

Table des matières

1. Théorème de Hilbert et bases de Gröbner

- 1. Quelques rappels
- 2. Division des polynômes
- 3. Théorème de Hilbert
- 4. Bases de Gröbner
- 5. Critère de Buchberger

2. Géométrie

- 1. Polynômes et variétés affines

1. Théorème de Hilbert et bases de Gröbner

Quelques rappels

Polynômes, notations et rappels

Définition 1.1

Soit k un corps.

1. On note $R = k[x_1, \dots, x_n]$ l'anneau de polynômes à coefficients dans k . Un élément de cet anneau est appelé **polynôme**.
2. On note $k(x_1, \dots, x_n)$ le corps des fractions de R (rappelons que R est un anneau intègre). C'est le corps des **fractions rationnelles**. Rapellons que l'on a

$$k(x_1, \dots, x_n) = \left\{ \frac{P}{Q} \mid P, Q \in R \text{ avec } Q \neq 0 \right\}.$$

Définition 1.2

Un **monôme** est un polynôme de la forme $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ avec $\alpha_i \in \mathbb{N}$ pour tout $i \in [1, n]$. On le note également x^α avec $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Le **degré total** de x^α est $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Remarque 1.3

1. Pour $\alpha = (0, \dots, 0)$ on a $x^\alpha = 1$ l'unité de l'anneau R .
2. Les monômes forment une base du k -espace vectoriel R : tout polynôme P s'écrit de manière unique comme somme finie de monômes :

$$P = \sum_{\alpha} a_{\alpha} x^{\alpha}$$

avec $a_{\alpha} \in k$ et $a_{\alpha} = 0$ sauf pour un nombre fini de $\alpha \in \mathbb{N}^n$.

Définition 1.4

1. Dans l'écriture, $P = \sum_{\alpha} a_{\alpha} x^{\alpha}$, le scalaire a_{α} est appelé **coefficent** du monôme x^{α} dans P .
2. Le **degré total** de P est défini par

$$\deg(P) = \sup\{|\alpha| \mid a_{\alpha} \neq 0\}.$$

3. Un polynôme est dit **homogène** si tous les monômes apparaissant avec un coefficient non nul ont le même degré total.

Exemple 1.5

Le polynôme $x_1 x_2 x_3 + x_2^3 - 10x_1^2 x_3$ est homogène. Le polynôme $x - 1^2 + x_2$ n'est pas homogène.

Idéaux, notations et rappels

Définition 1.6

Dans un anneau (commutatif) A , un **idéal** est un sous-ensemble I qui est un sous-groupe pour l'addition et tel que l'implication suivante est satisfaite: $a \in A, b \in I \Rightarrow ab \in I$.

Exemple 1.7

L'exemple typique d'un idéal est obtenu à partir d'une combinaison linéaire d'éléments de l'anneau: soit $(a_{\lambda})_{\lambda} \in \Lambda$ une famille d'éléments de A (cette famille est indexée par l'ensemble Λ et peut être infinie). On définit $(a_{\lambda} \mid \lambda \in \Lambda)$ l'**idéal engendré par la famille** $(a_{\lambda})_{\lambda} \in \Lambda$ comme l'ensemble des combinaisons linéaires finies des $(a_{\lambda})_{\lambda} \in \Lambda$ à coefficients dans A . Explicitement

$$(a_{\lambda} \mid \lambda \in \Lambda) = \left\{ \sum_{\lambda \in \Lambda} b_{\lambda} a_{\lambda} \mid b_{\lambda} \in A \text{ et } b_{\alpha} = 0 \text{ sauf pour un nombre fini de } \lambda \in \Lambda \right\}.$$

E Typesetting math: 54%

Soit A un anneau.

1. Vérifier que $(a_\lambda \mid \lambda \in \Lambda)$ est un idéal de A .
2. Vérifiez que tout idéal de A est de cette forme.

Exemple 1.9

Un cas particulier de l'exemple 1.7 précédent est le cas d'une famille $(a_\lambda)_{\lambda \in \Lambda}$ finie. Dans ce cas on indexe les éléments de la famille par des entiers, typiquement $a_1, \dots, a_r \in A$ avec $r \in \mathbb{N}$, $r \geq 1$. Dans ce cas on note (a_1, \dots, a_r) l'idéal engendré par cette famille.

Exemple 1.10

Dans l'anneau des polynômes R , voici quelques exemples de tels idéaux.

1. L'idéal nul : $(0) = \{0\}$.
2. L'anneau lui-même : $(1) = R$.
3. L'idéal "irrelevant" : $(x_1, \dots, x_n) = R \setminus (\mathbf{k}^\times)$ où \mathbf{k}^\times est l'ensemble des éléments inversibles de \mathbf{k} c'est-à-dire $\mathbf{k} \setminus \{0\}$.

Définition 1.11

Soit A un anneau

1. Un idéal I de A est dit de **type fini** s'il existe une famille finie d'éléments $a_1, \dots, a_r \in A$ telle que $I = (a_1, \dots, a_r)$.
2. Un anneau A est dit **noethérien** si tout idéal de A est de type fini.

Le premier objectif de ce cours sera de donner une preuve constructive d'un théorème classique dû à Hilbert.

Théorème 1.12 (Théorème de Hilbert)

L'anneau R est noethérien.

L'objectif n'est pas tant le résultat en lui-même mais plutôt la méthode, complètement effective, ainsi que les outils développés qui serviront par la suite pour d'autres problèmes algébro-géométriques.

Avant cela, nous rappelons quelques résultats qui donnent une caractérisation de l'idéal $(a_\lambda)_{\lambda \in \Lambda}$ ainsi qu'un critère effectif d'égalité entre idéaux.

Lemme 1.13

Une intersection quelconque d'idéaux est un idéal.

Exercice 1.14

Donner une preuve du lemme précédent.

Proposition 1.15

Pour tout sous-ensemble E d'un anneau A il existe un unique plus petit idéal contenant E . C'est l'idéal (E) engendré par la famille des éléments de E .

Exercice 1.16

Donner une preuve de la proposition précédente.

Corollaire 1.17

Soit A un anneau et I un idéal. Soient a_1, \dots, a_r des éléments de A . Alors on a l'équivalence

$$(a_1, \dots, a_r) \subset I \Leftrightarrow a_i \in I, \text{ pour tout } i \in [1, r].$$

Exercice 1.18

Donner une preuve du corollaire précédent.

On obtient enfin un critère simple d'égalité d'idéaux.

Corollaire 1.19

Soit A un anneau et soient $a_1, \dots, a_r, b_1, \dots, b_\ell$ des éléments de A . Alors on a l'équivalence

$$(a_1, \dots, a_r) = (b_1, \dots, b_\ell) \Leftrightarrow \begin{cases} a_i \in (b_1, \dots, b_\ell) & \text{pour tout } i \in [1, r], \text{ et} \\ b_j \in (a_1, \dots, a_r) & \text{pour tout } j \in [1, \ell]. \end{cases}$$

Exercice 1.20

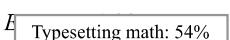
Donner une preuve du corollaire précédent.

Exemple 1.21

Pour un corps \mathbf{k} de caractéristique différente de 2, on a l'égalité $(x+y, x-y) = (x, y)$. En effet, l'inclusion de gauche à droite est claire et valable pour tout corps. Par contre, on a

$$x = \frac{1}{2}(x+y) + \frac{1}{2}(x-y) \text{ et } x = \frac{1}{2}(x+y) - \frac{1}{2}(x-y).$$

En caractéristique 2, on a l'inclusion stricte $(x+y, x-y) = (x+y) \subsetneq (x, y)$.

 Dans l'anneau $\mathbf{k}[x_1, x_2]$, pour quels corps de base \mathbf{k} a-t-on l'égalité d'idéaux $(2x_1^2 + 3x_2^2 - 11, x_1^2 - x_2^2 - 3) = (x_1^2 - 4, x_2^2 - 1)$?

Théorème de Hilbert pour les polynômes à une variable

C'est un résultat bien connu que l'anneau des polynômes à une variable est principal. Nous présentons une preuve constructive qui sera le modèle de la preuve du théorème de Hilbert dans le cas général.

Définition 1.23

Soit $P \in \mathbb{k}[x]$ un polynôme. Pour $P \neq 0$, il existe des scalaires $a_0, \dots, a_r \in \mathbb{k}$ avec $a_r \neq 0$ tels que $P = a_r x^r + \dots + a_0$. On a $\deg(P) = r$. Le polynôme $a_r x^r$ est appelé **terme dominant** de P . On écrira $\text{LT}(P) = a_r x^r$.

Remarque 1.24

On a $\deg(P) = \deg(\text{LT}(P))$.

Exemple 1.25

Soit $P = 2x^3 + 4x^7 - x^4$. On a $\text{LT}(P) = 4x^7$.

Remarque 1.26 (Divisibilité des monômes)

1. Il est très simple de tester si un monôme ax^r non nul de $\mathbb{k}[x]$ divise un autre monôme non nul bx^ℓ de $\mathbb{k}[x]$. En effet ax^r divise bx^ℓ si et seulement si $r \leq \ell$.

En particulier ax^r divise bx^ℓ si et seulement si $\deg(ax^r) \leq \deg(bx^\ell)$.

2. La même chose est vraie pour les polynômes à plusieurs variables. Le monôme ax^α divise bx^β si et seulement si $\alpha \leq \beta$ pour l'ordre (non total) qui compare chaque coefficient.

Proposition 1.27 (Division euclidienne)

Soit $P_1 \in \mathbb{k}[x]$ un polynôme non nul.

Pour tout $P \in \mathbb{k}[x]$, il existe un unique couple (Q, S) d'éléments de $\mathbb{k}[x]$ tels que $P = QP_1 + S$ avec $S = 0$ ou $\deg(S) < \deg(P_1)$.

On donne une preuve sous forme d'algorithme.

Algorithme 1.28

Entrée : P, P_1 .

Sortie : Q, S .

$Q := 0$ et $S := P$.

Tant que $S \neq 0$ et que $\text{LT}(P_1)$ divise $\text{LT}(S)$ faire :

$$\begin{aligned} Q &:= Q + \text{LT}(S)/\text{LT}(P_1), \\ S &:= S - (\text{LT}(S)/\text{LT}(P_1))P_1. \end{aligned}$$

Donner (Q, S) .

Preuve : Vérifions que cet algorithme fait ce qu'on lui demande. À chaque tour de l'algorithme, on a toujours l'égalité

$$P = QP_1 + S = (Q + \text{LT}(S)/\text{LT}(P_1))P_1 + (S - (\text{LT}(S)/\text{LT}(P_1))P_1).$$

Par ailleurs, l'algorithme s'arrête lorsque ($S \neq 0$ et $\text{LT}(P_1)$ divise $\text{LT}(S)$) est fausse. On a donc en sortie l'alternative $S = 0$ ou $\text{LT}(P_1)$ ne divise pas $\text{LT}(S)$ c'est-à-dire l'alternative $S = 0$ ou $\deg(\text{LT}(P_1)) > \deg(\text{LT}(S))$ c'est-à-dire l'alternative $S = 0$ ou $\deg(P_1) > \deg(S)$.

Il reste à vérifier que l'algorithme termine. À chaque étape, soit S devient nul, soit son degré diminue. En effet, l'opération $S := S - (\text{LT}(S)/\text{LT}(P_1))P_1$ consiste à éliminer grâce à P_1 le terme dominant de S . Au bout d'un nombre fini d'opérations, si S n'est pas nul, son degré sera donc plus petit que celui de P_1 .

Vérifions enfin que cette écriture est unique. Si on a deux écritures $P = QP_1 + S$ et $P = Q'P_1 + S'$, alors on a $P_1(Q - Q') = S' - S$. Si $S \neq S'$, alors $P_1(Q - Q') \neq 0$ et on a

$$\deg(P_1) \leq \deg(P_1(Q - Q')) = \deg(S' - S) \leq \max(\deg(S), \deg(S')) < \deg(P_1).$$

Une contradiction. On en déduit $S = S'$ et comme $\mathbb{k}[x]$ est intègre et $P_1 \neq 0$, on a $Q = Q'$. □

Corollaire 1.29

Tout idéal de $\mathbb{k}[x]$ est principal : tout idéal I est de la forme $I = (P)$ avec $P \in \mathbb{k}[X]$. De plus P est unique à multiplication par un scalaire non nul près.

Preuve : Si $I = (0)$, on a fini. On suppose donc que I contient au moins un élément non nul et on pose

$$r = \min\{\deg(Q) \mid Q \in I \text{ et } Q \neq 0\}.$$

Par hypothèse l'ensemble ci-dessus est non vide et admet donc un minimum. Soit alors $Q \in I$ tel que $Q \neq 0$ et $\deg(Q) = r$. On montre l'égalité $I = (Q)$. Comme $Q \in I$, on a l'inclusion $(Q) \subset I$. Soit donc $P \in I$. La division euclidienne nous donne des polynômes R et S tels que $P = QR + S$ avec $S = 0$ ou $\deg(S) < \deg(Q)$. On peut réécrire $S = P - QR$ et comme $P, Q \in I$, on obtient $S \in I$. Par minimalité de $r = \deg(Q)$, on déduit $S = 0$ donc $P = QR \in (Q)$.

Il reste à montrer l'unicité. Si $(P) = (P')$ alors $P = QP'$ et $P' = Q'P$. On obtient $P = QQ'P$ et donc $QQ' = 1$ (l'anneau est intègre). En particulier $\deg(Q) + \deg(Q') = 0$ donc $\deg(Q) = \deg(Q') = 0$ donc Q et Q' sont des constantes non nulles. □

Typesetting math: 54%

Division des polynômes

Ordres admissibles

On a vu qu'un point crucial de la preuve du théorème de Hilbert pour les polynômes à une variable est l'utilisation de l'ordre pour comparer les monômes et déterminer la divisibilité. Les choses sont plus complexes lorsqu'on a au moins deux variables et nous aurons besoin de choisir des ordres ayant de bonnes propriétés sur l'ensemble des exposants des monômes.

Rappelons la notion d'ordre et d'ordre total.

Définition 1.30

Soit E un ensemble et \mathfrak{R} une relation.

1. La relation \mathfrak{R} est une **relation d'ordre** si elle est réflexive (pour tout $e \in E$, on a $e\mathfrak{R}e$), antisymétrique (si $e\mathfrak{R}f$ et $f\mathfrak{R}e$ alors $e = f$) et transitive (si $e\mathfrak{R}f$ et $f\mathfrak{R}g$ alors $e\mathfrak{R}g$).

En général, on note une relation d'ordre avec le symbole \leq . La relation ($a \leq b$ et $a \neq b$) est notée $a < b$.

2. Une relation d'ordre \leq est dite **totale** si pour tout $e, f \in E$, on a $e \leq f$ ou $f \leq e$.

Définition 1.31

Un **ordre admissible** sur $R = k[x_1, \dots, x_n]$ est une relation d'ordre $<$ sur l'ensemble des monômes (ou de manière équivalente sur l'ensemble \mathbb{N}^n des exposants) vérifiant des conditions suivantes:

1. L'ordre $<$ est total.
2. L'ordre $<$ est compatible avec la multiplication: si $x^\alpha < x^\beta$ alors $x^\alpha x^\gamma < x^\beta x^\gamma$.
3. L'ordre $<$ est bien ordonné : tout ensemble non vide de monômes a un élément minimal pour $<$.

Remarque 1.32

1. La première condition permet d'écrire tout polynôme comme une suite strictement décroissante de monômes.
2. La seconde condition parle d'elle-même : compatibilité avec la multiplication, si $x^\alpha < x^\beta$ alors $x^\alpha x^\gamma = x^{\alpha+\gamma} < x^{\beta+\gamma} = x^\beta x^\gamma$.
3. La troisième condition impose la propriété très utile suivante : l'ensemble des monômes inférieurs à un monôme donné est fini. En effet, s'il un tel ensemble était infini, on pourrait construire une suite décroissante infinie contredisant la condition d'ordre bien ordonné.

Exemples d'ordres admissibles

Définition 1.33

L'**ordre lexicographique** $<_{lex}$ est défini par :

$$x^\alpha <_{lex} x^\beta \Leftrightarrow \text{le premier coefficient non nul de } \beta - \alpha \text{ est } > 0.$$

Il est à noter que l'on "lit" les éléments α et β de gauche à droite.

Définition 1.34

L'**ordre lexicographique inversé** $<_{revlex}$ est défini par :

$$x^\alpha <_{revlex} x^\beta \Leftrightarrow \text{le dernier coefficient non nul de } \beta - \alpha \text{ est } > 0.$$

On peut voir cet ordre comme un ordre lexicographique où on "lit" les éléments α et β de droite à gauche.

Définition 1.35

L'**ordre lexicographique gradué** est défini par :

$$x^\alpha <_{deglex} x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{ou} \\ |\alpha| = |\beta| \text{ et } x^\alpha <_{lex} x^\beta. \end{cases}$$

On compare d'abord les degrés puis on applique l'ordre lexicographique.

Définition 1.36

L'**ordre lexicographique gradué inversé** est défini par :

$$x^\alpha <_{degrevlex} x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{ou} \\ |\alpha| = |\beta| \text{ et } x^\alpha >_{revlex} x^\beta. \end{cases}$$

On compare d'abord les degrés puis on applique l'opposé de l'ordre lexicographique inversé.

Remarque 1.37

Une définition équivalente de l'ordre lexicographique gradué inverse est la suivante :

$$x^\alpha <_{degrevlex} x^\beta \Leftrightarrow \begin{cases} |\alpha| < |\beta|, \\ \text{ou} \\ |\alpha| = |\beta| \text{ et le dernier coefficient non nul de } \beta - \alpha \text{ est } < 0. \end{cases}$$

Typesetting math: 54%

Exemple 1.38

Soit n un entier et $R = \mathbb{k}[x_1, \dots, x_n]$.

1. On a les ordres suivants sur les monômes de degrés 1.

Pour \prec_{lex}	$x_1 > x_2 > \dots > x_n$.
Pour \prec_{revlex}	$x_1 < x_2 < \dots < x_n$.
Pour \prec_{deglex}	$x_1 > x_2 > \dots > x_n$.
Pour $\prec_{degrevalex}$	$x_1 > x_2 > \dots > x_n$.

2. Pour $n = 3$, on a les ordres suivants sur les monômes de degrés 2.

Pour \prec_{lex}	$x_1^2 > x_1x_2 > x_1x_3 > x_2^2 > x_2x_3 > x_3^2$.
Pour \prec_{revlex}	$x_1^2 < x_1x_2 < x_2^2 < x_1x_3 < x_2x_3 < x_3^2$.
Pour \prec_{deglex}	$x_1^2 > x_1x_2 > x_1x_3 > x_2^2 > x_2x_3 > x_3^2$.
Pour $\prec_{degrevalex}$	$x_1^2 > x_1x_2 > x_2^2 > x_1x_3 > x_2x_3 > x_3^2$.

3. On a $x_1^2x_2^4x_3^6 \prec_{lex} x_1^5x_2^4x_3^2$ et $x_1^2x_2^4x_3^6 \succ_{deglex} x_1^5x_2^4x_3^2$.

Lemme 1.39

Les ordres \prec_{lex} , \prec_{revlex} , \prec_{deglex} et $\prec_{degrevalex}$ sont admissibles.

Exercice 1.40

Donner une preuve du lemme précédent.

Algorithme de division des polynômes

Nous supposerons désormais que l'anneau des polynômes R est muni d'un ordre admissible \prec .

Définition 1.41

Soit $P \in R$ non nul. On écrit $P = \sum_{\alpha} a_{\alpha} x^{\alpha}$.

1. Le **multidegré** de P est $\text{mdeg}(P) = \max\{\beta \mid a_{\beta} \neq 0\}$.

Soit $\alpha = \text{mdeg}(P)$.

2. Le **monôme dominant** de P est le monôme $\text{LM}(P) = x^{\alpha}$.

3. Le **coefficent dominant** de P est le scalaire $\text{LC}(P) = a_{\alpha}$.

4. Le **terme dominant** de P est le polynôme $\text{LT}(P) = a_{\alpha} x^{\alpha}$.

Remarque 1.42

Le multidegré, le monôme dominant et le terme dominant du polynôme nul 0 ne sont pas définis.

Il est à noter que le monôme dominant $\text{LM}(P)$ et le terme dominant $\text{LT}(P)$ dépendent de l'ordre \prec choisi. On les note parfois $\text{LM}_{\prec}(P)$ et $\text{LT}_{\prec}(P)$.

Exemple 1.43

Pour $P = 5x_1^2x_3 + 2x_1x_2x_3^2 \in \mathbb{C}[x_1, x_2, x_3]$, on a

$$\text{LT}_{\prec_{lex}}(P) = 5x_1^2x_3 \text{ et } \text{LT}_{\prec_{degrevalex}}(P) = 2x_1x_2x_3^2.$$

Lemme 1.44

Soient $P, Q \in R$ des polynômes non nuls.

1. On a $\text{mdeg}(PQ) = \text{mdeg}(P) + \text{mdeg}(Q)$ et $\text{LT}(PQ) = \text{LT}(P)\text{LT}(Q)$.

2. Si $P + Q \neq 0$, on a $\text{mdeg}(P + Q) \leq \max(\text{mdeg}(P), \text{mdeg}(Q))$.

3. Si $\text{mdeg}(P) < \text{mdeg}(Q)$ alors $\text{LT}(P + Q) = \text{LT}(Q)$.

Exercice 1.45

Donner une preuve du lemme précédent.

Nous donnons maintenant un algorithme de division semblable à la division euclidienne.

Proposition 1.46 (Algorithme de division)

Soit $F = (P_1, \dots, P_r)$ une famille ordonnée de polynômes non nuls.

Pour tout $P \in R$, il existe des polynômes (Q_1, \dots, Q_r, S) dans R tels que

$$P = P_1Q_1 + \dots + P_rQ_r + S$$

e Typesetting math: 54% ns suivantes soient satisfaites :

1. pour tout $i \in [1, r]$, on a $P_i Q_i = 0$ ou $\text{LT}(P_i Q_i) \leq \text{LT}(P)$.
2. $S = 0$ ou S est une combinaison linéaire de monômes dont aucun n'est divisible par $\text{LT}(P_1), \dots, \text{LT}(P_r)$.

Définition 1.47

Dans la proposition ci-dessus, le polynôme S est appelé **reste de la division** de P par F . Il est noté $S = \overline{P}^F$

On donne une preuve sous forme d'algorithme.

Algorithme 1.48

Entrée : P, P_1, \dots, P_r .

Sortie : Q_1, \dots, Q_r, S .

$Q_i := 0$ pour $i \in [1, r]$ et $S := 0$.

$T := P$.

(On introduit une variable locale T qui désigne le polynôme intermédiaire des divisions à chaque étape.)

Tant que $T \neq 0$ faire :

i := 1

 division := faux.

 Tant que $i \leq r$ et division = faux faire :

 Si $\text{LT}(P_i)$ divise $\text{LT}(T)$ alors (On divise T par P_i et on arrête)

$Q_i := Q_i + \text{LT}(T)/\text{LT}(P_i)$

$T := T - (\text{LT}(T)/\text{LT}(P_i))P_i$

 division := vrai.

 Sinon $i := i + 1$ (On essaie le polynôme suivant de F)

 Si division = faux faire : (si aucun élément de F n'a marché, on regarde le coefficient suivant de T)

$S := S + \text{LT}(T)$

$T := T - \text{LT}(T)$.

Donner (Q_1, \dots, Q_r, S) .

Preuve : Vérifions que cet algorithme fait ce qu'on lui demande.

1. Commençons par montrer qu'à chaque tour de l'algorithme, on a toujours l'égalité :

$$P = Q_1 P_1 + \dots + Q_r P_r + S + T.$$

On a deux cas à considérer. Si $\text{LT}(P_i)$ divise $\text{LT}(T)$ alors on a l'égalité $P_i Q_i + T = P_i(Q_i + \text{LT}(T)/\text{LT}(P_i)) + T - (\text{LT}(T)/\text{LT}(P_i))P_i$. Les autres termes de l'égalité restant inchangés, le résultat en résulte. Si on a aucune divisibilité et que la variable "division" a encore la valeur "faux" alors on a l'égalité : $S + T = (S + \text{LT}(T)) + (T - \text{LT}(T))$ les autres termes sont inchangés.

2. On voit donc qu'en fin d'algorithme, comme $T = 0$, on aura l'égalité voulue.

3. Montrons maintenant que l'algorithme s'arrête effectivement. Pour cela il suffit de montrer que le multi-degré de la variable locale T diminue à chaque étape. On a les deux même cas à considérer. Si $\text{LT}(P_i)$ divise $\text{LT}(T)$ alors T devient $T - (\text{LT}(T)/\text{LT}(P_i))P_i$ et on a éliminé son terme dominant. Si on a aucune divisibilité et que la variable "division" a encore la valeur "faux" alors T devient $T - \text{LT}(T)$ et le multi-degré a encore diminué.

4. La condition sur S est claire : on ne change S que lorsque la variable "division" a la valeur "faux" c'est-à-dire qu'aucun des $\text{LT}(P_i)$ ne divise $\text{LT}(T)$ et on ajour alors $\text{LT}(T)$ à S .

5. Il reste à montrer les conditions sur $P_i Q_i$. Mais on a vu que le multi-degré de T est décroissant au cours de l'algorithme avec $T = P$ en début d'algorithme. On a donc toujours $\text{LT}(T) \leq \text{LT}(P)$. Comme les monômes apparaissant dans Q_i sont de la forme $\text{LT}(T)/\text{LT}(P_i)$, si $P_i Q_i$ est non nul, on a toujours $\text{LT}(P_i Q_i) \leq \text{LT}(T) \leq \text{LT}(P)$.

□

Exemple 1.49

Soit < l'ordre lexicographique et soient $P_1 = x_1 x_2 + 1$ et $P_2 = x_2^2 - 1$. Soit enfin $P = x_1 x_2^2 - x_1$.

1. Pour $F = (P_1, P_2)$, l'algorithme de division donne le résultat suivant:

$$P = x_1 x_2^2 - x_1 = x_2(x_1 x_2 + 1) + 0 \cdot (x_2^2 - 1) + (-x_1 - x_2).$$

2. Pour $F = (P_2, P_1)$, l'algorithme de division donne le résultat suivant:

$$P = x_1 x_2^2 - x_1 = x_1(x_2^2 - 1) + 0 \cdot (x_1 x_2 + 1) + 0.$$

En particulier, on voit deux choses :

- L'algorithme de division dépend de l'ordre de la famille.
- La condition $P^F = 0$ est une condition suffisante pour l'appartenance $P \in (P_1, \dots, P_r)$ mais non nécessaire.

Nous verrons que les bases de Gröbner fournissent une solution à ces deux problèmes : la division ne dépend plus de l'ordre et l'annulation du reste est une condition nécessaire et suffisante à l'appartenance à un idéal.

Exemple 1.50

Typesetting math: 54% aphique et soit $P = x_1^2 x_2 + x_1 x_2^2 + x_2^3$.

1. Soit $F = (P_1, P_2)$ avec $P_1 = x_1x_2 - 1$ et $P_2 = x_2^2 - 1$. L'algorithme de division nous donne :

$$\begin{aligned} P &= x_1^2x_2 + x_1x_2^2 + x_2^2 \\ &= x_1(x_1x_2 - 1) + x_1x_2^2 + x_1 + x_2^2 \\ &= x_1(x_1x_2 - 2 - 1) + x_2(x_1x_2 - 1) + x_1 + x_2^2 + x_2 \\ &= (x_1 + x_2)(x_1x_2 - 2 - 1) + 1 \cdot (x_2^2 - 1) + x_1 + x_2 + 1. \end{aligned}$$

2. Soit $F = (P_1, P_2)$ avec $P_1 = x_2^2 - 1$ et $P_2 = x_1x_2 - 1$. L'algorithme de division nous donne :

$$P = x_1^2x_2 + x_1x_2^2 + x_2^2 = (x_1 + 1)(x_2^2 - 1) + x_1(x_1x_2 - 1) + 2x_1 + 1.$$

Exercice 1.51

Calculer le reste de la division du polynôme $P = x_1^7x_2^2 + x_1^3x_2^2 - x_2 + 1$ dans les cas suivants.

1. Avec l'ordre $>_{deglex}$ et la famille $F = (x_1x_2^2 - x_1, x_1 - x_2^3)$.
2. Avec l'ordre $>_{lex}$ et la famille $F = (x_1x_2^2 - x_1, x_1 - x_2^3)$.
3. Avec l'ordre $>_{deglex}$ et la famille $F = (x_1 - x_2^3, x_1x_2^2 - x_1)$.
4. Avec l'ordre $>_{lex}$ et la famille $F = (x_1 - x_2^3, x_1x_2^2 - x_1)$.

Théorème de Hilbert

Fixons un ordre admissible $<$.

Idéaux monomiaux

Les idéaux monomiaux sont une classe d'idéaux pour lesquels les problèmes de division, appartenance, existence d'une base, etc. sont très facile à résoudre.

Définition 1.52

Un idéal I de R est dit **monomial** s'il existe un sous-ensemble $A \subset \mathbb{N}^n$ d'exposants (eventuellement infini) tel que $I = (x^\alpha \mid \alpha \in A)$.

Le premier problème auquel on se consacre est le problème d'appartenance : pour I un idéal monomial et $P \in R$, à quelle condition a-t-on $P \in I$?

On commence par le cas où P est un monôme.

Lemme 1.53

Soient $I = (x^\alpha \mid \alpha \in A)$ un idéal monomial et x^β un monôme. On a alors l'équivalence ($x^\beta \in I \Leftrightarrow$ il existe $\alpha \in A$ tel que x^α divise x^β).

Preuve : L'implication de droite à gauche est claire. Réciproquement, on écrit $x^\beta = \sum_{\alpha \in A} P_\alpha x^\alpha$ avec $P_\alpha \in R$ et $P_\alpha = 0$ sauf pour un nombre fini d'entre eux. En développant les $P_\alpha x^\alpha$ en monômes, on voit que x^β doit apparaître dans l'un d'entre eux au moins. Il existe donc un x^α qui divise x^β .

□

Le cas général en découle.

Lemme 1.54

Soit $I = (x^\alpha \mid \alpha \in A)$ un idéal monomial et soit $P \in R$. On a équivalence entre les propositions suivantes :

1. $P \in I$.
2. Tous les monômes de P appartiennent à I .
3. P est une combinaison linéaire de monômes de I .

Preuve : Les implications (2. \Rightarrow 3.) et (3. \Rightarrow 1.) sont claires. On montre (1. \Rightarrow 2.). On procède par récurrence sur le nombre de monômes de P . Si P est un monôme, le résultat est clair. Sinon, on écrit $\text{LT}(P) = cx^\beta$ et $P = cx^\beta + (P - \text{LT}(P))$. On écrit $P = \sum_{\alpha \in A} P_\alpha x^\alpha$ avec $P_\alpha \in R$ et $P_\alpha = 0$ sauf pour un nombre fini d'entre eux. En développant les $P_\alpha x^\alpha$ en monômes, on voit que x^β doit apparaître dans l'un d'entre eux au moins. Il existe donc un x^α qui divise x^β donc $\text{LT}(P) \in I$. On en déduit $P - \text{LT}(P) \in I$ et le résultat en découle par récurrence.

□

On obtient un critère d'égalité pour les idéaux monomiaux.

Corollaire 1.55

Deux idéaux monomiaux sont égaux si et seulement si ils contiennent les même monomes.

On en déduit le théorème de Hilbert pour les idéaux monomiaux.

Théorème 1.56 (Lemme de Dickson)

Soit $I = (x^\alpha \mid \alpha \in A)$ un idéal monomial. Alors il existe un sous-ensemble fini $\alpha_1, \dots, \alpha_r \in A$ tel que $I = (x^{\alpha_1}, \dots, x^{\alpha_r})$. En particulier I est de type fini.

Preuve : On procède par récurrence sur le nombre de variables n . Si $n = 1$, alors $I = (x_1^\alpha \mid \alpha \in A)$. On pose $\beta = \min\{\alpha \in A\}$ (il est à noter que dans ce cas A est un ensemble d'entiers). Pour tout $\alpha \in A$, on a $\beta \leq \alpha$ donc x_1^β divise x_1^α et donc $x_1^\alpha \in (x_1^\beta)$. On en déduit $I = (x_1^\beta)$.

Supposons le résultat prouvé pour $n - 1$ variables. On écrit les monômes en les variables x_1, \dots, x_{n-1}, x_n sous la forme $x^\alpha ym$ où x^α est un $\frac{1}{\text{Typesetting math: } 54\%} \frac{1}{\text{Typesetting math: } 54\%} \frac{1}{\text{Typesetting math: } 54\%}$ première variables x_1, \dots, x_{n-1} et $\alpha \in \mathbb{N}^{n-1}$. On considère l'idéal $J \subset k[x_1, \dots, x_{n-1}]$ suivant (obtenu par "projection" $\frac{1}{\text{Typesetting math: } 54\%} \frac{1}{\text{Typesetting math: } 54\%} \frac{1}{\text{Typesetting math: } 54\%}$ $x_n | \alpha_1, \dots, \alpha_{n-1}$) :

$$J = (x^\alpha \mid \text{il existe } m \text{ tel que } x^\alpha y^m \in I).$$

Il est clair que J est un idéal monomial. Par hypothèse de récurrence, il existe des exposants $\alpha_1, \dots, \alpha_r$ de \mathbb{N}^{n-1} tels que $J = (x^{\alpha_1}, \dots, x^{\alpha_r})$.

Pour chaque $i \in [1, r]$, il existe, par définition de J , un entier $m_i \in \mathbb{N}$ tel que $x^{\alpha_i} y^{m_i} \in I$. On pose $m_0 = \max\{m_1, \dots, m_r\}$. Maintenant pour chaque $k \in [0, m_0 - 1]$, on considère l'idéal $J_k \subset \mathbb{k}[x_1, \dots, x_{n-1}]$ défini par (la “section” de I engendré par les monômes où y apparaît à la puissance k) :

$$J_k = (x^\alpha \mid x^\alpha y^k \in I).$$

Il est clair que J_k est un idéal monomial pour tout $k \in [0, m_0 - 1]$. Par hypothèse de récurrence, il existe des exposants $\alpha_{k,1}, \dots, \alpha_{k,r_k}$ de \mathbb{N}^{n-1} tels que $J_k = (x^{\alpha_{k,1}}, \dots, x^{\alpha_{k,r_k}})$. Nous allons maintenant montrer l'égalité :

$$I = (x^{\alpha_i} y^{m_0}, x^{\alpha_{k,j}} y^k \mid i \in [1, r], k \in [0, m_0 - 1], j \in [1, r_k]).$$

On commence par montrer que les monômes de droites sont dans I . Pour $i \in [1, r]$, on a $x^{\alpha_i} y^{m_i} \in I$. Et comme $m_0 \geq m_i$, on a en déduit $x^{\alpha_i} y^{m_0} = x^{\alpha_i} y^{m_i} y^{m_0 - m_i} \in I$. Pour $k \in [0, m_0 - 1]$ et $j \in [1, r_k]$, on a $x^{\alpha_{k,j}} \in J_k$ et par définition $x^{\alpha_{k,j}} y^k \in I$.

Réciprocement, montrons que tout monôme de I est divisible par l'un des monômes de droite. Soit donc $x^\alpha y^\ell \in I$. De deux choses l'une : soit $\ell \geq m_0$, soit $\ell \in [0, m_0 - 1]$. Dans le premier cas, on a par définition $x^\alpha \in J$ donc il existe un $i \in [1, r]$ tel que x^{α_i} divise x^α . Par ailleurs comme $\ell \geq m_0$, le monôme y^{m_0} divise y^ℓ . On en déduit que $x^{\alpha_i} y^{m_0}$ divise $x^\alpha y^\ell$. Dans le second cas, on a $\ell \in [0, m_0 - 1]$ et $x^\alpha \in J_\ell$. En particulier, il existe un $j \in [1, r_\ell]$ tel que $x^{\alpha_{\ell,j}}$ divise x^α . On en déduit que $x^{\alpha_{\ell,j}} y^\ell$ divise $x^\alpha y^\ell$.

On a donc montré que I est de type fini $I = (x^{\beta_1}, \dots, x^{\beta_r})$. Il reste à vérifier que l'on peut prendre pour générateurs des éléments de A . Mais pour tout i , on a $x^{\beta_i} \in I$ donc par le Lemme 1.53, il existe $\alpha_i \in A$ tel que x^{α_i} divise x^{β_i} . On peut donc remplacer x^{β_i} par x^{α_i} ce qui prouve le résultat. \square

Exemple 1.57

Voici quelques exemples de base obtenues à partir de la méthode développée dans la preuve ci-dessus.

1. Soit $I = (x_1^3 x_2^3, x_1^4 x_2^2, x_1^2 x_2^5)$. On applique la méthode du théorème précédent. On a tout d'abord $J = (x_1^3, x_1^4, x_1^2) = (x_1^2)$. On a donc $m_1 = 5 = m_0$. On a ensuite

$$J_0 = J_1 = (0), J_2 = (x_1^4), J_3 = (x_1^3) \text{ et } J_4 = (0).$$

On en déduit une base pour I :

$$I = (x_1^2 x_2^5, x_1^4 x_2^2, x_1^3 x_2^3).$$

2. Soit $I = (x_1^4 x_2^2, x_1^3 x_2^4, x_1^2 x_2^5)$. On applique la méthode du théorème précédent. On a tout d'abord $J = (x_1^4, x_1^3, x_1^2) = (x_1^2)$. On a donc $m_1 = 5 = m_0$. On a ensuite

$$J_0 = J_1 = (0), J_2 = (x_1^4) = J_3 \text{ et } J_4 = (x_1^3).$$

On en déduit une base pour I :

$$I = (x_1^2 x_2^5, x_1^4 x_2^2, x_1^4 x_2^3, x_1^3 x_2^4).$$

Corollaire 1.58

Soit $<$ un ordre sur \mathbb{N}^n (ou sur les monômes de R) satisfaisant les deux premières conditions pour être un ordre admissible (c'est-à-dire que l'ordre est total et compatible avec la multiplication). Alors $<$ est admissible si et seulement si $x^\alpha \geq x^0$ pour tout $\alpha \in \mathbb{N}^n$.

Preuve : Supposons que l'ordre est admissible et soit x^α le plus petit monôme pour l'ordre $<$. On doit montrer que $\alpha = 0$. Si ce n'est pas le cas, on a $x^\alpha < x^0$ et en multipliant par x^α on obtient $x^{2\alpha} < x^\alpha$ contredisant la minimalité de x^α .

Réciprocurement, il nous faut montrer que tout ensemble non vide de monômes a un élément minimal. Soit $\{x^\alpha \mid \alpha \in A\}$ un tel ensemble de monômes avec A non vide. On pose $I = (x^\alpha \mid \alpha \in A)$. Par le lemme de Dickson, il existe des éléments $\alpha_1, \dots, \alpha_r \in A$ tels que $I = (x^{\alpha_1}, \dots, x^{\alpha_r})$. Quitte à réordonner les termes, on peut supposer que l'on a $x^{\alpha_1} < \dots < x^{\alpha_r}$. Nous allons montrer que x^{α_1} est le minimum de $\{x^\alpha \mid \alpha \in A\}$. Soit donc x^α avec $\alpha \in A$ un élément de cet ensemble. On a $x^\alpha \in I$ et donc il existe un i tel que x^{α_i} divise x^α . On a donc $\alpha = \alpha_i + \beta$ avec $\beta \in \mathbb{N}^n$. Par hypothèse, on a $\beta \geq 0$ et donc $\alpha = \alpha_i + \beta \geq \alpha_i \geq \alpha_1$ ce qui prouve le résultat. \square

Le théorème de Hilbert

Nous allons maintenant montrer le théorème de la base de Hilbert de manière effective. Un outil essentiel et qui servira également plus tard est l'idéal des termes dominants (encore une fois on a choisi un ordre admissible $<$).

Définition 1.59

Soit $I \subset R$ un idéal.

1. L'**ensemble des termes dominants** $\text{LT}(I)$ de I est défini par :

$$\text{LT}(I) = \{\text{LT}(P) \mid P \in I\}.$$

Typesetting math: 54%

2. L'**idéal des termes dominants** de I est l'idéal ($\text{LT}(I)$) engendré par $\text{LT}(I)$.

Remarque 1.60

L'idéal $(\text{LT}(I))$ est monomial (on peut remplacer $\text{LT}(P)$ par $\text{LM}(P)$ dans la définition).

Exemple 1.61

Soit $I \subset \mathbb{k}[x_1, x_2]$ et $<$ l'ordre lexicographique.

1. Pour $I = (x_1 + x_2)$, on a $(\text{LT}(I)) = (x_1)$. On remarque en particulier que l'on a $(\text{LT}(I)) \not\subseteq I$ et $I \not\subseteq (\text{LT}(I))$.
2. Pour $I = (P_1, P_2)$ avec $P_1 = x_1^3 - 2x_1x_2$ et $P_2 = x_1^2x_2 - 2x_2^2 + x_1$, remarquons que l'on a pas $(\text{LT}(I)) = (\text{LT}(P_1), \text{LT}(P_2))$. En effet, $(\text{LT}(P_1), \text{LT}(P_2)) = (x_1^3, x_1^2x_2)$. Cependant, on a

$$x_1P_2 - x_2P_1 = x_1(x_1^2x_2 - 2x_2^2 + x_1) - x_2(x_1^3 - 2x_1x_2) = x_1^2$$

et donc $x_1^2 \in I$. En particulier $x_1^2 = \text{LT}(x_1^2) \in \text{LT}(I)$ mais $x_1^2 \notin (\text{LT}(P_1), \text{LT}(P_2))$. Dans cet exemple, on a donc une inclusion stricte $(\text{LT}(P_1), \text{LT}(P_2)) \subsetneq (\text{LT}(I))$.

Proposition 1.62

Soit $I \subset R$ un idéal. Alors il existe P_1, \dots, P_r dans I tels que $(\text{LT}(I)) = (\text{LT}(P_1), \dots, \text{LT}(P_r))$.

Preuve : L'idéal $(\text{LT}(I))$ est monomial engendré par la famille $\{\text{LT}(P) \mid P \in I\}$. Le lemme de Dickson nous donne le résultat. \square

Théorème 1.63 (Théorème de la base de Hilbert)

Tout idéal $I \subset R$ est de type fini.

Preuve : On peut supposer $I \neq (0)$. On écrit alors $(\text{LT}(I)) = (\text{LT}(P_1), \dots, \text{LT}(P_r))$ avec $P_1, \dots, P_r \in I$. Nous suffit de montrer que l'on a l'égalité : $I = (P_1, \dots, P_r)$.

L'inclusion $(P_1, \dots, P_r) \subset I$ est claire. Soit donc $P \in I$. En utilisant l'algorithme de division, on écrit

$$P = P_1Q_1 + \dots + P_rQ_r + S.$$

Si $S = 0$, on a terminé. Supposons donc $S \neq 0$. On a alors par construction que pour tout $i \in [1, r]$, le polynôme $\text{LT}(P_i)$ ne divise aucun monôme de S . Mais on a $S = P - Q_1P_1 - \dots - Q_rP_r \in I$. En particulier $\text{LT}(S) \in (\text{LT}(I)) = (\text{LT}(P_1), \dots, \text{LT}(P_r))$ et donc l'un des $\text{LT}(P_i)$ divise $\text{LT}(S)$. Une contradiction. \square

On en déduit le corollaire habituel qui affirme que R est noethérien.

Corollaire 1.64

Toute suite croissante d'idéaux de R est stationnaire.

Preuve : Soit $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$ une suite croissante d'idéaux. On voit alors que $I = \cup_n I_n$ est un idéal. Il existe donc $P_1, \dots, P_r \in I$ tels que $I = (P_1, \dots, P_r)$. Pour chaque i , il existe n_i tel que $P_i \in I_{n_i}$. Soit $N = \max\{n_i \mid i \in [1, r]\}$. On a alors $I = (P_1 \dots P_r) \subset I_N \subset I$ et donc $I = I_N$. La suite est stationnaire. \square

Exercice 1.65

Soit $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$ une suite croissante d'idéaux, montrer que la réunion $I = \cup_n I_n$ est un idéal.

Bases de Gröbner

Définition

La base construite dans la preuve précédente du théorème de Hilbert a des propriétés très spéciales. On fixe toujours un ordre admissible $<$.

Définition 1.66

Soit $I \subset R$ un idéal. Un sous-ensemble fini $\{P_1, \dots, P_r\}$ de I est appelé **base de Gröbner** de I si on a

$$(\text{LT}(I)) = (\text{LT}(P_1), \dots, \text{LT}(P_r)).$$

Exemple 1.67

Soit $I \subset R$ un idéal.

1. L'exemple 1.61.2 avec $I = (P_1, P_2)$ mais $(\text{LT}(P_1), \text{LT}(P_2)) \subsetneq (\text{LT}(I))$ où $P_1 = x_1^3 - 2x_1x_2$ et $P_2 = x_1^2x_2 - 2x_2^2 + x_1$, montre que tout sous-ensemble générateur de I n'est pas nécessairement une base de Gröbner de I .

2. Soit $n = 3$, $\mathbb{k} = \mathbb{R}$ et $I = (x_1 + x_3, x_2 - x_3)$. Nous allons montrer que $(x_1 + x_3, x_2 - x_3)$ est une base de Gröbner de I pour l'ordre lexicographique.

Nous devons donc montrer l'égalité $(\text{LT}(I)) = (\text{LT}(x_1 + x_3), \text{LT}(x_2 - x_3)) = (x_1, x_2)$. On a toujours l'inclusion $(x_1, x_2) \subset (\text{LT}(I))$.

Soit donc $P \in I$ non nul. Il existe $P_1, P_2 \in R$ tels que $P = (x_1 + x_3)P_1 + (x_2 - x_3)P_2$. Si le monôme $\text{LM}(P) = x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}$ n'est pas dans l'idéal (x_1, x_2) , alors $\text{LM}(P) = x_3^{\alpha_3}$. Mais alors par définition de l'ordre lexicographique, on a $P \in \mathbb{k}[x_3]$. Mais P s'annule sur les points $(t, -t, t)$ pour tout $t \in \mathbb{R}$. Comme P est un polynôme en la seule variable x_3 qui s'annule pour tous les réels, P doit être le polynôme nul. Une contradiction.

Typesetting math: 54%

Proposition 1.68

Tout idéal $I \subset R$ admet une base de Gröbner et pour toute base de Gröbner (P_1, \dots, P_r) , on a $I = (P_1, \dots, P_r)$.

Preuve : L'existence d'une base de Gröbner est donnée par la Proposition 1.62 : on choisit $P_1, \dots, P_r \in I$ tels que $(LT(I)) = (LT(P_1), \dots, LT(P_r))$. La preuve du théorème de Hilbert nous donne une preuve de la dernière assertion car on a alors aussi $I = (P_1, \dots, P_r)$. \square

Nous allons maintenant étudier les propriétés des bases de Gröbner plus en détails. Nous verrons ainsi qu'elles peuvent être utilisées pour bien plus qu'une simple preuve du théorème de Hilbert. Nous donnerons également des algorithmes pour construire des bases de Gröbner.

Nous commençons par montrer que les bases de Gröbner sont bien adaptées à l'algorithme de division.

Proposition 1.69

Soit $G = (P_1, \dots, P_r)$ une base de Gröbner pour un idéal $I \subset R$ et soit $P \in R$ un polynôme. Alors il existe un unique polynôme S tel que

1. il existe $Q \in I$ tel que $P = Q + S$;
2. $S = 0$ ou S est une combinaison linéaire de monômes dont aucun n'est divisible par $LT(P_1), \dots, LT(P_r)$.

En particulier, le reste de la division de P par G est indépendant de l'ordre de la base.

Preuve : L'algorithme de division nous donne des polynômes Q_1, \dots, Q_r, S tels que $P = Q_1 P_1 + \dots + Q_r P_r + S$ et tels que S vérifie la condition 2. ci-dessus. En posant $Q = Q_1 P_1 + \dots + Q_r P_r$, on a la condition 1. et l'existence.

Montrons maintenant l'unicité. Soient donc $P = Q + S = Q' + S'$ deux décompositions vérifiant les conditions 1; et 2. ci-dessus. On a $S - S' = Q' - Q \in I$. Si $S \neq S'$ alors $S - S' \neq 0$ et $LT(S - S') \in LT(I) = (LT(P_1), \dots, LT(P_r))$. Il existe donc un indice i tel que $LT(P_i)$ divise $LT(S - S')$. C'est impossible car aucun monôme de S ni de S' n'est divisible par $LT(P_i)$. On a donc $S = S'$ et $Q = Q'$.

De la dernière assertion découle directement de l'unicité de S . \square

On en déduit un critère effectif (au moins si on a une base de Gröbner) d'appartenance à un idéal.

Corollaire 1.70

Si G est une base de Gröbner de I et $P \in R$. Alors $P \in I$ si et seulement si le reste $\overline{\{P\}^G}$ de la division de P par G est nul.

Exercice 1.71

Soit $G = (P_1, \dots, P_r)$ et $I = (P_1, \dots, P_r)$.

On a montré au corollaire précédent que si G est une base de Gröbner d'un idéal I , alors on a l'équivalence $P \in I$ si et seulement si $\overline{\{P\}^G} = 0$.

Montrer que la réciproque est vraie, à savoir que si pour tout polynôme $P \in R$ on a l'équivalence $P \in I$ si et seulement si $\overline{\{P\}^G} = 0$, alors G est une base de Gröbner de I .

Critère de Buchberger

L'exemple 1.67.2 montre qu'il n'est pas simple en général de prouver qu'une famille d'éléments est une base de Gröbner. Nous allons introduire dans ce paragraphe une méthode pour décider si une famille est une base de Gröbner.

Pour ce faire, on introduit une nouvelle opération sur les polynômes.

Définition 1.72

Soient $P, Q \in R$ des polynômes non nuls. Soit $LT(P) = a x^{\alpha}$ et $LT(Q) = b x^{\beta}$.

1. Le plus petit commun multiple de $LT(P)$ et $LT(Q)$ est le monôme x^{γ} avec $\gamma = (\gamma_1, \dots, \gamma_n)$ défini par $\gamma_i = \max(\alpha_i, \beta_i)$ pour tout $i \in [1, n]$.

2. Le **S-polynôme** $S(P, Q)$ de P et Q est défini par

$$S(P, Q) = (x^{\gamma} / LT(P))P - (x^{\gamma} / LT(Q))Q.$$

Remarque 1.73

Le principe du S-polynôme est de produire à partir d'une combinaison linéaire de P et Q un polynôme où l'on a éliminé les termes dominants de P et Q et donc avec un "nouveau terme dominant".

Exemple 1.74

Reprenons l'idéal de l'exemple 1.61.2. On a $I = (P_1, P_2)$ avec $P_1 = x_1^3 - 2x_1x_2$ et $P_2 = x_1^2x_2 - 2x_2^2 + x_1$ et on prend l'ordre lexicographique. On a alors pour plus petit commun multiple $x^{\gamma} = x_1^3x_2$ et

$$S(P_1, P_2) = x_2 P_1 - x_1 P_2 = x_2(x_1^3 - 2x_1x_2) - x_1(x_1^2x_2 - 2x_2^2 + x_1) = -x_1^2.$$

C'est en utilisant l'opposé de cet élément qu'on a montré que (P_1, P_2) n'est pas une base de Gröbner de I car on a $x_1^2 \in I$, en particulier $x_1^2 = LT(x_1^2) \in LT(I)$ mais $x_1^2 \notin \overline{\{P_1, P_2\}}$.

Remarque 1.75

On a toujours $S(P, Q) \in (P, Q)$ et $\overline{\{S(P, Q)\}} \subseteq \overline{\{(P, Q)\}} \in (P, Q)$. Cette opération permet donc de construire de nouveaux éléments de l'idéal avec de nouveaux termes dominants ce qui permettra de compléter la famille en une base de Gröbner.

Exemple 1.76

$S(P_1, P_2) <$ l'ordre lexicographique.

1. Soient $P = x_1^5x_2 + x_1^2 + 1$ et $Q = 2x_1^3x_2^2 + x_1x_2$. On a $x^\gamma = x_1^5x_2^2$ et

$$S(P,Q) = x_2P - 1/2 x_1^2Q = x_1^2x_2 + x_2 - 1/2 x_1^3x_2.$$

2. Soient $P = x_1^3x_2 - 2x_1^2x_2^2 + x$ et $Q = 3x_1^4 - x_2$. On a $x^\gamma = x_1^4x_2$ et

$$S(P,Q) = x_1P - 1/3 x_2Q = -2x_1^3x_2^2 + x_1^2 + 1/3 x_2^2.$$

On en déduit

$$\overline{S(P,Q)}^{\{P,Q\}} = -4x_1^2x_2^3 + x_1^2 + 2x_1x_2 + 1/3 x_2^2.$$

En particulier $\text{LT}(\overline{S(P,Q)}^{\{P,Q\}}) = 4x_1^2x_2^3$ n'est pas divisible par $\text{LT}(P)$ ni par $\text{LT}(Q)$. Donc $\text{LT}(\overline{S(P,Q)}^{\{P,Q\}})$ n'est pas divisible par $\text{LT}(P)$ ni par $\text{LT}(Q)$.

Lemme 1.77

Soit $P = c_1P_1 + \dots + c_rP_r$ avec $c_i \in \mathbb{k}$ et $P_i \in R$ tels que $\text{mdeg}(P_i) = \gamma$ pour tout $i \in [1,r]$.

Si $\text{mdeg}(P) < \gamma$, alors P est une combinaison linéaire à coefficients dans \mathbb{k} des S -polynômes $(S(P_i, P_j))_{i,j \in [1,r]}$ et on a $S(P_i, P_j) = 0$ ou $\text{mdeg}(S(P_i, P_j)) < \gamma$ pour tout $i,j \in [1,r]$.

Preuve : Soit $d_i = \text{LC}(P_i)$ le coefficient dominant de P_i de telle sorte que l'on a $\text{LT}(P_i) = d_i x^\beta$ pour tout $i \in [1,r]$. Remarquons que par hypothèse on a $\sum_i c_i d_i = 0$.

On commence par calculer $S(P_i, P_j)$. Le plus grand commun multiple des termes dominants est $x^\gamma = x^\beta$ et on obtient

$$S(P_i, P_j) = (x^\beta \text{LT}(P_i))P_j - (x^\beta \text{LT}(P_j))P_i = P_i/d_i - P_j/d_j.$$

On pose $Q_i = P_i/d_i$ de telle sorte que $\text{LC}(Q_i) = 1$, $\text{LT}(Q_i) = x^\beta$, $P = \sum_i c_i d_i Q_i$ et $S(P_i, P_j) = Q_i - Q_j$. On écrit

$$\begin{aligned} P &= c_1d_1(Q_1-Q_2) + \dots + (c_1d_1+c_2d_2)(Q_2-Q_3) + \dots + c_r d_r(Q_r-Q_1) \\ &\quad + (c_1d_1 + \dots + c_{r-1}d_{r-1})(Q_{r-1}-Q_r) + \dots + (c_1d_1 + \dots + c_{r-1}d_{r-1})Q_r. \end{aligned}$$

Le dernier terme s'annule et $Q_i - Q_{i+1} = S(P_i, P_{i+1})$. On obtient donc

$$P = c_1d_1 S(P_1, P_2) + \dots + c_r d_r S(P_r, P_1).$$

Le résultat en découle. Pour montrer la dernière assertion, il suffit de remarquer que $\text{LT}(Q_i) = x^\beta = \text{LT}(Q_j)$ donc si $S(P_i, P_j) = Q_i - Q_j$ est non nul, son terme dominant est strictement inférieur à x^β . □

Nous pouvons maintenant donner un critère pour qu'une famille de polynômes forme une base de Gröbner.

Théorème 1.78 (Critère de Buchberger)

Soit $I = (P_1, \dots, P_r)$ un idéal. Alors $G = \{P_1, \dots, P_r\}$ est une base de Gröbner pour I si et seulement si $\overline{S(P_i, P_j)}^G = 0$ pour toute paire (i,j) d'éléments de $[1,r]$ avec $i \neq j$.

Preuve : Si G est une base de Gröbner alors $S(P_i, P_j) \in (P_i, P_j) \setminus I$ et $\overline{S(P_i, P_j)}^G = 0$.

Réciproquement, on suppose que l'on a $\overline{S(P_i, P_j)}^G = 0$ pour toute paire (i,j) d'éléments de $[1,r]$ avec $i \neq j$. Soit $P \in I$ non nul, on veut montrer $\text{LT}(P) \in (\text{LT}(P_1), \dots, \text{LT}(P_r))$. Comme $P \in I$, on peut écrire

$$P = P_1Q_1 + \dots + P_rQ_r$$

avec $Q_i \in R$. On pose $m_i = \text{mdeg}(P_iQ_i)$ et $\beta = \max\{\text{mdeg}(P_iQ_i) \mid i \in [1,r]\}$. D'après le Lemme 1.44, on a $\text{mdeg}(P) \leq \beta$.

On considère maintenant toutes les écritures $P = P_1Q_1 + \dots + P_rQ_r$ possibles et pour chacune de ces écritures le multi-degré $\beta = \max\{\text{mdeg}(P_iQ_i) \mid i \in [1,r]\}$. Comme l'ordre $<$ est admissible, l'ensemble de ces multi-degrés a un minimum et on choisit Q_1, \dots, Q_r pour lesquels ce minimum est atteint. On cherche à montrer que $\text{mdeg}(P) = \beta$.

En effet, si $\text{mdeg}(P) = \beta$, il existe alors $i \in [1,r]$ tel que $\text{mdeg}(f) = \text{mdeg}(P_iQ_i)$ donc $\text{LT}(P) = \text{LT}(P_iQ_i)$ et $\text{LT}(P_i)$ divise $\text{LT}(P)$ ce qui impose $\text{LT}(P) \in (\text{LT}(P_1), \dots, \text{LT}(P_r))$.

Il reste à montrer que la condition de minimalité impose $\text{mdeg}(P) = \beta$. Par l'absurde, supposons que l'on a $\text{mdeg}(P) < \beta$. On sépare alors les termes de degré β dans l'écriture ci-dessus :

$$\begin{aligned} P &= \sum_i m_i = \beta P_i Q_i + \sum_i m_i = \beta P_i Q_i \quad \&= \sum_i m_i = \beta P_i \text{LT}(Q_i) + \sum_i m_i = \beta P_i (Q_i - \text{LT}(Q_i)) + \sum_i m_i = \beta P_i Q_i. \end{aligned}$$

Les monômes qui apparaissent dans les deux dernières sommes sont de multi-degré strictement inférieur à β ce qui signifie que la première somme est de multi-degré strictement inférieur à β . Pour les indices i tels que $m_i = \beta$, on écrit, $\text{LT}(Q_i) = c_i x^{\{a_i\}}$. La somme

$$\sum_i m_i = \beta P_i \text{LT}(Q_i) = \sum_i m_i = \beta c_i (x^{\{a_i\}} P_i)$$

satisfait alors les hypothèses du Lemme 1.77 et il existe des scalaires $c_{\{j,k\}}$ tels que

$$\sum_i m_i = \beta P_i \text{LT}(Q_i) = \sum_i m_i, m_k = \beta c_{\{j,k\}} S(x^{\{a_j\}} P_j, x^{\{a_k\}} P_k).$$

On calcule maintenant les S -polynômes ci-dessus. On a $\text{LM}(x^{\{a_j\}} P_j) = x^\beta$ pour tout j tel que $m_j = \beta$. On en déduit

$$\begin{aligned} S(x^{\{a_j\}} P_j, x^{\{a_k\}} P_k) &= \frac{x^\beta}{x^{\{a_j\}} P_j} - \frac{x^\beta}{x^{\{a_k\}} P_k} \\ &= x^{\{a_j\}} P_k - x^{\{a_k\}} P_j. \end{aligned}$$

avec $\beta_{\{j,k\}} = \max(\text{mdeg}(P_j), \text{mdeg}(P_k))$. Il est à noter que comme $x^{\{a_j\}} P_j$ et $x^{\{a_k\}} P_k$ ont le même multi-degré (égal à β), on a $\text{mdeg}(S(x^{\{a_j\}} P_j, x^{\{a_k\}} P_k)) < \beta$ et donc $\text{mdeg}(S(P_i, P_j)) < \beta$. On obtient donc

$$\sum_i m_i = \beta P_i \text{LT}(Q_i) = \sum_i m_i, m_k = \beta c_{\{j,k\}} x^{\{\beta - \beta_{\{j,k\}}\}} S(P_j, P_k).$$

Nous utilisons maintenant notre hypothèse, à savoir $\overline{S(P_j, P_k)}^G = 0$. Ceci impose en particulier, en utilisant l'algorithme de

Typesetting math: 54% $\overline{S(P_j, P_k)}$ en R tels que

$S(P_j, P_k) = \sum_{\ell} S_{j,k,\ell} P_\ell$,

avec $\deg(S_{j,k,\ell}) \leq \deg(S(P_j, P_k)) < \beta_{j,k}$. On obtient donc

$P = \sum_{m,j,m,k} \beta_{j,k} \sum_{\ell} c_{j,k,\ell} x^{\beta_j - \beta_{j,k}} S_{j,k,\ell} P_\ell + \sum_{m,i} \beta_i P_i (Q_i - \text{LT}(Q_i)) + \sum_{m,i} \beta_i P_i Q_i$.

Chaque facteur de la première somme a un multi-degré strictement inférieur à $\beta_j - \beta_{j,k} + \beta_{j,k} = \beta_j$ et la chose est vraie des facteurs des deux dernières sommes. On a donc obtenu une nouvelle écriture de P avec des facteurs de degré strictement inférieurs à β_j ce qui contredit la minimalité de β_j . \square

Exemple 1.79

Reprenons l'Exemple 1.67.2. Soit $R = \mathbb{k}[x_1, \dots, x_n]$ avec $n = 3$ et $\mathbb{k} = \mathbb{R}$. Soit $I = (x_1 + x_3, x_2 - x_3)$, soit $P_1 = x_1 + x_3$, soit $P_2 = x_2 - x_3$ et soit $G = \{P_1, P_2\}$. Montrons que G est une base de Gröbner de I pour l'ordre lexicographique. Pour celà il suffit de montrer que $\overline{S(P_1, P_2)}^G = 0$. Or on a

$$S(P_1, P_2) = \frac{x_1 x_2}{x_1} P_1 - \frac{x_1 x_2}{x_2} P_2 = x_2 x_3 + x_1 x_3.$$

L'algorithme de division donne

$$S(P_1, P_2) = x_3(x_1 + x_3) + x_3(x_2 - x_3) = x_3 P_1 + x_3 P_2$$

et donc $\overline{S(P_1, P_2)}^G = 0$.

Exemple 1.80

Autre exemple, soit $I = (x_2 - x_1^2, x_3 - x_1^3)$ et montrons que $G = \{x_2 - x_1^2, x_3 - x_1^3\}$ est une base de Gröbner de I pour l'ordre lexicographique avec $x_2 > x_3 > x_1$. Calculons

$$S(x_2 - x_1^2, x_3 - x_1^3) = \frac{x_2 x_3}{x_2} (x_2 - x_1^2) - \frac{x_2 x_3}{x_3} (x_3 - x_1^3) = x_1^3 x_2 - x_1^2 x_3.$$

L'algorithme de division donne

$$S(x_2 - x_1^2, x_3 - x_1^3) = x_1^3 x_2 - x_1^2 x_3 = x_1^3 (x_2 - x_1^2) - x_1^2 (x_3 - x_1^3)$$

et donc $\overline{S(x_2 - x_1^2, x_3 - x_1^3)}^G = 0$.

Exercice 1.81

On a vu que aux Exemples 1.67.2. et 1.79 que $(x_1 + x_3, x_2 - x_3)$ est une base de Gröbner de $\mathbb{k}[x_1, x_2, x_3]$ pour l'ordre lexicographique. Dans cet exercice on se propose de vérifier que le reste de la division polynomiale ne dépend pas de l'ordre des éléments d'une base de Gröbner.

1. Effectuer la division de $x_1 x_2$ par $(x_1 + x_3, x_2 - x_3)$.

2. Effectuer la division de $x_1 x_2$ par $(x_2 - x_3, x_1 + x_3)$.

3. Comparer les restes et les quotients et remarquer que le reste ne dépend pas de l'ordre mais que les quotients en dépendent.

Exercice 1.82

Soit $I \subset R$ un idéal et G une base de Gröbner de I .

1. Montrer que $\overline{P}^G = \overline{Q}^G$ si et seulement si $P - Q \in I$.

2. Montrer que $\overline{P+Q}^G = \overline{P}^G + \overline{Q}^G$ et $\overline{PQ}^G = \overline{\overline{P}^G \overline{Q}^G}$.

Algorithme de Buchberger

Dans cette section, on se propose de construire de manière effective des bases de Gröbner d'un idéal. Le principe est de satisfaire le critère de Buchberger et donc d'ajouter aux générateurs de l'idéal autant de S-polynômes que nécessaire.

Théorème 1.83

Soit $I = (P_1, \dots, P_r)$ un idéal non nul de R . L'algorithme suivant détermine une base de Gröbner pour I en un nombre fini d'opérations.

Algorithme 1.84

Entrée : $F = \{P_1, \dots, P_r\}$.

Sortie : Une base de Gröbner G de I avec $F \subset G$.

$G := F$

Faire :

$G' := G$

Pour toute paire $P \neq Q$ de G' , faire :

$S := \overline{S(P, Q)}^G$.

Si $S \neq 0$ faire $G := G \cup \{S\}$.

Tant que $G' \neq G$.

Donner G .

Preuve 1.85

À chaque étape, l'ensemble G augmente et au départ $G = F$ donc on a toujours $F \subset G$. Montrons que $G \subset I$. C'est clair au départ puisqu'on a $G = F \subset I$. Par ailleurs, à chaque étape, on ajoute à G des éléments de la forme $S = \overline{S(P, Q)}^G$ avec $P, Q \in I$ et $G' \subset I$. On a donc $S = S(P, Q) - \sum_i Q_i S_i$ avec $S_i \in I$ et $S(P, Q) \subset (P, Q) \subset I$ ce qui prouve $S \in I$ et donc $G \subset I$. On voit donc que G est une famille génératrice de l'idéal I .

Typesetting math: 54%

Lorsque l'algorithme s'arrête, on a $G = G'$ et donc tous les restes $S = \overline{\{S(P,Q)\}^G}$ des S -polynômes formés à partir d'éléments de G et obtenue après division par G sont soit nuls soit déjà dans G . Mais si les sont dans G , le reste doit être nul donc dans tous les cas $S = 0$ et G est une base de Gröbner d'après le critère de Buchberger.

Il nous reste à montrer que l'algorithme s'arrête. Pour cela, notons $G = (G_1, \dots, G_s)$ et $(\text{LT}(G)) = (\text{LT}(G_1), \dots, \text{LT}(G_s))$. On considère l'évolution de cet idéal. À chaque étape, comme G est obtenu à partir de G' (l'ensemble G à l'étape précédente) en y ajoutant des éléments, on a toujours $(\text{LT}(G')) \subsetneq (\text{LT}(G))$. Montrons que si $G' \subsetneq G$ alors $(\text{LT}(G')) \subsetneq (\text{LT}(G))$. En effet, si G a un nouvel élément, il est de la forme $S = \overline{\{S(P,Q)\}^G}$ avec $P, Q \in G'$. En particulier par l'algorithme de division $\text{LT}(S)$ n'est divisible par aucun des termes dominants des éléments de G' . On a donc $\text{LT}(S) \notin (\text{LT}(G'))$ mais $\text{LT}(S) \in (\text{LT}(G))$. Au cours de l'algorithme, on produit donc une suite strictement croissante d'idéaux, les $(\text{LT}(G))$. Cette suite ne peut être infinie car R est noethérien donc l'algorithme s'arrête.

Remarque 1.86

Cet algorithme n'est pas optimal. Par exemple, une fois qu'un reste $S = \overline{\{S(P,Q)\}^G}$ est nul, il reste nul tout au long de l'algorithme et il n'est pas utile de le recalculer.

Exemple 1.87

On se place dans $\text{kk}[x_1, x_2]$ avec l'ordre lexicographique gradué. Soient $P_1 = x_1^3 - 2x_1x_2$, $P_2 = x_1^2x_2 - 2x_2^2 + x_1$ et $I = (P_1, P_2)$. Testons tout d'abord si $\{P_1, P_2\}$ est une base de gröbner de I . On a

$$S(P_1, P_2) = x_2P_1 - x_1P_2 = -x_1^2 \text{ et } \overline{\{S(P_1, P_2)\}} = -x_1^2.$$

Ainsi $\{P_1, P_2\}$ n'est pas une base de Gröbner. On applique l'algorithme de Buchberger. A la première étape, on ajoute $P_3 = \overline{\{S(P_1, P_2)\}} = -x_1^2$. On recalcule les S -polynômes (sachant qu'on a pas besoin de recalculer $S(P_1, P_2)$ dont on a déjà ajouté le reste). On a $S(P_1, P_3) = P_1 + x_1P_3 = -2x_1x_2$ et $S(P_2, P_3) = P_2 + x_2P_3 = -2x_2^2 + x_1$. On obtient

$$\overline{\{S(P_1, P_3)\}} = -2x_1x_2 \text{ et } \overline{\{S(P_2, P_3)\}} = -2x_2^2 + x_1.$$

Donc $\{P_1, P_2, P_3\}$ n'est pas une base de Gröbner. On continue et on pose $P_4 = -2x_1x_2$ et $P_5 = -2x_2^2 + x_1$. On a

- $S(P_1, P_4) = x_2P_1 + 1/2x_1^2P_4 = -2x_1x_2$,
- $S(P_1, P_5) = x_2^2P_1 + 1/2x_1^3P_5 = -2x_1x_2^2 + x_1^4$,
- $S(P_2, P_4) = P_2 + 1/2x_2P_4 = -2x_2^2 + x_1$,
- $S(P_2, P_5) = x_2P_2 + 1/2x_1^2P_5 = 1/2x_1^3 - 2x_2^3 + x_1x_2$,
- $S(P_3, P_4) = -x_2P_3 + 1/2x_1P_4 = 0$,
- $S(P_3, P_5) = -x_2^2P_3 + 1/2x_1^2P_5 = 1/2x_1^3$ et
- $S(P_4, P_5) = -1/2x_2P_4 + 1/2x_1P_5 = 1/2x_1^2$.

On vérifie que

$$\overline{\{S(P_i, P_j)\}} = 0$$

pour tout $i, j \in [1, 5]$. Donc $\{P_1, P_2, P_3, P_4, P_5\}$ est une base de Gröbner de I .

Remarque 1.88

On a maintenant une méthode effective pour tester l'appartenance à un idéal, le problème $P \in I$. En effet, on commence par construire une base finie de I . Puis une base de Gröbner G de I et enfin on calcule $\overline{\{P\}}^G$. On a $(P \in I \Leftrightarrow \overline{\{P\}}^G = 0)$.

Exemple 1.89

Soit $I = (P_1, P_2)$ avec $P_1 = x_1x_3 - x_2^2$ et $P_2 = x_1^3 - x_3^2$. On se demande si $P = x_1x_2 - 5x_3^2 + x_1$ est dans I .

On choisit pour ordre < l'ordre lexicographique gradué. On commence par déterminer une base de Gröbner G . On obtient $G = \{x_1x_3 - x_2^2, x_1^3 - x_3^2, x_1^2x_2^2 - x_3^3, x_1x_2^4 - x_3^4, x_2^6 - x_3^5\}$. On constate alors que $\text{LT}(P) \notin (\text{LT}(Q) \vee Q \in G)$. Donc $P \notin \overline{\{P\}}^G$.

Bases de Gröbner réduites

L'algorithme de Buchberger produit des bases de Gröbner qui peuvent être de très grande taille. Nous allons maintenant expliquer comment obtenir des bases de Gröbner "minimales".

On commence par le lemme suivant.

Lemme 1.90

Soit G une base de Gröbner d'un idéal I . Soit $P \in G$ tel que $\text{LT}(P) \in (\text{LT}(Q) \vee Q \in G \setminus \{P\})$. Alors $G \setminus \{P\}$ est encore une base de Gröbner de I .

Preuve : Il faut vérifier que $(\text{LT}(I)) = (\text{LT}(Q) \vee Q \in G \setminus \{P\})$. Mais on sait que $(\text{LT}(I)) = (\text{LT}(Q) \vee Q \in G)$. Comme $\text{LT}(P) \in (\text{LT}(Q) \vee Q \in G \setminus \{P\})$, on a $(\text{LT}(Q) \vee Q \in G \setminus \{P\}) = (\text{LT}(Q) \vee Q \in G) = (\text{LT}(I))$. □

Ce qui conduit naturellement à la définition suivante.

Définition 1.91

Une base de Gröbner G d'un idéal I est dite **minimale** si les conditions suivantes sont satisfaites:

1. Pour tout $P \in G$, on a $\text{LC}(P) = 1$.
2. Pour tout $P \in G$, on a $\text{LT}(P) \notin (\text{LT}(Q) \vee Q \in G \setminus \{P\})$.

Pour les bases de Gröbner minimales, on a unicité de l'ensemble des monômes dominants de la base.

J Typesetting math: 54%

Soient G et G' deux bases de Gröbner minimales d'un idéal I . Alors on a

$$\{\text{LT}(Q) \setminus \text{vert } Q \in G\} = \{\text{LT}(Q') \setminus \text{vert } Q' \in G'\}.$$

Preuve : Par définition des bases de Gröbner, on a

$$(\{\text{LT}(Q) \setminus \text{vert } Q \in G\}) = (\text{LT}(I)) = (\{\text{LT}(Q') \setminus \text{vert } Q' \in G'\}).$$

En particulier, pour tout $Q \in G$, il existe $Q' \in G'$ tel que $\text{LT}(Q')$ divise $\text{LT}(Q)$. De même pour ce Q' , il existe $Q'' \in G$ tel que $\text{LT}(Q'')$ divise $\text{LT}(Q')$. On en déduit que $\text{LT}(Q'')$ divise $\text{LT}(Q)$. Si on avait $Q \neq Q''$, alors $\text{LT}(Q) \in (\text{LT}(P) \setminus \text{vert } P \in G \setminus \{Q\})$, une contradiction à la minimalité. Ainsi $Q = Q''$ et donc $\text{LT}(Q)$ et $\text{LT}(Q')$ ne diffèrent que d'un scalaire. Comme $\text{LC}(Q) = 1 = \text{LC}(Q')$, on a déduit $\text{LT}(Q) = \text{LT}(Q')$. Ainsi on a montré $\{\text{LT}(Q) \setminus \text{vert } Q \in G\} \subset \{\text{LT}(Q') \setminus \text{vert } Q' \in G'\}$. Par symétrie, on a l'inclusion inverse et le résultat. \square

Cependant on a base unicité de la base minimale comme le montre l'exemple suivant.

Exemple 1.93

Reprenons l'Exemple 1.87. On a

$$(\text{LT}(I)) = (\text{LT}(P_1), \text{LT}(P_2), \text{LT}(P_3), \text{LT}(P_4), \text{LT}(P_5)) = (x_1^3, x_1^2 x_2, -x_1^2, -2x_1 x_2, -2x_2^2).$$

En remplaçant P_3, P_4 et P_5 par $-P_3, -1/2 P_4$ et $-1/2 P_5$ on obtient une base avec coefficients dominants égaux à 1. On a donc $(\text{LT}(I)) = (x_1^3, x_1^2 x_2, x_1^2, x_1 x_2, x_2^2)$. On voit alors que les deux premiers monômes sont engendrés par les autres. On peut donc supprimer P_1 et P_2 pour obtenir une base de Gröbner minimale de I :

$$(-P_3, -1/2 P_4, -1/2 P_5) = (x_1^2, x_1 x_2, x_2^2 - 1/2 x_1).$$

Remarquons qu'on obtient d'autres bases minimales en prenant

$$(x_1^2 + a x_1 x_2, x_1 x_2, x_2^2 - 1/2 x_1)$$

pour tout $a \in \mathbb{k}$. On a donc pas unicité des bases minimales.

Pour remédier à ce problème, on a besoin de conditions un peu plus fortes.

Définition 1.94

Une base de Gröbner G d'un idéal I est dite **réduite** si les conditions suivantes sont satisfaites:

1. Pour tout $P \in G$, on a $\text{LC}(P) = 1$.
2. Pour tout $P \in G$, aucun monôme de P n'est dans $(\text{LT}(Q) \setminus \text{vert } Q \in G \setminus \{P\})$.

Exemple 1.95

Reprenons les Exemples 1.87 et 1.93. Rappelons que l'ordre est l'ordre lexicographique gradué. Parmis les bases minimales

$$(x_1^2 + a x_1 x_2, x_1 x_2, x_2^2 - 1/2 x_1)$$

pour tout $a \in \mathbb{k}$, on voit que seule la base $(x_1^2, x_1 x_2, x_2^2 - 1/2 x_1)$ est réduite.

Remarque 1.96

Une base réduite est minimale.

Proposition 1.97

Soient $<$ un ordre admissible et I un idéal non nul de R . Alors I admet une unique base de Gröbner réduite.

Preuve : Soit G une base de Gröbner minimale et soit $P \in G$. On dira que P est réduit pour G s'il satisfait la seconde condition des bases réduites à savoir qu'aucun monôme de P n'est dans l'idéal $(\text{LT}(Q) \setminus \text{vert } Q \in G \setminus \{P\})$.

On va modifier chaque élément de G pour le rendre réduit. On remarque tout d'abord que le Lemme 1.92 impose qu'un élément $P \in G$ est réduit pour G si et seulement si il est réduit pour tout base minimale G' de I le contenant. En effet, le Lemme 1.92 nous dit que l'ensemble des termes dominants des bases réduites est toujours le même ainsi la condition d'être réduit est identique dans G ou G' . L'avantage de cette remarque est de pouvoir modifier un élément d'une base minimale tout en préservant le caractère réduit d'autres monômes de cette base.

Prenons $P \in G$. S'il est réduit, il n'y a rien à faire. Sinon, on pose $P' = \overline{P} \setminus \{G \setminus \{P\}\}$ et $G' = (G \setminus \{P\}) \cup \{P'\}$.

Montrons tout d'abord que G' est aussi une de Gröbner base minimale. Comme $P' \in I$, on a $G' \subset I$. Par ailleurs, on a $\text{LT}(P) \not\in (\{\text{LT}(Q) \setminus Q \in G \setminus \{P\}\})$. En particulier aucun terme dominant des polynômes de $G \setminus \{P\}$ ne divise $\text{LT}(P)$ ce qui impose que $\text{LT}(P)$ est un monôme de P' . On a donc $\text{LT}(P') = \text{LT}(P)$. En particulier $(\text{LT}(I)) = (\text{LT}(Q) \setminus \text{vert } Q \in G) = (\text{LT}(Q) \setminus \text{vert } Q \in G')$ et comme la condition de minimalité ne dépend que des termes dominants, on a que G' est bien une base de Gröbner minimale de I .

Montrons maintenant que P' est réduit pour G' . Ceci est imposé par définition et par la condition imposée sur le reste dans l'algorithme de division : aucun des monômes dominants d'éléments de $G \setminus \{P\} = G' \setminus \{P'\}$ ne divise les monômes de P' .

En procédant de cette manière avec chaque terme de G , on obtient une base déduite.

Il reste à montrer que cette base est unique. Soient donc G et G' deux bases de Gröbner réduites pour I . En particulier ces bases sont minimales donc le Lemme 1.92 impose

$$\{\text{LT}(Q) \setminus \text{vert } Q \in G\} = \{\text{LT}(Q) \setminus \text{vert } Q \in G'\}.$$

Pour tout $P \in G$, il existe donc $P' \in G'$ tel que $\text{LT}(P') = \text{LT}(P)$. On veut montrer que $P' = P$. On regarde $P - P' \in I$. On a donc $\overline{P - P'} \setminus \{G\} = 0$. Mais les termes dominants de P et P' s'annulent dans $P - P'$ donc $\overline{P - P'} \setminus \{G\} = \overline{P - P'} \setminus \{G \setminus \{P\}\}$. De plus aucun autre monôme de P ni de P' n'est divisible par un élément de $\{\text{LT}(Q) \setminus \text{vert } Q \in G \setminus \{P\}\} = \{\text{LT}(Q) \setminus \text{vert } Q \in G'\}$ Typesetting math: 54% ce qui impose que $\overline{P - P'} \setminus \{G\} = \overline{P - P'} \setminus \{G \setminus \{P\}\} = \overline{P - P'} \setminus \{G' \setminus \{P'\}\} = P - P'$. En particulier, on obtient $P' = P$.

□

Remarque 1.98

Les bases de Gröbner réduites nous donnent une méthode effective pour tester l'égalité entre idéaux, le problème $I = J$. En effet, on construit des bases de Gröbner réduites G et G' de I et J . On a alors ($I = J \Leftrightarrow G = G'$).

Au prochain chapitre, nous donnerons des applications des bases de Gröbner à des problèmes de type géométrique.

2. Géométrie

Polynômes et variétés affines

Dans ce chapitre, nous rappelons des définitions concernant les liens entre géométrie (algébrique affine) et polynômes.

La plupart de ces notions ont été vues en M1 ou dans le cours “courbes algébriques”. Nous passerons donc rapidement sur les preuves éventuelles.

Variétés affines

On fixe kk un corps et n un entier naturel. Rappelons que l'on pose $R = \text{kk}[x_1, \dots, x_n]$.

Définition 2.1

Soit $S \subset R$ un sous-ensemble. La **variété affine associée à S** est le sous-ensemble de kk^n défini par

$$V(S) = \{(a_1, \dots, a_n) \in \text{kk}^n \mid \forall P(a_1, \dots, a_n) = 0 \text{ pour tout } P \in S\}.$$

Un sous-ensemble V de kk^n est appelé **variété affine** s'il existe $S \subset R$ tel que $V = V(S)$.

Lorsque S est fini composé des éléments P_1, \dots, P_r , on écrira

$$V(S) = V(\{P_1, \dots, P_r\}) = V(P_1, \dots, P_r).$$

Exemple 2.2

Les ensembles suivants $V \subset \mathbb{R}^3$ sont des variétés affines

1. $V = V(x_1^2 + x_3^2 - 1)$ est un cylindre.
2. $V = V(x_1^2 + x_2^2 + (x_3 - 1)^2 - 4)$ est une sphère.
3. $V = V((x_1^2 + x_3^2 - 1)(x_1^2 + x_2^2 + (x_3 - 1)^2 - 4))$ est la réunion des deux précédents.
4. $V = V(x_1^2 + x_3^2 - 1, x_1^2 + x_2^2 + (x_3 - 1)^2 - 4)$ est l'intersection des deux précédents.

Par contre l'ensemble $\mathbb{R} \setminus \{0\}$ n'est pas une variété affine.

Lemme 2.3

Soit $S \subset R$ et I l'idéal de R engendré par S . Alors on a $V(S) = V(I)$.

Preuve : Exercice. □

Lemme 2.4

Soit V une variété affine, alors il existe un nombre fini de polynômes P_1, \dots, P_r tels que $V = V(P_1, \dots, P_r)$.

Preuve : C'est le théorème de Hilbert. □

Lemme 2.5

On a les résultats suivants.

1. L'intersection de variétés affines est encore une variété affine.
2. La réunion d'un nombre fini de variétés affines est encore une variété affine.
3. L'ensemble kk^n est une variété affine.
4. L'ensemble vide est une variété affine.
5. Un ensemble fini de points est une variété affine.

Preuve : Exercice. □

Les bases de Gröbner vont nous permettre de répondre aux questions :

1. La variété affine V est-elle vide ?
2. Si la variété affine V a un nombre fini de points, peut-on les décrire ?
3. Peut-on déterminer la “dimension” de la variété affine V ?
4. Peut-on déterminer si la variété affine V est régulière ou lisse ?
5. Peut-on déterminer le “lieu singulier” de la variété affine V ?

Exemple 2.6

Considérons dans \mathbb{C} le système d'équations polynomiales suivant:

$$\begin{cases} x_2^2 + x_3^2 = 1 \\ x_1^2 + x_3^2 = x_2 \\ x_1 = x_3 \end{cases}$$

On en cherche les solutions c'est-à-dire l'ensemble $V = V(S)$ avec $S = \{P_1, P_2, P_3\}$ où $P_1 = x_1^2 + x_2^2 + x_3^2 - 1$, $P_2 = x_1^2 + x_3^2 - x_2$ et $P_3 = x_1 - x_3$. On a $V(S) = V(I)$ avec $I = (P_1, P_2, P_3)$ l'idéal engendré par ces trois polynômes. Si on détermine une base de Gröbner G pour I pour l'ordre lexicographique, on obtient $G = \{Q_1, Q_2, Q_3\}$ avec $Q_1 = x_1 - x_3$, $Q_2 = -x_2 + x_3^2$ et $Q_3 = x_3^4 + (1/2)x_2^2 - 1/4$.

Il suffit donc de résoudre les systèmes $Q_1 = 0$, $Q_2 = 0$ et $Q_3 = 0$. On obtient pour la troisième équation

$$x_3 = \pm \sqrt{-1} \sqrt{5}$$

En injectant dans la seconde équation on trouve y et dans la première on obtient x . Le système a donc quatre solutions.

Idéaux des variétés affines

Définition 2.7

Soit V un sous-ensemble de \mathbb{k}^n (par nécessairement une variété affine). On définit l'**idéal de V** noté $I(V)$ par

$$I(V) = \{P \in \mathbb{k}[x_1, \dots, x_n] \mid \forall P(a_1, \dots, a_n) = 0 \text{ pour tout } (a_1, \dots, a_n) \in V\}.$$

Lemme 2.8

L'ensemble $I(V)$ est bien un idéal de $R = \mathbb{k}[x_1, \dots, x_n]$.

Preuve : Exercice. □

Lemme 2.9

Soit I un idéal de R . On a toujours $I \subset I(V(I))$.

Preuve : Exercice. □

Remarque 2.10

Si V est une variété affine de la forme $V = V(I)$, alors on a en général $I(V(I)) = I(V) \neq I$.

Exemple 2.11

Voici deux exemples symptomatiques pour lesquels on a $I(V(I)) \neq I$ avec une unique variable et le corps $\mathbb{k} = \mathbb{R}$ des nombres réels.

1. Si $I = (x_1^2)$, on a $V(I) = \{0\}$ et $I(V(I)) = (x_1)$.
2. Si $I = (x_1^2 + 1)$, on a $V(I) = \emptyset$ et $I(V(I)) = \mathbb{R}[x_1]$.

Dans le premier cas, la variété $V(I)$ ne "voit" pas les puissances. Dans le second cas, il "manque des points".

Le lien entre I et $I(V(I))$ est subtil et dépend du corps. Ainsi si on remplace \mathbb{R} par \mathbb{C} dans le second exemple, on obtient pour $I = (x_1^2 + 1)$ que $V(I) = \{\pm i\}$ et $I(V(I)) = I$.

Lemme 2.12

Soit V un sous-ensemble de \mathbb{k}^n .

1. On a $V \subset V(I(V))$.
2. Soit V une variété algébrique, on a toujours $V = V(I(V))$.

Preuve : Exercice. □

Lemme 2.13

Soient $V, W \subset \mathbb{k}^n$ des sous-ensembles et $I, J \subset R$ des idéaux.

1. On a $V \subset W \Rightarrow I(W) \subset I(V)$.
2. On a $I \subset J \Rightarrow V(J) \subset V(I)$.

Preuve : Exercice. □

Corollaire 2.14

Pour tout ensemble V et tout idéal I , on a $I(V) = I(V(I(V)))$ et $V(I) = V(I(V(I)))$.

Preuve : Exercice. □

