Bases de Gröbner

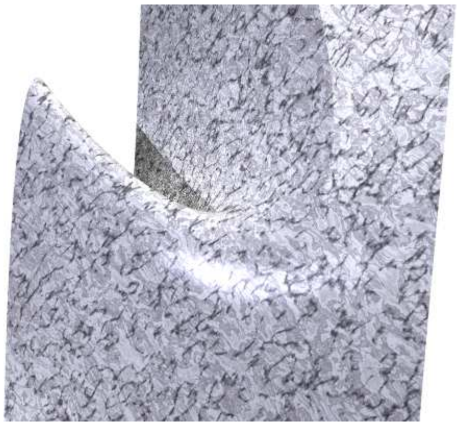
Vincent Zoonekynd
zoonek@math.jussieu.fr

Résumé

Nous exposons la notion de base de Gröbner, les principaux algorithmes qui la font intervenir (généralisations de la division euclidienne et du pivot de Gauss) et ses applications pour des calculs sur des polynômes à plusieurs indéterminées. Notre présentation s'inspire fortement de [CLO].

Introduction

Alors que tout un chacun manipule avec dextérité les polynômes à une indéterminée, nous restons particulièrement perplexes face à des polynômes à plusieurs indéterminées — tout au plus les polynômes symétriques nous sont-ils familiers. Ils sont pourtant omniprésents : par exemple, les mouvements du bras d'un robot sont décrits par des polynômes. La raison de la complexité du sujet est la suivante : l'étude des polynômes se ramène à l'étude de l'ensemble de leurs zéros. Pour les polynômes à une indéterminée, ce sont des ensembles finis, mais pour les polynômes à plusieurs indéterminées, c'est bien plus compliqué.



Les zéros du polynôme $y^2 - x^3 - zx$

Néanmoins, nous allons voir qu'une généralisation très simple de la division euclidienne permet d'effectuer des calculs dans l'anneau $k[x_1, \ldots, x_n]$ des polynômes à plusieurs indéterminées.

Division euclidienne

Commençons par rappeler la division euclidienne des polynômes à une indéterminée. Soient f et g de tels polynômes, dont on écrit les termes de plus haut degré en premier. On cherche à diviser f par g. Si le terme dominant de g ne divise pas celui de f, la division est finie : le quotient est nul et le reste est égal à f. En cas contraire, soit q le quotient de ces termes dominants ; on l'ajoute au quotient, on remplace f par $f - qg$ et on recommence.

Regardons sur un exemple : tentons de diviser $f = x^5$ par $g = x^2 + x + 1$. Le premier terme du quotient est $x^5/x^2 = x^3$ et le premier reste est

$$x^5 - x^3(x^2 + x + 1) = -x^4 - x^3,$$

ce qui s'écrit

$$f = x^3 g + (-x^4 - x^3).$$

On est maintenant amené à diviser $-x^4 - x^3$ par $x^2 + x + 1$, ce qui donne

$$-x^4 - x^3 = -x^2(x^2 + x + 1) + x.$$

Finalement, on cherche à diviser x par $x^2 + x + 1$, mais on ne peut pas : la division est finie et son résultat s'écrit

$$f = (x^3 - x^2)g + x.$$

On peut même poser la division.

$$\begin{array}{r|l}
x^5 \phantom{{}+x^4+x^3-x} & x^2 + x + 1 \\ \cline{2-2}
x^5 + x^4 + x^3 \phantom{{}-x} & x^3 - x^2 \\
- x^4 - x^3 \phantom{{}-x} & \\
- x^4 - x^3 - x & \\
x &
\end{array}$$

Avec plusieurs variables

Peut-on généraliser cet algorithme aux polynômes à plusieurs variables ? Le seul problème est de définir quel est le terme dominant d'un tel polynôme : il nous faut un ordre entre ses monômes — nous prendrons l'ordre lexicographique. Le même algorithme est maintenant utilisable.

On peut aussi vouloir diviser un polynôme f par plusieurs polynômes $g_1, \ldots, g_m$, *i.e.*, chercher à écrire

$$f = q_1 g_1 + \cdots + q_m g_m + r.$$

Il suffit de diviser par le permier polynôme et, quand on ne peut plus, de prendre le suivant et ainsi de suite. On s'arrête quand on ne peut plus diviser par aucun des polynômes.

Regardons sur un exemple. Cherchons à diviser $f = x^2y - xy$ par $g_1 = x^2 + y^2$ et $g_2 = y + 2$. Commençons par effectuer la division de f par g_1 ; il vient

$$f = yg_1 - xy - y^3.$$

Comme le reste n'est pas divisible par g_1, on essaye de le diviser par g_2, il vient alors

$$f = yg_1 - xg_2 + (2x - y^3).$$

Comme le reste a maintenant changé, regardons s'il ne serait pas à nouveau divisible par g_1 : ce n'est pas le cas. La division semble alors terminée, car on ne peut plus diviser ni par g_1 ni par g_2.

En fait, si on insiste, on peut quand même la poursuivre : le seul problème est que le terme dominant du reste, $2x$, n'est pas divisible par le terme dominant de g_1 ou g_2, *i.e.*, x^2 ou y. Mais si on met ce terme de côté, on peut continuer, en divisant $-y^3$ par g_1 et g_2 ; après calculs, il vient

$$f = yg_1 + (-x - y^2 + 2y - 4)g_2 + (2x + 8).$$

Cette fois-ci, on ne peut vraiment plus continuer, la division est terminée.

On peut remarquer que l'on aurait obtenu un resultat different en divisant par (g_2,g_1), en l'occurrence

$$f = (x^2 - x + 2y - 4)g_2 - 2g_1 + (2x + 8).$$

Neanmoins, le reste est le même : est-ce toujours le cas ? Eh bien, non ; si on divise $f = x^2y^2$ par $g_1 = xy$ et $g_2 = xy + y$, on n'obtient pas le même reste selon l'ordre des diviseurs.

$$f = xyg_1 + 0 \cdot g_2 + 0$$
$$f = (xy - y)g_2 + 0 \cdot g_1 + y^2.$$

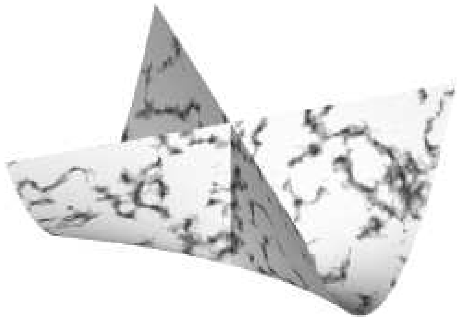
Interlude : les idéaux

L'un des buts — non encore atteint, patience — de l'algorithme précédent pouvait être de chercher si le polynôme f pouvait s'écrire

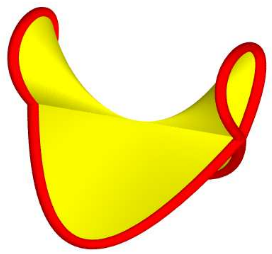
$$f = q_1g_1 + q_2g_2.$$

L'ensemble des polynômes de cette forme s'appelle l'*idéal* engendré par g_1 et g_2 et se note $\langle g_1,g_2\rangle$. Pour les polynômes à une indéterminée, nous nous étions limités à la division par un seul polynôme, car tous les idéaux de $k[x]$ sont de la forme $\langle g\rangle$ pour un polynôme g ; mais ce n'est plus vrai pour les polynômes à plusieurs indéterminées : c'est pour cette raison que nous avons tenté de diviser par un ensemble de polynômes.

Cette notion d'idéal a une interprétation géométrique : à un idéal $I \subset k[x_1,\ldots,x_n]$ on associe l'ensemble des points de $\mathbf{C}^n$ qui annulent tous les éléments de I. Si on a un système de générateurs de I, il suffit en fait de demander les points qui annulent ces générateurs. Les parties de $\mathbf{C}^n$ ainsi obtenues sont appelées *variétés affines*. Les figures suivantes donnent quelques exemples (sur $\mathbf{R}$). On pourra remarquer que des idéaux différents peuvent définir la même partie de $\mathbf{C}^n$, c'est par exemple le cas de $\langle x\rangle$ et $\langle x^2\rangle$.



La surface d'équation $x^2 - y^2z = 0$



Une courbe définie par les équations $x^2 - y^2z^2 + z^3 = 0$ et $x^2 + y^2 + z^2 = 1$, i.e., à l'intersection de deux surfaces.

Bases de Gröbner

La raison pour laquelle le reste de notre division n'est pas uniquement déterminé est la suivante : au cours de la division, le reste peut être une de combinaison « linéaire » des générateurs de notre idéal faisant disparaître les termes dominants et rendant ainsi la division impossible. Dans l'exemple précédent,

$$g_2 - g_1 = y$$

donne un reste non nul par la division par g_1 et g_2 : son terme dominant ne divise ni celui de g_1 ni celui de g_2. Pour pallier ce problème, nous allons agrandir la famille génératrice de l'idéal pour y inclure de telles combinaisons linéaires.

Plus formellement, étant donnés deux polynômes f et g, de termes dominants respectifs ax^α et bx^β, où α et β sont des multi-indices, on note $x^{\alpha\vee\beta}$ le plus petit multiple commun de x^α et x^β et on considère leur *polynôme S*, défini par

$$S(f,g) = bx^{\alpha\vee\beta-\alpha}f + ax^{\alpha\vee\beta-\beta}g.$$

C'est la combinaison « linéaire » la plus simple qui fait disparaître les termes dominants. On dit qu'un ensemble $G = \{f_1,\dots,f_n\}$ de polynômes est une *base de Gröbner* si la division du polynôme S de deux quelconques d'entre eux par G donne un reste nul.

Dès lors, pour obtenir une base de Gröbner, on procède ainsi : on part d'une famille de polynômes et on rajoute les restes des S-polynômes jusqu'à ce que tous ces restes soient nuls (on peut montrer que cet algorithme se termine).

Regardons ce qui se passe sur un exemple, l'idéal engendré par

$$\begin{aligned} f_1 &= x^3 - 2xy \\ f_2 &= x^2y - 2y^2 + x. \end{aligned}$$

Le S-polynôme de f_1 et f_2 est $-x^2$ et le reste de sa division par (f_1,f_2) est $-x^2$. On pose donc

$$f_3 = -x^2.$$

Le S-polynôme de f_1 et f_3 est $-2xy$ et le reste de sa division par (f_1,f_2,f_3) est $-2xy$; on pose donc

$$f_4 = -2xy.$$

Le S-polynôme de f_1 et f_4 est $-2xy^2$ mais le reste de sa division par (f_1,f_2,f_3,f_4) est nul. Par contre le S-polynôme de f_1 et f_4 est $x - 2y^2$ et le reste de sa division par (f_1,f_2,f_3,f_4) est $x - 2y^2$; on pose donc

$$f_5 = x - 2y^2.$$

Remarquons maintenant que le S-polynôme de f_1 et f_5 est $2x^2y^2 - 2xy$ et que son reste par la division par $(f_1,\dots,f_5)$ est $4y^3$; on pose donc

$$f_6 = 4y^3.$$

On peut désormais vérifier que les restes de tous les S-polynômes sont nuls : on a enfin obtenu une base de Gröbner.

On remarquera que l'on peut enlever certains de ces polynômes, en l'occurrence ne retenir que g_4 et g_5, tout en gardant une base de Gröbner — mais nous ne nous attarderons pas sur ce point.

Nous admettrons le résultat suivant : *Soit $g_1,\dots,g_n$ une base de Gröbner, un polynôme f est dans l'idéal $\langle g_1,\dots,g_n\rangle$ si et seulement si le reste de sa division par $g_1,\dots,g_n$ est nul.*

Applications

Nous donnons maintenant quelques applications des bases de Gröbner, sous forme d'exerices. Certains sont résolus, les autres sont laissés à la sagacité du lecteur. Nous utiliserons le logiciel de calcul formel Mupad, [M], qui est gratuit.

Le polynôme $x^2y - 2xy + 1$ est-il dans l'idéal engendré par $x^2 - x + 2y^2$ et $x + 2y - 1$?

Il suffit de chercher une base de Gröbner de notre idéal et de calculer le reste de la division.

```
export(groebner):
p1:= poly(x^2 - x + 2*y^2, [x,y]):
p2:= poly(x + 2*y - 1, [x,y]):
G:= gbasis([p1,p2], LexOrder);
```

$$x + 2y - 1, \quad -y + 3y^2$$

```
p:= poly(x^2*y - 2*x*y + 1, [x,y]):
normalf(p, G, LexOrder);
```

$$5y/9 - 1$$

Comme le reste est non nul, on sait que le polynôme n'est pas dans l'idéal.

Comment l'ordinateur résout-il le système d'équations suivant ?

$$\begin{aligned} x^2 - x + 2y^2 &= 0 \\ x^2 + y^2 &= 1 \end{aligned}$$

Remarquons tout d'abord que l'ordinateur sait résoudre ce système tout seul.

```
solve({x^2 - x + 2*y^2, x^2 + y^2-1});
```

$$(-2,i\sqrt{3}), \quad (-2,-i\sqrt{3}), \quad (1,0)$$

Mais comment fait-il ? Procède-t-il par tâtonnements et substitutions, comme on nous l'apprend à l'école ? Utilise-t-il une méthode plus systématique ? Comme vous l'avez dèjà deviné, il s'agit de bases de Gröbner. Résoudre ce système revient à chercher les points (x,y,z) qui annullent tous les polynômes de l'idéal $\langle g_1,g_2\rangle$ et il suffit de prendre une famille génératrice, par exemple une base de Gröbner pour l'ordre lexicographique.

```
p1:=poly(x^2 - x + 2*y^2,[x,y]):
p2:=poly(x^2 + y^2-1,[x,y]):
gbasis([p1,p2], LexOrder);
```

$$x - y^2 - 1, \quad 3y^2 + y^4$$

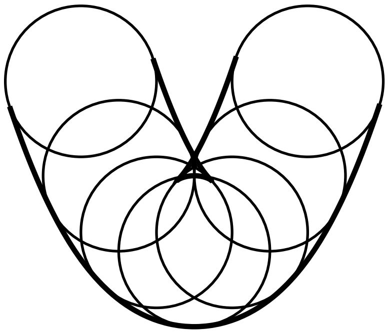
Le système que l'on obtient est bien plus agréable : la variable x a été éliminée de la seconde équation. Nous venons de voir que les bases de Gröbner permettent de trianguler des systèmes d'équations polynômiales (et non plus simplement linéaires, comme pour le pivot de Gauss), que l'on peut ensuite résoudre par substitutions.

Donner l'équation de l'enveloppe des cercles

$$(x-t)^2 + (y-t^2)^2 = 1.$$

Nous voulons éliminer la variable t dans le système suivant.

$$\begin{aligned}(x-t)^2 + (y-t^2)^2 &= 1\\ (t-x) - 2t(y-t^2) &= 0\end{aligned}$$



Il suffit de calculer une base de Gröbner pour l'ordre lexicographique.

```
p1:=poly((x-t)^2+(y-t^2)^2-1,[t,x,y]):
p2:=poly(t-x -2*t*(y-t^2), [t,x,y]);
gbasis([p1,p2], LexOrder);
%1[5]
```

On obtient un résultat : l'équation implicite d'une courbe, que nous ne recopions pas. Mais attention : tout ce que nous savons, c'est que *si* un point est solution de nos équations, *alors* il est sur la courbe d'équation ci-dessus. La réciproque est fausse en général, mais nous éluderons le problème. Signalons simplement que les polynômes de la base de Gröbner trouvée ne faisant intervenir que les variables x et y engendrent l'idéal $I \cap k[x,y]$; en d'autres termes, ils décrivent la plus petite variété algébrique contenant l'enveloppe recherchée.

Quels sont les points singuliers de l'enveloppe que l'on vient de trouver ?

Trouver une équation implicite du tore.

Soient I et J des idéaux de $k[x_1,\dots,x_n]$; montrer que $I \cap J = \langle 1 - y_1 - y_2, Iy_1, Jy_2\rangle \cap k[x_1,\dots,x_n]$. En déduire un algorithme permettant de calculer l'intersection de deux idéaux.

Pour en savoir plus...

[BW] B. Buchberger and F. Winkler, *Gröbner bases and applications*, LMSLNS 251, Cambridge University Press, 1998.

[CLO] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties and algorithms*, Springer–Verlag, 1992.

[E] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer–Verlag, 1995.

[M] `http://www.mupad.de/`.

[S] B. Sturmfels, *Algorithms in invariant theory*, Springer–Verlag, 1993.