Solutions exactes et solutions approchées d'équations polynomiales

François Loeser (*Université Paris 6*)

1. – Préliminaires et présentation du problème

On considère dans ce texte des systèmes d'équations polynomiales à coefficients dans le corps $\mathbb{C}$ des nombres complexes. Un tel système correspond à la donnée de r polynômes $F_1, \ldots, F_r$ appartenant à l'algèbre $\mathbb{C}[x_1, \ldots, x_m]$ des polynômes en m variables à coefficients complexes. On note $Z(F)$ l'ensemble des solutions dans $\mathbb{C}^m$ du système

$$(F) = \begin{cases} F_1(x_1, \ldots, x_m) = 0 \\ \cdots \\ F_r(x_1, \ldots, x_m) = 0. \end{cases}$$

Une partie de $\mathbb{C}^m$ de la forme $Z(F)$ est appelée *sous-ensemble algébrique* de $\mathbb{C}^m$.

On peut également s'intéresser aux séries qui sont solutions du système (F). Plus précisément, on considère l'ensemble des m-uplets de séries formelles, ou « arcs formels »,

$$x_i(t) = \sum_{j \in \mathbb{N}} a_{i,j} t^j,$$

avec $a_{i,j}$ appartenant à $\mathbb{C}$, qui sont solutions du système (F), c'est-à-dire telles que les séries $F_k(x_1(t), \ldots, x_m(t))$ obtenues par substitution soient identiquement nulles pour $1 \leqslant k \leqslant r$. On note $Z_\infty(F)$ ce sous-ensemble de $\mathbb{C}[[t]]^m$. On pourrait aussi considérer les séries convergentes qui sont solutions du système (F), mais, pour ce qui nous concerne ici, la recherche de solutions convergentes est essentiellement équivalente à celle de solutions formelles, au vu du résultat suivant de M. Artin :

Théorème 1.1 ([1]). *Soit $(x_1(t), \ldots, x_m(t))$ un m-uplet de séries formelles solution du système (F). Pour tout entier $n \geqslant 0$, il existe un m-uplet de séries convergeant au voisinage de l'origine, $(\tilde{x}_1(t), \ldots, \tilde{x}_m(t))$, solution du système (F), et vérifiant*

$$x_i(t) \equiv \tilde{x}_i(t) \mod t^{n+1},$$

pour $1 \leqslant i \leqslant m$.

Comment trouver les solutions séries formelles du système (F) ? L'approche naturelle consiste à procéder par approximations successives : à partir d'une solution approchée donnée, disons modulo t^{n+1}, c'est-à-dire d'un m-uplet de séries formelles $(x_1(t), \ldots, x_m(t))$ telles que les séries $F_k(x_1(t), \ldots, x_m(t))$ obtenues par substitution soient toutes divisibles par t^{n+1}, on cherche à construire une solution modulo t^{n+2}. Comme le fait d'être une solution approchée modulo t^{n+1} ne dépend clairement pas des termes d'ordre $\geqslant n+1$ apparaissant dans les

séries $x_i(t)$, il sera plus commode de considérer les solutions approchées modulo t^{n+1} comme des éléments de $(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m$, via le morphisme de troncation

$$\tau_n : \mathbb{C}[[t]]^m \to (\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m.$$

Pour $n' \geqslant n$, on dispose également d'un morphisme de troncation

$$\tau_{n',n} : (\mathbb{C}[t]/t^{n'+1}\mathbb{C}[t])^m \to (\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m.$$

Bien entendu, on a une identification naturelle $\mathbb{C}[t]/t^{n+1}\mathbb{C}[t] \simeq \mathbb{C}^{n+1}$. On note $Z_n(F)$ le sous-ensemble de $(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m$ formé des solutions approchées de (F) modulo t^{n+1}. Pour une solution approchée modulo t^{n+1}, se relever en une vraie solution est par définition équivalent à être dans l'image de $Z_\infty(F)$ par τ_n ; de même se relever en une solution approchée modulo $t^{n'+1}$ équivaut à être dans l'image de $Z_{n'}(F)$ par $\tau_{n',n}$. On remarquera que, avec nos notations, $Z_0(F)$ s'identifie naturellement à $Z(F)$.

Il est important de remarquer que, en général, une solution approchée modulo t^{n+1} ne se relève pas nécessairement en une solution approchée modulo t^{n+2}. En effet, considérons le système F composé uniquement de l'équation à 2 variables $x_1^2 - x_2^3 = 0$: le couple $(x_1(t) = t, x_2(t) = t)$ est une solution approchée modulo t^2 qui n'admet aucun relèvement en une solution approchée modulo t^3 (et encore moins en une vraie solution !). Ceci est lié au fait que l'origine est un point singulier de la courbe d'équation $x_1^2 - x_2^3 = 0$ dans $\mathbb{C}^2$; plus généralement, pour F quelconque, l'obstruction à relever les solutions approchées provient des points singuliers de $Z(F)$, c'est-à-dire des points au voisinage desquels $Z(F)$ n'est pas une variété analytique complexe.

En théorie, il est facile de tester si une solution approchée modulo t^{n+1} se relève ou non modulo $t^{n'+1}$: on part d'une solution approchée $(x_1^0(t), \dots x_m^0(t))$ modulo t^{n+1}, vue comme m-uplet de polynômes de degré $\leqslant n$, on considère un m-uplet $(x_1(t), \dots x_m(t))$ de polynômes de degré $\leqslant n'$ se projetant sur $(x_1^0(t), \dots x_m^0(t))$, et on développe les séries $F_i(x_1(t), \dots x_m(t))$ à l'ordre n'. La condition pour ces séries d'être nulles à l'ordre n' se traduit par un nombre fini d'équations polynomiales portant sur les $m(n - n')$ coefficients indéterminés. Le relèvement existe si et seulement si ce système admet une solution dans $\mathbb{C}^{m(n-n')}$.

D'après le résultat fondamental suivant, dû à M. Greenberg, pour savoir si une solution approchée modulo t^{n+1} se relève en une **vraie** solution, il suffit de savoir si elle se relève en une solution approchée modulo $t^{\gamma(n)+1}$, avec $\gamma(n)$ un entier $\geqslant n$ ne dépendant que de n et de (F), ce qui peut être vérifié par la méthode précédente.

Théorème 1.2 ([6]). *Pour tout entier $n \geqslant 0$, il existe un entier $\gamma(n) \geqslant n$, ne dépendant que de (F), tel que*

$$\tau_n(Z_\infty(F)) = \tau_{\gamma(n),n}(Z_{\gamma(n)}(F)).$$

De plus, il est possible de choisir la fonction $n \mapsto \gamma(n)$ majorée par une fonction affine de n.

L'objet de ce petit texte est d'essayer de raconter des résultats obtenus récemment sur la façon dont les ensembles $\tau_n(Z_\infty(F))$ varient avec n.

2. – Interlude : parties constructibles et semi-algébriques

En général, la projection d'un sous-ensemble algébrique de $\mathbb{C}^m$ n'est pas nécessairement algébrique. Ainsi la projection sur l'une des droites de coordonnées de l'hyperbole d'équation $x_1x_2 - 1$ dans $\mathbb{C}^2$ est égale à $\mathbb{C} \setminus \{0\}$, qui n'est certainement pas un sous-ensemble algébrique de $\mathbb{C}^2$. Pour pallier cette difficulté on introduit la notion de sous-ensemble *constructible* de $\mathbb{C}^m$. La famille des sous-ensembles constructibles de $\mathbb{C}^m$, $\mathcal{S}(\mathbb{C}^m)$, est la plus petite famille de parties de $\mathbb{C}^m$ contenant les sous-ensembles algébriques qui soit stable par intersection et réunion finie et passage au complémentaire (c'est la sous-algèbre de Boole de l'ensemble des parties de $\mathbb{C}^m$ engendrée par les sous-ensembles algébriques). Autrement dit, un sous-ensemble constructible de $\mathbb{C}^m$ est décrit par un ensemble fini de conditions de la forme $F_i = 0$ et $G_j \neq 0$ avec F_i et G_j des polynômes à coefficients complexes. D'après un théorème de C. Chevalley (en fait une version "moderne" de la théorie classique de l'élimination), l'image d'une partie constructible par une application polynomiale est toujours constructible : on a $\pi(\mathcal{S}(\mathbb{C}^m)) \subset \pi(\mathcal{S}(\mathbb{C}^{m'}))$ pour toute application polynomiale $\pi : \mathbb{C}^m \to \mathbb{C}^{m'}$. Considérons des parties constructibles Z et Z' de $\mathbb{C}^m$ et $\mathbb{C}^{m'}$ respectivement. On dit que Z et Z' sont *strictement isomorphes* s'il existe une application rationnelle (c'est à dire dont les composantes sont des fractions rationnelles) $F : Z \to Z'$ qui soit bijective et d'inverse F^{-1} également rationnelle. Avec cette définition, l'hyperbole d'équation $x_1x_2 - 1$ dans $\mathbb{C}^2$ est strictement isomorphe à $\mathbb{C} \setminus \{0\}$. S'il existe des partitions finies A_i, $i \in I$ et A'_i, $i \in I$ de Z et Z' respectivement en parties constructibles telles que, pour tout $i \in I$, A_i soit strictement isomorphe à A'_i, on dit que Z et Z' sont *isomorphes*

Le théorème de Chevalley reste valable lorsque $\mathbb{C}$ est remplacé par un corps algébriquement clos quelconque. En général, pour K un corps et m un entier $\geqslant 0$, on note $\mathcal{S}(K^m)$ la plus petite sous-algèbre de Boole de l'ensemble des parties de K^m contenant les parties algébriques de K^m (c'est à dire définies par des équations polynomiales à coefficients dans K), telle que $\pi(\mathcal{S}(K^m))$ soit contenu dans $\mathcal{S}(K^{m'})$ pour toute application polynomiale $\pi : K^m \to K^{m'}$. On remarquera que, nécessairement, les parties $Z_{F,n}$ définies par la condition « $F(x)$ est une puissance n-ième dans K », avec F un polynôme en m-variables à coefficients dans K, et n un entier $\geqslant 2$, doivent appartenir à $\mathcal{S}(K^m)$. Lorsque $K = \mathbb{R}$, il résulte du théorème de Tarski-Seidenberg que $\mathcal{S}(\mathbb{R}^m)$ est exactement l'algèbre de Boole engendrée par les parties de la forme $Z_{F,2}$, c'est à dire définies par la condition $F \geqslant 0$, avec F un polynôme à coefficients réels. Les éléments de $\mathcal{S}(\mathbb{R}^m)$ sont appelés parties semi-algébriques de $\mathbb{R}^m$. Ce sont les sous-ensembles décrits par un nombre fini de conditions de la forme $F_i = 0$, $G_j \geqslant 0$ et $H_k \neq 0$ avec F_i, G_j et H_k des polynômes à coefficients réels.

Bien que cela soit moins connu, il existe d'autres corps pour lesquels les ensembles $\mathcal{S}(K^m)$ admettent une description agréable. Considérons, par exemple, le corps $\mathbb{Q}_p$ des nombres p-adiques, pour p un nombre premier. C'est le complété de $\mathbb{Q}$ pour la norme p-adique $|x| = p^{-v_p x}$. Ici $v_p x$ désigne la valuation p-adique de x, c'est-à-dire l'exposant de p dans la décomposition en facteurs premiers de x. On convient que 0 a pour valuation ∞. Il résulte d'un théorème de Macintyre que $\mathcal{S}(\mathbb{Q}_p^m)$ est alors exactement l'algèbre de Boole engendrée par les $Z_{F,n}$. Pour se convaincre que les parties algébriques de $\mathbb{Q}_p^m$ appartiennent

bien à cette algèbre de Boole, on remarquera que, si F est un polynôme à coefficients dans $\mathbb{Q}_p$, F s'annule en un point a de $\mathbb{Q}_p$ si et seulement si $pF^2(a)$ est un carré. Les éléments de $\mathcal{S}(\mathbb{Q}_p^m)$ sont appelés semi-algébriques par analogie avec le cas réel. La démonstration originelle de Macintyre [7] utilisait la théorie des modèles et une démonstration élémentaire (sans logique) du théorème de Macintyre a été ultérieurement donnée par Denef [3].

Retournons maintenant à l'objet de cet exposé, à savoir les séries formelles. On considère le corps des fractions $K = \mathbb{C}((t))$ de l'anneau des séries formelles $\mathbb{C}[[t]]$. Les éléments de K sont de la forme $f = \sum_{i\in\mathbb{Z}} a_i t^i$ avec $a_i = 0$ pour $i \ll 0$. On note $\mathrm{ord}(f)$ l'ordre d'une telle série f, à savoir le plus petit i tel que a_i soit non nul et on pose $\mathrm{in}\,(f) = a_{\mathrm{ord}(f)}$. Lorsque f est la série nulle, on convient que $\mathrm{ord}(f) = \infty$ et que $\mathrm{in}\,(f) = 0$. Il résulte maintenant d'un théorème de Pas [9] que les éléments de $\mathcal{S}(K^m)$ appartiennent à l'algèbre de Boole engendrée par les parties définies par les conditions du type suivant

$$\mathrm{ord}F(x(t)) \geqslant \mathrm{ord}G(x(t)) + \ell \tag{2.1}$$

$$\mathrm{ord}F(x(t)) \equiv \ell \mod d \tag{2.2}$$

$$F(\mathrm{in}\,(G_1(x(t))), \ldots, \mathrm{in}\,(G_q(x(t)))) = 0 \tag{2.3}$$

portant sur un m-uplet $x(t)$ d'éléments de K. Ici F, G et les G_i sont des polynômes à coefficients dans K, d ainsi que ℓ sont des entiers. Si dans la définition de $\mathcal{S}(K^m)$ on ne considère que les parties algébriques de K^m définies par des équations polynomiales à coefficients dans $\mathbb{C}$ et des images de tels ensembles par des applications polynomiales à coefficients dans $\mathbb{C}$, on obtient une sous-algèbre de Boole $\mathcal{S}_0(K^m)$ de $\mathcal{S}(K^m)$. Il résulte également du théorème de Pas que les éléments de $\mathcal{S}_0(K^m)$ appartiennent à l'algèbre de Boole engendrée par les parties définies par les conditions du type (2.1), (2.2), (2.3) avec maintenant F, G et les G_i des polynômes à coefficients dans $\mathbb{C}$ et non plus dans $K = \mathbb{C}((t))$. Les éléments de cette algèbre de Boole seront appelés ensembles semi-algébriques.

3. – L'anneau universel associé aux ensembles constructibles

Il est possible de construire un anneau universel $\mathcal{M}$ à partir des ensembles constructibles de la façon suivante. À toute partie constructible Z de $\mathbb{C}^m$ (ici m est variable), on associe un symbole $[Z]$. On considère le quotient du groupe abélien libre engendré par ces symboles par les relations

$$[Z] = [Z'] \quad \text{si } Z \text{ est isomorphe à } Z'$$

et

$$[Z \cup Z'] = [Z] + [Z'] - [Z \cap Z'].$$

On obtient ainsi un groupe abélien que l'on note $\mathcal{M}$ et que l'on munit d'une structure d'anneau en posant $[Z][Z'] = [Z \times Z']$. On remarquera que l'unité est donnée par la classe d'un point. L'anneau $\mathcal{M}$ est universel dans le sens suivant : toute application F qui à un ensemble constructible Z associe un élément $F(Z)$ d'un anneau A qui ne dépend que de la classe d'isomorphisme de Z, est de plus additive (elle vérifie $F(Z \cup Z') = F(Z) + F(Z') - F(Z \cap Z')$) et multiplicative (elle vérifie $F(Z \times Z') = F(Z)F(Z')$) se factorise nécessairement à travers

$\mathcal{M}$. Un exemple de telle application est donné par la caractéristique d'Euler-Poincaré $\chi : \mathcal{M} \to \mathbb{Z}$, mais on peut en construire beaucoup d'autres. En fait, l'anneau $\mathcal{M}$ n'est pas encore tout à fait celui que l'on va utiliser. Appelons $\mathbb{L}$ la classe de la droite affine $\mathbb{C}$ dans $\mathcal{M}$. On va considérer l'anneau $\mathcal{M}_{\mathrm{loc}}$ obtenu en inversant formellement l'élément $\mathbb{L}$. En termes techniques c'est l'anneau localisé $\mathcal{M}[\mathbb{L}^{-1}]$. On a un morphisme naturel d'anneaux $\mathcal{M} \to \mathcal{M}_{\mathrm{loc}}$, mais a priori il n'est pas injectif : en effet deux éléments de $\mathcal{M}$ ont même image dans $\mathcal{M}_{\mathrm{loc}}$ s'il deviennent égaux après multiplication par une puissance adéquate de $\mathbb{L}$. Grosso modo regarder les ensembles constructibles dans $\mathcal{M}$ revient à les considérer « à découpage près », tandis que les regarder dans $\mathcal{M}_{\mathrm{loc}}$ revient à les considérer « à découpage et stabilisation par un espace affine près ».

4. – Les énoncés

Après tous ces détours, il est maintenant temps de revenir à notre question première : comment les ensembles $\tau_n(Z_\infty(F))$ varient-ils avec n ?

Pour cela commençons par remarquer que $\tau_n(Z_\infty(F))$ est une partie constructible de

$$(\mathbb{C}[t]/t^{n+1}\mathbb{C}[t])^m \simeq \mathbb{C}^{(n+1)m}.$$

En effet, par le théorème de Greenberg 1.2, $\tau_n(Z_\infty(F))$ est l'image par une application polynomiale d'un ensemble algébrique et est donc constructible d'après le théorème de Chevalley. On peut donc considérer la classe $[\tau_n(Z_\infty(F))]$ de $\tau_n(Z_\infty(F))$ dans l'anneau $\mathcal{M}_{\mathrm{loc}}$. Formons la série génératrice

$$P(T) := \sum_{n\in\mathbb{N}} [\tau_n(Z_\infty(F))]T^n$$

dans l'anneau $\mathcal{M}_{\mathrm{loc}}[[T]]$.

On a le résultat de rationalité suivant :

Théorème 4.1 ([4]). *Dans l'anneau $\mathcal{M}_{\mathrm{loc}}[[T]]$, la série génératrice $P(T)$ est égale à une combinaison linéaire à coefficients dans l'anneau de polynômes $\mathcal{M}_{\mathrm{loc}}[T]$ de séries de la forme $(1-\mathbb{L}^aT^b)^{-N}$, avec a dans $\mathbb{Z}$, b et N dans $\mathbb{N}\setminus\{0\}$.*

Une conséquence de ce résultat est que les $\tau_n(Z_\infty(F))$ ont un comportement asymptotique particulièrement simple : pour n assez grand ils vérifient une relation linéaire de récurrence à coefficients dans $\mathcal{M}_{\mathrm{loc}}$.

Ceci ne nous dit toutefois rien sur la valeur de $\tau_n(Z_\infty(F))$ pour n très grand. En fait, on va voir que, convenablement renormalisés, les $\tau_n(Z_\infty(F))$ ont une limite quand $n \to \infty$. Pour pouvoir parler de limite, il faut tout d'abord disposer d'une topologie. Pour cela on va considérer la dimension virtuelle des éléments de $\mathcal{M}_{\mathrm{loc}}$: pour tout entier m dans $\mathbb{Z}$, on note F^m le sous-groupe abélien de $\mathcal{M}_{\mathrm{loc}}$ engendré par les fractions de la forme $[S]\mathbb{L}^{-i}$ avec S de dimension complexe $\leqslant -m+i$; les éléments de F^m sont ceux de dimension virtuelle $\leqslant -m$: plus m est grand, plus F^m est petit. Ceci permet de munir $\mathcal{M}_{\mathrm{loc}}$ d'une structure topologique (uniforme, pour les puristes) compatible avec la structure d'anneau et on peut considérer l'anneau complété $\widehat{\mathcal{M}}$, introduit par M. Kontsevich.

Théorème 4.2 ([4]). *Si $Z(F)$ est non vide et de dimension complexe r, alors la suite $n \mapsto [\tau_n(Z_\infty(F))]\mathbb{L}^{-(n+1)r}$ est de Cauchy dans $\mathcal{M}_{\mathrm{loc}}$ et a une limite non nulle $\mu(Z_\infty(F))$ dans $\widehat{\mathcal{M}}$.*

Concrètement, ce résultat affirme que, à un facteur affine « trivial » près, les ensembles $\tau_n(Z_\infty(F))$ ont une limite virtuelle quand $n \to \infty$. Il est en fait possible de donner des « formules » pour cette limite, pour lesquelles nous renvoyons à [4].

5. – L'analogie avec le p-adique

Heuristiquement les énoncés des théorèmes 4.1 et 4.2 ont été découverts par analogie avec le cas p-adique. Par définition l'anneau $\mathbb{Z}_p$ des entiers p-adiques est le complété de $\mathbb{Z}$ pour la norme p-adique. C'est aussi l'ensemble des éléments de $\mathbb{Q}_p$ de norme p-adique $\leqslant 1$. Les éléments de $\mathbb{Z}_p$ s'écrivent de façon unique comme des séries $\sum_{i\in\mathbb{N}} a_i p^i$ avec a_i dans $\{0,\dots,p-1\}$. On voit ainsi apparaître une analogie naturelle entre les séries formelles et les entiers p-adiques, le nombre premier p correspondant à la variable t. Il est de plus clair à partir de cette écriture que $\mathbb{Z}_p/p^i\mathbb{Z}_p$ est isomorphe à $\mathbb{Z}/p^i\mathbb{Z}$ pour tout i. Considérons maintenant un système (F) d'équations polynomiales comme celui du début de ce texte, mais dont les coefficients appartiennent à $\mathbb{Z}_p$ au lieu d'appartenir à $\mathbb{C}$. Notons $Z(F)(\mathbb{Z}_p)$ la partie de $\mathbb{Z}_p^m$ formée des solutions du système à coefficients dans $\mathbb{Z}_p$. Dans cette situation l'analogue de l'ensemble des tronqués $\tau_n(Z_\infty(F))$ est tout simplement l'image de l'ensemble $Z(F)(\mathbb{Z}_p)$ dans $(\mathbb{Z}_p/p^i\mathbb{Z}_p)^m$. Comme $(\mathbb{Z}_p/p^i\mathbb{Z}_p)^m$ est un ensemble fini, il en est de même de l'image de $Z(F)(\mathbb{Z}_p)$, et la seule chose raisonnable à faire est d'étudier son cardinal que l'on note N_i.

Le résultat de rationalité suivant, dont le théorème 4.1 est l'analogue, est dû à J. Denef et répond à une question posée par J.-P. Serre.

Théorème 5.1 ([2]). *La série de Poincaré $Q(T) := \sum_{i\in\mathbb{N}} N_i T^i$ est le développement en série d'une fraction rationnelle.*

Quant au théorème 4.2, il est l'analogue du résultat suivant de J. Oesterlé :

Théorème 5.2 ([8]). *Si $Z(F)(\mathbb{Z}_p)$ est non vide et de dimension r, alors la suite $n \mapsto N_n p^{-(n+1)r}$ a une limite non nulle dans $\mathbb{R}$.*

6. – Les ingrédients

La preuve du théorème 5.1 utilise de façon essentielle que la série de Poincaré $Q(T)$ est égale, à un grain de sel près, à l'intégrale

$$Z(s) := \int_{\mathbb{Z}_p^m} d(x, Z(F)(\mathbb{Z}_p))^{-s}. \tag{6.1}$$

Ici $\mathbb{Z}_p^m$ est muni de la mesure de Lebesgue, dont la construction dans le cas p-adique est similaire, en bien plus simple, à celle du cas réel, $d(x, Z(F)(\mathbb{Z}_p))$ désigne la distance de x à $Z(F)(\mathbb{Z}_p)$ et s est relié à T par la relation $T = p^{-s}$. On voit apparaître avec l'intégrale $Z(s)$ les deux ingrédients essentiels de la preuve du théorème 4.1 qui sont

- l'utilisation de l'intégration pour la mesure de Lebesgue
- l'utilisation de la fonction distance d.

Déjà dans le cas complexe, la fonction distance à un ensemble algébrique n'est pas en général polynomiale, mais seulement semi-algébrique (au sens que son graphe est un ensemble semi-algébrique réel). De même, dans le cas p-adique, le graphe de la fonction distance est semi-algébrique.

La démonstration des théorèmes 4.1 et 4.2 procède par analogie avec le cas p-adique. Un rôle clé est ainsi joué par la théorie des ensembles semi-algébriques sur $\mathbb{C}((t))$, qui est un analogue de la théorie des ensembles semi-algébriques p-adiques, ainsi que par un analogue géométrique de l'intégration p-adique, l'intégration motivique. Pour développer cette théorie de l'intégration motivique on construit une mesure μ, qui à une partie semi-algébrique Z de $\mathbb{C}[[t]]^m$ associe un élément $\mu(Z)$ de $\widehat{\mathcal{M}}$, de la façon suivante : on démontre, par une preuve analogue à celle du théorème 5.2, que la suite $n \mapsto [\tau_n(Z)]\mathbb{L}^{-(n+1)m}$ est de Cauchy dans $\mathcal{M}_{\mathrm{loc}}$ (ce qui donne essentiellement le théorème 4.2) ; le volume motivique $\mu(Z)$ est égal à la limite de cette suite dans $\widehat{\mathcal{M}}$. Cette mesure permet également d'intégrer des fonctions « semi-algébriques » et en particulier d'exprimer la série de Poincaré $P(T)$ en fonction d'un analogue de l'intégrale $Z(s)$ définie en (6.1). Pour démontrer la rationalité de $P(T)$ on peut alors suivre la stratégie de la preuve du théorème 5.2, qui utilise de façon essentuielle le théorème de résolution des singularités d'Hironaka et la formule de changement de variable dans les intégrales. Dans le présent contexte l'analogue de la formule de changement de variable se ramène à un énoncé purement géométrique démontré dans [4].

Remarque. Supposons que les polynômes F_i soient à coefficients rationnels. Les coefficients de la série $P(T)$ sont alors des classes de parties constructibles définies par des équations à coefficients rationnels et on peut considérer leur nombre de points dans le corps fini à p éléments $\mathbb{F}_p$, au moins pour presque tout nombre premier p. On pourrait imaginer qu'en procédant ainsi il soit possible de récupérer les séries $P_p(T)$, au moins pour presque tout nombre premier p, à partir de la série $P(T)$. En fait il n'en est rien ; il est cependant possible (cf. [5]), mais cela demande plus de travail, de construire une autre série de Poincaré, de nature arithmétique celle-ci, vérifiant une telle propriété de spécialisation.

Références

1. M. Artin, *On the solutions of analytic equations*, Invent. Math. **5**(1968), 277–291.
2. J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Invent. Math. **77** (1984), 1–23.
3. J. Denef, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.
4. J. Denef, F. Loeser, *Germs of arcs on singular algebraic varieties and motivic integration*, Inv. Math. **135** (1999), 201–232.
5. J. Denef and F. Loeser, *Definable sets, motives and p-adic integrals*, preprint octobre 1999, math/9910107.
6. M. Greenberg, *Rational points in Henselian discrete valuation rings*, Inst. Hautes Études Sci. Publ. Math. **31** (1966), 59–64.
7. A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.

8. J. Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbb{Z}_p^N$*, Invent. math. **66** (1982), 325–341.
9. J. Pas, *Uniform p-adic cell decomposition and local zeta functions*, J. reine angew. Math. **399** (1989), 137–172.

Rectificatif à l'article de H. Darmon intitulé : « La Conjecture de Shimura-Taniyama-Weil est enfin démontrée[1] »

Yves HELLEGOUARCH (*Université de Caen*)

Le présent rectificatif concerne un point de cet article dont l'importance est plus historique que mathématique et qui peut se résumer par une question : qui a inventé les « courbes de Frey » ?

Dans son article, H. Darmon semble donner une réponse en écrivant que « C'est Frey qui a eu l'idée d'associer à une solution non triviale (a, b, c) de l'équation $x^p + y^p = z^p$ une courbe elliptique $E_{a,b,c}$ (appelée maintenant « courbe de Frey ») donnée par l'équation $y^2 = x(x - a^p)(x + b^p)$ ».

Comme le reconnaît H. Darmon lui-même, la formulation de cette phrase est « fâcheuse » car elle suggère que c'est Frey qui, le premier, a eu cette idée. Or si une chose est bien claire, c'est que ce n'est pas Frey qui a **le premier** utilisé cette construction et remarqué **le premier** les étranges propriétés de faible ramification de la $p-$torsion de cette courbe (qui font douter de l'existence de celle-ci).

Voici, par exemple, le contenu d'une lettre que Jean-Pierre Serre m'a adressée le 16 janvier 1986 et qui pose la question :

> *Dans votre thèse, vous aviez utilisé la courbe elliptique*
>
> $$E_{a,b,c} \qquad y^2 = x(x - a^p)(x - c^p)$$
>
> *associée à une solution $a^p + b^p = c^p$ de l'équation de Fermat, et vous aviez étudié les propriétés de ramification de ses points de division par p.*
>
> *Vous savez peut-être que cette construction a été reprise tout récemment par G. Frey. Si l'on combine cette idée avec certaines* ***conjectures*** *sur les formes modulaires* mod p *que j'avais faites vers 1974, on trouve une contradiction (ce qui démontre Fermat ! mais hélas* ***modulo*** *mes conjectures).*
>
> *Je vous écris, d'abord pour vous raconter ces développements récents (qui peuvent vous intéresser), et puis aussi pour vous demander des références sur la courbe $E_{a,b,c}$: où apparaît-elle pour la première fois ? Est-ce dans votre thèse, ou chez Demjanenko ? Ou ailleurs ? Pouvez-vous avoir l'obligeance de me renseigner ?*

[1] *Gazette des mathématiciens* n° 83 (janvier 2000).