Introduction aux bases de Gröbner: théorie et pratique

par Denis MONASSE
professeur de Mathématiques Spéciales au Lycée Louis Le Grand

Notations et rappels

On désignera par K un corps commutatif (pour simplifier, en fait la théorie s'adapte parfaitement au cas d'un anneau factoriel noetherien quelconque). On désigne par $x_1, \dots, x_n$ des indéterminées et par $K[x_1, \dots, x_n]$ l'anneau des polynômes en ces indéterminées, à coefficients dans K.

On notera $X = \{x_1^{i_1} \dots x_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{N}\}$ (ensemble des *termes*). On appellera *monôme* le produit d'un scalaire par un terme, c'est à dire un polynôme de la forme $\alpha x_1^{i_1} \dots x_n^{i_n}$, et, lorsque $\alpha \neq 0$, on appellera degré de ce monôme l'entier $i_1 + \dots + i_n$. Le degré d'un polynôme P, noté $\deg P$, sera le plus grand degré de ses monômes non nuls.

On appelle *idéal* de $K[x_1, \dots, x_n]$ toute partie $\mathcal{I}$ de $K[x_1, \dots, x_n]$ vérifiant les trois propriétés

(i) le polynôme nul est dans $\mathcal{I}$
(ii) si P_1 et P_2 sons dans $\mathcal{I}$, il en est de même de $P_1 - P_2$
(iii) si P est dans $\mathcal{I}$ et si Q est un polynôme quelconque, PQ appartient à $\mathcal{I}$.

Un exemple fondamental d'idéal est l'ensemble des polynômes qui s'annulent sur une partie donnée de K^n. On montre que $K[x_1, \dots, x_n]$ vérifie les deux propriétés suivantes (équivalentes) qui caractérisent les anneaux dits noetheriens

Théorème. *(i) il n'existe pas de suite strictement croissante d'idéaux de $K[x_1, \dots, x_n]$, ou encore, toute suite croissante d'idéaux, $\mathcal{I}_0 \subset \mathcal{I}_1 \subset \dots \subset \mathcal{I}_p \subset \dots$, est stationnaire (c'est à dire qu'il existe un N tel que*

$$p \geq N \quad \Rightarrow \mathcal{I}_p = \mathcal{I}_N$$

(ii) *pour tout idéal $\mathcal{I}$ de $K[x_1, \dots, x_n]$, il existe une famille finie $(f_1, \dots, f_p)$ d'éléments de $\mathcal{I}$ telle que*

$$\mathcal{I} = \{f_1 g_1 + \dots + f_p g_p \mid g_1, \dots, g_p \in K[x_1, \dots, x_n]\}$$

Une telle famille $(f_1, \dots, f_p)$ sera par la suite appelée une base de l'idéal $\mathcal{I}$. Le but recherché ici est, étant donné un idéal, de trouver un moyen algorithmique d'en donner une base particulière qui permette de tester facilement l'appartenance ou non d'un polynôme à l'idéal et permette même de calculer aisément une forme réduite d'un polynôme quelconque modulo l'idéal.

Ordres sur les termes

Soit $X = \{x_1^{i_1} \dots x_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{N}\}$ l'ensemble des termes en $x_1, \dots, x_n$. On appellera *ordre admissible* sur X toute relation d'ordre *totale* (notée $\preceq$) vérifiant

(i) pour tout terme t, on a $1 \preceq t$
(ii) si s, t et u sont des termes et si $s \preceq t$, alors $su \preceq tu$

Exemples fondamentaux: on rencontrera par la suite deux exemples fondamentaux d'ordres admissibles sur les termes; d'une part l'ordre *lexicographique pur* défini par

$$x_1^{i_1} \dots x_n^{i_n} \prec x_1^{i_1} \dots x_n^{i_n} \iff \exists k \in [1, n], \quad i_1 = j_1, \dots, i_{k-1} = j_{k-1} \text{ et } i_k < j_k$$

d'autre part l'ordre du *degré total* défini par

$$x_1^{i_1} \dots x_n^{i_n} \prec x_1^{i_1} \dots x_n^{i_n} \iff \begin{cases} \deg(x_1^{i_1} \dots x_n^{i_n}) < \deg(x_1^{j_1} \dots x_n^{j_n}) \\ \text{ou } \deg(x_1^{i_1} \dots x_n^{i_n}) = \deg(x_1^{j_1} \dots x_n^{j_n}) \text{ et} \\ \quad \exists k \in [1, n], \quad i_n = j_n, \dots, i_{k+1} = j_{k+1} \text{ et } i_k > j_k \end{cases}$$

Exemple: dans $K[x, y, z]$ on a pour l'ordre du degré total

$$1 \prec z \prec y \prec x \prec z^2 \prec yz \prec xz \prec y^2 \prec xy \prec x^2 \prec \dots$$

Dans la suite, nous supposerons que nous nous sommes fixés un ordre admissible sur l'ensemble des termes X. Tout polynôme non nul p possède alors un unique monôme dominant au sens de cet ordre. Nous noterons $M(p)$ ce monôme. Il s'écrit sous la forme $M(p) = \alpha x_1^{i_1} \dots x_n^{i_n}$ et nous poserons $\alpha = \mathrm{hc}(p)$ (coefficient dominant de p) et $x_1^{i_1} \dots x_n^{i_n} = \mathrm{ht}(p)$ (terme dominant de p).

Réduction modulo une partie

Soit tout d'abord p et q deux polynômes en $x_1^{i_1} \dots x_n^{i_n}$. Supposons que q possède un monôme αt divisible par le terme dominant de p. Posons alors $t = u\,\mathrm{ht}(p)$ et $q' = q - \frac{\alpha}{\mathrm{hc}(p)} up = q - \frac{\alpha t}{M(p)} p$. On constate que q ne contient plus le terme t et que $q - q'$ ne contient que des monômes strictement inférieurs à t. On dira alors que q' a été obtenu à partir de q par *réduction modulo* p et l'on notera $q \underset{p}{\mapsto} q'$.

Si $P = \{p_1, \dots, p_n\}$ est une partie finie de polynômes, on écrira $q \underset{P}{\mapsto} q'$ s'il existe p_i tel que $q \underset{p_i}{\mapsto} q'$. On dira que q est *réductible* modulo P s'il admet une réduction modulo P, c'est à dire si l'un des ses monômes est divisible par le terme dominant de l'un des p_i. Dans le cas contraire on dira que q est *irréductible* modulo P. On notera $\underset{P}{\mapsto}^+$ la clôture transitive de la relation $\underset{P}{\mapsto}$ c'est à dire que

$$q \underset{P}{\mapsto}^+ q' \quad \Longleftrightarrow \quad q = q' \text{ ou } \exists q_1, \dots, q_p, \quad q \underset{P}{\mapsto} q_1 \underset{P}{\mapsto} \cdots \underset{P}{\mapsto} q_p \underset{P}{\mapsto} q'$$

On dira encore dans ce cas que q' est une réduction de q modulo P.

Enfin on dira que q' est une *réduite* de q modulo P si $q \underset{P}{\mapsto}^+ q'$ et si q' est irréductible modulo P. On notera dans ce cas $q \underset{P}{\mapsto}^* q'$. On remarquera que cette réduite de q n'est pas en général unique et on se gardera de faire toute conclusion hâtive sur les propriétés de la réduction modulo une partie, en dehors des trois propriétés suivantes qui nous serviront dans la suite.

Lemme 1. *Soit P une partie de $K[x_1, \dots, x_n]$, $p, q, r \in K[x_1, \dots, x_n]$ tels que $p - q \underset{P}{\mapsto} r$. Alors il existe $\tilde{p}$ et $\tilde{q}$ tels que $p \underset{P}{\mapsto}^+ \tilde{p}$, $q \underset{P}{\mapsto}^+ \tilde{q}$ et $r = \tilde{p} - \tilde{q}$.*

Soit ν le terme de $p - q$ qui est éliminé dans la réduction, si bien que $r = (p - q) - \alpha\nu \frac{s}{M(s)}$ avec $s \in P$. Appelons β le coefficient de ν dans p et γ celui de ν dans q. On a $\beta - \gamma = \alpha \neq 0$, donc l'un au moins des deux est non nul. Posons $u = \nu / \mathrm{ht}(s)$, $\tilde{p} = p - \frac{\beta}{\mathrm{hc}(s)} us$, $\tilde{q} = q - \frac{\gamma}{\mathrm{hc}(s)} us$. Il est clair que $\tilde{p}$ et $\tilde{q}$ répondent à la question.

Lemme 2. *Soit P une partie de $K[x_1, \dots, x_n]$ et $p, q \in K[x_1, \dots, x_n]$ tels que $p - q \underset{P}{\mapsto}^+ 0$. Alors il existe $r \in K[x_1, \dots, x_n]$ tel que $p \underset{P}{\mapsto}^+ r$ et $q \underset{P}{\mapsto}^+ r$ (autrement dit p et q admettent une réduction commune).*

Nous procéderons par récurrence sur le nombre N de réductions qui amène $p - q$ à 0. Si ce nombre est 0, c'est que $p - q = 0$ et $r = p = q$ convient. Sinon, soit h le résultat de la première réduction de $p - q$. D'après le lemme précédent, il existe $\tilde{p}$ et $\tilde{q}$ tels que $p \underset{P}{\mapsto}^+ \tilde{p}$, $q \underset{P}{\mapsto}^+ q$ et $h = \tilde{p} - \tilde{q}$. Mais il faut $N - 1$ réductions pour ramener $h = \tilde{p} - \tilde{q}$ à 0, et l'hypothèse de récurrence nous assure que $\tilde{p}$ et $\tilde{q}$ ont une réduction commune. Il en est donc de même de p et q.

Lemme 3. *Si $p \in K[x_1, \dots, x_n]$ et si $p \underset{P}{\mapsto} p'$, pour tout polynôme $q \in K[x_1, \dots, x_n]$, les polynômes $p + q$ et $p' + q$ ont une réduction commune.*

Soit $r \in P$ tel que $p' = p - \alpha u r / \mathrm{hc}(r)$ et soit $t = u\,\mathrm{ht}(r)$ le terme annulé dans la réduction. Soit $q \in K[x_1, \dots, x_n]$ et appelons β le coefficient de t dans q. C'est également celui de t dans $p' + q$ puisque t n'apparaît plus dans p'. Le coefficient de t dans $p + q$ est $\alpha + \beta$. Posons donc $\tilde{r} = r / \mathrm{hc}(r)$. On a alors

$$p + q \underset{P}{\mapsto}^+ s = (p + r) - (\alpha + \beta) u \tilde{r}$$

$$p' + q \underset{P}{\mapsto}^+ s' = (p' + r) - \beta u \tilde{r}$$

et $s - s' = (p - p') - \alpha u \tilde{r} = 0$ si bien que $s = s'$ est une réduction commune à $p + q$ et $p' + q$.

Bases de Gröbner

Definition. *Soit G une partie finie de $K[x_1, \ldots, x_n]$ et $\mathcal{I}(G)$ l'idéal engendré par cette partie. On dira que G est une base de Gröbner (sous entendu, de $\mathcal{I}(G)$) si*

$$\forall p \in K[x_1, \ldots, x_n], \quad p \in \mathcal{I}(G) \iff p \underset{G}{\mapsto}^* 0$$

Commentaires: Il est clair que les réductions de p s'effectuent en soustrayant à p des éléments de $\mathcal{I}(G)$. L'implication $p \underset{G}{\mapsto}^* 0 \Rightarrow p \in \mathcal{I}(G)$ est donc toujours vraie. C'est ici l'implication inverse qui nous intéresse. On a également facilement la caractérisation suivante des bases de Gröbner

Proposition. *Une partie G de $K[x_1, \ldots, x_n]$ est une base de Gröbner si et seulement si le seul polynôme de $\mathcal{I}(G)$ irréductible modulo G est le polynôme nul.*

Démonstration: 2pt$\Leftarrow$ Si $p \in \mathcal{I}(G)$, alors p a une réduction terminale modulo G qui est un élément irréductible de $\mathcal{I}(G)$ et qui doit donc être le polynôme nul.

2pt$\Rightarrow$ C'est évident, puisqu'un élément de $\mathcal{I}(G)$ doit pouvoir se réduire à 0, donc ne doit pas être irréductible s'il est non nul.

La principale contribution de Buchberger a été de montrer que l'objet essentiel qui permettait à la fois de caractériser et de construire des bases de Gröbner était le polynôme suivant

Définition. *Soit $p, q \in K[x_1, \ldots, x_n]$. On pose*

$$S(p,q) = M(p) \vee M(q) \left(\frac{p}{M(p)} - \frac{q}{M(q)} \right)$$

où comme d'habitude le symbole $\vee$ désigne le PPCM (ici de deux monômes!).

On a alors le théorème suivant dont la démonstration est un peu longue, mais très instructive

Théorème (Buchberger). *Soit G une partie finie de $K[x_1, \ldots, x_n]$. On a équivalence des trois propriétés*
(i) G est une base de Gröbner
(ii) Pour tous éléments p et q de G, le polynôme $S(p,q)$ est réductible à 0 modulo G.
(iii) Tout élément de $K[x_1, \ldots, x_n]$ a une unique réduction terminale modulo G.

Démonstration: 2pt(i)$\Rightarrow$(ii) Si p et q sont dans IG, ils sont dans IG et il en est donc de même de $S(p,q)$ qui doit en conséquence être réductible à 0 modulo G si G est une base de Gröbner.

2pt(ii)$\Rightarrow$(iii) Nous démontrerons ce résultat par récurrence sur le terme de plus haut degré de p (le principe de récurrence s'appliquant trivialement à l'ensemble totalement ordonné X). Si ce terme est 1, c'est que le polynôme p est constant et il admet alors une unique réduction (qui est terminale) qui est soit lui même (si G ne contient pas de polynôme constant), soit 0 (si G contient un polynôme constant). Nous supposerons donc que p a pour terme dominant t et que le résultat est vrai pour tout polynôme dont le terme dominant est strictement inférieur à t.

Si t est irréductible modulo G, alors toute réduction de p ne portera que sur les monômes strictement inférieurs, donc sur le polynôme $p - M(p)$. La réduction terminale de $p - M(p)$ étant unique, il en sera donc de même de celle de p. On supposera donc que p est réductible modulo G. Soit $g_1 \in G$ tel que $\mathrm{ht}(g_1)$ divise $M(p)$ et soit p_1 le résultat de la réduction de $M(p)$ modulo g_1. Soit d'autre part p_2 l'unique réduction terminale de $p - M(p)$ et q l'unique réduction terminale de $p_1 + p_2$, si bien que l'on a la chaîne de réductions

$$p \underset{G}{\mapsto}^+ M(p) + p_2 \underset{G}{\mapsto} p_1 + p_2 \underset{G}{\mapsto}^* q$$

Nous allons montrer que toute autre réduction terminale $p \underset{G}{\mapsto}^* r$ conduit au même résultat. Décomposons donc cette autre réduction de la manière suivante $p - M(p) \underset{G}{\mapsto}^+ p_3$, $M(p) \underset{g_2}{\mapsto} p_1'$, $p_1' + p_3 \underset{G}{\mapsto}^* r$ (la première réduction pouvant ne rien faire, elle n'est pas supposée terminale), si bien que l'on a la chaîne de réductions

$$p \underset{G}{\mapsto}^+ M(p) + p_3 \underset{G}{\mapsto} p_1' + p_3 \underset{G}{\mapsto}^* r$$

Nous distinguerons deux cas suivant que g_2 est égal ou non à g_1.

Si g_2 est égal à g_1, on a $p'_1 = p_1$. Nous allons montrer dans ce cas que p_1+p_2 et p_1+p_3 ont une réduction commune. Remarquons que la réduction non terminale $p - M(p) \underset{G}{\mapsto}^+ p_3$ peut être terminée et que comme la réduction terminale de $p - M(p)$ est unique, elle doit fatalement aboutir à p_2. Il existe donc une réduction $p_3 \underset{G}{\mapsto}^+ p_2$. Soit ℓ sa longueur (c'est à dire le nombre de réductions élémentaires effectuées). Si $\ell = 0$, c'est que $p_2 = p_3$ et il est évident que $p_1 + p_2$ et $p_1 + p_3$ ont une réduction commune. Supposons donc que $p_1 + f$ et $p_1 + p_3$ ont une réduction commune si $p_3 \underset{G}{\mapsto}^+ f$ en $\ell - 1$ étapes. Ecrivons alors la réduction $p_3 \underset{G}{\mapsto}^+ p_2$ sous la forme $p_3 \underset{G}{\mapsto}^+ f \underset{G}{\mapsto} p_2$. D'après le lemme 3, comme p_2 est une réduction de f, $p_1 + f$ et $p_1 + p_2$ ont une réduction commune g (que l'on peut bien entendu supposer terminale),

$$p_1 + f \underset{G}{\mapsto}^* g, \quad p_1 + p_2 \underset{G}{\mapsto}^* g$$

D'autre part, par notre hypothèse de récurrence (sur ℓ), $p_1 + f$ et $p_1 + p_3$ ont une réduction commune h (que l'on peut également supposer terminale),

$$p_1 + f \underset{G}{\mapsto}^* h, \quad p_1 + p_3 \underset{G}{\mapsto}^* h$$

Mais, comme le terme dominant de $p_1 + f$ est strictement inférieur à t, $p_1 + f$ a une unique réduction terminale et donc $g = h$. Dans ce cas, $p_1 + p_2$ et $p_1 + p_3$ ont $g = h$ comme réduction (terminale) commune. Mais alors, on a aussi (toujours par notre hypothèse de récurrence sur l'unicité de la réduction terminale) $q = g$ et $r = h$ et donc finalement $r = q$.

Il nous reste donc à examiner le cas où $g_2 \neq g_1$. Rappelons que nous avons la chaîne de réductions

$$p \underset{G}{\mapsto}^+ M(p) + p_3 \underset{G}{\mapsto} p'_1 + p_3 \underset{G}{\mapsto}^* r$$

Nous pouvons également construire une autre chaîne de réductions par $p - M(p) \underset{G}{\mapsto}^+ p_3$, $M(p) \underset{g_1}{\mapsto} p_1$, $p_1 + p_3 \underset{G}{\mapsto}^* \tilde{r}$. D'après le premier cas que nous avons examiné, elle conduit au même résultat que notre chaîne de réductions de référence et donc $\tilde{r} = q$. Mais alors

$$(p'_1 + p_3) - (p_1 + p_3) = p'_1 - p_1 = M(p)\left[\frac{g_1}{M(g_1)} - \frac{g_2}{M(g_2)}\right]$$

qui est le produit de $S(g_1, g_2)$ par un monôme car $M(g_1) \vee M(g_2)$ divise $M(p)$. On en déduit d'après (ii), que ce polynôme a une réduction à 0 modulo G. En appliquant le lemme 2, on trouve que $p'_1 + p_3$ et $p_1 + p_3$ ont une réduction commune, et par notre hypothèse de récurrence une même et unique réduction terminale. On a donc $r = \tilde{r} = q$.

2pt(iii)⇒(i) Posons $G = \{g_1, \ldots, g_n\}$. Soit $p \in \mathcal{I}(G)$ et écrivons $p = \sum h_i g_i$. Nous allons montrer par récurrence sur le plus grand des termes dominants des polynômes $h_1 g_1, \ldots, h_n g_n$ (les *composantes* de p) que p a une réduction à 0 modulo G. Soit t ce terme dominant. Si $t = 1$, alors p est constant ainsi que chacun des $h_i g_i$. Donc les g_i qui interviennent effectivement sont constants et soit $p = 0$, soit p a une réduction nulle modulo un g_i constant. Ceci démarre la récurrence. Supposons donc que tout polynôme de $\mathcal{I}(G)$ dont le plus grand des termes dominants des composantes est strictement inférieur à t admet une réduction à 0 modulo G. Notons $h_1 g_1, \ldots, h_m g_m$ les composantes non nulles de p qui contiennent le terme t et montrons par récurrence sur m que p a une réduction à 0.

Si $m = 1$, on a

$$p = h_1 g_1 + \sum h_i g_i \underset{g_1}{\mapsto} p'_1 = (h_1 - M(h_1))g_1 + \sum h_i g_i$$

qui a une réduction à 0 d'après notre hypothèse de récurrence sur t (on a supprimé le seul terme égal à t dans la somme). Supposons donc notre résultat vrai pour $m - 1$ et montrons le pour m. Pour cela écrivons $p = h_1 g_1 + h_2 g_2 + \sum_{i=3}^{\cdots} h_i g_i = p_1 + p_2$ avec $p_1 = M(h_1)g_1 + (M(h_2) + \alpha \operatorname{ht}(h_2))g_2$ et $p_2 = (h_1 - M(h_1))g_1 + (h_2 - M(h_2) - \alpha \operatorname{ht}(h_2))g_2 + \sum_{i=3}^{\cdots} h_i g_i$

Lemme: On peut choisir α de telle sorte que p_1 soit de la forme $\beta u S(g_1, g_2)$ pour un scalaire β et un terme $u \in X$

On remarque que $M(h_1)M(g_1) = \lambda t$, $M(h_2)M(g_2) = \mu t$, $\mathrm{ht}(h_2)M(g_2) = \nu t$, d'où

$$M(h_1)g_1 + (M(h_2) + \alpha\,\mathrm{ht}(h_2))g_2 = t\left(\lambda\frac{g_1}{M(g_1)} + (\mu + \alpha\nu)\frac{g_2}{M(g_2)}\right)$$

qui est de la forme voulue dès que $\mu + \alpha\nu = -\lambda$ car t est un multiple commun de $M(g_1)$ et $M(g_2)$.

Faisons donc ce choix de α. Le polynôme p_2 est dans l'idéal, et il a au plus $m-1$ composantes de terme dominant t, donc il admet, par notre hypothèse de récurrence sur m une réduction à 0. Il ne reste plus à montrer que le fait que p_1 admet une réduction à 0. Mais on a

$$\frac{M(g_1) \vee M(g_2)}{M(g_1)} g_1 \underset{g_2}{\mapsto} S(g_1, g_2) \overset{+}{\underset{G}{\mapsto}} q$$

pour un certain q irréductible d'une part, et aussi

$$\frac{M(g_1) \vee M(g_2)}{M(g_1)} g_1 \underset{g_1}{\mapsto} 0$$

D'après (iii), on a $q = 0$ et donc $S(g_1, g_2)$ admet une réduction terminale à 0 (unicité de la réduction terminale). Comme p_1 admet $S(g_1, g_2)$ comme réduction, p_1 admet 0 comme réduction terminale modulo G, ce qui achève la démonstration.

Au vu de (iii), la réduction terminale d'un élément p modulo une base de Gröbner G est donc unique. Nous la noterons $\mathrm{Red}(p, G)$. On a le résultat suivant

Corollaire. *Soit G une base de Gröbner. On a*

$$\forall p, q \in K[x_1, \ldots, x_n], \quad p - q \in \mathcal{I}(G) \iff \mathrm{Red}(p, G) = \mathrm{Red}(q, G)$$

autrement dit les éléments irréductibles modulo G décrivent exactement les classes modulo l'idéal $\mathcal{I}(G)$.

2pt$\Rightarrow$ Supposons $r = \mathrm{Red}(p, G) = \mathrm{Red}(q, G)$, alors $p - r \in \mathcal{I}(G)$ et $q - r \in \mathcal{I}(G)$ et donc $p - q = (p - r) - (q - r) \in \mathcal{I}(G)$.

2pt$\Leftarrow$ Supposons que $p - q \in \mathcal{I}(G)$, alors $p - q$ a une réduction à 0 et d'après le lemme 3, ils ont une réduction commune, et par unicité de la réduction terminale, ils ont même réduction terminale, soit $\mathrm{Red}(p, G) = \mathrm{Red}(q, G)$.

Existence de bases de Gröbner

Théorème. *Soit $P \subset K[x_1, \ldots, x_n]$ et $\mathcal{I}$ l'idéal engendré par P. Alors $\mathcal{I}$ admet une base de Gröbner contenant P.*

Nous allons procéder de la manière suivante en distinguant deux cas. Dans le premier cas, pour tout couple $(p, q) \in P \times P$, on a $S(p, q) \underset{G}{\mapsto}^* 0$. Alors P est une base de Gröbner d'après la caractérisation (ii). Dans le deuxième cas, on peut trouver un couple $(p, q) \in P \times P$ tel que $S(p, q) \underset{P}{\mapsto}^* r \neq 0$. Nous poserons $P_1 = P \bigcup \{r\}$. Comme $S(p, q)$ appartient à $\mathcal{I}(P)$, r appartient aussi à $\mathcal{I}(P)$ et donc $\mathcal{I}(P_1) = \mathcal{I}(P)$. Nous remplacerons donc P par P_1 et recommencerons le processus avec P_1. Nous obtiendrons ainsi une suite de bases de $\mathcal{I}$ vérifiant

$$P = P_0 \subset P_1 \subset \cdots P_n \subset \cdots$$

Montrons que le processus s'arrête au bout d'un nombre fini d'opération. Pour cela soit H_k l'ensemble des termes dominants des éléments de P_k. Remarquons que, si nous posons $P_{k+1} = P_k \bigcup \{r_k\}$, r_k est irréductible modulo P_k, donc son terme dominant n'est divisible par aucun des éléments de H_k. Le lemme suivant montrera que son terme dominant n'appartient pas à l'idéal engendré par H_k. Nous en déduisons que la suite des idéaux engendrés par les H_k est strictement croissante, ce qui nécessite que cette suite soit finie (lemme de Noether).

> *Lemme: Soit $t_1, \ldots, t_k, t \in X$. Alors t appartient à l'idéal engendré par $t_1, \ldots, t_k$ si et seulement si il est multiple de l'un d'entre eux.*
>
> Ecrivons $t = \sum_i f_i t_i$. Puisque le terme t apparaît dans la somme à droite, il doit apparaître avec un coefficient non nul dans au moins l'un des $f_i t_i$, mais alors c'est qu'il est multiple de t_i.

L'algorithme de Buchberger

La première chose à faire est de mettre en place un algorithme permettant de calculer une réduction terminale d'un polynôme q modulo une partie P de $K[x_1, \ldots, x_n]$. Nous supposerons donnée une fonction `SelectPoly` qui admet comme paramètre une partie de $K[x_1, \ldots, x_n]$ et qui en renvoie un élément (suivant une stratégie quelconque), ainsi qu'une fonction `Reducteurs` qui admet comme paramètre un polynôme p et une partie Q de $K[x_1, \ldots, x_n]$ et qui renvoie l'ensemble des polynômes de Q dont le terme dominant divise l'un des monômes de p. On obtient alors la procédure suivante

```
procedure Reduce(p,Q)
    r:=p;  q:=0;
    while r ≠ 0 do
      while Reducteurs(r,Q)≠ ∅ do
        f:=SelectPoly(Reducteurs(r,Q));
        r:= r-M(r)*f/M(f);
      od;
      q:=q+M(r); r:=r-M(r);
    od;
    return(q);
 end;
```

En ce qui concerne la construction d'une base de Gröbner, elle suit exactement la méthode décrite dans le précédent paragraphe. Elle admet comme paramètre une partie P de $K[x_1, \ldots, x_n]$ et renvoie une base de Gröbner de l'idéal engendré par P

```
procedure GrobnerBase(P)
   G:=P;  k:=length(G);
   B:={[i,j] | 1≤i<j≤k };
   while B ≠ ∅ do
      [i,j]:=SelectPair(B);# sélectionne une paire suivant une statégie
      B:=B \ {[i,j]};
      h:=Reduce(S(G[i],G[j]),G);
      if h≠0 then
```

```
            G:=G ∪ {h}; k:=k+1;
            B:=B ∪ {[i,k] | 1≤i<k};
        fi;
    od;
    return(G);
end;
```

Améliorations de l'algorithme

Le premier problème qui se pose est celui de la non-unicité des bases de Gröbner (en fait toute partie de l'idéal qui contient une base de Gröbner en est encore une). Pour résoudre ce problème on peut introduire la terminologie suivante

Définition. *On dit qu'une partie G de $K[x_1, \ldots, x_n]$ est réduite si $\forall g \in G, \quad g = Reduce(g, G \setminus \{g\}$; on dit qu'elle est normalisée si tout élément de G a pour coefficient dominant 1.*

Buchberger démontre alors le résultat suivant

Proposition. *Si deux parties G et H de $K[x_1, \ldots, x_n]$ sont réduites, normalisées et si elles engendrent le même idéal, alors elles sont égales.*

Buchberger donne alors un nouvel algorithme permettant de construire une base de Gröbner normalisée et réduite à partir d'une base de Gröbner. Les détails en sont plutôt techniques et ne seront pas abordés ici.

En ce qui concerne la complexité de l'algorithme, celle-ci est difficile à estimer. On constate cependant qu'au fur et à mesure que la longueur k de G augmente, le nombre de paires $[i, j]$ à considérer augmente. Heureusement, Buchberger montre qu'un certain nombres de ces paires ne sont pas à considérer à l'aide du lemme suivant

Lemme. *Si $M(p) \wedge M(q) = 1$, alors $S(p, q) \underset{\{p,q\}}{\mapsto}^{+} 0$.*

Démonstration On a dans ce cas $M(p) \vee M(q) = M(p)M(q)$ et donc $S(p, q) = M(q)p - M(p)q = M(q)(p - M(p)) - M(p)(q - M(q))$. Mais comme $M(p)$ et $M(q)$ contiennent des variables distinctes, les polynômes $p - M(p)$ et $q - M(q)$ n'ont aucun terme en commun et aucun terme ne disparaît dans le calcul de $M(q)(p - M(p)) - M(p)(q - M(q))$. Il suffit ensuite de remarquer que $M(p) \underset{p}{\mapsto} p - M(p)$ et que $M(q) \underset{q}{\mapsto} q - M(q)$ pour avoir $S(p, q) \underset{\{p,q\}}{\mapsto}^{+} 0$.

Il suffit donc de modifier la fonction `SelectPair` pour qu'elle ne renvoie pas les couples en question. Buchberger présente également d'autres améliorations qui diminuent considérablement la complexité de l'algorithme, mais qui sont purement techniques.

Applications

Espaces quotients

Soit $\mathcal{I}$ un idéal de $K[x_1, \ldots, x_n]$, G une base de Gröbner et désignons par T_0 l'ensemble des termes (monômes normalisés) qui sont irréductibles modulo G (c(est à dire qui ne sont pas divisibles par le terme dominant d'un élément de G) et soit π la projection canonique de $K[x_1, \ldots, x_n]$ dans $K[x_1, \ldots, x_n]/\mathcal{I}$. Alors on a

Théorème. *$\mathcal{U} = (\pi(t))_{t \in T_0}$ est une base de $K[x_1, \ldots, x_n]/\mathcal{I}$.*

Demonstration On sait que tout élément p de $K[x_1, \ldots, x_n]$ est réductible modulo G (donc congru modulo $\mathcal{I}$ à un polynôme p_0 qui est irréductible modulo G, donc combinaison linéaire d'élements de T_0. On en déduit que $\mathcal{U}$ est une famille génératrice du quotient.

De plus, si $(\alpha_t)_{t \in T_0}$ est une famille de scalaires telle que $\sum_{t \in T_0} \alpha_t \pi(t) = 0$, on a $\sum_{t \in T_0} \alpha_t t \in \mathcal{I}$ et donc $\sum_{t \in T_0} \alpha_t t \underset{G}{\mapsto}^{*} 0$. Mais ceci n'est possible que si $\sum_{t \in T_0} \alpha_t t = 0$, puisque ce polynôme est irréductible modulo G. On a donc $\forall t \in T_0, \quad \alpha_t = 0$. Donc la famille est également libre. C'est par conséquent une base de l'espace quotient.

Ceci, combiné à la fonction de réduction, permet donc de calculer de manière formelle dans le quotient sans difficulté.

Résolubilité de systèmes d'équations et d'inéquations polynomiales

Soit

$$(S) \quad \begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \end{cases}$$

un système d'équations polynomiales et soit $\mathcal{I}$ l'idéal de $K[x_1, \ldots, x_n]$ engendré par $p_1, \ldots, p_q$. Soit G une base de Gröbner de cet idéal. Le *Nullstellensatz* de Hilbert assure que ce système a des solutions dans la cloture algébrique de K si et seulement si $1 \notin \mathcal{I}$. Or, on a

$$1 \in \mathcal{I} \quad \Longleftrightarrow \quad 1 \underset{G}{\mapsto}^* 0 \quad \Longleftrightarrow \quad 1 \in G$$

puisque soit 1 appartient à G, soit 1 est irréductible modulo G. On obtient donc le théorème suivant

Théorème. *Soit*

$$(S) \quad \begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \end{cases}$$

un système d'équations polynomiales et soit $\mathcal{I}$ l'idéal de $K[x_1, \ldots, x_n]$ engendré par $p_1, \ldots, p_q$ et G une base de Gröbner de cet idéal. Alors le système (S) a des solutions si et seulement si $1 \notin G$.

C'est par exemple ce théorème qui est appliqué par la fonction `solvable` de Maple, qui se contente en fait de construire une base de Gröbner et de tester ensuite l'appartenance de 1 à cette base.

Un petit peu d'astuce permet d'étendre cette méthode à un système mixte composé d'équations et d'inéquations polynomiales. En effet on a,

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \\ q_1(x_1, \ldots, x_n) \neq 0 \\ \cdots \\ q_r(x_1, \ldots, x_n) \neq 0 \end{cases} \text{ a des solutions } \Longleftrightarrow \quad \begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \\ y_1 q_1(x_1, \ldots, x_n) - 1 = 0 \\ \cdots \\ y_r q_r(x_1, \ldots, x_n) - 1 = 0 \end{cases} \text{ a des solutions}$$

en introduisant de nouvelles inconnues $y_1, \ldots, y_r$.

Cette possibilité de tester la résolubilité d'un système d'équations et d'inéquations algébriques a été appliquée avec succès par *Wu* et son école pour la démonstration automatique de théorèmes de géométrie euclidienne. En effet, en introduisant des inconnues convenables, la plupart des théorèmes de la géométrie euclidienne classique peuvent se traduire sous la forme

$$\left.\begin{array}{c} P_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ P_q(x_1, \ldots, x_n) = 0 \\ Q_1(x_1, \ldots, x_n) \neq 0 \\ \cdots \\ Q_r(x_1, \ldots, x_n) \neq 0 \end{array}\right\} \Rightarrow R(x_1, \ldots, x_n) = 0$$

où les P_i décrivent les relations entre les objets (un point est le milieu de deux autres, un point est sur le cercle circonscrit à trois autres, etc.) tandis que les Q_j traduisent les conditions de validité du théorème (trois points ne sont pas alignés, etc.). La relation R traduit la conclusion du théorème (trois points sont alignés, etc.). Or cette implication logique est manifestement équivalente à la condition

$$\left.\begin{array}{c} P_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ P_q(x_1, \ldots, x_n) = 0 \\ Q_1(x_1, \ldots, x_n) \neq 0 \\ \cdots \\ Q_r(x_1, \ldots, x_n) \neq 0 \\ R(x_1, \ldots, x_n) \neq 0 \end{array}\right\} \text{ n'a pas de solution}$$

que l'on sait maintenant résoudre.

Nombre de solutions d'un système d'équations polynomiales

Soit

$$(S) \quad \begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \end{cases}$$

un système d'équations polynomiales et soit $\mathcal{I}$ l'idéal de $K[x_1, \ldots, x_n]$ engendré par $p_1, \ldots, p_q$. Désignons par V l'ensemble des solutions de (S). La variété algébrique V a comme algèbre de fonctions le quotient $K[x_1, \ldots, x_n]/\mathcal{I}$. On en déduit facilement que V est un ensemble fini si et seulement si $K[x_1, \ldots, x_n]/\mathcal{I}$ est de dimension finie (théorie du degré d'une variété algébrique). Mais, si G est une base de Gröbner de $\mathcal{I}$, on a exhibé plus haut une base du quotient $K[x_1, \ldots, x_n]/\mathcal{I}$, à savoir $\mathcal{U} = (\pi(t))_{t \in T_0}$, où T_0 désigne l'ensemble des monômes normalisés irréductibles modulo G. On en déduit que (S) a un nombre fini de solutions si et seulement si T_0 est fini. Nous allons en déduire un critère simple pour que le système n'ait qu'un nombre fini de solutions (dans la cloture algébrique de K)

Théorème. *Soit*

$$(S) \quad \begin{cases} p_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ p_q(x_1, \ldots, x_n) = 0 \end{cases}$$

un système d'équations polynomiales et soit $\mathcal{I}$ l'idéal de $K[x_1, \ldots, x_n]$ engendré par $p_1, \ldots, p_q$. Soit G une base de Gröbner de $\mathcal{I}$ et H l'ensemble des termes dominants des éléments de G. Alors le système (S) a un nombre fini de solutions si et seulement si

$$\forall i \in \{1, \ldots, n\}, \exists m_i \in \mathbb{N}, \quad x_i^{m_i} \in H$$

La condition est bien entendu suffisante puisque si elle est vérifiée, tout monôme normalisé irréductible doit être de la forme $t = x_1^{k_1} \ldots x_n^{k_n}$ avec $k_1 < m_1, \ldots, k_n < m_n$ ce qui ne laisse qu'un nombre fini de possibilités pour les éléments de T_0.

Inversement, la condition est nécessaire, car si $\forall m \in \mathbb{N}$, $x_i^m \notin H$, tous les monômes x_i^m sont irréductibles normalisés et donc éléments de T_0 qui est par conséquent infini.

Résolution de systèmes d'équations polynomiales

Pour le moment, nous ne nous sommes pas intéressés à l'ordre admissible utilisé sur l'ensemble X des monômes normalisés. Signalons cependant que celui-ci intervient dans l'efficacité des algorithmes utilisés et que de ce point de vue l'ordre par le degré total donne des algorithmes plus rapides que l'ordre lexicographique pur. Nous allons cependant voir que ce dernier a le gros avantage de conduire à la résolution explicite du système d'équations par trigonalisation du système.

Supposons en effet que le système (S) que nous avons déjà considéré n'a qu'un nombre fini de solutions $(a_1^{(i)}, \ldots, a_n^{(i)})$, $i = 1, \ldots, p$. Considérons alors le polynôme $P = \prod_{i=1}^{p}(x_n - a_n^{(i)})$. Ce polynôme est nul sur l'ensemble des zéros de (S) et le Nullstellensatz implique qu'une de ses puissances appartient à l'idéal $\mathcal{I}$, donc doit être réductible à 0 modulo G. Mais pour l'ordre lexicographique pur, les polynômes en x_n sont minimaux, c'est à dire qu'ils ne peuvent être réduits que par d'autres polynômes en x_n. On voit donc que la base de Gröbner doit contenir des polynômes en x_n (en fait un seul si elle est réduite) et les $a_n^{(i)}$ sont exactement les racines de ces polynômes.

En fait la méthode peut s'étendre en remarquant le résultat suivant

Lemme. *Soit G une base de Gröbner de l'idéal $\mathcal{I}$ de $K[x_1, \ldots, x_n]$ pour l'ordre lexicographique pur. Soit $k \in \{1, \ldots, n\}$, $G_k = G \bigcap K[x_k, \ldots, x_n]$ et $\mathcal{I}_k = \mathcal{I} \bigcap K[x_k, \ldots, x_n]$. Alors $\mathcal{I}_k$ est l'idéal de $K[x_k, \ldots, x_n]$ engendré par G_k.*

Soit $p \in \mathcal{I}_k$. Alors on a $p \underset{G}{\mapsto}^+ 0$. Mais pour l'ordre lexicographique pur, une réduction d'un polynôme de $K[x_k, \ldots, x_n]$ doit se faire toute entière dans $K[x_k, \ldots, x_n]$ (ces polynômes sont minimaux en un certain sens) et donc p appartient à l'idéal engendré par G_k.

Inversement, remarquons tout d'abord que G_k est une base de Gröbner dans $K[x_k, \ldots, x_n]$, car si $p, q \in G_k \subset G$, on a $S(p, q) \underset{G}{\mapsto}^+ 0$, on a $S(p, q) \underset{G}{\mapsto}^+ 0$, et toujours par la même remarque de minimalité des polynômes de $K[x_1, \ldots, x_n]$ (où se trouve $S(p, q)$) on a $S(p, q) \underset{G_k}{\mapsto}^+ 0$. La condition (ii) du théorème principal assure alors que G_k est une base de Gröbner. Donc, si p appartient à l'idéal engendré par G_k, on a $p \underset{G_k}{\mapsto}^+ 0$ et donc $p \underset{G}{\mapsto}^+ 0$. On a donc $p \in I(\bigcap K[x_1, \ldots, x_n])$.

On voit donc, que pour l'ordre lexicographique pur, le système donné par une base de Gröbner est triangulaire et conduit donc à une résolution en cascade. La dernière équation (une équation en x_n) permet de déterminer les valeurs de x_n. En reportant dans l'avant dernière (une équation en x_{n-1} et x_nn onb détermine les valeurs correspondantes de x_{n-1} et ainsi de suite, de manière tout à fait analogue à l'algorithme du pivot.

Simplification modulo des relations et substitutions généralisées

Une des principales applications des bases de Gröbner en calcul formel, et ce qui fait en grande partie leur intérêt, est leur aptitude à simplifier des espressions modulo des relations. Supposons en effet que $x_1, \ldots, x_n$ soient des variables (au sesn large: ce peut être des expressions algébriques "gelées" pour la circonstance) liées par des relations

$$(R) p_1(x_1, \ldots, x_) = 0, \ldots, p_q(x_1, \ldots, x_) = 0$$

Alors simplifier une expression $q(x_1, \ldots, x_n)$ modulo les relations (R) c'est tout simplement calculer l'image de Q dans le quotient de $K[x_1, \ldots, x_n]$ par l'idéal $\mathcal{I}$ engendré par ces relations. Connaissant une base de Gröbner $\mathcal{G}$ de $\mathcal{I}$, il suffit donc de prendre la réduction terminale de Q par $\mathcal{G}$.

C'est la démarche utilisée par la fonction Maple `simplify` qui admet une syntaxe complête

`simplify`(*expression*,{*relations*},[*variables*],*ordre*)

où *expression* est l'expression à simplifier, {*relations*} est l'ensemble des relations entre les variables, [*variables*] est la liste (ordonnée) des variables. Le paramètre facultatif *ordre* est l'ordre à utiliser; soit *tdeg* si l'ordre est l'ordre total (c'est le défaut), *plex* si l'on souhaite l'odre lexicographique pur sur les variables. Dans le premier cas, la simplification se fera en donnant comme première priorité la diminution du degré de l'expression et comme seconde priorité l'élimination des premières variables de la liste. Dans le second cas, priorité sera donnée à l'élimination des premières variables de la liste.

Bibliographie

Algorithms for Computer Algebra, par Geddes, Czapor et Labahn, ed. Kluwer Academic Publishers