Algèbre commutative et effectivité

Alexandre Guillemot

26 septembre 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

Préliminaires sur les anneaux de polynômes, idéaux, noethérianité

Dans ce chapitre, tous les anneaux seront 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 Anneaux noéthériens

1.1.1 Définition

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	

1.1.2 Théorème de la base de hilbert

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 $I = (\{f_{i,j}\}_{0,1 \leq i,j \leq N, r_i})$: 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, $f - S \in (\{f_{i,j}\})$ et $S \in (\{f_{i,j}\})$, donc finalement $f \in (\{f_{i,j}\})$.
   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. $\square$

1.2 Division multivariée

1.2.1 Ordres monomiaux

Fixons $k \in \mathbf{Fld}$. Rappelons que si $I \overset{\text{id}}{\subseteq} k[x]$ non nul, alors $\exists g \in k[x]$ t.q. $I = (g)$ (car $k[x]$ est principal, euclidien). Soit $f \in k[x]$, alors $f \in (g) \iff g \mid f \iff$ 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 $I \overset{\text{id}}{\subseteq} k[x]$, $I = (f_1, \cdots, f_r)$. Alors $I = (\text{pgcd}(f_1, \cdots, f_r))$

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 $k[x_1, x_2, x_3]$, $x_1^2 >_{lex} x_1 x_2 >_{lex} x_2^2 >_{lex} x_3^{2097434}$
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. Posons

$$m_1 = \min\{\alpha_1 \mid \alpha \in F\}$$

et notons $\alpha^{(1)} \in F$ tq $\alpha_1^{(1)} = m_1$. Posons de plus

$$F_1 = \{\beta \in F \mid \beta \leq \alpha^{(1)}\}$$

Remarquons alors que F_1 est non vide (il contient $\alpha^{(1)}$). Construisons maintenant m_i, $\alpha^{(i)}$ et F_i par récurrence : supposons que l'on a construit F_{i-1} non vide, alors on constuit m_i comme

$$m_i := \min\{\alpha_i \mid \alpha \in F_{i-1}\}$$

Il existe alors $\alpha^{(i)} \in F_{i-1}$ tq $\alpha_i^{(i)} = m_i$, puis finalement on construit F_i comme

$$F_i := \{\beta \in F_{i-1} \mid \beta \leq \alpha^{(i)}\}$$

Remarquons finalement que F_i est encore non vide, puisqu'il contiens $\alpha^{(i)}$. Maintenant F_n n'admet pas d'élément minimal, car sinon en notant β un tel élément, et prenons $\gamma \in F$. Alors $\gamma \leq \beta$ implique que γ est dans F_n, puisque $\gamma \leq \beta \leq \alpha^{(n)}$, et ainsi $\gamma = \beta$ par minimalité de β dans F_n. Ainsi β serait un élément minimal de F, qui n'en admet pas. Ainsi il existe $\beta \in F_n$ tel que $\beta < \alpha^{(n)}$. Maintenant comme $\alpha^{(n)} \leq \alpha^{(n-1)} \leq \cdots \leq \alpha^{(1)}$, on a $F_n \subseteq F_{n-1} \subseteq \cdots \subseteq F_0 := F$, et donc pour tout $i \in [\![1, n]\!]$, $\beta \in F_{i-1}$.

Posons maintenant $m_2 = \min\{\alpha_2 \mid \alpha \in F_1\}$, et prenons $\alpha^{(2)} \in F_1$ tq $\alpha_2^{(2)} = m_2$, $\alpha_1^{(2)} = m_1$. On construit alors $F_2 := \{\beta \in F_1 \mid \beta < \alpha^{(2)}$, puis de manière récursive m_i et F_i pour $i \in [\![1, n]\!]$. F_n est infini, et $F_n \subseteq F_{n-1} \subseteq \cdots \subseteq F_1 \subseteq F$. Soit $\beta \in F_n$ tq $\beta < \alpha^{(n)}$, alors $\beta_i \geq \alpha_i^{(n)}$ par construction de $\alpha^{(n)}$. Ainsi $\beta - \alpha^{(n)} \in \mathbb{Z}^n_{\geq 0}$ Alors $\beta - \alpha^n < 0$, car sinon on aurait $\beta \geq \alpha^{(n)}$. □

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 $\mathrm{mdeg}(f) = \max\{\alpha \in \mathbb{N}^n \mid \lambda_\alpha \neq 0\}$
2. Le coefficient dominant de f $\mathrm{LC}(f) = \lambda_{\mathrm{mdeg}(f)}$

3. Le mo,ome dominant de f est $\mathrm{LM}(f) = x^{\mathrm{mdeg}(f)}$
4. Le terme dominant de f est $\mathrm{LT}(f) = \lambda_{\mathrm{mdeg}(f)} x^{\mathrm{mdeg}(f)}$

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 $\mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_r)$.

Algorithm 1 Réalise la division euclidienne 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**
  - $b = True$
  - $i \leftarrow 1$
  - **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**
    - $h = LT(g)$
    - $g \leftarrow g - h$
    - $R \leftarrow R + h$
  - **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)

$$\begin{aligned} &= x_1 f_2 + x_2^2 \\ &= x_1 f_1 + x_2 f_2 + 0 \end{aligned}$$

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

1.3 Bases de Gröbner

1.3.1 Définition

> **Définition 1.3.1.** (Base de Gröbner, 1) Soit $I \overset{\mathrm{id}}{\subseteq} k[x_1, \cdots, x_n]$ non nul. Une base de Gröbner de I est un ensemble fini $G \subseteq I$ tq
> 1. $I = (G)$,
> 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 (g).
2. Si $0 \neq g \in k[x_1, \cdots, x_n]$, alors $\{g\}$ est une BDG de (g).

Comment peut-on avoir $f \in (f_1, \cdots, f_r)$ 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 $\mathrm{LT}(f_i)$.

1.3.2 Idéaux monomiaux

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 $I = (m_1, \cdots, m_r)$ (par convention $\{0\}$ est monomial).

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

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

Démonstration. Si m est divisible par l'un des m_i, il est clair que $m \in (m_1, \cdots, m_r)$. Pour prouver l'implication réciproque, supposons que $m \in (m_1, \cdots, m_r)$. 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 $\mathrm{LT}(f) \in (\{\mathrm{LT}(f_i)\})$ 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 $(\mathrm{LT}(I)) = (\mathrm{LT}(G))$

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

Démonstration. def 1 $\Rightarrow$ def 2 : Soit $f \in I$ si $\mathrm{LT}(f) \notin (\mathrm{LT}(G))$, 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 $LT(g) \in (LT(I)) = (LT(G))$ 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 $(\mathrm{LT}(G)) = (\mathrm{LT}(I))$. D'après 1.1.1, $\exists H \overset{\text{fini}}{\subseteq} \mathrm{LT}(I)$ tq $(H) = (\mathrm{LT}(I))$. 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

1.4.1 Critère 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 $G = \{g_1, \cdot, g_r\} \subseteq k[x_1, \cdots, x_r]$. Alors G est une BDG de (G) 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 $LT(f) \in (LT(G))$. Or $I = (g_1, \cdots, g_r)$. Donc il existe $q_1, \cdots, q_r \in k[x_1, \cdots, x_n]$ tq

$$f = \sum q_i g_i$$

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 $LM(f) \in (LT(G))$.

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
$$f = \sum_j LT(q_{i_j}) g_{i_j} + \sum_i q'_i g_i$$
(et donc $LM(q'_i g_i) \leq \mathbb{M}$). 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 $\sum_j LC(h_j) = 0$, 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.
$$S(h_j, h_{j+1}) = \frac{1}{LC(h_j)} h_j - \frac{1}{LC(h_{j+1})} h_{j+1}$$

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, cjaque $b_i^j q_i$ est de mdeg au plus mdeg$S(g_{i_j}, g_{i_{j+1}})$. Mais alors

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

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.

$\square$

Corollaire 1.4.1. *(Algorithme de Buchberger) Soit* $I = (f_1, \cdots, f_r) \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. *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) 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 $(LT(G^n))$. En particulier, $LT(\overline{S(f,g)}^{G^n}) \notin (LT(G^n))$. On a donc $(LT(G^n)) \subsetneq (LT(G^{n+1}))$ 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 Groebner réduites, unicité

Ex 1.5.1. $(x-y, y-z) = (x-z, y-z)$. Les deux couples de générateurs sont des bdg pour l'ordre lex.

1.5.1 Définition

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 $G = \{g1, \cdots, g_r\}$ une bdg de I idéal.*

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

Démonstration.

1. Comme G est une bdg, $(LT(G)) = (LT(I))$. Maintenant si $LT(g_i) \mid LT(g_j)$, alors $(LT(G \backslash \{g_j\})) = (LT(G))$ et donc $G \backslash \{g_j\}$ est une bdg.
2. $(LT(G)) = (LT(H))$ 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 $g = g'$. □

1.6 Théorie de l'élimination

1.6.1 Définition

Définition 1.6.1. 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 1.6.1. $I = (x - y + 1, x + y)$. Alors $I_1 = (2y - 1)$. $I_2 = \{0\}$.

Théorème 1.6.1. *(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 Groebner de I_l est G_l.*

Démonstration. Clairement, $G_l \subseteq I_l$ donc $(LT(G_l)) \subseteq (LT(I_l))$. Il faut montrer $\supseteq$. Soit $f \in I_l$. Alors $f \in I$, d'où $LT(f) \in (LT(G))$. On sait que $f \in k[x_{l+1}, \cdots, x_n]$. Soit $g \in G$ tq

$LT(g) \mid LT(f)$. D'où $LT(g) \in k[x_{l+1}, \cdots, x_n]$. Comme $<$ est l'ordre lex, on en déduite que $g \in k[x_{l+1}, \cdots, x_n]$. Donc $g \in G_l$ et $LT(f) \in (LT(G_l))$. □

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

1.6.2 Application 1 : Intersection d'idéaux

Problème : $I = (f_1, \cdots, f_r)$, $J = (g_1, \cdots, g_s)$. 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

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

Théorème 1.6.2. *Avec les notations ci-dessus,*

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

Démonstration. $\subseteq$: Soit $f \in I \cap J$, alors $f = tf + (1-t)f \in (tI + (1-t)J)$, puis $f \in k[x_1, \cdots, x_n]$.
$\supseteq$: Soit $f \in (tI + (1-t)J) \cap k[x_1, \cdots, x_n]$. 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 1.6.1. *Si $I = (f_1, \cdots, f_r)$, $J = (g_1, \cdots, g_s)$. Alors une bdf de $I \cap J$ pour l'ordre lex est obtenue en calculant une bdg de $(tI + (1-t)J) \overset{\text{id}}{\subseteq} k[t, x_1, \cdots, x_n]$ et en élimnant t (i.e. en prenant l'intersection avec $k[x_1, \cdots, x_n]$).*

1.6.3 Application 2 : extension

Supposons que k est un corps algébrique clos. Soit $I = (f_1, \cdots, f_r) \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$. Supposons que $(a_1, \cdots, a_n) \in V(I_1)$. Ce point s'étend en $(a_1, \cdots, a_n) \in V(I)$ si la condition 1.6.3 est vérifiée

$$f_i(x_1, \cdots, x_n) = g_i(x_2, \cdots, x_n) x_1^{N_i} + \text{ termes dont le deg en } x_1 \text{ est } < N_i \tag{1.1}$$

et $(a_2, \cdots, a_n) \notin V(g_1, \cdots, g_r)$.

1.6.4 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 $Syl(f, g, x)$ Ecrire la définition de la matrice de sylvester

Définition 1.6.2. Le résultant de f et g est $Res(f, g, x) := \det Syl(f, g, x)$

Proposition 1.6.1. *$Res(f, g, x) = 0 \iff f$ et g ont un facteur non constant en commun.*