# Algèbre commutative et effectivité

Alexandre Guillemot

17 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. □

## 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 $\beta$ un tel élément, et prenons $\gamma \in F$. Alors $\gamma \leq \beta$ implique que $\gamma$ est dans $F_n$, puisque $\gamma \leq \beta \leq \alpha^{(n)}$, et ainsi $\gamma = \beta$ par minimalité de $\beta$ dans $F_n$. Ainsi $\beta$ 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 $\beta - \alpha^{(n)} \in \mathbb{Z}^n_{>0}$ 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 $\text{mdeg}(f) = \max_{>}\{\alpha \in \mathbb{N}^n \mid \lambda_\alpha \neq 0\}$
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 $\mathrm{LT}(f) = \lambda_{\mathrm{mdeg}(f)}\mathrm{mdeg}(f)$

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

**Algorithme**

1. Initialisation : $f^{(0)} := f$, $Q_1^{(0)}, \cdots, Q_r^{(0)} = 0$, $R^{(0)} = 0$.
2. Etapte $m \geq 1$ : Si $f^{(m-1)} = 0$, alors $Q_i := Q_i^{(m_1)}$ et $R = R^{(m-1)}$, terminer l'algo. Sinon, si $\mathrm{LT}(f_1) \mid \mathrm{LT}(f^{(m_1)})$, effectuer :

$$\begin{aligned} f^{(m)} &\leftarrow f^{(m-1)} - \frac{\mathrm{LT}(f^{(m-1)})}{\mathrm{LT}(f_1)} f_1 \\ Q_1^{(m)} &\leftarrow Q_1^{(m-1)} + \frac{\mathrm{LT}(f^{(m-1)})}{\mathrm{LT}(f_1)} \\ Q_i^{(m)} &\leftarrow Q_i^{(m_1)},\ i \neq 1 \\ R^{(m)} &\leftarrow R^{(m-1)} \end{aligned}$$

Sinon si $\mathrm{LT}(f_2) \mid \mathrm{LT}(f^{(m-1)})$, effectuer

$$\begin{aligned} f^{(m)} &\leftarrow f^{(m-1)} - \frac{\mathrm{LT}(f^{(m-1)})}{\mathrm{LT}(f_2)} f_2 \\ Q_2^{(m)} &\leftarrow Q_2^{(m-1)} + \frac{\mathrm{LT}(f^{(m-1)})}{\mathrm{LT}(f_2)} \\ Q_i^{(m)} &\leftarrow Q_i^{(m_1)},\ i \neq 2 \\ R^{(m)} &\leftarrow R^{(m-1)} \end{aligned}$$

sinon si $\mathrm{LT}(f_3) \mid \mathrm{LT}(f^{(m-1)})$, effectuer ...
sinon si $\mathrm{LT}(f_r) \mid \mathrm{LT}(f^{(m-1)})$, effectuer ...
sinon effectuer

$$\begin{aligned} f^{(m)} &\leftarrow f^{(m-1)} - \mathrm{LT}(f^{(m-1)}) \\ R^{(m)} &\leftarrow R^{(m-1)} + \mathrm{LT}(f^{(m-1)}) \\ Q_i^{(m)} &\leftarrow Q_i^{(m-1)} \end{aligned}$$

**Rq 1.2.2.** A la fin de l'étape $m \geq 0$,

$$f^{(m)} + \sum Q_i^{(m)} f_i + R^{(m)} = f$$

Si $f^{(m)} = 0$, alors on a bien $\sum Q_i^{(m)} f_i + R^{(m)} = f$ et alors $R^{(m)} = 0$ ou aucun des termes de $R^{(n)}$ n'est divisible par $\mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_r)$. La procédure s'arrête : sinon, on aurait $f^{(0)}, f^{(1)}, \cdots$ avec $\mathrm{mdeg} f^{(0)} > \mathrm{mdeg} f^{(1)} > \cdots$ et ainsi $\{\alpha \mid \exists m \in \mathbb{N},\, \alpha = \mathrm{mdeg} f^{(m-1)}\}$ n'a pas d'éléments minimal.

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

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

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 Groöbner, 1) Soit $I \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$ non nul. Une base de Groöbner 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 Groöbner de l'idéal nul.

**Ex 1.3.1.**
1. Si $0 \neq g \in k[x]$, alors $\{g\}$ est une BDG (base de Groöbner) de $(g)$.
2. Si $0 \neq g \in k[x_1, \cdots, x_n]$, alors $\{g\}$ est une BDG (base de Groöbner) 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 $m \in (m_1, \cdots, m_r) \iff m$ est divisible par l'un des $m_i$.*

*Démonstration.* Exercice □

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** $E \subseteq k[x_1, \cdots, x_n]$,

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

**Définition 1.3.3.** (Base de Groöbner, 2) Une base de Groöbner 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 Groöbner 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

$$f - \sum Q_i^{(m)} g_i - R^{(m)} = f^{(m)}$$

et $f - \sum Q_i^{(m)} g_i \in I$. Si $R^{(m)}$, alors $f^{(m)} \in I$, donc $\mathrm{LT}(f^{(m)}) \in (\mathrm{LT}(G))$. D'où $R^{(m+1)} = 0$ puis récurrence. □

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

*Démonstration.* On cherche $G \overset{\text{fini}}{\subseteq} I$ tq $(\mathrm{LT}(G)) = (\mathrm{LT}(I))$. D'après le thm de la base de Hilbert, $\exists H \overset{\text{fini}}{\subseteq} \mathrm{LT}(I)$ 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

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

**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 $\forall g, h \in G$, $\overline{S(g,h)}^G = 0$*