Algèbre commutative et effectivité

Alexandre Guillemot

14 novembre 2022

Table des matières

Introduction

L'objectif de ce cours est de "résoudre" des systèmes d'équations polynômiales. Formellement, si $f \in k[x_1, \cdots, x_n]$, $I = (f_1, \cdots, f_r)$, alors

$$f \in I \iff \exists g_1, \cdots, g_r \in k[x_1, \cdots, x_n] \mid f = f_1 g_1 + \cdots + f_r g_r$$

On voudrait ainsi déterminer si $f \in I$. Références : 2 livres de Cox, Little, O'Shea

Chapitre 1

Bases de Gröbner

Dans ce chapitre, tous les anneaux sont supposés commutatifs. Fixons dès à présent un $k \in \mathbf{Fld}$ (on supposera toujours qu'on dispose d'algorithmes pour les opérations du corps).

1.1 Préliminaires

Définition 1.1.1. (Anneau noéthérien) Un anneau est noéthérien si toute suite croissante d'idéaux $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ est stationnaire i.e.

$$\exists N \in \mathbb{N} \mid \forall m \geq N,\ I_m = I_N$$

Proposition 1.1.1. *Un anneau est noéthérien si et seulement si tout idéal de A est finiment engendré.*

Ex 1.1.1. Voici des exemples d'anneaux noéthériens/non noéthériens

Anneaux noéthériens	Anneaux non noéthériens
$\mathbb{Q}$	$k[\mathbb{N}]$
Plus généralement, tout corps k	
$\mathbb{R}[x]$	
Plus généralement, tout PID	
$\mathbb{Z}$	
$k[x_1, \cdots, x_n]$ (conséquence de 1.1.1)	
Anneaux finis	
Anneaux artiniens	

Théorème 1.1.1. *(Théorème de la base de Hilbert) Soit A un anneau noéthérien. Alors $A[x]$ est un anneau noéthérien.*

Corollaire 1.1.1. *Si k est un corps, alors $k[x_1, \cdots, x_n]$ est noeth pour $n \in \mathbb{N}$.*

Démonstration. On veut montrer que tout idéal $I \overset{\text{id}}{\subseteq} A[x]$ est finiment engendré. Soit $I \overset{\text{id}}{\subseteq} A[x]$, montrons qu'il est finiment engendré. Pour chaque $n \in \mathbb{N}$, soit

$$I_n := \{a_n \in A \mid \exists a_0 + a_1 x + \cdots + a_n x^n \in I\}$$

Il est facile de voir que $I_n \overset{\text{id}}{\subseteq} A$. Ensuite (I_i) est croissante, car si $a_i \in I_i$ pour un $i \in \mathbb{N}$, alors $\exists f \in I$ tq le coefficient directeur de f soit a_i. Mais alors $xf(x) \in I$ est de degré $i+1$ et son coefficient directeur est encore a_i, d'où $a_i \in I_{i+1}$. Ainsi cette suite d'idéaux est stationnaire (A noeth). Notons $N \in \mathbb{N}$ tq $m \geq N \Rightarrow I_m = I_N$. Les idéaux $I_0, \cdots, I_N$ sont finiment engendrés, notons $\{a_{i,j}\}_{1 \leq j \leq r_i}$ des familles génératrices pour I_i, pour tout $i \in [\![0, N]\!]$. Pour chaque $a_{i,j}$, $\exists f_{ij} \in I$ tq $\deg(f_{ij}) \leq i$ et le terme de degré i de $f_{i,j}$ est $a_{i,j}$ (par définition de I_i). Montrons que $I = \langle \{f_{i,j}\}_{0,1 \leq i,j \leq N, r_i} \rangle$: soit $f \in I$,

1. si $\deg(f) = 0$, alors posons $a \in A$ tq $f = ax^0$. Ainsi $a \in I_0$, ainsi $\exists b_1, \cdots, b_{r_0}$ tq $a = \sum_{i=1}^{r_0} b_i a_{0,i}$. Or $f_{0,i} = a_{0,i} x^0$, ainsi $f = \sum_{i=1}^{r_0} b_i f_{0,i}$.
2. Si $d = \deg f > 0$, notons b le coeff directeur de f. Ainsi $b \in I_d$
   Cas où $d \leq N$: On peut écrire $b = \sum_{i=1}^{r_d} \lambda_i a_{d,i}$ avec $\lambda_i \in A$. Posons $S = \sum_{i=1}^{r_d} \lambda_i f_{d,i}$, alors le coefficient directeur de S est précisément b (et $\deg S \leq d$). Ainsi $\deg(f - S) < d$, et $f - S \in I$. Par hypothèse de récurrence, $f - S \in \langle \{f_{i,j}\} \rangle$ et $S \in \langle \{f_{i,j}\} \rangle$, donc finalement $f \in \langle \{f_{i,j}\} \rangle$.
   Cas où $d > N$: Notons b le coeff directeur de f, $b \in I_d = I_N \Rightarrow b = \sum \lambda_i a_{N,i}$. Posons $T := \sum \lambda_i f_{N,i} X^{d-N}$ est de degré d et de coeff directeur b, puis on conclut comme précedemment en regardant le polynômes $f - T$.

Ainsi les idéaux de $A[x]$ sont finiment engendrés, donc $A[x]$ est noeth. □

1.2 Division multivariée

1.2.1 Ordres monomiaux

Fixons $k \in$ **Fld**. Rappelons que si $I \overset{\text{id}}{\subseteq} k[x]$ non nul, alors $\exists g \in k[x]$ t.q. $I = \langle g \rangle$ (car $k[x]$ est principal, euclidien). Soit $f \in k[x]$, alors $f \in \langle g \rangle \iff g \mid f \iff$ le reste de la division euclidienne de f par g est nul (et on dispose d'un algorithme pour réaliser la division euclidienne). Question : peut-on généraliser à $k[x_1, \cdots, x_n]$?

Rq 1.2.1. Soit $I \overset{\text{id}}{\subseteq} k[x]$, $I = \langle f_1, \cdots, f_r \rangle$. Alors $I = \langle \text{pgcd}(f_1, \cdots, f_r) \rangle$

Définition 1.2.1. (Ordre monomial) Un ordre monomial sur $k[x_1, \cdots, x_n]$ est une relation d'ordre $\leq$ sur l'ensemble des $\{x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha \in \mathbb{N}^n\}$ tq

1. $\leq$ est un ordre total (pour tout $x^\alpha, x^\beta \in k[x_1, \cdots, x_n]$, $(x^\alpha \leq x^\beta) \vee (x^\beta \leq x^\alpha)$).
2. $x^\alpha \leq x^\beta \Rightarrow \forall \gamma \in \mathbb{N}^n$, $x^{\alpha+\gamma} \leq x^{\beta+\gamma}$
3. $1 \leq x^\alpha$ pour tout $\alpha \in \mathbb{N}^n$.

Notation. On écrira $\alpha \leq \beta$ au lieu de $x^\alpha \leq x^\beta$.

Ex 1.2.1.

1. Dans $k[x]$, il est facile de vérifier qu'il n'existe qu'un seul ordre monomial $\leq$: $x^n \leq x^m \iff n \leq m$.
2. Ordre lexicographique $\leq_{lex}$: soient $\alpha, \beta \in \mathbb{N}^n$ tq $\alpha \neq \beta$,

$$\alpha <_{lex} \beta \iff \exists 1 \leq r \leq n \mid \alpha_i = \beta_i \text{ pour } i < r \text{ et } \alpha_r < \beta_r$$

   (i.e. le premier coeff non nul d $\beta - \alpha$ est positif). Par exemple, dans $k[x_1, x_2, x_3]$, $x_1^2 >_{lex} x_1x_2 >_{lex} x_2^2 >_{lex} x_3^{2097434}$
3. Ordre lexicographique gradué $\leq_{deglex}$: Pour $\alpha \in \mathbb{N}^n$, notons $|\alpha| = \sum \alpha_i$. Alors soient $\alpha \neq \beta$ dans $\mathbb{N}^n$,

$$\alpha <_{deglex} \beta \iff (|\alpha| < |\beta|) \vee (|\alpha| = |\beta| \wedge \alpha <_{lex} \beta)$$

4. Ordre lexicographique renversé gradué $<_{degrevlex}$:

$$\alpha <_{degrevlex} \beta \iff (|\alpha| < |\beta|) \vee (|\alpha| = |\beta| \wedge (\exists r \in [\![1, n]\!] \mid \forall i \in [\![r+1, n]\!], \alpha_i = \beta_i \text{ et } \alpha_r > \beta_r))$$

   (la deuxième condition reviens a vérifier que le dernier coeff non nul de $\beta - \alpha$ est négatif dans le cas où $|\alpha| = |\beta|$)

Exercice. Vérifier que ces ordres sont des ordres monomiaux.

Dans sage, on appelle "term orders" de tels ordres.

Proposition 1.2.1. *Soit $\leq$ un ordre sur $\mathbb{N}^n$ satisfaisant les propriétés 1 et 2 de la def 1.2.1. Alors tfae*

3. $0_{\mathbb{N}^n} \leq \alpha$, $\forall \alpha \in \mathbb{N}^n$
4. *$\leq$ est un bon ordre : $\forall E \subseteq \mathbb{N}^n$ non vide, E contient un élément minimal pour $<$.*

Démonstration. $4 \Rightarrow 3$: Supposons qu'il existe $\alpha \in \mathbb{N}^n$ tq $\alpha < 0$, alors $2\alpha < \alpha$, $3\alpha < 2\alpha$ et ainsi de suite, donc $\cdots < 2\alpha < \alpha < 0$, mais alors $\{m\alpha \mid m \in \mathbb{N}\}$ n'a pas d'élément minimal, donc $\leq$ n'est pas un bon ordre.

$3 \Rightarrow 4$: Supposons qu'il existe $F \subseteq \mathbb{N}^n$ non vide et sans élément minimal. Alors considérons l'idéal $I = \langle x^\alpha \mid \alpha \in F \rangle$, d'après le théorème de la base de Hilbert, il existe un sous-ensemble fini de F, noté $\{\alpha_1, \cdots, \alpha_r\}$ tel que $I = \langle x^{\alpha_1}, \cdots, x^{\alpha_r} \rangle$. Alors considérons $m = \min\{\alpha_1, \cdots, \alpha_r\}$, c'est un élément de F. Mais par hypothèse, il existe $\beta \in F$ tel que $\beta < s$. Mais comme $x^\beta \in I$, il existe $1 \leq i \leq r$ tel que $x^{\alpha_i} \mid x^\beta$, et ainsi $\beta - \alpha_i \in \mathbb{N}^n$. Mais $\beta - \alpha_i < 0$ car sinon on aurait $\beta \geq \alpha_i \geq m$. □

1.2.2 Algorithme de division multivariée

Fixons maintenant un ordre monomial $\leq$ sur $k[x_1, \cdots, x_n]$.

Définition 1.2.2. Soit $f = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha x^\alpha \in k[x_1, \cdots, x_n] \backslash \{0\}$,

1. Le multidegré de f est $\text{mdeg}(f) = \max\{\alpha \in \mathbb{N}^n \mid \lambda_\alpha \neq 0\}$
2. Le coefficient dominant de f $\text{LC}(f) = \lambda_{\text{mdeg}(f)}$
3. Le mo,ome dominant de f est $\text{LM}(f) = x^{\text{mdeg}(f)}$
4. Le terme dominant de f est $\text{LT}(f) = \lambda_{\text{mdeg}(f)} x^{\text{mdeg}(f)}$

Soit $(f_1, \cdots, f_r)$ un r-tuple de polynômes non nuls de $k[x_1, \cdots, x_n]$. Soit $f \in k[x_1, \cdots, x_n]$, on cherche $Q_1, \cdots, Q_r, R \in k[x_1, \cdots, x_n]$ tq

1. $f = Q_1 f_1 + \cdots + Q_r f_r + R$
2. $R = 0$ ou aucun des termes de R n'est divisible par $\text{LT}(f_1), \cdots, \text{LT}(f_r)$.

Algorithm 1 Réalise la division multivariée de f par $f_1, \cdots, f_r$

function DIVISION MULTIVARIÉE($f, f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$)
  $g \leftarrow f$
  $Q_1, \cdots, Q_r \leftarrow 0$
  $R \leftarrow 0$
  while $g \neq 0$ **do**
    $b \leftarrow True$
    $i \leftarrow 1$
    while b **and** $i \leq r$ **do**
      if $\mathrm{LT}(f_i) \mid \mathrm{LT}(g)$ **then**
        $g \leftarrow g - \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)} f_i$
        $Q_i \leftarrow Q_i + \frac{\mathrm{LT}(g)}{\mathrm{LT}(f_i)}$
        $b \leftarrow False$
      end if
      $i \leftarrow i + 1$
    end while
    if b **then**
      $h \leftarrow LT(g)$
      $g \leftarrow g - h$
      $R \leftarrow R + h$
    end if
  end while
  return $R, Q_1, \cdots, Q_r$
end function

Rq 1.2.2. Après chaque tour de boucle while principale, on a toujours

$$f = g + \sum Q_i f_i + R$$

au vu des calculs réalisés dans la boucle. Et comme l'algorithme se termine lorsque $g = 0$, on obtiens finalement

$$f = \sum Q_i f_i + R$$

et aucun des termes de R n'est divisible par $\mathrm{LT}(f_i)$ vu que l'on ajoute que des termes divisibles par aucun des $\mathrm{LT}(f_i)$ dans l'algorithme. Finalement, l'algorithme termine puisque à chaque étape de la boucle while principale, le multidegré de g diminue strictement au vu des calculs effectués et du fait que $\leq$ est une relation d'ordre monomiale.

Notation. Le reste obtenu s'écrira $\bar{f}^{f_1,\cdots,f_t}$. Si $F = \{f_1, \cdots, f_r\}$, on écrira $\bar{f}^F$.

Rq 1.2.3. L'algo donne l'exitence de Q_i et R tq $f = \sum Q_i f_i + R$ satisfaisant les conditions imposées précédemment. Ces Q_i et R ne sont pas uniques.

Ex 1.2.2. $k[x_1, x_2]$, $<_{lex} =: <$, $f = x_1^2 + x_1x_2 + x_2^2$, $f_1 = x_1$, $f_2 = x_1 + x_2$. Alors

$$f = (x_1 + x_2)f_1 + x_2^2$$

(Résultat obtenu en appliquant l'algorithme de division multivariée)

$$\begin{aligned} &= x_1f_2 + x_2^2 \\ &= x_1f_1 + x_2f_2 + 0 \end{aligned}$$

donc $f \in (f_1, f_2)$ mais $\bar{f}^{f_1,f_2} \neq 0$!

1.3 Bases de Gröbner

Définition 1.3.1. (Base de Gröbner, 1) Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ non nul. Une base de Gröbner de I est un ensemble fini $G \subseteq I$ tq

1. $I = \langle G \rangle$,
2. $f \in I \iff \bar{f}^G = 0$

Par convention, $\emptyset$ est une base de Gröbner de l'idéal nul.

Ex 1.3.1.
1. Si $0 \neq g \in k[x]$, alors $\{g\}$ est une bdg (base de Gröbner) de $\langle g \rangle$.
2. Si $0 \neq g \in k[x_1, \cdots, x_n]$, alors $\{g\}$ est une bdg de $\langle g \rangle$.

Comment peut-on avoir $f \in \langle f_1, \cdots, f_r \rangle$ mais $\bar{f}^{f_1,\cdots,f_r} \neq 0$? Il faut qu'à une étape de la division, $\mathrm{LT}(f)$ ne soit pas divisible par aucun des $\mathrm{LT}(f_i)$.

Définition 1.3.2. (Idéal monomial) Un idéal $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ est monomial s'il existe des monômes $m_1, \cdots, m_r$ tq $I = \langle m_1, \cdots, m_r \rangle$ (par convention $\{0\}$ est monomial).

Proposition 1.3.1. *Soient $m_1, \cdots, m_r \in k[x_1, \cdots, x_n]$ des monômes, alors*

$$m \in \langle m_1, \cdots, m_r \rangle \iff m \text{ est divisible par l'un des } m_i$$

Démonstration. Si m est divisible par l'un des m_i, il est clair que $m \in \langle m_1, \cdots, m_r \rangle$. Pour prouver l'implication réciproque, supposons que $m \in \langle m_1, \cdots, m_r \rangle$. Alors on peut écrire

$$m = \sum_{i=1}^{r} a_i m_i$$

avec $a_i \in k[x_1, \cdots, x_n]$. Maintenant écrivons chaque a_i comme

$$a_i(x) = \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha^i x^\alpha$$

Alors

$$m = \sum_{i=1}^{r} \sum_{\alpha \in \mathbb{N}^n} \lambda_\alpha^i x^\alpha m_i$$

Maintenant comme m est un monome, il va exister i, α tels que $m = \lambda x^\alpha m_i$, donc $m_i \mid m$. □

Soient $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$. $\mathrm{LT}(f)$ divisible par l'un des $\mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_r)$ si et seulement si $\mathrm{LT}(f) \in \langle \{\mathrm{LT}(f_i)\} \rangle$ d'après la proposition précédente.

Notation. Soit $E \subseteq k[x_1, \cdots, x_n]$, on note

$$\mathrm{LT}(E) := \{\mathrm{LT}(f) \mid f \in E\}$$

Définition 1.3.3. (Base de Gröbner, 2) Une base de Gröbner d'un idéal $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ est un ensemble (fini) $G \subseteq I$ tq $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle$

Théorème 1.3.1. *Les deux définitions de bases de Gröbner sont équivalentes.*

Démonstration. def 1 $\Rightarrow$ def 2 : Soit $f \in I$ si $\mathrm{LT}(f) \notin \langle \mathrm{LT}(G) \rangle$, alors $\mathrm{LT}(f)$ n'est divisible par aucun des $\mathrm{LT}(g)$, $g \in G$ donc $\bar{f}^G \neq 0$.
def 2 $\Rightarrow$ def 1 : Notons $G = \{g_1, \cdots, g_r\}$. Soit $f \in I$, on veut que $\bar{f}^G = 0$. Il suffit de montrer que le reste est nul à chaque étape de l'algo de division. Or à l'étape 0 il l'est, puis en supposant qu'il l'est à l'étape m, on a

$$f = g + \sum Q_i g_i \in I$$

et donc $g \in I$. Ainsi $LT(g) \in \langle LT(I) \rangle = \langle LT(G) \rangle$ et donc il existe un g_i tel que $LT(g_i) \mid LT(g)$ daprès 1.3.1, et ainsi le reste est inchangé à cette étape. □

Théorème 1.3.2. *Tout $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ admet une base de Gröbner.*

Démonstration. On cherche $G \overset{\text{fini}}{\subseteq} I$ tq $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. D'après 1.1.1, $\exists H \overset{\text{fini}}{\subseteq} \mathrm{LT}(I)$ tq $\langle H \rangle = \langle \mathrm{LT}(I) \rangle$. Notons $h_1, \cdots, h_r$ des polynômes de I dont les termes dominants sont les éléments de H. Alors $\{h_1, \cdots, h_r\}$ est une BDG de I. □

1.4 Algorithme de Buchberger

Définition 1.4.1. $f, g \in k[x_1, \cdots, x_n]$, alors

$$S(f,g) := \frac{\mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{ppcm}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g$$

Théorème 1.4.1. *(Critère de Buchberger) Soit $G = \{g_1, \cdots, g_r\} \subseteq k[x_1, \cdots, x_r]$. Alors G est une BDG de $I := \langle G \rangle$ si et seulement si $\forall g, h \in G$, $\overline{S(g,h)}^G = 0$*

Démonstration. $\Rightarrow$: G BDF, $f, g \in G$. Comme $S(f,g) \in I$, alors $\overline{S(f,g)}^G = 0$.
$\Leftarrow$: Supposons que pour tout $g, h \in G$, alors $\overline{S(g,h)}^G = 0$. Soit $f \in I$, on veut mq $LT(f) \in \langle LT(G) \rangle$. Or $I = \langle g_1, \cdots, g_r \rangle$. Donc il existe $q_1, \cdots, q_r \in k[x_1, \cdots, x_n]$ tq

$$f = \sum_{i=1}^{r} q_i g_i$$

Alors $LM(f) \leq \max_i \{LM(q_i g_i)\} = \mathbb{M}$.

1. Si $LM(f) = \mathbb{M}$: Alors $LM(f) = LT(q_i g_i)$ pour un certain i. Mais $LM(q_i g_i) = LM(q_i) LM(g_i)$ et donc $LM(f) \in \langle LT(G) \rangle$.

2. Si $LM(f) < \mathbb{M}$: Soit $1 \leq i_1 < i_2 < \cdots < i_s \leq r$ les indices tels que $LM(q_{i_j} g_{i_j}) = \mathbb{M}$. Alors on peut réécrire f comme

$$f = \sum_{j=1}^{s} LT(q_{i_j}) g_{i_j} + \sum_{i=1}^{r} q'_i g_i$$

(et donc $LM(q'_i g_i) < \mathbb{M}$). Considérons $\sum_j LT(q_{i_j}) g_{i_j}$, on peut l'exprimer en fonction des $S(g_{i_j}, g_{i_{j+1}})$. Pour le voir, notons $h_j = LT(q_{i_j}) g_{i_j}$, alors

$$\begin{aligned}
\sum_j h_j =& LC(h_1) \left(\frac{h_1}{LC(h_1)} - \frac{h_2}{LC(h_2)} \right) \\
&+ (LC(h_1) + LC(h_2)) \left(\frac{h_2}{LC(h_2)} - \frac{h_3}{LC(h_3)} \right) \\
&+ (LC(h_1) + LC(h_2) + LC(h_3)) \left(\frac{h_3}{LC(h_3)} - \frac{h_4}{LC(h_4)} \right) \\
&+ \cdots \\
&+ (LC(h_1) + \cdots + LC(h_{s-1})) \left(\frac{h_{s-1}}{LC(h_{s-1})} - \frac{h_s}{LC(h_s)} \right) \\
&+ (LC(h_1) + \cdots + LC(h_s)) \frac{h_s}{LC(h_s)}
\end{aligned}$$

Or $\sum_j LC(h_j) = 0$ car $LM(f) < \mathbb{M}$, donc le dernier terme s'annule et donc on a bien

$$\sum_j h_j = \sum_{j=1}^{s-1} \left(\sum_{k=1}^{j} LC(h_k) \right) S(h_j, h_{j+1})$$

Rq 1.4.1. Si f et g sont de même multidegré,

$$S(f, g) := \frac{1}{\mathrm{LC}(f)} f - \frac{1}{\mathrm{LC}(g)} g$$

Ainsi,

$$S(h_j, h_{j+1}) = \frac{1}{LC(h_j)} h_j - \frac{1}{LC(h_{j+1})} h_{j+1}$$

De plus,

$$\begin{aligned}
S(h_j, h_{j+1}) &= \frac{1}{LC(h_j)} h_j - \frac{1}{LC(h_{j+1})} h_{j+1} \\
&= \frac{LT(q_{i_j})}{LC(q_{i_j} g_{i_j})} g_{i_j} - \frac{LT(q_{i_{j+1}})}{LC(q_{i_{j+1}} g_{i_{j+1}})} g_{i_{j+1}} \\
&= \frac{LM(q_{i_j})}{LC(g_{i_j})} g_{i_j} - \frac{LM(q_{i_{j+1}})}{LC(g_{i_{j+1}})} g_{i_{j+1}} \\
&= \frac{LM(g_{i_j} q_{i_j})}{LT(g_{i_j})} g_{i_j} - \frac{LM(g_{i_{j+1}} q_{i_{j+1}})}{LT(g_{i_{j+1}})} g_{i_{j+1}} \\
&= m_j S(g_{i_j}, g_{i_{j+1}})
\end{aligned}$$

pour un certain monôme m_j. Donc

$$\begin{aligned}
f &= \sum_j LT(g_{i_j}) g_{i_j} + \sum_i q'_i g_i \\
&= \sum_j h_j + \sum_i q'_i g_i \\
&= \sum_{j=1}^{s-1} \left(\sum_{k=1}^{j} LC(h_k) \right) S(h_j, h_{j+1}) + \sum_i q'_i g_i \\
&= \sum_{j=1}^{s-1} m_j \left(\sum_{k=1}^{j} LC(h_k) \right) S(g_{i_j}, g_{i_{j+1}}) + \sum_i q'_i g_i
\end{aligned}$$

et $\max(LM(q'_i g_i)) < \mathbb{M}$. Par hypothèse, $\overline{S(g_{i_j}, g_{i_{j+1}})}^{G} = 0$. Donc l'algorithme de division multivariée donne

$$S(g_{i_j}, g_{i_{j+1}}) = \sum_{i=1}^{r} b_i^j g_i$$

Par définition de l'algorithme, chaque $b_i^j q_i$ est de multidegré au plus $mdeg(S(g_{i_j}, g_{i_{j+1}}))$. Mais alors

$$\mathrm{mdeg}(m_j S(g_{i_j}, g_{i_{j+1}})) = \mathrm{mdeg}(S(h_j, h_{j+1})) < \mathbb{M}$$

Donc

$$\begin{aligned}
f &= \sum_{j=1}^{s-1} \left(\sum_{k=1}^{j} LC(h_k) \right) m_j S(g_{i_j}, g_{i_{j+1}}) + \sum_i q'_i g_i \\
&= \sum c_i g_i
\end{aligned}$$

avec $LM(c_i g_i) < \mathbb{M}$. Par récurrence sur la différence entre $LM(f) - \mathbb{M}$, on peut conclure.

□

Corollaire 1.4.1. *(Algorithme de Buchberger) Soit* $I = \langle f_1, \cdots, f_r \rangle \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. *Posons* $G^0 = \{f_1, \cdots, f_r\}$ *et pour* $n \geq 1$, *on définit*

$$G^n = G^{n-1} \cup \left\{ \overline{S(f,g)}^{G^{n-1}} \mid f, g \in G^{n-1}, \overline{S(f,g)}^{G^{n-1}} \neq 0 \right\}$$

Alors il existe $N \in \mathbb{N}$ *tel que* $n \geq N \Rightarrow G^n = G^N$. *Dans ce cas,* G^N *est une bdg de* I.

Démonstration. Si $G^n = G^{n+1}$, alors par le critère de Buchberger G^n est une bdg. Il faut donc montrer que la suite $(G^n)_n$ est stationnaire. Supposons le contraire, alors pour tout $n \geq 0, \exists f, g \in G^n$ tq $\overline{S(f,g)}^{G^n} \neq 0$. Par définition de l'algorithme de division multivariée, aucun des termes de $\overline{S(f,g)}^{G^n}$ n'est dans $\langle LT(G^n) \rangle$. En particulier, $LT\left(\overline{S(f,g)}^{G^n}\right) \notin \langle LT(G^n) \rangle$. On a donc $\langle LT(G^n) \rangle \nsubseteq \langle LT(G^{n+1}) \rangle$ et donc on obtiens une suite d'idéaux strictement croissante dans $k[x_1, \cdots, x_n]$, contradiction. □

Rq 1.4.2. L'algorithme de Buchberger n'est pas optimal. Pour des versions optimisées, voir les algorithmes F4 et F5 (Faugère)

1.5 Bases de Gröbner réduites, unicité

Ex 1.5.1. $\langle x - y, y - z \rangle = \langle x - z, y - z \rangle \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Les deux couples de générateurs sont des bdg de l'idéal qu'ils engendrent pour l'ordre lex, on n'a donc pas toujours unicité des bases de Gröbner.

Définition 1.5.1. (bdg réduite) Soit G une bdg de $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Cette base est réduite si

1. Pour tout $g \in G$, $LC(g) = 1$
2. Pour tout $g, h \in G$ distincts, aucun monôme de g n'est divisible par $LT(h)$.

Théorème 1.5.1. *Tout idéal* $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ *admet une unique bdg réduite.*

Rq 1.5.1. La bdg réduite dépend de l'ordre monomial!

On aura besoin d'outils de réduction.

Lemme 1.5.1. *Soit $G = \{g_1, \cdots, g_r\}$ une bdg de I idéal.*

1. *Si $1 \leq i, j \leq r$ distincts sont tq $LT(g_i) \mid LT(g_j)$, alors $G \backslash \{g_j\}$ est une bdg de I*
2. *Si $h_1, \cdots, h_r \in I$ sont tq $\mathrm{mdeg}(h_i) = \mathrm{mdeg}(g_i)$, alors $H = \{h_1, \cdots, h_r\}$ est une bdg de I.*

Démonstration.
1. Comme G est une bdg, $\langle LT(G) \rangle = \langle LT(I) \rangle$. Maintenant si $LT(g_i) \mid LT(g_j)$, alors $\langle LT(G \backslash \{g_j\}) \rangle = \langle LT(G) \rangle$ et donc $G \backslash \{g_j\}$ est une bdg.
2. $\langle LT(G) \rangle = \langle LT(H) \rangle$ vu que $LM(G) = LM(H)$.

□

Démonstration. (1.5.1) Soit $G = \{g_1, \cdots, g_r\}$ une bdg de I.

1. Divisons chaque g_i par $LC(g_i)$. On peut donc supposer que $LC(g_i) = 1$.
2. Chaque fois que $LT(g_i) \mid LT(g_j)$, on peut toujours retirer g_j et toujours avoir une bdg. On peut donc supposer que $\forall i \neq j$, $LT(g_i) \nmid LT(g_j)$.
3. Enfin, pour chaque i, considérons $\bar{g}_i^{G \backslash \{g_i\}} \in I$, et par définition aucun monôme de $\bar{g}_i^{G \backslash \{g_i\}}$ n'est divisible par un des $LT(g_j)$, et $LT\left(\bar{g}_i^{G \backslash \{g_i\}}\right) = LT(g_i)$. Par le 2 du lemme, alors $\left\{\bar{g}_1^{G \backslash \{g_1\}}, \cdots, \bar{g}_r^{G \backslash \{g_r\}}\right\}$ est une bdg, qui de plus est réduite.

Ceci prouve l'existence d'une bdg réduite pour I. Reste à montrer l"unicité : soient G, G' deus bdg réduites de I. Soit $g \in G$, il existe $g' \in G'$ tel que $LT(g') \mid LT(g)$. De même, il existe $g'' \in G$ tel que $LT(g'') \mid LT(g')$, et ainsi $LT(g'') \mid LT(g)$, donc $g'' = g$, et donc $LT(g') = LT(g)$. Ainsi on a montré que $LT(G) = LT(G')$. Considérons maintenant $g - g' \in I$, en particulier $\overline{g - g'}^G = 0$. Notons que si $h \in G \backslash \{g\}$, alors aucun des termes de g n'est divisible par $LT(h)$. De même pour g', car $LT(G) = LT(G')$. De même aucun monôme de $g - g'$ n'est divisible par $LT(g)$ car $LT(g) = LT(g')$ donc $LT(g - g') < LT(g)$. D'où $\overline{g - g'}^G = g - g' = 0$ donc $g = g'$. □

Chapitre 2

Théorie de l'élimination

2.1 Théorème d'élimination

Définition 2.1.1. (Idéaux d'élimination) Soit $E \subseteq k[x_1, \cdots, x_n]$. On pose

1. $E_1 = E \cap k[x_2, \cdots, x_n]$
2. $E_2 = E \cap k[x_3, \cdots, x_n]$
3. $\cdots$
4. $E_{n-1} = E \cap k[x_n]$
5. $E_n = E \cap k$

Si $E = I$ est un idéal, les I_i sont appelés idéaux d'élimination de I.

Ex 2.1.1. $I = \langle x - y + 1, x + y \rangle$. Alors $I_1 = \langle 2y - 1 \rangle$. $I_2 = \{0\}$.

Théorème 2.1.1. *(Théorème d'élimination) Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$, soit $<$ l'ordre lex avec $x_1 > \cdots > x_n$. Soit G une bdg de I. Pour chaque $l \in [\![1, n]\!]$, une base de Gröbner de I_l est G_l.*

Démonstration. Clairement, $G_l \subseteq I_l$ donc $\langle LT(G_l) \rangle \subseteq \langle LT(I_l) \rangle$. Il faut montrer $\supseteq$. Soit $f \in I_l$. Alors $f \in I$, d'où $LT(f) \in \langle LT(G) \rangle$. On sait que $f \in k[x_{l+1}, \cdots, x_n]$. Soit $g \in G$ tq $LT(g) \mid LT(f)$, alors $LT(g) \in k[x_{l+1}, \cdots, x_n]$. Comme $<$ est l'ordre lex, on en déduit que $g \in k[x_{l+1}, \cdots, x_n]$. Donc $g \in G_l$ et $LT(f) \in \langle LT(G_l) \rangle$. □

Par conséquent, une bdg pour l'ordre lex contient des éléments qui font intervenir de moins en moins de variables.

2.2 Application 1 : Intersection d'idéaux

Problème : $I = \langle f_1, \cdots, f_r \rangle$, $J = \langle g_1, \cdots, g_s \rangle$. Calculer des générateurs de $I \cap J$. Pour cela, on ajoute une variable t.

Notation. SI $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ et $f \in k[t]$, on pose

$$fI = \langle fp \mid p \in I \rangle \overset{\text{id}}{\subseteq} k[t, x_1, \cdots, x_n]$$

Théorème 2.2.1. *Avec les notations ci-dessus,*

$$I \cap J = \langle tI + (1-t)J \rangle \cap k[x_1, \cdots, x_n]$$

Démonstration. $\subseteq$: Soit $f \in I \cap J$, alors $f = tf + (1-t)f \in \langle tI + (1-t)J \rangle$, puis $f \in k[x_1, \cdots, x_n]$.
$\supseteq$: Soit $f \in \langle tI + (1-t)J \rangle \cap k[x_1, \cdots, x_n]$. Posons

$$\begin{array}{rccc} \varepsilon_\lambda : & k[t, x_1, \cdots, x_n] & \to & k[x_1, \cdots, x_n] \\ & h & \mapsto & h(\lambda, x_1, \cdots, x_n) \end{array}$$

Remarquons alors que $\varepsilon_0(tI) = \{0\}, \varepsilon_1(tI) = I$. De même, $\varepsilon_0((1-t)J) = J, \varepsilon_1((1-t)J) = \{0\}$. Ecrivons $f = f' + f''$ avec $f' \in tI$, $f'' \in (1-t)J$. Alors $\varepsilon_0(f) = \varepsilon_0(f'') \in J$. $\varepsilon_1(f) = \varepsilon_1(f') \in I$. Et $\varepsilon_0(f) = \varepsilon_1(f) = f$ vu que $f \in k[x_1, \cdots, x_n]$. □

Corollaire 2.2.1. *Si $I = \langle f_1, \cdots, f_r \rangle$, $J = \langle g_1, \cdots, g_s \rangle$. Alors une bdg de $I \cap J$ pour l'ordre lex est obtenue en calculant une bdg de $\langle tI + (1-t)J \rangle \overset{\text{id}}{\subseteq} k[t, x_1, \cdots, x_n]$ et en éliminant t (i.e. en prenant l'intersection avec $k[x_1, \cdots, x_n]$).*

2.3 Application 2 : extension

Soit k un corps algébriquement clos. On veut montrer le théorème suivant :

Théorème 2.3.1. *(Théorème d'extension) Soit $I = (f_1, \cdots, f_r) \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Notons*

$$f_i(x_1, \cdots, x_n) = g_i(x_2, \cdots, x_n) x_1^{N_1} + h_i$$

où $\deg_{x_1} h_i < N_i$. Alors soit $(a_2, \cdots, a_n) \in V(I_1)$ tel que $(a_2, \cdots, a_n) \notin V(g_1, \cdots, g_r)$, il existe $a_1 \in k$ tel que $(a_1, \cdots, a_n) \in V(I)$.

Pour cela, nous aurons besoin des résultants.

2.3.1 Résultants

On veut une façon de déterminer si deux polynômes ont un facteur non trivial en commun. **Idée :** soient $f, g \in k[x]$ de degré $d, e > 0$ respectivement. Alors f et g ont un facteur commun non constant ssi $\exists \alpha, \beta \in k[x]$ tq

1. $\alpha, \beta \neq 0$
2. $\alpha f + \beta g = 0$
3. $\deg \alpha < e$, $\deg \beta < d$.

$f = \sum_{i=0}^{d} a_i x^i$, $g = \sum_{i=0}^{e} b_i x^i$, $\alpha = \sum_{i=0}^{e-1} \alpha_i x^i$, $\beta = \sum_{i=0}^{d-1} \beta_i x^i$. Il suffit de vérifier si

$$(\alpha_0 + \alpha_1 x + \cdots + \alpha_{e-1} x^{e-1}) f + (\beta_0 + \beta_1 x + \cdots + \beta_{d-1} x^{d-1}) g = 0$$

admet une solution non nulle en les α_i, β_i. Ce système est donné par la matrice de Sylvester

$$Syl(f,g,x) = \begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & \ddots & 0 \\ a_{d-1} & \vdots & \ddots & a_0 & b_{e-1} & \vdots & \ddots & b_0 \\ a_d & a_{d-1} & & a_1 & b_e & b_{e-1} & & b_1 \\ 0 & a_d & \ddots & \vdots & 0 & b_e & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{d-1} & \vdots & \ddots & \ddots & b_{e-1} \\ 0 & \cdots & 0 & a_d & 0 & \cdots & 0 & b_e \end{bmatrix} \in \mathrm{M}_{d+e}(k)$$

Définition 2.3.1. Le résultant de f et g est $Res(f,g,x) := \det Syl(f,g,x)$

Proposition 2.3.1. *$Res(f,g,x) = 0 \iff$ f et g ont un facteur non constant en commun.*

Proposition 2.3.2. *Fixons $d, e \geq 1$. Il existe $A, B \in \mathbb{Z}[X_0, \cdots, X_d, Y_0, \cdots, Y_e, x]$ tq pour tout $f, g \in k[x]$ avec $\deg f, \deg g = d, e$, on a*

$$Res(f,g,x) = A(a_0, \cdots, a_d, b_0, \cdots, b_e, x) f + B(a_0, \cdots, a_d, b_0, \cdots, b_e, x) g$$

Démonstration. $Syl(f,g,x)$ est la matrice de l'application linéaire

$$\begin{array}{rccc} \varphi : & k[x]_{<e} \times k[x]_{<d} & \to & k[x]_{<e+d} \\ & (\alpha, \beta) & \mapsto & \alpha f + \beta g \end{array}$$

dans les bases canoniques de $k[x]_{<e}, k[x]_{<d}$. Soit M la transposée de la comatrice de $Syl(f,g,x)$. Alors par définition,

$$Syl(f,g,x)M = Res(f,g,x)I_{d+e}$$

donc

$$Syl(f,g,x)M \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} Res(f,g,x) \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Maintenant M times vecteur est un vecteur dont les coord sont des polynômes évalués en les a_i et b_j. Ainsi

$$\varphi(P_0 + P_1X + \cdots + P_{e-1}X^{e-1}, Q_0 + Q_1X + \cdots + Q_{d-1}X^{d-1}) = Res(f,g,x)$$

où $P_i, Q_j \in \mathbb{Z}[a_i, b_j]$.

$$\Rightarrow (P_0 + P_1X + \cdots + P_{e-1}X^{e-1})f + (Q_0 + Q_1X + \cdots + Q_{d-1}X^{d-1})g = Res(f,g,x)$$

Ainsi on pose $A = P_0 + P_1X + \cdots + P_{e-1}X^{e-1}$, $B = Q_0 + Q_1X + \cdots + Q_{d-1}X^{d-1}$. □

Rq 2.3.1. La proposition et sa preuve restent vraies si on remplace k par un anneau commutatif.

2.3.2 Théorème d'extension

$f, g \in k[x_1, \cdots, x_n]$, alors $Res(f,g,x_1) \in k[x_2, \cdots, x_n]$. Notons $I = (f_1, \cdots, f_r) \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$, pour tout i

$$f_i = g_i(x_2, \cdots, x_n)x_1^{N_1} + \text{ termes de } \deg_{x_1} < N_1$$

Lemme 2.3.1. *Le théorème d'extension est vrai pour $n = 2$.*

Démonstration. Notons $\deg f_1 = d, \deg f_2 = e$. Alors il existe $A, B \in \mathbb{Z}[X_0, \cdots, X_d, Y_0, \cdots, Y_e, x_1, \cdots, x_n]$. Alors

$$\begin{aligned} Res(f_1, f_2, x_1) =& A(a_0, \cdots, a_d, b_0, \cdots, b_e, x_2, \cdots, x_n, x_1)f_1 + \\ & B(a_0, \cdots, a_d, b_0, \cdots, b_e, x_2, \cdots, x_n, x_1)f_2 \end{aligned}$$

Le membre de droite de cette égalité est dans I, et $Res(f_1, f_2, x_1) \in k[x_1, \cdots, x_n]$. Ainsi $Res(f_1, f_2, x_1) \in I \cap k[x_2, \cdots, x_n] = I_1$. Soit $(c_2, \cdots, c_b) \in V(I_1)$. En particulier, $Res(f_1, f_2, x_1)(c_2, \cdots, c_n) = 0$.

On cherche $c_1 \in k$ solution commune de $f_1(x_1, c_2, \cdots, c_n) = 0$ et $f_2(x_1, c_2, \cdots, c_n)$. Comme k est algébriquement clos, $f_1(x_1, c_2, \cdots, c_n)$ et $f_2(x_1, c_2, \cdots, c_n)$ ont un zéro commun si et seulement si leur pgcd est non trivial ssi leur résultat s'annule. Maintenant

$$Res(f_1(x_1, c_2, \cdots, c_n), f_2(x_1, c_2, \cdots, c_n), x_1) = Res(f_1(x_1, \cdots, x_n), f_1(x_1, \cdots, x_n), x_1)(c_2, \cdots, c_n)$$

En effet, on a supposé que $(c_2, \cdots, c_n) \notin V(g_1, g_2)$, et alors deux cas se présentent :

1. aucun des g_i ne s'annule en $(c_2, \cdots, c_n)$, dans ce cas

$$\deg_{x_1} f_i(x_1, c_2, \cdots, c_n) = \deg_{x_1} f(x_1, \cdots, x_n)$$

   et donc l'égalité précédente est vraie.

2. l'un des g_i s'annule en $(c_2, \cdots, c_n)$. Sans perte de généralité, supposons que g_2 s'annule (et donc g_1 ne s'annule pas) en $(c_2, \cdots, c_n)$. En remplaçant f_2 par $f_2' = f_2 + x_1^N f_1$, avec $N >> 0$ ($N \geq \deg_{x_1} f_2$), on se ramène au cas 1 en remarquant que f_1, f_2 one une solution commune en c_1 si et seulement si f_1, f_2' ont une solution commune en c_1.

d'où $f_1(x_1, c_2, \cdots, c_n)$ et $f_2(x_1, c_2, \cdots, c_n)$ ont un zéro commun c_1. □

Définition 2.3.2. Soient $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$. Considérons

$$u_2 f_2 + \cdots + u_r f_r \in k[x_1, \cdots, x_n, u_2, \cdots, u_r]$$

Alors

$$Res(f_1, u_2 f_2 + \cdots + u_r f_r, x_1) = \sum_{\alpha \in \mathbb{N}^{r-1}} h_\alpha(x_2, \cdots, x_n) u^\alpha \in k[x_2, \cdots, x_n, u_2, \cdots, u_r]$$

et les $h_\alpha \in k[x_1, \cdots, x_n]$ sont les résultants généralisés de $f_1, \cdots, f_r$ par rapport à x_1.

Démonstration. (Théorème d'extension) On cherche une racine commune aux $f_i(x_1, c_2, \cdots, c_n)$. Le cas $r = 2$ a été fait dans le lemme 2.3.1. Ainsi supposons que $r \geq 3$, et supposons sans perte de généralité que $g_1(c_2, \cdots, c_n) \neq 0$. On a

$$Res(f_1, u_2 f_2 + \cdots + u_r f_r, x_1) = \sum_{\alpha \in \mathbb{N}^{r-1}} h_\alpha(x_2, \cdots, x_n) u^\alpha$$

Montrons que $h_\alpha \in I_1$, pour tout $\alpha \in \mathbb{N}^{r-1}$. Par la proposition, il existe

$$\tilde{A}, \tilde{B} \in \mathbb{Z}[u_2, \cdots, u_r, x_1, \cdots, x_n, X_0, \cdots, X_d, Y_0, \cdots, Y_e]$$

tq

$$Af_A + B(u_2f_2 + \cdots + u_rf_r) = Res(f_1, u_2f_2 + \cdots + u_rf_r, x_1) = \sum_{\alpha \in \mathbb{N}^{r-1}} h_\alpha(x_2, \cdots, x_n)u^\alpha$$

où A, B sont des évaluations de $\tilde{A}$ et $\tilde{B}$. Ecrivons

$$A = \sum_\alpha A_\alpha u^\alpha$$
$$B = \sum_\alpha B_\alpha u^\alpha$$

Alors

$$\sum_\alpha h_\alpha u^\alpha = \sum_\alpha (\underbrace{A_\alpha f_1}_{\in I})u^\alpha + \sum_{i=2}^{r} \sum_\beta (\underbrace{B_\beta f_i}_{\in I})u^{\beta + e_i}$$

où $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ (le 1 est à la i-ème position). Par comparaison des coeffs devant chaque u^α, on obtient que $h_\alpha \in I$ pour tout $\alpha \in \mathbb{N}^{r-1}$. Par définition, $h_\alpha \in k[x_2, \cdots, x_n]$ donc $h_\alpha \in I_1$. En particulier, $h_\alpha(c_2, \cdots, c_n) = 0$ pour tout $\alpha \in \mathbb{N}^{r-1}$.

1. Supposons que $g_2(c_2, \cdots, x_n) \neq 0$ et $\deg_{x_1} f_2 > \max(\deg_{x_1}(f_i))_{3 \leq i \leq r}$. Alors

   $$\deg_{x_1}(u_2f_2 + \cdots + u_rf_r) = \deg_{x_1}((u_2f_2 + \cdots + u_rf_r)(c_2, \cdots, c_n))$$

   Alors

   $$0 = Res(f_1, u_2f_2 + \cdots + u_rf_r, x_1)(c_2, \cdots, c_n) = Res(f_1(c_2, \cdots, c_n), u_2f_2(c_2, \cdots, c_n) + \cdots + u_rf_r(c_2, \cdots, c_n), x_1)$$

   Alors $f_1(x_1, c_2, \cdots, c_n)$ et $\sum_{i=2}^r u_i f_i(x_1, c_2, \cdots, c_n)$ ont un facteur en commun non constant dans $k[u_2, \cdots, u_r][x_1]$. Comme $f_1(x_1, c_2, \cdots, c_n) \in k[x_1]$, ce facteur commun $D(x_1)$ est dans $k[x_1]$. En évaluant u_j en 1 et u_k en 0 pour $k \neq j$, on obtient que $D(x_1) \mid f_j(x_2, c_2, \cdots, c_n)$ pour chaque j. Ainsi il existe $c_1 \in k$ tq $f_i(c_1, \cdots, c_n) = 0$ pour tout i (on prend une racine de D, qui existe car $k = \bar{k}$).
2. On se ramène au cas 1 en remplaçant f_2 par $x_1^N f_1 + f_2$ avec N suffisament grand.

□

2.4 Application 3 : variétés paramétrées

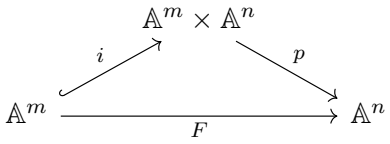
Une variété est $V(I)$, $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Paramètres ? $x = t$, $y = 2t$ est une paramtrisation d'une variété $V(y - 2x)$. Donnons un autre exemple : $x = t^2$, $y = t^3$ est la paramétrisation de $V(y^2 - x^3)$. Un dernier exemple : $x = s^2 + t^2$, $y = s^2 - t^2$, $z = st$. Il est difficile de savoir directement si c'est une variété. Formalisme : on a des équations polynomiales

$$\begin{cases} x_1 = f_1(t_1, \cdots, t_m) \\ \vdots \\ x_n = f_n(t_1, \cdots, t_m) \end{cases}$$

De façon équivalente, on a un morphisme de variétés

$$\begin{array}{rccc} F : & \mathbb{A}^m & \to & \mathbb{A}^n \\ & (t_1, \cdots, t_m) & \mapsto & (f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m)) \end{array}$$

Quetion : quelle est la plus petite variété contenant $F(\mathbb{A}^m)$? Idée : considérer le graphe de F : $\{(\underline{t}, F(\underline{t})) \in \mathbb{A}^m \times \mathbb{A}^n\}$. C'est l'ensemble $V(x_1 - f_1, \cdots, x_n - f_n) \subseteq \mathbb{A}^m \times \mathbb{A}^n$. Considérons le diagramme commutatif



où i est l'inclusion

$$\begin{array}{rccc} i : & \mathbb{A}^m & \to & \mathbb{A}^m \times \mathbb{A}^n \\ & t & \mapsto & (t, f(t)) \end{array}$$

et p la projection sur la deuxième coordonnée.

Théorème 2.4.1. *(Implicitisation) Soit k un corps infini, notons $I = (x_i - f_i \mid 1 \leq i \leq n) \overset{\text{id}}{\subseteq} k[t_1, \cdots, t_m, x_1, \cdots, x_n]$. Alors $\overline{F(\mathbb{A}^m)} = V(I_m)$ où I_m est l'idéal d'élimination $I \cap k[x_1, \cdots, x_n]$.*

On montre d'abord le cas où $k = \bar{k}$.

Théorème 2.4.2. *(Théorème de cloture) Supposons que k est algébriquement clos. Soit $I = (f_1, \cdots, f_r) \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Soit $1 \leq l \leq n$ un entier et considérons I_l. Enfin soit*

$$\begin{array}{rccc} \pi_l : & \mathbb{A}^n & \to & \mathbb{A}^{n-l} \\ & (x_1, \cdots, x_n) & \mapsto & (x_{l+1}, \cdots, x_n) \end{array} \tag{2.1}$$

Alors $\overline{\pi_l(V(I))} = V(I_l)$.

Démonstration. Découle du nullstellensatz : déja, $\pi_l(V(I)) \subseteq (I_l)$. En effet, si $(a_1, \cdots, a_n) \in V(I)$, alors $\pi_l(a_1, \cdots, a_n) = (a_{l+1}, \cdots, a_n)$. Mais si $g \in I_l$, alors $g \in I$ donc $g(a_1, \cdots, a_n) = 0$ puis g ne fait pas intervenir les l premières variables. Ainsi $(a_{l+1}, \cdots, a_n) \in V(I_l)$. Soit $f \in I(\pi_l(V(I))) \subseteq k[x_{l+1}, \cdots, x_n]$, puis considérons f comme élément de $k[x_1, \cdots, x_n]$. Alors $f \in I(V(I))$ puisque f ne fait pas intervenir les l première variables. Ainsi $\exists N > 0$ tel que $f^N \in I$. Mais f ne fait pas intervenir les l premières variables, donc $f^N \in I_l$. et ainsi $f \in \sqrt{I_l} = I(V(I_l))$. Donc $I(\pi_l(V(I))) \subseteq I(V(I_l))$. On applique V :

$$V(I_l) \supseteq V(I(\pi_l(V(I)))) \supseteq V(I(V(I_l))) \supseteq V(\sqrt{I_l}) = V(I_l)$$

donc toutes ces inclusions sont des égalités. □

Démonstration. (2.4.1)

Cas 1 : k algébriquement clos On veut montrer que $\overline{F(\mathbb{A}^n)} = V(I_m)$ où $I = (x_i - f_i)$. Le théorème de cloture appliqué à p et $V(I)$: $\overline{p(V(I))} = V(I_m)$. Mais $p(V(I)) = F(\mathbb{A}^n)$.

Cas 2 : k n'est pas algébriquement clos Soit $\bar{k}$ sa clôture algébrique. Le morphisme $F : \mathbb{A}_k^m \to \mathbb{A}_k^n$ s'étend naturellement en un morphisme $\bar{F} : \mathbb{A}_{\bar{k}}^n \to \mathbb{A}_{\bar{k}}^m$ qui envoie $\underline{t}$ sur $\underline{f}(\underline{t})$. Notons $\bar{I} = (x_i - f_i) \overset{\text{id}}{\subseteq} \bar{k}[x_1, \cdots, x_n]$. Par ce qui précède, $\overline{\bar{F}(\mathbb{A}_{\bar{k}}^n)} = V((\bar{I})_m)$. Or les générateurs de $(\bar{I})_m$ dans une BDG pour l'odre lex sont dans $k[x_1, \cdots, x_n]$, et ainsi $(\bar{I})_m = \overline{I_m}$. Finalement, on a (comme précédemment) que $F(\mathbb{A}_k^m) \subseteq V(I_m)$. Supposons que $V(J)$ est une autre variété tq $F(\mathbb{A}_k^m) \subseteq V(J) \subseteq V(I_m)$ où $J \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Prenons $g \in J$, alors $g \circ F \in k[t_1, \cdots, t_m]$. Alors $g \circ F$ s'annule sur $\mathbb{A}^m$ (car $F(\mathbb{A}_k^m) \subseteq V(J)$). Comme le corps est ifini, $g \circ F = 0$. En particulier, $g \circ F$, vu comme élément de $\bar{K}[t_1, \cdots, t_n]$ s'annule sur $\mathbb{A}_{\bar{k}}^m$ et est donc nul. Donc

$$\bar{F}(\mathbb{A}_{\bar{k}}^m) \subseteq V(\bar{J})$$

Or $\overline{\bar{F}(\mathbb{A}_{\bar{k}}^n)} = V(\bar{I}_m)$. Ainsi $V(\bar{I}_m) \subseteq V(\bar{J})$, donc $V(I_m) \subseteq V(J)$. □

Chapitre 3

Changements de bases de Grobner

3.1 Ordres matriciels

Définition 3.1.1. Soit $M \in M_{m,n}(\mathbb{R})$. On définit une relation $<_M$ sur $\mathbb{N}^n$ de la façon suivante :

$$\alpha <_M \beta \iff M\alpha <_{lex} M\beta$$

Ex 3.1.1. Sur $k[x_1, x_2, x_3]$, I_3 convient pour $<_{lex}$,

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

convient pour $<_{deglex}$,

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

convient pour $<_{degrevlex}$.

Rq 3.1.1.

$$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & 1 \end{bmatrix}$$

convient aussi pour lex.

Définition 3.1.2. (Noyau à droite) Le noyau à droite de $M \in M_{m,n}(\mathbb{R})$ est

$$\ker M := \{v \in \mathbb{R}^n \mid Mv = 0\}$$

Proposition 3.1.1. *Soit $M \in M_{m,n}(\mathbb{R})$, alors*

1. $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$,
$$\alpha <_M \beta \iff \alpha + \gamma <_M \beta + \gamma$$
2. *Si* $\ker M \cap \mathbb{Z} = \{0\}$, *alors* $\forall \alpha \neq \beta \in \mathbb{N}^n$, $(\alpha <_M \beta) \vee (\beta <_M \alpha)$.
3. *S'il existe une matrice $T \in M_{m,m}(\mathbb{R})$ triangulaire inférieure dont les coefficients diagonaux sont strictements positifs et t.q. $TM \in M_{m,n}(\mathbb{R}_{\geq 0})$, alors $\forall \alpha \in \mathbb{N}^n$, $0 \leq_M \alpha$.*

Démonstration. 1.

$$\begin{aligned} \alpha <_M \beta &\iff M\alpha <_{lex} M\beta \\ &\iff M\alpha + M\gamma <_{lex} M\beta + M\gamma \\ &\iff M(\alpha+\gamma) <_{lex} M(\beta+\gamma) \\ &\iff \alpha + \gamma <_M \beta + \gamma \end{aligned}$$

2. Soient $\alpha \neq \beta \in \mathbb{N}^n$, alors
$$\begin{aligned} \alpha <_M \beta \vee \beta <_M \alpha &\iff M\alpha <_{lex} M\beta \vee M\beta <_{lex} M\alpha \\ &\iff M\alpha \neq M\beta \iff \alpha - \beta \notin \ker M \end{aligned}$$
et comme $\ker M \cap \mathbb{Z}^n = 0$ et $\alpha \neq \beta$, alors $\alpha - \beta \notin \ker M$ est toujours vraie.
3. Notons w_i les lignes de M. TM est obtenue en effectuant les opérations suivantes :
   — Remplacer w_1 par un multiple strictement positif de w_1.
   — Remplacer w_2 par un multiple strictement positif de w_2 plus une combinaison linéaire de w_1.
   — Remplacer w_3 par un multiple strictement positif de w_3 plus une combinaison linéaire de w_1, w_2.
   — $\vdots$

   Pour comparer $\alpha, \beta \in \mathbb{N}^n$ pour $<_M$ on calcule
$$M\alpha = \begin{bmatrix} w_1 \cdot \alpha \\ \vdots \\ w_b \cdot \alpha \end{bmatrix}, M\beta = \begin{bmatrix} w_1 \cdot \beta \\ \vdots \\ w_b \cdot \beta \end{bmatrix}$$

Montrons que $<_M = <_{TM}$. Notons $T = (T_{ij})_{1 \leq i,j \leq m}$. Alors

$$TM = \begin{bmatrix} t_{11}w_1 \\ t_{21}w_1 + t_{22}w_2 \\ t_{31}w_1 + t_{32}w_2 + t_{33}w_3 \\ \vdots \end{bmatrix}$$

Maintenant

$$\alpha <_M \beta \iff \begin{cases} w_1\alpha < w_2\beta \\ \text{ou alors } w_1\alpha = w_1\beta \text{ et } w_2\alpha < w_2\beta \\ \text{ou alors } w_1\alpha = w_1\beta \text{ et } w_2\alpha = w_2\beta \text{ et } w_3\alpha < w_3\beta \\ \vdots \end{cases}$$

$$\iff \begin{cases} t_{11}w_1\alpha < t_{11}w_1\beta \\ \text{ou alors } t_{11}w_1\alpha = t_{11}w_1\beta \text{ et } t_{22}w_2\alpha + t_{21}w_1\alpha < t_{22}w_2\beta + t_{21}w_1\beta \\ \vdots \end{cases}$$

$$\iff TM\alpha <_{lex} TM\beta \iff \alpha <_{TM} \beta$$

et aini $<_M = <_{TM}$. Maintenant comme $TM \in M_{m,n}(\mathbb{R}_{\geq 0})$, pour tout $\alpha \in \mathbb{N}^n$, $TM\alpha \in \mathbb{R}^n_{\geq 0}$ et donc $0 \leq_{TM} \alpha$, d'où $0 \leq_M \alpha$.

□

Corollaire 3.1.1. *Pour tout T triangulaire inférieure avec coefficients diagonaux strictement positifs, alors $<_{TM} = <_M$.*

Corollaire 3.1.2. *Si une ligne de M est combinaison linéaire des lignes au dessus, alors la retirer ne change pas l'ordre matriciel.*

Corollaire 3.1.3. *Tout ordre matriciel est égal à un ordre matriciel $<_M$, où M a au plus n lignes.*

Ex 3.1.2. $M = \begin{bmatrix} 1 & \sqrt{2} \end{bmatrix}$ définit un ordre monomial.

Corollaire 3.1.4. *Tout ordre monomial matriciel est égal à $<_M$ où M a exactement n lignes.*

Démonstration. D'après le corolaire précédent, on peut prendre M avec moins de n lignes. Mais alors rajouter des lignes de zéros ne change pas l'ordre. □

Rq 3.1.2. Si $n \geq 2$, alors $k[x_1, \cdots, x_n]$ admet une infinité d'ordres monomiaux. Par exemple, pour $n = 2$, pour tout $a \in \mathbb{N}$, on définit

$$M_a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

Alors $y >_{M_a} x^a$ et $y <_{M_a} x^{a+1}$, donc les $<_{M_a}$ définissent une infinité d'ordre monomiaux différents.

Théorème 3.1.1. *(Robbiano, 1985) Tout ordre monomial est un ordre matriciel.*

Démonstration. Soit $<$ un ordre monomial sur $\mathbb{N}^n$.

Etape 1 : $<$ s'étend en un unique ordre total additif sur $\mathbb{Z}^n$: si $\alpha, \beta \in \mathbb{Z}^n$, alors $\exists \gamma \in \mathbb{Z}^n$ tel que $\alpha + \gamma, \beta + \gamma \in \mathbb{N}^n$. On pose ainsi

$$\alpha < \beta \iff \alpha + \gamma < \beta + \gamma$$

Clairement, cette définition ne dépend pas du choix de γ. Donc $<$ est étendu en un ordre total à $\mathbb{Z}^n$.

Etape 2 : L'ordre total additif $<$ sur $\mathbb{Z}^n$ s'étend en un unique ordre total additif sur $\mathbb{Q}^n$: si $\alpha, \beta \in \mathbb{Q}^n$, alors $\exists \lambda \in \mathbb{N}^n$ tq $\lambda\alpha, \lambda\beta \in \mathbb{Z}^n$. Ainsi on pose

$$\alpha < \beta \iff \lambda\alpha < \lambda\beta$$

Ceci ne dépend pas de λ, et on a ainsi étendu $<$ à un ordre total additif sur $\mathbb{Q}^n$.

Etape 3 : Soient

$$H_- = \{v \in \mathbb{Q}^n \mid v < 0\}$$
$$H_+ = \{v \in \mathbb{Q}^n \mid v > 0\}$$

Ainsi $\mathbb{Q}^n = H_- \sqcup \{0\} \sqcup H_+$. Alors considérons les adhérences $\bar{H}_-$, $\bar{H}_+$ dans $\mathbb{R}$, puis $I_0 = \bar{H}_- \cap \bar{H}_+$. Montrons que I_0 est un sev de $\mathbb{R}^n$ de codimension 1.

- H_+, H_- sont stables pas somme.
- H_+, H_- sont stables par produit par des éléments de $\mathbb{Q}_{>0}$.
- L'opération $\sigma : v \mapsto -v$ est une bijection de H_+ dans H_-.

Ainsi

- $\bar{H}_+, \bar{H}_-$ sont stables par somme.
- $\bar{H}_+, \bar{H}_-$ sont stables par produits par des éléments de $\mathbb{R}_{\geq 0}$.
- $\sigma : v \mapsto -v$ induit une bijection entre $\bar{H}_+$ et $\bar{H}_-$.

Par conséquent, I_0 est stable par somme et produit par un réél quelconque. Comme $I_0 \neq \emptyset$, car $0 \in I_0$, ceci donne que I_0 est un sev de $\mathbb{R}^n$. Montrons que $\dim I_0 = n-1$ en montrant que $I_0 \neq \mathbb{R}^n$, et que $\mathbb{R}^n \backslash I_0$ n'est pas connexe. Puisque $\mathbb{Q}^n_{>0} \cap H_- = \emptyset$, on obtiens que $I_0 \neq \mathbb{R}^n$. De plus, $\mathbb{R}^n \backslash I_0 = (\bar{H}_+ \backslash I_0) \sqcup (\bar{H}_- \backslash I_0)$, et ces deux composantes sont des fermés, donc $\mathbb{R}^n \backslash I_0$ n'est pas connexe.

Etape 4 : Soit w_1 un vecteur non nul, orthogonal à I_0 tel que pour tout $h \in \bar{H}_+$, alors $\langle w_1, h \rangle \geq 0$ (w_1 existe quitte à le multiplier par -1, et est unique à produit par $\mathbb{R}_{>0}$ près). Alors pour tout $v \in \mathbb{R}^n$,

— $v \in \bar{H}_+ \iff \langle w_1, v \rangle \geq 0$
— $v \in \bar{H}_- \iff \langle w_1, v \rangle \leq 0$
— $v \in I_0 \iff \langle w_1, v \rangle = 0$

Si $v, v' \in \mathbb{Q}^n$, alors $v < v' \iff v - v' < 0 \iff v - v' \in H_- \Leftarrow \langle w_1, v - v' \rangle < 0$. Le vecteur w_1 sera la première ligne d'une matrice M telle que $<_M = <$ sur $\mathbb{N}^n$.

Etape 5 : Si $\langle v - v', w_1 \rangle = 0$, alors $v - v' \in I_0$. Soit $G_1 = I_0 \cap \mathbb{Q}^n$, alors G_1 est une $\mathbb{Q}$-ev de dimension au plus $n-1$. Posons

$$H_{1,+} = \{v \in G_1 \mid v > 0\}$$
$$H_{1,-} = \{v \in G_1 \mid v < 0\}$$

$I_1 = \bar{H}_{1,+} \cap \bar{H}_{1,-}$. Comme pour I_0, on montre que I_1 est un sev de codim 1 dans $\bar{G}_1$. Soit w_2 un vecteur orthogonal à I_1 dans $\bar{G}_1$ tq $\forall h \in \bar{H}_{1,r}$, $\langle w_2, h \rangle \geq 0$. On a donc

$$\alpha <_{\begin{bmatrix} w_1 \\ w_2 \end{bmatrix}} \beta \Rightarrow \begin{cases} w_1\alpha < w_1\beta \\ \text{ou } w_1\alpha = w_1\beta \text{ et } w_2\alpha < w_2\beta \\ \text{ou } w_1\alpha = w_1\beta \text{ et } w_2\alpha = w_2\beta \end{cases}$$

Etape 6 : On pose $G_2 = \mathbb{Q}^n \cap I_1$. et ainsi de suite. On construit au plus n vecteur $w_1, \cdots, w_m$ tq

$$\alpha <_{\begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}} \beta \iff \alpha < \beta$$

□

3.2 Bases de Gröbner marquées, universelles

Notation. — $<$ ordre monomial, $E \subseteq k[x_1, \cdots, x_n]$. Alors

$$LT_<(E) := \{LT_<(f) \mid f \in E\}$$

—

$$Mon(E) = \{(LT_<(E)) \mid < \text{ ordre monomial}\}$$

Théorème 3.2.1. *Soit $I \overset{\text{id}}{\subsetneq} k[x_1, \cdots, x_n]$. Alors $Mon(I)$ est fini.*

Démonstration. Supposons le contraire, pour chaque $J \in Mon(I)$, soit $<^J$ un ordre monomial tel que $J = (LT_{<^J}(I))$. Soit

$$\Sigma = \{<^J \mid J \in Mon(I)\}$$

Par le théorème de la base de Hilbert il existe $f_1, \cdots, f_r \in I$ tq $I = (f_1, \cdots, f_r)$. Chaque f_i n'a qu'un nombre fini de termes, puisque Σ est infini, $\exists \Sigma_1 \subseteq \Sigma$ infini tel que $\forall i \in [\![1, r]\!]$, $LT_<(f_i)$ prend la même valeur pour tout $< \in \Sigma_1$. Posons

$$J := (LT_<(f_1), \cdots, LT_<(f_r))$$

pour $< \in \Sigma_1$. Montrons que $\{f_1, \cdots, f_r\}$ n'est pas une bdg de I, pour $< \in \Sigma_1$. Si c'était le cas, alors ce serait une bdg pour tout $<' \in \Sigma_1$:

$$(LT_<(I)) = (LT_<(f_i)) = (LT_{<'}(f_i)) \subseteq (LT_{<'}(I))$$

puis si un monôme m est dans $(LT_{<'}(I))$ mais pas dans $(LT_<(I))$, alors la division de m par $f_1, \cdots, f_r$ donne un reste non nul, pour $<$ comme pour $<'$. Mais si $m = LT_{<'}(f)$, $f \in I$, alors le reste de la dibision de f par $f_1, \cdots, f_r$ pour $<$ est nul. Ce reste contient pourtant le terme m, contradiction. Donc $\{f_1, \cdots, f_r\}$ est une bdg pour tout $<' \in \Sigma_1$, donc pour tout $<, <' \in \Sigma_1$,

$$(LT_<(I)) = (LT_{<'}(I))$$

mais par définition de Σ_1, si $< \neq <'$, alors $(LT_<(I)) \neq (LT_{<'}(I))$, contradiction. Ainsi $\{f_1, \cdots, f_r\}$ n'est pas une bdg pour I et pour $< \in \Sigma_I$. Il existe donc $f_{r+1} \in I$ tq $LT_<(f_{r+1}) \notin (LT_<(f_i))$. Alors $\exists \Sigma_2 \subseteq \Sigma_1$ infini tel que les valeurs de $LT_<(f_i)$, $i \in [\![1, r+1]\!]$, sont les mêmes pour tout $< \in \Sigma_2$. Comme plus haut, on mq $(f_1, \cdots, f_{r+1})$ n'est pas une bdg de I pour $< \in \Sigma_2$. Donc $\exists f_{r+2} \in I$ tel que $LT_<(f_{r+2}) \notin (LT_<(f_1), \cdots, LT_<(f_{r+1}))$ pour $< \in \Sigma_2$. Ainsi on construit par récurrence une famille d'ensembles infinis $\Sigma \supseteq \Sigma_1 \supseteq \Sigma_2 \supseteq \cdots$ et des éléments $f_1, f_2, \cdots$ pour $<_i \in \Sigma_i$ tels que

$$(LT_{<_1}(f_1), \cdots, LT_{<_1}(f_{r+1})) \nsubseteq (LT_{<_2}(f_1), \cdots, LT_{<_1}(f_{r+2})) \supseteq \cdots$$

ce qui contredit la noethérianité de $k[x_1, \cdots, x_n]$. □

Définition 3.2.1. (Base de grobner marquée) Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Une base de grobner marquée pour I est un ensemble de polynômes $\{g_1, \cdots, g_r\} \subseteq I$ et un choix de monôme m_i de g_i tel qu'il existe un ordre monomial $<$ pour lequel $\{g_1, \cdots, g_r\}$ est la base de grobner réduite et $m_i = LT_<(g_i)$.

Corollaire 3.2.1. *L'ensemble des bdg marquée de I est en bijection avec $Mon(I)$, et est donc fini.*

Démonstration. Soit $\{(g_1, m_1), \cdots, (g_r, m_r)\}$ une badg marquée de I. Supposons que $<, <'$ sont deux ordres monomiaux pour lesquels $\{(g_1, m_1), \cdots, (g_r, m_r)\}$ est la base de grobner marquée. Alors

$$(LT_<(I)) = (LT_{<'}(I))$$

En effet, $(LT_<(I)) = (LT_<(g_i)) = (m_i) = (LT_{<'}(g_i)) = (LT_{<'}(I))$. On a donc défini une application

$$\begin{array}{rccc} \phi: & \{\text{bdg marquées}\} & \to & Mon(I) \\ & \{(g_i, m_i)\} & \mapsto & (LT_<(I)) \end{array}$$

où $<$ est un ordre pour lequel $\{(g_i, m_i)\}$ est une bdg marquée. On définit une inverse ψ à ϕ : Soit $J \in Mon(I)$, puis soient $<, <'$ tq $J = (LT_<(I)) = (LT_{<'}(I))$. Alors $<$ et $<'$ définissent la même bdg marquée de I. Soit $\{(g_i, m_i)\}$ la base de groebner marquée pour $<$. Ainsi

$$\begin{aligned} (LT_<(g_i)) &= (LT_<(I)) \\ &= (LT_{<'}(I)) \supseteq (LT_{<'}(g_i)) \end{aligned}$$

Pour chaque i, $LT_{<'}(g_i)$ est divisible par l'un des $LT_<(g_j)$, mais comme (g_i) est une bdg réduite, ceci entraine que $LT_{<'}(g_i) = LT_<(g_i)$. En particulier (g_i, m_i) est une bdg, réduite et marquée pour l'ordre $<'$. On a donc défini

$$\begin{array}{rccc} \psi: & Mon(I) & \to & \{\text{bdg marquées}\} \\ & J & \mapsto & \{(g_i, m_i)\} \end{array}$$

et il est clair que ϕ et ψ sont mutuellement inverses. □

Corollaire 3.2.2. *Il existe un ensemble fini $\mathcal{U} \subseteq I$ tel que $\mathcal{U}$ est une bdg de I, quelque soit l'ordre monomial.*

Définition 3.2.2. Ce $\mathcal{U}$ est appelé base de grobner universelle.

3.3 Éventail de Gröbner

Définition 3.3.1.

1. Un cône dans $\mathbb{R}^n$ est un ensemble ayant la forme
$$C(v_1, \cdots, v_r) := \left\{ \sum_{finie} \lambda_i v_i \mid \lambda_i \geq 0 \right\}$$
De façon équivalente, un cône est une intersection de demi espaces fermés.
2. Un hyperplan de définition d'un cône C est hyperplan $H = v^\perp$ tel que $v \cdot C \geq 0$.
3. Une face d'un cône C est une intersection de $\mathcal{C}$ avec l'un de ses hyperplans de définition. Remarquons que les faces d'un cône sont des cônes.
4. La dimension d'un cône est la dimension du sous-espace de $\mathbb{R}^n$ qu'il engendre.
5. Les faces de dimension 1 de C sont les rayons de $\mathcal{C}$.
6. Les faces de codimension 1 de C sont les facettes de $\mathcal{C}$.
7. Un éventail est un ensemble $\mathcal{F}$ de cônes tels que
— $C \in \mathcal{F} \Rightarrow$ toute face de C est dans $\mathcal{F}$.
— $C, C' \in \mathcal{F} \Rightarrow C \cap C' \in \mathcal{F}$ et est une face de C et C'.

Définition 3.3.2. Soit $w \in \mathbb{R}^n_+$. Le w degré d'un monôme x^α est $\deg_w x^\alpha = w \cdot \alpha$. Un polynôme est w-homogène si tous ses termes ont le même w-degré. Si $0 \neq F \in k[X_1, \cdots, X_n]$, on pose
$$LT_w(f) = \sum \text{termes de } f \text{ de } w\text{-degré maximal}$$
Si $E \subseteq k[X_1, \cdots, X_n]$, $LT_w(E) = \{LT_w(f) \mid f \in E\}$.

Notation. Si $<_M$ est un ordre monomial, on écrira LT_M au lieu de $LT_{<M}$.

Proposition 3.3.1. *Soit $<_M$ un ordre monomial, soit $w \in \mathbb{R}^n_+$. Posons*
$$\bar{M} := \begin{bmatrix} w \\ M \end{bmatrix}$$
de sorte que $<_{\bar{M}}$ soit un ordre monomial.

1. $\forall f \in k[X_1, \cdots, X_n]$, $LT_{\bar{M}}(f) = LT_M(LT_w(f))$

2. Si $I \overset{\text{id}}{\subseteq} k[X_1, \cdots, X_n]$, alors

$$\langle LT_M \langle LT_w(I)\rangle\rangle = \langle LT_{\bar{M}}(I)\rangle$$

3. Si $\bar{G}$ est une bdg de I pour $<_{\bar{M}}$, alors $LT_w(\bar{G})$ est une bgd de $\langle LT_w(I)\rangle$ pour $<_M$.

Lemme 3.3.1. *Soit $w \in \mathbb{R}_+^n$. Tout polynôme $f \in k[X_1, \cdots, X_n]$ s'écrit de façon unique comme*

$$f = \sum_{d\in\mathbb{N}} f_{(d)}$$

où $f_{(d)}$ est homogène de w-degré d.

Démonstration. On construit une telle décomposition en réunissant les monômes de même w-degré. Pour l'unicité, il suffit de remarquer que deux monômes de w-degré différent sont forcément différents. □

Démonstration. 1. Notons $x^\alpha = LT_M(LT_w(f))$, puis considérons un autre terme x^β de f (avec $\alpha \neq \beta$). Déjà, x^α est de w-degré maximal, puisque c'est un monôme de $LT_w(f)$. Alors si $w\cdot\beta < w\cdot\alpha$, on a bien $\alpha >_{\bar{M}} \beta$. Sinon, $w\cdot\beta = w\cdot\alpha$, donc x^β est un terme de $LT_w(f)$, mais donc $\alpha >_M \beta$ par définition de α. Et alors on a encore $\alpha >_{\bar{M}} \beta$, donc finalement $x^\alpha = LT_{\bar{M}}(f)$.

2. $\supseteq$:

$$\langle LT_{\bar{M}}(I)\rangle = \langle LT_M LT_w(I)\rangle \subseteq \langle LT_M \langle LT_w(I)\rangle\rangle$$

$\subseteq$: Il suffit de montrer que $LT_M \langle LT_w(I)\rangle \subseteq \langle LT_{\bar{M}}(I)\rangle$. Soit $f \in \langle LT_w(I)\rangle$. Alors

$$f = \sum_{i=1}^{r} q_i LT_w(f_i)$$

avec $q_i \in k[X_1, \cdots, X_n]$, $f_i \in I$.

$$\begin{aligned} f &= \sum_{d\in\mathbb{N}} \sum_{i=1}^{r} (q_i LT_w(f_i))_{(d)} \\ &= \sum_{d} \sum_{i=1}^{r} (q_i)_{(d-\deg_w LT_w f_i)} LT_w(f_i) \end{aligned}$$

Si $\sum_{i=1}^{r}(q_i)_{(d-\deg_w LT_w f_i)}LT_w(f_i) \neq 0$, alors

$$\sum_{i=1}^{r}(q_i)_{(d-\deg_w LT_w f_i)}LT_w(f_i) = LT_w\left(\sum_{i=1}^{r}(q_i)_{(d-\deg_w LT_w f_i)}f_i\right) \in LT_w(I)$$

Si $\deg_w LT_M(f) = d$, alors

$$LT_M(f) = LT_M\left(\sum(q_i)_{(d-\deg_w LT_w f_i)}LT_w(f_i)\right) \in LT_M LT_w(I) = LT_{\bar{M}}(I)$$

3.

$$\begin{aligned}\langle LT_M\langle LT_w(I)\rangle\rangle &= \langle LT_{\bar{M}}(I)\rangle \\ &= \left\langle LT_{\bar{M}}(\bar{G})\right\rangle \\ &= \left\langle LT_M LT_w(\bar{G})\right\rangle\end{aligned}$$

□

Proposition 3.3.2. *Soit $<$ un ordre monomial. Soit $I \overset{\text{id}}{\subsetneq} k[X_1,\cdots,X_n]$. Soit B l'ensemble des monômes qui ne sont pas dans $\langle LT_<(I)\rangle$. Soit $\pi : k[X_1,\cdots,X_n] \twoheadrightarrow k[X_1,\cdots,X_n]$, alors $\pi(B)$ est un base du k-ev $k[X_1,\cdots,X_n]/I$.*

Démonstration. Soit G une bdg de I pour $<$. Si $0 \neq f \in k[X_1,\cdots,X_n]$, $\bar{f}^G$ est combinaison linéaire des éléments de B. Or $\pi(f) = \pi(\bar{f}^G)$, d'où $\pi(f)$ est combinaison linéaire des éléments de $\pi(B)$. De plus, $\pi(B)$ est libre car aucu,e combinaison linéaire d'éléments de B n'est dans I. □

Corollaire 3.3.1. *Si $<\neq<'$ sont deux ordres monomiaux, alors on ne peut pas avoir $\langle LT_<(I)\rangle \nsubseteq \langle LT_{<'}(I)\rangle$.*

Démonstration. Si on avait une inclusion stricte, alors on aurait que $B' \nsubseteq B$, et donc $\pi(B') \nsubseteq \pi(B)$ sont deux bases du même espace vectoriel, impossible. □

Définition 3.3.3. Soit $I \overset{\text{id}}{\subsetneq} k[X_1,\cdots,X_n]$. Soit $w \in \mathbb{R}_+^n$.

$$C[w] := \left\{w' \in \mathbb{R}_+^n \mid \langle LT_w(I)\rangle = \langle LT_{w'}(I)\rangle\right\} \tag{3.1}$$

Proposition 3.3.3. *Soit $<_M$ un ordre monomial, et*

$$\bar{M} = \begin{bmatrix} w \\ M \end{bmatrix}$$

Soit $\bar{G}$ la bdg réduite de I pour $w_{\bar{M}}$. Alors

$$C[w] = \{w' \in \mathbb{R}^n_+ \mid \forall g \in \bar{G},\, LT_w(g) = LT_{w'}(g)\}$$

Démonstration.

$\subset$: Soit $w' \in C[w]$. Alors $\langle LT_w(I)\rangle = \langle LT_{w'}(I)\rangle$. Par la prop précédente, $LT_w(\bar{G})$ est ma bdg réduite de $\langle LT_w(I)\rangle$ pour $<_M$. Soit $g \in \bar{G}$,

$$\overline{LT'_w(g)}^{LT_w(\bar{G})} = 0$$

Alors $LT_M LT_{w'}(g) \in \left\langle LT_M LT_w(\bar{G})\right\rangle = \left\langle LT_{\bar{M}}(\bar{G})\right\rangle$. Comme $\bar{G}$ est réduite, le seul terme de g qui soit dans $\left\langle LT_{\bar{M}}(\bar{G})\right\rangle$ est $LT_{\bar{M}}(g)$. Donc

$$LT_M LT_{w'}(g) = LT_{\bar{M}}(g) = LT_M LT_w(g)$$

$LT_w(g) = LT_M LT_w(g) = h$, $LT_{w'}(g) = LT_M LT_{w'}(g) + h' = LT_M LT_w(g) + h'$. Donc $LT_w(g) - LT_{w'}(g) = h - h'$. Or $LT_w(g) - LT_{w'}(g) \in \langle LT_w(I)\rangle$. Donc $\overline{h - h'}^{LT_w(\bar{G})} = 0$. Or aucun des termes de h ou h' n'est divisible par un élément de $LT_M LT_w(\bar{G}) = LT_{\bar{M}}(\bar{G})$. D'où $h - h' = 0$, et $h = h'$. Donc $LT_w(g) = LT_{w'}(g)$. Ceci montre $\subseteq$.

$\supseteq$: Soit $w' \in \mathbb{R}^n_+$ tq $\forall g \in \bar{G}$, $LT_w(g) = LT_{w'}(g)$. Alors

$$\langle LT_w(I)\rangle = \left\langle LT_w(\bar{G})\right\rangle = \left\langle LT_{w'}(\bar{G})\right\rangle \subseteq \langle LT_{w'}(I)\rangle$$

Si l'inclusion était stricte, alors on aurait $\langle LT_M \langle LT_w(I)\rangle\rangle \nsubseteq \langle LT_M \langle LT_{w'}(I)\rangle\rangle$ (en effet, si $J \subseteq J'$ et $\langle LT_M(J)\rangle = \langle LT_M(J')\rangle$, alors une bdg de J pour $<_M$ est forcément une bdg de J' pour J', et donc $J = J'$). Maintenant

$$\langle LT_{\bar{M}}(I)\rangle = \langle LT_M \langle LT_w(I)\rangle\rangle \nsubseteq \langle LT_M \langle LT_{w'}(I)\rangle\rangle = \left\langle LT_{\begin{bmatrix} w \\ M \end{bmatrix}}(I)\right\rangle$$

contradiction avec le corollaire précédent. Donc $\langle LT_w(I)\rangle = \langle LT_{w'}(I)\rangle$, d'où $w' \in C[w]$. □

Corollaire 3.3.2. *$C[w]$ est un cône relativement ouvert, i.e. une intersection de demi-espaces ouverts et d'hyperplans.*

Démonstration. Soient $<_M$ un ordre monomial, $\bar{M} = \begin{bmatrix} w \\ M \end{bmatrix}$, $\bar{G}$ une bdg réduite de I pour $<_{\bar{M}}$. Alors

$$C[w] = \{w' \in \mathbb{R}^n_+ \mid \forall g \in \bar{G},\, LT_w(g) = LT_{w'}(g)\}$$

Donc

$$\begin{aligned} w' \in C[w] &\iff \forall g \in \bar{G},\, LT_w(g) = LT_{w'}(g) \\ &\iff \forall g \in \bar{G}, \begin{cases} \text{Si } x^\alpha \text{ et } x^\beta \text{ sont deux monômes de } LT_w(g), \text{ alors } w' \cdot \alpha = w' \cdot \beta \\ \text{Si } x^\alpha \text{ est monôme de } LT_w(g) \text{ et } x^\beta \text{ est un monôme de } g \text{ mais pas} \\ \text{de } LT_w(g), \text{ alors } w' \cdot \alpha > w' \cdot \beta \end{cases} \\ &\iff \begin{cases} w' \in (\alpha - \beta)^\perp \\ w' \cdot (\alpha - \beta) > 0 \end{cases} \end{aligned}$$

□

Ex 3.3.1. $I = \langle y^3 - xy, x^2 - y \rangle$. $y^3 - xy, x^2 - y$ bdg réduite pour degrevlex (matrice associée

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \\ -1 & 0 \end{bmatrix}$$

) $w = (1,1)$. $v = (v_1, v_2) \in C[w]$, on a

$$\begin{cases} v \cdot (0,3) > v \cdot (1,1) \\ v \cdot (2,0) > v \cdot (0,1) \end{cases} \iff \begin{cases} -v_1 + 2v_2 > 0 \\ 2v_1 - v_2 > 0 \end{cases}$$

Corollaire 3.3.3. *$\overline{C[w]}$ est un cone.*

Démonstration. $\overline{C[w]}$ est défini en remplaçant les inégalités strictes du dernier corollaire par des $\leq$. □

Définition 3.3.4. On définit l'éventail de groebner $GF(I)$ comme l'ensemble des $\overline{C[w]}$.

Théorème 3.3.1. *$GF(I)$ est un éventail fini.*

Démonstration. Il faut montrer que

1. Toute face de $\overline{C[w]}$ a la forme $\overline{C[w']}$

2. $\overline{C[w]} \cap \overline{C[w]}$ est une face de $\overline{C[w]}$ et $\overline{C[w']}$.
3. $GF(I)$ est fini (On le montrera plus tard).

Prouvons les deux premiers points :

1. Soit F une face de $\overline{C[w]}$. F est défini en remplaçant certaines des inégalités "> 0" dans la définition de $C[w]$ par "$= 0$". Soit $w' \in F$, pour tout $g \in \bar{G}$, les termes de $LT_w(g)$ sont tous des termes de $LT_{w'}(g)$. Posons

$$\overline{\overline{M}} = \begin{bmatrix} w' \\ w \\ M \end{bmatrix}$$

Alors

$$\begin{aligned} \left\langle LT_{\overline{\overline{M}}}(I) \right\rangle &= \langle LT_{w'} \langle LT_{\bar{M}}(I) \rangle \rangle && (3.2) \\ &= \left\langle LT_{w'} \left\langle LT_{\bar{M}}(\bar{G}) \right\rangle \right\rangle && (3.3) \\ &= \left\langle LT_{\bar{M}}(\bar{G}) \right\rangle && (3.4) \\ &= \langle LT_{\bar{M}}(I) \rangle && (3.5) \end{aligned}$$

(3.3) = (3.4) : $f \in \left\langle LT_{\bar{M}}(\bar{G}) \right\rangle$, alors

$$\begin{aligned} \sum_{i=1}^{r} g_i LT_{\bar{M}}(g_i) &= \sum_{d \geq 0} \sum_{i} (g_i)_{d - \deg_{w'} LT_{\bar{M}}(g_i)} LT_{\bar{M}}(g_i) \\ \Rightarrow LT_{w'}(f) &= \sum_{i} (g_i)_{d - \deg_{w'} LT_{\bar{M}}(g_i)} LT_{\bar{M}}(g_i) \in \left\langle LT_{\bar{M}}(\bar{G}) \right\rangle \end{aligned}$$

En particulier, $\bar{G}$ est une bdg pour $w_{\overline{\overline{M}}}$. Donc

$$C[w'] = \{w'' \in \mathbb{R}^n_+ \mid \forall g \in \bar{G},\ LT_{w'}(g) = LT_{w''}(g)\}$$

Si w' est "génériqueé (i.e. que toute inégalité définissant F est stricte pour w'). Alors $\overline{C[w']} = F$ car $w'' \in \overline{C[w']}$ ssi w'' satisfaisant aux mêmes (in)égalités que w'.

2. Soient $w, w' \in \mathbb{R}^n_+$. Condiréons $\overline{C[w]} \cap \overline{C[w']}$. Si $w'' \in \overline{C[w]} \cap \overline{C[w']}$, alors $\overline{C[w'']}$ est une face de $\overline{C[w]}$ et de $\overline{C[w']}$, par ce qui précède. Prenons w'' dans l'intérieur relatif, on obtiens que $\overline{C[w'']} = \overline{C[w]} \cap \overline{C[w']}$.

□

Rq 3.3.1. En sage, on dispose de la procédure `groebner_fan()`

3.4 Le cône maximal d'une bdg marquée

Soit $G = \{(g_i, x^{\alpha_i})\}_{1 \leq i \leq r}$ une bdgm. Écrivons

$$g_i = x^{\alpha_i} + \sum_{\beta \neq \alpha_i} c_{i,\beta} x^{\beta}$$

Fixons $<_M$ ordre monomial pour lequel g est la bdgm. Notons w la première ligne de M. Alors $\forall i \in [\![1, r]\!]$, $\forall \beta$ tq $c_{i,\beta} \neq 0$,

$$w \cdot \alpha_i \geq w \cdot w \cdot \beta \iff w \cdot (\alpha_i - \beta) \geq 0$$

Lemme 3.4.1. *Il existe $w' \in \mathbb{R}^n_+$ tel que $\forall i \in [\![1, r]\!]$, $\forall \beta \neq \alpha_i$ t.q. $c_{i,\beta} \neq 0$,*

$$w' \cdot \alpha_i > w' \cdot \beta$$

Alors G est une bdgm pour $<_{\begin{bmatrix} w' \\ M \end{bmatrix}}$

Démonstration. On peut modifier w ainsi : S'il existe i, β tq $c_{i,\beta} \neq 0$ mais $w \cdot \alpha_i = w \cdot \beta$. Alors $w \in (\alpha_i - \beta)^{\perp}$. Soit $v \in \mathbb{R}^n$ t.q. $v \cdot (\alpha_i - \beta) > 0$. Alors $(w + \varepsilon v) \cdot (\alpha_i - \beta) > 0$ pour tout $\varepsilon > 0$. Pour que les autres inégalités soient respectées, il sufit de prendre $0 < \varepsilon$ petit. On montre que si $w \cdot (\alpha_j - \beta') = 0$, on peut choisir v non-nul dans $(\alpha_j - \beta')^{\perp}$. □

Définition 3.4.1. Avec les notations précédentes, le cône de G est $C_G := C[w']$.

Rq 3.4.1. C_G est de dimension n, car c'est l'intersection d'un nombre fini de demi-espaces ouverts. En particulier, $\bar{C}_G$ est un cône maximal de l'éventail de Groebner. De plus, tout cône maximal de $GF(I)$ a cette forme. Tout cône a la forme $\overline{C[w]}$. Par ce qui précède, on peut trouver $w'' \in \mathbb{R}^n_+$ tel que $\bar{G}$ est la bdg pour $\begin{bmatrix} w'' \\ M \end{bmatrix}$ et $LT_{w''}(g)$ sont dest monômes. Donc $\overline{C[w]} \subseteq \overline{C[w'']}$. Comme $\overline{C[w'']}$ est de dimension n, tous les cônes maximaux de $GF(I)$ sont de dimension n et ont la forme $\overline{C[w'']}$.

Corollaire 3.4.1. *$GF(I)$ est fini.*

Ex 3.4.1. $k[x, y]$, $I = \langle x^2 - y, xy - y^3, y^5 - y^2 \rangle$. Calculons $GF(I)$: ses cônes maximaux ont la forme $\bar{C}_G$.

3.5 Changement de base de Groebner

Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$

- Soit G_0 une bdg marquée de I pour $<_{M_0}$, on note w_0 la première ligne de M_0, et on calcule C_{G_0}.
- On cherche G_1 une bdg marquée de I pour $<_{M_1}$, on note w_1 la première ligne de M_1.
- On trace dans $GF(I)$ un segment de droite de w_0 à w_1. Soit w_{der} de dernier point du segment $[w_0, w_1]$ qui soit toujours dans $\overline{C_{G_0}}$ (il existe et est unique par convexité de $\overline{C_{G_0}}$).
- Posons

$$M_0' = \begin{bmatrix} w_0 \\ M_1 \end{bmatrix}, \; M_{der} = \begin{bmatrix} w_{der} \\ M_1 \end{bmatrix}$$

et G_0' et G_{der} les base de Groebner associées.

Comment passer de G_0 à G_0' ?

3.5.1 De G_0 à G_0'

On sait que

- $LT_{w_0}(G_0)$ est une bdg réduite de $\langle LT_{w_0}(I)\rangle$ pour M_0.
- $LT_{w_0}(G_0')$ est une bdg réduite de $\langle LT_{w_0}(I)\rangle$ pour M_1.

Soit $H = \{h_1, \cdots, h_s\}$ la bdg réduite de $\langle LT_{w_0}(I)\rangle$ pour M_1.

Rq 3.5.1. La base de Groebner de $\langle LT_{w_0}(I)\rangle = \langle LT_{w_0}(G_0)\rangle$ est facile à calculer car les $LT_{w_0}(G_0)$ sont "presque des monômes".

Ecrivons

$$h_j = \sum_{g \in G_0} P_{j,g} LT_{w_0}(g)$$

comme résultat de la division multivariée par $LT_{w_0}(G_0)$ pour M_0. Posons

$$\overline{h_j} = \sum_{g \in G_0} P_{j,g} g \in I$$

Alors $\overline{H} = \{\overline{h_1}, \cdots, \overline{h_s}\}$ est une bdg de I pour M_0'. En effet,

$$\begin{aligned} \left\langle LT_{M_0'}(I) \right\rangle &= \langle LT_{M_1} \langle LT_{w_0}(I)\rangle\rangle \\ &= \langle LT_{M_1}(H)\rangle \\ &= \left\langle LT_{M_0'}(\overline{H}) \right\rangle \end{aligned}$$

Prenons G_0' la bdg réduite qui est la réduction de $\overline{H}$.

3.5.2 De G'_0 à G_{der}

— $LT_{w_0}(G'_0)$ est une bdg réduite de $\langle LT_{w_0}(I)\rangle$ pour M_1.
— $LT_{w_{der}}(G'_0)$ est une bdg réduite de $\langle LT_{w_{der}}(I)\rangle$ pour M'_0.

car G'_0 est une bdg de I pour $\begin{bmatrix} w_{der} \\ M'_0 \end{bmatrix}$. En effet, si $f \in I$, alors réalisons l'algorithme de division multivariée :

$$f = \sum_{g \in G'_0} q_g g \tag{3.6}$$

Alors $LT_{M'_0}(f) = \max_{g\in G'_0}(LT_{M'_0} q_g g)$. Donc $LT_{w_{der}}(f)$ contiens $LT_{M'_0}(f)$ comme terme, car $w_{der} \in \overline{C_{G'_0}}$. On en déduit que

$$LT_{\begin{bmatrix} w_{der} \\ M'_0 \end{bmatrix}}(f) = LT_{M'_0}(f)$$

et ainsi

$$\left\langle LT_{M'_0}(I)\right\rangle = \left\langle LT_{\begin{bmatrix} w_{der} \\ M'_0 \end{bmatrix}}(I)\right\rangle$$

Finalement

$$\begin{aligned}\left\langle LT_{\begin{bmatrix} w_{der} \\ M'_0 \end{bmatrix}}(I)\right\rangle &= \left\langle LT_{M'_0}(I)\right\rangle \\ &= \left\langle LT_{M'_0}(G'_0)\right\rangle \\ &= \left\langle LT_{M'_0} LT_{w_{der}} G'_0\right\rangle \\ &= \left\langle LT_{\begin{bmatrix} w_{der} \\ M'_0 \end{bmatrix}}(G'_0)\right\rangle\end{aligned}$$

Soit $H = \{h_1, \cdots, h_s\}$ une bdg de $\langle LT_{w_{der}}(I)\rangle$ pour M_{der}.

Rq 3.5.2. Le calcul de H est peu couteux, car les éléments de $LT_{w_{der}}(G'_0)$ sont presque tous des monômes. Posons

$$h_j = \sum_{g \in G'_0} P_{j,g} LT_{w_{der}}(g)$$

(division multivariée), et

$$\overline{h_j} = \sum_{g \in G'_0} P_{j,g} g \in I$$

Alors $\overline{H} = \{\overline{h_1}, \cdots, \overline{h_s}\}$ est une bdg de I pour $M_{der} = \begin{bmatrix} w_{der} \\ M_1 \end{bmatrix}$:

$$\begin{aligned} \langle LT_{M_{der}}(I) \rangle &= \langle LT_{M_{der}} \langle LT_{w_{der}}(I) \rangle \rangle \\ &= \langle LT_{M_{der}}(H) \rangle \\ &= \left\langle LT_{M_{der}}(\overline{H}) \right\rangle \end{aligned}$$

Finalement, posons G_{der} la réduction de $\overline{H}$.

3.5.3 $\overline{C_{G_{der}}}$ est plus proche de w_1 que $C_{G'_0}$

Il suffit de voir que si on avance un peu sur le segment qui relie w_{der} à w_1, on reste dans $\overline{C_{G_{der}}}$. Si $g \in G_{der}$, alors $LT_{M_{der}}(g)$ est un terme de $LG_{w_{der}}(g)$. Si on remplace w_{der} par $w_{der} + \varepsilon(w_1 - w_{der})$, $0 < \varepsilon$ petit. Alors dans ce cas $LT_{M_{der}}(g)$ ne change pas. Ainsi on peut répéter les étapes précédentes jusqu'à obtenir w_1.

Chapitre 4

Sous-anneaux, polynômes symétriques, théorie des invariants

4.1 Sans nom pour le moment

Soient $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$. On s'est intéressés à la question d'appartenance $f \in \langle f_1, \cdots, f_r \rangle$. On veut maintenant savoir si $f \in k[f_1, \cdots, f_r]$, où $k[f_1, \cdots, f_r]$ désigne l'image du morphisme

$$\begin{array}{rccc} \phi : & k[y_1, \cdots, y_r] & \to & k[x_1, \cdots, x_n] \\ & y_i & \mapsto & f_i \end{array}$$

Ex 4.1.1. Dans $k[x]$ $\langle x^2 \rangle$ est très différent de $k[x^2]$.

Rq 4.1.1. Un sous-anneau d'un anneau de polynômes n'est pas nécessairement finiment engendré. Par exemple, $k[x, xy, xy^2, \cdots] \subset k[x, y]$ n'est pas finiment engendré.

Proposition 4.1.1. *Soient* $f_1, \cdots, f_r \in k[x_1, \cdots, x_n]$,

$$\phi : k[y_1, \cdots, y_r] \to k[x_1, \cdots, x_n]$$

,$<$ un ordre monomial sur $k[x_1, \cdots, x_n ny1, \cdots, y_r]$ tel que tout monôme faisant intervenir un x_i est plus grand que tout monôme en les y_j (par exemple $<_{lex}$), $J = \langle f_1 - y_1, \cdots, f_r - y_r \rangle$, et $G = \{g_1, \cdots, g_s\}$ une bdg de J pour $<$. Alors $f \in k[f_1, \cdots, f_r] \iff \overline{f}^G \in k[y_1, \cdots, y_r]$. Dans ce cas,

$$f = \phi(\overline{f}^G)$$

Démonstration.

$\Leftarrow$: Supposons que $\overline{f}^G \in k[y_1, \cdots, y_r]$, et soit

$$f = \sum_{i=1}^{s} q_i g_i + \overline{f}^G$$

le résultat de la division de f par G. Alors on a

$$f = \phi(f) = \sum_{i=1}^{s} \phi(q_i)\phi(g_i) + \phi(\overline{f}^G)$$

et $\phi(g_i) = 0$ car $g_i \in \langle f_i - g_i \mid 1 \leq i \leq s \rangle$, et ainsi $f = \phi(\overline{f}^G) \in k[f_1, \cdots, f_r]$.

$\Rightarrow$: Supposons que $f \in k[f_1, \cdots, f_r]$. Supposons que $g_{u+1}, \cdots, g_s$ sont les éléments de G tels que $LT(g_{u+1}), \cdots, LT(g_s) \in k[y_1, \cdots y_r]$. D'après l'hypothèse sur $<$, $g_{u+1}, \cdots, g_s \in k[y_1, \cdots, y_r]$. Soit $p \in k[y_1, \cdots, y_r]$ tel que $\phi(p) = f$. Montrons que $p = \overline{f}^G$. On dispose aussi d'un morphisme

$$\begin{array}{rccc} \Phi : & k[x_1, \cdots, x_n, y_1, \cdots, y_r] & \to & k[x_1, \cdots, x_n] \\ & x_i & \mapsto & x_i \\ & y_i & \mapsto & f_i \end{array}$$

On a que $\ker \Phi = J$. On a aussi que $\Phi(p) = f$. Aussi, on peut écrire

$$f = \sum_{i=1}^{s} q_i g_i + \overline{f}^G$$

d'où $f = \Phi(f) = \Phi(\overline{f}^G)$, et ainsi $p - \overline{f}^G \in \ker \Phi = J$. Donc $\overline{p - \overline{f}^G}^G = 0$ et ainsi $\overline{p}^G = \overline{\overline{f}^G}^G = \overline{f}^G$. Comme $p \in k[y_1, \cdots, y_r]$, $LT(p) \in k[y_1, \cdots, y_r] \in k[y1, \cdots, y_r]$ ne peut être divisible par $L(g_1), \cdots, LT(g_u)$ qui font intervenir les x_i. Comme les $g_{u+1}, \cdots, g_s \in k[y_1, \cdots, y_s]$, on a bien que $\overline{p}^G \in k[y_1, \cdots, y_r]$ ce qui conclut la preuve. □

Notation.

$$\begin{array}{rccc} \phi : & k[y_1, \ldots, y_r] & \to & k[x_1, \cdots, x_n] \\ & y_i & \mapsto & f_i \end{array}$$

$F = (f_1, \cdots, f_r)$. Alors on note $\ker \phi =: I_F$, $\ker \Phi = J_f$.

Proposition 4.1.2.

$$I_F = J_F \cap k[y_1, \cdots, y_r]$$

Démonstration. Clairement, $\ker \phi = \ker \Phi \cap k[y_1, \cdots y_r]$. □

Rq 4.1.2. 1. $k[f_1, \cdots, f_r] \simeq k[y_1, \cdots, y_r]/I_F$.

2. D'après le théorème d'implicitisation, $V(I_F)$ est la variété paramétrée par les f_i.

4.2 Polynômes symétriques

L'action du groupe symétrique $\mathfrak{S}_n$ sur $\{1, \cdots, n\}$ induit une action sur $k[x_1, \cdots, x_n]$ donnée par $\sigma \in \mathfrak{S}_n$, $f \in k[x_1, \cdots, x_n]$, alors

$$(f \cdot \sigma)(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$$

Définition 4.2.1. Un poynôme symétrique est un polynôme f tel que $f \cdot \sigma = f$. L'ensemble des polynômes symétriques est $k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$.

Ex 4.2.1. Si $n = 3$, alors $x_1 + x_2 + x_3$, $x_1x_2 + x_1x_3 + x_2x_3$, $x_1x_2x_3$ sont des polynômes symétriques.

Proposition 4.2.1. *$k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ est un sous-anneau de $k[x_1, \cdots, x_n]$.*

Définition 4.2.2. Pour $i \in \{1, \cdots, n\}$, le $i$ème polynôme symétrique élémentaire est

$$\sigma_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq n} x_{j_1} x_{j_2} \cdots x_{j_i}$$

Ex 4.2.2. Si $n = 3$, $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.

Théorème 4.2.1. *(Théorème de structure des polynômes symétriques) L'anneau $k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ est $k[\sigma_1, \cdots, \sigma_n]$. De plus, le morphisme*

$$\begin{array}{rccc} \phi : & k[y_1, \cdots, y_n] & \to & k[x_1, \cdots, x_n] \\ & y_i & \mapsto & \sigma_i \end{array}$$

est injectif d'image $k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$.

Démonstration. L'inclusion $k[\sigma_1, \cdots, \sigma_n] \subseteq k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ est évidente car les σ_i sont symétriques. Montrons $\supseteq$: Soit $f \in k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ non nul. Soit $<=<_{lex}$ avec $x_1 > x_1 > \cdots > x_n$. Posons $LT(f) = \lambda x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. Puisque f est symétrique, tout monôme $x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n}$ ($\sigma \in \mathfrak{S}^n$) apparaît dans f. Donc $a_1 \geq a_2 \geq \cdots \geq a_n$. Considérons

$$h = \lambda \sigma_1^{a_1 - a_2} \sigma_2^{a_2 - a_3} \cdots \sigma_{n-1}^{a_{n-1} - a_n} \sigma_n^{a_n}$$

Alors $LT(h) = LT(f)$, donc $f = h + (f - h)$ et $f - h$ est symétrique de terme dominant $< LT(f)$ et $h \in k[\sigma_1, \cdots, \sigma_n]$. Par récurrence, $f \in k[\sigma_1, \cdots, \sigma_n]$. Il reste à montrer que ϕ est

injectif : soit $g \in \ker \phi$, si $y_1^{b_1} \cdots y_n^{b_n}$ est un monôme de g, alors $\phi(y_1^{b_1}, \cdots, y_n^{b_n}) = \sigma_1^{b_1} \cdots \sigma_n^{b_n}$ apparaît dans $\phi(g)$. Son terme dominant est $x_1^{b_1+\cdots+b_n} x_2^{b_2+\cdots+b_n} \cdots x_n^{b_n}$. Mais la fonction

$$\begin{array}{ccc} \mathbb{N}^n & \to & \mathbb{N}^n \\ (b_1, \cdots, b_n) & \mapsto & (b_1 + \cdots + b_n, b_2 + \cdots + b_n, \cdots, b_n) \end{array}$$

est injective, donc tous les termes de g sont envoyés par ϕ sur des polynômes de termes dominants différents, leur somme ne peut donc s'annuler que si elle est vide, i.e. $g = 0$. □

Corollaire 4.2.1. *L'écriture de $f \in k[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ comme polynôme en les σ_i est unique.*

Ex 4.2.3. Soit $n \geq 2$, et considérons

$$f = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

C'est un polynômes en n variables, qui est symétrique. Il existe donc $\Delta \in \mathbb{Z}[y_1, \cdots, y_n]$ tel que $f = \Delta(\sigma_1, \cdots, \sigma_n)$. On définit Δ comme le discriminant d'ordre n. Par exemple, dans $\mathbb{Z}[x_1, \cdots, x_n][T]$ considérons $P = \prod_{i=1}^n (T - X_i)$. Alors le dixcriminant de P est Δ.

Définition 4.2.3. Pour tout $l \geq 1$, on pose

$$p_l = \sum_{i=1}^{l} x_i^l$$

Rq 4.2.1. p_l est symétrique.

Théorème 4.2.2. *Supposons que k est ce caractéristique 0. Alors*

$$k[X_1, \cdots, X_n]^{\mathfrak{S}_n} = k[p_1, \cdots, p_n]$$

Démonstration. On sait que $k[x_1, \cdots, x_n]^{\mathfrak{S}_n} = k[\sigma_1, \cdots, \sigma_n]$. Il suffit donc de montrer que $\sigma_k \in k[p_1, \cdots, p_n]$, $\forall k \in [\![1, n]\!]$. Montrons le par récurrence sur k. Si $k = 1$, $\sigma_1 = p_1$ ok. Si $k > 1$, on utilise l'identité de Newton :

$$p_k - \sigma_1 p_{k-1} + \sigma_2 p_{k-2} - \cdots + k(-1)^k \sigma_k = 0 \tag{4.1}$$

Si cette identité est vraie, alors par récurrence $\sigma_k \in k[p_1, \cdots, p_n]$. Il faut montrer l'identité :

$$\begin{aligned} P_n(T) &= \prod_{i=1}^{n} (T - X_i) \\ &= T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n \end{aligned}$$

Alors

$$0 = \sum_{i=1}^{n} P_i(X_i) = p_n - \sigma_1 p_{n-1} + \cdots + n(-1)^n \sigma_n \tag{4.2}$$

donc la formule est vraie pour $k = n$. Montrons finalement la formule pour $k < n$: pour tout $(n-k)$-uplt de variables parmi $X_1, \cdots, X_n$, envoyer ces variables vers 0, l'identité 4.1 tiens toujours. On se retrouve alors dans la situation 4.2 qui vaut 0. Donc les coefficients devant les monômes ne faisant pas intervenir les $(n-k)$ variables sont tous nuls. Faisons varier le $(n-k)$-uplet, on obtient le résultat. □

4.3 Théorie des invariants

Supposons que k est un corps algébriquement clos, de caractéristique nulle. On note $GL_n(k)$ le groupe des matrices $n \times n$ inversibles. Soit L le sev de $k[x_1, \cdots, x_n]$ des polynômes homogènes de degré 1. C'est un k ev de dimension n ayant pour base $(x_1, \cdots, x_n)$. Dans cette base, tout élément de L s'écrit comme $\sum \lambda_i x_i$, et alors $GL_n(k)$ agit donc sur L par multiplication à gauche sur $(\lambda_1, \cdots, \lambda_n)$. Ceci induit une action de $GL_n(k)$ sur tout $k[x_1, \cdots, x_n]$.

Notation. $(f.A)(x_1, \cdots, x_n) = f(A \cdot (x_1, \cdots, x_n))$

Remarquons que si G est un sous-groupe fini de $GL_n(k)$, alors G agit de la même manière sur $k[x_1, \cdots, x_n]$. Ainsi soit G un tel sous-groupe, est-ce-que $k[X_1, \cdots, X_n]^G$ est-il finiment engendré.

Ex 4.3.1. $n = 3$, prenons

$$G = \left\langle \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \right\rangle \simeq \mathbb{Z}/3\mathbb{Z}$$

agit par permutation cyclique de x_1, x_2, x_3. Par exemple, $f = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ est un polynômes G invariant.

Ex 4.3.2. Soit

$$G = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{bmatrix} \right\rangle$$

avec ζ une racine cubique primitive de l'unité. Par exemple x_1, x_2^2, x_3^3 sont G invariants. $x_1 x_2 x_3$ est G invariant. $(x_1^3 - 1)(x_2^3 - 1)(x_3^3 - 1)$ est G-invariant.

Définition 4.3.1. L'opérateur de Reynolds de G est

$$\begin{array}{rccc} R_G: & k[x_1,\cdots,x_n] & \to & k[x_1,\cdots,x_n]^G \\ & f & \mapsto & \frac{1}{|G|}\sum_{A\in G} f\cdot A \end{array}$$

Proposition 4.3.1. ??

1. *$R_G(f)$ est G-invariant, pour tout $f \in k[x_1,\cdots,x_n]$.*
2. *R_G est k-linéaire (mais n'est pas un morphisme d'anneaux).*
3. *Si $f \in k[x_1,\cdots,x_n]^G$, alors $R_G(f) = f$.*

Démonstration. Ok □

Ex 4.3.3. Prenons $G = \mathfrak{S}_n$ agissant par permutation. Alors

$$R_G(x_1) = \frac{1}{n}((n-1)!x_1 + (n-1)!x_2 + \cdots + (n-1)!x_n) = \frac{1}{n}\sigma_1$$

De même, $R_G(x_2) = \frac{1}{n}\sigma_1$.

Théorème 4.3.1 (Emmy Noether)**.** *Supposons que $k = \bar{k}$, $car(k) = 0$, G est un sous-groupe fini de $GL_n(k)$. Alors $k[x_1,\cdots,x_n]^G$ est engendré par les $R_G(x^\beta)$ avec $\deg x^\beta \leq |G|$ est finiment engendré.*

Démonstration.

L'inclusion $k[R_G(x^\beta) \mid |\beta| \leq |G|] \subseteq k[x_1,\cdots,x_n]^G$ est clair d'après le point 1 de la proposition .

Soit $f \in k[x_1,\cdots,x_n]^G$, notons le $f = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha x^\alpha$. Alors $f = R_G(f) = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha R_G(x^\alpha)$. Ceci montre que $k[x_1,\cdots,x_n]^G = k[R_G(x^\alpha) \mid \alpha \in \mathbb{N}^n]$. Il suffit donc de montrer que pour tout $\alpha \in \mathbb{N}^n$, alors $R_G(x^\alpha) \in k[R_G(x^\beta) \mid |\beta| \leq |G|]$.

Notation. Soit $A \in G \overset{\text{sgfini}}{\subseteq} GL_n(k)$, notons

$$A = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix}$$

Alors on définit

$$(A.x)^\alpha = (A_1x)^{\alpha_1}(A_2x)^{\alpha_2}\cdots(A_nx)^{\alpha_n}$$

Ainsi $x^\alpha = (Ax)^\alpha$.

On a donc

$$R_G(x^\alpha) = \frac{1}{|G|}\sum_{A\in G}(Ax)^\alpha$$

Soient $u_1, \cdots, u_n$ est variables. Pour $A \in G$, soit

$$z_A = (u_1A_1x + \cdots + u_nA_nx) \in k[x_1, \cdots, x_n, u_1, \cdots, u_n]$$

Pour tout $k > 0$, écrivons

$$\begin{aligned} z_1^k &= (u_1A_1x + \cdots + u_nA_nx)^k \\ &= \sum_{|\alpha|\leq k} a_\alpha (Ax)^\alpha u^\alpha \end{aligned}$$

où $a_\alpha \in k$ ne dépend pas de A. Soit

$$\begin{aligned} S_k &= \sum_{A\in G} z_A^k \\ &= \sum_{A\in G}\sum_{|\alpha|\leq k} a_\alpha (Ax)^\alpha u^\alpha \\ &= \sum_{|\alpha|\leq k} a_\alpha \left(\sum_{A\in G}(Ax)^\alpha\right) u^\alpha \\ &= \sum_{|\alpha|\leq k} a_\alpha |G| R_G(x^\alpha) u^\alpha \end{aligned}$$

Or S_k est un polynôme symétrique en les z_A. Par le théorème précédent, tout polynôme symétrique en les z_A est un polynôme en les $p_1 = S_1, \cdots, p_{|G|} = S_{|G|}$. En particulier, S_k est un polynôme en les $S_1, \cdots, S_{|G|}$, disons $S_k = F(S_1, \cdots, S_{|G|})$. Donc

$$\sum_{|\alpha|\leq k} a_\alpha |G| R_G(x^\alpha) u^\alpha = S_k = F(S_1, \cdots, S_{|G|})$$

$$= F\left(\sum_{|\beta|\leq 1} a_\beta^1 |G| R_G(X)^\beta u^\beta, \cdots, \sum_{|\beta|\leq |G|} a_\beta^{|G|} |G| R_G(X)^\beta u^\beta\right) \in k[u_1, \cdots, u_n, R_G(x^\beta) \mid |\beta| \leq |G|]$$

En comparant les coeffs devant u^α, on obtient que $R_G(x^\alpha) \in k[R_G(x^\beta) \mid |\beta| \leq |G|]$. □

4.3.1 Interprétation géométrique

On suppose toujours que $k = \bar{k}$, $car k = 0$. G agit sur $k[X_1, \cdots, X_n]$, et G agit sur $\mathbb{A}^n$. Insérer le diagramme commutatif ! Ainsi

$$k[y_1, \cdots, y_r]/I_F \simeq k[X_1, \cdots, X_n]^G \hookrightarrow k[X_1, \cdots, X_n]$$

On applique les foncteur variété à ce diagramme, on obtient un morphisme $\pi : \mathbb{A}^n_x \to V(I_F) \subseteq \mathbb{A}^r_y$.

Théorème 4.3.2. *1. π est surjective,*

2. Si $p, q \in \mathbb{A}^n$, alors $\pi(p) = \pi(q) \iff Gp = Gq$ (Gp, Gq sont les G-orbites de p et q)

Rq 4.3.1. $V(I_F)$ est en bijection est en bijections avec $\mathbb{A}^n/G$, et $k[V(I_F)] \simeq k[X_1, \cdots, X_n]^G$.

Démonstration. 1. On voit le morphisme de $\mathbb{A}^n_x$ dans $\mathbb{A}^r_y$ comme définissant une variété paramétrée. Par le théorème d'implicitisation, $V(I_F) = \overline{\pi(\mathbb{A}^n)}$. On veut montrer que $V(I_F) \subseteq \pi(\mathbb{A}^n)$. Soit $b = (b_1, \cdots, b_r) \in V(I_F)$. On pose

$$J = \langle y_1 - f_1, \cdots, y_r - f_r \rangle \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n, y_1, \cdots, y_r]$$

$$\begin{array}{ccc} k[x_1, \cdots, x_n, y_1, \cdots, y_n] & & \\ & \searrow^{\Phi} & \\ k[y_1, \cdots, y_r] & \longrightarrow & k[x_1, \cdots, x_n] \end{array}$$

$J = \ker \Phi$. On cherche $(a_1, \cdots, a_n) \in \mathbb{A}^n_x$ tel que $\pi(a) = b$. De façon équivalente, $(a_1, \cdots, a_n, b_1, \cdots, b_r) \in V(J)$. On applique le théorème d'extension : rappelons que si $(a_{i+1}, \cdots, a_n, b_1, \cdots, b_r)$ est une solution partielle de $J \cap k[x_{i+1}, \cdots, x_n, y_1, \cdots, y_r]$ et s'il existe $h_i \in J \cap k[x_i, \cdots, x_n, y_1, \cdots, y_r]$ avec

$$h_i = g_i(x_{i+1}, \ldots, x_n, y) x_i^{N_i} + \text{ termes en } \deg_{X_i} < N_i$$

et $g_i(a_{i+1}, \cdots, a_n, b) \neq 0$ alors la solution s'étend en une solution $(a_i, a_{i+1}, \cdots, a_n, b)$. Trouvons un tel h_i pour chaque i : pour chaque $h \in k[x_1, \cdots, x_n]$, considérons

$$\prod_{A \in G} (u - hA) = \sum_{j=0}^{|G|} g_j(x) u^j \in k[u, x]$$

Comme ce polynôme est G invariant, on a que $g_j(x) \in k[x]^G$, $\forall j$. On sait que l'on peut écrire $k[x]^G = k[f_1, \cdots, f_r]$. Ainsi $\exists p_0, \cdots, p_{|G|-1} \in k[y_1, \cdots, y_r]$ tels que

$g_j(x) = p_j(f_1, \cdots, f_r)$ (remarquons que l'on traite pas le cas $|G|$ puisque $g_{|G|} = 1$). En évaluant u en h, on trouve 0 :

$$\begin{aligned} 0 &= \sum_{j=0}^{|G|} p_j(f_1, \cdots, f_r) h^j \\ &= \sum_{j=0}^{|G|-1} p_j(f_1, \cdots, f_r) h^j + h^{|G|} \end{aligned}$$

On applique à $h = x_i$:

$$h_i := \sum_{j=0}^{|G|-1} p_j(y_1, \cdots, y_r) x_i^j + x_i^{|G|} \in J$$

puisque $h_i(f_1, \cdots, f_r) = 0$ d'après l'équation précédente. Avec ce choix de h_i pour tout i, on peut appliquer le théorème d'extension récursivement. On a ainsi montré que π est surjective.

2. $\pi : \mathbb{A}^n \to V(I_F)$, puisque les f_i sont G invariants,

$$\pi(Ax) = (f_1(Ax), \cdots, f_r(Ax)) = (f_1(x), \cdots, f_r(x)) = \pi(x)$$

Il reste à montrer que si $Ga \neq Gb$, alors $\pi(a) \neq \pi(b)$. Il suffit de trouver $g \in k[x_1, \cdots, x_n]^G$ tel que $g(a) \neq g(b)$. Posons $E = (Gb \cup Ga) \backslash \{a\}$. C'est un ensemble fini, donc c'est une variété algébrique (au sens d'ensemble algébrique dans l'autre cours). Soit $L \overset{\text{id}}{\subseteq} k[X]$ tel que $E = V(L)$, comme $a \notin E$, il existe $f \in L$ tel que $f(a) \neq 0$. Prenons maintenant $g = R_G(f) \in k[x_1, \cdots, x_n]^G$. Alors $g(b) = 0$, et $g(a) =\neq 0$.

□

Rq 4.3.2. $\pi : \mathbb{A}^n \to V(I_f)$ n'est plus forcément surjective si $k \neq \bar{k}$. Par exemple prenons $\mathbb{R}[x_1, x_2]^{\mathfrak{S}_2} = \mathbb{R}[\sigma_1, \sigma_2]$. Alors $I_F = \ker(y_i \in k[y_1, y_2] \mapsto \sigma_k k[x_1, x_2]) = 0$. Donc $V(I_F) = \mathbb{A}^2_y$ mais

$$\begin{array}{rccc} \pi : & \mathbb{A}^2 & \to & \mathbb{A}^2_y \\ & (x_1, x_2) & \mapsto & (x_1 + x_2, x_1 x_2) \end{array}$$

n'est pas surjective sur $\mathbb{R}$: en effet, si $(y_1, y_2) = \pi(x_1, x_2) = (x_1 + x_2, x_1 x_2)$ et ainsi $(X - x_1)(X - x_2) = X^2 - \sigma_1 X + \sigma_2 = X^2 - y_1 X + y_2$ donc $X^2 - y_1 X + y2$ a des racines réelles, i.e. $y_1^2 - 4y_2 \geq 0$.