Bases de Gröbner

Axel Mauroy et Killian Le Milbeau

ENS Rennes

27/09/2023

Table des matières

Théorème de la base de Hilbert

Définition (Idéal des termes dominants)

Soit I un idéal de $k[x_1, ..., x_n]$, $I \neq \{0\}$, on note $LT(I)$ l'ensemble des termes dominants des éléments de I :

$$LT(I) = \left\{ LT(f) \;\middle|\; f \in I \backslash \{0\} \right\}$$

On note $\left\langle LT(I) \right\rangle$ l'idéal engendré par les éléments de $LT(I)$.

Supposons que $I = \left\langle f_1, ..., f_s \right\rangle$, pour tout $i \in [\![1 \; ; \; s]\!]$ on a

$$LT(f_i) \in LT(I) \subseteq \left\langle LT(I) \right\rangle$$

D'où,

$$\left\langle LT(f_1), ..., LT(f_s) \right\rangle \subseteq \left\langle LT(I) \right\rangle$$

Cette inclusion peut être stricte.

Théorème de la base de Hilbert

Exemple :

On prend l'ordre lexicographique sur les mônomes de $\mathbb{R}[x, y]$ avec $y < x$. Soient $I =< f_1, f_2 >$ l'idéal de $\mathbb{R}[x, y]$ engendré par les polynômes $f_1 = xy + 1$ et $f_2 = y^2 - 1$.
Considérons le polynôme

$$f = xy^2 - x$$

.

Théorème de la base de Hilbert

Proposition

Soit I un idéal non-nul de $k[x_1, \ldots, x_n]$, alors
(i) *L'idéal $\langle LT(I) \rangle$ est monomial;*
(ii) *Il existe des polynômes $g_1, \ldots, g_t \in I$, tels que*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$$

Théorème de la base de Hilbert

Théorème (de la base de Hilbert)

Tout idéal I de $k[x_1, ..., x_n]$ possède un nombre fini de générateur, c'est-à-dire qu'il existe des polynômes $g_1, ..., g_t \in I$ tels que

$$I = \langle g_1, ..., g_t \rangle$$

Autrement dit, tout idéal I de $k[x_1, ..., x_n]$ possède une base finie.

Théorème de la base de Hilbert

Axel Mauroy et Killian Le Milbeau

Voici une première application importante du théorème de la base de Hilbert qui expose un fait algébrique à propos des idéaux de $k[x_1, ..., x_n]$:

Proposition (Condition de chaine ascendante)

Soit une suite croissante (ascendante) d'idéaux de $k[x_1, ..., x_n]$

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$$

Alors, il existe un rang $N \geq 1$ *tel que :*

$$I_N = I_{N+1} = I_{N+2} = ...$$

Proposition

Toute suite ascendante d'idéaux se stabilise si et seulement si, tout idéal I *possède un nombre fini de générateur.*

Bases de Gröbner

La base $(g_1, ..., g_t)$ fournit par le théorème de la base de Hilbert a la propriété

$$\langle LT(I) \rangle = \langle LT(g_1), ..., LT(g_t) \rangle$$

Définition (Bases de Gröbner)

Un ordre monomial étant fixé, un sous-ensemble $G = \{g_1, ..., g_t\}$ de l'idéal I de $k[x_1, ..., x_n]$ est appelé base de Gröbner si,

$$\langle LT(I) \rangle = \langle LT(g_1), ..., LT(g_t) \rangle$$

Remarque 1 : Dans la littérature, on peut trouver l'appellation "base standard" pour une base de Gröbner.
Remarque 2 : En utilisant la convention $\langle \emptyset \rangle = \{0\}$, on défini $\emptyset$ comme étant la base de Gröbner de l'ensemble $\{0\}$.

Exemple 1 :

Reprenons l'ordre lexicographique sur les monômes de $\mathbb{R}[x, y]$ tel que $y < x$. On considère les polynômes $f_1 = xy + 1$ et $f_2 = y + 1$ et l'idéal $I =< f_1, f_2 >$ de $\mathbb{R}[x, y]$.
Montrons que $\{f_1, f_2\}$ n'est pas une base de Gröbner de I.

Exemple 2 :

On prend l'ordre lexicographique sur $\mathbb{Q}[x, y, z]$ avec $x < y < z$.
Considérons les polynômes $g_1 = z + x$ et $g_2 = y - x$ de $\mathbb{Q}[x, y, z]$, ainsi que l'idéal $I =< g_1, g_2 >$ de $\mathbb{Q}[x, y, z]$.
Montrons que $G = \{g_1, g_2\}$ est une base de Gröbner de I.

En résumé :

Proposition

Un ordre monomial étant fixé, tout idéal non nul I de $k[x1, ..., xn]$ *possède une base de Gröbner. De plus, toute base de Gröbner d'un idéal forme une base de cet idéal.*

Retour sur le théorème de la base de Hilbert

On peut aussi énoncer une deuxième application du théorème de la base de Hilbert, cette fois plus géométrique.

Définition (Variétés algébriques affines)

On considère les variétés algébriques affines comme étant l'ensemble des solutions d'un système polynômial fini :

$$\mathbf{V}(f_1, ..., f_s) = \left\{(a_1, ..., a_n) \in k^n \;\middle|\; \forall i,\ f_i(a_1, ..., a_n) = 0\right\}$$

Définition (Variété algébrique affine d'un idéal)

Soit I un idéal de $k[x_1, ..., x_n]$, on note

$$\mathbf{V}(I) = \left\{(a_1, ..., a_n) \in k^n \;\middle|\; \forall f \in I,\ f(a_1, ..., a_n) = 0\right\}$$

Retour sur le théorème de la base de Hilbert

Proposition

L'ensemble $\boldsymbol{V}(I)$ défini précédemment est bien une variété affine. En particulier, si $I =< f_1, ..., f_s >$, alors $\boldsymbol{V}(I) = \boldsymbol{V}(f_1, ..., f_s)$.

Ainsi, les variétés sont déterminées par les idéaux.