Séries formelles
à plusieurs variables

Cyrille CHENAVIER et Adya MUSSON-LEYMARIE

Table des matières

1. Motivations

Les séries formelles sont des sommes infinies, pour lesquelles on ne se pose pas de question autour du rayon de convergence. En particulier, celles-ci ne sont pas nécessairement à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$. Leur étude apparaît naturellement en géométrie : résolution d'équations aux dérivées partielles en géométrie différentielle ou problème de désingularisation en géométrie algébrique.

Motivée par la définition de séries numériques en analyse, celle des séries formelles nécessite d'introduire une topologie sur les polynômes telle que les séries formelles sont les limites de suites de polynômes convergentes pour cette topologie. L'idée sous-jacente de cette topologie est que deux polynômes sont d'autant plus proches qu'ils coïncident jusqu'à un haut degré. En effet, un polynôme donné peut être vu comme étant une somme partielle dans laquelle on ajoute itérativement des termes de degrés de plus en plus élevés, afin de ne pas modifier la somme partielle en cours de construction. Lorsque la construction itérative est infinie, la somme partielle tend vers une somme infinie qui sera alors une série. Par exemple, on considère, pour une seule variable x et pour un entier $n \in \mathbb{N}$, le polynôme :

$$f_n(x) = 1 + x + \cdots + x^n.$$

Lorsque $m \in \mathbb{N}$ est un entier supérieur à n, le polynôme $f_m(x)$ coïncide avec $f_n(x)$ jusqu'à l'ordre n, et les termes $x^{n+1}, \cdots, x^m$ sont ceux que l'on a ajoutés à la somme partielle $f_n(x)$. Intuitivement, la suite de polynômes $\big(f_n(x)\big)_n$ doit tendre vers la série :

$$f(x) = \sum_{n\in\mathbb{N}} x^n = 1 + x + x^2 + \cdots.$$

En reprenant l'exemple précédent, plus n et m sont grands, plus les polynômes $f_n(x)$ et $f_m(x)$ coïncident jusqu'à un degré élevé, et plus la topologie que l'on cherche à définir doit rendre leur distance petite. Pour formaliser cette idée, en supposant que $n < m$, on stipule que la distance entre $f_n(x)$ et $f_m(x)$ est égale à $1/2^{n+1}$. Dans la section suivante, on va voir que cette notion de distance s'étend naturellement aux polynômes multivariés. Une fois que cette distance sera définie, il faudra étendre l'espace des polynômes en un espace contenant toutes les limites des suites de polynômes pour cette distance. Cela sera formalisé par une complétion de Cauchy, et cette complétion sera précisément l'espace des séries formelles.

2. Construction

2.1 Polynômes multivariés et valuations

On commence par rappeler la construction des polynômes multivariés. On fixe ainsi un corps $\mathbb{K}$ et un ensemble fini $\{x_1, \cdots, x_d\}$ d'indéterminées. Un *monôme* en les indéterminées $\{x_1, \cdots, x_d\}$ est une expression de la forme

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_d^{\alpha_d},$$

où $\alpha = (\alpha_1, \cdots, \alpha_d) \in \mathbb{N}^d$. Le *degré* du monôme $\mathbf{x}^\alpha$, est par définition

$$\deg\big(\mathbf{x}^\alpha\big) = |\alpha| = \alpha_1 + \cdots + \alpha_d.$$

Un *polynôme* multivarié en les $x_1, \cdots, x_d$ est une combinaison linéaire finie de monômes :

$$f(x_1, \cdots, x_d) = \sum_{\alpha\in\mathbb{N}^d} f_\alpha \mathbf{x}^\alpha,$$

où chaque f_α appartient à $\mathbb{K}$ et sont presque tous nuls, *i.e.*, ils sont tous nuls sauf un nombre fini. Lorsque l'on voudra alléger les notations, on notera f pour $f(x_1,\cdots,x_d)$. On note $\mathbb{K}[x_1,\cdots,x_d]$ l'ensemble des polynômes multivariés. Le dernier ingrédient dont on a besoin pour définir la distance entre deux polynômes multivariés est la notion de *valuation* d'un polynôme $f(x_1,\cdots,x_d)$: il s'agit du plus petit degré d'un monôme figurant avec un coefficient non nul dans $f(x_1,\cdots,x_d)$:

$$\mathrm{val}(f) = \min\left\{\deg\left(\mathbf{x}^\alpha\right) \mid f_\alpha \neq 0\right\}.$$

Dans le cas où le polynôme $f(x_1,\cdots,x_d)$ est nul, la convention est de poser $\mathrm{val}(f)=\infty$. On peut désormais introduire la définition de la distance entre deux polynômes.

Définition 2.1.1. On définit la distance dist sur $\mathbb{K}[x_1,\cdots,x_d]$ par

$$\mathrm{dist}(f,g) = \frac{1}{2^{\mathrm{val}(f-g)}}.$$

Dans la remarque suivante, on vérifie que dist vérifie bien les axiomes d'une distance.

Remarque 2.1.2. Étant donnés des polynômes f, g et h, on a :

- $\mathrm{val}(f-f) = \mathrm{val}(0) = \infty$ et donc $\mathrm{dist}(f,f) = 1/2^\infty = 0$,
- $\mathrm{val}(f-g) = \mathrm{val}(g-f)$ et donc $\mathrm{dist}(f,g) = \mathrm{dist}(g,f)$,
- $\mathrm{val}(f-h) \geq \min\left\{\mathrm{val}(f-g), \mathrm{val}(g-h)\right\}$, et donc

$$\mathrm{dist}(f,h) \leq \frac{1}{2^{\min\{\mathrm{val}(f-g),\mathrm{val}(g-h)\}}} \leq \frac{1}{2^{\mathrm{val}(f-g)}} + \frac{1}{2^{\mathrm{val}(g-h)}} = \mathrm{dist}(f,g) + \mathrm{dist}(g,h).$$

L'inégalité $\mathrm{val}(f-h) \geq \min\left\{\mathrm{val}(f-g), \mathrm{val}(g-h)\right\}$ s'interprète de la façon suivante : si f et g coïncident jusqu'à un degré n et que g et h coïncident jusqu'à un degré $m \geq n$, alors f et h coïncident au moins jusqu'au degré n. On illustre la notion de valuation ainsi que l'inégalité précédente sur les exemples suivants.

Exemple 2.1.3. Dans nos exemples, on considère un nombre de variables d au plus égal à 3. Au lieu de noter les variables $\{x_1,\cdots,x_d\}$, on note $\{x\}$ pour $d=1$, $\{x,y\}$ pour $d=2$ et $\{x,y,z\}$ pour $d=3$.

1. En une seule variable, $\mathrm{val}(f)$ n'est rien d'autre que la plus petite puissance de x figurant dans f. Par exemple, pour $f(x) = x^{n+1}+\cdots+x^m$, avec $n<m$, on a $\mathrm{val}(f) = n+1$. En particulier, en reprenant la suite de polynômes de la première section définie par

   $$f_n(x) = 1 + x + \cdots + x^n,$$

   on a bien comme annoncé

   $$\mathrm{dist}\left(f_n, f_m\right) = \frac{1}{2^{\mathrm{val}\left(x^{n+1}+\cdots+x^m\right)}} = \frac{1}{2^{n+1}}.$$

2. On considère les polynômes de trois variables :

   $$f(x,y,z) = 1+3z+2xy, \quad g(x,y,z) = 3z+5y^2, \quad h(x,y,z) = 2x+yz.$$

   On a donc

   $$f-g = 1+2xy-5y^2, \quad g-h = -2x+3z+5y^2-yz, \quad f-h = 1-2x+3z+2xy-yz,$$

   et donc

   $$\mathrm{val}(f-g) = 0, \quad \mathrm{val}(g-h) = 1, \quad \mathrm{val}(f-h) = 0.$$

   Dans cet exemple, on remarque que $\mathrm{val}(f-h) = \min\left\{\mathrm{val}(f-g), \mathrm{val}(g-h)\right\}$. Si on veut avoir une inégalité stricte, on peut prendre

   $$f'(x,y,z) = x+yz, \quad g'(x,y,z) = y, \quad h'(x,y,z) = x-z^3,$$

   de sorte que

   $$\mathrm{val}\left(f'-g'\right) = 1, \quad \mathrm{val}\left(g'-h'\right) = 1, \quad \mathrm{val}\left(f'-h'\right) = 2.$$

2.2 Définition des séries formelles

Avant de définir les séries formelles, on fait quelques rappels. Étant donné un espace métrique (X,d), une *suite de Cauchy* est une suite $(x_n)_n \subseteq X$ telle que $d(x_n,x_m) \to 0$ quand $n,m \to \infty$. Le *complété de Cauchy* de X est l'espace métrique $(\overline{X},\overline{d})$, où $\overline{X}$ est l'ensemble des suites de Cauchy de X, modulo la relation d'équivalence $(x_n)_n \sim (y_n)_n$ si $d(x_n,y_n) \to 0$ quand $n \to \infty$, et $\overline{d}$ est définie par :

$$\overline{d}(x,y) = \lim_{n\to\infty} d(x_n,y_n),$$

où $x = (x_n)_n$ et $y = (y_n)_n$ sont des suites de Cauchy. Il s'avère que $\overline{d}$ est bien définie, *i.e.*, ne dépend pas des représentants choisis de x et y, que X s'identifie à un sous-espace de $\overline{X}$ en envoyant x sur la suite constante égale à x, que la restriction de $\overline{d}$ à X est égale à d et que $(\overline{X},\overline{d})$ est *complet, i.e.*, toutes les suites de Cauchy convergent. Par convention, on note d au lieu $\overline{d}$ la distance induite par d sur $\overline{X}$. Enfin, si $x \in \overline{X}$ correspond à la suite de Cauchy $(x_n)_n$, alors X étant inclus dans $\overline{X}$, la suite $(x_n)_n$ peut être vue comme une suite dans $\overline{X}$ et il s'avère qu'en tant que suite de $\overline{X}$, elle tend vers x pour la topologie induite par d.

Comme précédemment, on considère une algèbre de polynômes $\mathbb{K}[x_1,\cdots,x_d]$, munie de la métrique dist.

Définition 2.2.1. L'espace des séries formelles, noté $\mathbb{K}[[x_1,\cdots,x_d]]$, est le complété de Cauchy de $\mathbb{K}[x_1,\cdots,x_d]$ pour la distance dist. La métrique dist sur $\mathbb{K}[x_1,\cdots,x_d]$ s'étend en une métrique sur $\mathbb{K}[[x_1,\cdots,x_d]]$, toujours notée dist, et la topologie induite est appelée topologie $(x_1,\cdots,x_d)$-*adique*.

Cette définition signifie qu'une série formelle est une classe d'équivalence de suites de Cauchy de polynômes, où deux suites $(f_n)_n$, et $(g_n)_n$ sont équivalentes si $\mathrm{dist}(f_n,g_n) \to 0$ lorsque $n \to \infty$, et la série formelle correspondant à $(f_n)_n$ est la limite de cette suite dans $\mathbb{K}[[x_1,\cdots,x_d]]$. Or, pour que $(f_n)_n$ converge, il suffit qu'elle soit de Cauchy, *i.e.*, que $\mathrm{dist}(f_n,f_m) \to 0$ lorsque $n,m \to \infty$. Par définition de dist, cela signifie que plus n et m sont grands, plus f_n et f_m coïncident jusqu'à un haut degré, ce qui signifie intuitivement que f_n est bien la somme partielle de la série limite. On illustre cela par des exemples.

Exemple 2.2.2.

1. On reprend la suite de polynômes de l'introduction définie par $f_n(x) = 1 + x + \cdots + x^n$. On a déjà vu que pour $n < m$, on a $\mathrm{dist}(f_n,f_m) = 1/2^{n+1}$ qui tend vers 0 quand $n,m \to \infty$, de sorte que $(f_n)_n$ est bien une suite de Cauchy. Sa limite est notée

   $$f(x) = \sum_{n\in\mathbb{N}} x^n,$$

   puisqu'elle représente bien l'expression $1 + x + x^2 + \cdots$. Une autre façon d'obtenir cette série est de considérer la suite de polynômes définie par

   $$g_n(x) = 1 + x + \cdots + x^{n^2}.$$

   Il s'agit également d'une suite de Cauchy puisque pour $n < m$, on a $\mathrm{dist}(g_n,g_m) = 1/2^{n^2+1}$, qui tend bien vers 0 quand $n,m \to \infty$. De plus, $(g_n)_n$ est équivalente à $(f_n)_n$ puisque

   $$\mathrm{dist}(f_n,g_n) = \frac{1}{2^{n+1}} \to 0 \text{ quand } n \to \infty.$$

2. On souhaite définir la série formelle correspondant à l'expression

   $$1 + x + y + x^2 + xy + y^2 + x^3 + x^2y + xy^2 + y^3 + \cdots, \tag{1}$$

contenant tous les monômes de deux variables. Une façon de procéder est de considérer la suite de polynômes définie par

$$f_n(x,y) = 1 + x + y + \cdots + x^n + x^{n-1}y + \cdots + xy^{n-1} + y^n,$$

contenant tous les monômes de degré au plus n. Pour $n < m$, on a

$$f_n(x,y) - f_m(x,y) = -\left(x^{n+1} + \cdots + y^{n+1} + \cdots + x^m + \cdots + y^m\right),$$

et donc $\mathrm{dist}\left(f_n, f_m\right) = 1/2^{n+1} \to 0$ quand $n, m \to \infty$. On a donc bien une suite de Cauchy, dont on note la limite, *i.e.*, la classe d'équivalence de suite de Cauchy qu'elle représente, par

$$F(x,y) = \sum_{\alpha \in \mathbb{N}^2} \mathbf{x}^\alpha.$$

3. Plus généralement, pour un nombre quelconque de variable, on souhaite qu'une série formelle soit représentée par une expression de la forme

$$f(x_1, \cdots, x_d) = \sum_{\alpha \in \mathbb{N}^d} f_\alpha \mathbf{x}^\alpha,$$

où les f_α sont des éléments de $\mathbb{K}$, dont on ne suppose plus qu'ils sont tous nuls sauf un nombre fini. Alors, on peut construire $f(x_1, \cdots, x_d)$ comme étant la limite de la suite de Cauchy définie par

$$f_n(x_1, \cdots, x_d) = \sum_{|\alpha| \leq n} f_\alpha \mathbf{x}^\alpha,$$

contenant tous les monômes de degré au plus n avec le coefficient f_α prescrit. Pour $n < m$, on a

$$f_n(x_1, \cdots, x_d) - f_m(x_1, \cdots, x_d) = -\left(\sum_{|\alpha| \geq n+1} f_\alpha \mathbf{x}^\alpha\right),$$

de sorte que $\mathrm{dist}\left(f_n, f_m\right) \leq 1/2^{n+1} \to 0$ lorsque $n, m \to \infty$, *i.e.*, $\left(f_n\right)_n$ est bien une suite de Cauchy. Dans la remarque 3.1.2, on verra comment donner un sens plus formel à l'expression (1).

Maintenant que le séries formelles ont été définies, on va s'intéresser aux propriétés algébriques et topologiques de $\mathbb{K}[[x_1, \cdots, x_d]]$.

3. Propriétés algébriques et topologiques

On fixe un ensemble de séries formelles $\mathbb{K}[[x_1, \cdots, x_d]]$. Par construction, il s'agit d'un espace métrique complet. On va montrer que cet ensemble a une structure de $\mathbb{K}$-algèbre, dont on analysera certaines propriétés algébriques. On rappellera également que les idéaux de cet anneau sont fermés pour la topologie $(x_1, \cdots, x_d)$-adique induite par dist.

3.1 Structure d'algèbre et dualité

On commence par montrer que $\mathbb{K}[[x_1, \cdots, x_d]]$ admet une structure de $\mathbb{K}$-algèbre. Pour cela, on note qu'une suite de polynômes $\left(f_n\right)_n$ tend vers un polynôme f si et seulement si pour tout entier k il existe un rang n_0 à partir duquel $\mathrm{dist}\left(f_n, f\right) \leq 1/2^{k+1}$, *i.e.*, $\left(f_n\right)_n$ tend vers f si et seulement si pour tout degré k, les

coefficients des monômes de degré au plus k dans f_n et f coïncident à partir d'un certain rang. Soient des suites $(f_n)_n$ et $(g_n)_n$ tendant vers f et g dans $\mathbb{K}[x_1,\cdots,x_d]$, un scalaire λ, un degré k, un monôme $\mathbf{x}^\alpha$ de degré au plus k et un rang n_0 à partir duquel les coefficients des monômes de degré au plus k coïncident dans f_n et f d'une part et dans g_n et g d'autre part. Alors, en notant $(h\,|\,\mathbf{x}^\alpha) = h_\alpha$ le coefficient de $\mathbf{x}^\alpha$ dans un polynôme h, on a à partir de ce même n_0 :

$$(\lambda f_n\,|\,\mathbf{x}^\alpha) = \lambda\,(f_n\,|\,\mathbf{x}^\alpha) = \lambda\,(f\,|\,\mathbf{x}^\alpha) = (\lambda f\,|\,\mathbf{x}^\alpha),$$

car $(f_n\,|\,\mathbf{x}^\alpha) = (f\,|\,\mathbf{x}^\alpha)$, puis

$$(f_n+g_n\,|\,\mathbf{x}^\alpha) = (f_n\,|\,\mathbf{x}^\alpha) + (g_n\,|\,\mathbf{x}^\alpha) = (f\,|\,\mathbf{x}^\alpha) + (g\,|\,\mathbf{x}^\alpha) = (f+g\,|\,\mathbf{x}^\alpha),$$

car $(f_n\,|\,\mathbf{x}^\alpha) = (f\,|\,\mathbf{x}^\alpha)$ et $(g_n\,|\,\mathbf{x}^\alpha) = (g\,|\,\mathbf{x}^\alpha)$, et enfin

$$(f_n g_n\,|\,\mathbf{x}^\alpha) = \sum_{\beta+\gamma=\alpha} \left(f_n\,\middle|\,\mathbf{x}^\beta\right)\left(g_n\,|\,\mathbf{x}^\gamma\right) = \sum_{\beta+\gamma=\alpha} \left(f\,\middle|\,\mathbf{x}^\beta\right)\left(g\,|\,\mathbf{x}^\gamma\right) = \left(fg\,|\,\mathbf{x}^\alpha\right),$$

car pour (β,γ) tel que $\beta+\gamma=\alpha$, les degrés $\deg(\mathbf{x}^\beta)$ et $\deg(\mathbf{x}^\gamma)$ sont au plus égaux à k, et donc

$$\left(f_n\,\middle|\,\mathbf{x}^\beta\right) = \left(f\,\middle|\,\mathbf{x}^\beta\right) \qquad \text{et} \qquad \left(g_n\,|\,\mathbf{x}^\gamma\right) = \left(g\,|\,\mathbf{x}^\gamma\right).$$

On en déduit que les suites $(\lambda f_n)_n$, $(f_n+g_n)_n$ et $(f_n g_n)_n$ tendent respectivement vers λf, $f+g$ et fg, ce qui montre que les opérations de $\mathbb{K}$-algèbre sont continues sur $\mathbb{K}[x_1,\cdots,x_d]$. Ainsi, ces opérations s'étendent par passage à la limite sur $\mathbb{K}[[x_1,\cdots,x_d]]$: étant donnés $\lambda\in\mathbb{K}$ et des suites de polynômes $(f_n)_n$ et $(g_n)_n$ tendant vers des séries f et f, on pose

$$\lambda f = \lim(\lambda f_n), \quad f+g = \lim(f_n+g_n), \quad fg = \lim(f_n g_n).$$

Ces opérations reviennent respectivement à multiplier les coefficients de la série f par λ, à sommer les coefficients d'un même monôme des séries f et g et à sommer les produits des coefficients donnant un même monôme dans f et g.

Avant de s'intéresser à la structure d'anneau de $\mathbb{K}[[x_1,\cdots,x_d]]$, on s'intéresse à structure d'espace vectoriel, qui est bien défini puisque l'on sait sommer deux séries et les multiplier par des scalaires.

Proposition 3.1.1. *En tant qu'espace vectoriel,* $\mathbb{K}[[x_1,\cdots,x_d]]$ *s'identifie au dual de* $\mathbb{K}[x_1,\cdots,x_d]$.

Démonstration. Il s'agit de construire un isomorphisme d'espace vectoriels entre $\mathbb{K}[[x_1,\cdots,x_d]]$ et le dual $\mathbb{K}[x_1,\cdots,x_d]^\star$ des polynômes. Pour cela, $\mathbb{K}[x_1,\cdots,x_d]$ ayant une base composée de l'ensemble des monômes

$$[x_1,\cdots,x_d] = \left\{\mathbf{x}^\alpha \;\middle|\; \alpha\in\mathbb{N}^d\right\},$$

et une forme linéaire étant déterminée uniquement par l'image des vecteurs d'une base, il suffit de construire une application linéaire

$$\varphi : \mathbb{K}[[x_1,\cdots,x_d]] \to \mathscr{F}([x_1,\cdots,x_d],\mathbb{K}),$$

où $\mathscr{F}([x_1,\cdots,x_d],\mathbb{K})$ est l'ensemble des fonctions de $[x_1,\cdots,x_d]$ dans $\mathbb{K}$, muni des opérations d'espace vectoriel point par point, *i.e.*, pour $f,g\in\mathscr{F}([x_1,\cdots,x_d],\mathbb{K})$ et $\lambda\in\mathbb{K}$, on a pour tout $\mathbf{x}^\alpha\in[x_1,\cdots,x_d]$:

$$(f+\lambda g)(\mathbf{x}^\alpha) = f(\mathbf{x}^\alpha) + \lambda g(\mathbf{x}^\alpha).$$

On se donne une série formelle f correspondant à une suite de Cauchy de polynômes $(f_n)_n$, si bien que pour chaque monôme $\mathbf{x}^\alpha$, le scalaire $\left(f_n\,\middle|\,\mathbf{x}^\alpha\right)$ est constant à partir d'un certain rang; en effet, si ce n'était pas le cas, il existerait une infinité d'entiers $m\geq n$ tels que $\left(f_n\,\middle|\,\mathbf{x}^\alpha\right) \neq \left(f_m\,\middle|\,\mathbf{x}^\alpha\right)$, *i.e.*, tels que

$$\operatorname{dist}(f_n,f_m) \geq \frac{1}{2^{|\alpha|}},$$

de sorte que $\operatorname{dist}(f_n, f_m)$ ne tendrait pas vers 0. On définit $\varphi(f)$ par : pour tout $\mathbf{x}^\alpha \in [x_1, \cdots, x_d]$, on pose

$$\varphi(f)\left(\mathbf{x}^\alpha\right) = \left(f_n \,\middle|\, \mathbf{x}^\alpha\right),$$

où n est un rang suffisamment grand tel que la suite $\left(\left(f_n \,\middle|\, \mathbf{x}^\alpha\right)\right)_n$ soit constante. Cette définition ne dépend pas du choix de la suite $(f_n)_n$ tendant vers f d'après la notion de suite de Cauchy équivalentes ; en effet si on se donne une suite de Cauchy $(f'_n)_n$ équivalente à $(f_n)_n$, alors $\operatorname{dist}(f_n, f'_n) \to 0$ quand $n \to \infty$, et donc pour tout monôme $\mathbf{x}^\alpha$, il existe un rang à partir duquel $\left(f_n \,\middle|\, \mathbf{x}^\alpha\right) = \left(f'_n \,\middle|\, \mathbf{x}^\alpha\right)$. L'application φ est linéaire car étant données des suites de Cauchy de polynômes $(f_n)_n$ et $(g_n)_n$ tendant vers des séries f et g, un scalaire λ et un monôme $\mathbf{x}^\alpha$, on a $\left(f_n + \lambda g_n \,\middle|\, \mathbf{x}^\alpha\right) = \left(f_n \,\middle|\, \mathbf{x}^\alpha\right) + \lambda\left(g_n \,\middle|\, \mathbf{x}^\alpha\right)$, et donc

$$\varphi\left(f + \lambda g\right)\left(\mathbf{x}^\alpha\right) = \varphi(f)\left(\mathbf{x}^\alpha\right) + \lambda\varphi(g)\left(\mathbf{x}^\alpha\right).$$

Cette égalité étant vraie pour tout monôme, on a $\varphi(f + \lambda g) = \varphi(f) + \lambda\varphi(g)$. Pour montrer que φ est un isomorphisme, il suffit de constater que son inverse est donnée par

$$\varphi^-(f) = (f_n)_n,$$

où la suite de polynômes $(f_n)_n$ est définie par

$$f_n = \sum_{|\alpha| \leq n} f\left(\mathbf{x}^\alpha\right)\mathbf{x}^\alpha.$$

Il s'agit bien d'une suite de Cauchy puisque, pour $n \geq m$, on a $f_n - f_m = 0$ ou $\operatorname{val}(f_n - f_m) = m + 1$, et donc $\operatorname{dist}(f_n, f_m) \to 0$ quand $n, m \to \infty$. Le fait que φ^- est bien l'inverse de φ découle d'un calcul élémentaire. □

Remarque 3.1.2. La démonstration de la proposition 3.1.1, permet de donner un sens algébrique à l'expression (1) :

$$f = \sum_{\alpha \in \mathbb{N}^d} \left(f \,\middle|\, \mathbf{x}^\alpha\right)\mathbf{x}^\alpha = \sum_{\alpha \in \mathbb{N}^d} f_\alpha \mathbf{x}^\alpha.$$

En effet, en tant qu'élément de $\mathscr{F}([x_1, \cdots, x_d], \mathbb{K})$, f est la fonction définie par

$$f\left(\mathbf{x}^\alpha\right) = \left(f \,\middle|\, \mathbf{x}^\alpha\right) = f_\alpha.$$

La donnée d'une telle fonction $\mathbf{x}^\alpha \mapsto f_\alpha$ peut s'écrire sous forme condensée comme dans (1).

3.2 Idéaux de séries formelles

On s'intéresse maintenant à la structure d'anneau de $\mathbb{K}[[x_1, \cdots, x_d]]$. Tout d'abord, $\mathbb{K}[[x_1, \cdots, x_d]]$ est un *anneau local, i.e.*, il admet un unique idéal maximal, à savoir l'idéal $(x_1, \cdots, x_d)$ engendré par les indéterminées. Pour montrer ce résultat, on a besoin de la proposition suivante.

Proposition 3.2.1. *Une série formelle f est inversible si et seulement si $\left(f \,\middle|\, 1\right) \neq 0$,* i.e.*, si et seulement si le coefficient constant de f est non nul.*

Démonstration. Tout d'abord, si f est inversible d'inverse g, on a $fg = 1$ et donc

$$1 = \left(fg \,\middle|\, 1\right) = \left(f \,\middle|\, 1\right)\left(g \,\middle|\, 1\right),$$

donc $\left(f \,\middle|\, 1\right)$ est non nul, d'inverse $\left(g \,\middle|\, 1\right)$. Pour la réciproque, on commence par supposer que $\left(f \,\middle|\, 1\right) = 1$, et on construit l'inverse g de f par l'intermédiaire d'une suite de Cauchy $(g_n)_n$. Pour $n = 0$, on pose

$$g_0 = 1,$$

si bien que

$$fg_0 = f = 1 + (f-1) = 1 + \sum_{|\alpha|\geq 1} (f \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha = 1 + h^{(\geq 1)},$$

où étant donné un entier k, $h^{(\geq k)}$ désigne une série formelle de valuation au moins k, *i.e.*, dont tous les monômes figurant avec un coefficient non nul sont de degré au moins k. Pour $n = 1$, on pose

$$g_1 = g_0 - \sum_{i=1}^{d} (f \,|\, x_i)\, x_i = 1 - \sum_{i=1}^{d} (f \,|\, x_i)\, x_i,$$

de sorte que

$$\begin{aligned} fg_1 &= \left(1 + \sum_{i=1}^{d} (f \,|\, x_i)\, x_i + \sum_{|\alpha|\geq 2} (f \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right)\left(1 - \sum_{i=1}^{d} (f \,|\, x_i)\, x_i\right) \\ &= 1 + \sum_{i=1}^{d} (f \,|\, x_i)\, x_i - \sum_{i=1}^{d} (f \,|\, x_i)\, x_i + h^{(\geq 2)} \\ &= 1 + h^{(\geq 2)}. \end{aligned}$$

On suppose maintenant que $g_1, \cdots, g_n$ sont construits, que pour $0 \leq k \leq n-1$, g_{k+1} est de la forme

$$g_{k+1} = g_k + h^{(k+1)},$$

où $h^{(k+1)}$ est un polynôme homogène de degré $k+1$ et que fg_n est de la forme

$$fg_n = 1 + h^{(\geq n+1)}. \tag{2}$$

En posant $h^{(n+1)}$ la composante homogène de degré $n+1$ de $fg_n - 1$:

$$h^{(n+1)} = \sum_{|\alpha|=n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha,$$

et en utilisant que les monômes de degré au plus n figurent avec un coefficient nul dans $fg_n - 1$, on a

$$\begin{aligned} f\left(g_n - h^{(n+1)}\right) &= fg_n - fh^{(n+1)} \\ &= 1 + (fg_n - 1) - f\left(\sum_{|\alpha|=n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) \\ &= 1 + \left(\sum_{|\alpha|\geq n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) - \left(1 + \sum_{|\alpha|\geq 1} (f \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right)\left(\sum_{|\alpha|=n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) \\ &= 1 + \left(\sum_{|\alpha|=n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) + \left(\sum_{|\alpha|\geq n+2} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) - \left(\sum_{|\alpha|=n+1} (fg_n - 1 \,|\, \mathbf{x}^\alpha)\mathbf{x}^\alpha\right) + h^{(\geq n+2)} \\ &= 1 + \tilde{h}^{(\geq n+2)}. \end{aligned}$$

Ainsi, en posant $g_{n+1} = g_n - h^{(n+1)}$, on a

$$fg_{n+1} = 1 + \tilde{h}^{(\geq n+2)}.$$

On donc construit une suite de polynômes $(g_n)_n$ qui, d'après (2), est une suite de Cauchy, donc converge vers une série g. Toujours d'après (2), et en utilisant que $(g \,|\, \mathbf{x}^\alpha) = (g_n \,|\, \mathbf{x}^\alpha)$ pour tout monôme $\mathbf{x}^\alpha$ de degré au plus n, on obtient que $fg = 1$, *i.e.*, g est bien l'inverse de f. Maintenant, si f est une série avec coefficient constant $(f \,|\, 1)$ non nul, alors la série

$$f' = \frac{1}{(f \,|\, 1)} f,$$

vérifie $(f' \mid 1) = 1$, donc d'après la construction précédente admet une inverse g' et en posant

$$g = \frac{1}{(f \mid 1)} g',$$

on a

$$fg = (f \mid 1) f' \left(\frac{1}{(f \mid 1)} g' \right) = f'g' = 1,$$

de sorte que f est inversible d'inverse g. □

On peut maintenant montrer que $\mathbb{K}[[x_1, \cdots, x_d]]$ est effectivement un anneau local.

Théorème 3.2.2. *L'anneau $\mathbb{K}[[x_1, \cdots, x_d]]$ est un anneau local, dont l'unique idéal maximal est $(x_1, \cdots, x_d)$.*

Démonstration. On rappelle qu'un anneau commutatif A est local d'unique idéal maximal $\mathfrak{m}$ si et seulement si $0 \neq 1$ et que la somme de deux éléments non inversible est non inversible ; de plus $\mathfrak{m}$ est composé des éléments non inversibles de A. Or, d'après la proposition 3.2.1, les éléments non inversibles de $\mathbb{K}[[x_1, \cdots, x_d]]$ sont les séries dont le terme constant est nul, et la somme de deux séries dont les termes constants sont nul a un terme constant nul. Ainsi, $\mathbb{K}[[x_1, \cdots, x_d]]$ est local et son idéal maximal est composé des séries dont le terme constant est nul, *i.e.*, il s'agit de l'idéal $(x_1, \cdots, x_d)$. □

On termine cette section en énonçant sans le démontrer un résultat répondant à une question naturelle. Comme anneau, $\mathbb{K}[[x_1, \cdots, x_d]]$ admet des idéaux et comme espace topologique, $\mathbb{K}[[x_1, \cdots, x_d]]$ a des ouverts et des fermés. On peut alors se demander si les idéaux vérifient des propriétés topologiques, dont la réponse est donnée par le résultat suivant.

Théorème 3.2.3 ([5])**.** *Tout idéal de $\mathbb{K}[[x_1, \cdots, x_d]]$ est fermé pour la topologie $(x_1, \cdots, x_d)$-adique.*

Une démonstration constructive de ce résultat apparaît dans [3].

4. Bases standards et réécriture

Les bases standards sont les analogues pour les séries formelles des bases de Gröbner pour les polynômes. On commence par faire quelques rappels sur les bases de Gröbner avant de présenter les bases standards.

4.1 Rappels sur les bases de Gröbner

Les bases de Gröbner permettent de réaliser les calculs avec des polynômes dans des logiciels de calcul formel. L'un de leurs nombreux intérêts est en effet de résoudre des systèmes d'équations polynomiales par une procédure analogue à l'algorithme de Gauss pour les systèmes linéaires. L'algorithme de Gauss consiste à trianguler le système considéré afin d'exprimer chaque indéterminée x_i en fonction des indéterminées x_j, avec $j < i$, puis de résoudre le système en calculant x_2 en fonction de x_1 (qui peut prendre une valeur unique ou paramétrique), puis x_3 en fonction de x_1, x_2, *etc* $\cdots$. Pour les systèmes polynomiaux, on peut adapter cet méthode en ordonnant les monômes et en exprimant grâce aux équations du système chaque monôme en fonction des monômes qui lui sont inférieurs, puis de résoudre itérativement le système triangulé obtenu. Or, si en une seule variable les monômes sont naturellement

ordonnés par le degré, il n'existe pas d'ordre naturel en plusieurs variables. Les ordres monomiaux ont été introduits pour régler ce problème.

On fixe comme précédemment une algèbre de polynômes $\mathbb{K}[x_1, \cdots, x_d]$, et on rappelle que l'ensemble des monômes est noté :

$$[x_1, \cdots, x_d] = \left\{ \mathbf{x}^\alpha \mid \alpha \in \mathbb{N}^d \right\}.$$

Définition 4.1.1. Un *ordre monomial* sur $[x_1, \cdots, x_d]$ est un ordre total $\prec$ sur $[x_1, \cdots, x_d]$, compatible à la multiplication monomiale et tel que 1 soit inférieur à tous les autres monômes :

$$\forall \alpha, \beta, \gamma \in \mathbb{N}^d : \quad \left(\mathbf{x}^\beta \prec \mathbf{x}^\gamma \right) \Rightarrow \left(\mathbf{x}^{\alpha+\beta} \prec \mathbf{x}^{\alpha+\gamma} \right) \qquad \text{et} \qquad \forall \alpha \in \mathbb{N}^d \setminus \{(0, \cdots, 0)\} : \quad 1 \prec \mathbf{x}^\alpha.$$

Une fois l'ordre monomial fixé, tout polynôme non nul $f \in \mathbb{K}[x_1, \cdots, x_d]$ s'écrit sous la forme :

$$f(x_1, \cdots, x_d) = \mathrm{lc}(f)\,\mathrm{lm}(f) - \mathrm{rem}(f),$$

où $\mathrm{lm}(f) \in [x_1, \cdots, x_d]$ est le plus grand monôme figurant dans f, $\mathrm{lc}(f)$ est son coefficient et $\mathrm{rem}(f)$ est l'opposé des termes plus petits que $\mathrm{lm}(f)$ figurant dans f. Le monôme $\mathrm{lm}(f)$, le coefficient $\mathrm{lc}(f)$ et le polynôme $\mathrm{rem}(f)$ sont respectivement appelés *monôme dominant*, *coefficient dominant* et *reste* de f.

Exemple 4.1.2. On considère trois variables $\{x, y, z\}$ et $\prec$ l'ordre *lexicographique* induit par $z \prec y \prec x$, *i.e.*,

$$x^\alpha y^\beta z^\gamma \prec x^{\alpha'} y^{\beta'} z^{\gamma'} \quad \text{ssi} \quad \begin{cases} \alpha < \alpha' & \text{ou} \\ \alpha = \alpha', \beta < \beta' & \text{ou} \\ \alpha = \alpha', \beta = \beta', \gamma < \gamma'. \end{cases}$$

On considère de nouveau les polynômes :

$$f(x, y, z) = 1 + 3z + 2xy, \quad g(x, y, z) = 3z + 5y^2, \quad h(x, y, z) = 2x + yz.$$

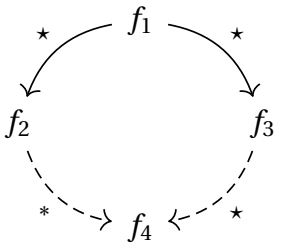
On a

$$\mathrm{lc}(f)\,\mathrm{lm}(f) = 2xy, \quad \mathrm{lc}(g)\,\mathrm{lm}(g) = 5y^2, \quad \mathrm{lc}(h)\,\mathrm{lm}(h) = yz.$$

On peut maintenant définir les bases de Gröbner.

Définition 4.1.3. Une famille de polynômes G est une *base Gröbner* de l'idéal I qu'elle engendre si pour tout $f \in I \setminus \{0\}$, il existe $g \in G$ tel que $\mathrm{lm}(g)$ divise $\mathrm{lm}(f)$.

Cette définition abstraite caractérise une propriété calculatoire très puissante, appelée *confluence* et représentée par le diagramme suivant :



(3)

Les flèches représentent intuitivement des suites de calculs élémentaires, appelés *étapes de réécriture*, où on remplace un monôme dominant d'un $g \in G$ par $\mathrm{rem}(g)/\mathrm{lc}(g)$. Par exemple, pour deux variables $\{x, y\}$, l'ordre lexicographique induit par $y \prec x$ et l'ensemble de polynômes $G = \{g_1, g_2, g_3\}$, où

$$g_1(x, y) = x^2 - y, \quad g_2(x, y) = xy - x, \quad g_3(x, y) = -y^2 + y,$$

alors, on a l'étape de réécriture

$$f(x,y) = x^2y + 2xy + 1 \to_{yg_1} 2xy + y^2 + 1, \tag{4}$$

car on a remplacé le monôme $x^2y = y\,\mathrm{lm}(g_1)$ figurant dans $f(x,y)$ par $y\,\mathrm{rem}(g_1) = y^2$, l'indice yg_1 signifiant que l'on a dû multiplier $g_1(x,y)$ par y pour réaliser cette étape de réécriture. Les étoiles $\star$ dans le diagramme (3) signifient qu'on peut enchaîner plusieurs étapes de réécriture, par exemple, reprenant l'exemple précédent, on a $f(x,y) \xrightarrow{\star} 2x + y + 1$ car

$$f(x,y) \to_{yg_1} 2xy + y^2 + 1 \to_{2g_2} 2x + y^2 + 1 \to_{-g_3} 2x + y + 1. \tag{5}$$

En effet, dans la deuxième étape, on a remplacé $2xy = 2\,\mathrm{lm}(g_2)$ par $2x = 2\,\mathrm{rem}(g_2)$ et dans la troisième, on a remplacé $y^2 = -\,\mathrm{lm}(g_3)$ par $y = -\,\mathrm{rem}(g_3)$. Enfin, la propriété de confluence schématisée dans (3), signifie que les calculs sont déterministes, *i.e.*, le résultat final ne dépend pas des calculs intermédiaires. Par exemple, au lieu d'éliminer x^2y en utilisant $yg_1(x,y)$ dans la première étape (4), on aurait pu éliminer le même monôme en utilisant $xg_2(x,y)$. Cela aurait alors induit la suite de réécriture

$$f(x,y) = x^2y + 2xy + 1 \to_{xg_2} x^2 + 2xy + 1 \to_{g_1} 2xy + y + 1 \to_{2g_2} 2x + y + 1,$$

ce qui donne bien le même résultat final que (5). On réfère à [1] pour la démonstration que les bases de Gröbner caractérisent la confluence.

On finit cette section sur les bases de Gröbner en illustrant leur intérêt pour la résolution de systèmes polynomiaux, tiré de [4, Section 3.1] : on cherche à résoudre sur $\mathbb{C}^3$ le système

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1. \end{cases} \tag{6}$$

Les équations de (6) engendrent un idéal de $\mathbb{C}[x,y,z]$, dont on peut calculer une base de Gröbner relativement à l'ordre lex induit par $z \prec y \prec x$. Il s'avère que les solutions d'un système d'équations polynomiales ne dépendent que de l'idéal qu'elles engendrent, si bien que les solutions de (6) sont les mêmes que celles du système induit par une base de Gröbner, et dans ce cas, ce dernier s'exprime de la façon suivante :

$$\begin{cases} x + y + z^2 = 1 \\ y^2 - y - z^2 + z = 0 \\ 2yz^2 + z^4 - z^2 = 0 \\ z^6 - 4z^4 + 4z^3 - z^2 = 0. \end{cases} \tag{7}$$

Alors, les solutions $\mathbf{x} = (a,b,c) \in \mathbb{C}^3$ de (7) doivent vérifier que c est solution de $z^6 - 4z^4 + 4z^3 - z^2$. En remarquant que ce polynôme admet 0 et 1 comme racines doubles, on montre que c peut prendre les valeurs $0, 1$ et $-1 \pm \sqrt{2}$. En remplaçant successivement z par ces valeurs dans les deux équations ne faisant intervenir que y et z, à savoir $2yz^2 + z^4 - z^2 = 0$ et $y^2 - y - z^2 + z = 0$, on en déduit les valeurs que b peut prendre en fonction de c. Finalement, en remplaçant le couple (y,z) par les couples (b,c) calculés à partir des trois équations du bas dans la première équation $x + y + z^2 = 1$, on trouve la valeur de a. En notant $\alpha = -1 \pm \sqrt{2}$, on obtient que le système (7), et donc le système (6), admet les 5 solutions :

$$(1,0,0), \qquad (0,1,0), \qquad (0,0,1), \qquad (\alpha,\alpha,\alpha).$$

On réfère à [4] pour des exemples d'applications des bases de Gröbner.

4.2 Bases standards et confluence topologique

On fixe une algèbre de séries formelles $\mathbb{K}[[x_1,\cdots,x_d]]$ et un ordre monomial $\prec$. L'*ordre opposé* de $\prec$, noté $\prec_{\text{op}}$, est défini par $\mathbf{x}^\alpha \prec_{\text{op}} \mathbf{x}^\beta$ si $\mathbf{x}^\beta \prec \mathbf{x}^\alpha$. Comme pour les polynômes, on note $\text{lm}(f)$ le plus grand monôme pour $\prec_{\text{op}}$ figurant dans une série non nulle f et $\text{lc}(f)$ son coefficient. Il est naturel de considérer l'ordre opposé pour deux raisons :

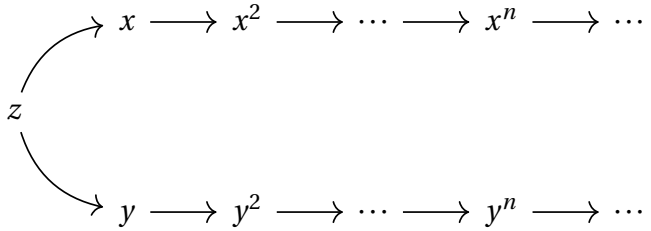
- si la série est infinie, alors elle n'a pas de plus grand monôme pour $\prec$, en revanche elle en a un plus petit, *i.e.*, le monôme dominant est bien défini pour l'ordre opposé uniquement,
- les séries formelles peuvent être pensées comme des développements de Taylor, pour lesquels ce sont les monômes de petits degrés qui ont un rôle dominant, or en général, on considère un ordre $\prec$ qui est compatible au degré, et donc les monômes de petits degrés sont plus grands pour $\prec_{\text{op}}$.

Définition 4.2.1. Une famille de séries formelles S est une *base standard* de l'idéal I qu'elle engendre si pour tout $f \in I \setminus \{0\}$, il existe $g \in S$ telle que $\text{lm}(g)$ divise $\text{lm}(f)$.

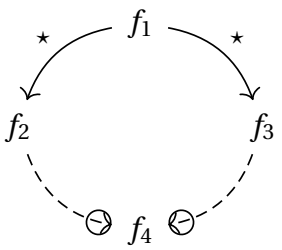
Comme pour les bases de Gröbner, la définition abstraite de base standard caractérise une propriété calculatoire fondamentale. On commence par noter qu'il ne s'agit pas de confluence car les séries formelles, comme illustré sur l'exemple suivant : on considère l'ensemble G composé des séries formelles

$$g_1(x,y,z) = z - x, \quad g_2(x,y,z) = z - y, \quad g_3(x,y,z) = x - x^2, \quad g_4(x,y,z) = y - y^2.$$

Ces 4 séries engendrent un idéal I dont aucune série ne contient de terme constant. Or, pour un ordre monomial $\prec$ tel que $x \prec_{\text{op}} y \prec_{\text{op}} z$, on a $\text{lm}\left(g_1\right) = \text{lm}\left(g_2\right) = z$, $\text{lm}\left(g_3\right) = x$ et $\text{lm}\left(g_4\right) = y$, ce qui permet de conclure que G est une base standard. Or, on a les réécritures $z \to y$, $z \to x$, $y \to y^2$ et $x \to x^2$, de sorte que



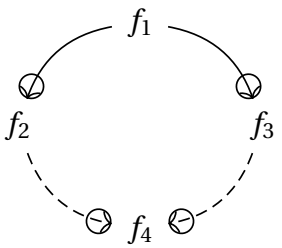
et ce diagramme ne se refermera jamais, de sorte que la relation de réécriture $\to$ n'est pas confluente. En revanche, les deux suites $(x^n)_n$ et $\left(y^n\right)_n$ tendent vers 0 pour la topologie $(x_1,\cdots,x_d)$-adique de sorte que la propriété de confluence est en fait atteinte à la limite. Cette notion de confluence est appelée *confluence topologique* et représentée par le diagramme :



(8)

où $g \multimap g'$ signifie que g peut se réécrire en un nombre fini d'étapes arbitrairement proche de g' pour la distance dist. Dans [2], il est montré que les bases standards caractérisent la confluence topologique. Si la propriété de confluence topologique apparaît naturellement dans l'étude des bases standards, en informatique, dans le cadre des réécritures infinies apparaît une autre notion de confluence, dite

confluence infinitaire, représentée par le diagramme



(9)

Cette propriété est en général plus forte que la confluence topologique, car si $f_1 \xrightarrow{\star} f_2$ et $f_1 \xrightarrow{\star} f_3$ comme dans (8), alors on a $f_1 \multimap f_2$ et $f_1 \multimap f_3$ comme dans (9). Ainsi, si on peut refermer les diagrammes de la forme (9), on peut *a fortiori* refermer les diagrammes de la forme (8). Dans [3], il est montré que en général, *i.e.*, pour des systèmes de réécriture quelconques ne portant pas nécessairement sur des séries formelles, la confluence infinitaire est strictement plus forte que la confluence topologique. Le second résultat principal [3], est de montrer que dans le cas des réécritures sur les séries formelles, ces deux propriétés de confluence sont en fait équivalentes et caractérisent donc les bases standards.

Références

[1] Franz BAADER et Tobias NIPKOW : *Term rewriting and all that*. Cambridge University Press, Cambridge, 1998.

[2] Cyrille CHENAVIER : Topological rewriting systems applied to standard bases and syntactic algebras. *J. Algebra*, 550:410–431, 2020.

[3] Cyrille CHENAVIER, Thomas CLUZEAU et Adya MUSSON-LEYMARIE : Topological closure of formal power series ideals and application to topological rewriting theory. *arXiv preprint arXiv :2402.05511*, 2024.

[4] David A. COX, John LITTLE et Donal O'SHEA : *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth édition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[5] Oscar ZARISKI et Pierre SAMUEL : *Commutative algebra. Vol. II*, volume Vol. 29 de *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1975. Reprint of the 1960 edition.