UN LEMME D'INTERPOLATION

par

Serge CANTAT

L'inégalité ultramétrique valable dans le monde p-adique annihile certains problèmes de convergence que l'on rencontre fréquemment en analyse complexe. Ce texte illustre ce phénomène en présentant un lemme d'interpolation dû à Jason Bell et Bjorn Poonen qui peut être utilisé pour étudier les transformations algébriques, et les groupes qu'elles engendrent.

1. Le problème du centre

Considérons une fonction polynomiale d'une variable complexe qui s'annule à l'origine et dont le degré d est supérieur ou égal à 2. Nous la noterons f, et écrirons

$$f(z) = \lambda z + a_2 z^2 + \ldots + a_d z^d \tag{1.1}$$

avec $a_d \neq 0$; le coefficient λ est la dérivée de f à l'origine. Nous supposerons que le module de λ est égal à 1 et que λ n'est pas une racine de l'unité ; ainsi

$$f'(0) = \lambda = \exp(2i\pi\theta) \text{ avec } \theta \text{ irrationnel.} \tag{1.2}$$

L'application $f\colon \mathbf{C} \to \mathbf{C}$ fixe donc l'origine et son comportement infinitésimal en ce point fixe est celui d'une rotation irrationnelle. Chaque orbite de cette rotation $r_\theta\colon z \mapsto \exp(2i\pi\theta)z$ est dense dans un cercle centré à l'origine et le Zentrumproblem, ou **problème du centre** [**20**], demande ce qu'il en est pour les orbites de f. Bien sûr, l'orbite

$$z,\ f(z),\ f^2(z),\ f^3(z),\ \ldots,\ f^n(z),\ \ldots \tag{1.3}$$

ne ressemble pas du tout à celle d'une rotation lorsque $|z|$ est grand, car alors la suite $(f^n(z))$ tend rapidement vers l'infini. Mais au voisinage de l'origine, il se pourrait que la dynamique de f soit semblable à celle de la rotation r_θ ; en fait, on démontre facilement que les trois propriétés suivantes sont équivalentes (voir [**18**] par exemple) :

- L'application f est localement conjuguée à la rotation r_θ au voisinage de l'origine : il existe deux ouverts $\mathcal{U}$ et $\mathcal{V}$ de $\mathbf{C}$ contenant 0 et un difféomorphisme holomorphe $\varphi\colon\ \mathcal{U} \to \mathcal{V}$ tel que $\varphi \circ f = r_\theta \circ \varphi$.
- Il existe un ouvert $\mathcal{U} \subset \mathbf{C}$ contenant l'origine qui est f-invariant et sur lequel f induit un difféomorphisme $f_{|\mathcal{U}}\colon\ \mathcal{U} \to \mathcal{U}$.
- Il existe un voisinage f-invariant de l'origine sur lequel l'action de f s'étend en une action du groupe compact $\mathbf{R}/\mathbf{Z}$: les itérés f^n de f correspondent aux éléments $n\theta$ de ce groupe.

Lorsque ces propriétés sont satisfaites, on dit que f est **linéarisable au voisinage de l'origine**, ou encore que f est **conjuguée à la rotation** r_θ. Le problème du centre demande de déterminer à quelles conditions f est effectivement linéarisable. C'est un problème redoutable lié aux propriétés d'approximation diophantienne de l'angle θ ; cette relation est bien illustrée par l'exemple suivant.

Théorème 1.1 **(Cremer, 1927).** — *Soit $f(z) = \lambda z + a_2 z^2 + \dots a_d z^d$ un polynôme complexe de degré $d \geq 2$. Si $|\lambda^q - 1|^{1/d^q}$ tend vers 0 le long d'une suite infinie d'entiers (q_i), alors f n'est pas linéarisable au voisinage de l'origine.*

La preuve est très élégante, et très *dynamique*. Tout d'abord, nous pouvons supposer que le coefficient dominant a_d de f est égal à 1, car en conjuguant f à l'aide d'une homothétie $z \mapsto \alpha z$ dont le rapport satisfait $\alpha^{d-1} a_d = 1$ on se ramène à $a_d = 1$, et cette conjugaison ne change ni la valeur de λ, ni la linéarisabilité locale de f au voisinage de 0. Ensuite, on remarque que l'hypothèse faite sur λ entraine $|\lambda| = 1$. Si λ est une racine de l'unité, f ne peut être localement conjugué à $z \mapsto \lambda z$ car f serait alors périodique [(1)], tandis que ses itérés f^n sont de degré $d^n \geq 2^n$. Nous pouvons donc désormais supposer $\lambda = \exp(2i\pi\theta)$ avec θ irrationnel.

Si f est conjuguée à la rotation r_θ sur un voisinage $\mathcal{U}$ de l'origine, le seul point périodique de f dans $\mathcal{U}$ est le point fixe 0 ; en effet, toutes les orbites de r_θ sont infinies, exceptée celle du point fixe. Pour montrer que f n'est pas linéarisable, nous allons donc montrer qu'il existe des points périodiques $z \neq 0$ arbitrairement proches

[(1)] La périodicité locale est équivalente à la périodicité globale sur $\mathbf{C}$: si $f^n(z) = z$ au voisinage de l'origine, alors les polynômes $f^n(z)$ et z doivent coïncider.

de 0. Pour s'en convaincre, écrivons l'équation aux points fixes pour le q-ème itéré de f. Puisque $a_d = 1$, et puisque la dérivée de f^q à l'origine vaut λ^q, l'équation $f^q(z) - z = 0$ est de la forme

$$(\lambda^q - 1)z + \ldots + z^{d^q} = 0. \tag{1.4}$$

Un point est périodique de période divisant q si, et seulement si c'est une racine de cette équation polynomiale. En notant les racines α_i (répétées suivant leur multiplicité), cette équation équivaut à

$$z \prod_{i=1}^{d^q-1} (z - \alpha_i) = 0, \tag{1.5}$$

où le terme correspondant à la racine évidente $\alpha_0 = 0$ a été isolé (c'est le point fixe 0). Le produit des α_i pour $i \geq 1$ est égal à $\lambda^q - 1$. Donc la racine non nulle de module minimal vérifie $|\alpha_j|^{1/(d^q-1)} \leq |\lambda^q - 1|^{1/(d^q-1)}$. L'hypothèse du théorème de Cremer assure donc l'existence de racines arbitrairement petites, c'est-à-dire de points périodiques arbitrairement proches de l'origine, lorsqu'on choisit convenablement les périodes q_i. □

On dispose maintenant de réponses très satisfaisantes au problème du centre. Le premier résultat fondamental est celui de Siegel, qui montre que f est effectivement linéarisable lorsqu'il existe un nombre réel $M > 0$ tel que

$$q^{-M} < |\lambda^q - 1| \tag{1.6}$$

pour tout entier $q \geq 1$. Ce théorème est ensuite affiné par Bruno. La **condition de Bruno**, plus faible que celle de Siegel, demande aussi que l'angle $\theta \in [0, 1[$ ne soit pas trop bien approché par les nombres rationnels ; en notant (p_n/q_n) la suite des meilleures approximations rationnelles de θ, il s'agit d'imposer que

$$\sum_n \frac{\log q_{n+1}}{q_n} \tag{1.7}$$

soit une somme finie. Grâce aux travaux de Yoccoz, nous savons maintenant que cette condition est optimale : si elle n'est pas vérifiée par θ, alors $z \mapsto \lambda z + z^2$ n'est pas linéarisable au voisinage de l'origine, et ceci s'explique par la présence d'orbites périodiques arbitrairement proches de l'origine. Je n'en dirai pas plus, renvoyant lectrices et lecteurs à [**20**] et à [**26, 21**], l'unique but de ce chapitre étant de décrire la difficulté du problème du centre en dynamique complexe.

Nous allons maintenant progressivement nous diriger vers des questions analogues en dynamique p-adique, en effectuant tout d'abord un petit détour par la méthode des différences divisées.

2. Les différences divisées de Newton

Considérons une suite $n \mapsto u(n)$ de nombres réels, et cherchons un polynôme P, de degré d, qui prend les mêmes valeurs $P(j) = u(j)$ pour j entre 0 et d ; c'est une version du problème d'interpolation de Lagrange, et l'on peut donc construire P explicitement par la formule de Lagrange. Il existe aussi un procédé itératif dû à Newton qui utilise l'opérateur différentiel discret Δ associant à toute suite $(u(n))$ la suite de ses différences successives

$$(\Delta u)(n) = u(n+1) - u(n). \tag{2.1}$$

Les trois premières valeurs sont $u(1) - u(0)$, $u(2) - u(1)$ et $u(3) - u(2)$. Si l'on applique deux fois Δ, le résultat commence donc par $(\Delta^2 u)(0) = u(2) - 2u(1) + u(0)$, $(\Delta^2 u)(1) = u(3) - 2u(2) + u(1)$, etc. Avec trois itérations,

$$(\Delta^3 u)(0) = u(3) - 3u(2) + 3u(1) - u(0). \tag{2.2}$$

L'algorithme de Newton nécessite justement de lister les premières valeurs des différences successives, c'est-à-dire de calculer la suite de nombres $A_u(m)$ définie par

$$A_u(m) = \Delta^m(u)(0) = \sum_0^m (-1)^{m-j} \binom{m}{j} u(j). \tag{2.3}$$

Théorème 2.1. — *Soit $(u(n))$ une suite de nombres réels. Le polynôme d'interpolation de degré $\leq d$ défini par les contraintes $P(j) = u(j)$ pour $0 \leq j \leq d$ est égal à*

$$P(t) = \sum_0^d A_u(m) \frac{t(t-1)\cdots(t-m+1)}{m!}$$

où les coefficients $A_u(m)$ sont définis par l'équation (2.3).

La démonstration est presque une évidence, une fois les remarques suivantes en tête. D'une part, les polynômes binomiaux

$$\binom{t}{j} = \frac{t(t-1)\cdots(t-j+1)}{j!} \tag{2.4}$$

forment une base de l'espaces des polynômes à une variable. D'autre part, les relations d'additivité dans le triangle de Pascal stipulent que l'image du polynôme binomial de degré j par Δ est celui de degré $j-1$. Ainsi, le polynôme d'interpolation P que l'on cherche peut-être écrit comme une combinaison linéaire

$$P = \sum_0^d a_j \begin{pmatrix} t \\ j \end{pmatrix} \tag{2.5}$$

des polynômes binomiaux de degré au plus d. Le terme constant a_0 doit être égal à $u(0)$, car les polynômes binomiaux de degré > 0 s'annulent tous à l'origine. Puis, appliquant Δ, et évaluant à l'origine, on trouve $a_1 = \Delta(u)(0) = A_u(1)$, etc.

3. Les nombres p-adiques et l'interpolation de Mahler

Nous allons maintenant appliquer la méthode de Newton pour des suites de nombres p-adiques.

3.1. Nombres p-adiques. — Soit p un nombre premier. Si a est un nombre entier non nul, il peut être décomposé en le produit $p^s u$ d'une puissance positive de p et d'un nombre entier u premier à p. L'entier s est la **valuation p-adique** de a, notée $v_p(a)$. La **valeur absolue** p-adique de a est alors définie par

$$|a|_p = p^{-v_p(a)}, \tag{3.1}$$

et par $|a|_p = 0$ lorsque a est nul. Elle s'étend aux nombres rationnels en posant

$$\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p} = p^{-s}, \tag{3.2}$$

lorsque $a/b = p^s u/v$ avec u et v entiers premiers à p. Pour $a = 12 = 4 \times 3$, on trouve $|a|_2 = 1/4$, $|a|_3 = 1/3$, et $|a|_p = 1$ pour tous les autres nombres premiers. L'entier $a = 89$ n'est pas divisible par 5, et sa norme 5-adique est donc égale à 1 ; pour être plus précis, on peut écrire

$$a = 4 + 2 \times 5 + 3 \times 5^2, \tag{3.3}$$

les trois termes étant respectivement de taille 1, $1/5$ et $1/25$ pour la valeur absolue 5-adique.

La valeur absolue $|\cdot|_p$ vérifie

$$|a \times b|_p = |a|_p \times |b|_p \quad \text{et} \quad |a+b|_p \leq \max\{|a|_p, |b|_p\}. \tag{3.4}$$

La seconde propriété est **l'inégalité ultramétrique**. C'est une version renforcée de l'inégalité triangulaire qui provient de la remarque suivante : soient $a = p^s u$ et $b = p^t v$ deux entiers avec u et v premiers à p et $s \leq t$, alors $a + b = p^s w$ avec $w = u + p^{t-s} v$; lorsque w est premier à p on obtient $|a+b|_p = p^{-s} = |a|_p$; lorsque w n'est pas premier à p alors $t = s$, p divise $w = u + v$ et $|a+b|_p < |a|_p = |b|_p$.

En complétant $\mathbf{Q}$ pour la valeur absolue $|\cdot|_p$, on obtient le corps $\mathbf{Q}_p$ des nombres p-adiques. La multiplicativité et l'inégalité ultramétrique restent valables ; les valeurs prises par $|\cdot|_p$ sur $\mathbf{Q}_p$ sont les puissances entières p^m de p, avec $m \in \mathbf{Z}$.

3.2. Le disque unité $\mathbf{Z}_p$ (voir [23]). — Notons $\mathbf{Z}_p$ l'adhérence de $\mathbf{Z}$ dans $\mathbf{Q}_p$. Chaque élément $a \in \mathbf{Z}_p$ peut être décomposé en une série convergente

$$a = \sum_{i=0}^{+\infty} a(i)p^i \tag{3.5}$$

dont les coefficients $a(i)$ sont des entiers compris entre 0 et $p-1$, les sommes à support fini correspondant aux éléments de $\mathbf{Z}$ (voir l'exemple fourni par l'équation (3.3)). L'ensemble $\mathbf{Z}_p$ est un sous-anneau de $\mathbf{Q}_p$. C'est aussi le "disque unité" de $\mathbf{Q}_p$, formé des nombres de norme ≤ 1 (ce disque est fermé et ouvert, car c'est aussi l'ensemble des nombres de norme $< p$).

L'ensemble des éléments $c \in \mathbf{Q}_p$ de norme < 1 coïncide avec l'ensemble $p\mathbf{Z}_p$. C'est l'unique idéal maximal de l'anneau $\mathbf{Z}_p$, et le quotient $\mathbf{Z}_p/p\mathbf{Z}_p$ s'identifie au corps fini

$$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p/p\mathbf{Z}_p \tag{3.6}$$

via l'application qui applique $a = \sum_{i=0}^{+\infty} a(i)p^i$ sur le premier coefficient $a(0)$. L'ensemble $\mathbf{Z}_p$ peut donc être décomposé en p sous-ensembles correspondant aux p classes possibles dans $\mathbf{Z}/p\mathbf{Z}$; ce sont les disques $c + p\mathbf{Z}_p$, où $c \in \{0, \ldots, p-1\}$. Géométriquement, l'inégalité ultramétrique et le fait que l'ensemble $p^{\mathbf{Z}}$ des valeurs absolues possibles soit discret montrent que les disques $\mathbb{D}(c;r) = \{a \in \mathbf{Q}_p : \ |c-a|_p \leq r\}$ sont à la fois fermés et ouverts, que deux disques qui s'intersectent sont emboités l'un dans l'autre, que tout point d'un disque est un centre, ... On pourra consulter [**15**] et [**23**] pour les démonstrations de ces résultats et la géométrie des nombres p-adiques.

Par exemple, lorsque $p = 5$, $\mathbf{Z}_5$ est constitué de cinq disques (simultanément ouverts et fermés) de rayon $1/5$. Ces disques sont deux-à-deux disjoints. Puis, chacun de ces disques est lui même constitué de cinq disques de rayon $1/25$, etc. Un point de $\mathbf{Z}_5$ est uniquement déterminé par la succession des disques de rayon 5^{-s} qui le contiennent : ceci correspond au développement $a = \sum_{i=0}^{+\infty} a(i)5^i$ de l'équation (3.5), et montre que $\mathbf{Z}_5$ est un ensemble de Cantor.

3.3. Interpolation p-adique. — Nous allons maintenant nous intéresser, en suivant Kurt Mahler, à l'interpolation d'une suite $(u(n))_{n\in\mathbf{Z}}$ d'entiers p-adiques. La fonction $u\colon \mathbf{Z} \to \mathbf{Z}_p$ est uniformément continue pour la topologie p-adique (sur $\mathbf{Z}$ et $\mathbf{Z}_p$) si et seulement si, pour tout entier $M > 0$, il existe un entier $N > 0$ tel que

$$|u(n) - u(m)|_p \leq p^{-M} \tag{3.7}$$

dès que p^N divise $n-m$. Autrement dit, $u(n)-u(m)$ est divisible par une grande puissance de p lorsque $n-m$ l'est.

***Théorème 3.1* (Mahler, [17]). —** *Soit $u\colon \mathbf{Z}\to\mathbf{Z}_p$ une suite uniformément continue d'entiers p-adiques. La série*

$$\overline{u}(t)=\sum_{m\geq 0}A_u(m)\binom{t}{m}=\sum_{m\geq 0}A_u(m)\frac{t(t-1)\cdots(t-m+1)}{m!}$$

converge uniformément sur $\mathbf{Z}_p$ vers l'unique fonction continue $\overline{u}\colon \mathbf{Z}_p\to\mathbf{Z}_p$ prolongeant u.

Les coefficients $A_u(m)$ sont les coefficients obtenus par la méthode des différences divisées (voir la formule (2.3)). Ainsi, dans le monde p-adique, la méthode de Newton fournit l'extension continue de $u\colon \mathbf{Z}\to\mathbf{Z}_p$ à l'adhérence $\mathbf{Z}_p$ de $\mathbf{Z}$ dans $\mathbf{Q}_p$. La preuve n'est pas difficile (on pourra consulter [**17**] ou [**23**]), mais nécessite l'inégalité ultramétrique (voir [**12**], §2.1).

4. Interpolation p-adique dynamique

Nous pouvons maintenant revenir au problème du centre, mais pour des transformations d'une variable p-adique.

4.1. Difféomorphismes analytiques p-adiques. — L'énoncé principal étant valable pour des transformations de plusieurs variables, nous nous placerons d'emblée dans ce cadre. Nous considèrerons donc des polynômes $f\in\mathbf{Q}_p[x_1,\ldots,x_k]$, que nous écrirons sous la forme

$$f(\mathbf{x})=\sum_{J\in\mathbf{N}^k}a_J\mathbf{x}^J \tag{4.1}$$

où $\mathbf{x}=(x_1,\ldots,x_k)$ et $\mathbf{x}^J=x_1^{j_1}\cdots x_k^{j_k}$ lorsque $J=(j_1,\ldots,j_k)$; les coefficients a_J appartiennent à $\mathbf{Q}_p$ pour tout multi-indice et sont nuls excepté pour un nombre fini de multi-indices. Un tel polynôme détermine une unique application, encore notée f, de $\mathbf{Z}_p^k$ vers $\mathbf{Q}_p$; cette application est à valeurs dans $\mathbf{Z}_p$ si $f\in\mathbf{Z}_p[x_1,\ldots,x_k]$. La **norme de Gauss** $\|\ f\ \|$ est définie par

$$\|\ f\ \|=\max|a_J|_p. \tag{4.2}$$

Elle est multiplicative $\|\ fg\ \|=\|\ f\ \|\|\ g\ \|$ (c'est le lemme de Gauss). L'**algèbre de Tate** est la complétion de $\mathbf{Q}_p[\mathbf{x}]$ pour cette norme ; elle sera notée $\mathbf{Q}_p\langle\mathbf{x}\rangle$, et $\mathbf{Z}_p\langle\mathbf{x}\rangle$

désignera le sous-anneau obtenu par complétion de $\mathbf{Z}_p[x_1,\dots,x_k]$. Les éléments de $\mathbf{Z}_p\langle\mathbf{x}\rangle$ sont donnés par des séries entières

$$f(\mathbf{x}) = \sum_{J\in\mathbf{N}^k} a_J \mathbf{x}^J \tag{4.3}$$

à coefficients dans $\mathbf{Z}_p$ telles que $|a_J|_p$ converge vers 0 lorsque J tend vers l'infini dans $\mathbf{N}^k$. Ces séries convergent uniformément dans le polydisque $\mathbf{Z}_p^k$

Remarque 4.1. **—** La norme de Gauss est une norme du supremum, au sens où $\| f \|$ est le maximum des valeurs absolues $|f(z)|_p$, mais pour z dans le polydisque unité d'une clôture algébrique $\overline{\mathbf{Q}_p}$ de $\mathbf{Q}_p$ (il faudrait d'abord étendre $|\cdot|_p$ à une telle clôture pour être précis). Les éléments de $\mathbf{Z}_p\langle\mathbf{x}\rangle$ sont précisément les séries entières f convergeant uniformément sur $\mathbf{Z}_p^k$ telles que $|f(z)|_p \leq 1$ pour tout z dans le polydisque unité de $(\overline{\mathbf{Q}_p})^k$.

Nous dirons que f est congrue à g modulo p^s si $\| f-g \| \leq p^{-s}$. Autrement dit, $f \equiv g \mod (p)$ si les coefficients de $f-g$ sont tous dans $p^s\mathbf{Z}_p$ (nous dirons qu'ils sont tous divisibles par p^s). Ces notions s'étendent aux transformations $\mathbf{Z}_p^k \to \mathbf{Z}_p^k$ qui sont définies par k séries entières $f_j \in \mathbf{Z}_p\langle\mathbf{x}\rangle$. Les transformations analytiques ainsi obtenues forment un semi-groupe pour la composition : le groupe des **difféomorphismes analytiques** (au sens de Tate) de $\mathbf{Z}_p^k$ est, par définition, le groupe des éléments inversibles de ce semi-groupe ; nous le noterons $\mathsf{Diff}\langle\mathbf{Z}_p^k\rangle$.

Exemple 4.2. **—** Un élément f de $\mathsf{Diff}\langle\mathbf{Z}_p\rangle$ est déterminé par une série $f(\mathbf{x}) = \sum_{j\geq 0} a_j\mathbf{x}^j$ de la variable $\mathbf{x} = x_1$ dont les coefficients tendent vers 0 dans $\mathbf{Z}_p$ lorsque j tend vers l'infini. En réduisant modulo p chacun des coefficients de f nous obtenons donc un polynôme d'une variable $\overline{f}(\mathbf{x}) \in \mathbf{F}_p[\mathbf{x}]$. L'application réciproque f^{-1} fournit un autre polynôme $\overline{f^{-1}}$ tel que $\overline{f}\circ\overline{f^{-1}}(\mathbf{x}) = \mathbf{x}$, si bien que $\overline{f}$ et $\overline{f^{-1}}$ sont des polynômes de degré 1. Ceci montre que les coefficients a_i de f satisfont les conditions de congruence $|a_0|_p \leq 1$, $|a_1|_p = 1$ et $|a_j|_p < 1$ pour $j \geq 2$. Réciproquement, si ces conditions sont satisfaites et a_j tend vers 0 lorsque j tend vers l'infini, alors f est un élément de $\mathsf{Diff}\langle\mathbf{Z}_p\rangle$ (on peut démontrer ce fait directement en explicitant les coefficients de f^{-1} à partir de ceux de f, ou appliquer le théorème de Bell et Poonen énoncé ci-dessous).

Une description analogue est valable en dimension plus grande. Pour que $f = (f_1,\dots,f_k)$, avec les f_i dans $\mathbf{Z}_p[\mathbf{x}_1,\dots,\mathbf{x}_k]$ soit un élément de $\mathsf{Diff}\langle\mathbf{Z}_p^k\rangle$ il faut et il suffit que la réduction $\overline{f}$ soit un automorphisme polynomial de l'espace affine sur $\mathbf{F}_p$; mais contrairement au cas de la dimension 1, ceci ne borne pas le degré des formules définissant $\overline{f}$ (voir le paragraphe 5.1).

Le groupe $\mathsf{Diff}\langle \mathbf{Z}_p^k \rangle$ agit par isométries sur le polydisque $\mathbf{Z}_p^k$ pour la distance

$$\mathsf{dist}(z,z') = \max_{1\leq i\leq k} |z_i - z_i'|_p. \tag{4.4}$$

En effet, si $f\colon \mathbf{Z}_p^k \to \mathbf{Z}_p$ appartient à $\mathbf{Z}_p\langle \mathbf{x}\rangle$ l'inégalité ultramétrique montre que f est 1-lipschitzienne. Donc si h est un élément $\mathsf{Diff}\langle \mathbf{Z}_p^k \rangle$, alors h est une transformation 1-lipschitzienne de $\mathbf{Z}_p^k$ pour la distance dist, l'application réciproque aussi, et h est en fait une isométrie. En particulier, h permute les polydisques de rayons p^{-s} pour tout $s \geq 1$. Ces disques sont paramétrés par l'ensemble fini $\mathbb{A}^k(\mathbf{Z}/p^s\mathbf{Z})$, et l'action de h sur ces disques peut être décrite de la manière suivante. Tout d'abord, développons h en une série

$$h(\mathbf{x}) = \sum_{j\geq 0} A_j(\mathbf{x}) \tag{4.5}$$

de termes $A_j\colon \mathbf{Z}_p^k \to \mathbf{Z}_p^k$ qui sont polynômiaux, homogènes et de degrés respectifs j. Les coefficients des polynômes A_j sont dans $\mathbf{Z}_p$ et peuvent être réduits modulo p^s. Puisque ces coefficients tendent vers 0 avec j, le résultat est un automorphisme polynomial de l'espace affine, mais sur l'anneau $\mathbf{Z}/p^s\mathbf{Z}$ (l'inverse est obtenu en appliquant le même procédé à h^{-1}). L'action sur l'ensemble fini $\mathbb{A}^k(\mathbf{Z}/p^s\mathbf{Z})$ correspond à celle sur les disques de rayon p^{-s}.

4.2. Zéros isolés. — Soit $f(z) = \sum_{j\geq 0} a_j z^j$ une série à coefficients dans $\mathbf{Z}_p$ qui converge dans le disque unité $\mathbf{Z}_p$ et n'est pas identiquement nulle. Alors f n'a qu'un nombre fini de zéros dans $\mathbf{Z}_p$: c'est le principe des zéros isolés dans le disque (ouvert et compact) $\mathbf{Z}_p$. On peut même donner une version effective de ce principe. Pour cela, on regarde le maximum des valeurs absolues $|a_j|_p$, puis le plus grand indice $\ell(f)$ tel que $|a_{\ell(f)}|_p$ atteint ce maximum ; c'est un entier positif car $|a_j|_p$ tend vers 0 si f converge dans $\mathbf{Z}_p$. On montre alors que f s'annule au plus $\ell(f)$ fois dans $\mathbf{Z}_p$, à moins d'être la série nulle.

D'autres théorèmes classiques concernant les fonctions analytiques s'étendent aux séries convergentes de la variable p-adique. Nous renvoyons au livre de Alain Robert [**23**] pour ces énoncés, et notamment pour le lemme de Hensel qui remplace la méthode itérative de Newton pour trouver un zéro d'une fonction.

4.3. Théorème de Jason Bell et Bjorn Poonen. — Le lemme d'interpolation évoqué dans le titre de cet article est le théorème suivant.

Théorème 4.3 **(Jason Bell, Bjorn Poonen [2, 22]). —** *Soit $f\colon \mathbf{Z}_p^k \to \mathbf{Z}_p^k$ une transformation analytique, au sens de Tate, du polydisque $\mathbf{Z}_p^k$. Si $f \equiv \mathrm{Id} \mod (p^c)$ avec $c > 1/(p-1)$, il existe une application $\Phi\colon \mathbf{Z}_p \times \mathbf{Z}_p^k \to \mathbf{Z}_p^k$ telle que*

1. Φ *est analytique au sens de Tate.*
2. Φ *détermine une action du groupe additif* $(\mathbf{Z}_p,+)$ *sur* $\mathbf{Z}_p^k$ *; autrement dit,* $\Phi(s+t,\mathbf{x})=\Phi(s,\Phi(t,\mathbf{x}))$ *pour tous* $(s,t,\mathbf{x})\in\mathbf{Z}_p\times\mathbf{Z}_p\times\mathbf{Z}_p^k$.
3. *Cette action étend celle de* f *:* $\Phi(n,\mathbf{x})=f^n(\mathbf{x})$ *pour tout* $n\geq 0$.
4. *L'application* $t\in\mathbf{Z}_p\mapsto\Phi(t,\cdot)\in\mathsf{Diff}\langle\mathbf{Z}_p^k\rangle$ *est continue.*
5. $\Phi(t,\mathbf{x})\equiv \mathrm{Id} \mod (p^{c-1/(p-1)})$ *pour tout* $t\in\mathbf{Z}_p$.

En particulier, f *est un difféomorphisme analytique de* $\mathbf{Z}_p^k$ *dont l'inverse est* $\Phi(-1,\cdot)$.

Ainsi, f est inclus dans un **flot analytique** p-adique $\Phi(t,\cdot)$, le temps t du flot variant dans le groupe additif compact $(\mathbf{Z}_p,+)$.

***Remarque 4.4.* —** Ce théorème ne répond pas au problème du centre ; d'ailleurs, nous n'avons pas supposé que f fixait l'origine ! Mais il inscrit f dans un flot qui est défini sur le polydisque $\mathbf{Z}_p^k$ ce qui, dans le cas complexe, serait suffisant pour linéariser f.

***Remarque 4.5.* —** L'hypothèse de congruence $f\equiv \mathrm{Id} \mod (p^c)$ n'est guère restrictive. Pour s'en convaincre, supposons d'entrée que f est un élément de $\mathsf{Diff}\langle\mathbf{Z}_p^k\rangle$. Alors f agit par permutation sur l'ensemble fini des disques de rayons p^{-2}. Il existe donc un entier $m>0$ tel que f^m fixe le polydisque $p^2\mathbf{Z}_p^k$, ce qui signifie que le coefficient constant dans le développement en termes homogènes

$$f^m(\mathbf{x})=\sum_{j\geq 0}A_j(\mathbf{x}) \tag{4.6}$$

est divisible par p^2 : $A_0\equiv 0 \mod (p^2)$. Modulo p, le terme linéaire de $(f^m)^\ell(\mathbf{x})$ est alors égal à $A_1^\ell(\mathbf{x})$ et comme $\mathsf{GL}_k(\mathbf{Z}/p\mathbf{Z})$ est fini, il existe un itéré positif de f dont le terme constant est égal à $0 \mod (p^2)$ et le terme linéaire est égal à $\mathrm{Id} \mod (p)$. Choisissons un tel itéré f^n, notons $f^n=\sum_{j\geq 0}B_j(\mathbf{x})$ son développement en termes homogènes, et conjuguons cette transformation par l'homothétie de rapport p :

$$p^{-1}f^n(p\mathbf{x})=B_0/p+B_1(\mathbf{x})+p\sum_{j\geq 2}p^{j-2}B_j(\mathbf{x}). \tag{4.7}$$

Puisque $B_0\equiv 0 \mod (p^2)$ et $B_0\equiv \mathrm{Id} \mod (p)$, la transformation $p^{-1}f^n(p\mathbf{x})$ est congrue à l'identité modulo p. Lorsque $p\geq 3$, ceci est suffisant pour appliquer le théorème de Bell et Poonen. Ainsi, *quitte à remplacer* $f\in\mathsf{Diff}\langle\mathbf{Z}_p^k\rangle$ *par un itéré positif et à zoomer pour observer sa dynamique dans le polydisque* $p\mathbf{Z}_p^k$*, la transformation fait partie d'un flot analytique paramétré par le groupe additif* $(\mathbf{Z}_p,+)$.

Remarque 4.6. **—** Si $f(\mathbf{x}) = -\mathbf{x}$ et $p = 2$, alors $f \equiv \mathrm{Id} \mod (p)$, et l'action de f ne peut-être étendue en un flot, car sinon le flot $\Phi(t,\mathbf{x})$ satisferait $\Phi(n,\mathbf{x}) = \mathbf{x}$ pour tout entier pair, et par le principe des zéros isolés, $\Phi(1,\mathbf{x}) = f(\mathbf{x})$ serait aussi l'identité. Cette remarque montre que l'inégalité $c > (p-1)^{-1}$ est nécessaire lorsque $p = 2$; elle l'est aussi quand $p \geq 3$ si $\mathbf{Q}_p$ est remplacé par une extension finie contenant une racine de l'unité d'ordre p.

4.4. Démonstration du théorème. — La preuve initiale de Bell (voir [**2**]) a été grandement simplifiée par Bjorn Poonen (voir [**22**]). Avant de la présenter, remarquons qu'il s'agit à nouveau d'un théorème d'interpolation : ici, chaque point z de $\mathbf{Z}_p^k$ donne naissance à une orbite $n \mapsto f^n(z)$, et l'on cherche une application continue $t \mapsto \Phi(t,z)$ qui prolonge cette suite en une application continue définie sur $\mathbf{Z}_p$, c'est-à-dire que $\Phi(n,z) = f^n(z)$ pour tout $n \geq 0$. L'interpolation doit être faite "en famille", c'est-à-dire pour tout z, et doit donner naissance à une application analytique $\Phi(t,\mathbf{x})$, mais les idées essentielles sont déjà présentes dans la méthode des différences divisées de Newton et le théorème de Mahler.

Dans la situation qui nous intéresse, l'opérateur de différence Δ transforme la suite $n \mapsto f^n(z)$ en la suite $n \mapsto f^n \circ f(z) - f^n(z)$. Introduisons donc un nouvel opérateur linéaire $\Delta_f \colon (\mathbf{Z}_p\langle\mathbf{x}\rangle)^k \to (\mathbf{Z}_p\langle\mathbf{x}\rangle)^k$ en posant

$$\Delta_f(h) = h \circ f - h \tag{4.8}$$

pour tout $h \in (\mathbf{Z}_p\langle\mathbf{x}\rangle)^k$. Puisque $f \equiv \mathrm{Id} \mod (p^c)$, on remarque que

$$h \circ f \equiv h \mod (p^c) \tag{4.9}$$

pour tout h ; pour s'en convaincre, il suffit de tester cette congruence lorsque h est un monôme, ce qui est facile, puis de l'étendre à $(\mathbf{Z}_p\langle\mathbf{x}\rangle)^k$ par linéarité et par densité de $(\mathbf{Z}_p[\mathbf{x}])^k$ dans $(\mathbf{Z}_p\langle\mathbf{x}\rangle)^k$. L'image de Δ_f est donc contenue dans $p^c(\mathbf{Z}_p\langle\mathbf{x}\rangle)^k$, et par récurrence nous obtenons l'inclusion

$$\Delta_f^m((\mathbf{Z}_p\langle\mathbf{x}\rangle)^k) \subset p^{mc}(\mathbf{Z}_p\langle\mathbf{x}\rangle)^k \tag{4.10}$$

pour tout entier $m \geq 1$. Nous utiliserons en particulier que $\| \Delta_f(\mathrm{Id}) \| \leq p^{-mc}$.

Nous pouvons maintenant former la série de Mahler et Newton

$$\Phi(t,\mathbf{x}) = \sum_{m\geq 0} \Delta_f^m(\mathrm{Id}) \begin{pmatrix} t \\ m \end{pmatrix} = \sum_{m\geq 0} \frac{\Delta_f^m(\mathrm{Id})}{m!} t(t-1)\cdots(t-m+1) \tag{4.11}$$

dont les premiers termes sont

$$\mathbf{x} + (f(\mathbf{x}) - \mathbf{x})t + (f^2(\mathbf{x}) - 2f(\mathbf{x}) + \mathbf{x})\frac{t(t-1)}{2} + \ldots \tag{4.12}$$

Il s'agit tout d'abord de montrer que Φ converge. Puisque les polynômes $t(t-1)\cdots(t-m)$ sont à coefficients entiers, leur norme de Gauss vaut 1. Ensuite, on remarque que $v_p(m!) = [\frac{m}{p}] + [\frac{m}{p^2}] + [\frac{m}{p^3}] + \ldots$, ce qui entraine

$$|m!|_p \geq p^{-m/(p-1)}. \tag{4.13}$$

Comme $\| \Delta_f^m(\mathrm{Id}) \| \leq p^{-mc}$, avec $c > 1/(p-1)$, il s'ensuit que la série définissant Φ converge uniformément pour la norme de Gauss sur $\mathbf{Z}_p \times \mathbf{Z}_p^k$. Ainsi, l'équation (4.11) détermine bien un élément Φ de l'anneau de Tate $\mathbf{Z}_p\langle t, \mathbf{x}\rangle^k$.

Puisque Φ est définie en utilisant la méthode de Newton pour la suite $n \mapsto f^n(\mathbf{x})$, la relation $\Phi(n,\mathbf{x}) = f^n(x)$ est satisfaite pour tout entier $n \geq 0$ (on peut aussi remarquer directement que $\Phi(n,\mathbf{x}) = (\mathrm{Id} + \Delta_f)^n(\mathbf{x}) = f^n(\mathbf{x})$, où Id est l'opérateur identité $\mathrm{Id}\colon h \mapsto h$). Puisque $f^{n+m} = f^n \circ f^m$, on en déduit que

$$\Phi(s+t,\mathbf{x}) = \Phi(s,\Phi(t,\mathbf{x})) \tag{4.14}$$

lorsque $s = n$ et $t = m$ sont entiers, et par le principe des zéros isolés pour toute paire $(s,t) \in \mathbf{Z}_p^2$. En particulier, $\Phi(t,\mathbf{x})$ est un difféomorphisme de $\mathbf{Z}_p^k$ pour tout t, d'inverse $\Phi(-t,\mathbf{x})$, ce qui montre que $f(\mathbf{x})$ est un difféomorphisme d'inverse $\Phi(-1,\mathbf{x})$.

Les assertions (4) et (5) du théorème découlent également de la définition explicite de Φ, et nous renvoyons à [**22**] pour les détails.

5. Temps de passage d'une orbite le long d'une sous-variété

Si l'on se donne un sous-ensemble quelconque P de $\mathbf{Z}$, il est possible de trouver un difféomorphisme f d'une variété compacte M, une sous-variété W de M et un point x de M tel que $f^m(x)$ appartient à W si et seulement si m appartient à P. Ce n'est plus possible si l'on impose à M, f et W d'être "algébriques" : ce sera notre première application du lemme d'interpolation dynamique de Bell et Poonen.

5.1. Skolem, Mahler et Lech. — Considérons une relation de récurrence linéaire,

$$u(n+d+1) = a_d u(n+d) + a_{d-1}u(n+d-1) + \cdots + a_0 u(n) \tag{5.1}$$

dont les coefficients sont des nombres complexes. Le théorème de Thoralf Skolem, Kurt Mahler et Christer Lech stipule que l'ensemble

$$P = \{n \in \mathbf{Z}\,;\, u(n) = 0\} \tag{5.2}$$

est une réunion finie de progressions arithmétiques, certaines pouvant être de raison nulle (voir [**16**]). Autrement dit, pour toute condition initiale $(u(0),\ldots,u(d))$, il

existe un entier ℓ et des entiers r_i et s_i, avec $1 \leq i \leq \ell$, tels que

$$P = \bigcup_{i=1}^{\ell} \{r_i k + s_i \; ; \; k \in \mathbf{Z}\} \, . \tag{5.3}$$

Il s'agit maintenant d'un cas particulier du théorème suivant, dû à Jason Bell, Dragos Ghioca et Thomas Tucker.

***Théorème 5.1* (Bell, Ghioca, Tucker [3]). —** *Soit f un automorphisme polynomial de l'espace affine complexe de dimension k. Soit W une sous-variété algébrique de $\mathbb{A}^k_{\mathbf{C}}$ et z un point de $\mathbb{A}^k_{\mathbf{C}}$. L'ensemble*

$$Pas_f(z;W) = \{n \in \mathbf{Z} \; ; \; f^n(z) \in W\}$$

des temps de passage de l'orbite de z sur la variété W est une réunion finie de progressions arithmétiques.

Un automorphisme de l'espace affine est, par définition, une transformation polynomiale inversible $f \colon \mathbb{A}^k(\mathbf{C}) \to \mathbb{A}^k(\mathbf{C})$ dont la l'inverse est aussi définie par des formules polynomiales. Par exemple, la transformation du plan

$$(x,y) \mapsto (y + Q(x), x) \tag{5.4}$$

est un tel automorphisme, quelque soit le polynôme $Q \in \mathbf{C}[x]$. Pour retrouver l'énoncé initial de Skolem, Mahler et Lech, il suffit de poser $k = d+1$, $z = (u(0), u(1), \ldots, u(d))$, $W = \{(x_0, \ldots, x_d) \in \mathbb{A}^k ; \; x_d = 0\}$, et de considérer la transformation linéaire

$$f(x_0, \ldots, x_d) = (x_1, \ldots, x_d, a_d x_d + a_{d-1} x_{d-1} + \cdots + a_0 x_0). \tag{5.5}$$

***Remarque 5.2*. —** Le théorème 5.1 est une version simplifiée de l'énoncé obtenu par Bell, Ghioca et Tucker, l'espace affine pouvant être remplacé par une autre variété algébrique (une surface K3 par exemple).

***Remarque 5.3*. —** Le théorème de Skolem, Mahler et Lech et celui de Bell, Ghioca et Tucker cachent un problème ouvert qui est bien décrit dans le chapitre 3.9 de [**24**] : il s'agit d'estimer la taille du plus petit entier n tel que $u(n) = 0$ (resp. $f^n(x) \in W$) en fonction des données initiales lorsqu'un tel entier existe.

5.2. Démonstration p-adique. — Démontrons le théorème 5.1 en supposant que f, W, et z ne sont pas définis sur $\mathbf{C}$ mais sur l'anneau $\mathbf{Z}_p$, avec $p \geq 3$. Autrement dit, z est un point de $\mathbb{A}^k(\mathbf{Z}_p) = \mathbf{Z}_p^k$, l'automorphisme f est défini par des formules polynomiales à coefficients dans $\mathbf{Z}_p$, et W est définie par un système fini d'équations polynomiales $E_i(\mathbf{x}) = 0$ qui sont aussi à coefficients dans $\mathbf{Z}_p$.

Quitte à conjuguer f par la translation $\mathbf{x} \mapsto \mathbf{x}+z$ et à changer W en $W-z$, nous pouvons supposer que $z=0$. D'après la remarque 4.5, il existe un entier $m>0$ tel que l'automorphisme $g(\mathbf{x}) = p^{-1}f^m(p\mathbf{x})$ vérifie les hypothèses du théorème de Bell et Poonen. Nous pouvons donc trouver un flot analytique $\Phi\colon \mathbf{Z}_p \times \mathbf{Z}_p^k \to \mathbf{Z}_p^k$ tel que $\Phi(t,\mathbf{x}) = g^t(\mathbf{x})$ dès que t appartient à $\mathbf{Z}$. Considérons alors les m variétés $W_j := p^{-1}f^j(W)$ obtenues en appliquant f^j pour $0 \leq j \leq m-1$ et en effectuant une homothétie de rapport $1/p$. L'ensemble $Pas_f(z;W)$ des temps de passages coïncide maintenant avec l'union des m ensembles P_j définis par

$$P_j = mPas_g(0,W_j) - j = \left\{ms - j\ ;\ s \in \mathbf{Z}\ \text{ et }\ g^s(0) \in W_j\right\}. \tag{5.6}$$

L'indice j étant fixé, deux cas peuvent se produire. Ou bien l'orbite de l'origine sous l'action de g n'intersecte W_j qu'un nombre fini de fois ; ou bien cette intersection est infinie. Dans ce deuxième cas, si $F \in \mathbf{Z}_p[\mathbf{x}]$ est une fonction polynomiale s'annulant sur W_j, alors $t \in \mathbf{Z}_p \mapsto F \circ \Phi(t,0)$ est une fonction analytique p-adique qui est nulle en tout point de l'ensemble infini $Pas_g(0,W_j)$. Par le principe des zéros isolés, $F \circ \Phi(t,0)$ est identiquement nulle, et donc $g^n(0) \in W_j$ pour tout n. Ainsi, $Pas_g(0,W_j) = \mathbf{Z}$ et P_j est égal à la progression arithmétique $m\mathbf{Z}+j$.

Nous avons donc bien montré que $Pas_f(z,W)$ est une union finie de progressions arithmétiques (de raisons nulles ou divisant m).

5.3. Du complexe au p-adique. — L'argument précédent ne fonctionne que si l'ensemble des données, à savoir f, W et z, sont définis par des formules à coefficients dans $\mathbf{Z}_p$. Voici un lemme qui permet de se ramener à cette situation.

Lemme 5.4. — *Soient K une extension de type fini du corps $\mathbf{Q}$ et S une partie finie de K. Il existe un nombre premier p et un plongement ι de K dans $\mathbf{Q}_p$ tel que $|\iota(s)|_p = 1$ pour tout élément non nul s de S. L'ensemble des p qui conviennent a une densité strictement positive parmi les nombres premiers.*

La seconde assertion signifie qu'il existe une constante $\alpha > 0$ telle que, parmi les n premiers nombres premiers, au moins αn nombres premiers conviennent, du moins lorsque n est suffisamment grand ; cette positivité de la densité ne sera pas utilisée dans ce texte.

Une fois ce lemme à notre disposition, nous pouvons démontrer le théorème 5.1. Le problème initial est posé sur le corps des nombres complexes, mais ne fait intervenir qu'un nombre fini de données algébriques à savoir f, W, et z. On fixe donc un système d'équations pour W, et l'on note S le sous-ensemble fini de $\mathbf{C}$ constitué des coordonnées de z et des coefficients qui apparaissent dans les équations de W et

dans les formules définissant f. Le lemme assure l'existence d'un plongement ι de $\mathbf{Q}(S)$ dans $\mathbf{Q}_p$ qui envoie S dans $\mathbf{Z}_p$. Appliquant ι aux données du problème, nous obtenons un automorphisme ${}^\iota f$, une sous-variété ${}^\iota W$ et un point ${}^\iota z$ de l'espace affine $\mathbb{A}_{\mathbf{Q}_p}$. Les temps de passage de l'orbite de ${}^\iota z$ sur ${}^\iota W$ ou de l'orbite de z sur W sont les mêmes, si bien que le paragraphe précédent termine la démonstration.

Le lemme 5.4 peut être démontré à l'aide du théorème de Chebotarev (voir [**16**]). Si l'on cherche juste un nombre premier p (disons $p \geq 3$) qui convient, on peut aussi raisonner de la manière suivante.

Démonstration du lemme 5.4. — Ecrivons K comme une extension algébrique d'une extension transcendante pure L de $\mathbf{Q}$. En notant ℓ le degré de transcendance de L sur $\mathbf{Q}$, nous pouvons fixer un isomorphisme $L \simeq \mathbf{Q}(t_1, \dots t_\ell)$ où les t_i sont des indéterminées. Le théorème de l'élément primitif montre qu'il existe $\alpha \in K$ tel que $K = L[\alpha]$. Soit χ le polynôme minimal de α sur L ; quitte à multiplier χ par un élément non nul de $\mathbf{Z}[t_1, \dots, t_\ell]$, nous pouvons supposer que χ appartient à l'anneau $\mathbf{Z}[t_1, \dots, t_\ell][x]$. Le discriminant de χ par rapport à la variable x sera noté δ : c'est un élément de $\mathbf{Z}[t_1, \dots, t_d]$.

Pour chaque élément s de l'ensemble $S \subset K$, il existe un polynôme $g_s \in L[x]$ tel que $s = g_s(\alpha)$. Nous fixerons g_s, ainsi qu'un polynôme $b_s \in \mathbf{Z}[t_1, \dots, t_l]$ tel que $b_s \times g_s$ soit un élément de $\mathbf{Z}[t_1, \dots, t_\ell][x]$. Le résultant de $\chi(x)$ et de $(b_s g_s)(x)$ sera noté R_s : c'est un élément de $\mathbf{Z}[t_1, \dots, t_\ell]$.

Choisissons des entiers $(a_1, \dots, a_\ell)$ tels que :

- $\delta(a_1, \dots, a_\ell)$ n'est pas nul ;
- $\chi(a_1, \dots, a_\ell)(x)$ n'est pas un polynôme constant (de la variable x) ;
- pour tout $s \in S$, $b_s(a_1, \dots, a_\ell)$ et $R_s(a_1, \dots, a_\ell)$ ne sont pas nuls.

Puis, notons $\mathcal{B}$ l'ensemble des nombres premiers p tels que (a) ces trois propriétés restent valables modulo p et (b) le polynôme $\chi(a_1, \dots, a_\ell)(x)$ a une racine modulo p. Le lemme 5.5, démontré ci-dessous, montre que $\mathcal{B}$ est un ensemble infini.

Maintenant, fixons un nombre premier p dans $\mathcal{B}$. Comme $\mathbf{Z}_p$ n'est pas dénombrable, nous pouvons trouver ℓ nombres $\tau_i \in \mathbf{Z}_p$ tels que $\mathbf{Q}(\tau_1, \dots, \tau_\ell)$ soit une extension transcendante pure de $\mathbf{Q}$. Le polynôme $\chi(a_1 + p\tau_1, \dots, a_\ell + p\tau_\ell)(x)$ a une racine modulo p ; comme $\delta(a_1, \dots, a_\ell)$ n'est pas nul modulo p, le lemme de Hensel assure l'existence d'une racine $\overline{\alpha} \in \mathbf{Z}_p$ de $\chi(a_1 + p\tau_1, \dots, a_\ell + p\tau_\ell)(x)$. Il existe donc un unique homomorphisme $\iota : K \to \mathbf{Q}_p$ tel que $\iota(t_i) = \tau_i$ et $\iota(\alpha) = \overline{\alpha}$. Cet homomorphisme envoie S dans $\mathbf{Z}_p$ car les nombres $\iota(b_s(a_1, \dots, a_\ell))$ sont dans $\mathbf{Z}_p$ et ne sont pas nuls modulo p, donc sont de norme p-adique égale à 1. □

Lemme 5.5. — *Soit $h(x) \in \mathbf{Z}[x]$ un polynôme à coefficients entiers de degré $d \geq 1$. Il existe une infinité de nombres premiers p tels que h ait une racine modulo p.*

Démonstration. — Dans le cas contraire, il existe un entier k et des nombres premiers $p_1, \ldots, p_k$ tels que toutes les valeurs $h(n)$ de h pour $n \in \mathbf{Z}$ sont de la forme

$$h(n) = (\pm 1) \prod_{j=1}^{k} p_j^{\alpha_j(n)}. \tag{5.7}$$

L'ensemble $h(\mathbf{Z}) \cap [-M, M]$ contient donc au plus $2(\log(M)/\log(2))^k$ éléments. Par ailleurs, $|h(n)|$ est de l'ordre de n^d lorsque n tend vers $+\infty$. Donc le cardinal $h(\mathbf{Z}) \cap [-M, M]$ est de l'ordre de $M^{1/d}$ lorsque M est grand. C'est une contradiction. □

Remarque 5.6. — Le lemme 5.4 est un outil efficace pour plonger un corps de type fini dans $\mathbf{Q}_p$ en contrôlant les valeurs absolues de certains éléments. En voici un autre, dû à Emmanuel Breuillard, Tsachik Gelander et Jacques Tits (voir [**25**], Lemma 4.1, et [**4**], § 2) : *si A est un anneau intègre de type fini et P est une partie infinie de A, il existe un corps local $\mathbf{k}$ et un plongement $\iota : A \to \mathbf{k}$ tel que $\iota(P)$ ne soit pas borné.*

6. Groupes de transformations algébriques

En guise de conclusion, nous allons voir comment la stratégie présentée au paragraphe précédent peut être utilisée pour étudier la structure des groupes de type fini agissant fidèlement par transformations polynomiales ou rationnelles.

6.1. Les propriétés de Malcev et Selberg. — Nous dirons qu'un groupe Γ est

- **résiduellement fini** si, pour tout élément γ de Γ distinct de l'identité, il existe un groupe fini F et un homomorphisme $\alpha : \Gamma \to F$ tel que $\alpha(\gamma) \neq 1_F$.
- **virtuellement sans torsion** s'il existe un sous-groupe d'indice fini $\Gamma_0 \subset \Gamma$ qui est sans torsion (i.e. tout élément γ de Γ_0 engendre un sous-groupe cyclique infini).

Anatolii V. Malcev et Atle Selberg ont montré que tout groupe linéaire de type fini vérifie ces deux propriétés.

Théorème 6.1 **(Bass et Lubotzky, [1]).** — *Soit Γ un groupe de type fini. Soit $\mathbf{k}$ un corps et X une variété algébrique définie sur $\mathbf{k}$. Si Γ se plonge dans le groupe des automorphismes $\mathsf{Aut}(X_{\mathbf{k}})$, alors Γ est résiduellement fini et virtuellement sans torsion.*

Nous nous contenterons d'esquisser la démonstration de ce théorème d'Hyman Bass et Alexander Lubotzky lorsque le corps $\mathbf{k}$ est de caractéristique nulle et la variété X est l'espace affine. Nous supposerons donc que Γ est un sous-groupe de $\mathsf{Aut}(\mathbb{A}^k_{\mathbf{k}})$. Puisque Γ est de type fini, nous pouvons fixer une partie finie et symétrique $S = \{g_1, \ldots, g_s\} \subset \Gamma$ engendrant Γ, puis remplacer $\mathbf{k}$ par l'extension de type finie $\mathbf{k}_0$ de $\mathbf{Q}$ engendrée par l'ensemble C_S des coefficients des formules polynomiales définissant les g_i. Le lemme 5.4 fournit un nombre premier $p \geq 3$ et un plongement $\iota\colon \mathbf{k}_0 \to \mathbf{Q}_p$ telle que $\iota(C_S) \subset \mathbf{Z}_p$. Le groupe Γ peut donc être plongé dans le groupe des automorphismes h de $\mathbb{A}^k_{\mathbf{Q}_p}$ tels que h et h^{-1} sont définis par des formules à coefficients dans $\mathbf{Z}_p$. Ainsi, Γ devient un sous-groupe de $\mathsf{Diff}\langle \mathbf{Z}^k_p \rangle$. En particulier, Γ agit sur l'ensemble fini des polydisques de rayon p^{-r}, ceci pour tout $r > 0$. Nous obtenons ainsi des homomorphismes à valeurs dans le groupe $\mathsf{Bij}(\mathbb{A}^k(\mathbf{Z}/p^r\mathbf{Z}))$ des permutations de $\mathbb{A}^k(\mathbf{Z}/p^r\mathbf{Z})$. Ceux-ci suffisent à montrer que Γ est résiduellement fini, car une isométrie de $\mathbf{Z}^k_p$ fixant chaque polydisque est l'identité.

Notons maintenant Γ_0 le sous-ensemble de Γ constitué des éléments $f \in \Gamma$ tel que le développement de Taylor $f(\mathbf{x}) = A_0 + A_1(\mathbf{x}) + \sum_{m\geq 2} A_m(\mathbf{x})$ satisfasse $A_0 \equiv 0 \mod (p^2)$ et $A_1 \equiv \mathrm{Id} \mod (p)$; d'après la remarque 4.5, Γ_0 est un sous-groupe d'indice fini de Γ et si f est un élément de Γ_0 alors le théorème de Bell et Poonen peut être appliqué à $p^{-1}f(p\mathbf{x})$; il existe donc un flot analytique Φ tel que $\Phi(n,\mathbf{x}) = (p^{-1}f(p\mathbf{x}))^n$ pour tout n dans $\mathbf{Z}$. Si $f^m = \mathrm{Id}$, avec $m \geq 1$, alors $\Phi(nm,\mathbf{x}) = \mathrm{Id}$ pour tout n dans $\mathbf{Z}$, et donc $\Phi(t,\mathbf{x}) = \mathrm{Id}$ pour tout t par le principe des zéros isolés, ce qui entraine $f = \mathrm{Id}$. Nous avons donc montré que Γ_0 est sans torsion.

Remarque 6.2. **—** La démonstration que nous venons de donner est la même que celle de Bass et Lubotzky, qui elle même reprend les arguments de Malcev et Selberg. Elle remonte à Minkowski, qui a montré dans [**19**] que le sous-groupe de $\mathsf{GL}_k(\mathbf{Z})$ formé des matrices qui sont égales à l'identité modulo 3 est sans torsion.

6.2. Le programme de Zimmer. **—** Soit Γ le groupe $\mathsf{SL}_{r+1}(\mathbf{Z})$, avec $r \geq 1$. Plus généralement, soit Γ un réseau d'un groupe de Lie G tel que l'algèbre de Lie de G est simple et le nombre de composantes connexes de G est fini. L'action adjointe de G sur son algèbre de Lie est une représentation linéaire dont le noyau est fini. Le **rang** de G est la dimension maximale d'un sous-groupe connexe $A \subset G$ dont l'action adjointe est diagonalisable ; le groupe A est alors isomorphe à $(\mathbf{R}^*_+)^r$ où r est le rang de G. Par exemple, $\mathsf{SL}_{r+1}(\mathbf{R})$ est de rang r, tandis que $\mathsf{SO}_{p,q}(\mathbf{R})$ est de rang $\min(p,q)$. Dire que Γ est un réseau signifie que Γ est un sous-groupe discret de

G, et qu'il existe une partie $\Omega \subset G$ de mesure de Haar finie telle que $\Gamma\Omega = G$; c'est le cas de $\Gamma = \mathsf{SL}_{r+1}(\mathbf{Z})$ dans $G = \mathsf{SL}_{r+1}(\mathbf{R})$.

La conjecture suivante est l'analogue, pour les transformations birationnelles des variétés projectives, d'une conjecture de Robert J. Zimmer pour les difféomorphismes des variétés réelles compactes (voir [**9, 13**]).

Conjecture 6.3. — *Soit* $\mathbf{k}$ *un corps. Soit* $X_{\mathbf{k}}$ *une variété projective de dimension* d *définie sur* $\mathbf{k}$*. Soit* Γ *un réseau d'un groupe de Lie* G *de rang* $r \geq 2$*. Si* Γ *se plonge dans le groupe des transformations birationnelles* $\mathsf{Bir}(X_{\mathbf{k}})$*, alors* $d \geq r$*.*

Il se trouve que le lemme d'interpolation de Bell et Poonen peut être utile pour aborder cette conjecture. Pour expliquer l'idée générale, supposons que $\mathsf{SL}_{r+1}(\mathbf{Z})$ se plonge dans le groupe des automorphismes de l'espace affine de dimension k définis (ainsi que leurs inverses) par des formules à coefficients dans $\mathbf{Z}_p$. En changeant $\mathsf{SL}_{r+1}(\mathbf{Z})$ en un sous-groupe Γ d'indice fini, et en conjuguant Γ par l'homothétie $\mathbf{x} \mapsto p\mathbf{x}$, on peut alors supposer que $f \equiv \mathbf{x} \mod (p)$ pour tout élément f de Γ. Ainsi, chaque élément f peut être inclus dans un flot analytique p-adique. Il s'agit alors de montrer que le groupe Γ tout entier peut-être inclus dans un "groupe de Lie p-adique" $G \subset \mathsf{Diff}\langle \mathbf{Z}_p^k \rangle$ qui est localement isomorphe à $\mathsf{SL}_{r+1}(\mathbf{Z}_p)$. C'est ce que nous démontrons avec Junyi Xie en utilisant la propriété des groupes de congruence pour $\mathsf{SL}_{r+1}(\mathbf{Z})$ (ou une présentation de $\mathsf{SL}_{r+1}(\mathbf{Z})$ par générateurs et relations). La conclusion $k \geq r+1$ découle alors de la théorie de Lie, dans le cadre p-adique. Le théorème suivant reprend cette idée, mais il nécessite des arguments complémentaires utilisant la propriété (T) de Kazhdan et les estimées de Lang-Weil pour pouvoir être appliqué aux groupes de transformations birationnelles.

Théorème 6.4 **(Cantat, Junyi Xie [10]).** — *Soit* Γ *un réseau d'un groupe de Lie (presque) simple et connexe de rang* r *qui n'est pas cocompact. Soit* $\mathbf{k}$ *un corps de caractéristique nulle. Si* Γ *agit fidèlement sur une* $\mathbf{k}$*-variété projective* X *par transformations birationnelles, alors* $\dim(X_{\mathbf{k}}) \geq r$*.*

L'hypothèse stipulant que Γ n'est pas cocompact correspond à l'utilisation que nous faisons de la propriété des sous-groupes de congruence (connue dans ce cadre). L'hypothèse sur la caractéristique du corps est utilisée pour passer à un corps p-adique. Il se peut que ces deux hypothèses soient superflues.

Remarque 6.5. — Aaron Brown, David Fisher et Sebastian Hurtado ont récemment démontré la conjecture de Zimmer pour les actions de réseaux cocompacts par difféomorphismes sur des variétés compactes. Leur démonstration semble pouvoir

s'étendre à tous les réseaux (voir [**6, 5, 9**]). Les actions de difféomorphismes de classe $\mathcal{C}^1$ sur le cercle et celles de difféomorphismes holomorphes sur les variétés kählériennes compactes avaient été traitées dans [**14**] et [**8, 11**]. Les techniques présentées dans ces articles sont très différentes, et c'est d'ailleurs dans la variété des techniques employées que réside l'un des intérêts majeur de cette conjecture.

Remarque 6.6. **—** En caractéristique p, il est intéressant de voir que le groupe de Nottingham, c'est-à-dire le groupe des séries formelles $z + \sum_k a_k z^k$ à coefficients dans $\mathbf{Z}/p\mathbf{Z}$ (muni de la composition), contient tous les pro-p groupes qui sont engendrés topologiquement par un nombre fini d'éléments [**7**].

Remerciements. **—** Ce texte s'appuie sur trois interventions orales : à Lille lors du deuxième congrès de la Société Mathématique de France, au colloquium de mathématiques de Nantes et à celui de Toulouse. Il s'inspire d'un exposé de Bjorn Poonen donné lors d'une conférence organisée à Chicago par Laura de Marco. Il doit beaucoup aux nombreuses discussions que j'ai eues avec Marc Abboud, Pascal Autissier, Antoine Chambert-Loir, Antoine Ducros, Junyi Xie. François Maucourant, Olga Paris-Romaskevich et le rapporteur m'ont permis d'améliorer considérablement la présentation : un grand merci à eux.

Références

[1] Hyman Bass and Alexander Lubotzky. Automorphisms of groups and of schemes of finite type. *Israel J. Math.*, 44(1) :1–22, 1983.

[2] Jason P. Bell. A generalised Skolem-Mahler-Lech theorem for affine varieties. *J. London Math. Soc. (2)*, 73(2) :367–379, 2006.

[3] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. The dynamical Mordell-Lang problem for étale maps. *Amer. J. Math.*, 132(6) :1655–1675, 2010.

[4] Emmanuel Breuillard and Tsachik Gelander. A topological Tits alternative. *Ann. of Math. (2)*, 166(2) :427–474, 2007.

[5] Aaron Brown, David Fisher, and Sebastian Hurtado. Zimmer's conjecture for actions of $SL(m, \mathbf{Z})$. *arXiv :1710.02735*, pages 1–41, Octobre 2017.

[6] Aaron Brown, David Fisher, and Sebastian Hurtado. Zimmer conjecture : sub exponential growth, measure rigidity, and strong property (T). *arXiv :1608.04995*, pages 1–32, Septembre 2016.

[7] Rachel Camina. Subgroups of the Nottingham group. *J. Algebra*, 196(1) :101–113, 1997.

[8] Serge Cantat. Version kählérienne d'une conjecture de Robert J. Zimmer. *Ann. Sci. École Norm. Sup. (4)*, 37(5) :759–768, 2004.

[9] Serge Cantat. Progrès récents concernant le programme de Zimmer. *Astérisque*, 2017. Séminaire Bourbaki, Vol. à paraitre.

[10] Serge Cantat and Junyi Xie. Algebraic actions of discrete groups : the p-adic method. *Acta Math.*, 220(2) :239–295, 2018.

[11] Serge Cantat and Abdelghani Zeghib. Holomorphic actions, Kummer examples, and Zimmer program. *Ann. Sci. Éc. Norm. Supér. (4)*, 45(3) :447–489, 2012.

[12] Jean-Pierre Demailly. *Analyse numérique et équations différentielles*. Grenoble Sciences. EDP Sciences, Les Ulis, fourth edition, 2016.

[13] David Fisher. Groups acting on manifolds : around the Zimmer program. In *Geometry, rigidity, and group actions*, Chicago Lectures in Math., pages 72–157. Univ. Chicago Press, Chicago, IL, 2011.

[14] Étienne Ghys. Actions de réseaux sur le cercle. *Invent. Math.*, 137(1) :199–231, 1999.

[15] Svetlana Katok. *p-adic analysis compared with real*, volume 37 of *Student Mathematical Library*. American Mathematical Society, Providence, RI ; Mathematics Advanced Study Semesters, University Park, PA, 2007.

[16] Christer Lech. A note on recurring series. *Ark. Mat.*, 2 :417–421, 1953.

[17] Kurt Mahler. An interpolation series for continuous functions of a p-adic variable. *J. Reine Angew. Math.*, 199 :23–34, 1958.

[18] John Milnor. *Dynamics in one complex variable*, volume 160 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, third edition, 2006.

[19] Hermann Minkowski. Zur Theorie der positiven quadratischen Formen. *J. Reine Angew. Math.*, 101 :196–202, 1887.

[20] Ricardo Pérez Marco. Solution complète au problème de Siegel de linéarisation d'une application holomorphe au voisinage d'un point fixe (d'après J.-C. Yoccoz). *Astérisque*, (206) :Exp. No. 753, 4, 273–310, 1992. Séminaire Bourbaki, Vol. 1991/92.

[21] Ricardo Pérez Marco. Sur les dynamiques holomorphes non linéarisables et une conjecture de V. I. Arnold. *Ann. Sci. École Norm. Sup. (4)*, 26(5) :565–644, 1993.

[22] Bjorn Poonen. p-adic interpolation of iterates. *Bull. Lond. Math. Soc.*, 46(3) :525–527, 2014.

[23] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[24] Terence Tao. *Structure and randomness*. American Mathematical Society, Providence, RI, 2008. Pages from year one of a mathematical blog.

[25] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20 :250–270, 1972.

[26] Jean-Christophe Yoccoz. Théorème de Siegel, nombres de Bruno et polynômes quadratiques. *Astérisque*, (231) :3–88, 1995. Petits diviseurs en dimension 1.

SERGE CANTAT, Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
E-mail : serge.cantat@univ-rennes1.fr