} I$. Il reste à étudier $\tilde{I}_\lambda$.
Rappelons que si f est un élément non nul de S de degré pondéré d, on a

$$\tilde{f} = t^d f(X_1/t^{a_1}, \ldots, X_n/t^{a_n}) \quad \tilde{f}(X_1, \ldots, X_n, \lambda) = \lambda^d f(X_1/\lambda^{a_1}, \ldots, X_n/\lambda^{a_n}).$$

Pour $\lambda \neq 0$, considérons l'automorphisme φ_λ de k-algèbres de S défini par $\varphi_\lambda(X_i) = X_i/\lambda^{a_i}$. L'image d'un polynôme f non nul de degré d est $f(X_1/\lambda^{a_1}, \ldots, X_n/\lambda^{a_n}) = \lambda^{-d}\tilde{f}(X_1, \ldots, X_n, \lambda)$, donc l'image de l'idéal I est l'idéal $\tilde{I}_\lambda$ et $S/\tilde{I}_\lambda$ est isomorphe à S/I. Il reste à montrer que $S[t]/\tilde{I}$ est plat sur $k[t]$.
Rappelons (cf. 5.5.9) que $\tilde{I}$ possède la propriété suivante $\tilde{I} = (\tilde{I} : t^\infty)$. Donc en particulier $\tilde{I} = (\tilde{I} : t)$.
Soit $F \in S[t]$, $F \notin \tilde{I}$, tel qu'il existe $\lambda \in k$ avec $(t-\lambda)F \in \tilde{I}$, et supposons que F soit de degré minimum pour cette propriété. Ecrivons F en mettant en évidence ses composantes homogènes : $F = F_d + F_{d-1} + \cdots + F_0$ avec F_j homogène de degré j et $F_d \neq 0$. Puisque $\tilde{I}$ est homogène, il contient les composantes homogènes de $(t-\lambda)F \in \tilde{I}$. On a en particulier $tF_d \in \tilde{I}$ donc $F_d \in \tilde{I}$. On en déduit $(t-\lambda)(F - F_d) \in \tilde{I}$. Puisque si $F - F_d$ est non nul, son degré est strictement plus petit que celui de F, on a $F = F_d$ ce qui donne une contradiction.

□

Exemples 5.6.9. On choisit $n = 2$ et l'ordre lexicographique. Soit $I = (X_1^3, X_1^2X_2 - X_2^3)$. On a vu qu'on a in $I = (X_1^3, X_1^2X_2, X_1X_2^3, X_2^5)$. On choisit $a_1 = 3$ et $a_2 = 1$ et on construit une famille plate avec l'idéal $\tilde{I} = (X_1^3, X_1^2X_2 - t^4X_2^3, X_1X_2^3, X_2^5)$.

A titre d'exercice, le lecteur pourra construire une famille plate "reliant" l' idéal :

$$I = (X_1, X_2) \cap (X_1 - 1, X_2) \cap (X_1, X_2 - 1)$$

qui définit les 3 points $(0,0)$, $(0,1)$, $(1,0)$ du plan affine, à l'idéal $(X_1, X_2)^2$.

Chapitre 6

Idéaux initiaux génériques. Idéaux Borel-fixes

Dans tout ce chapitre, on supposera que **la caractéristique du corps k est égale à 0** et qu'un ordre monomial **compatible avec le degré** est fixé sur S.

6.1 Action du groupe linéaire

Les notions définies dans les chapitres précédents (bases de Gröbner, idéaux initiaux) dépendent non seulement de l'ordre choisi, mais encore du choix des coordonnées comme le montrent les exemples suivants :

Exemple 6.1.1. On a vu en 5.1.6 que si on choisit $n = 4$, $I = (X_1X_3 - X_2^2, X_1X_4 - X_2X_3, X_2X_4 - X_3^2)$ et l'ordre lexicographique, les trois générateurs forment une base de Gröbner et on a $\operatorname{in} I = (X_1X_3, X_1X_4, X_2X_4)$.
Si maintenant on échange X_1 et X_2, toujours pour l'ordre lexicographique, une base de Gröbner de I est formée de $(X_2X_3 - X_1^2, X_2X_4 - X_1X_3, X_1X_4 - X_3^2, X_2X_4^2 - X_3^3)$
et on a $\operatorname{in} I = (X_1^2, X_1X_3, X_1X_4, X_2X_4^2)$.

Définitions 6.1.1. Le *groupe linéaire d'ordre n*, noté GL_n, est le groupe des automorphismes de l'espace vectoriel k^n de dimension n. Il est isomorphe au groupe des matrices carrées inversibles d'ordre n.
On s'intéressera aux sous-groupes particuliers suivants :
– $\mathcal{B}_i$ sous-groupe (de Borel) des matrices triangulaires inférieures,
– $\mathcal{B}_s$ sous-groupe des matrices triangulaires supérieures,
– $\mathcal{D}$ sous-groupe des matrices diagonales.

Définition 6.1.2. *Le groupe linéaire* agit sur S *(par changement de variable) de la manière suivante : soient $g \in GL_n$ défini par $g(X_i) = \sum_j g_{ij}X_j$ et $f \in S$; on pose*

$$g(f) = f(g(X_1), \ldots, g(X_n)).$$

Si I est un idéal de S, on note $g(I) = \{g(f) \mid f \in I\}$ qui est encore un idéal.

Exemple 6.1.3. On a défini en section 5.4 l'homogénéisé $\tilde{f}$ d'un élément f de S relativement à un degré pondéré défini par $\deg X_i = a_i$. Il vérifie en particulier, si λ est un scalaire non nul,

$$\tilde{f}(X_1, \dots, X_n, \lambda) = \lambda^d f(X_1/\lambda^{a_1}, \dots, X_n/\lambda^{a_n})$$

qu'on peut encore écrire $\tilde{f}(X_1, \dots, X_n, \lambda) = \lambda^d g_\lambda(f)$ où g_λ est l'élément diagonal de GL_n défini par $g_\lambda(X_i) = X_i/\lambda^{a_i}$.
En particulier la fibre pour $\lambda \neq 0$ de la famille plate construite en 5.6.2, famille qui relie un idéal I à son idéal initial $\operatorname{in} I$, est définie par l'idéal $g_\lambda(I)$.

On s'intéressera en particulier à la restriction de cette action aux sous-groupes $\mathcal{B}_i$, $\mathcal{B}_s$ et $\mathcal{D}$.

Lemme 6.1.4. *On a les propriétés suivantes :*
i) Soit $g \in \mathcal{B}_s$; pour tout $f \in S$ non nul on a $\exp g(f) = \exp f$; pour tout idéal I non nul de S on a $\operatorname{in} g(I) = \operatorname{in} I$.
ii) Soit $g \in \mathcal{B}_i$; pour tout monôme m de S il existe un scalaire $\lambda \neq 0$ tel que tous les termes non nuls de $g(m) - \lambda m$ soient $> m$; en particulier on a $\exp g(m) \geqslant \exp m$.
iii) Soit $g \in GL_n$; alors $g \in \mathcal{B}_s \Leftrightarrow \exp g(X_1) > \exp g(X_2) > \cdots > \exp g(X_n)$.
iv) Un idéal est stable par l'action de $\mathcal{D}$ si et seulement si il est monomial.

Démonstration. i) Soit $g \in \mathcal{B}_s$. On a $g(X_i) = \sum_{j \geqslant i} g_{ij} X_j$ et en particulier $\operatorname{in} g(X_i) = g_{ii} X_i$, $\exp g(X_i) = \exp X_i$.
Soit $m = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un monôme. On a

$$g(m) = \prod_{i=1}^{n} g(X_i)^{\alpha_i} \quad , \quad \exp g(m) = \sum_{i=1}^{n} \alpha_i \exp g(X_i) = \exp m.$$

Soit $f = \sum_{i=1}^{r} \lambda_i m_i$ où les m_i sont des monômes avec

$$m_1 > m_2 > \cdots > m_r \quad \text{et} \quad \lambda_i \neq 0.$$

On a $g(f) = \sum_{i=1}^{r} \lambda_i g(m_i)$ et $\exp g(f) = \exp g(m_1) = \exp m_1 = \exp f$.
ii) Soit $g \in \mathcal{B}_i$. On a $g(X_i) = \sum_{j \leqslant i} g_{ij} X_j$ et en particulier $\exp g(X_i) \geqslant \exp X_i$.
Soit $m = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un monôme. On a

$$g(m) = \prod_{i=1}^{n} g(X_i)^{\alpha_i} \quad , \quad \exp g(m) = \sum_{i=1}^{n} \alpha_i \exp g(X_i) \geqslant \exp \sum_{i=1}^{n} \alpha_i \exp X_i = \exp m.$$

iii) Soit $g \in GL_n$ tel que $\exp g(X_1) > \exp g(X_2) > \cdots > \exp g(X_n)$. Puisque $g(X_1), \dots, g(X_n)$ sont des formes linéaires, leurs termes initiaux sont des monômes de degré 1 (multipliés par une constante non nulle) et nécessairement $\exp g(X_i) = \exp X_i$ pour tout i. Celà entraîne que $g(X_i)$ ne fait intervenir que des X_j avec $j \geqslant i$, et $g \in \mathcal{B}_s$.
iv) Soient $g \in \mathcal{D}$ et m un monôme. Il existe $\lambda \neq 0$ tel qu'on ait $g(m) = \lambda m$. Si I est un idéal monomial, il est engendré par des monômes $(m_1, \dots, m_r)$. On a $g(I) = (g(m_1), \dots, g(m_r)) = (m_1, \dots, m_r) = I$.
Inversement, soit I un idéal non nul stable par $\mathcal{D}$, ce qu'on peut écrire :

$$\forall f \in I \quad \forall \lambda_1 \dots \lambda_n \quad \text{tous non nuls} \quad f(\lambda_1 X_1, \dots, \lambda_n X_n) \in I.$$

Soient $(f_1, \dots f_r)$ une base de Gröbner réduite de I et $g \in \mathcal{D}$. Puisque $\operatorname{in} g(f_i)$ et $\operatorname{in} f_i$ sont proportionnels, $(g(f_1), \dots g(f_r)$ est une base de Gröbner de $g(I) = I$, réduite à normalisation près. On en déduit, à cause de l'unicité d'une telle base, que pour tout i, il existe $a_i \neq 0$ tel que $g(f_i) = a_i f_i$. Nous allons montrer que celà entraîne que les f_i sont des monômes donc que I est un idéal monomial.
Soit par exemple $f_1 = \lambda_1 m_1 + \dots + \lambda_k m_k$ où les m_i sont des monômes avec

$$m_1 > m_2 > \dots > m_k \quad \text{et} \quad \lambda_i \neq 0.$$

On a

$$g(f_1) = \lambda_1 g(m_1) + \dots + \lambda_k g(m_k) = a_1 f_1 \quad \text{et} \quad \exp g(m_1) > \exp g(m_2) > \dots > \exp g(m_k).$$

Alors nécessairement $g(m_1) = a_1 m_1, \dots, g(m_k) = a_1 m_k$.
On a donc montré que pour tout $g \in \mathcal{D}$, il existe a_1 (dépendant de g) tel qu'on ait $g(m_1) = a_1 m_1, \dots, g(m_k) = a_1 m_k$. Supposons que k soit supérieur ou égal à 2 et posons $m_1 = X_1^{\alpha_1} \dots X_n^{\alpha_n}$, $m_2 = X_1^{\beta_1} \dots X_n^{\beta_n}$. Alors pour tous $\lambda_1 \dots \lambda_n$ tous non nuls, on a

$$\lambda_1^{\alpha_1} \dots \lambda_n^{\alpha_n} = \lambda_1^{\beta_1} \dots \lambda_n^{\beta_n}$$

$$\lambda_1^{\alpha_1 - \beta_1} \dots \lambda_n^{\alpha_n - \beta_n} = 1$$

ce qui est impossible si le corps est infini.
Donc $k = 1$ et f_1 est un monôme.

□

Remarque 6.1.5. La propriété ii) n'est pas vraie pour un polynôme quelconque. Choisissons par exemple $n = 2$ et l'ordre lexicographique.
Soient $f = X_1^2 - X_2^2$ et g défini par $g(X_1) = X_1$, $g(X_2) = X_1 + X_2$. On a

$$g(f) = X_1^2 - (X_1 + X_2)^2 = -2X_1X_2 - X_2^2$$

et $\operatorname{in} g(f) = -2X_1X_2$, $\operatorname{in} f = X_1^2$ et $\exp g(f) < \exp f$.

6.2 Idéaux initiaux génériques

Nous allons montrer le théorème suivant, du à Galligo :

Théorème 6.2.1. *Pour tout idéal homogène I, il existe un ouvert de Zariski non vide U de GL_n, stable par $\mathcal{B}_s$, et un idéal monomial J de S tels que pour tout $g \in U$ on ait $\operatorname{in} g(I) = J$.*

Définition 6.2.2. Avec les notations de 6.2.1, l'idéal J est appelé *idéal initial générique de I* et noté $\operatorname{gin} I$.

Nous commençons par montrer plusieurs lemmes techniques :

Lemme 6.2.3. *Soit J un idéal monomial de S, m_1, ..., m_N des monômes de degré d, deux à deux distincts, qui engendrent un sous-espace vectoriel noté $< m_1, \ldots, m_N >$ de S_d. Alors on a :*

$$dim\, J_d \cap < m_1, \ldots, m_N >= \ card\, J_d \cap \{m_1, \ldots, m_N\}.$$

Démonstration. Puisque l'espace vectoriel $J \cap < m_1, \ldots, m_N >$ contient l'ensemble $J \cap \{m_1, \ldots, m_N\}$, il contient également l'espace vectoriel engendré par cet ensemble, noté $< J \cap \{m_1, \ldots, m_N\} >$. Donc on a l'inclusion :

$$< J \cap \{m_1, \ldots, m_N\} > \subseteq \ J \cap < m_1, \ldots, m_N > .$$

Inversement soit f un élément de $J \cap < m_1, \ldots, m_N >$. On a donc $f = \sum_{i=1}^{N} \lambda_i m_i \in J$. Puisque J est monomial, on en déduit que pour tout $i \in [1, N]$, on a :
– ou bien $\lambda_i = 0$
– ou bien $m_i \in J \cap \{m_1, \ldots, m_N\}$, et donc $f \in < J \cap \{m_1, \ldots, m_N\} >$.
On a donc l'inclusion inverse :

$$J \cap < m_1, \ldots, m_N > \subseteq < J \cap \{m_1, \ldots, m_N\} > .$$

Ces deux sous-espaces vectoriels sont donc égaux, ainsi que leurs dimensions.

□

Lemme 6.2.4. *Soient I un idéal homogène de S, m_1, ..., m_N les monômes de degré d rangés par ordre décroissant, $k \leqslant N$ et p_k la projection de S_d sur le sous-espace vectoriel $< m_1, \ldots, m_k >$ parallèlement au sous-espace vectoriel $< m_{k+1}, \ldots, m_N >$. Alors on a :*

$$\dim p_k(I_d) = \ dim(in\, I \cap < m_1, \ldots, m_k >) = \ card\,(in\, I \cap \{m_1, \ldots, m_k\}).$$

Démonstration. L'intersection $\mathrm{in}\, I \cap \{m_1, \ldots, m_k\}$, si elle n'est pas vide, est formée de r termes initiaux d'éléments de I, soient $\mathrm{in}\, f_1$, ...,$\mathrm{in}\, f_r$ qu'on peut supposer rangées par ordre décroissant :

$$\mathrm{in}\, f_1 > \cdots > \mathrm{in}\, f_r \geqslant m_k.$$

Puisque l'ordre est compatible avec le degré, on peut supposer que le f_i sont homogènes de degré d. Nous allons montrer que $p_k(f_1)$, ...,$p_k(f_r)$ sont linéairement indépendants. Sinon il existe des scalaires λ_i non tous nuls tels qu'on ait $\sum \lambda_i p_k(f_i) = 0$. Alors
– ou bien $\sum \lambda_i f_i = 0$
– ou bien tous les monômes de $\sum \lambda_i f_i$ sont dans l'espace vectoriel $< m_{k+1}, \ldots, m_N >$, donc sont plus petits que m_k et ne peuvent être l'un des $\mathrm{in}\, f_i$. En particulier on a $\exp \sum \lambda_i f_i < \sup \exp f_i$.
Dans les deux cas on en déduit que il existe deux indices i et j avec $\mathrm{in}\, f_i = \mathrm{in}\, f_j$,ce qui donne une contradiction.
Montrons par récurrence que pour tout $f \in I_d$, $p_k(f_1)$, ...,$p_k(f_r)$ et $p_k(f)$ sont liés.
– C'est vrai pour $f = 0$.

– Soit $f \neq 0$. C'est encore vrai si $p_k(f) = 0$. Sinon f possède des monômes supérieurs ou égaux à m_k. Son terme initial est aussi supérieur ou égal à m_k, donc appartient à $\operatorname{in} I \cap \{m_1, \ldots, m_k\}$ autrement dit il existe i tel qu'on ait $\operatorname{in} f = \lambda_i \operatorname{in} f_i$.
On a $\exp(f - \lambda_i f_i) < \exp f$ et par hypothèse de récurrence, $p_k(f_1)$, …,$p_k(f_r)$ et $p_k(f - \lambda_i f_i)$ sont liés d'où le résultat.

Donc la dimension de $p_k(I_d)$ est égale à r.
Si l'intersection $\operatorname{in} I \cap \{m_1, \ldots, m_k\}$ est vide, tout élément de I_d a un terme initial inférieur à m_k donc contenu dans l'espace vectoriel $< m_{k+1}, \ldots, m_N >$, et $p_k(I_d)$ est nul.
La deuxième égalité est le résultat de 6.2.3. □

On obtient en particulier le corollaire suivant, qui est un raffinement du fait que les dimensions de I_d et $(\operatorname{in} I)_d$ sont égales.

Corollaire 6.2.5. *Avec les mêmes notations qu'au lemme ci-dessus, les dimensions de $p_k(I_d)$ et $p_k((in\, I)_d)$ sont égales.*

Démonstration. On applique le résultat du lemme à la fois à I et à $\operatorname{in} I$. □

Remarque 6.2.6. Pour calculer la dimension de $(\operatorname{in} I \cap < m_1, \ldots, m_k >)$ on procède donc de la manière suivante : on range les monômes de degré d par ordre décroissant, ce qui donne une base de S_d. On écrit I_d dans cette base, et on obtient ainsi une matrice $M(I_d)$, qui a un nombre de lignes égal à la dimension de I_d et $\binom{n+d-1}{d}$ colonnes.
La dimension de $(\operatorname{in} I \cap < m_1, \ldots, m_k >)$ est égale au rang de la sous-matrice $M_k(I_d)$ formée des k premiers vecteurs colonnes de $M(I_d)$.

Lemme 6.2.7. *Soient J et J' deux idéaux monomiaux et d_0 un entier. Si pour tout $d \leqslant d_0$, pour tout $k \in \mathbb{N}$, si m_1, …, m_k sont les k premiers monômes de degré d rangés par ordre décroissant, les deux ensembles $J \cap \{m_1, \ldots, m_k\}$ et $J' \cap \{m_1, \ldots, m_k\}$ ont le même cardinal, alors les idéaux engendrés par les monômes de degré $\leqslant d_0$ de J et J' sont égaux.*
En particulier $J = J'$ si et seulement si, pour tout $d \in \mathbb{N}$, avec les mêmes notations, les deux ensembles $J \cap \{m_1, \ldots, m_k\}$ et $J' \cap \{m_1, \ldots, m_k\}$ ont le même cardinal.

Démonstration. Soit $d \in \mathbb{N}$. Supposons que pour tout $k \in \mathbb{N}$, les deux ensembles
$J \cap \{m_1, \ldots, m_k\}$ et $J' \cap \{m_1, \ldots, m_k\}$ aient le même cardinal. On va montrer, par récurrence sur k, que pour tout k les deux ensembles $J \cap \{m_1, \ldots, m_k\}$ et $J' \cap \{m_1, \ldots, m_k\}$ sont égaux. Ceci entraînera que J et J' contiennent les mêmes monômes de degré d et on obtiendra en faisant varier d les deux résultats annoncés.
– Si $k = 1$: card $J \cap \{m_1\}$ = card $J' \cap \{m_1\} = 0$ ou 1. Dans les deux cas, $J \cap \{m_1\}$ et $J' \cap \{m_1\}$ sont égaux (à l'ensemble vide ou à $\{m_1\}$).
– Si $k > 1$, par hypothèse de récurrence, les deux ensembles $J \cap \{m_1, \ldots, m_{k-1}\}$ et $J' \cap \{m_1, \ldots, m_{k-1}\}$ sont égaux et de cardinal r. Alors le cardinal de $J \cap \{m_1, \ldots, m_k\}$ (resp. de $J' \cap \{m_1, \ldots, m_k\}$) est égal à $r + 1$ ou r suivant que J contient ou non m_k.

– si c'est $r+1$, J et J' contiennent m_k et

$$\begin{aligned} J \cap \{m_1, \ldots, m_k\} &= J \cap \{m_1, \ldots, m_{k-1}\} \cup \{m_k\} \\ &= J' \cap \{m_1, \ldots, m_{k-1}\} \cup \{m_k\} = J' \cap \{m_1, \ldots, m_k\} \end{aligned}$$

– si c'est r, m_k n'est contenu ni dans J, ni dans J' et

$$J \cap \{m_1, \ldots, m_k\} = J \cap \{m_1, \ldots, m_{k-1}\} = J' \cap \{m_1, \ldots, m_{k-1}\} = J' \cap \{m_1, \ldots, m_k\}.$$

□

Démonstration. de 6.2.1.
Soit $g \in GL_n$. Reprenons les notations de 6.2.6 : on range les monômes de degré d par ordre décroissant, on écrit $g(I_d)$ dans cette base et on obtient ainsi une matrice $M(g(I_d))$. On note $M_k(g(I_d))$ la sous-matrice des k premiers vecteurs colonnes.
Soit U_d le sous-ensemble de GL_n formé des g tels que le rang de $M_k(g(I_d))$ soit maximum pour tout $k \leqslant \binom{n+d-1}{d}$. Son complémentaire est défini par l'annulation des mineurs de $M_k(g(I_d))$ d'un certain rang, qui sont des polynômes en les coordonnées de g, donc est fermé dans GL_n, et U_d est ouvert.
De plus, pour tout $g \in \mathcal{B}_s$, on a $\operatorname{in} g(I) = \operatorname{in} I$ (cf. 6.1.4). Le rang de $M_k(g(I_d))$ est égal à la dimension de $(\operatorname{in} g(I) \cap < m_1, \ldots, m_k >)$ donc au rang de $M_k(I_d)$: il est indépendant de $g \in \mathcal{B}_s$. On en déduit que l'ouvert U_d est stable par $\mathcal{B}_s$.

Fixons d et soit $U(d) = \bigcap_{d' \leqslant d} U_{d'}$.
Alors, $\forall d' \leqslant d$, $\forall k \leqslant \binom{n+d'-1}{d'}$, le rang de $M_k(g(I_{d'}))$ est indépendant de $g \in U(d)$.
Or, d'après 6.2.4, ce rang est égal au cardinal de $\operatorname{in} g(I_{d'}) \cap \{m_1, \ldots, m_k\})$, qui est donc indépendant de $g \in U(d)$.
On en déduit en utilisant 6.2.7 qu'il existe un idéal monomial $J(d)$ tel que pour tout $g \in U(d)$, l'idéal engendré par les éléments de degré inférieur ou égal à d de $\operatorname{in}(g(I))$ (contenu dans $\operatorname{in}(g(I))$) est égal à $J(d)$, et pour tout $d' \leqslant d$, la dimension de $J(d)_{d'}$ est le maximum des dimensions de $\operatorname{in}(g(I))_{d'}$ lorsque g varie dans GL_n.
La suite des ouverts $U(d)$ est décroissante et la suite des idéaux $J(d)$ est croissante, donc stationnaire. Soit $J(d_0)$ l'idéal réunion (ou limite) des $J(d)$. On va montrer que c'est l'idéal cherché.
Soit U l'ouvert $U(d_0)$. Par définition de d_0 on a $J(d_0+1) = J(d_0)$. De plus, pour tout $g \in U$, $J(d_0)$ est égal à l'idéal engendré par les éléments de degré inférieur ou égal à d_0 de $\operatorname{in}(g(I))$. En particulier la composante homogène de degré d_0+1 de $\operatorname{in}(g(I))$ contient celle de $J(d_0)$, qui est aussi celle de $J(d_0+1)$.
Donc pour $g \in U$, la dimension de $\operatorname{in}(g(I))_{d_0+1}$ est supérieure ou égale à à celle de $J(d_0+1)_{d_0+1}$, qui réalise le maximum des dimensions possibles des $\operatorname{in}(g(I))_{d_0+1}$ lorsque g varie dans GL_n. On en déduit l'égalité des dimensions et l'égalité des idéaux $\operatorname{in}(g(I))$ et $J(d_0)$ en degré d_0+1. On fait la même démonstration en tout degré..

□

Exemple 6.2.8. On choisit $n = 3$, $I = (X_1^2, X_1X_2, X_1X_3 + X_3^2)$ et l'ordre lexicographique inverse.

Un élément g de $GL(3)$ est défini par une matrice :

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{pmatrix}$$

et $g(I) = (g(X_1)^2, g(X_1)g(X_2), g(X_1)g(X_3) + g(X_3)^2)$ avec :

$$g(X_1) = \alpha_1 X_1 + \alpha_2 X_2 + \alpha_3 X_3$$

$$g(X_2) = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3$$

$$g(X_3) = \gamma_1 X_1 + \gamma_2 X_2 + \gamma_3 X_3.$$

Pour $d = 2$ les monômes rangés par ordre décroissant sont :

$$X_1^2 > X_1X_2 > X_2^2 > X_1X_3 > X_2X_3 > X_3^2.$$

La matrice $M(g(I_2))$ est la matrice $3, 6$ obtenue en juxtaposant les deux matrices $3, 3$ suivantes :

$$\begin{pmatrix} \alpha_1^2 & 2\alpha_1\alpha_2 & \alpha_2^2 \\ \alpha_1\beta_1 & \alpha_1\beta_2 + \alpha_2\beta_1 & \alpha_2\beta_2 \\ \alpha_1\gamma_1 + \gamma_1^2 & \alpha_1\gamma_2 + \alpha_2\gamma_1 + 2\gamma_1\gamma_2 & \alpha_2\gamma_2 + \gamma_2^2 \end{pmatrix}$$

$$\begin{pmatrix} \alpha_1\alpha_3 & 2\alpha_2\alpha_3 & \alpha_3^2 \\ \alpha_1\beta_3 + \alpha_3\beta_1 & \alpha_2\beta_3 + \alpha_3\beta_2 & \alpha_3\beta_3 \\ \alpha_1\gamma_3 + \alpha_3\gamma_1 + 2\gamma_1\gamma_3 & \alpha_2\gamma_3 + \alpha_3\gamma_1 + 2\gamma_2\gamma_3 & \alpha_3\gamma_3 + \gamma_3^2 \end{pmatrix}$$

Pour $k = 1$ on a :

$$M_1(g(I_2)) = \begin{pmatrix} \alpha_1^2 \\ \alpha_1\beta_1 \\ \alpha_1\gamma_1 + \gamma_1^2 \end{pmatrix}$$

et son rang est maximum (égal à 1) sur l'ouvert où α_1 et γ_1 ne sont pas tous deux nuls. On dira que le rang générique est 1. On en déduit que $\operatorname{gin} I$ contient X_1^2.
Pour $k = 2$ on a :

$$M_2(g(I_2)) = \begin{pmatrix} \alpha_1^2 & 2\alpha_1\alpha_2 \\ \alpha_1\beta_1 & \alpha_1\beta_2 + \alpha_2\beta_1 \\ \alpha_1\gamma_1 + \gamma_1^2 & \alpha_1\gamma_2 + \alpha_2\gamma_1 + 2\gamma_1\gamma_2 \end{pmatrix}$$

et son rang générique est égal à 2. On en déduit que $\operatorname{gin} I$ contient X_1X_2.
Pour $k = 3$ on va montrer que le rang générique de $M_3(g(I_2))$ est égal à 3. Pour celà il suffit de trouver un g particulier pour lequel le rang est 3. Par exemple :

$$\text{si} \quad g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{alors} \quad M_3(g(I_2)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

On en déduit que $\operatorname{gin} I$ contient X_2^2.

En revanche, si g est l'identité, c'est-à-dire pour le système de coordonnées de départ, $M_3(I_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ qui est de rang 2, inférieur au rang générique.
On montre en poursuivant le calcul que $\operatorname{gin} I$ est l'idéal (X_1^2, X_1X_2, X_2^2) et il distinct de $\operatorname{in} I = (X_1^2, X_1X_2, X_1X_3)$.

Au paragraphe suivant, nous allons mettre en évidence une autre propriété de l'idéal initial générique : il est "Borel-fixe", c'est-à-dire invariant sous l'action du sous-groupe de Borel $\mathcal{B}_i$ des matrices triangulaires inférieures.

6.3 Idéaux Borel-fixes

Définition 6.3.1. Soit $k \in [1, n-1]$. La *transformation élémentaire d'ordre k* est une application de l'ensemble des monômes dans lui-même définie par :

$$\begin{aligned} e_k(m) &= mX_k/X_{k+1} \text{ si } X_{k+1} \text{ divise } m \\ &= 0 \text{ sinon.} \end{aligned}$$

Remarque 6.3.2. Si $e_k(m) \neq 0$ alors on a : $e_k(m) > m$. En effet on a toujours $X_k > X_{k+1}$. Si on multiplie les deux membres de l'inégalité par le monôme m/X_{k+1} on obtient $e_k(m) = mX_k/X_{k+1} > m$.

Proposition 6.3.3. *Soit J un idéal monomial. Les propriétés suivantes sont équivalentes :*
i) Pour tout monôme $m \in J$, pour tout $k \in [1, n-1]$ on a $e_k(m) \in J$.
ii) J est Borel-fixe (c'est-à-dire $g(J) = J$ pour tout $g \in \mathcal{B}_i$).
iii) Pour tout $g \in \mathcal{B}_i$ on a $\operatorname{in} g(J) = J$.

Démonstration. *i)* $\Rightarrow$ *ii)* Le sous-groupe $\mathcal{B}_i$ est engendré par les matrices diagonales et les matrices de la forme $I_d + tE_{k+1,k}$ où t est un scalaire et $E_{k+1,k}$ la matrice élémentaire d'indices $k+1, k$. J étant monomial est stable par l'action de $\mathcal{D}$. Pour montrer que J est Borel-fixe, il suffit donc de montrer qu'il est laissé invariant par l'automorphisme linéaire g correspondant à une matrice $I_d + tE_{k+1,k}$.
On a $g(X_i) = X_i$ pour $i \neq k+1$ et $g(X_{k+1}) = X_{k+1} + tX_k$.
Soit $m = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un monôme. On a :

$$\begin{aligned} g(m) &= X_1^{\alpha_1} \dots X_k^{\alpha_k} (X_{k+1} + tX_k)^{\alpha_{k+1}} X_{k+2}^{\alpha_{k+2}} \dots X_n^{\alpha_n} \\ &= \sum_{p=0}^{\alpha_{k+1}} \binom{\alpha_{k+1}}{p} t^p X_1^{\alpha_1} \dots X_k^{\alpha_k} X_{k+1}^{\alpha_{k+1}-p} X_{k+2}^{\alpha_{k+2}} X_n^{\alpha_n} \\ &= \sum_{p=0}^{\alpha_{k+1}} \binom{\alpha_{k+1}}{p} t^p X_k^p (m/X_{k+1}^p) \\ &= \sum_{p=0}^{\alpha_{k+1}} \binom{\alpha_{k+1}}{p} t^p e_k^p(m). \end{aligned}$$

et donc $g(m) \in J$.
ii) $\Rightarrow$ *iii)* Soit $g \in \mathcal{B}_i$. Puisque $g(J) = J$, on a $\operatorname{in} g(J) = \operatorname{in} J = J$.
iii) $\Rightarrow$ *i)* Soit g correspondant à une matrice $I_d + E_{k+1,k}$ et $m = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un monôme de J. On va montrer par récurrence décroissante sur q que $e_k^q(m) \in J \cap g(J)$.
Si $q > \alpha_{k+1}$ on a $e_k^q(m) = 0$.
Si $q \leqslant \alpha_{k+1}$ on a :

$$g(m) = \sum_{p=0}^{q} \binom{\alpha_{k+1}}{p} e_k^p(m) + \sum_{p=q+1}^{\alpha_{k+1}} \binom{\alpha_{k+1}}{p} e_k^p(m) \in g(J).$$

Par hypothèse de récurrence,

$$\sum_{p=q+1}^{\alpha_{k+1}} \binom{\alpha_{k+1}}{p} e_k^p(m) \in J \cap g(J)$$

donc

$$f = \sum_{p=0}^{q} \binom{\alpha_{k+1}}{p} e_k^p(m) \in g(J).$$

Puisque $\operatorname{in} g(J) = J$, le terme initial de f appartient donc à J.
Or $e_k^q(m) > \dots > e_k(m) > m$ et puisque la caractéristique de k est nulle, $\binom{\alpha_{k+1}}{q}$ n'est pas nul. On a donc $\operatorname{in} f = \binom{\alpha_{k+1}}{q} e_k^q(m) \in J$. De plus, on peut écrire :

$$g(e_k^q(m)) = e_k^q(m) + \sum_{r \geqslant 1} \lambda_r e_k^{r+q}(m) \in g(J).$$

Toujours par hypothèse de récurrence, $\sum_{r \geqslant 1} \lambda_r e_k^{r+q}(m) \in J \cap g(J)$, et donc $e_k^q(m) \in g(J)$. Appliquant ce résultat pour $q = 1$ on obtient $e_k(m) \in J$.

□

Avant de montrer le prochain théorème, nous avons besoin d'un lemme :

Lemme 6.3.4. *Soient J un idéal monomial et g un élément de $\mathcal{B}_i$. On reprend les notations de 6.2.4 : soient m_1, …, m_N les monômes de degré d rangés par ordre décroissant, $k \leqslant N$ et p_k la projection de S_d sur le sous-espace vectoriel $< m_1, \dots, m_k >$ parallèlement au sous-espace vectoriel $< m_{k+1}, \dots, m_N >$. Alors la dimension de $p_k(J_d)$ est inférieure ou égale à celle de $p_k(g(J_d))$.*

Démonstration. Puisque J est monomial, $p_k(J_d)$ est engendré par les monômes de J_d appartenant à $< m_1, \dots, m_k >$. La dimension r de $p_k(J_d)$ est donc égale au nombre de monômes de J_d supérieurs ou égaux à m_k. Soient $m'_1, \dots, m'_r$ ces monômes.
D'après 6.1.4, il existe des scalaires λ_i tels que pour tout $i \in [1, r]$, tous les termes non nuls de $g(m'_i) - \lambda_i m'_i$ soient supérieurs à m'_i. En particulier $p_k g(m'_i) = g(m'_i)$. Donc $p_k(g(J_d))$ contient r monômes distincts et est de dimension $\geqslant r$. □

Théorème 6.3.5. *Soit I un idéal homogène Son idéal initial générique $\operatorname{gin} I$ est Borel-fixe.*

Démonstration. Soit U l'ouvert de GL_n tel que pour tout $g \in U$ on ait $\operatorname{in} g(I) = \operatorname{gin} I$. Quitte à faire un changement linéaire de coordonnées, on peut supposer qu'il contient l'identité, c'est-à-dire que $\operatorname{in} I = \operatorname{gin} I$. Notons-le J.
En reprenant les notations de 6.2.6, le résultat de 6.3.4 s'écrit :

$$\forall g \in \mathcal{B}_i\,, \ \operatorname{rang} M_k(J_d) \leqslant \operatorname{rang} M_k(g(J_d)).$$

D'autre part on a construit en 5.6.2 une famille plate d'idéaux $\mathcal{I}$ qui relie un idéal I à son idéal initial $\operatorname{in} I$, dont la fibre pour $\lambda \neq 0$ est l'idéal $g_\lambda(I)$, où g_λ est l'élément diagonal de GL_n défini par $g_\lambda(X_i) = X_i/\lambda^{a_i}$.
On a donc $\mathcal{I}_0 = \operatorname{in} I = J$, $\mathcal{I}_\lambda = g_\lambda(I)$ et $\operatorname{in} \mathcal{I}_\lambda = \operatorname{in} g_\lambda(I) = \operatorname{in} I = J$.
La famille $g(\mathcal{I})$ obtenue par transformation par g est encore plate, donc par semi-continuité, il existe un ouvert U_g de $\operatorname{Spec} k[t]$ tel que pour tout $\lambda \in U_g$:

$$\operatorname{rang} M_k(g(\mathcal{I}_0)_d = \operatorname{rang} M_k(g(J_d)) \leqslant \operatorname{rang} M_k(g(\mathcal{I}_\lambda)_d.$$

D'autre part, on a vu dans la construction de l'idéal $\operatorname{gin} I = J$ que pour tout g le rang de $M_k(g(I)_d$ est inférieur ou égal à celui de $M_k(J)_d$. En mettant toutes ces inégalités ensemble on a :

$$\operatorname{rang} M_k(J_d) \leqslant \operatorname{rang} M_k(g(J_d)) \leqslant \operatorname{rang} M_k(g(I)_d \leqslant \operatorname{rang} M_k(J_d)$$

et donc l'égalité :

$$\operatorname{rang} M_k(J_d) = \operatorname{rang} M_k(g(J_d)).$$

Ceci étant vrai pour tout d, pour tout k, on conclut que $J = \operatorname{in} g(J)$ et donc en utilisant la caractérisation de 6.3.3 que J est Borel-fixe.

□

Exemple 6.3.6. Voici quelques exemples d'idéaux Borel-fixes :
– pour 2 variables, les idéaux engendrés par des "segments initiaux", c'est-à-dire tous les monômes $X_1^i X_2^j$ avec $i + j = r$ et $0 \leqslant j \leqslant s \leqslant r$.
– pour 3 variables, les idéaux $(X_1^3, X_1^2X_2, X_1X_2^2)$ et $(X_1^3, X_1^2X_2, X_1^2X_3)$.
– Le produit, l'intersection, la somme d'idéaux Borel-fixes sont encore Borel-fixes.

Nous allons mettre en évidence certaines propriétés des idéaux Borel-fixes qui expliquent leur intérêt.

Proposition 6.3.7. *Soit J un idéal monomial Borel-fixe. Pour tout $j \leqslant n$ et pour tout $N \in \mathbb{N}$ on a :*

$$(J : X_j^N) = (J : (X_1, \ldots, X_j)^N).$$

Démonstration. Il nous faut montrer que si m est un monôme tel que $mX_j^N \in J$, alors :

$$\forall m' = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_j^{\alpha_j} \in S_N \quad mm' \in J.$$

Or on a :

$$e_1^{\alpha_1} e_2^{\alpha_1+\alpha_2} \ldots e_{j-1}^{\alpha_1+\ldots\alpha_{j-1}} X_j^n = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_j^{\alpha_j} = m'.$$

En utilisant le fait que J est invariant par les transformations élémentaires et que si m_1 et m_2 sont deux monômes tels qu'on ait $e_k(m_2) \neq 0$, on a $e_k(m_1m_2) = m_1 e_k(m_2)$, on en déduit le résultat. □

Ce résultat va nous donner un critère simple pour déterminer si un idéal est saturé ou non. Rappelons la définition d'un idéal saturé :

Définition 6.3.8. Soit I un idéal homogène de S. On dit qu'il est *saturé* s'il vérifie pour tout $N \in \mathbb{N}$ $I = (I : (X_1, \ldots, X_n)^N)$, ce qu'on peut écrire aussi $I = (I : (X_1, \ldots, X_n)^\infty)$.

Corollaire 6.3.9. *Soit I un idéal homogène de S et $\operatorname{gin} I$ son idéal initial générique pour l'ordre lexicographique inverse. Alors I est saturé si et seulement si aucun monôme générateur de $\operatorname{gin} I$ ne fait intervenir X_n.*

Démonstration. Si I est saturé, on peut montrer (voir par exemple Green) que son idéal initial générique pour l'ordre lexicographique inverse $\operatorname{gin} I$ est saturé. On a donc $\operatorname{gin} I = (\operatorname{gin} I : (X_1, \ldots, X_n)^\infty) = (\operatorname{gin} I : X_n^\infty)$ donc aucun monôme générateur de $\operatorname{gin} I$ ne fait intervenir X_n.
Inversement supposons qu'on ait $\operatorname{gin} I = (\operatorname{gin} I : (X_1, \ldots, X_n)^\infty) = (\operatorname{gin} I : X_n^\infty)$. Quitte à faire un changement linéaire de coordonnées, on peut supposer que $\operatorname{in} I = \operatorname{gin} I$. On a :

$$\operatorname{in}(I : (X_1, \ldots, X_n)^\infty) \subseteq (\operatorname{in} I : (X_1, \ldots, X_n)^\infty) = \operatorname{in} I.$$

En effet, soit $f \in S$ tel que pour tout monôme m de degré N on ait $mf \in I$. On a alors aussi $m\operatorname{in} f \in \operatorname{in} I$, donc $\operatorname{in} f \in \operatorname{in} I : (X_1, \ldots, X_n)^N$. Or

$$I \subseteq (I : (X_1, \ldots, X_n)^\infty) \quad \text{donc} \quad \operatorname{in} I \subseteq \operatorname{in}(I : (X_1, \ldots, X_n)^\infty)$$

d'où l'égalité des idéaux initiaux et des idéaux.

□

Chapitre 7

Conditions de croissance des idéaux (Macaulay)

Dans tout ce chapitre, on fait les conventions suivantes sur les coefficients binomiaux :

$$\binom{n}{p} = 0 \text{ pour } n \in \mathbb{Z},\, p \geqslant 0 \text{ et } n < p \quad , \quad \binom{n-1}{-1} = \begin{cases} 1 & \text{pour } n = 0 \\ 0 & \text{sinon} \end{cases}$$

Avec cette convention, la formule de Pascal $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ est valable pour tous $n > p \geq 0$.
Soit I un idéal homogène de S. L'anneau gradué S/I est une k-algèbre de type fini, engendrée par sa composante de degré 1, ce que certains auteurs appellent une **G-algèbre standard**. Les fonctions de Hilbert de ces algèbres ont été caractérisées par Macaulay. C'est ce que nous allons faire en utilisant les idéaux Borel-fixes.

7.1 Développement binomial

Proposition 7.1.1. *Soient α et i des entiers strictement positifs. Alors α peut s'écrire de manière unique sous la forme :*

$$\alpha = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + \cdots + \binom{m_j}{j}$$

avec $m_i > m_{i-1} > \cdots > m_j \geq j \geq 1$.

Démonstration. L'existence et l'unicité vont découler des inégalités suivantes :

$$\binom{m_i}{i} \leq \alpha < \binom{m_i+1}{i} = \binom{m_i}{i} + \binom{m_i-1}{i-1} + \cdots + \binom{m_i-i+1}{1} + 1$$

dont on déduit, si une telle écriture existe, $m_i = \sup\{k \mid \binom{k}{i} \leq \alpha\}$.
Montrons, par récurrence sur α, le résultat suivant : pour tout $i > 0$ il existe une et une seule écriture comme ci-dessus.
– Pour $\alpha = 1$, $\alpha = \binom{i}{i}$.

– Pour $\alpha > 1$, posons $m_i = \sup\{k \mid \binom{k}{i} \leq \alpha\}$ et soit $\alpha' = \alpha - \binom{m_i}{i}$. Par hypothèse de récurrence, on peut écrire :

$$\alpha' = \binom{m_{i-1}}{i-1} + \cdots + \binom{m_j}{j}$$

avec $m_{i-1} > \cdots > m_j \geq j \geq 1$, et donc

$$\alpha = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + \cdots + \binom{m_j}{j}.$$

De plus, on a, par définition de m_i,

$$\binom{m_{i-1}}{i-1} \leq \alpha' = \alpha - \binom{m_i}{i} < \binom{m_i+1}{i} - \binom{m_i}{i} = \binom{m_i}{i-1}$$

donc $m_{i-1} < m_i$.

L'unicité découle de celle de m_i et de celle de l'écriture de α'.

□

Définitions 7.1.1. L'expression de α en fonction des coefficients binomiaux établie en 7.1.1 est appelée le *développement i-binomial* de α. Si on ne précise pas i, on dira que c'est un *développement binomial* de α

On définit alors :

$$\alpha^{<i>} = \binom{m_i+1}{i+1} + \binom{m_{i-1}+1}{i} + \cdots + \binom{m_j+1}{j+1}$$

$$\alpha^{[i]} = \binom{m_i+1}{i} + \binom{m_{i-1}+1}{i-1} + \cdots + \binom{m_j+1}{j+1}$$

$$\alpha_{[i]} = \binom{m_i-1}{i} + \binom{m_{i-1}-1}{i-1} + \cdots + \binom{m_j-1}{j}$$

et $0^{<i>} = 0^{[i]} = 0_{[i]} = 0$.

Remarque 7.1.2. Les écritures de $\alpha^{<i>}$ et $\alpha^{[i]}$ sont des développements binomiaux (de $\alpha^{<i>}$ et $\alpha^{[i]}$), celle de $\alpha_{[i]}$ l'est aussi si $m_j > j$.

Exemple 7.1.3. $25 = \binom{6}{3}+\binom{3}{2}+\binom{2}{1}$, $25^{<3>} = \binom{7}{4}+\binom{4}{3}+\binom{3}{2} = 41$, $25^{[3]} = \binom{7}{3}+\binom{4}{2}+\binom{3}{1} = 44$, $25_{[3]} = \binom{5}{3} + \binom{2}{2} + \binom{1}{1} = 12$.

Remarque 7.1.4. Si $0 < \alpha \leq i$, les coefficients binomiaux qui apparaissent dans le développement i-binomial de α sont égaux à 1. On en déduit facilement qu'on a alors $\alpha^{<i>} = \alpha$.

Proposition 7.1.5. . *Soient α, β et i des entiers strictement positifs avec $\alpha < \beta$. Alors on a $\alpha^{<i>} < \beta^{<i>}$, $\alpha^{[i]} < \beta^{[i]}$ et $\alpha_{[i]} \leq \beta_{[i]}$.*

Démonstration. Ecrivons les développements i-binomiaux :

$$\alpha = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + \cdots + \binom{m_j}{j}, \quad \beta = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_{j'}}{j'}.$$

Posons :

$$k = \sup\{\, l \in \mathbb{N} \mid m_l \neq n_l \,\} \quad \text{et} \quad \gamma = \binom{m_i}{i} + \cdots + \binom{m_{k+1}}{k+1}$$

$$\alpha - \gamma = \alpha_1 \quad \beta - \gamma = \beta_1 \quad \text{avec} \quad 0 \leq \alpha_1 < \beta_1.$$

Alors on a :

$$\alpha^{<i>} = \gamma^{<i>} + \alpha_1^{<k>} \quad \beta^{<i>} = \gamma^{<i>} + \beta_1^{<k>}$$

$$\alpha^{[i]} = \gamma^{[i]} + \alpha_1^{[k]} \quad \beta^{[i]} = \gamma^{[i]} + \beta_1^{[k]}$$

$$\alpha_{[i]} = \gamma_{[i]} + \alpha_{1[k]} \quad \beta_{[i]} = \gamma_{[i]} + \beta_{1[k]}.$$

Quitte à retrancher un même nombre à α et β, on peut donc supposer qu'on a $m_i \neq n_i$ ou $\alpha = 0$.
Si $\beta \neq 0$, alors $\beta^{<i>} > 0$, $\beta^{[i]} > 0$ et $\beta_{[i]} \geq 0$ donc le résultat est vrai pour $\alpha = 0$.
Si $m_i < n_i$, alors $\alpha < \binom{m_i+1}{i} \leq \binom{n_i}{i} \leq \beta$. De même si $m_i > n_i$, alors $\alpha > \beta$. Donc si $\alpha < \beta$, on a $m_i < n_i$, $m_i + 1 < n_i + 1$ et $\alpha^{<i>} < \beta^{<i>}$, $\alpha^{[i]} < \beta^{[i]}$.
Pour montrer la deuxième inégalité, il faut faire apparaître les coefficients binomiaux éventuels égaux à 1. Plus précisément, on écrit :

$$\alpha = \binom{m_i}{i} + \cdots + \binom{m_k}{k} + (k-j), \quad \beta = \binom{n_i}{i} + \cdots + \binom{n_{k'}}{k'} + (k'-j')$$

avec $m_1 > \cdots > m_k > k \geq j$, $n_1 > \cdots > n_{k'} > k' \geq j'$ et $m_i \leq n_i$. Alors soit $m_i = i$ et $\alpha_{[i]} = 0$, soit $m_i > i$ et

$$\alpha_{[i]} = \binom{m_i - 1}{i} + \cdots + \binom{m_k - 1}{k}, \quad \beta_{[i]} = \binom{n_i - 1}{i} + \cdots + \binom{n_{k'} - 1}{k'}$$

et $\alpha_{[i]} \leq \beta_{[i]}$ puisque $m_i < n_i$. □

Lemme 7.1.6. *Soient α et i des entiers tels que $\alpha > 0$ et $i > 1$. On a :*

$$(\alpha^{[i]})_{[i]} = \alpha \quad , \quad (\alpha_{[i]})^{[i]} \leq \alpha \quad , \quad (\alpha - \alpha_{[i]})^{<i-1>} \geq \alpha$$

Démonstration. L'égalité $(\alpha^{[i]})_{[i]} = \alpha$ est immédiate.
Comme ci-dessus, écrivons le développement i-binomial de α sous la forme :

$$\alpha = \binom{m_i}{i} + \cdots + \binom{m_k}{k} + (k-j).$$

On a :

$$\alpha_{[i]} = \binom{m_i - 1}{i} + \binom{m_{i-1} - 1}{i-1} + \cdots + \binom{m_k - 1}{k}$$

$$(\alpha_{[i]})^{[i]} = \binom{m_i}{i} + \cdots + \binom{m_k}{k} = \alpha - (k-j) \leq \alpha.$$

$$\begin{aligned}(\alpha - \alpha_{[i]}) &= (\binom{m_i}{i} - \binom{m_i - 1}{i}) + \cdots + (\binom{m_k}{k} - \binom{m_k - 1}{k}) + (k-j) \\ &= \binom{m_i - 1}{i-1} + \cdots \binom{m_{k-1}}{k-1} + (k-j) \\ &= \binom{m_i - 1}{i-1} + \cdots \binom{m_k - 1}{k-1} + \binom{k-2}{k-2} + \cdots + \binom{j-1}{j-1}\end{aligned}$$

C'est un développement binomial sauf si $j = 1$.
Si $j \neq 1$, on a :

$$(\alpha - \alpha_{[i]})^{i-1} = \binom{m_i}{i} + \cdots + \binom{m_k}{k} + \binom{k-1}{k-1} + \cdots + \binom{j}{j} = \alpha.$$

Si $j = 1$,

$$\begin{aligned}(\alpha - \alpha_{[i]}) &> \binom{m_i - 1}{i-1} + \cdots \binom{m_k - 1}{k-1} + \binom{k-2}{k-2} + \cdots + \binom{j}{j} \\ (\alpha - \alpha_{[i]})^{<i-1>} &> (\binom{m_i - 1}{i-1} + \cdots \binom{m_k - 1}{k-1} + \binom{k-2}{k-2} + \cdots + \binom{j}{j})^{i-1} \\ &> \binom{m_i}{i} + \cdots + \binom{m_k}{k} + \binom{k-1}{k-1} + \cdots + \binom{j+1}{j+1} = \alpha - 1\end{aligned}$$

donc $(\alpha - \alpha_{[i]})^{<i-1>} \geq \alpha$.

□

Lemme 7.1.7. *Soient α, β et i des entiers tels que $\alpha > 0$ et $i > 1$ et $\alpha \leq \beta^{<i-1>}$. Alors on a : $\alpha^{[i]} \leq \alpha + \beta^{[i-1]}$.*

Démonstration. Ecrivons les développements i-binomiaux :

$$\alpha = \binom{m_i}{i} + \cdots + \binom{m_j}{j}, \quad \beta = \binom{n_{i-1}}{i-1} + \cdots + \binom{n_{j'}}{j'} \quad \beta^{<i-1>} = \binom{n_{i-1}+1}{i} + \cdots + \binom{n_{j'}+1}{j'+1}.$$

Si $m_i \neq n_{i-1} + 1$, $\alpha \leq \beta^{<i-1>} \Leftrightarrow m_i < n_{i-1} + 1$. On a alors :

$$\begin{aligned}\alpha^{[i]} - \alpha &= \binom{m_i + 1}{i} + \cdots + \binom{m_j + 1}{j} - (\binom{m_i}{i} + \cdots + \binom{m_j}{j}) \\ &= \binom{m_i}{i-1} + \cdots + \binom{m_j}{j-1} \\ &< \binom{n_{i-1}+1}{i-1} + \cdots + \binom{n_{j'}+1}{j'} = \beta^{[i-1]}.\end{aligned}$$

On laisse au lecteur le soin de traiter le cas général. □

7.2 Conditions de Macaulay

Nous allons montrer simultanément les 3 résultats suivants :

Théorème 7.2.1 (Estimation de Macaulay sur la croissance des idéaux)**.** *Soit I un idéal homogène de S. La fonction de Hilbert h de S/I vérifie $h(0) = 1$ et $h(i+1) \leq h(i)^{<i>}$ pour tout $i \geq 1$.*

Théorème 7.2.2 (Restriction à une section hyperplane)**.** *Sous les mêmes hypothèses, soit H une forme linéaire générale de S et h_H la fonction de Hilbert de $S/(I + (H))$. Alors pour tout $i \geq 1$ on a : $h_H(i) \leq h(i)_{[i]}$.*

Proposition 7.2.3. *Sous les mêmes hypothèses, on a : $h_(i) \leq (\sum_{j=0}^{i} h(j))_{[i]}$.*

La démonstration se fera en plusieurs étapes.
On fixe pour la suite l'ordre lexicographique inverse.
Notons $A(i,n)$ (resp. $B(i,n)$, resp. $C(i,n)$) la propriété énoncée dans 7.2.1 (resp. 7.2.2, resp. 7.2.3).

Lemme 7.2.4. $C(i, n-1) \Rightarrow B(i,n)$.

Démonstration. On va montrer qu'on peut se ramener au cas où I est monomial Borel-fixe et $H = X_n$.
Soit U l'ouvert de GL_n tel que pour tout $g \in U$ on ait $\operatorname{in} g(I) = \operatorname{gin} I$. Soit V l'ensemble des $g^{-1}(X_n)$, $g \in U$. C'est un ouvert de S_1. De plus, pour tout $H \in V$ on a :

$$h_H(i) = \dim(S/I + (H))_i = \dim(S/g(I) + (X_n))_i = \dim(S/\operatorname{in}(g(I) + (X_n)))_i.$$

De plus puisque $g \in U$ on a

$$\operatorname{gin} I + (X_n) = \operatorname{in} g(I) + (X_n) = \operatorname{in}(g(I) + (X_n)).$$

Donc $h_H(i) = \dim(S/\operatorname{gin} I + (X_n))_i$.
De plus S/I et $S/\operatorname{gin} I$ ont la même fonction de Hilbert donc si l'inégalité de 7.2.2 est prouvée pour $\operatorname{gin} I$ et la forme linéaire X_n, elle est aussi vraie pour I et $H \in V$.
Supposons maintenant I monomial Borel-fixe et $H = X_n$.
On définit pour tout $j \geq 0$ l'idéal J_j monomial de $S' = k[X_1, \ldots, X_{n-1}]$ par

$$J_j = (I : (X_n^j)) \cap k[X_1, \ldots, X_{n-1}]$$

Soient m un monôme de J_j et $p \in [1, \ldots, n-1]$ un entier. On a $mX_n^j \in I$, et en utilisant les transformations élémentaires, $X_p X_n^{j-1} \in I$ donc $X_p m$ appartient à J_{j-1}.
On définit alors un idéal monomial J' de S' par :

$$J'_0 = J_{i,0} \quad J'_1 = J_{i-1,1} \quad \ldots \quad J'_i = J_{0,i} \quad J'_{i+k} = (X_1, \ldots, X_{n-1})^k J'_i.$$

C'est bien un idéal puisque $(X_1, \ldots, X_{n-1})J_j$ est contenu dans J_{j-1}. On a alors :

$$I_i = J_{0,i} + X_n J_{1,i-1} + \cdots + X_n^i J_{i,0} = J'_i + X_n J'_{i-1} + \cdots + X_n^i J'_0$$

$$(I + (X_n))_i = J'_i$$

On a donc $h(i) = \sum_{j=0}^{i} h_{S'/J'}(j)$.
Par hypothèse $h_{S'/J'}(i) \leq (\sum_{j=0}^{i} h_{S'/J'}(j))_{[i]} = h(i)_{[i]}$. □

Lemme 7.2.5. $B(i,n) \Rightarrow A(i-1,n)$.

Démonstration. On a

$$\dim(S/I+(H))_i = \dim(S/I)_i - \dim((H)S/I)_i \geq \dim(S/I)_i - \dim(S/I)_{i-1}$$

ou encore

$$h(i) \leq h(i-1) + h_H(i) \leq h(i-1) + h(i)_{[i]}.$$

On en déduit en utilisant 7.1.6 :

$$h(i) \leq (h(i) - h(i)_{[i]})^{<i-1>} \leq h(i-1)^{<i-1>}.$$

□

Lemme 7.2.6. *$A(i-1,n)$ et $C(i-1,n) \Rightarrow B(i,n)$.*

Démonstration. De $h_(i-1) \leq (\sum_{j=0}^{i-1} h(j))_{[i-1]}$ on déduit :

$$h_(i-1)^{[i-1]} \leq ((\sum_{j=0}^{i-1} h(j))_{[i-1]})^{[i-1]} \leq \sum_{j=0}^{i-1} h(j)$$

De $h(i) \leq h(i-1)^{<i-1>}$ on déduit, en utilisant 7.1.7 :

$$h(i)^{[i]} \leq h(i) + h_(i-1)^{[i-1]} \leq \sum_{j=0}^{i} h(j)$$

$$(h(i)^{[i]})_{[i]} = h(i) \leq (\sum_{j=0}^{i} h(j))_{[i]}.$$

□

Exemple 7.2.7. On choisit $n=3$ et $I=(X_1X_2^3, X_2^2X_3, X_2X_3^2, X_3^4)$. On a :

$$h(0)=1 \quad h(1)=2 \quad h(3)=1 \quad h(4)=0$$

$$h(1)^{<1>}=3 \quad h(2)^{<2>}=4$$

Démonstration. (de 7.2.1, 7.2.2 et 7.2.3).
On démontre $C(i,n)$ par récurrence sur $n+i \geq 2$.
– pour $n=1$, l'idéal I est engendré par un monôme X^δ. On a $h(j)=1$ pour $j<\delta$ et $h(j)=0$ pour $j \geqslant \delta$ d'où :
  – pour $i<\delta$

$$\sum_{j=0}^{i} h(j) = i+1 = \binom{i+1}{i} \Rightarrow (\sum_{j=0}^{i} h(j))_{[i]} = \binom{i}{i} = 1 = h(i)$$

– pour $i \geqslant \delta$

$$\sum_{j=0}^{i} h(j) = \delta = \binom{i}{i} + \cdots + \binom{i-\delta+1}{i-\delta+1} \Rightarrow (\sum_{j=0}^{i} h(j))_{[1]} = 0 = h(i)$$

– pour $i = 1$, $(h(0) + h(1))_{[i]} = h(0) + h(1) - 1 = h(1)$
– pour $n > 1$ et $i > 1$, $C(i-1, n)$ et $C(i, n-1) \Rightarrow C(i, n)$.

□

Le théorème de Macaulay 7.2.1 admet une réciproque que nous allons montrer maintenant.

Théorème 7.2.8. *Soit h une fonction de $\mathbb{N}$ dans $\mathbb{N}$ vérifiant $h(0) = 1$, $h(1) = n$ et $h(i+1) \leq h(i)^{<i>}$ pour tout $i \geq 1$. Alors il existe un idéal homogène I de S tel qu'on ait $h = h_{S/I}$.*

Lemme 7.2.9. *Fixons l'ordre lexicographique sur S. Soient $m_0 = X_1^{\alpha_1} \dots X_n^{\alpha_n}$ un monôme, d son degré, N le cardinal de l'ensemble des monômes m de S de degré d avec $m < m_0$, N' le cardinal de l'ensemble des monômes m de S de degré $d+1$avec $m < m_0 X_n$. Alors on a $N^{<d>} = N'$.*

Démonstration. On considère pour tout $p \in [1, n-1]$ l'ensemble $\mathcal{M}_p$ des monômes $m = X_1^{\beta_1} \dots X_n^{\beta_n}$ de degré d avec

$$\beta_1 = \alpha_1, \quad \dots, \quad \beta_{p-1} = \alpha_{p-1}, \quad \beta_p < \alpha_p.$$

On veut donc évaluer le cardinal de la réunion (disjointe) de $\mathcal{M}_1$,..., $\mathcal{M}_{n-1}$.
Pour tout $p \in [1, n-1]$, $\mathcal{M}_p$ est en bijection avec l'ensemble des $\beta_p, \dots, \beta_n$ avec

$$\beta_p < \alpha_p \quad \text{et} \quad \beta_p + \cdots + \beta_n = d - \sum_{i=1}^{p-1} \alpha_i.$$

Si $\alpha_p = 0$, $\mathcal{M}_p$ est vide. Sinon, en donnant successivement à β_p les valeurs $0, \dots \alpha_p - 1$ on obtient :

$$\begin{aligned} \#\mathcal{M}_p &= \sum_{j=0}^{\alpha_p - 1} \binom{n-p-1+d-\sum_{i=1}^{p-1}\alpha_i - j}{d-\sum_{i=1}^{p-1}\alpha_i - j} \\ &= \binom{n-p-1+d-\sum_{i=1}^{p-1}\alpha_i}{d-\sum_{i=1}^{p-1}\alpha_i} + \cdots + \binom{n-p+d-\sum_{i=1}^{p}\alpha_i}{d-\sum_{i=1}^{p}\alpha_i + 1} \end{aligned}$$

et on remarque que c'est un développement $(d - \sum_{i=1}^{p-1} \alpha_i)$-binomial d'une forme particulière : les nombres qui apparaissent en haut des coefficients binômiaux décroissent régulièrement de 1.
En ajoutant tous ces nombres, on obtient :

$$N = \sum_{p=1}^{n-1} \#\mathcal{M}_p = \sum_{p=1}^{n-1} \sum_{j=0}^{\alpha_p - 1} \binom{n-p-1+d-\sum_{i=1}^{p-1}\alpha_i - j}{d-\sum_{i=1}^{p-1}\alpha_i - j}.$$

On remarque que c'est encore un développement binomial (même si certains des exposants α_i sont nuls).
Sur cette forme on voit immédiatement que si N le cardinal de l'ensemble des monômes de degré d et inférieurs à $X_1^{\alpha_1} \dots X_n^{\alpha_n}$, $N^{<d>}$ est le cardinal de l'ensemble des monômes de degré $d+1$ et inférieurs à $X_1^{\alpha_1} \dots X_n^{\alpha_n+1}$.

□

Démonstration. (de 7.2.8). On met sur S l'ordre lexicographique homogène et pour tout $d \in \mathbb{N}$ on range les monômes par ordre croissant : $m_{d,1} < m_{d,2} < \cdots$.
Avec ces notations le résultat de 7.2.9 peut encore s'écrire :

$$X_n m_{d,N+1} = m_{d+1,N^{<d>}+1}.$$

De l'inégalité $h(d+1) \leq h(d)^{<d>}$ on déduit :

$$m_{d+1,h(d+1)} \leq m_{d+1,h(d)^{<d>}}.$$

On considère alors l'espace vectoriel J_d engendré par les monôme de degré d supérieurs à $m_{d,h(d)}$. On va montrer que la somme J des J_d est un idéal de S, c'est-à-dire que J est stable par multiplication par X_i pour tout $i = 1, \dots, n$.
Soit $m \in J_d$. On a donc

$$m > m_{d,h(d)} \Rightarrow X_i m \geq X_n m \geq X_n m_{d,h(d)+1} = m_{d+1,h(d)^{<d>}+1} > m_{d+1,h(d+1)}$$

et $X_i m \in J_{d+1}$. □