

Bases de Gröbner

Antoine BOIVIN

2 décembre 2016

Table des matières

1	Ordre monomial	2
1.1	Généralités	2
1.2	Exemples d'ordres monomiaux	3
2	Algorithme de division	5
3	Idéaux monomiaux	6
4	Bases de Gröbner	8
4.1	Généralités	8
4.2	Propriétés des bases de Gröbner	10
5	Algorithme de Buchberger	11
6	Théorèmes d'élimination et d'extension	12
7	Géométrie	14
7.1	Généralités	14
7.2	Géométrie de l'élimination	16
8	Nullstellensatz	17
A	Graphe	18
A.1	Généralités	18
A.2	Equations polynomiales	19

B	Ordre	19
C	Anneau noethérien	20
D	Algèbre	22
D.1	Polynômes irréductibles et factorisation	22
E	Résultant	23
F	Implication	24

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. $\forall \alpha, \beta, \gamma \in \mathbb{N}^n, X^\alpha \geq X^\beta \Rightarrow X^{\alpha+\gamma} \geq X^{\beta+\gamma}$ (compatible avec le produit)
2. \geq est un bon ordre

On note $X^\alpha > X^\beta$ si $X^\alpha \geq X^\beta$ et $\alpha \neq \beta$ 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. Comme \geq est un bon ordre alors il existe un plus petit élément que l'on notera X^α alors : $X^\alpha \leq 1$ et donc $X^{2\alpha} \leq X^\alpha$ (par la compatibilité avec le produit).

Or comme X^α 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 1.3. Soit \geq un ordre monomial et $\alpha, \beta \in \mathbb{N}^n$. Si X^α divise X^β alors $X^\alpha \leq X^\beta$.

Démonstration. Si X^α divise X^β alors il existe $\gamma \in \mathbb{N}^n$ tel que : $X^\beta = X^\gamma X^\alpha$. Or, $1 \leq X^\gamma$, d'où, par compatibilité avec le produit, $X^\alpha \leq X^{\alpha+\gamma} = X^\beta$. □

Définition 1.4. Soit $P := \sum_{\alpha} p_{\alpha} X^{\alpha} \in k[X_1, \dots, X_n]$ et \geq un ordre monomial.

1. Le monôme dominant de P est : $LM(P) := \max\{X^{\alpha} \in \mathcal{M} \mid a_{\alpha} \neq 0\}$
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 1.5 (Ordre lexicographique \geq_{lex}). Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ alors $X^{\alpha} \geq_{lex} X^{\beta}$ si, et seulement si, $\alpha = \beta$ ou le premier coefficient non nul en lisant par la gauche de $\alpha - \beta$ est positif.

Démonstration. Montrons que \geq_{lex} est un ordre monomial.

α, β, γ désigneront des éléments quelconques de \mathbb{N}^n de composantes respectives $\alpha_i, \beta_i, \gamma_i$ 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 : $\alpha_{\ell} > \beta_{\ell} \geq \gamma_{\ell}$ ou $\alpha_{\ell} \geq \beta_{\ell} > \gamma_{\ell}$ 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 le produit.

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 stricte décroissance de u . \square

Définition et propriété 1.6 (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 1.7 (Ordre lexicographique gradué renversé $\geq_{grevlex}$). Soient $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$ alors $X^\alpha \geq_{grevlex} X^\beta$ si, et seulement si, $|\alpha| > |\beta|$ ou $(|\alpha| = |\beta| \text{ et le premier coefficient non nul en lisant par la droite de } \beta - \alpha \text{ est positif})$.

Exemple 1.8. Ordre lexicographique :

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

Pour $n = 3$,

$$X^2 Y^2 Z^4 >_{lex} X^1 Y^4 Z^{42}$$

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

Ordre lexicographique graduée :

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

Pour $n = 3$,

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

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

Ordre lexicographique graduée renversée :

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

Pour $n = 3$,

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

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

2 Algorithme de division

Lemme 2.1. Soit $f, g \in k[X_1, \dots, X_n]$ tels que $\text{LT}(f) = \text{LT}(g)$ alors $\text{LM}(f - g) < \text{LM}(f) = \text{LM}(g)$

Démonstration. Soit $\alpha, \alpha_1, \dots, \alpha_n \in \mathbb{N}^n$ tel que : $X^\alpha > X^{\alpha_1} > \dots > X^{\alpha_n}$ et $f = pX^\alpha + \sum p_{\alpha_i}X^{\alpha_i}$ et $g = pX^\alpha + \sum q_{\alpha_i}X^{\alpha_i}$ alors $\text{LM}(f - g) = \text{LM}(\sum (p_{\alpha_i} - q_{\alpha_i})X^{\alpha_i}) \leq X^{\alpha_1} < X^\alpha = \text{LM}(f) = \text{LM}(g)$ \square

Algorithme 1 Algorithme de division

Théorème 2.2. 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**

$i := 1$

$\text{divisionoccured} := \text{false}$

Tant que $i \leq s$ et $\text{divisionoccured} = \text{false}$ **faire**

Si $\text{LT}(f_i) \mid \text{LT}(p)$ **alors**

$a_i := a_i + \text{LT}(p) / \text{LT}(f_i)$

$p := p - (\text{LT}(p) / \text{LT}(f_i))f_i$

Sinon

$i := i + 1$

fin Si

fin Tant que

Si $\text{divisionoccured} = \text{false}$ **alors**

$r := r + \text{LT}(p)$

$p := p - \text{LT}(p)$

fin Si

fin Tant que

Démonstration. Remarquons tout d'abord que lors de chaque itération de la boucle, une de ses deux instructions est exécutée :

1. Si $\text{LT}(f_i) \mid \text{LT}(p)$ alors on fait la division de p par f_i
2. Sinon on ajoute $\text{LT}(p)$ à r (et on retire $\text{LT}(p)$ 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 de p est strictement décroissante tant que $p \neq 0$. Si l'algorithme ne s'arrêtait pas, on aurait alors une suite infinie strictement croissante ce qui contredirait le fait que \geq soit 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 :

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

On en déduit, 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 :

$$\begin{aligned} \sum_{i=0, i \neq j}^s a_i f_i + a'_j f_j + p' + r &= \sum_{i=0, i \neq j}^s a_i f_i + \left(a_j + \frac{LT(p)}{LT(f_j)} \right) f_j + p - \frac{LT(p)}{LT(f_j)} f_j + r \\ &= \sum_{i=0, i \neq j}^s a_i f_i + a_j f_j + p + r = f. \end{aligned}$$

- sinon, $f = \sum_{i=0, i \neq j}^s a_i f_i + a_j f_j + p + r = \sum_{i=0, i \neq j}^s a_i f_i + a_j f_j + (p - LT(p)) + (r + LT(p))$.

On finit par obtenir que, lorsque $p = 0$ (et on sait que cela arrivera), $f = \sum_{i=1}^s a_i f_i + r$ où r est, par définition, 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 :

$$I = \langle X^\alpha | \alpha \in A \rangle = \left\{ \sum P_\alpha X^\alpha \mid P_\alpha \in k[X_1, \dots, X_n] \right\}.$$

Lemme 3.2. Soit $I := \langle X^\alpha | \alpha \in A \rangle$ un idéal monomial. Alors $X^\beta \in I$ si, et seulement si, il existe un $\alpha \in A$ tel que X^α divise X^β .

Démonstration. \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 $\alpha_1, \dots, \alpha_s \in A$ telle que $X^\beta = \sum_{i=1}^s P_i X^{\alpha_i}$.

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

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 de base canonique \mathcal{M} , 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 $p \in \mathbb{N}^n$ et un $i \in \llbracket 1, s \rrbracket$, $\beta = \alpha_i + p$ c'est-à-dire qu'il existe un $i \in \llbracket 1, s \rrbracket$ tel que X^{α_i} divise X^β . \square

Lemme 3.3. 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) \Rightarrow (2) \Rightarrow (1) est évident.

(1) \Rightarrow (3) se montre comme le lemme précédent. \square

Corollaire 3.4. Deux idéaux monomiaux sont égaux si, et seulement si, ils contiennent les mêmes monômes.

Démonstration. \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 $X^\alpha \in I$. Comme on a (*) alors $X^\alpha \in I' \cap \mathcal{M}$ 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' , $I = I'$. \square

Lemme 3.5. 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^{α_i} divise X^{β_i} (*) alors $I = \langle X^{\alpha_1}, \dots, X^{\alpha_s} \rangle$.

Démonstration. 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 3.6 (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. 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 $A \subset k[X_1, \dots, X_n]$ et $(p_i)_{i \in A}$ une suite d'éléments de k^* . Alors :*
 $\langle p_f f | f \in A \rangle = \langle A \rangle$ (*)

Démonstration. 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, $P = \sum_{f \in A} \frac{\alpha_f}{p_f} (p_f f) \in I_1$ □

Corollaire 4.3. *En particulier, $\langle LT(f) | f \in A \setminus \{0\} \rangle = \langle LM(f) | f \in A \setminus \{0\} \rangle$.*

Démonstration. Pour tout $f \in k[X_1, \dots, X_n], f \neq 0, LT(f) = LC(f)LM(f)$. On conclut grâce au lemme □

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

1. $\langle LT(I) \rangle$ est un idéal monomial.

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

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

(2) Comme $\langle LT(I) \rangle$ 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 : $LT(I) = \langle LM(g_1), \dots, LM(g_s) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$ \square

Théorème 4.5 (de la base de Hilbert). *Tout idéal I de $k[X_1, \dots, X_n]$ admet une base finie.*

Démonstration. Si $I = \{0\}$ alors I est engendré par la famille finie $\{0\}$. Sinon, on a, d'après la proposition précédente, l'existence de $f_1, \dots, f_s \in I$, tels que $\langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$. Montrons que $I = \langle f_1, \dots, f_s \rangle$.

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

\subset : Soit $f \in I$ alors la division de f par f_1, \dots, f_s 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 ??, $LT(r)$ est divisible par un des $LT(f_i)$ ce qui est en contradiction avec la définition de r .

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

Définition 4.6. Soit \geq un ordre monomial. Un sous-ensemble $G = \{g_1, \dots, g_s\}$ d'un idéal I est une base de Gröbner si $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Corollaire 4.7. *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. 1. c.f. prop ??

2. c.f. démonstration du théorème de la base de Hilbert. \square

4.2 Propriétés des bases de Gröbner

Propriété 4.8. 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. 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 : $\begin{cases} f = g_1 + r_1 \\ f = g_2 + r_2 \end{cases}$ 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 ??). 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 4.9. 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 $f \in I$ si, et seulement si, le reste de la division de f par G est nul.

Démonstration. \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 4.10. On notera \overline{f}^F le reste de f par le n -uplet ordonné $F = \{f_1, \dots, f_s\}$. Si F est une base de Gröbner alors on peut considérer F comme un ensemble.

Définition 4.11. 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^γ le plus petit multiple commun de $\text{LM}(f)$ et $\text{LM}(g)$, noté $\text{PPCM}(\text{LM}(f), \text{LM}(g)) := X^\gamma$.

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

Lemme 4.12. 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 i tel que $c_i \neq 0$.

Si $\text{LM}(G) < X^\delta$ 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 $X^{\gamma_{j,k}} = \text{PPCM}(\text{LT}(g_j), \text{LT}(g_k))$. De plus, chacun des $X^{\delta - \gamma_{j,k}}$ est strictement inférieur à X^δ .

Démonstration. A faire □

Théorème 4.13. 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 si, et seulement si, pour tout couple (i, j) , $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$

Démonstration. 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 $F \subset G$
 $G := F$

Répéter

$G' := G$

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 $\text{LT}(P) \in \langle \text{LT}(G \setminus \{P\}) \rangle$. Alors $G \setminus \{P\}$ est une base de Gröbner de I .

Démonstration. 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 . \square

Définition 5.2. Une base de Gröbner minimale G 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 5.3. Une base de Gröbner réduite G 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 5.4. 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. A faire \square

6 Théorèmes 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 pème idéal d'élimination de I l'idéal I_p de $k[X_{p+1}, \dots, X_n]$ défini par : $I_p = k[X_{p+1}, \dots, X_n] \cap I$, $0 \leq p \leq n-1$

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 $p \in \llbracket 0, n \rrbracket$, l'ensemble $G_p = G \cap k[X_{p+1}, \dots, X_n]$ est une base de Gröbner du pème idéal d'élimination I_p .

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

Montrons que G_p est une base de I_p .

Comme $G_p \subset I_p$ (car $G \subset I$) alors $\langle G_p \rangle \subset I_p$.

Soit $f \in I_p$ alors d'après le théorème de division par G , il existe $h_1, \dots, h_m \in k[X_1, \dots, X_n]$ tels que $f = \sum_{k=1}^m h_k g_k //$ car G est une base de Gröbner de I et $f \in I$.

Or pour tout $p > r$, $g_i > X^{p+1} \geq LM(f)$ et donc aucun terme de f ne peut

être divisible par un $LT(g_i)$. L'algorithme n'incrmente pas les h_p (avec $p > r$) et donc sont tous nuls.

D'où, $f = \sum_{k=1}^r h_k g_k$ et donc $f_p \in \langle G_p \rangle$, ce qui finit de montrer l'égalité $\langle G_p \rangle = I_p$.

(Le même argument permet de montrer que si $f \in I_p$, $\overline{f}^G = \overline{f}^{G_p}$).

Montrons maintenant que G est une base de Gröbner de I_p .

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

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

Comme $S(g_i, g_j)$ est de la forme $Pg_i + Qg_j$ ($P, Q \in k[X_{p+1}, \dots, X_n]$) et I_p est un idéal alors $S(g_i, g_j) \in I_p \subset I$ 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. \square

Théorème 6.3 (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 partielle $(a_2, \dots, a_n) \in Z(I_1)$. 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 6.4. Soit $I = \langle f_1, \dots, f_s \rangle$ un idéal de $\mathbb{C}[X_1, \dots, X_n]$ et supposons qu'il existe $i \in \llbracket 1, n \rrbracket$ 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 $c \in \mathbb{C} \setminus \{0\}$. 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. 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 $(a_2, \dots, a_n) \in \mathbb{C}^{n-1}$). \square

Exemple 6.5. Soit S_1 le système $\begin{cases} x^2 = y \\ x^2 = z \end{cases}$ et son ensemble de solutions

$Z(x^2 - y, x^2 - z)$. Notons $I = \langle x^2 - y, x^2 - z \rangle$ et I_1 son premier idéal d'élimination.

On peut calculer une base de Gröbner de I : $I = \langle x^2 - z, y - z \rangle$ d'où $I_1 = \langle y - z \rangle$ D'où $Z(I_1) = \{(c, c) | c \in k\}$

On peut remarquer que les termes dominants de $x^2 - y$ et $x^2 - z$ ne s'annulent pas. D'où, d'après le théorème d'extension, on peut étendre toutes les

solutions partielles dans \mathbb{C} .

Si on travaille dans \mathbb{R} , on peut étendre la solution (c, c) en une solution de S_1 si, et seulement si $c \geq 0$.

Soit S_2 le système $\begin{cases} xy = 1 \\ xz = 1 \end{cases}$ et $I = \langle xy - 1, xz - 1 \rangle$.

On peut calculer une base de Gröbner de I : $I = \langle xz - 1, y - z \rangle$ d'où $I_1 = \langle y - z \rangle$. On en déduit que $Z(I_1) = \{(c, c) | c \in \mathbb{C}\}$

On peut étendre toutes les solutions partielles sauf la solution $(0, 0)$ (car $0x = 1$ n'a pas de solutions) où les termes dominants de $xy - 1$ et $xz - 1$ en x s'annulent

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 : $Z(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in k^n | \forall i \in \llbracket 1, s \rrbracket, f_i(a_1, \dots, a_n) = 0\}$.

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. 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 $V \cup W = Z(f_i g_j | 1 \leq i \leq s, 1 \leq j \leq r)$ (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 $f_{i_0}(a) \neq 0$. Alors, comme pour tout $j \in \llbracket 1, r \rrbracket, f_{i_0}(a) g_j(a) = 0$, alors, par intégrité de k , 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. \square

Définition 7.4. 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 7.5. 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 7.6. 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 7.7. 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 7.8. 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. $0_{k[X_1, \dots, X_n]} \in I(V)$ 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 7.9. 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. 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 7.10. $\langle X^2, Y^2 \rangle \neq I(Z(X^2, Y^2))$.

$x^2 = y^2 = 0 \Rightarrow x = y = 0$.

D'où $Z(X^2, Y^2) = \{(0, 0)\}$ et donc $I(Z(X^2, Y^2)) = \langle X, Y \rangle \neq \langle X^2, Y^2 \rangle$

Propriété 7.11. 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. (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 7.12. Soit π_p la projection $\mathbb{C}^n \rightarrow \mathbb{C}^{n-p}$ définie par : $\forall (a_1, \dots, a_n) \in \mathbb{C}^n, \pi_p(a_1, \dots, a_n) = (a_{p+1}, \dots, a_n)$. (Cette application est surjective)

Lemme 7.13. Soit I_p le pème 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-p} , $\pi_p(V) \subset Z(I_p)$.

Démonstration. Pour montrer cette égalité, il faut montrer que $\forall a \in \pi_p(V), \forall f \in I_p, f(a) = 0$.

Soient $a = (a_{p+1}, \dots, a_n) \in \pi_p(V)$ et $f \in I_p$.

Comme π_p 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_{p+1}, \dots, X_n alors $f(a) = f(a') = 0$.

□

Théorème 7.14. 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. \supset : c.f. Lemme ??

\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 $a \in \langle g_1, \dots, g_s \rangle$ et donc dans $\langle f_1, \dots, f_s \rangle \cap V(I_1)$

□

Théorème 7.15 (de fermeture). Soit $V = Z(f_1, \dots, f_s) \subset \mathbb{C}^n$ et soit I_p le pème idéal d'élimination de $\langle f_1, \dots, f_s \rangle$. Alors

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

Corollaire 7.16. *Supposons qu'il existe $i \in \llbracket 1, n \rrbracket$ tel que f_i s'écrit de la forme : $f_i = cX_1^N + \text{termes de degré} < N$ en X_1 où $N > 0$ et $c \in \mathbb{C} \setminus \{0\}$ non nul. Alors $\pi(V) = Z(I_1)$*

8 Nullstellensatz

Lemme 8.1. *Soit $f \in k[X_1, \dots, X_n]$, avec k algébriquement clos.*

Alors il existe un point $(a_2, \dots, a_n) \in k^{n-1}$ tel que le polynôme $\tilde{f} = f(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1)$ est de la forme $cx_1^N + \text{termes de degré} < N$ en x_1 avec $c \neq 0$ et $N > 0$.

Démonstration. Soit $f \in k[X_1, \dots, X_n]$.

Pour montrer que \tilde{f} peut s'écrire sous la forme décrite, on va d'abord déterminer le coefficient en X_1^N , ce qui va montrer qu'il est constant puis montrer qu'il est non nul.

On peut écrire f sous la forme : $f = \sum_{l=1}^N h_l$ où h_l est l -homogène et $h_N \neq 0$. On en déduit que le coefficient en x_1^N de $f(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1)$ est celui de $h_N(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1)$.

h_N est de la forme $\sum_{|l|=N} \alpha_l X^l$.

D'où $h_N(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1) = \sum_{|(l_1, \dots, l_n)|=N} \alpha_l x_1^{l_1} \prod_{j=2}^n (x_j + a_jx_1)^{l_j}$.

On en déduit que le coefficient de $f(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1)$ en x_1^N est $\sum_{|(l_1, \dots, l_n)|=N} \alpha_l a_2^{l_2} \dots a_n^{l_n} = h_N(1, a_2, \dots, a_n)$.

Comme on a supposé $h_N \neq 0$ alors, en particulier, il existe $(a_1, \dots, a_n) \in k^n$ tel que $a_1^N h_N(1, a_2, \dots, a_n) = h_N(a_1, a_2, \dots, a_n) \neq 0$ (car k est infini), autrement dit, par intégrité de k , $h_N(1, a_2, \dots, a_n) \neq 0$.

Ce qui termine la preuve que $f(x_1, x_2 + a_2x_1, \dots, x_n + a_nx_1)$ est de la forme $cx_1^N + \text{termes de degré} < N$ en x_1 . \square

Théorème 8.2 (Nullstellensatz faible). *Soit k un corps algébriquement clos et I un idéal de $k[X_1, \dots, X_n]$ tel que $Z(I) = \emptyset$ alors $I = k[X_1, \dots, X_n]$.*

Démonstration. Par récurrence sur le nombre de variable,

Initialisation :

Soit $I \subset k[X]$ un idéal tel que $Z(I) = \emptyset$.

On peut remarquer que $I \neq \{0\}$ car $Z(\{0\}) = k[X]$.

Comme $k[X]$ est principal alors il existe $P \neq 0$ tel que $I = Pk[X]$.

D'où $Z(I) = Z(P)$ et donc $0 = \text{Card}(Z(I)) = \text{card}(Z(P))$.

Comme k est algébriquement clos alors P est constant et $I = k[X]$.

Hérédité :

Soit $n \in \mathbb{N}$ et supposons que pour tout idéal I de $k[X_2, \dots, X_n]$, $Z(I) = \emptyset \Rightarrow I = k[X_2, \dots, X_n]$.

Soit $I = \langle f_1, \dots, f_s \rangle \subset k[X_1, \dots, X_n]$ un idéal tel que $Z(I) = \emptyset$.

Quitte à changer I par \tilde{I} (cf. Lemme précédent), on peut supposer que f_1 est de la forme $cX_1^N +$ terme de degré $< N$ en X_1 avec $c \neq 0$ et $N > 0$.

On peut donc utiliser le corollaire du théorème de fermeture :

$Z(I_1) = \pi_1(Z(I)) = \pi_1(\emptyset) = \emptyset$ où $\pi_1 : k^n \rightarrow k^{n-1}$ est la projection canonique et I_1 le premier idéal d'élimination de I .

D'où, par hypothèse de récurrence, $I_1 = k[X_2, \dots, X_n]$ c'est-à-dire

$1 \in I_1 \subset I$.

D'où $I = k[X_1, \dots, X_n]$ □

Théorème 8.3 (Nullstellensatz). *Soit k un corps algébriquement clos. Si $f, f_1, \dots, f_s \in k[X_1, \dots, X_n]$ tel que $f \in I(Z(f_1, \dots, f_s))$ alors il existe un $m \geq 1$ tel que*

$$f^m \in \langle f_1, \dots, f_s \rangle$$

. (Et réciproquement)

A Graphe

A.1 Généralités

Définition A.1. Un graphe non orienté est un couple (S, A) , où S est un ensemble fini non vide (des éléments sont les sommets) et A est une partie de l'ensemble $\mathcal{P}_2(S)$ des paires d'éléments de S (les éléments de A sont les arêtes).

Définition A.2. Soit $G := (A, S)$ un graphe non orienté. Les sommets s, t sont dits adjacents si $(s, t) \in A$

Définition A.3. Soit $p \in \mathbb{N}^*$.

Notons $C_p = \{x_1, \dots, x_p\}$ un ensemble de couleurs. Un graphe $G := (A, S)$ est coloriable si on peut associer à chaque sommet de G une couleur de C_p tel que deux sommets adjacents n'aient pas la même couleur.

A.2 Equations polynomiales

Soit $G := (A, S)$ un graphe non orienté et $p \in \mathbb{N}^*$.

Soit $n := \text{Card}(A)$.

Associons à chaque sommet de G la variable x_i et à chaque couleur une racine p ème de l'unité *i.e.* $\forall i \in \llbracket 1, n \rrbracket, x_i^p = 1$.

On impose de plus, que si x_i et x_j sont adjacents alors $x_i \neq x_j$. Cela revient à dire que $\sum_{k=0}^{p-1} x_i^k x_j^{p-1-k} = 0$.

En effet, $0 = x_i^p - x_j^p = \underbrace{(x_i - x_j)}_{\neq 0} \sum_{k=0}^{p-1} x_i^k x_j^{p-1-k}$. G est coloriable avec p

couleurs si, et seulement si,

le système $\begin{cases} \forall i \in \llbracket 1, n \rrbracket, x_i^p = 1 \\ \forall i, j \in \llbracket 1, n \rrbracket, x_i \text{ et } x_j \text{ sont adjacents, } \sum_{k=0}^{p-1} x_i^k x_j^{p-1-k} = 0 \end{cases}$ a une solution

B Ordre

Soit un ensemble A et une relation d'ordre \leq sur A .

Définition B.1. On dit que \leq est un bon ordre si toute partie non vide de A admet un plus petit élément, c'est-à-dire :

$\forall C \subset A, C \neq \emptyset, \exists c \in C, \forall b \in C, c \leq b$.

Définition B.2. On dit que \leq est un ordre bien fondé si toute partie non vide de A admet un élément minimal, c'est-à-dire :

$\forall C \subset A, C \neq \emptyset, \exists c \in C, \forall b \in C, b \leq c \Rightarrow c = b$.

Propriété B.3. Soit A un ensemble et \leq une relation d'ordre sur A .

\leq est total et bien fondé ssi \leq est un bon ordre.

Démonstration. Supposons que \leq est total et bien fondé.

Soit $C \subset A$ non vide.

Alors il existe un élément minimal c de C (\leq bien fondé) tel que :

$\forall b \in C, b \leq c \Rightarrow c = b$.

D'où $\forall b \in C, b > c$ ou $c = b$ car \leq est total.

c'est-à-dire $\forall b \in C, b \geq c$.

ou encore que c est le plus petit élément de C .

\leq est donc un bon ordre.

Supposons que \leq est un bon ordre.

Soit $x, y \in A$. Alors $\{x, y\}$ admet un plus petit élément et donc $x \leq y$ ou $y \leq x$.

\leq est donc total.

Soit $C \subset A$ alors il existe $c \in C$ tel que $\forall b \in C, c \leq b$.

Alors si $b \leq c$ alors, par antisymétrie, $b = c$.

Cela permet d'en déduire que \leq est un ordre bien fondé.

□

Propriété B.4. Soit A un ensemble et \leq une relation d'ordre sur A .

\leq est bien fondé ssi il n'existe pas de suite infinie strictement décroissante.

Démonstration. Montrons cet énoncé par contraposée :

\leq n'est pas bien fondée ssi il existe une suite infinie strictement croissante c'est-à-dire il existe une partie S de A tel que pour tout $c \in S$, il existe $b \in S$ tel que $c > b$

(car $\text{non}(A \Rightarrow B) \Leftrightarrow (A \text{ et } \text{non}(B))$) et donc $(b \leq c \Rightarrow c = b) \Leftrightarrow (b \leq c \text{ et } b \neq c) \Leftrightarrow (b < c)$

Soit $\alpha_1 \in S$ alors il existe $\alpha_2 \in S$ tel que $\alpha_1 > \alpha_2$.

En itérant ce processus, on construit une suite $(\alpha_i)_{i \in \mathbb{N}}$ strictement décroissante.

Réciproquement, supposons l'existence d'une telle suite alors l'ensemble $\{\alpha_i | i \in \mathbb{N}\} \subset A$ n'admet pas d'élément minimal donc \leq n'est pas bien fondé. □

C Anneau noethérien

Définition et propriété C.1. Soit A un anneau commutatif. Alors les deux conditions suivantes sont équivalentes :

1. Toute suite croissante d'idéaux de A est stationnaire.
2. Tout idéal I de A est de type fini c'est-à-dire qu'il existe une famille finie $f_1, \dots, f_n \in I$ telle que : $I = \langle f_1, \dots, f_n \rangle$

Un tel anneau est alors dit noethérien.

Démonstration. Montrons $(1) \Rightarrow (2)$.

Supposons donc que toute suite croissante d'idéaux de A est stationnaire.

Soit \mathcal{I} un idéal de A et considérons la suite d'idéal (I_n) définie par : $I_0 = \langle 0 \rangle$ et pour tout $n \in \mathbb{N}$, $I_{n+1} = \langle I_n, a_{n+1} \rangle$ où $a_{n+1} \in \mathcal{I} \setminus I_n$ si $I_n \neq \mathcal{I}$ et $I_{n+1} = I_n$

sinon.

Alors (I_n) est croissante et plus précisément, elle est strictement croissante tant que $I_n \neq \mathcal{I}$ et constante sinon.

On en déduit que (I_n) est stationnaire (c.f. (1)) et donc qu'il existe $N \in \mathbb{N}$ tel que :

$$\forall n \geq N, \mathcal{I} = I_n = I_N = \langle a_1, \dots, a_n \rangle.$$

Montrons maintenant que $(2) \Rightarrow (1)$.

Supposons donc que tout idéal I de A est de type fini.

Soient (I_n) une suite croissante d'idéaux et $I := \bigcup_{n \in \mathbb{N}} I_n$.

Par hypothèse, il existe donc $a_1, \dots, a_p \in I$ tel que $I = \langle a_1, \dots, a_p \rangle$. De plus, comme $a_1, \dots, a_p \in \bigcup_{n \in \mathbb{N}} I_n$ alors pour tout a_i il existe n_i tel que $a_i \in I_{n_i}$ avec $1 \leq i \leq p$.

Posons maintenant $N := \max_{1 \leq i \leq p} n_i$.

Alors pour tout $n \geq N$, $a_1, \dots, a_p \in I_n$. D'où :

$$\langle a_1, \dots, a_p \rangle \subset I_N \subset I_n \subset I = \langle a_1, \dots, a_p \rangle.$$

Et donc pour tout $n \geq N$, $I = I_n = I_N$. (I_n) est donc stationnaire.

□

Exemple C.2. Tout anneau principal est noethérien car chaque idéal d'un anneau principal A est de la forme aA où $a \in A$.

En particulier, tout corps est noethérien (les idéaux d'un corps sont $\{0\}$ et lui-même).

Théorème C.3 (de la base de Hilbert). *Soit A un anneau noethérien. Alors $A[X]$ est aussi un anneau noethérien.*

Démonstration. Soient I un idéal de $A[X]$, J l'idéal engendré par les coeff et pour tout $n \in \mathbb{N}$, $J_n = \langle \{a | aX^n + \sum_{k=0}^{n-1} a_k X^k \in I\} \rangle$ des idéaux de A .

Comme A est noethérien alors il existe $x_1, \dots, x_r \in I$, tels que $J = \langle x_1, \dots, x_r \rangle$ et pour tout $n \in \mathbb{N}$, $y_{1,n}, \dots, y_{m_n,n}$ tels que $J_n = \langle y_{1,n}, \dots, y_{m_n,n} \rangle$.

Il existe donc des polynômes Q_1, \dots, Q_r de I ayant pour coefficient dominant x_i et pour tout $n \in \mathbb{N}$, des polynômes $R_{1,n}, \dots, R_{m_n,n}$ qui ont pour coefficient en X^n égale à $y_{m_n,n}$.

Montrons que $I = \langle Q_1, \dots, Q_r, R_{1,1}, \dots, R_{m_1,1}, \dots, R_{1,N}, \dots, R_{m_N,N} \rangle$ où $N := \max_i \deg(Q_i)$.

Notons I' cet idéal (inclus dans I car engendré par des éléments de I) et montrons, par récurrence sur le degré de P , que si $P := \sum a_i X^i \in I'$ alors $P \in I$.

Initialisation : Si $P = 0$ alors $P \in I$ et $P \in I'$ (car ce sont des sous-groupes additifs de $A[X]$)

Hérédité : Soit $d \in \mathbb{N}$ et supposons que pour tout polynômes de degré P de degré strictement inférieur à d que si $P \in I$ alors $P \in I'$.

Soit $P := \sum_{k=0}^d a_k X^k \in I$.

- Si $d \leq N - 1$ alors $a_d \in J_d$, il existe donc $\lambda_1, \dots, \lambda_{m_d}$ tel que $a_d = \sum_{k=1}^{m_d} \lambda_k y_{k,d}$. On en déduit que $T := P - \sum_{k=1}^{m_d} \lambda_k R_{k,d}$ est de degré inférieur à $n - 1$. Comme P et les $R_{k,d}$ sont dans I alors T aussi et par hypothèse de récurrence $T \in I$. Comme les $R_{k,d}$ sont aussi dans I' alors $P = T + \sum_{k=1}^{m_d} \lambda_k R_{k,d}$ est dans I' .
- Si $d \geq N$, alors $a_d \in J$, il existe donc $\lambda_1, \lambda_r \in A$ tel que $a = \sum_{k=1}^r \lambda_k x_k$ et donc $P - \sum_{k=1}^m \lambda_i X^{n-\deg(Q_i)} Q_i$ est de degré inférieur à $n - 1$. On en déduit comme pour le cas $d \leq N - 1$ que $P \in I'$.

Conclusion : D'après le principe de récurrence, $I \subset I'$ et donc $I = I' = A[X]$ est donc noethérien. \square

Corollaire C.4. $\mathbb{Z}[X_1, \dots, X_n], k[X_1, \dots, X_n]$ sont des anneaux noethériens.

D Algèbre

D.1 Polynômes irréductibles et factorisation

Définition D.1. Un polynôme $P \in k[X_1, \dots, X_n]$ est irréductible sur k si P est non constant et qu'il n'est pas le produit de deux polynômes non constants de $k[X_1, \dots, X_n]$

Propriété D.2. *Tout polynôme non constant de $k[X_1, \dots, X_n]$ peut s'écrire comme produit de polynômes irréductible sur k .*

Théorème D.3. *Soit $P \in k[X_1, \dots, X_n]$ irréductible sur k et supposons que P divise le produit QR , avec $Q, R \in k[X_1, \dots, X_n]$. Alors P divise Q ou R .*

Théorème D.4. *Tout polynôme non constant $f \in k[X_1, \dots, X_n]$ peut s'écrire comme un produit $f = f_1 \dots f_r$ d'irréductible sur k . De plus, $f = g_1 \dots g_s$ est une autre factorisation en irréductible sur k , alors $r = s$ et les g_i peuvent être permutés de tel sorte que pour tout i , g_i soit un multiple de f_i .*

E Résultant

Soient R un anneau commutatif intègre de corps de fractions L ainsi que :
 $A := \sum_{k=0}^p a_k X^k \in R_p[X]$ et $B := \sum_{k=0}^q b_k X^k \in R_q[X]$.

On appelle la matrice de Sylvester la matrice :

$$S_{p,q}(A, B) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b_0 & 0 & \ddots & 0 & 0 \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & b_0 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & b_1 & \ddots & 0 & 0 \\ a_{p-1} & \vdots & \ddots & a_1 & b_q & \vdots & \vdots & \ddots & b_0 & 0 \\ a_p & a_{p-1} & \ddots & \vdots & 0 & b_q & \vdots & \ddots & b_1 & b_0 \\ 0 & a_p & \ddots & \vdots & 0 & 0 & b_q & \ddots & \vdots & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_{p-1} & \vdots & \vdots & 0 & \ddots & b_q & \vdots \\ 0 & 0 & \cdots & a_p & 0 & 0 & 0 & \cdots & 0 & b_q \end{pmatrix}.$$

On notera par $\text{Res}_{p,q}(A, B)$ le déterminant de $S_{p,q}(A, B)$

Propriété E.1. $\text{Res}_{p,q}(A, B)$ est nul si, et seulement si, il existe $P \in R_{q-1}[X]$ et $Q \in R_{p-1}[X]$ non tous deux nuls tels que $AP + BQ = 0$

Propriété E.2. Il existe $P \in R_{q-1}[X]$ et $Q \in R_{p-1}[X]$ non tous deux nuls tels que $AP + BQ = \text{Res}_{p,q}(A, B)$

Définition E.3. Le résultant des polynômes $A, B \in R[X]$ de degrés respectifs $p, q \geq 0$ est l'élément $\text{Res}(A, B) = \text{Res}_{p,q}(A, B)$

Remarque E.4. Lien entre les valeurs de $\text{Res}_{p,q}(A, B)$ et de $\text{Res}(A, B)$:

- Si $p = \deg(A)$ et $q = \deg(B)$ alors, par définition, $\text{Res}(A, B) = \text{Res}_{p,q}(A, B)$
- Si $p = \deg(A)$ et $q > \deg(B)$ alors $\text{Res}_{p,q}(A, B) = ((-1)^p a_p)^{q-\deg B} \text{Res}(A, B)$
- Si $p > \deg(A)$ et $q = \deg(B)$ alors $\text{Res}_{p,q}(A, B) = b_q^{p-\deg A} \text{Res}(A, B)$
- Si $p > \deg(A)$ et $q > \deg(B)$ alors $\text{Res}_{p,q}(A, B) = 0$

Propriété E.5. Soit $A = QB + A_1$ une division euclidienne, avec $A_1 \neq 0$. Alors, avec les mêmes notations que précédemment, $\text{Res}(A, B) = b_q^{\deg(A)-\deg(A_1)} \text{Res}(A_1, B)$

Lemme E.6. Si $B = (X - \beta)C$, alors $\text{Res}(A, B) = A(\beta)\text{Res}(A, C)$

Théorème E.7. Si $A := a(X - \alpha_1) \dots (X - \alpha_p)$ et $B := b(X - \beta_1) \dots (X - \beta_q)$, alors :

$$\text{Res}(A, B) = b^p A(\beta_1) \dots A(\beta_q) = b^p a^q \prod_{i=1}^p \prod_{j=1}^q (\beta_j - \alpha_i) = (-1)^{pq} a^q B(\alpha_1) \dots B(\alpha_q)$$

Corollaire E.8. Supposons le corps L algébriquement clos. Alors $\text{Res}(A, B) = 0$ si, et seulement si, les polynômes A et B ont une racine commune.

F Implicitation

Soit S l'ensemble paramétré par le système suivant :
$$\begin{cases} x_1 = f_1(t_1, \dots, t_m) \\ \vdots \\ x_n = f_n(t_1, \dots, t_m) \end{cases} \quad (\dagger)$$

où $f_i \in k[T_1, \dots, T_m]$ et $(t_1, \dots, t_m) \in k^m$.

On peut voir S comme l'image de la fonction $F : k^m \rightarrow k^n$ définie par :

$$\forall t \in k^m, F(t) = (f_1(t), \dots, f_n(t)).$$

S n'est pas nécessairement une variété affine (cf exercices).

Le système (\dagger) définit tout de même une variété $V = Z(X_1 - f_1, \dots, X_n - f_n) \subset k^{n+m}$.

On a donc $V = \{(t_1, \dots, t_n, x_1, \dots, x_m) \in k^{n+m} \mid \forall i \in \llbracket 1, m \rrbracket, x_i - f_i(t_1, \dots, t_n) = 0\}$

D'où, $V = \{(t_1, \dots, t_n, f_1(t_1, \dots, t_n), \dots, f_m(t_1, \dots, t_n)) \in k^{n+m} \mid (t_1, \dots, t_n) \in k^m\} (*)$. Autrement dit, V est le graphe de F .

Soient $i : k^m \rightarrow k^{n+m}$
 $(t_1, \dots, t_m) \mapsto (t_1, \dots, t_n, f_1(t_1, \dots, t_n), \dots, f_m(t_1, \dots, t_n))$

et $\pi_m : k^{n+m} \rightarrow k^n$
 $(t_1, \dots, t_n, x_1, \dots, x_m) \mapsto (t_1, \dots, t_n)$ Alors, on a :

$$\begin{array}{ccc} & k^{n+m} & \\ i \nearrow & & \searrow \pi_m \\ k^m & \xrightarrow{F} & k^n \end{array}$$

i.e. $F = \pi_m \circ i$.

Avec $(*)$, on a $i(k^m) = V$ et donc $\pi_m(V) = F(k^m)$.

Autrement dit, l'image d'une paramétrisation est la projection de son graphe.

Théorème F.1. Soit $F : \mathbb{C}^m \rightarrow \mathbb{C}^n$ une fonction déterminée par la paramétrisation polynomiale (\dagger) .

Soit I l'idéal $\langle X_1 - f_1, \dots, X_n - f_n \rangle \subset \mathbb{C}[T_1, \dots, T_m, X_1, \dots, X_n]$ et I_m son

m ème idéal d'élimination. Alors $Z(I_m)$ est le plus petit idéal de \mathbb{C}^n contenant $F(\mathbb{C}^m)$

Références

- [1] Pierre Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. École Polytechnique, 2011.
- [2] Donal O'Shea David Cox, John Little. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer New York, 1992.
- [3] J.P. Ramis, X. Buff, A. Warusfel, E. Halberstadt, and F. Moulin. *Mathématiques : Tout-en-un pour la Licence niveau L2*. Dunod, 2014.