

# Bases de Gröbner

Moi

October 26, 2016

## Contents

<b>1</b>	<b>Ordre monomial</b>	<b>1</b>
1.1	Généralités . . . . .	1
1.2	Exemples d'ordres monomiaux . . . . .	2
<b>2</b>	<b>Algorithme de division</b>	<b>3</b>
<b>3</b>	<b>Idéaux monomiaux</b>	<b>6</b>
<b>4</b>	<b>Bases de Gröbner</b>	<b>8</b>
4.1	Généralités . . . . .	8
4.2	Propriétés des bases de Gröbner . . . . .	9
<b>5</b>	<b>Algorithme de Buchberger</b>	<b>11</b>
<b>6</b>	<b>Théorème d'élimination et d'extension</b>	<b>12</b>
<b>7</b>	<b>Géométrie</b>	<b>13</b>
7.1	Généralités . . . . .	13
7.2	Géométrie de l'élimination . . . . .	15

## 1 Ordre monomial

### 1.1 Généralités

**Définition 1.1** *Un ordre monomial est une relation d'ordre total  $\geq$  de  $\mathcal{M}$  telle que :*

1.  $\forall \alpha, \beta, \gamma \in \mathbb{N}^n, X^\alpha \geq X^\beta \Rightarrow X^{\alpha+\gamma} \geq X^{\beta+\gamma}$

2.  $\geq$  est un bon ordre

On note  $X^\alpha > X^\beta$  si  $X^\alpha \geq X^\beta$  et  $\alpha \neq \beta$  (compatible avec l'addition) et  $X^\alpha \leq X^\beta$  si  $X^\beta \geq X^\alpha$

**Propriété 1.2** Soit  $\geq$  un ordre monomial. 1 est le plus petit élément de  $\mathcal{M}$  pour  $\geq$ .

**Démonstration 1.3** Comme  $\geq$  est un bon ordre alors il existe un plus petit élément que l'on notera  $x^\alpha$  alors :  $X^\alpha \leq 1$  et donc  $X^{2\alpha} \leq X^\alpha$  (par la compatibilité avec l'addition).

Or comme  $X^\alpha$  est le petit élément de  $\mathcal{M}$  alors  $X^\alpha \leq X^{2\alpha}$ .

Donc, par antisymétrie,  $X^\alpha = X^{2\alpha}$  d'où  $\alpha = 2\alpha$  et donc  $\alpha = 0$ .

On en déduit que  $1 = X^0$  est le plus petit élément de  $\mathcal{M}$ .

**Corollaire 1.4** Soit  $\geq$  un ordre monomial et  $\alpha, \beta \in \mathbb{N}^n$ . Si  $X^\alpha | X^\beta$  alors  $X^\alpha \leq X^\beta$ .

**Démonstration 1.5** Si  $X^\alpha | X^\beta$  alors il existe  $\gamma \in \mathbb{N}^n$  tel que :  $X^\beta = X^\gamma X^\alpha$ . Or comme  $1 \leq X^\gamma$  alors par compatibilité avec l'addition,  $X^\alpha \leq X^{\alpha+\gamma} = X^\beta$ .

**Définition 1.6** Soit  $P := \sum_{\alpha} p_{\alpha} X^{\alpha}$  et  $\geq$  un ordre monomial.

1. Le monôme dominant de  $P$  est :  $LM(P) := \max\{X^{\alpha} \in \mathcal{M} | a_{\alpha} \neq 0\}$
2. Le multidegré de  $f$  est l'élément de  $\mathbb{N}^n$ , noté  $\text{multideg}(P)$ , tel que  $x^{\text{multideg}(P)} = LM(P)$
3. Le coefficient dominant de  $P$  est  $LC(P) := a_{\text{multideg}(P)}$
4. Le terme dominant de  $P$  est  $LT(P) := LC(P) \cdot LM(P)$

## 1.2 Exemples d'ordres monomiaux

**Définition et propriété 1.7 (Ordre lexicographique  $\geq_{\text{lex}}$ )** Soient  $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$  alors  $X^\alpha \geq_{\text{lex}} X^\beta$  si, et seulement si,  $\alpha = \beta$  ou le premier coefficient non nul en lisant par la gauche de  $\alpha - \beta$  est positif.

**Démonstration 1.8** Montrons que  $\geq$  est un ordre monomial.

$\alpha, \beta, \gamma$  désigneront des éléments quelconques de  $\mathbb{N}^n$  et si  $\alpha \neq \beta$ ,  $\ell(\alpha, \beta)$  désignera la première composante, en partant de la gauche, non nulle de  $\alpha - \beta$  i.e.  $\ell(\alpha, \beta) := \min\{r \in \llbracket 1, n \rrbracket \mid a_r \neq b_r\}$ .

Montrons tout d'abord que c'est bien une relation d'ordre.

**Réflexivité :**

$X^\alpha \geq X^\alpha$  (c.f. premier cas)

**Antisymétrie :**

Supposons que  $X^\alpha \geq X^\beta$  (i) et  $X^\beta \geq X^\alpha$  (ii).

Supposons, par l'absurde, que  $X^\alpha \neq X^\beta$ .

On a avec (i) que  $\alpha_{\ell(\alpha, \beta)} > \beta_{\ell(\alpha, \beta)}$  et avec (ii) que  $\alpha_{\ell(\alpha, \beta)} < \beta_{\ell(\alpha, \beta)}$ . D'où une contradiction.

On a donc  $X^\alpha = X^\beta$ .

**Transitivité :**

Supposons que  $X^\alpha \geq X^\beta$  (i) et  $X^\beta \geq X^\gamma$  (ii).

Si  $\alpha = \beta$ ,  $\alpha = \gamma$  ou  $\alpha = \beta$  alors l'inégalité  $X^\alpha \geq X^\gamma$  est évidente.

Sinon, posons  $\ell := \min\{\ell(\alpha, \beta), \ell(\beta, \gamma)\}$ .

On a avec (i) et (ii), que :  $\alpha_\ell < \beta_\ell \leq \gamma_\ell$  ou  $\alpha_\ell \leq \beta_\ell < \gamma_\ell$  et pour tout  $k < \ell$ ,  $\alpha_k = \beta_k = \gamma_k$ .

On a donc  $X^\alpha \geq X^\gamma$ .

**Montrons que  $\geq_{lex}$  est compatible avec l'addition.**

Si  $\alpha = \beta$  alors  $X^{\alpha+\gamma} = X^{\beta+\gamma}$  et donc  $X^{\alpha+\gamma} \geq_{lex} X^{\beta+\gamma}$

Sinon, comme  $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$  alors  $\ell(\alpha, \beta) = \ell(\alpha + \gamma, \beta + \gamma)$  et donc si  $X^\alpha \geq_{lex} X^\beta$  alors  $X^{\alpha+\gamma} \geq_{lex} X^{\beta+\gamma}$ .

**Montrons maintenant que  $\geq_{lex}$  est un bon ordre, par l'absurde.**

Supposons donc que  $\geq_{lex}$  n'est pas un bon ordre et donc qu'il existe une suite  $u := (X^{(a_1, i, \dots, a_n, i)})_{i \in \mathbb{N}}$  strictement décroissante.

On en déduit que la suite  $u_1 := (a_{1, i})_{i \in \mathbb{N}}$  est décroissante (sinon  $u$  ne serait pas décroissante) et est donc stationnaire car  $\mathbb{N}$  est bien ordonné.

Alors il existe  $N_1 \in \mathbb{N}$  tel que  $\forall p \geq N_1, u_{1, p} = u_{1, N_1}$ .

Considérons maintenant la suite  $u_2 := (a_{2, i})_{i \geq N_1}$ . Elle est décroissante et donc stationnaire ...

On construit ainsi une suite  $(N_i)_{i \geq 1}$  tel que  $\forall n \geq N_i, u_{i, n} \geq u_{i, N_i}$ .

On en déduit que  $\forall p \geq N_n, \forall i \in \llbracket 1, n \rrbracket, u_{i, p} = u_{i, N_n}$  ou encore  $\forall p \geq N_n, X^{u_{1, p}, \dots, u_{n, p}} = X^{u_{1, N_n}, \dots, u_{n, N_n}}$ , ce qui est contradictoire avec la décroissance de  $u$ .

**Définition et propriété 1.9 (Ordre lexicographique gradué  $\geq_{grlex}$ )** Soient

$\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$  alors  $X^\alpha \geq_{grlex} X^\beta$  si, et seulement si,  $|\alpha| > |\beta|$  ou  $(|\alpha| = |\beta| \text{ et } \alpha \geq_{lex} \beta)$ .

**Définition et propriété 1.10 (Ordre lexicographique gradué renversé  $\geq_{grelex}$ )**

Soient  $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$  alors  $X^\alpha \geq_{grelex} X^\beta$  si, et

seulement si,  $|\alpha| > |\beta|$  ou  $(|\alpha| = |\beta|$  et le premier coefficient non nul en lisant par la droite de  $\beta - \alpha$  est positif).

**Exemple 1.11** *Ordre lexicographique :*

$X_1 >_{lex} X_2 >_{lex} \dots >_{lex} X_n$  Pour  $n = 3$ ,  $X^2Y^2Z^4 >_{lex} X^1Y^4Z^{42}$   
 $X^3Y^2Z^4 >_{lex} X^3Y^2Z^3$

*Ordre lexicographique graduée :*

$X_1 >_{grlex} X_2 >_{grlex} \dots >_{lex} X_n$

Pour  $n = 3$ ,

$XY^4Z^8 >_{grlex} X^7Y^2Z^3$

$X^4Y^7Z >_{grlex} X^3Y^3Z^6$

*Ordre lexicographique graduée renversée :*

$X_1 >_{grevlex} X_2 >_{grevlex} \dots >_{lex} X_n$

Pour  $n = 3$ ,

$X^5Y^3Z^2 >_{grevlex} X^3Y^2Z^4$

$X^4Y^3Z^2 >_{grevlex} X^2Y^5Z^2$

## 2 Algorithme de division

**Lemme 2.1** Soit  $\alpha, \alpha_1, \dots, \alpha_n \in \mathbb{N}^n$  tel que :  $X^\alpha > X^{\alpha_1} > \dots > X^{\alpha_n}$ . Soit  $f, g \in k[X_1, \dots, X_n]$  tels que  $LT(f) = LT(g)$  alors  $LM(f - g) < LT(f) = LT(g)$

**Démonstration 2.2** Soit  $f := pX^\alpha + \sum p_{\alpha_i}X^{\alpha_i}$  et  $g := pX^\alpha + \sum q_{\alpha_i}X^{\alpha_i}$  alors  $LM(f - g) = LM(\sum p_{\alpha_i}X^{\alpha_i}) \leq X^{\alpha_1} < X^\alpha = LM(f) = LM(g)$

**Théorème 2.3**

---

**Algorithme 1** Algorithme de division

---

**Entrées :**  $f_1, \dots, f_s, f$ **Sortie :**  $a_1, \dots, a_s, r$  $a_1 := 0; \dots; a_s := 0; r := 0$  $p := 0$ **Tant que**  $p \neq 0$  **faire** $i := 1$  $divisionoccured := false$ **Tant que**  $i \leq s$  **et**  $divisionoccured = false$  **faire****Si**  $LT(f_i) | LT(p)$  **alors** $a_i := a_i + LT(p) / LT(f_i)$  $p := p - (LT(p) / LT(f_i)) f_i$ **Sinon** $i := i + 1$ **fin Si****fin Tant que****Si**  $divisionoccured = false$  **alors** $r := r + LT(p)$  $p := p - LT(p)$ **fin Si****fin Tant que**

---

**Démonstration 2.4** Remarquons tout d'abord que lors de chaque itération de la boucle, une de ses deux instructions :

1. Si  $LT(f_i) | LT(p)$  alors on fait la division de  $p$  par  $f_i$
2. Sinon on ajoute  $LT(p)$  à  $r$  (et on retire  $LT(p)$  à  $p$ ).

Montrons d'abord que l'algorithme s'arrête i.e. il existe une étape où  $p = 0$ . Pour cela, montrons que la suite des monômes dominants des différentes valeurs  $p$  est strictement décroissante tant que  $p \neq 0$ . Si l'algorithme ne s'arrêtait pas, on aurait une suite infinie strictement croissante ce qui contredit le fait que  $\geq$  est un bon ordre.

-Si on fait une division (par  $f_j$ ) alors  $p$  prend la valeur  $p' := p - \frac{LT(p)}{LT(f_j)} f_j$ .  
-Si cette valeur est nulle alors l'algorithme s'arrête sinon comme on a l'égalité

$$: LT \left( \underbrace{\frac{LT(p)}{LT(f_j)} f_j}_{\in k^* \mathcal{M}} \right) = \frac{LT(p)}{LT(f_j)} LT(f_j) = LT(p).$$

On en déduit donc, d'après le lemme, que  $LM(p') < LM(p)$ .

-Sinon,  $p$  prend la valeur  $p - LT(p)$ . Par le même argument que précédemment,  $LM(p - LT(p)) < LM(p)$ .

Ce qui permet de conclure.

Montrons maintenant qu'à chaque étape que  $f = \sum_{i=0}^s a_i f_i + p + r$ .

Initialisation de l'algorithme ("0ème itération") : Comme  $a_1 = \dots = a_s = r = 0$  et  $p = f$  alors l'égalité est vérifiée.

Hérédité : Soit  $n \in \mathbb{N}$  et supposons qu'à la  $n$ ème itération de la boucle,  $f = \sum_{i=0}^s a_i f_i + p + r = \sum_{i=0, i \neq j}^s a_i f_i + a_j f_j + p + r$  pour tout  $j \in \llbracket 1, n \rrbracket$  alors :

- si on fait une division ( $p$  avec  $f_j$ ) alors : la nouvelle valeur  $p'$  de  $p$  est  $p - \frac{LT(p)}{LT(f_j)} f_j$  et celle de  $a_i$  est  $a'_j = a_j + \frac{LT(p)}{LT(f_j)}$ . et donc :

$\sum_{i=0, i \neq j}^s a_i f_i + a'_j f_j + p' + r = \sum_{i=0, i \neq j}^s a_i f_i + \left( a_j + \frac{LT(p)}{LT(f_j)} \right) f_j + p - \frac{LT(p)}{LT(f_j)} f_j + r$   
 $= \sum_{i=0, i \neq j}^s a_i f_i + a_j f_j + p + r = f$ . On obtient donc, lorsque  $p = 0$  (et on sait que cela arrivera), que  $f = \sum_{i=1}^s a_i f_i + r$  et  $r$  est, par définition dans l'algorithme, une somme d'éléments non divisibles par les  $LT(f_i)$

### 3 Idéaux monomiaux

**Définition 3.1** Un idéal monomial est un idéal de  $k[X_1, \dots, X_n]$  tel qu'il existe une partie  $A$  de  $\mathbb{N}^n$  telle que  $I = \langle X^\alpha | \alpha \in A \rangle = \{ \sum P_\alpha X^\alpha | P_\alpha \in k[X_1, \dots, X_n] \}$ .

**Lemme 3.2** Soit  $I := \langle X^\alpha | \alpha \in A \rangle$  un idéal monomial. Alors  $X^\beta \in I$  ssi il existe un  $\alpha \in A$  tel que  $X^\alpha$  divise  $X^\beta$ .

**Démonstration 3.3**  $\Leftarrow$  Evident

$\Rightarrow$  Si  $X^\beta \in I$  alors il existe une famille de polynômes  $P_1, \dots, P_s \in k[X_1, \dots, X_n]$  et d'exposants  $\alpha_1, \dots, \alpha_s \in \mathbb{N}^n$  telle que  $X^\beta = \sum_{i=1}^s P_i X^{\alpha_i}$ .

On peut alors remarquer qu'en utilisant les expressions  $P_i := \sum p_{i,\alpha} X^\alpha$  alors  $X^\beta$  est de la forme  $\sum_{\gamma \in \Gamma} p_\gamma X^\gamma$  où  $\Gamma := \{\gamma \in \mathbb{N}^n | \exists n \in \mathbb{N}, \exists i \in \llbracket 1, s \rrbracket, \gamma = \alpha_i + n\}$ .

Et donc  $X^\beta - \sum_{\gamma \in \Gamma} p_\gamma X^\gamma = 0$  (\*)

Comme  $k[X_1, \dots, X_n]$  est un  $k$ -espace vectoriel dont  $\mathcal{M}$  est une base, on

déduit de (\*) que  $p_\gamma = \begin{cases} 0 & \text{si } \gamma \neq \beta \\ 1 & \text{sinon} \end{cases}$  (dans le cas contraire, on aurait une

combinaison linéaire (d'élément d'une base) nulle à coefficients non nuls).

On en déduit que  $\beta \in \Gamma$  et donc qu'il existe un  $n \in \mathbb{N}^n$  et un  $i \in \llbracket 1, s \rrbracket$ ,  $\beta = \alpha_i + n$  c'est-à-dire qu'il existe un  $i \in \llbracket 1, s \rrbracket$  tel que  $X^{\alpha_i}$  divise  $X^\beta$ .

**Lemme 3.4** Soit  $I$  un idéal monomial et  $f \in k[X_1, \dots, X_n]$ .

Les propositions suivantes sont équivalentes :

1.  $f \in I$ .
2. Tous les termes de  $f$  sont dans  $I$ .
3.  $f$  est une  $k$ -combinaison linéaire de monômes dans  $I$ .

**Démonstration 3.5** (3)  $\Rightarrow$  (2)  $\Rightarrow$  (1) est évident.

(1)  $\Leftrightarrow$  (3) se montre comme le lemme précédent.

**Corollaire 3.6** Deux idéaux monomiaux sont égaux ssi ils contiennent les mêmes monômes.

**Démonstration 3.7**  $\Rightarrow$  Evident

$\Leftarrow$  Soit  $I, I'$  deux idéaux monomiaux tel que  $I \cap \mathcal{M} = I' \cap \mathcal{M}$ .

Si  $f := \sum p_\alpha X^\alpha$  alors d'après le lemme précédent, pour tout  $\alpha \in A$ , le monôme  $X^\alpha \in I$  alors, par hypothèse,  $X^\alpha \in I' \cap \mathcal{M}$  d'où  $X^\alpha \in I'$  et en réutilisant le lemme,  $f \in I'$ .

On en déduit que  $I \subset I'$  et donc par symétrie de rôle de  $I$  et  $I'$ ,  $I = I'$ .

**Lemme 3.8** Soit  $I := \langle X^\alpha | \alpha \in A \rangle$  un idéal monomial et supposons qu'il ait une base finie  $\langle X^{\beta_1}, \dots, X^{\beta_s} \rangle$ . Supposons aussi qu'il existe une famille  $\alpha_1, \dots, \alpha_s$  tel que pour tout  $i \in \llbracket 1, s \rrbracket$ ,  $X^{\alpha_i}$  divise  $X^{\beta_i}$  (\*) alors  $I = \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$ .

**Démonstration 3.9** D'après (\*), on a :  $\forall i \in \llbracket 1, s \rrbracket, X^{\beta_i} \in \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$ .  
D'où, comme on a, de plus,  $X^{\alpha_1}, \dots, X^{\alpha_s} \in I$ ,  
 $I = \langle X^{\beta_1}, \dots, X^{\beta_s} \rangle \subset \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle \subset I$ .  
On en déduit que  $I = \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$

**Théorème 3.10 (Lemme de Dickson)** Un idéal monomial  $I := \langle X^\alpha | \alpha \in A \rangle$  peut être écrit sous la forme  $I = \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$ , où  $\alpha_1, \dots, \alpha_s$ . En particulier,  $I$  admet une base finie.

**Démonstration 3.11** A faire.

## 4 Bases de Gröbner

### 4.1 Généralités

**Notation 4.1** Soit  $I$  un idéal non réduit à  $\{0\}$  de  $k[X_1, \dots, X_n]$ .  
On note  $LT(I)$  l'ensemble des termes dominants des éléments de  $I$  i.e.  
 $LT(I) := \{cX^\alpha | \exists f \in I, LT(f) = cX^\alpha\}$

**Lemme 4.2** Soient  $A \subset k[X_1, X_n]$  et  $(p_i)_{i \in A}$  une suite d'éléments de  $k^*$ . Alors  
:  
 $\langle p_f f | f \in A \rangle = \langle A \rangle$  (\*)  
En particulier,  $\langle LT(f) | f \in A \setminus \{0\} \rangle = \langle LM(f) | f \in A \setminus \{0\} \rangle$  car pour tout  
 $f \in k[X_1, \dots, X_n], f \neq 0, LT(f) = LC(f)LM(f)$

**Démonstration 4.3** On notera  $I_1$  l'idéal à gauche de l'égalité (\*) et  $I_2$  celui de droite.

$\subset$  : Soit  $P = \sum_{f \in A} \alpha_f (p_f f) \in I_1$  alors, par associativité du produit,  $P = \sum_{f \in A} (\alpha_f p_f) f \in I_2$

$\supset$  : Soit  $P = \sum_{f \in A} \alpha_f f \in I_2$  alors, par associativité du produit,  $P = \sum_{f \in A} \frac{\alpha_f}{p_f} (p_f f) \in I_1$

**Propriété 4.4** Soit  $I \subset k[X_1, \dots, X_n]$  un idéal. Alors :

1.  $LT(I)$  est un idéal monomial.
2. Il existe  $g_1, \dots, g_s \in I$  tel que :  $LT(I) = \langle LT(g_1), \dots, LT(g_s) \rangle$ .

**Démonstration 4.5** (1) D'après le lemme précédent, on a  $\langle LM(g) | g \in I \setminus \{0\} \rangle = \langle LT(g) | g \in I \setminus \{0\} \rangle = LT(I)$  ce qui montre que  $LT(I)$  est un idéal monomial.



(2) Comme  $LT(I)$  est un idéal monomial engendré par  $LM(g)$  (avec  $g \in I \setminus \{0\}$ ) alors, d'après le lemme de Dickson, il existe  $g_1, \dots, g_s$  tel que  $LT(I) = \langle LM(g_1), \dots, LM(g_s) \rangle$ . On conclut en utilisant le lemme précédent :

$$LT(I) = \langle LM(g_1), \dots, LM(g_s) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$$

**Théorème 4.6 (de la base d'Hilbert)** *Tout idéal  $I$  de  $k[X_1, \dots, X_n]$  admet une base finie.*

**Démonstration 4.7** *Si  $I = \{0\}$  alors  $I$  est engendré par la famille finie  $\{0\}$ .*

*Sinon, on a, d'après la proposition précédente, l'existence de  $f_1, \dots, f_s \in I$ ,  $LT(I) = \langle LT(f_1), \dots, LT(f_s) \rangle$ . Montrons que  $I = \langle f_1, \dots, f_s \rangle$ .*

$\supset : f_1, \dots, f_s \in I$

$\subset : \text{Soit } f \in I \text{ alors la division de } f \text{ par } f_1, \dots, f_s \text{ s'écrit : } f = \sum_{i=1}^s \alpha_i f_i + r$   
où chaque terme de  $r$  n'est pas divisible par des  $LT(f_i)$ .

*Pour montrer l'inclusion, il nous faut montrer que  $r = 0$ .*

*Supposons, par l'absurde, que  $r \neq 0$ .*

*On a  $r = f - \sum_{i=1}^s \alpha_i f_i \in I$  d'où  $LT(r) \in \langle LT(I) \rangle = \langle f_1, \dots, f_s \rangle$ .*

*Alors d'après le lemme 2 du ch 4, on a  $LT(r)$  est divisible avec un des  $LT(f_i)$  ce qui est en contradiction avec la définition de  $r$ .*

*On en déduit alors que  $r = 0$  et donc  $f \in \langle f_1, \dots, f_s \rangle$ .*

**Définition 4.8** *Soit  $\geq$  un ordre monomial. Un sous-ensemble  $G = \{g_1, \dots, g_s\}$  d'un idéal  $I$  est une base de Gröbner si  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$ .*

**Définition 4.9** *Corollaire : Soit  $\geq$  un ordre monomial. Alors tout idéal de  $k[X_1, \dots, X_n]$  non réduit à  $\{0\}$  a une base de Gröbner. De plus, tout base de Gröbner est une base de  $I$ .*

**Démonstration 4.10** *(cf celle du théorème de la base d'Hilbert.)*

## 4.2 Propriétés des bases de Gröbner

**Propriété 4.11** *Soit  $G = \{g_1, \dots, g_s\}$  une base de Gröbner d'un idéal  $I$  de  $k[X_1, \dots, X_n]$  et  $f \in I$ . Alors il existe un unique  $r \in k[X_1, \dots, X_n]$  vérifiant :*

1. *Tous les termes de  $r$  ne sont divisible par aucun des  $LT(g_i)$*
2. *Il existe  $g \in I$  tel que  $f = g + r$*

**Démonstration 4.12** *L'algorithme de division nous donne l'existence d'un tel  $r$ . Montrons son unicité.*

*Supposons, par l'absurde, l'existence de deux restes  $r_1$  et  $r_2$ ,  $r_1 \neq r_2$  vérifiant (1) et (2).*

*Alors :* 
$$\begin{cases} f = g_1 + r_1 \\ f = g_2 + r_2 \end{cases} \quad \text{et donc } r_1 - r_2 = g_1 - g_2 \in I.$$

*D'où, comme  $r_1 \neq r_2$  alors  $LT(r_1 - r_2) \in \langle LT(I) \rangle = \langle g_1, \dots, g_s \rangle$  et donc  $LT(r_1 - r_2)$  est divisé par un des  $LT(g_i)$  (cf Lemme 2 para 4). On obtient donc une contradiction car aucun terme de  $r_1$  et  $r_2$  n'est divisible par des  $LT(g_i)$ . D'où  $r_1 = r_2$ .*

**Corollaire 4.13** *Soit  $G = \{g_1, \dots, g_s\}$  une base de Gröbner d'un idéal  $I$  de  $k[X_1, \dots, X_n]$  et  $f \in k[X_1, \dots, X_n]$ . Alors  $f \in I$  ssi le reste de la division de  $f$  par  $G$  est nul.*

**Démonstration 4.14**  $\Leftarrow$  : *Evident*

$\Rightarrow$  : *Soit  $f \in I$ . La décomposition  $f = f + 0$  respecte les deux conditions de la proposition. Alors par unicité du reste, le reste de la division de  $f$  par  $G$  est nul.*

**Notation 4.15** *On notera  $\overline{f}^F$  le reste de  $f$  par le  $n$ -uple ordonné  $F = \{f_1, \dots, f_s\}$ . Si  $f$  est une base de Gröbner alors on peut considérer  $F$  comme un ensemble.*

**Définition 4.16** *Soit  $f, g \in k[X_1, \dots, X_n]$  des polynômes non nuls.*

1. *Si  $\text{multideg}(f) = \alpha = (\alpha_1, \dots, \alpha_n)$  et  $\text{multideg}(g) = \beta = (\beta_1, \dots, \beta_n)$  alors posons  $\gamma = (\gamma_1, \dots, \gamma_n)$  où  $\gamma_i = \max(\alpha_i, \beta_i)$ . On appelle  $X^\gamma$  le plus petit multiple commun de  $LM(f)$  et  $LM(g)$ , noté  $\text{PPCM}(LM(f), LM(g)) := X^\gamma$ .*

2. *Le  $S$ -polynôme de  $f$  et  $g$  est le polynôme :  $S(f, g) := \frac{X^\gamma}{LT(f)}f - \frac{X^\gamma}{LT(g)}g$*

**Lemme 4.17** *Soit  $G = \sum_{i=1}^s c_i X^{\alpha_i} g_i$ , où  $c_1, \dots, c_s \in k$  et  $\alpha_i + \text{multideg}(g_i) = \delta \in \mathbb{N}^n$  pour  $c_i \neq 0$ .*

*Si  $LM(G) < X^\delta$  alors il existe des constantes  $(c_{j,k})$  tel que  $G = \sum_{j,k} c_{j,k} X^{\delta - \gamma_{j,k}} S(g_j, g_k)$  où  $X^{\gamma_{j,k}} = \text{PPCM}(LT(g_j), LT(g_k))$ . De plus, chacun des  $X^{\delta - \gamma_{j,k}}$  est strictement inférieur à  $X^\delta$ .*

**Démonstration 4.18** *A faire*

**Théorème 4.19** Soit  $I$  un idéal de  $k[X_1, \dots, X_n]$ . Alors une base  $G = \{g_1, \dots, g_n\}$  de  $I$  est une base de Gröbner de  $I$  ssi pour tout couple  $(i, j)$ ,  $i \neq j$ ,  $\overline{S(g_i, g_j)}^G = 0$

**Démonstration 4.20** A faire

## 5 Algorithme de Buchberger

---

**Algorithme 2** Algorithme de Buchberger

---

**Entrées :**  $F = (f_1, \dots, f_s)$

**Sortie :** Une base de Gröbner  $G = (g_1, \dots, g_t)$  de  $I$ , avec  $F \subset G$

$G := F$

**repeat**

$G' := G$

**Pour** chaque paire  $\{p, q\} \in G'^2$ ,  $p \neq q$  **faire**

$S := \overline{S(p, q)}^{G'}$

**Si**  $S \neq 0$  **alors**

$G := G \cup \{S\}$

**fin Si**

**fin Pour**

**Jusqu'à**  $G = G'$

---

**Lemme 5.1** Soit  $G$  une base de Gröbner d'un idéal  $I$  de  $k[X_1, \dots, X_n]$  et  $P \in G$  tel que  $LT(P) \in \langle LT(G \setminus \{P\}) \rangle$ . Alors  $G \setminus \{P\}$  est une base de Gröbner de  $I$ .

**Démonstration 5.2** Comme  $G$  est une base de Gröbner de  $I$  alors  $\langle LT(G) \rangle = \langle LT(I) \rangle$ . Si  $LT(P) \in \langle LT(G \setminus \{P\}) \rangle$  alors  $\langle LT(G \setminus \{P\}) \rangle = \langle LT(G) \rangle = \langle LT(I) \rangle$  d'où  $G \setminus \{P\}$  est une base de Gröbner de  $I$ .

**Définition 5.3** Une base de Gröbner minimale d'un idéal  $I$  de  $k[X_1, \dots, X_n]$  est une base de Gröbner de  $I$  telle que :

1.  $\forall P \in G, LC(P) = 1$

2.  $\forall P \in G, LT(P) \notin \langle LT(G \setminus \{P\}) \rangle$

**Définition 5.4** Une base de Gröbner réduite d'un idéal  $I$  de  $k[X_1, \dots, X_n]$  est une base de Gröbner de  $I$  telle que :

1.  $\forall P \in G, LC(P) = 1$

2. Pour tout  $P \in G$ , aucun monôme de  $P$  n'appartient à  $\langle LT(G \setminus \{P\}) \rangle$ .

**Propriété 5.5** Soit  $I$  un idéal non nul de  $k[X_1, \dots, X_n]$ . Alors, pour un ordre monomial fixé,  $I$  a une unique base de Gröbner réduite.

**Démonstration 5.6** A faire

## 6 Théorème d'élimination et d'extension

**Définition 6.1** Soit  $I = \langle f_1, \dots, f_s \rangle$  un idéal de  $k[X_1, \dots, X_n]$ . On appelle  $k$ ème idéal d'élimination de  $I$  l'idéal  $I_k$  de  $k[X_{k+1}, \dots, X_n]$  défini par :  $I_k = k[X_{k+1}, \dots, X_n] \cap I$

**Théorème 6.2 (d'élimination)** Soit  $I$  un idéal de  $k[X_1, \dots, X_n]$  et  $G$  une base de Gröbner de  $I$  selon l'ordre lexicographique (que l'on notera ici seulement  $\geq$ ). Alors, pour tout  $k \in \llbracket 0, n \rrbracket$ , l'ensemble  $G_k = G \cap k[X_{k+1}, \dots, X_n]$  est une base de Gröbner du  $k$ ème idéal d'élimination  $I_k$ .

**Démonstration 6.3** Soit  $k \in \llbracket 0, n \rrbracket$ . Posons  $G = \{g_1, \dots, g_m\}$  et tel que  $G_k = \{g_1, \dots, g_r\}$  (quitte à renommer les éléments).

Montrons que  $G_k$  est une base de  $I_k$ .

Comme  $G_k \subset I_k$  (car  $G \subset I$ ) alors  $\langle G_k \rangle \subset I_k$ .

Soit  $f \in I_k$  alors d'après le théorème de division par  $G$ , il existe  $h_1, \dots, h_m \in k[X_1, \dots, X_n]$ ,

$f = \sum_{i=1}^m h_i g_i$  car ( $G$  est une base de Gröbner de  $I$  et  $f \in I$ )

or pour tout  $k > r, g_i > X^{k+1} \geq LM(f)$  et donc aucun terme de  $f$  ne peut être divisible par un  $LT(g_i)$ . L'algorithme n'incrmente pas les  $h_k (k > r)$  et donc sont tous nuls.

D'où,  $f = \sum_{i=1}^r h_i g_i$  et donc  $f_k \in \langle G_k \rangle$ , ce qui finit de montrer l'égalité  $\langle G_k \rangle = I_k$ .

(Le même argument permet de montrer que si  $f \in I_k, \bar{f}^G = \bar{f}^{G_k}$ ).

Montrons maintenant que  $G$  est une base de Gröbner de  $I_k$ .

Il suffit, pour cela, de montrer que pour tout  $1 \leq i < j \leq r, \overline{S(g_i, g_j)}^{G_k} = 0$ .

Soit  $i, j \in \llbracket 1, r \rrbracket, i < j$ .

Comme  $S(g_i, g_j)$  est de la forme  $Pg_i + Qg_j$  ( $P, Q \in k[X_{k+1}, \dots, X_n]$ ) et  $I_k$  est un idéal alors  $S(g_i, g_j) \in I_k \subset I$  d'où comme  $G$  est une base de Gröbner

alors  $\overline{S(g_i, g_j)}^G = 0$  et donc d'après la remarque précédente,

$\overline{S(g_i, g_j)}^{G_k} = 0$ . Ce qui permet de conclure.

**Théorème 6.4 (d'extension)** Soit  $I = \langle f_1, \dots, f_s \rangle$  un idéal de  $\mathbb{C}[X_1, \dots, X_n]$  et  $I_1$  le premier idéal d'élimination.

Ecrivons, pour  $i \in \llbracket 1, s \rrbracket$ ,  $f_i$  sous la forme

$$f_i = g(X_2, \dots, X_n)X_1^{N_i} + \text{termes de degré} < N_i \text{ en } X_1$$

où  $N_i \geq 0$  et  $g_i \in \mathbb{C}[X_2, \dots, X_n]$  non nul si  $f_i \neq 0$  ( $g_i = 0$  si  $f_i = 0$ ).

Supposons qu'on ait une solution partiel  $(a_2, \dots, a_n) \in Z(I_1)$ . Si  $(a_2, \dots, a_n) \notin Z(g_1, \dots, g_s)$  alors il existe  $a_1 \in \mathbb{C}$  tel que  $(a_1, \dots, a_n) \in Z(I)$ .

**Corollaire 6.5** Soit  $I = \langle f_1, \dots, f_s \rangle$  un idéal de  $\mathbb{C}[X_1, \dots, X_n]$  et supposons qu'il existe  $i \in \llbracket 1, s \rrbracket$  tel que  $f_i$  s'écrit de la forme

$$f_i = cX_1^N + \text{termes de degré} < N \text{ en } X_1$$

où  $N > 0$  et  $c \in \mathbb{C} \neq \{0\}$  non nul. Si  $I_1$  est le premier idéal d'élimination de  $I$  et  $(a_2, \dots, a_n) \in Z(I_1)$  alors il existe  $a_1 \in \mathbb{C}$  tel que  $(a_1, \dots, a_n) \in Z(I)$ .

**Démonstration 6.6** Conséquence immédiate du théorème d'extension.

(Comme  $g_i = c \neq 0$  alors  $Z(g_1, \dots, g_s) = \emptyset$  et donc  $(a_2, \dots, a_n) \notin Z(g_1, \dots, g_s)$  pour tout  $(a_2, \dots, a_n) \in \mathbb{C}^{n-1}$ ).

## 7 Géométrie

### 7.1 Généralités

**Définition 7.1** Soit  $f_1, \dots, f_s$  des polynômes de  $k[X_1, \dots, X_n]$ . On appelle variété affine définie par  $f_1, \dots, f_s$  l'ensemble :  $Z(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n \mid \forall i \in \llbracket 1, s \rrbracket, f_i(a_1, \dots, a_n) = 0\}$ .

**Exemple 7.2** Cercle ; graphe d'une fonction polynomiale / fonction rationnelle ; Paraboloïde de révolution ; Cône ; "Twisted Cubic"

**Lemme 7.3** : Si  $V, W \subset k^n$  sont des variétés affines alors  $V \cup W$  et  $V \cap W$  aussi.

**Démonstration 7.4** Supposons  $V = Z(f_1, \dots, f_s)$  et  $W = Z(g_1, \dots, g_r)$ .

Alors  $V \cap W = Z(f_1, \dots, f_s, g_1, \dots, g_r)$  et  $V \cup W = Z(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq r)$  (que l'on notera  $Z(f_i g_j)$ ).

Montrons la deuxième égalité :

Soit  $a = (a_1, \dots, a_n) \in V$  alors  $\forall i \in \llbracket 1, s \rrbracket, f_i(a) = 0$  et donc  $\forall i \in \llbracket 1, s \rrbracket, \forall j \in \llbracket 1, r \rrbracket, f_i g_j(a) = 0$  d'où  $V \subset Z(f_i g_j)$ . On obtient de la même façon que  $W \subset Z(f_i g_j)$ . D'où  $V \cup W \subset Z(f_i g_j)$ .

Soit  $a = (a_1, \dots, a_n) \in Z(f_i g_j)$ . Si  $a \in V$  alors c'est fini. Sinon, il existe un  $i_0 \in \llbracket 1, s \rrbracket$  tel que  $f_{i_0}(a) = 0$ . Alors, comme pour tout  $j \in \llbracket 1, r \rrbracket, f_{i_0}(a)g_j(a) = 0$ , tous les  $g_j(a)$  sont nuls et donc  $a \in W$ .

On en déduit donc  $Z(f_i g_j) \subset V \cup W$  et donc l'égalité voulue.

**Définition 7.5** Soit  $V = Z(f_1, \dots, f_s) \subset k^n$ . Alors une représentation paramétrique de  $V$  consiste en des fractions rationnelles  $r_1, \dots, r_n \in k(X_1, \dots, X_n)$  telles que les points  $(x_1, \dots, x_n)$  tels que  $\forall j \in \llbracket 1, n \rrbracket, x_j = r_j(t_1, \dots, t_n)$  sont dans  $V$ .

**Définition 7.6**  $I$  est dit finement engendré s'il existe  $f_1, \dots, f_s$  tels que  $I = \langle f_1, \dots, f_s \rangle$ .  $\{f_1, \dots, f_s\}$  est alors appelée base de  $I$ .

**Propriété 7.7** Si  $\{f_1, \dots, f_s\}$  et  $\{g_1, \dots, g_r\}$  sont des bases d'un même idéal de  $k[X_1, \dots, X_n]$  alors  $Z(f_1, \dots, f_s) = Z(g_1, \dots, g_r)$

**Définition 7.8** Soit  $V \subset k^n$  une variété affine. Alors on pose  $I(V) := \{f \in k[X_1, \dots, X_n] \mid \forall a \in V, f(a) = 0\}$

**Lemme 7.9** Soit  $V \subset k^n$  une variété affine. Alors  $I(V)$  est un idéal de  $k[X_1, \dots, X_n]$ , appelé idéal de  $V$ .

**Démonstration 7.10**  $0_{k[X_1, \dots, X_n]} \in I(V)$  car  $\forall x \in k^n, 0_{k[X_1, \dots, X_n]}(x) = 0$ . Soit  $f, g \in I(V)$  et  $a \in V$  alors  $(f + g)(a) = f(a) + g(a) = 0$  et donc  $f + g \in I(V)$ . Soit  $f \in I(V)$ ,  $h \in k[X_1, \dots, X_n]$  et  $a \in V$  alors  $(fh)(a) = f(a)h(a) = 0h(a) = 0$  et donc  $fh \in I(V)$ .

**Lemme 7.11** Soit  $f_1, \dots, f_s \in k[X_1, \dots, X_n]$ . Alors  $\langle f_1, \dots, f_s \rangle \subset I(Z(f_1, \dots, f_s))$ . L'inclusion réciproque n'est pas toujours vraie.

**Démonstration 7.12** Soit  $f \in \langle f_1, \dots, f_s \rangle$  i.e. il existe  $h_1, \dots, h_s$  tels que  $f = \sum_{i=1}^s h_i f_i$ . Comme  $f_1, \dots, f_s$  s'annule en  $V(f_1, \dots, f_s)$  alors  $f = \sum_{i=1}^s h_i f_i$  aussi, ce qui permet de dire que  $f \in I(Z(f_1, \dots, f_s))$

**Exemple 7.13**  $\langle X^2, Y^2 \rangle \neq I(Z(X^2, Y^2))$ .

**Propriété 7.14** Soit  $V \subset W$  des variétés affines de  $k^n$ . Alors :

1.  $V \subset W$  ssi  $I(V) \supset I(W)$
2.  $V = W$  ssi  $I(V) = I(W)$

**Démonstration 7.15** (1)  $\Rightarrow$  (2) . Montrons donc (1).

$\Rightarrow$  : Supposons  $V \subset W$ . Soit  $f \in I(W)$  alors pour tout  $a \in W$  et, en particulier, pour tout  $a \in V, f(a) = 0$ , c'est-à-dire  $f \in I(V)$  d'où  $I(W) \subset I(V)$ .

$\Leftarrow$  : Supposons  $I(W) \subset I(V)$ . Comme  $W$  est une variété alors il existe  $g_1, \dots, g_s \in k[X_1, \dots, X_n]$  tels que  $W = Z(g_1, \dots, g_s)$  alors  $g_1, \dots, g_s \in I(W) \subset I(V)$  et donc les  $g_i$  s'annulent sur  $V$ .

Comme  $W$  est l'ensemble des points sur lesquels les  $g_i$  s'annulent alors  $V \subset W$ .

## 7.2 Géométrie de l'élimination

Soit  $V = Z(f_1, \dots, f_s) \subset \mathbb{C}^n$

**Définition 7.16** Soit  $\pi_k$  la projection  $\mathbb{C}^n \rightarrow \mathbb{C}^{n-k}$  définie par :  $\forall (a_1, \dots, a_n) \in \mathbb{C}^n, \pi_k(a_1, \dots, a_n) = (a_{k+1}, \dots, a_n)$ . (Cette application est surjective)

**Lemme 7.17** Soit  $I_k$  le  $k$ ème idéal d'élimination de l'idéal  $\langle f_1, \dots, f_s \rangle$  de  $\mathbb{C}[X_1, \dots, X_n]$ . Alors, dans  $\mathbb{C}^{n-k}$ ,  $\pi_k(V) \subset Z(I_k)$ .

**Démonstration 7.18** Pour montrer cette égalité, il faut montrer que  $\forall a \in \pi_k(V), \forall f \in I_k, f(a) = 0$ .

Soient  $a = (a_{k+1}, \dots, a_n) \in \pi_k(V)$  et  $f \in I_k$ .

Comme  $\pi_k$  est surjective alors il existe un  $a' = (a_1, \dots, a_n)$  qui appartient à  $V$ . Alors  $f(a') = 0$  (car  $f \in \langle f_1, \dots, f_s \rangle$ ). Or comme  $f$  ne dépend que de  $X_{k+1}, \dots, X_n$  alors  $f(a) = f(a') = 0$ .

**Théorème 7.19** Soit  $g_i$  défini dans le théorème d'extension et  $I_1$  le premier idéal d'élimination de  $\langle f_1, \dots, f_s \rangle$ . On a alors l'égalité, dans  $\mathbb{C}^{n-1}$ ,  $Z(I_1) = \pi(V) \cup (Z(g_1, \dots, g_s) \cap Z(I_1))$

**Démonstration 7.20**  $\supset$  : c.f. Lemme 1

$\subset$  : Soit  $a := (a_2, \dots, a_n) \in Z(I_1)$ . Alors si  $a \notin \langle g_1, \dots, g_s \rangle$ , on a, d'après le théorème d'extension, l'existence d'un  $a_1 \in \mathbb{C}$  tel que  $(a_1, \dots, a_n) \in V$  et donc  $a \in \pi_1(V)$ .

Sinon  $a \in \langle f_1, \dots, f_s \rangle$  et donc dans  $\langle f_1, \dots, f_s \rangle \cap V(I_1)$

**Théorème 7.21 (de fermeture)** Soit  $V = Z(f_1, \dots, f_s) \subset \mathbb{C}^n$  et soit  $I_k$  le  $k$ ème idéal d'élimination de  $\langle f_1, \dots, f_s \rangle$ . Alors

1.  $Z(I_k)$  est la plus petite (au sens de l'inclusion) variété contenant  $\pi_k(V)$
2. Si  $V \neq \emptyset$ , alors il existe une variété affine  $W \subsetneq Z(I_k)$  telle que  $V(I_k) \setminus W \subset \pi_k(V)$

**Corollaire 7.22** Supposons qu'il existe  $i \in \llbracket 1, n \rrbracket$  tel que  $f_i$  s'écrit de la forme :  $f_i = cX_1^N + \text{termes de degré} < N \text{ en } X_1$  où  $N > 0$  et  $c \in \mathbb{C} \setminus \{0\}$  non nul.

Alors  $\pi(V) = V(I_1)$