Le théorème de Skolem, Mahler et Lech

Serge Cantat

LE THÉORÈME DE SKOLEM, MAHLER ET LECH

SERGE CANTAT

Ces notes constituent une version étendue et complétée du cours délivré à l'école polytechnique les 20 et 21 Avril 2023, le cours étant principalement tourné vers la démonstration du théorème de Skolem, Mahler et Lech, y compris dans un cadre non linéaire obtenu par Jason Bell.

INTRODUCTION : LES TEMPS DE PASSAGE

Soit X un ensemble. Les permutations de X forment un groupe pour la composition ; nous le noterons $\mathsf{Bij}(X)$. Si $f \in \mathsf{Bij}(X)$ les puissances f^n sont donc obtenues par composition ; ainsi, $f^0 = \mathsf{Id}_X$ est l'identité, f^{-1} est l'inverse de f, et $f^{n+1} = f \circ f^n$ pour tout $n \in \mathbf{Z}$.

Soit z un élément de X. L'**orbite** de z sous l'action de f est la suite $z_n = f^n(z)$, avec $n \in \mathbf{Z}$; l'orbite est donc ici considérée comme une suite paramétrée par un temps discret $n \in \mathbf{Z}$. L'ensemble $\mathrm{Orb}_f(z) := \{f^n(z)\,;\, n \in \mathbf{Z}\}$ sera aussi appelé orbite de z pour f. L'orbite de z est **périodique** s'il existe un entier $q \geq 1$ tel que $f^{n+q}(z) = f^n(z)$ pour tout $n \in \mathbf{Z}$; on dit alors que q est une période de z. De manière équivalente, l'orbite de z est périodique si $\mathrm{Orb}_f(z)$ est un ensemble fini. Si k désigne le cardinal de $\mathrm{Orb}_f(z)$, k est la plus petite période de z ; on dit alors que k est la période de z.

Si W est un sous-ensemble de X, l'ensemble des **temps de passage** de z dans W est, par définition, l'ensemble des entiers

$$\mathrm{Pas}_f(z;W) = \{n \in \mathbf{Z}\,;\, f^n(z) \in W\}; \tag{0.1}$$

l'ensemble des temps de passage positifs est $\mathrm{Pas}_f^+(z;W) = \{n \in \mathbf{N}\,;\, f^n(z) \in W\}$.

Les temps de passage peuvent former un sous-ensemble quelconque de $\mathbf{Z}$. En effet, soit T un tel sous-ensemble. Choisissons $X = \mathbf{Z}$, $f\colon X \to X$ la translation $s \mapsto s+1$ et $W = T$. Alors $\mathrm{Pas}_f(0;W) = T$.

Date: 2023.

Lorsque X est un espace vectoriel complexe, $f\colon X \to X$ est une transformation linéaire, et W est un sous-espace vectoriel, le théorème de Skolem, Mahler et Lech stipule que $\mathrm{Pas}_f(z;W)$ est une union finie de progressions arithmétiques (voir le § 2 ci-dessous). Le but principal de ce texte est de décrire comment l'analyse p-adique permet de montrer un tel énoncé, y compris dans le cadre plus général, non linéaire, où f est une transformation polynomiale de l'espace affine qui est inversible et dont l'inverse est aussi polynomiale. Auparavant, un peu en guise d'échauffement, un peu pour introduire d'autres méthodes issues de la théorie ergodique, nous analyserons une situation plus générale qui apparaît fréquemment en sciences physiques.

1. Théorèmes de récurrence

Ce paragraphe présente le cas, maintenant classique, où f préserve une mesure de probabilité et A est un ensemble de mesure strictement positive : nous verrons que l'ensemble $\mathrm{Pas}_f(z;A) \subset \mathbf{Z}$ a une densité strictement positive, ceci pour presque tout point z.

1.1. **Le théorème de récurrence de Poincaré.** Supposons que X est muni d'une tribu $\mathcal{T}$ et d'une mesure de probabilité μ, et que $f\colon X \to X$ est une application mesurable qui préserve μ. Ceci signifie que

$$\mu(f^{-1}(A)) = \mu(A) \tag{1.1}$$

pour tout $A \in \mathcal{T}$ (il n'est pas nécessaire de supposer f inversible pour l'instant).

Exemple 1.1. Soit $X \subset \mathbf{R}^2$ le carré $[-1/2,1/2]^2$, muni de la tribu des ensembles boréliens et de la mesure de Lebesgue. Soit $\mathbf{v}\colon \mathbf{R}^2 \to \mathbf{R}^2$ un champ de vecteurs de classe C^∞ qui est nul en dehors de X. En résolvant l'équation différentielle

$$\gamma'(t) = \mathbf{v}(\gamma(t)), \tag{1.2}$$

avec la condition initiale $\gamma(0) = z \in X$, on obtient une courbe $\gamma_z\colon \mathbf{R} \to \mathbf{R}^2$ tracée dans X. Fixons $t \in \mathbf{R}$, et notons $\Phi_t(z)$ l'application qui, à $z \in X$, associe $\gamma_z(t)$; ceci définit un homéomorphisme $\Phi_t\colon X \to X$ (de classe C^∞). Si $\mathbf{v}$ est à divergence nulle, ces homéomorphismes préservent tous la mesure de Lebesgue. Pour construire des exemples, il suffit donc de construire des champs de vecteurs à divergence nulle. Dans le disque de centre $(0,0)$ et de rayon $r < 1/2$, on peut prendre $\mathbf{v}(x,y) = h(x^2+y^2)(y,-x)$, où $s \in \mathbf{R} \mapsto h(s) \in \mathbf{R}$ est de classe C^∞ et est nulle si $|s| \geq r$; en changeant la fonction h, le centre du dique, et son

rayon, on construit ainsi de nombreux homéomorphismes du carré préservant l'aire, que l'on peut ensuite composer entre eux pour construire de nouveaux exemples d'homéomomorphismes du carré préservant la mesure de Lebesgue.

Soit A un élément de $\mathcal{T}$. Nous dirons que B est de **mesure totale** dans A si $B \in \mathcal{T}$, $B \subset A$ et $\mu(B) = \mu(A)$.

Théorème 1.2 (de récurrence de Poincaré)**.** *Soit $(X, \mathcal{T})$ un ensemble mesurable, muni d'une mesure de probabilité μ. Soit $f\colon X \to X$ une application mesurable préservant μ. Si $A \in \mathcal{T}$, il existe un sous-ensemble A_∞ de mesure totale dans A tel que pour tout $z \in A_\infty$, l'ensemble $\mathrm{Pas}_f^+(z, A_\infty)$ est infini.*

Montrons tout d'abord que l'orbite positive de presque tout $z \in A$ revient au moins une fois visiter A. Pour cela, considérons l'ensemble $B \in \mathcal{T}$ défini par

$$B = \{z \in A\,;\, f^n(z) \notin A, \forall n \geq 1\}\,; \tag{1.3}$$

il s'agit de montrer que $\mu(B) = 0$. Par définition, $f^{-j}(B) \cap B = \emptyset$ pour tout $j \geq 1$, donc $f^{-m}(B) \cap f^{-n}(B) = \emptyset$ pour tous $m \neq n \geq 0$; autrement dit, les $f^{-n}(B)$ sont deux à deux disjoints. La mesure de $\cup_{n\geq 0} f^{-n}(B)$ est donc égale à la somme des $\mu(f^{-n}(B))$, si bien que $\sum_{n\geq 1} \mu(f^{-n}(B)) \leq \mu(X) = 1$. Mais $\mu(f^{-n}(B)) = \mu(B)$ pour tout n car f préserve μ, donc $\mu(B) = 0$.

Reprenons cet argument en fixant un entier $N \geq 1$ et en notant B_N l'ensemble défini par

$$B_N = \{z \in A\,;\, f^n(z) \notin A, \forall n \geq N\}; \tag{1.4}$$

le cas $N = 1$ correspond à l'ensemble B étudié ci-dessus. Alors $f^{-Nj}(B_N) \cap B_N = \emptyset$ pour tout $j \geq 1$, donc $f^{-Nm}(B_N) \cap f^{-Nn}(B_N) = \emptyset$ pour tous $m \neq n \geq 0$. On en déduit comme précédemment que l'ensemble A_N des points de A dont l'orbite revient dans A après N itérations est de mesure totale. L'intersection A_∞ des A_N pour $N \geq 1$ est exactement l'ensemble des $z \in A$ dont l'orbite passe une infinité de fois dans A. Et $\mu(A_\infty) = \mu(A)$ parce que $\mu(A \setminus A_N) = 0$ pour tout N.

Si $z \in A_\infty$ et $f^s(z) \in A$ alors $f^s(z)$ appartient en fait à A_∞, car l'orbite de z doit passer une infinité de fois dans A après l'instant s. Les retours successifs de $f^n(z)$ dans A s'effecture donc en fait dans A_∞, et le théorème est établi.

Pour $z \in A_\infty$, nous noterons $r_A(z)$, le plus petit entier $r \geq 1$ tel que $f^r(z) \in A$; c'est le premier **temps de retour** de z dans A. On vérifie que l'ensemble

$$A_\infty(s) = \{z \in A_\infty\,;\, r_A(z) = s\} \tag{1.5}$$

appartient à $\mathcal{T}$ et que les $A_\infty(s)$ forment une partition de A_∞.

1.2. **Espérance du temps de retour, densité des temps de passage.** Nous dirons que $B \subset X$ est **f-invariant** si $f^{-1}(B) = B$, et que μ est **ergodique** pour l'action de f si tout sous-ensemble invariant $B \in \mathcal{T}$ est de mesure nulle ou totale, i.e. $\mu(B) = 0$ ou 1 (voir [6, 10] pour des exemples de transformations et mesures ergodiques).

Théorème 1.3 (de Rokhlin sur la moyenne des temps de retour)**.** *Soit $(X, \mathcal{T})$ un ensemble mesurable muni d'une mesure de probabilité μ. Soit $f : X \to X$ une bijection bimesurable préservant μ, pour laquelle μ est ergodique. Si $A \in \mathcal{T}$ et $\mu(A) > 0$, la moyenne des temps de retour $r_A(z)$, pour $z \in A$, est l'inverse de la mesure de A :*

$$\frac{1}{\mu(A)} \int_A r_A(z) d\mu(z) = \frac{1}{\mu(A)}.$$

Pour obtenir cette formule, conservons les notations employées au paragraphe précédent. Pour $0 \leq n \leq s-1$, les éléments de $f^n(A_\infty(s))$ sont exactement les z tels que $f^{-n}(z)$ est dans A_∞, $f^{s-n}(z)$ est dans A_∞, et aucun des $f^k(z)$ n'est dans A_∞ pour $-n < k < s-n$. Ces ensembles sont donc disjoints :

$$f^n(A_\infty(s)) \cap f^m(A_\infty(r)) = \emptyset \tag{1.6}$$

si $0 \leq n \leq s-1$, $0 \leq m \leq r-1$, et $(n,s) \neq (m,r)$. Les $f^n(A_\infty(s))$, avec $s \geq 1$ et $0 \leq n \leq s-1$, forment donc une partition de $A' := \cup_{n \geq 0} f^n(A_\infty)$. Par construction, $f(A') \subset A'$; puisque f est inversible et préserve μ, nous en déduisons que $f(A') = A'$ à un ensemble de mesure nulle près ; par ergodicité, nous obtenons $A' = X$, à un ensemble de mesure nulle près. Donc

$$1 = \mu(A') = \sum_{0 \leq n < s} \mu(f^n(A_\infty(s))) = \sum_s s\mu(A_\infty(s)) = \int_A r_A(z) d\mu(z), \tag{1.7}$$

ce qu'il fallait démontrer.

Considérons l'application $f_A : A_\infty \to A_\infty$ définie par les premiers retours : si $z \in A_\infty$, alors $f_A(z) = f^{r_A(z)}(z)$; de manière équivalente,

$$f_A(z) = f^s(z) \quad \text{si} \quad z \in A_\infty(s). \tag{1.8}$$

En utilisant comme ci-dessus la partition de A_∞ en les $A_\infty(s)$, on vérifie facilement que f_A préserve la mesure de probabilité

$$\mu_A = \frac{1}{\mu(A_\infty)} \mu_{|A_\infty} \tag{1.9}$$

et que μ_A est ergodique pour l'action de f_A (car μ est supposée ergodique).

Les passages successifs de l'orbite de z dans A correspondent aux points suivants : d'abord $f_A(z)$ à l'instant $r_1(z) = r_A(z)$, puis $f_A^2(z)$ à l'instant $r_1(z) + r_2(z)$ avec $r_2(z) = r_A(f_A(z))$, puis $f_A^3(z)$ à l'instant $r_1(z) + r_2(z) + r_3(z)$ avec $r_3(z) = r_A(f_A^2(z))$, etc. Ainsi, le n-ème temps de passage dans A est

$$r_A(z;n) = \sum_{j=0}^{n-1} r_A(f_A^j(z)). \tag{1.10}$$

Le théorème ergodique de Birkhoff [1] montre que

$$\lim_{n\to+\infty} \frac{1}{n} r_A(z;n) = \int_A r_A(z) d\mu_A(z) \tag{1.11}$$

pour presque tout z (c'est-à-dire pour z dans un sous-ensemble A_∞ de mesure 1 pour μ_A). Avec le théorème de Rokhlin, nous obtenons l'énoncé suivant : *pour presque tout $z \in A$, le n-ème temps de passage de l'orbite de z dans A est de l'ordre de $n/\mu(A)$; le nombre d'instants $n \le N$ pour lesquels $f^n(z) \in A$ est donc comparable à $N\mu(A)$ lorsque N est grand.*

Dans $\mathrm{Pas}_f^+(z;A)$, on peut alors trouver des progressions arithmétiques de longueur arbitraire : voir [10] et [11] pour l'interaction entre théorie ergodique, temps de passage, et étude des sous-ensembles $T \subset \mathbf{N}$ de densité positive.

Exemple 1.4 ([11], §3)**.** Soit q un réel > 4. Soit

$$T = \{r_1 < r_2 < \cdots < r_n < \ldots\} \tag{1.12}$$

une suite d'entiers ≥ 1 telle que $r_{n+1} \ge q r_n$. Considérons le cercle $X = \mathbf{R}/\mathbf{Z}$, l'intervalle $I := [1/3;2/3] \subset \mathbf{R}/\mathbf{Z}$ et les sous-ensembles Λ_n de $\mathbf{R}/\mathbf{Z}$ définis par

$$\Lambda_n = \{t \in \mathbf{R}/\mathbf{Z}\,;\, r_n t \in I\}. \tag{1.13}$$

La longueur de I est $1/3$, donc Λ_n est constitué de r_n intervalles fermés de longueur $(3r_n)^{-1}$ qui sont répétés périodiquement avec période r_n^{-1} ; par exemple, si r_n était égal à 5, on aurait les 5 intervalles $J_1 = [1/15;2/15]$, $J_2 = J_1 + 1/5$, …, jusqu'à $J_5 = J_1 + 4/5 = [13/15;14/15]$.

Comme $r_{n+1} > 4r_n$, chacun des intervalles constituant Λ_n contient au moins un des intervalles constituant Λ_{n+1} donc l'intersection Λ des compacts Λ_n n'est pas vide. Soit λ un élément de Λ et $f\colon X \to X$ la translation $f(t) = t + \lambda$; elle préserve la mesure de Lebesgue $\mu = dt$. Soit $A \subset X$ un intervalle de longueur $< 1/6$. Alors $f^r(A) = A + r\lambda$, donc si $t \in A$ et $f^r(t) \in A$, alors $t + r\lambda$ et t sont à

1. La démonstration du théorème de Birkhoff est nettement plus ardue que celle des théorèmes de Poincaré et Rokhlin ; voir [6].

distance $< 1/6$; comme $r_n\lambda \in [1/3, 2/3]$, ceci montre que $f^{r_n}(A) \cap A$ est vide pour tout n.

Ainsi, l'ensemble lacunaire T est disjoint de $\mathrm{Pas}_f(t;A)$ pour tout $t \in A$.

Par contre, si l'on considère un sous-ensemble $S = \{s_1 < s_2 < \cdots < s_n < \cdots\}$ de $\mathbf{N}$ et l'ensemble $D = \{s_j - s_i \,;\, s_i < s_j \in S\}$, alors pour toute transformation $f\colon X \to X$ comme dans le théorème 1.3 et toute partie $A \subset X$ de mesure positive, il existe un entier $d \in D$ et une partie $A' \subset A$ de mesure positive telle que $f^d(A') \subset A$. Ainsi, D contient toujours des temps de retour de A dans A.

2. Transformations algébriques et arithméticité des temps de passage

Nous énonçons maintenant le théorème de Skolem, Mahler et Lech, ainsi que la version non linéaire – mais polynomiale – obtenue par Bell (voir [17, 14, 13] *et* [2, 4]*).*

Théorème 2.1 (de Skolem, Mahler, et Lech)**.** *Soit V un espace vectoriel complexe de dimension finie. Soit $f\colon V \to V$ une application linéaire inversible. Si $z \in V$ et si W est un sous-espace de V, l'ensemble des temps de passage $\mathrm{Pas}_f(z;W)$ est une union finie de progressions arithmétiques.*

Ceci signifie qu'il existe un ensemble fini de couples $(a_i, r_i) \in \mathbf{Z} \times \mathbf{Z}$, $i \in I$, tels que

$$\mathrm{Pas}_f(z;W) = \bigcup_{i\in I} \{a_i + nr_i \,;\, n \in \mathbf{Z}\}. \tag{2.1}$$

Chaque $\{a_i + nr_i \,;\, n \in \mathbf{Z}\}$ est une progression arithmétique, dont la raison r_i peut-être nulle; l'ensemble $\mathrm{Pas}_f(z;W)$ est infini si et seulement si $r_i \neq 0$ pour au moins un i.

Un énoncé analogue vaut encore sans supposer f inversible si l'on restreint l'étude aux temps de passage positifs; dans ce cas, les progressions arithmétiques sont de la forme $\{a_i + nr_i \,;\, n \in \mathbf{N}\}$, avec les a_i et r_i dans $\mathbf{N}$. En effet, le sous-espace

$$V' = \bigcap_{n\geq 0} f^n(V) = \bigcap_{n=0}^{\dim(V)} f^n(V) \tag{2.2}$$

est un sous-espace strict de V, $f(V') = V'$ et $f_{|V'}\colon V' \to V'$ est inversible. De plus $f^n(z) \in V'$ pour tout $n \geq \dim(V)$, donc le théorème de Skolem, Mahler et Lech peut être appliqué à $f_{|V'}$, $W \cap V'$ et $f^{\dim(V)}(z)$ pour conclure que $\mathrm{Pas}_f^+(z;W)$ est une union finie de progressions arithmétiques.

Corollaire 2.2. *Si $(u(n))_{n\geq 0}$ est une suite de nombres complexes définie par une relation de récurrence linéaire*

$$u(n+m) = \alpha_0 u(n) + \alpha_1 u(n+1) + \cdots + \alpha_{m-1} u(n+m-1)$$

et des conditions initiales $u(0) = z_0$, …, $u(m-1) = z_{m-1}$, alors $\{n \in \mathbf{N} \,;\, u_n = 0\}$ est une union finie de progressions arithmétiques.

Démonstration. Notons V l'espace $\mathbf{C}^m$, $(\mathbf{x}_1, \ldots, \mathbf{x}_m)$ les coordonnées et $z = (z_0, \ldots, z_{m-1})$. Les vecteurs $\mathbf{u}(n) = (u(n), u(n+1), \ldots, u(n+m-1))$ vérifient la relastion de récurrence $\mathbf{u}(n+1) = M\mathbf{u}(n)$ où M est la matrice compagnon dont les $m-1$ premières lignes sont $(0,1,0,\ldots,0)$, $(0,0,1,0\ldots,0)$, …, et $(0,0,\ldots,0,1)$ et la dernière ligne est $(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$. Ainsi, en notant W l'hyperplan d'équation $\mathbf{x}_1 = 0$, $\{n \,;\, u(n) = 0\}$ coïncide avec $\mathrm{Pas}_M(z; W)$. □

Un inconvénient du théorème de Skolem, Mahler et Lech est l'absence d'effectivité du résultat. Le **problème de Skolem** est le suivant : *existe-t-il un algorithme qui, étant donnée une suite (u_n) définie par une relation de récurrence linéaire à coefficients entiers et une condition initiale, détermine si, oui ou non, u_n s'annule pour au moins un $n \in \mathbf{N}$?* À l'heure actuelle, ce problème est encore ouvert (voir [19, 3]).

Pour décrire le théorème de Jason Bell, quelques notions de géométrie algébrique sont nécessaires.

Soit $\mathbf{K}$ un corps. Soit $\mathbb{A}^m$ l'espace affine de dimension m sur $\mathbf{K}$, muni d'un jeu de coordonnées affines $(\mathbf{x}_1, \ldots, \mathbf{x}_m)$ fixé une fois pour toutes. Si f_1, f_2, …, f_m sont des polynômes à coefficients dans $\mathbf{K}$ en les variables $(\mathbf{x}_1, \ldots, \mathbf{x}_m)$, l'application $f\colon \mathbb{A}^m \to \mathbb{A}^m$ définie par

$$f(\mathbf{x}_1, \ldots, \mathbf{x}_m) = (f_1(\mathbf{x}_1, \ldots, \mathbf{x}_m), \ldots, f_m(\mathbf{x}_1, \ldots, \mathbf{x}_m)) \tag{2.3}$$

est, par définition, un endomorphisme (polynomial) de l'espace affine. Si les coefficients des f_i sont dans un sous-anneau R de $\mathbf{K}$, on dit que f est un **endomorphisme** défini sur R ; on note alors $f\colon \mathbb{A}^m_R \to \mathbb{A}^m_R$, ou $f \in \mathsf{End}(\mathbb{A}^m_R)$. La composition $f \circ g$ de deux éléments de $\mathsf{End}(\mathbb{A}^m_R)$ est encore un élément de $\mathsf{End}(\mathbb{A}^m_R)$. Les éléments inversibles de $\mathsf{End}(\mathbb{A}^m_R)$ pour cette loi de composition sont, par définition, les **automorphismes** de $\mathbb{A}^m_R$; ils forment un groupe, noté $\mathsf{Aut}(\mathbb{A}^m_R)$.

Nous noterons $\mathbb{A}^m(R) \simeq R^m$ l'ensemble des points de l'espace à coordonnées dans R. Le groupe $\mathsf{Aut}(\mathbb{A}^m_R)$ agit par permutations sur l'ensemble $\mathbb{A}^m(R)$; on obtient ainsi un homomorphisme de groupes $\mathsf{Aut}(\mathbb{A}^m_R) \to \mathsf{Bij}(R^m)$.

Exemple 2.3. Lorsque $m = 1$, les endomorphismes de $\mathbb{A}^1_{\mathbf{R}}$ sont exactement les polynômes univariés à coefficients dans R. Les automorphismes sont des polynômes de degré 1, car la relation $f \circ g(\mathbf{x}) = \mathbf{x}$ entraîne $\deg(f)\deg(g) = 1$. Un polynôme $f(\mathbf{x}) = a\mathbf{x} + b$ de degré 1 est un élément de $\mathsf{Aut}(\mathbb{A}^1_R)$ si, et seulement si a est inversible dans R ; par exemple, $f(\mathbf{x}) = 2\mathbf{x}+3$ est un élément de $\mathsf{Aut}(\mathbb{A}^1_{\mathbf{Q}})$ mais pas de $\mathsf{Aut}(\mathbb{A}^1_{\mathbf{Z}})$.

Exemple 2.4. Si $m = 2$ et $P \in R[\mathbf{x}_1]$, l'application $(\mathbf{x}_1, \mathbf{x}_2) \mapsto (\mathbf{x}_1, \mathbf{x}_2 + P(\mathbf{x}_1))$ est un automorphisme de $\mathbb{A}^m_R$. Ainsi, les degrés des formules définissant les automorphismes de $\mathbb{A}^m_R$ sont quelconques.

Un sous-ensemble W de $\mathbb{A}^m(\mathbf{K})$ est dit **algébrique** s'il existe des polynômes $P_i \in \mathbf{K}[\mathbf{x}_1, \ldots, \mathbf{x}_m]$ tels que $W = \{(z_1, \ldots, z_m) \in \mathbf{K}^m \, ; P_i(z_1, \ldots, z_m) = 0 \quad \forall i\}$ (l'anneau $\mathbf{K}[\mathbf{x}_1, \ldots, \mathbf{x}_m]$ étant noethérien, on peut toujours supposer que W est défini par un nombre fini d'équations, voir [12]).

Théorème 2.5 (de Bell sur l'arithméticité des temps de passage)**.** *Soit f un automorphisme de l'espace affine complexe $\mathbb{A}^m_{\mathbf{C}}$. Soit W un sous-ensemble algébrique de $\mathbb{A}^m$. Soit z un point de $\mathbb{A}^m(\mathbf{C})$. Alors l'ensemble des temps de passage* $\mathrm{Pas}_f(z; W)$ *est une union finie de progressions arithmétiques.*

Cet énoncé contient celui de Skolem, Mahler et Lech en prenant pour f un automorphisme linéaire et pour W un sous-espace vectoriel.

Exemple 2.6. Soit $P(\mathbf{x}_2, \mathbf{x}_3)$ un polynôme de deux variables à coefficients complexes. Soit $(u(n))_{n\geq 0}$ la suite définie par les conditions initiales $u(0) = x_0$, $u(1) = y_0$, $u(2) = z_0$ et la relation de récurrence

$$u(n+3) = u(n) + P(u(n+1), u(n+2)). \tag{2.4}$$

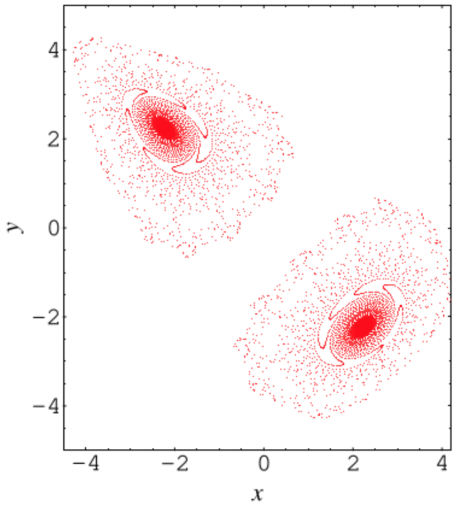
Cette relation peut être écrite sous la forme

$$(u(n+1), u(n+2), u(n+3)) = f(u(n), u(n+1), u(n+2)) \tag{2.5}$$

où $f(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = (\mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_1 + P(\mathbf{x}_2, \mathbf{x}_3))$. Avec W l'hyperplan d'équation $\mathbf{x}_1 = 0$, le théorème de Bell montre que les indices n pour lesquels $u(n) = 0$ forment une union finie de progressions arithmétiques (qui dépend de P et de (x_0, y_0, z_0)).

Exemple 2.7. Étant donnés deux nombres complexes a et b, avec $b \neq 0$, considérons l'application

$$h_{a,b}(\mathbf{x}_1, \mathbf{x}_2) = (\mathbf{x}_2 + 1 - a\mathbf{x}_1^2, b\mathbf{x}_1). \tag{2.6}$$



Cette transformation du plan est la composée de $(\mathbf{x}_1,\mathbf{x}_2)\mapsto(\mathbf{x}_1,\mathbf{x}_2+1-a\mathbf{x}_1^2)$, qui d'après l'exemple 2.4 est un automorphisme, et de $(\mathbf{x}_1,\mathbf{x}_2)\mapsto(\mathbf{x}_2,b\mathbf{x}_1)$, qui est un automorphisme linéaire ; c'est donc bien un automorphisme du plan. Son inverse est

$$(\mathbf{x}_1,\mathbf{x}_2)\mapsto(\mathbf{x}_2/b,\mathbf{x}_1-1+a\mathbf{x}_2^2/b^2).$$

La figure ci-contre montre les vingt mille premiers points de l'orbite de $z_0=(0,0)$ sous l'action de $h_{a,b}$, lorsque $a=0.2$ et $b=0.9991$.

On peut démontrer que le degré des formules définissant $h_{a,b}^n$ est égal à 2^n et qu'il existe une infinité dénombrable de points $z\in\mathbb{A}^2(\mathbf{C})$ qui ont une orbite périodique sous l'action de $h_{a,b}$. Lorsque $a\in\mathbf{R}$ et $b=\pm1$, $h_{a,b}$ préserve la mesure de Lebesgue, si bien que les techniques de la section 1 peuvent être appliquées à $h_{a,b}$.

Si l'on applique le théorème de Bell à $h_{a,b}$, on obtient le résultat suivant : *soit z un point du plan, et W une courbe plane définie par une équation polynomiale ; alors* $\mathrm{Orb}_{h_{a,b}}(z)\cap W$ *est fini.* (Voir l'exemple 7.7).

3. Fonctions analytiques

La démonstration du théorème de Bell emploie des outils élémentaires d'analyse p-adique : le but de cette partie est d'introduire les notions principales qui seront utilisées par la suite. Le lecteur pourra consulter les textes d'Antoine Chambert-Loir et de Jérôme Poineau dans ce volume pour des compléments à cette partie.

3.1. **Algèbre de Tate.** Notons $\mathbf{K}$ le corps $\mathbf{Q}_p$, $|\cdot|$ la valeur absolue $|\cdot|_p$, et $R\subset\mathbf{K}$ l'anneau $\mathbf{Z}_p$. Soit m un entier ≥ 1. L'espace affine $\mathbb{A}^m_{\mathbf{K}}$ est muni de ses coordonnées $(\mathbf{x}_1,\ldots,\mathbf{x}_m)$ et de la norme du supremum

$$\|\,(u_1,\ldots,u_m)\,\|_{sup}=\max\{|u_i|\;;\;1\leq i\leq m\}. \tag{3.1}$$

Les points à coordonnées dans R forment le polydisque unité

$$\mathbb{A}^m(R)=R^m=\{u\;;\;\|\,u\,\|_{sup}\leq 1\}. \tag{3.2}$$

Soit f un élément de $\mathbf{K}[\mathbf{x}_1,\dots,\mathbf{x}_m]$. En utilisant les notations $\mathbf{x}=(\mathbf{x}_1,\dots,\mathbf{x}_m)$ et $\mathbf{x}^I=\mathbf{x}_1^{i_1}\cdots\mathbf{x}_m^{i_m}$ pour tout multi-indice $I=(i_1,\dots,i_m)\in\mathbf{N}^m$, on peut écrire f de manière unique sous la forme $f(\mathbf{x})=\sum_I a_I\mathbf{x}^I$. La **norme de Gauss** est alors définie par

$$\| f \| = \max_I |a_I|; \tag{3.3}$$

c'est la norme du supremum dans la base des monômes $(\mathbf{x}^I)$. L'**algèbre de Tate** $\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle$ est la complétion de l'algèbre des polynômes pour cette norme.

Si une suite (f_n) de polynômes converge dans cette complétion, les coefficients $(a_{I,n})$ convergent individuellement vers une valeur limite $a_I\in\mathbf{K}$, car $\mathbf{K}$ est complet. Ainsi,

— les éléments de $\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle$ peuvent être représentés de manière unique comme des séries formelles $f\in\mathbf{K}[\![\mathbf{x}_1,\dots,\mathbf{x}_m]\!]$, $f(\mathbf{x})=\sum_I a_I\mathbf{x}^I$;

— les coefficients a_I d'un élément de $\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle$ tendent vers 0 dans $\mathbf{K}$ lorsque la longueur $|I|:=i_1+\cdots i_m$ tend vers $+\infty$ (car pour un polynôme les coefficients sont nuls si $|I|$ est suffisamment grand) ;

— par complétion, la norme de Gauss s'étend à $\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle$, avec la même formule $\| f \|=\max_I |a_I|$.

Réciproquement, toute série $f(\mathbf{x})=\sum_I a_I\mathbf{x}^I$ vérifiant $\lim_{|I|}|a_I|=0$ est la limite des polynômes obtenus à partir de f par troncature.

Notons

$$R\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle = \{f\in\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle\ ;\ \| f \|\le 1\} \tag{3.4}$$

$$= \{\sum_I a_I\mathbf{x}^I\ ;\ |a_I|\le 1,\ \forall I\in\mathbf{N}^m\} \tag{3.5}$$

$$= \{\sum_I a_I\mathbf{x}^I\ ;\ a_I\in R,\ \forall I\in\mathbf{N}^m\}. \tag{3.6}$$

Lemme 3.1. *Une série formelle $\sum_I a_I\mathbf{x}^I\in\mathbf{K}[\![\mathbf{x}_1,\dots,\mathbf{x}_m]\!]$ est un élément de $\mathbf{K}\langle\mathbf{x}_1,\dots,\mathbf{x}_m\rangle$ si, et seulement si $|a_I|$ tend vers 0 lorsque $|I|$ tend vers $+\infty$, si, et seulement si la série $\sum_I a_I z^I$ converge dans $\mathbf{K}$ pour tout $z\in R^m$.*

Il suffit en effet d'observer que la série converge pour $z=(1,1,\dots,1)$ si, et seulement si $|a_I|$ tend vers 0 lorsque I tend vers l'infini dans $\mathbf{N}^m$ et, dans ce cas, elle converge sur tout R^m. Voir [5] pour des compléments.

Remarque 3.2. Nous aurions pu introduire les mêmes définitions pour tout corps $\mathbf{K}$ ultramétrique complet. Notons $R=\{z\in\mathbf{K}\ ;\ |z|\le 1\}$ l'anneau de valuation, $R^\circ=\{z\in R\ ;\ |z|<1\}$ l'idéal maximal de R, et $\mathbf{k}=R/R^\circ$ le corps

résiduel. Si $\mathbf{K}$ est une extension de $\mathbf{Q}_p$ complète *dont le corps résiduel* $\mathbf{k}$ *est infini* et si $f \in \mathbf{K}\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$, alors $\| f \| = \max_{z \in R^m} |f(z)|$. En effet, considèrons le polynôme $F(\mathbf{x})$ obtenu en ne gardant de f que les monômes $a_I \mathbf{x}^I$ pour lesquels $|a_I| = \| f \|$, puis écrivons $F(\mathbf{x}) = aF_0(\mathbf{x})$ où $a \in \mathbf{K}$ vérifie $|a| = \| f \|$ et $F_0(\mathbf{x}) \in R[\mathbf{x}_1, \ldots, \mathbf{x}_m]$. Si $f = 0$, il n'y a rien à démontrer. Sinon $F_0(\mathbf{x})$ est un polynôme non nul dont tous les coefficients sont dans $R \setminus R^\circ$. Modulo R°, F_0 devient un polynôme non nul à coefficients dans $\mathbf{k}$; comme $\mathbf{k}$ est infini, il existe un m-uplet $u \in R^m$ tel que $F_0(u) \neq 0 \mod (R^\circ)$. Alors $|F_0(u)| = 1$ et l'inégalité ultramétrique donne $f(u) = \| f \|$.

Lorsque $\mathbf{K} = \mathbf{Q}_p$, le corps résiduel $\mathbf{F}_p$ est fini ; cet argument ne peut donc pas être appliqué ; l'exemple suivant illustre ce fait.

Exemple 3.3. Pour $k = 0$, posons $B_0 = 1$. Pour k entier ≥ 1, notons $B_k \in \mathbf{K}[\mathbf{x}]$ le polynôme binomial défini par

$$B_k(\mathbf{x}) = \binom{\mathbf{x}}{k} = \frac{\mathbf{x}(\mathbf{x}-1)\cdots(\mathbf{x}-k+1)}{k!}. \tag{3.7}$$

Ses coefficients sont rationnels et vérifient :

$$\max_i |a_i| = \left| \frac{1}{k!} \right|. \tag{3.8}$$

La valuation p-adique de $k!$ étant

$$v_p(k!) = \lfloor k/p \rfloor + \lfloor k/p^2 \rfloor + \cdots + \lfloor k/p^n \rfloor + \cdots, \tag{3.9}$$

nous obtenons

$$\left\lfloor \frac{k}{p} \right\rfloor \leq v_p(k!) \leq \frac{k}{p-1} \tag{3.10}$$

et $\left|\frac{1}{k!}\right| \geq p^{\lfloor \frac{k}{p} \rfloor}$. Par ailleurs, si $z \in \mathbf{N}$, $B_k(z) \in \mathbf{N}$, donc $|B_k(z)| \leq 1$; par passage à la limite,

$$|B_k(z)| \leq 1 \tag{3.11}$$

pour tout $z \in \mathbf{Z}_p$. La norme de Gauss de B_k est donc supérieure à $p^{\lfloor \frac{k}{p} \rfloor}$ tandis que $|B_k|$ est majorée par 1 sur le disque unité de $\mathbf{Q}_p$.

Lemme 3.4. *La norme de Gauss s'étend à la* $\mathbf{K}$*-algèbre* $\mathbf{K}\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$ *en une norme multiplicative et ultramétrique :* $\forall f, g \in \mathbf{K}\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$,

$$\| fg \| = \| f \| \| g \| \quad \textit{et} \quad \| f + g \| \leq \max\{\| f \|, \| g \|\}.$$

Démonstration. Si $f=\sum_I a_I\mathbf{x}^I$ et $g=\sum_I b_I\mathbf{x}^I$, et si I et J sont les plus petits multi-indices (pour l'ordre lexicographique) tels que $|a_I|=\| f \|$ et $|b_J|=\| g \|$, alors le coefficient c_{I+J} du produit $f(\mathbf{x})g(\mathbf{x})$ vérifie $|c_{I+J}|=\| f \|\| g \|$. □

3.2. **Le principe des zéros isolés.** L'énoncé suivant fournit une version effective du théorème des zéros isolés.

Théorème 3.5 (des zéros isolés de Strassman)**.** *Soit $f(\mathbf{x})=\sum_{k\geq 0}a_k\mathbf{x}^k$ un élément de $\mathbf{K}\langle\mathbf{x}\rangle\setminus\{0\}$. Soit N_f le plus grand indice N pour lequel $|a_N|=\|f\|$. Alors f s'annule au plus N_f-fois dans le disque fermé R, les racines étant comptées avec multiplicité.*

Ce théorème est démontré dans [5] en utilisant la théorie du polygone de Newton. Voici une version condensée de la démonstration, par récurrence sur N_f.

Supposons d'abord $N_f=0$, ce qui signifie que $|a_k|<|a_0|=\|f\|$ pour tout indice $k\geq 1$; l'inégalité ultramétrique montre alors que f ne s'annule pas dans R. Supposons maintenant le résultat montré pour $N_f=N$ et établissons le pour $N_f=N+1$. Si f a au moins une racine $z\in R$; alors

$$f(\mathbf{x})=f(\mathbf{x})-f(z) \tag{3.12}$$
$$=\sum_{k\geq 0}a_k(\mathbf{x}^k-z^k) \tag{3.13}$$
$$=(\mathbf{x}-z)\sum_{k\geq 1}a_k(\mathbf{x}^{k-1}+z\mathbf{x}^{k-2}+\cdots+z^{k-2}\mathbf{x}+z^{k-1}). \tag{3.14}$$

Ainsi, $f(\mathbf{x})=(\mathbf{x}-z)g(\mathbf{x})$ où la série $g(\mathbf{x})=\sum_{j\geq 0}b_j\mathbf{x}^j$ est définie par

$$\sum_{j\geq 0}b_j\mathbf{x}^j=\sum_{k\geq 1}a_k(\mathbf{x}^{k-1}+z\mathbf{x}^{k-2}+\cdots+z^{k-2}\mathbf{x}+z^{k-1}). \tag{3.15}$$

Le coefficient b_j est une combinaison linéaire à coefficients entiers des a_nz^m pour $n\geq j+1$ et $m\leq n-1$; puisque $|a_n|$ tend vers 0 quand n tend vers l'infini, l'inégalité ultramétrique montre que b_j est bien défini ; de plus, $|b_j|<\|f\|$ pour $j\geq N_f$; ainsi, $N_g<N_f$. L'hypothèse de récurrence montre donc que g a au plus N_f-1 racines dans R ; ainsi, f s'annule au plus N_f fois dans R.

L'entier N_{f-a} est majoré par $N_{f-f(0)}$, ceci quelque soit a dans $\mathbf{K}$. Le théorème de Strassman admet donc le corollaire suivant.

Corollaire 3.6. *Soit $f(\mathbf{x})=\sum_{k\geq 0}a_k\mathbf{x}^k$ un élément non constant de $\mathbf{K}\langle\mathbf{x}\rangle$. Il existe un entier N tel que $f(\mathbf{x})=a$ possède au plus N solutions dans R, ceci quelque soit a dans $\mathbf{K}$.*

4. La méthode des différences divisées et le théorème de Mahler

Cette section est un intermède. Elle est inutile pour la suite, mais la preuve du théorème de Bell et Poonen présentée dans la section suivante repose, dans un cadre plus difficile, sur des idées comparables.

4.1. **Différences divisées de Newton.** Soit f un polynôme univarié de degré d à coefficients dans un corps $\mathbf{K}$ de caractéristique nulle. Si l'on connaît les $d+1$ valeurs

$$f(0), f(1), \ldots, f(d-1), f(d) \tag{4.1}$$

on connaît f, car l'espace des polynômes de degré d est de dimension $d+1$. La méthode des différences divisées de Newton fournit un algorithme correspondant à cette affirmation.

Notons Δ l'opérateur de différence [2], qui à $f(\mathbf{x})$ associe $\Delta f(\mathbf{x}) = f(\mathbf{x}+1) - f(\mathbf{x})$. Les polynômes binomiaux $(B_m)_{m\geq 0}$ (voir l'exemple 3.3) forment une base de l'espace vectoriel $\mathbf{K}[\mathbf{x}]$ vérifiant $\Delta B_k = B_{k-1}$. Si le degré de f est égal à d, on peut donc écrire

$$f(\mathbf{x}) = \sum_{k=0}^{d} A_k B_k(\mathbf{x}) = \sum_{k=0}^{d} A_k \binom{\mathbf{x}}{k} \tag{4.2}$$

avec des $A_k \in \mathbf{K}$. Remarquons que $f(0) = A_0$ car tous les B_k de degré ≥ 1 s'annulent à l'origine ; ensuite, $\Delta f(0) = A_1$ car $\Delta f = \sum_{k=1}^{d} A_k B_{k-1}$, et ainsi de suite : $\Delta^n f(0) = A_n$ pour tout $n \geq 0$. Nous avons donc établi le théorème suivant.

Théorème 4.1. *Soit* $\mathbf{K}$ *un corps de caractéristique nulle. Tout polynôme* $f(\mathbf{x})$ *à coefficients dans* $\mathbf{K}$ *est une combinaison linéaire* $f(\mathbf{x}) = \sum_{k\geq 0} A_k B_k(\mathbf{x})$ *des polynômes binomiaux. Cette écriture est unique : les* A_k *sont donnés par*

$$A_k = \Delta^k f(0) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} f(k-j).$$

Supposons, par exemple, que f est de degré 3 et que ses premières valeurs sont $f(0) = 2$, $f(1) = 6$, $f(2) = -1$, $f(3) = 5$. En écrivant les premières valeurs

2. Ici, l'incrément entre $\mathbf{x}$ et $\mathbf{x}+1$ est égal à 1. Il n'y a donc pas de division (ou plutôt, on divisie par 1) dans notre « méthode des différences divisées ».

de $\Delta^k f$ sur la ligne numéro k, avec $0 \leq k \leq 3$, nous obtenons le tableau suivant

$$\begin{array}{llll} 2, & 6, & -1, & 5, \quad \dots \\ 4, & -7, & 6, & \dots \\ -11, & 13, & \dots & \\ 24, & \dots & & \end{array}$$

Par exemple, les premières valeurs de Δf sont $4 = f(1) - f(0)$, $-7 = f(2) - f(1)$, $6 = f(3) - f(2)$. La colonne de gauche, lue de haut en bas, fournit les $A_k = (\Delta^k f)(0)$. Ainsi, f étant de degré 3, nous obtenons

$$f(\mathbf{x}) = 2 + 4B_1(\mathbf{x}) - 11B_2(\mathbf{x}) + 24B_3(\mathbf{x}). \tag{4.3}$$

On pourra consulter [7] pour l'intérêt de cet algorithme de Newton en analyse numérique (voir aussi [9] pour quelques points historiques).

4.2. **Le théorème de Mahler.** Un théorème de Fritz Carlson montre comment étendre le théorème 4.1 du cas des fonctions polynomiales à celui des fonctions analytiques d'une variable complexe. On cherche alors à écrire la fonction analytique f comme une série infinie de fonctions $f(\mathbf{x}) = \sum_{k\geq 0} A_k B_k(\mathbf{x})$, les coefficients A_k étant donnés par la méthode des différences divisées ; il y a existence et unicité d'une telle écriture si la fonction $z \in \mathbf{C} \mapsto |f(z)|$ ne croît pas trop vite [3].

Le théorème de Mahler, lui, étend le procédé de Newton à n'importe quelle fonction continue $f\colon \mathbf{Z}_p \to \mathbf{Q}_p$. Avant de l'énoncer, considérons les séries de fonctions $\sum_{k\geq 0} a_k B_k(\mathbf{x})$ pour des coefficients $a_k \in \mathbf{Q}_p$. *Une telle série converge uniformément sur $\mathbf{Z}_p$ si, et seulement si $|a_k|_p$ tend vers* 0 *lorsque k tend vers* $+\infty$. En effet, comme remarqué à l'exemple 3.3, $|B_k|_p$ est majorée par 1 sur $\mathbf{Z}_p$, donc si (a_k) tend vers 0, la série converge. Réciproquement, si la série converge uniformément, les fonctions $x \mapsto |a_k B_k(x)|_p$ doivent tendre uniformément vers 0 sur $\mathbf{Z}_p$ lorsque k tend vers $+\infty$, donc $|a_k|_p = |a_k B_k(k)|_p$ tend vers 0.

Théorème 4.2 (Mahler, 1956)**.** *Soit $f\colon \mathbf{Z}_p \to \mathbf{Q}_p$ une fonction continue. Soit $(A_k)_{k\geq 0}$ la suite de nombres p-adiques définies par*

$$A_k = \Delta^k f(0) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} f(m-j).$$

3. Plus précisément, si $|f(z)| \leq C\exp(\alpha|z|)$ et $|f(iy)| \leq C\exp(\beta|y|)$ pour des constantes $C > 0$, $\alpha > 0$ et $0 < \beta < \pi$.

Alors A_k tend vers 0 *lorsque k tend vers* $+\infty$ *et* $f(\mathbf{x}) = \sum_{k=0}^{+\infty} A_k B_k(\mathbf{x})$.

Nous ne démontrerons pas ce théorème (voir pour cela [16]).

Remarque 4.3. Disons qu'une suite $u\colon \mathbf{N} \to \mathbf{Q}_p$ est uniformément continue si elle l'est comme application de $\mathbf{N} \subset \mathbf{Z}_p$ dans $\mathbf{Q}_p$: $\forall s > 0$, $\exists r > 0$,pour tous $n, m \in \mathbf{N}$,

$$\text{si } p^r \text{ divise } (n-m), \text{ alors } |u(n)-u(m)|_p \leq p^{-s}. \tag{4.4}$$

Une telle suite étant donnée, il existe une unique fonction continue $f\colon \mathbf{Z}_p \to \mathbf{Q}_p$ vérifiant $f(n) = u(n)$ pour tout $n \in \mathbf{N}$. Le théorème de Mahler montre que cette fonction est donnée par la série $f(\mathbf{x}) = \sum_{k\geq 0} A_k B_k(\mathbf{x})$ avec $A_k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} u(k-j)$.

5. Difféomorphismes et flots analytiques du polydisque

Nous introduisons ici le groupe des difféomorphismes analytiques de $\mathbb{A}^m(\mathbf{Z}_p)$ et la notion de flot analytique p-adique. Nous démontrons le théorème de Bell et Poonen, qui sera l'ingrédient clé pour démontrer le théorème 2.5.

Comme au paragraphe 3, $\mathbf{K}$ désigne le corps $\mathbf{Q}_p$, $|\cdot|$ la valeur absolue p-adique, et R l'anneau $\mathbf{Z}_p$.

5.1. **Endomorphismes et difféomorphismes.** Appelons **endomorphisme analytique** de R^m (ou de $\mathbb{A}^m(R)$) toute application $f\colon R^m \to R^m$ qui est analytique au sens de Tate, c'est-à-dire qu'il existe des éléments $f_i(\mathbf{x})$ de $R\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$ tels que

$$f(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})). \tag{5.1}$$

Nous noterons $\mathsf{End}\langle R^m \rangle$ l'ensemble de ces endomorphismes analytiques. C'est un R-module qui est stable par composition : si f et g appartiennent à $\mathsf{End}\langle R^m \rangle$, alors $g \circ f$ appartient à $\mathsf{End}\langle R^m \rangle$. Les éléments inversibles de ce monoïde forment un groupe, le groupe $\mathsf{Diff}\langle R^m \rangle$ des **difféomorphismes analytiques**; l'élément neutre est l'application identité $\mathsf{Id}_m(\mathbf{x}_1, \ldots, \mathbf{x}_m) = (\mathbf{x}_1, \ldots, \mathbf{x}_m)$.

Lemme 5.1. *Soit g un élément de* $\mathbf{K}\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$. *Alors* $g\colon R^m \to \mathbf{K}$ *est* $\|g\|$-*lipschitzienne :* $|g(x) - g(y)| \leq \|g\| |x-y|$ *pour toute paire* $(x,y) \in R^m \times R^m$.

Démonstration. Si $i \in \mathbf{N}^*$ et $(x,y) \in \mathbf{K}^2$ alors

$$|x^i - y^i| \leq \left|(x-y)(x^{i-1} + x^{i-2}y + \cdots + xy^{i-2} + y^{i-1})\right| \tag{5.2}$$

$$\leq |x-y| \max\{|x|; |y|\}^{i-1}, \tag{5.3}$$

ce qui montre que $x \mapsto x^i$ est 1-lipschitzienne sur R. Si i et j sont des entiers positifs, et x, y, z, w sont dans R, on obtient donc

$$|x^i z^j - y^i w^j| \leq \left|x^i z^j - y^i z^j + y^i z^j - y^i w^j\right| \tag{5.4}$$

$$\leq \max\{|z|^j |x-y|, |y|^i |z-w|\} \tag{5.5}$$

$$\leq \max\{|x-y|, |z-w|\}. \tag{5.6}$$

Plus généralement, tout monôme $\mathbf{x}^I$ est 1-lipschitzien sur R^m. L'inégalité ultramétrique montre alors le résultat pour tout élément g de $R\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$. □

Ce lemme implique directement le théorème suivant.

Théorème 5.2. *Le monoïde* $\mathsf{End}\langle R^m \rangle$ *et le groupe* $\mathsf{Diff}\langle R^m \rangle$ *agissent respectivement par transformations* 1*-lipschitziennes et par isométries sur* R^m *pour la distance induite par* $\|\cdot\|_{sup}$.

5.2. **Morphismes de réduction.** Les boules fermées de R^m de rayon $|p|^{-s}$ sont en bijection avec les éléments de $(R/p^s R))^m = (\mathbf{Z}/p^s\mathbf{Z})^m$ (voir [5]). Si f est un élément de $\mathsf{Diff}\langle R^m \rangle$, alors f agit par permutation sur cet ensemble fini de boules. Voici comment décrire cette action. En réduisant les coefficients de $f(\mathbf{x})$ modulo $p^s R$ on obtient une application polynomiale $\overline{f}\colon \mathbb{A}^m \to \mathbb{A}^m$ définie sur l'anneau $\mathbf{Z}/p^s\mathbf{Z}$; c'est un automorphisme polynomial de $\mathbb{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}$ dont l'inverse est donné par la réduction $\overline{f^{-1}}$ de f^{-1}. Ceci définit un homomorphisme

$$\mathsf{Diff}\langle R^m \rangle \to \mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}). \tag{5.7}$$

L'action de $\mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}/p^s\mathbf{Z}})$ sur les points de $\mathbb{A}^m$ à coordonnées dans $\mathbf{Z}/p^s\mathbf{Z}$ détermine un second homomorphisme

$$\mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}) \to \mathsf{Bij}(\mathbb{A}^m(\mathbf{Z}/p^s\mathbf{Z})). \tag{5.8}$$

Par composition, nous obtenons pour chaque $s \geq 1$ un homomorphisme

$$\Theta_s\colon \mathsf{Diff}\langle R^m \rangle \to \mathsf{Bij}(\mathbb{A}^m(\mathbf{Z}/p^s\mathbf{Z})). \tag{5.9}$$

Alors l'action de $f \in \mathsf{Diff}\langle R^m \rangle$ sur l'ensemble des boules de R^m de rayon $|p|^s$ coïncide avec celle de $\Theta_s(f)$ sur $\mathbb{A}^m(\mathbf{Z}/p^s\mathbf{Z})$. Le noyau de Θ_s fixe chacune de ces boules ; l'intersection des $\mathrm{Ker}(\Theta_s)$ pour $s \geq 1$ est donc réduite à $\{\mathsf{Id}_m\}$. Comme $\mathbb{A}^m(\mathbf{Z}/p^s\mathbf{Z})$ est fini, de cardinal p^{sm}, nous obtenons le lemme suivant.

Lemme 5.3. *Le noyau de* Θ_s *est d'indice fini dans* $\mathsf{Diff}\langle R^m \rangle$ *; l'intersection de ces noyaux est réduit à* $\{\mathsf{Id}_m\}$.

5.3. **Difféomorphismes proches de l'identité.** Soit c un réel positif. Si f appartient à $\mathsf{End}\langle R^m\rangle$, nous écrirons

$$f = 0 \mod (p^c) \tag{5.10}$$

si, et seulement si $\|f\| \leq |p|^c$; nous écrirons $f = g \mod (p^c)$ si $f - g = 0 \mod (p^c)$. Par exemple, l'application d'une variable définie par $f(\mathbf{x}) = p^2 + 3\mathbf{x} + 18\mathbf{x}^2 + p\mathbf{x}^3$ vérifie $f(\mathbf{x}) = 3\mathbf{x} + 18\mathbf{x}^2 \mod (p)$; si $p = 3$, $f(\mathbf{x}) = 0 \mod (p)$, et $f(\mathbf{x}) = p\mathbf{x} + p\mathbf{x}^3 \mod (p^2)$.

Lemme 5.4. *Soient g et h des éléments de $\mathsf{End}\langle R^m\rangle$ et f un élément de $\mathsf{Diff}\langle R^m\rangle$. Alors*

(1) $\|g \circ h\| \leq \|g\|\|h\|$ *et* $\|g \circ f\| = \|g\|$ *;*

(2) $\|g \circ (\mathsf{Id}_m + h) - g\| \leq \| h \|$ *;*

(3) $\|f^{-1} - \mathsf{Id}_m\| = \|f - \mathsf{Id}_m\|$.

Démonstration. Les coefficients des formules définissant $g \circ h$ sont des sommes de produits d'éléments a_I et b_J de R dont les valeurs absolues sont respectivement majorées par $\|g\|$ et $\|h\|$. Dans chaque produit apparaît au moins un coefficient vérifiant $|a_I| \leq \|g\|$ et un coefficient vérifiant $|b_J| \leq \|h\|$. Comme $\|g\| \leq 1$ et $\|h\| \leq 1$, nous obtenons $\|g \circ h\| \leq \|g\|\|h\|$. L'égalité $\|g \circ f\| = \|g\|$ s'en déduit en utilisant que $\|f\| = \|f^{-1}\| = 1$.

Pour montrer (2), il suffit de traiter le cas où g est une fonction monomiale $g(\mathbf{x}) = \mathbf{x}^I$; le cas général s'en déduit en écrivant chaque composante de g comme une composition linéaire de tels monômes et en utilisant l'inégalité ultramétrique. Or, pour $g(\mathbf{x}) = \mathbf{x}^I$,

$$g \circ (\mathsf{Id}_m + h) - g = A_1(h) + A_2(h) + \cdots A_{|I|}(h) \tag{5.11}$$

où chaque A_j est un polynôme homogène de degré j en $(\mathbf{x}_1, \ldots, \mathbf{x}_m)$ à coefficients dans R. Comme $\|h\| \leq 1$, $\|A_j(h)\| \leq \|h\|$ et $\|g \circ (\mathsf{Id}_m + h) - g\| \leq \|h\|$.

L'assertion (3) se déduit de la première en posant $g = f^{-1} - \mathsf{Id}_m$. □

Proposition 5.5. *Soit c un réel ≥ 1. Le sous-groupe de $\mathsf{Diff}\langle R^m\rangle$ formé des éléments f tels que $f = \mathsf{Id}_m \mod (p^c)$ est distingué. Si f est un tel élément, et si p^N divise n, alors $f^n = \mathsf{Id}_m \mod (p^{c+N})$. En particulier, si $f = \mathsf{Id}_m \mod (p)$ alors $f^{p^N} = \mathsf{Id}_m \mod (p^N)$.*

Démonstration. La première affirmation résulte du lemme 5.4 ci-dessus. Pour la deuxième, écrivons $f(\mathbf{x}) = \mathbf{x} + sh(\mathbf{x})$ où $s \in R$ vérifie $|s| \leq |p|^c$ et $h \in \mathsf{End}\langle R^m\rangle$.

L'assertion (2) du lemme 5.4 montre que

$$f^2(\mathbf{x}) = \mathbf{x} + sh(\mathbf{x}) + sh(\mathbf{x} + sh(\mathbf{x})) = \mathbf{x} + 2sh(\mathbf{x}) + s^2 h_2(\mathbf{x}) \tag{5.12}$$

pour un élément h_2 de $\mathsf{End}\langle R^m\rangle$. Après k itérations, $f^k = \mathsf{Id}_m + ksh + s^2 h_k$ pour un $h_k \in \mathsf{End}\langle R^m\rangle$. En prenant $k = p$, on obtient $f^p = \mathsf{Id}_m \mod (p^{c+1})$; l'égalité $f^{p^N} = \mathsf{Id}_m \mod (p^{c+N})$ s'en déduit par récurrence □

5.4. **Flots analytiques.** Soit $t \mapsto \Phi_t$ un homomorphisme du groupe additif $(R,+)$ vers le groupe $\mathsf{Diff}\langle R^m\rangle$:

$$\Phi_{t+s} = \Phi_t \circ \Phi_s \tag{5.13}$$

pour tous t, s dans R. On dispose alors d'une action de R sur R^m, définie par $(t,x) \mapsto \Phi_t(x)$; une telle action est appelée un **flot** (paramétré par R, sur le polydisque R^m). Si l'application $R \times R^m \to R^m$ définie par cette action est une application analytique au sens de Tate, c'est-à-dire que les m coordonnées de $(\mathbf{t},\mathbf{x}) \mapsto \Phi_{\mathbf{t}}(\mathbf{x})$ sont des éléments de $R\langle \mathbf{t}, \mathbf{x}_1, \ldots, \mathbf{x}_m\rangle$, nous dirons que Φ détermine un **flot analytique**. Nous identifierons Φ à l'action correspondante, Φ pouvant donc être considéré comme un homomorphisme ou comme un flot. L'orbite du flot passant par x en $t = 0$ est la courbe $t \in R \mapsto \Phi_t(x) \in R^m$.

À un tel flot Φ est associé un champ de vecteurs $X_\Phi \colon R^m \to R^m$, défini par

$$X_\Phi(x) = \left(\frac{\partial \Phi_t(x)}{\partial t}\right)_{t=0}. \tag{5.14}$$

Les orbites du flot correspondent alors aux courbes intégrales du champ X_Φ, mais ici ces "courbes" sont paramétrées par l'ensemble de Cantor $R = \mathbf{Z}_p$.

5.5. **Le théorème de Bell et Poonen.** Voici son énoncé (voir [2, 15]).

Théorème 5.6. *Soit f un élément de $\mathsf{End}\langle R^m\rangle$ vérifiant $f = \mathsf{Id}_m \mod (p^c)$ avec $c > \frac{1}{p-1}$. Il existe alors un flot analytique $\Phi \colon R \times R^m \to R^m$, $(\mathbf{t},\mathbf{x}) \mapsto \Phi_{\mathbf{t}}(\mathbf{x})$ tel que*

(1) $\Phi_n(\mathbf{x}) = f^n(\mathbf{x})$ pour tout $n \in \mathbf{N}$;

(2) $\|\Phi_t - \Phi_s\| \leq p^{\frac{1}{p-1}-c}|t-s|$, pour tous t, $s \in R$.

En particulier, $f \in \mathsf{Diff}\langle R^m\rangle$ et $f^{-1} = \Phi_{-1}$.

Pour $p \geq 3$, on peut prendre $c = 1$, pour $p = 2$ on peut prendre $c = 2$. Si $p \geq 3$ et $f = \mathsf{Id}_m \mod (p)$, ou si $p = 2$ et $f = \mathsf{Id}_m \mod (p^2)$, l'action de $\mathbf{Z}$ définie par $(n,x) \mapsto f^n(x)$ peut donc être étendue en une action analytique du groupe $(R,+)$ sur R^m.

Démonstration. Considérons, pour $x \in R^m$ fixé, la suite $u(n) = f^n(x)$. Nous cherchons une fonction $t \mapsto \Phi_t(x)$ qui interpole $(u(n))$, c'est-à-dire que $\Phi_n(x) = u(n)$ pour $n \in \mathbf{N}$. Pour cela, nous appliquerons la méthode de Mahler et Newton ; comme $u(n+1) - u(n) = f^{n+1}(x) - f^n(x) = f^n(f(x)) - f^n(x)$, nous sommes conduits à introduire l'opérateur Δ_f défini par

$$\Delta_f h(\mathbf{x}) = h \circ f(\mathbf{x}) - h(\mathbf{x}), \tag{5.15}$$

h pouvant être un élément de $\mathbf{K}\langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$ ou de $\mathsf{End}\langle R^m \rangle$. Du lemme 5.4, on déduit

$$\Delta_f h(\mathbf{x}) = h(\mathbf{x}) \mod (p^c) \tag{5.16}$$

pour tout $h \in \mathsf{End}\langle R^m \rangle$. Ainsi, $\|\Delta_f^k h\| \leq |p|^{kc}$ pour tout $h \in \mathsf{End}\langle R^m \rangle$. En particulier,

$$\|\Delta_f^k(\mathsf{Id}_m)\| \leq |p|^{kc}. \tag{5.17}$$

D'après l'équation (3.10), $v_p(k!) \leq \frac{k}{p-1}$. L'hypothèse $c > \frac{1}{p-1}$ permet ainsi d'affirmer que la série

$$\Phi_{\mathbf{t}}(\mathbf{x}) := \sum_{k \geq 0} B_k(\mathbf{t}) \Delta_f^k(\mathsf{Id}_m)(\mathbf{x}) \tag{5.18}$$

$$= \sum_{k \geq 0} \frac{\mathbf{t}(\mathbf{t}-1)\cdots(\mathbf{t}-k+1)}{k!} \Delta_f^k(\mathsf{Id}_m)(\mathbf{x}) \tag{5.19}$$

détermine bien un élément de $(R\langle \mathbf{t}, \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle)^m$.

Si n est un entier ≥ 1, les coefficients binomiaux $B_k(n)$ sont nuls dès que $k \geq n+1$, donc

$$\Phi_n(\mathbf{x}) = \sum_{k=0}^{n} \binom{n}{k} \Delta_f^k(\mathsf{Id}_m)(\mathbf{x}) \tag{5.20}$$

$$= (\mathsf{Id} + \Delta_f)^n(\mathsf{Id}_m)(\mathbf{x}) \tag{5.21}$$

$$= f^n(\mathbf{x}) \tag{5.22}$$

car l'opérateur $\mathsf{Id} + \Delta_f$ est l'opérateur de composition par f. Ceci établit l'égalité $\Phi_n(\mathbf{x}) = f^n(\mathbf{x})$ pour tout $n \geq 1$. En particulier, $\Phi_{n+m} = f^{n+m} = \Phi_n \circ \Phi_m$ pour toute paire d'entiers positifs. Par le théorème des zéros isolés, nous déduisons que $\Phi_{t+s}(u) = \Phi_t(\Phi_s(u))$ pour tout $u \in R^m$ et toute paire $(s,t) \in R^2$. Donc $\Phi_{\mathbf{t}+\mathbf{s}}(\mathbf{x}) = \Phi_{\mathbf{t}} \circ \Phi_{\mathbf{s}}(\mathbf{x})$ comme éléments de $\mathsf{Diff}\langle R^m \rangle$. Autrement dit, Φ est un flot analytique qui interpole la dynamique de f.

Il reste à estimer la norme de Gauss $\|\Phi_t - \Phi_s\|$. Posons $P_k(\mathbf{t}) = \mathbf{t}(\mathbf{t}-1)\cdots(\mathbf{t}-k+1)$; c'est un polynôme à coefficients dans $\mathbf{Z}$. Alors

$$\|\Phi_t(\mathbf{x}) - \Phi_s(\mathbf{x})\| \leq \max_{k\geq 0}\{|P_k(t) - P_k(s)| \cdot \|\frac{1}{k!}\Delta_f^k(\mathsf{Id}_m)\|\} \tag{5.23}$$

$$\leq |t-s| \cdot |p|^{c-\frac{1}{p-1}}. \tag{5.24}$$

Enfin, l'égalité $\Phi_{-1} \circ \Phi_1 = \Phi_0 = \mathsf{Id}_m$ montre que $f = \Phi_1$ est inversible. □

Exemple 5.7. Supposons $p = 2$ et $m = 1$, et considérons l'homothétie $f(\mathbf{x}) = -\mathbf{x}$. Alors $f = \mathsf{Id}_1$ modulo p. Pourtant, il n'existe pas de flot analytique $\Phi_{\mathbf{t}}$ pour lequel $\Phi_1 = f$ (voir le lemme 5.10 ci-dessous) ; il faut donc bien supposer $c > 1$ dans ce cas.

Exemple 5.8. Le théorème de Bell et Poonen peut être étendu aux corps complets $(\mathbf{K}, |\cdot|)$ contenant $\mathbf{Q}_p$. Supposons que $\mathbf{K}$ contient une racine de l'unité d'ordre p, notée ξ. On montre alors que $|\xi - 1| = p^{-\frac{1}{p-1}}$. L'homothétie $f(\mathbf{x}) = \xi\mathbf{x}$ vérifie donc l'égalité $f = \mathsf{Id}_1 \mod (p^c)$ avec $c = \frac{1}{p-1}$. Le lemme 5.10 montre donc à nouveau que f ne peut coïncider avec le temps 1 d'un flot analytique. La borne $c > \frac{1}{p-1}$ du théorème de Bell et Poonen est donc optimale.

5.6. **Le sous-groupe** D**.** Notons $o = (0,\ldots,0)$ l'origine de $\mathbb{A}^m_{\mathbf{K}}$. Considérons le sous-groupe D_o de $\mathsf{Diff}\langle R^m\rangle$ constitué des éléments $f \in \mathsf{Diff}\langle R^m\rangle$ fixant o modulo p ; le noyau de Θ_1 est contenu dans D_o (voir le § 5.2). L'application qui à $f \in \mathsf{D}_o$ associe la différentielle $(D\overline{f})_o$ détermine un homomorphisme de D_o vers $\mathsf{GL}_m(\mathbf{Z}/p\mathbf{Z})$.

Supposons maintenant que $f(o) = o \mod (p^2)$ et $(D\overline{f})_o = \mathsf{Id}_m \mod (p)$, et écrivons

$$f(\mathbf{x}) = A_0 + A_1(\mathbf{x}) + \cdots + A_j(\mathbf{x}) + \cdots \tag{5.25}$$

chaque $A_j(\mathbf{x})$ étant une application polynomiale homogène de degré j à coefficients dans R. Par hypothèse, $A_0 = o \mod (p^2)$ et $A_1 = \mathsf{Id}_m \mod (p)$. Maintenant, conjuguons f par l'homothétie de rapport p :

$$p^{-1}f(p\mathbf{x}) = \frac{A_0}{p} + A_1(\mathbf{x}) + pA_2(\mathbf{x}) + \cdots + p^{(j-1)}A_j(\mathbf{x}) + \cdots \tag{5.26}$$

Si $p \geq 3$ alors $\frac{1}{p-1} \leq \frac{1}{2}$ et $p^{-1}f(p\mathbf{x})$ satisfait aux hypothèses du théorème de Bell et Poonen (pour $p = 2$, on remplacera p par p^2 dans toutes les congruences imposées ci-dessus).

L'ensemble $\mathbb{A}^m(\mathbf{Z}/p^2\mathbf{Z})$ et le groupe $\mathsf{GL}_m(R/(p))$ sont finis. On obtient donc les deux premières propriétés de l'énoncé suivant.

Théorème 5.9. *Soit* D *le sous-groupe de* $\mathsf{Diff}\langle R^m\rangle$ *défini par*

$$f(o) = o \mod (p^2) \quad \textit{et} \quad (Df)_o = \mathsf{Id}_m \mod (p)$$

(resp. $f(o) = o \mod (p^4)$ *et* $(Df)_o = \mathsf{Id}_m \mod (p^2)$ *lorsque* $p = 2$*). Alors*

(1) D *est d'indice fini dans* $\mathsf{Diff}\langle R^m\rangle$ *;*

(2) pour tout $f \in \mathsf{D}$*, il existe un flot analytique* $\Phi\colon R \to \mathsf{Diff}\langle R^m\rangle$ *vérifiant* $\Phi_1(\mathbf{x}) = p^{-1}f(p\mathbf{x})$ *;*

(3) D *est sans torsion.*

La dernière assertion découle du lemme suivant, appliqué à $p^{-1}f(p\mathbf{x})$.

Lemme 5.10. *Soit* f *un élément de* $\mathsf{Diff}\langle R^m\rangle$ *pour lequel il existe un flot analytique* $\Phi\colon R \to \mathsf{Diff}\langle R^m\rangle$ *tel que* $f = \Phi_1$.

(1) Si $z \in R^m$ *est un point périodique de* f*, c'est un point fixe ;*

(2) Si f *est d'ordre fini, alors* $f = \mathsf{Id}_m$.

Démonstration. Soit k la période de z. Alors $\Phi_{kn}(z) = f^{kn}(z) = z$ pour tout $n \in \mathbf{Z}$ et, par le théorème des zéros isolés, $\Phi_t(z) = z$ pour tout $t \in R$. Ainsi, $f(z) = \Phi_1(z) = z$. Ceci montre (1), et (2) en résulte. □

6. Plongements de Lech

Le théorème de Bell concerne les transformations polynomiales à coefficients complexes, tandis que le théorème de Bell et Poonen concerne les corps p-adiques. Cette partie présente un lemme qui permettra de passer du complexe au p-adique.

Rappelons qu'un corps $\mathbf{K}$ est une **extension de type fini** de $\mathbf{Q}$ s'il contient $\mathbf{Q}$ et est engendré, en tant qu'extension de $\mathbf{Q}$, par un nombre fini d'éléments $\alpha_1, \ldots, \alpha_k$; tout élément de $\mathbf{K}$ peut alors être écrit comme un quotient

$$\frac{P(\alpha_1, \ldots, \alpha_k)}{Q(\alpha_1, \ldots, \alpha_k)} \tag{6.1}$$

où P et Q sont des éléments de $\mathbf{Z}[\mathbf{x}_1, \ldots, \mathbf{x}_k]$ et $Q(\alpha_1, \ldots, \alpha_k) \neq 0$.

Un **plongement** ι d'un corps $\mathbf{K}$ dans un corps $\mathbf{L}$ est un homomorphisme de corps injectif ; cette propriété est automatique si l'on prend soin d'imposer que $\iota(1) = 1$ ou, ce qui revient au même, que ι n'est pas identiquement nul.

Lemme 6.1 (de plongement de Lech)**.** *Soient* $\mathbf{K}$ *une extension de type fini du corps* $\mathbf{Q}$ *et* S *une partie finie de* $\mathbf{K}$*. Il existe un nombre premier* p *et un plongement* ι *de* $\mathbf{K}$ *dans* $\mathbf{Q}_p$ *tel que* $|\iota(s)|_p = 1$ *pour tout* $s \in S \setminus \{0\}$*. L'ensemble des* p *qui conviennent a une densité strictement positive parmi les nombres premiers.*

La dernière 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. Ce lemme nécessite de faire appel au théorème de Chebotarev (voir [13, 18]), ce qui dépasse le cadre de ce livre. La preuve que nous présenterons fournit seulement une infinité de nombres premiers p convenables, ce qui sera suffisant pour toutes nos utilisations du lemme de Lech. Cette démonstration emploie quelques ingrédients de théorie algébrique des nombres, et est donc reportée au § 9. Ici, nous nous contenterons de deux cas particuliers qui illustrent bien le cas général.

Soit $\mathbf{K}$ un corps de caractéristique nulle. Rappelons que $\xi \in \mathbf{K}$ est algébrique (sur $\mathbf{Q}$), s'il existe un polynôme $P \in \mathbf{Q}[\mathbf{t}] \setminus \{0\}$ tel que $P(\xi) = 0$. Les éléments algébriques de $\mathbf{K}$ forment un ensemble dénombrable car $\mathbf{Q}[\mathbf{t}]$ est dénombrable et chaque $P \in \mathbf{Q}[\mathbf{t}]$ a au plus $\deg(P)$ racines dans $\mathbf{K}$. Un élément de $\mathbf{K}$ est transcendant s'il n'est pas algébrique (par exemple $\pi = 3,141592...$ est transcendant).

Extensions transcendantes.– Supposons que $\mathbf{K} = \mathbf{Q}(\omega)$, où ω est transcendant, et que $S = \{\omega\}$.

Soit p un nombre premier. Comme $\mathbf{Z}_p$ n'est pas dénombrable [4] il existe des éléments transcendants dans $\mathbf{Z}_p$. Soit β un tel élément ; le nombre $\alpha = 1 + p\beta$ est transcendant et $|\alpha|_p = 1$.

Il existe alors un unique homomorphisme de corps $\iota\colon \mathbf{Q}(\omega) \to \mathbf{Q}_p$ tel que $\iota(\omega) = \alpha$: à la fraction $P(\omega)/Q(\omega)$, ι associe le nombre p-adique $P(\alpha)/Q(\alpha)$. Cet homomorphisme convient car $|\alpha|_p = 1$.

Extensions algébriques.– Supposons maintenant que $\mathbf{K}$ est le corps $\mathbf{Q}(\xi)$, où $\xi \neq 0$ est algébrique, et que $S = \{\xi\}$.

Soit $P(\mathbf{t}) \in \mathbf{Q}[\mathbf{t}]$ le polynôme minimal de ξ : c'est le polynôme unitaire de degré minimal tel que $P(\xi) = 0$; il est irréductible, donc à racines simples. Alors

4. $\mathbf{Z}_p$ est homéomorphe à un ensemble de Cantor, ses éléments correspondant aux séries $\sum a_n p^n$ avec $a_n \in \{0, 1, \ldots, p-1\}$

$\mathbf{K}$ s'identifie au quotient $\mathbf{Q}[\mathbf{t}]/(P)$ de $\mathbf{Q}[\mathbf{t}]$ par l'idéal engendré par P. Multiplions P par un entier $\neq 0$ pour obtenir un polynôme $Q(\mathbf{t})$ dont les coefficients sont entiers et globalement premiers entre eux. Notons D le discriminant de Q ; c'est un nombre entier non nul car les racines de P sont simples.

Lemme 6.2. *Soit $F(\mathbf{t}) \in \mathbf{Z}[\mathbf{t}]$ un polynôme à coefficients entiers de degré $d \geq 1$. Il existe une infinité de premiers p tels que F 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 $F(n)$ soit de la forme

$$F(n) = (\pm 1) \prod_{j=1}^{k} p_j^{\alpha_j(n)} \tag{6.2}$$

pour tout $n \in \mathbf{Z}$. L'ensemble $F(\mathbf{Z}) \cap [-M, M]$ contient donc au plus

$$2(\log(M)/\log(2))^k \tag{6.3}$$

éléments. Par ailleurs, $|F(n)|$ est de l'ordre de n^d lorsque n tend vers $+\infty$. Donc le cardinal de $F(\mathbf{Z}) \cap [-M, M]$ est de l'ordre de $M^{1/d}$ lorsque M est grand. C'est une contradiction. □

En appliquant ce lemme au polynôme Q, on trouve un nombre premier $p > \max(D, |Q(0)|)$ et une racine α_0 de Q modulo p. Cette racine est simple, car $D \neq 0 \mod (p)$; elle est non nulle car $Q(0) \neq 0 \mod (p)$. Le lemme de Hensel fournit une racine $\alpha \in \mathbf{Z}_p$ de Q dont la réduction modulo p coïncide avec α_0 (voir [5]). Il existe alors un unique homomorphisme $\iota \colon \mathbf{K} \to \mathbf{Q}_p$ qui envoie ξ sur α, et cet homomorphisme convient car $|\alpha|_p = 1$ (en effet, $\alpha_0 \neq 0 \mod (p)$).

7. Trois applications du théorème de Bell et Poonen

Nous présentons enfin quelques applications de la méthode p-adique basée sur le théorème de Bell et Poonen. L'arithméticité des temps de passage est présentée au paragraphe 7.2.

7.1. **Le théorème de Bass et Lubotzky.** Un groupe Γ est

- **de type fini** s'il est engendré par une partie finie $S \subset \Gamma$ (on peut alors supposer S symétrique, c'est-à-dire que $g \in S$ si, et seulement si $g^{-1} \in S$).
- **résiduellement fini** si, pour tout $\gamma \in \Gamma \setminus \{1_\Gamma\}$, il existe un groupe fini F et un homomorphisme $\alpha \colon \Gamma \to F$ 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 $\gamma \in \Gamma_0 \setminus \{1_\Gamma\}$ engendre un sous-groupe cyclique infini).

Anatolii V. Malcev et Atle Selberg ont montré que tout groupe linéaire de type fini est résiduellement fini et virtuellement sans torsion.

Théorème 7.1 (de Bass et Lubotzky)**.** *Soit* $\mathbf{K}$ *un corps de caractéristique nulle. Soit* m *un entier* ≥ 1*. Si* Γ *est un sous-groupe de type fini de* $\mathsf{Aut}(\mathbb{A}^m_{\mathbf{K}})$*, alors* Γ *est résiduellement fini et virtuellement sans torsion.*

Démonstration. 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 $\mathbf{K}_0$ de $\mathbf{Q}$ engendrée par l'ensemble C_S des coefficients des formules polynomiales définissant les g_i. Le lemme 6.1 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 $\mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}_p})$; ce faisant, Γ devient un sous-groupe de $\mathsf{Diff}\langle \mathbf{Z}_p^m \rangle$. D'après le lemme 5.3, $\mathsf{Diff}\langle \mathbf{Z}_p^m \rangle$ est résiduellement fini ; donc Γ aussi. Et si Γ_0 désigne l'intersection de Γ avec le sous-groupe D de $\mathsf{Diff}\langle \mathbf{Z}_p^m \rangle$ qui est fourni par le théorème 5.9, alors Γ_0 est sans torsion. Donc Γ est virtuellement sans torsion. □

Remarque 7.2. Cette démonstration d'Hyman Bass et Alexander Lubotzky reprend celle de Malcev et Selberg et remonte à Minkowski, qui a montré que le sous-groupe de $\mathsf{GL}_m(\mathbf{Z})$ formé des matrices qui sont égales à l'identité modulo 3 est sans torsion. Nous renvoyons à [1] pour des énoncés plus généraux.

7.2. **Arithméticité des temps de passage.** Démontrons le théorème de Bell, énoncé au paragraphe 2, théorème 2.5.

Fixons un système fini de r équations $P_i(\mathbf{x}) = 0$ définissant W. Notons A l'anneau de type fini engendré par les coordonnées de z, les coefficients des formules définissant f et f^{-1}, et les coefficients des $P_i(\mathbf{x})$. Le lemme 6.1 fournit un nombre premier $p \geq 3$ et un plongement $\iota\colon \mathrm{Frac}(A) \to \mathbf{Q}_p$ tel que $\iota(A) \subset \mathbf{Z}_p$. En appliquant ι aux coordonnées de z, aux coefficients des formules qui définissent f et f^{-1}, et aux coefficients des polynômes P_i, nous sommes ramenés au cas où les données du problème sont définies sur $\mathbf{Z}_p$. Nous supposerons donc désormais que f est un élément de $\mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}_p})$, que z appartient à $\mathbb{A}^m(\mathbf{Z}_p)$ et que W est un sous-ensemble algébrique défini par des équations $P_i(\mathbf{x}) = 0$ à coefficients dans $\mathbf{Z}_p$.

Notons maintenant ℓ l'indice du sous-groupe D de $\mathsf{Diff}\langle \mathbf{Z}_p^m \rangle$ qui est défini par le théorème 5.9 (cet indice ne dépend que de p et m). Pour $0 \leq j \leq \ell - 1$, notons W_j le sous-ensemble algébrique $f^{-j}(W) \subset \mathbb{A}^m_{\mathbf{Q}_p}$; il est défini par les équations $P_{i,j} := P_i \circ f^j \in \mathbf{Z}_p[\mathbf{x}]$, pour $1 \leq i \leq r$.

Conjuguons f par la translation de vecteur z afin de ramener z en l'origine o ; ce faisant, f est remplacé par $g(\mathbf{x}) = f(z+\mathbf{x}) - z$.

L'automorphisme $h := g^\ell$ appartient au groupe D. Il existe donc un flot analytique $\Phi_\mathbf{t}$ tel que $p^{-1}h(p\mathbf{x}) = \Phi_1(\mathbf{x})$. Et $p^{-1}h(p\mathbf{x})$ est obtenu en conjuguant f^ℓ par la transformation affine $\mathbf{x} \mapsto p\mathbf{x} + z$. Soit V_j l'image réciproque de W_j par cette transformation affine ; les polynômes $Q_{i,j}(\mathbf{x}) = P_{i,j}(p\mathbf{x} + z)$ forment un système d'équations définissant V_j. Alors

$$\mathrm{Pas}_h(o; V_j) = \{ n \in \mathbf{Z} \,;\, Q_{i,j}(\Phi_n(o)) = 0 \quad \forall 1 \leq i \leq r \} \tag{7.1}$$

Comme les fonctions $\mathbf{t} \mapsto Q_{i,j}(\Phi_\mathbf{t}(o))$ sont analytiques, le principe des zéros isolés montre que cet ensemble est soit fini, soit égal à $\mathbf{Z}$. Dans le second cas, l'orbite de o par h est entièrement contenue dans V_j. Puisque h est conjuguée à f^ℓ, nous venons de montrer le théorème pour f^ℓ à la place de f et pour chaque W_j à la place de W. Mais, en répartissant les entiers $n \in \mathbf{Z}$ suivant leur congruence modulo ℓ,

$$\mathrm{Pas}_f(z; W) = \bigcup_{j=0}^{\ell-1} \{\, n = k\ell + j \,;\, f^{\ell k}(z) \in f^{-j}(W) \} \tag{7.2}$$

$$= \bigcup_{j=0}^{\ell-1} \Big(j + \ell\, \mathrm{Pas}_{f^\ell}(z; f^{-j}(W)) \Big) . \tag{7.3}$$

Donc $\mathrm{Pas}_f(z; W)$ est bien une union finie de progressions arithmétiques.

Remarque 7.3. La démonstration montre que les raisons r_i divisent l'entier ℓ ; elles sont donc majorées par ℓ, et l'on peut toujours choisir $\ell \leq p^{3m}$ (voir la démonstration du théorème 7.8 ci-dessous).

7.3. **Uniformité.**

Théorème 7.4. *Soit $f \colon \mathbb{A}^m_\mathbf{K} \to \mathbb{A}^m_\mathbf{K}$ un automorphisme, où $\mathbf{K}$ est un corps de caractéristique nulle. Soit $Q \colon \mathbb{A}^m_\mathbf{K} \to \mathbb{A}^k_\mathbf{K}$ une application polynomiale. Soit z un élément de $\mathbb{A}^m(\mathbf{K})$. Si $\mathrm{Pas}_f(z; Q^{-1}(a))$ est fini pour tout $a \in \mathbb{A}^m(\mathbf{K})$, il existe*

un entier N tel que

$$\mathrm{card}(\mathrm{Pas}_f(z;Q^{-1}(a))) \leq N$$

pour tout $a \in \mathbb{A}^k(\mathbf{K})$.

Par exemple, si $Q(\mathbf{x}_1,\dots,\mathbf{x}_m) = (\mathbf{x}_1,\dots,\mathbf{x}_{m-1})$, ce théorème fournit une borne uniforme pour le nombre de passages de l'orbite de z dans une droite verticale (i.e. de vecteur directeur $\mathbf{e}_m = (0,\dots,0,1)$), sauf si l'orbite de z passe périodidiquement dans l'une de ces droites.

Démonstration. Nous pouvons supposer que toutes les données sont définies sur $\mathbf{Z}_p$; en particulier $f \in \mathsf{Diff}\langle \mathbf{Z}_p^m\rangle$ et $Q \in (\mathbf{Z}_p[\mathbf{x}])^k$. Si f est dans le groupe D, $p^{-1}f(p\mathbf{x})$ est égal à $\Phi_1(\mathbf{x})$ pour un flot analytique Φ_t. Par hypothèse, le nombre de solutions de $Q(\Phi_t(z)) = a$ est fini, ceci quelque soit $a \in \mathbb{A}^l(\mathbf{K})$. Il s'agit d'un système de k équations analytiques en la variable t, que l'on peut écrire sous la forme $\sum_n b_{i,n}t^n = a_i$ où les $b_{i,n}$ sont dans $\mathbf{Z}_p$ et tendent vers 0 lorsque n tend vers $+\infty$ et les a_i sont les coordonnées de a (l'indice i varie entre 1 et k). Le théorème de Strassman et son corollaire 3.6 permettent alors de majorer le nombre de solutions indépendamment de a.

Si f n'appartient pas à D, un itéré f^ℓ est dans D, et il suffit d'appliquer l'argument précédent aux fonctions $Q \circ f^j$ pour $0 \leq j \leq \ell$. □

7.4. **Orbites des automorphismes : transitivité.**

Théorème 7.5. *Il existe un automorphisme f de $\mathbb{A}^m_{\mathbf{Z}}$ agissant transitivement sur $\mathbb{A}^m(\mathbf{Z})$ si, et seulement si $m = 1$; dans ce cas $f(\mathbf{x}) = \mathbf{x}+1$ ou $\mathbf{x}-1$.*

Démonstration. Supposons $m = 1$. Les translations $\mathbf{x} \mapsto \mathbf{x}+1$ et $\mathbf{x} \mapsto \mathbf{x}-1$ agissent transitivement sur $\mathbf{Z}$. Un élément f de $\mathsf{Aut}(\mathbb{A}^1_{\mathbf{Z}})$ est une transformation affine $f(\mathbf{x}) = a\mathbf{x}+b$ avec $a,b \in \mathbf{Z}$ dont l'inverse est aussi à coefficients dans $\mathbf{Z}$; autrement dit, $a = \pm 1$. Si $a = -1$ alors f est d'ordre 2. Si $a = 1$, $f(\mathbf{x}) = \mathbf{x}+b$. Pour que f agisse transitivement, il faut donc que $f(\mathbf{x}) = \mathbf{x}+1$ ou $\mathbf{x}-1$.

Supposons maintenant que $m \geq 2$ et que $f \in \mathsf{Aut}(\mathbb{A}^m_{\mathbf{Z}})$ agit transitivement sur $\mathbb{A}^m(\mathbf{Z})$. Soit L la droite définie par $\mathbf{x}_i = 0$ pour $i \leq m-1$. L'orbite de o visite L une infinité de fois. Par le théorème d'arithméticité des temps de passage, il existe $a \geq 0$ et $r \geq 1$ tels que $f^{rn}(f^a(o)) \in L$ pour tout $n \in \mathbf{Z}$. Alors $L = f^r(L)$, car deux courbes irréductibles s'intersectant en un nombre infini de points sont égales [5].

5. Voici un argument direct : $f^r(L)$ est définie par les équations $\mathbf{x}_i \circ f^{-r} = 0$ pour $i \leq m-1$; en restriction à L, $\mathbf{x}_i \circ f^{-r}$ devient une fonction polynomiale d'une seule variable s'annulant

On en déduit que l'orbite de L sous l'action de f est contenue dans l'ensemble fini de courbes $\{f^j(L)\ ;\ 0 \leq j \leq r-1\}$. Et l'orbite de o est entièrement contenue dans l'union de ces courbes. En particulier, l'orbite de o est contenue dans le sous-ensemble algébrique défini par l'équation polynomiale $\prod_{j=0}^{r-1} \mathbf{x}_1 \circ f^j = 0$. Puisque le polynôme $\prod_{j=0}^{r-1} \mathbf{x}_1 \circ f^j$ n'est pas identiquement nul, il existe un point à coordonnées entières en lequel il ne s'annule pas, l'orbite de o ne peut pas passer par un tel point, une contradiction. □

L'argument utilisé pour cette démonstration fournit aussi la propriété suivante :

Théorème 7.6. *Soit* $\mathbf{K}$ *un corps de caractéristique* 0. *Soient* $f\colon \mathbb{A}^m_{\mathbf{K}} \to \mathbb{A}^m_{\mathbf{K}}$ *un automorphisme et* z *un élément de* $\mathbb{A}^m(\mathbf{K})$. *Si l'orbite de* $(f^n(z))_{n\in\mathbf{Z}}$ *intersecte un sous-ensemble algébrique strict de* $\mathbb{A}^m_{\mathbf{K}}$ *en une infinité d'instants, cette orbite ne peut pas être Zariski dense : il existe un polynôme* $Q \in \mathbf{K}[\mathbf{x}_1, \ldots, \mathbf{x}_m]$ *non identiquement nul tel que* $Q(f^n(z)) = 0$ *pour tout* $n \in \mathbf{Z}$.

Ce phénomène peut déjà être observé dans le cas linéaire. Supposons en effet que V est un espace vectoriel complexe de dimension finie, et que $f \in \mathsf{GL}(V)$. Soient $W \subset V$ un sous-espace, z un point de V et a et r des entiers ≥ 1 tels que $f^n(z) \in W$ dès que $n = a + rk$, $k \in \mathbf{Z}$. Changeons z en $w = f^a(z)$ et f en $g = f^k$. Alors $g^n(w) \in W$ pour tout $n \in \mathbf{Z}$. Notons W' le sous-espace vectoriel de W engendré par les $g^n(w)$. Il est g-invariant, donc périodique sous l'action de f, et $\mathrm{Orb}_f(z)$ est contenue dans l'union finie de sous-espaces $\cup_{n=0}^{k-1} f^n(W')$.

Le théorème d'arithméticité des temps de passage doit donc avant tout être considéré comme un théorème de finitude : *si l'orbite de z est Zariski dense, c'est-à-dire qu'elle n'est pas confinée dans un sous-ensemble algébrique strict, elle intersecte tout sous-ensemble algébrique strict de $\mathbb{A}^m_{\mathbf{K}}$ en un nombre fini de points.*

Exemple 7.7. Si l'on considère l'un quelconque des automorphismes de Hénon $h_{a,b}$ décrits dans l'exemple 2.7, on peut montrer que $h_{a,b}$ ne préserve aucune courbe algébrique $W \subset \mathbf{C}^2$. Lénoncé de finitude des temps de passage formulé à la fin de la section 2 résulte alors de l'argument que nous venons de décrire.

---

sur l'ensemble infini $\{f^{rn+a}(o)\ ;\ n \in \mathbf{Z}\}$, c'est donc la fonction nulle et $L \subset f^r(L)$; symétriquement, $f^r(L) \subset L$.

7.5. **Orbites des automorphismes : périodes.** Dans le théorème suivant, le cas $A = \mathbf{Z}$, $\mathbf{K} = \mathbf{Q}$ est déjà intéressant.

Théorème 7.8. *Soient* $\mathbf{K}$ *un corps de caractéristique nulle et* $A \subset \mathbf{K}$ *un sous-anneau de type fini. Pour tout entier* $m \geq 1$ *il existe un entier* $q_A(m)$ *vérifiant la propriété suivante. Pour tout* $f \in \mathsf{Aut}(\mathbb{A}^m_A)$ *et tout* $z \in \mathbb{A}^m(A)$*, ou bien* $\mathrm{Orb}_f(z)$ *est infini, ou bien* $\mathrm{card}(\mathrm{Orb}_f(z)) \leq q_A(m)$.

Lemme 7.9. *Soit* $\mathbf{F}_q$ *un corps fini à* q *éléments. Soit* m *un entier* ≥ 1*. Si* B *est un élément de* $\mathsf{GL}_m(\mathbf{F}_q)$*, alors* $B^s = \mathsf{Id}$ *pour un* $s \leq q^m - 1$*, et ceci est optimal.*

Démonstration. Le théorème de Cayley-Hamilton fournit une relation de dépendance linéaire à coefficients dans $\mathbf{F}_q$ entre les $m+1$ matrices Id, B, …, B^m. La sous-algèbre de $\mathrm{Mat}_m(\mathbf{F}_q)$ engendrée par B est donc un $\mathbf{F}_q$-espace vectoriel de dimension $\leq m$. Elle contient donc au plus $q^m - 1$ éléments non nuls et il existe $0 \leq k < \ell \leq q^m$ tels que $B^k = B^\ell$; en particulier, $B^s = \mathsf{Id}$ avec $s = \ell - k \leq q^m - 1$.

Pour montrer que cette estimation est optimale, considérons une extension de $\mathbf{F}_q$ de degré m ; une telle extension existe, est isomorphe à $\mathbf{F}_{q^m}$ et est un $\mathbf{F}_q$-espace vectoriel de dimension m (voir [12]). Le groupe $\mathbf{F}^\times_{q^m}$ est cyclique, d'ordre $q^m - 1$; soit ξ un générateur de ce groupe. Alors $x \mapsto \xi x$ est une transformation $\mathbf{F}_q$-linéaire de $\mathbf{F}_{q^m}$ d'ordre égal à $q^m - 1$. □

Démonstration du théorème 7.8. Soit $S \subset A \setminus \{0\}$ une partie finie telle que $A = \mathbf{Z}[S]$. Par le théorème de Lech, il existe un nombre premier $p \geq 3$ et un plongement $\iota\colon \mathrm{Frac}(A) \to \mathbf{Q}_p$ tel que $\iota(A)$ soit contenu dans $\mathbf{Z}_p$. Notons p_A le plus petit nombre premier vérifiant cette propriété. Nous allons voir que l'entier

$$q_A(m) := p_A^{3m} \tag{7.4}$$

convient ; pour $A = \mathbf{Z}$, on pourra donc choisir $q_{\mathbf{Z}}(m) = 27^m$.

Supposons donc l'orbite de z finie. Conjuguons f par la translation de vecteur z : nous obtenons un élément g de $\mathsf{Aut}(\mathbb{A}^m_A)$ et il s'agit de majorer la période de l'origine o sous l'action de g. En utilisant le plongement $\iota\colon \mathrm{Frac}(A) \to \mathbf{Q}_{p_A}$, nous pouvons supposer que g, g^{-1} et z sont à coefficients dans $\mathbf{Z}_{p_A}$.

L'ensemble $\mathbb{A}^m(\mathbf{Z}_{p_A}/(p_A^2\mathbf{Z}_{p_A}))$ est fini, de cardinal p_A^{2m}. Il existe donc un entier $k \leq p_A^{2m}$ tel que $g^k(o) = o \mod (p_A^2)$. Soit B la différentielle de g en o modulo p_A. Le lemme 7.9 montre que l'ordre de B dans $\mathsf{GL}_m(\mathbf{F}_{p_A})$ est majoré

par p_A^m. On trouve ainsi un entier $\ell \leq p_A^{3m}$ tel que

$$g^\ell(o) = o \mod (p_A^2) \tag{7.5}$$

$$Dg_o^\ell = \mathsf{Id} \mod (p_A). \tag{7.6}$$

Nous pouvons donc appliquer le théorème de Bell et Poonen : en restriction à $\mathbb{A}^m(\mathbf{Z}_{p_A})$, l'automorphisme polynomial $h(\mathbf{x}) = p_A^{-1} g^\ell(p_A \mathbf{x})$ coïncide avec le temps 1 d'un flot analytique $\Phi\colon \mathbf{Z}_{p_A} \to \mathsf{Diff}\langle \mathbf{Z}_{p_A}^m \rangle$. Le lemme 5.10 montre alors que h fixe o, car l'orbite de o est finie. La période de z sous l'action de f est donc majorée par ℓ, donc par $q_A(m)$. □

8. Annexe A : caractéristique positive et ensembles analytiques

Le théorème de Skolem, Mahler et Lech ne peut être étendu au cas où le corps des nombres complexes est remplacé par un corps de caractéristique positive, ni à celui où l'ensemble W est analytique, même si la transformation f est linéaire. Ce paragraphe présente quelques exemples illustrant ces remarques.

8.1. **Caractéristique positive.** Le théorème de Skolem, Mahler et Lech reste valable si l'on remplace le corps des nombres complexes par un corps $\mathbf{K}$ de caractéristique nulle. En effet, dans une base de l'espace vectoriel V, les coefficients de la matrice de f, les coordonnées de z, et les coefficients d'un système fini d'équations linéaires définissant W engendrent un sous-corps de $\mathbf{K}$ qui est une extension de $\mathbf{Q}$ de type fini ; mais une telle extension peut être plongée dans $\mathbf{C}$. La même remarque s'applique au théorème d'arithméticité de Bell.

Intéressons-nous maintenant au cas où le corps est de caractéristique positive. Soit p un nombre premier et $\mathbf{K}$ le corps $\mathbf{F}_p(\mathbf{t})$. Soit $V = \mathbf{K}^3$ et $f\colon V \to V$ la transformation linéaire diagonale définie par $f(x,y,z) = ((1+\mathbf{t})x, \mathbf{t}y, z)$. Soient $z = (1,1,1) \in V$ et $W = \{(x,y,z) \in V \,;\, x = y+z\}$. L'orbite de z sous l'action de f est

$$f^n(z) = ((1+\mathbf{t})^n, \mathbf{t}^n, 1) \tag{8.1}$$

et $f^n(z) \in W$ si et seulement si

$$(1+\mathbf{t})^n = 1 + \mathbf{t}^n. \tag{8.2}$$

En caractéristique p, $(a+b)^p = a^p + b^p$ car les coefficients binomiaux $\binom{p}{j}$ sont divisibles par p pour tout $1 \leq j \leq p-1$; donc $(a+b)^n = a^n + b^n$ dès que n est

une puissance de p. En particulier, $\mathrm{Pas}_f^+(z;W)$ contient $\{p^k\,;\,k\in\mathbf{N}^*\}$. Réciproquement, $\mathbf{t}$ étant une indéterminée, l'idéntité $(1+\mathbf{t})^n = 1+\mathbf{t}^n$ signifie que chaque coefficient binomial $\binom{n}{j}$ avec $1\le j\le n-1$ est divisible par p. On en déduit facilement que n est une puissance de p; en effet, le premier coefficient fournit $n=0 \mod(p)$, donc $n=p\ell$ pour un $\ell\ge 1$, puis le coefficient numéro p fournit

$$\frac{\ell(p\ell-1)\cdots(p\ell-p+1)}{(p-1)\cdots 2\cdot 1} = 0 \mod(p) \tag{8.3}$$

ce qui entraîne que ℓ est aussi divisible par p, etc. Finalement,

$$\mathrm{Pas}_f^+(z;W) = \{p^k\,;\,k\in\mathbf{N}^*\}. \tag{8.4}$$

Harm Derksen, dans [8], donne d'autres exemples pathologiques (par exemple $\{p^k\,;\,k\in\mathbf{N}^*\}\cup\{p^\ell+p^m;\ell,m\in\mathbf{N}^*\}$), et caractérise les ensembles $\mathrm{Pas}_f^+(z;W)$ qui peuvent apparaître dans le théorème de Skolem, Mahler et Lech en caractéristique $p>0$. Sa démonstration est effective, au sens où elle répond positivement au problème de Skolem en caractérisitque positive (voir l'énoncé du problème dans la section 2).

8.2. **Ensembles analytiques.** Soit M le tore $\mathbf{R}^2/\mathbf{Z}^2$. Soit $s\colon \mathbf{R}\to\mathbf{R}$ une fonction 1-périodique, c'est-à-dire que $s(t+1)=s(t)$. Alors s peut être considérée comme une fonction de $\mathbf{R}/\mathbf{Z}$ vers $\mathbf{R}$; en prenant ses valeurs modulo 1, on obtient une fonction $\overline{s}\colon \mathbf{R}/\mathbf{Z}\to\mathbf{R}/\mathbf{Z}$; le graphe $G(s)$ de $\overline{s}$ est alors une courbe tracée dans M. Si s est de classe C^k (resp. est analytique), $G(s)$ est également de classe C^k (resp. analytique).

Théorème 8.1. *Soit $z_n=(x_n,y_n)$ une suite de points du tore $\mathbf{R}^2/\mathbf{Z}^2$. Supposons que les x_n sont deux-à-deux distincts et que (z_n) est dense dans le tore. Il existe une fonction $s\colon\mathbf{R}\to\mathbf{R}$ qui est analytique et 1-périodique, et une suite croissante d'entiers $k_i\ge 1$ telles que*

(1) $\{n\,;\,z_n\in G(s)\}=\{k_i\,;\,i\ge 1\}$;

(2) $k_{i+1}-k_i > k_i$ pour tout $i\ge 1$.

8.2.1. *Application.* Considérons une matrice diagonale $A\in\mathsf{GL}_2(\mathbf{C})$ dont les deux valeurs propres α et β sont de module 1; écrivons

$$\alpha=\exp(2\mathrm{i}\pi a),\quad \beta=\exp(2\mathrm{i}\pi a). \tag{8.5}$$

Nous supposerons que 1, a et b sont $\mathbf{Q}$-linéairement indépendants (en particulier, a et b sont irrationnels).

Définissons $\varphi\colon M \to \mathbf{C}^2$ par $\varphi(x,y) = (e^{2i\pi x}, e^{2i\pi y})$; alors

$$\varphi(M) = \{(u,v) \in \mathbf{C}^2 \,;\, |u| = |v| = 1\} \tag{8.6}$$

et A préserve $\varphi(M)$; plus précisément,

$$A\varphi(x,y) = (e^{2i\pi(x+a)}, e^{2i\pi(y+b)}) = \varphi(x+a, y+b). \tag{8.7}$$

Puisque 1, a et b sont $\mathbf{Q}$-linéairement indépendants,

— l'ensemble $\{(x+na, y+nb) \,;\, n \in \mathbf{Z}\}$ est dense dans M, ceci quelque soit la condition initiale (x,y) ;

— modulo 1, les $x_n = x + na$ sont deux à deux distincts.

En appliquant le théorème précédent, nous obtenons :

Corollaire 8.2. *Il existe un élément A de $\mathsf{U}_2(\mathbf{C})$, un point $z_0 \in \mathbf{C}^2$, et une courbe analytique réelle $C \subset \mathbf{C}^2$ telle que l'ensemble des temps de passage $\mathrm{Pas}_A(z_0; C)$ soit infini mais ne contienne aucune progression arithmétique de longueur ≥ 3.*

En effet, considérons une suite (k_i) vérifiant la seconde assertion du théorème 8.1. Si (k_i) contenait une progression arithmétique a, $a+r$, $a+2r$, on pourrait écrire $a = k_\ell$, $a+r = k_m$, $a+2r = k_n$ avec $\ell < m < n$. On aurait alors $k_n - k_m > k_m$, soit $r > a+r$, ce qui est impossible car $a = k_\ell \geq 0$.

8.2.2. *Démonstration du théorème 8.1.* Nous allons construire simultanément la fonction s et la suite (k_i). Nous chercherons s sous la forme d'une série trigonométrique

$$s(t) = a_0 + \sum_{n \geq 1}^{\infty} a_n \cos(2\pi nt) + b_n \sin(2\pi nt), \tag{8.8}$$

à coefficients a_n et b_n réels. Si $a_n^2 + b_n^2$ tend exponentiellement vite vers 0, la fonction s est analytique.

Remarque préliminaire.– L'espace V_d des fonctions trigonométriques

$$P(t) = a_0 + \sum_{n \geq 1}^{d} a_n \cos(2\pi nt) + b_n \sin(2\pi nt) \tag{8.9}$$

est de dimension $2d+1$. Nous le munirons de la norme définie par

$$\|P\|^2 = a_0^2 + \sum_{n=1}^{d} a_n^2 + b_n^2. \tag{8.10}$$

Soit F une partie finie de $\mathbf{R}/\mathbf{Z}$ de cardinal $k < \dim(V_d)$. Soient δ et η des réels > 0. Il existe alors $\varepsilon > 0$, qui dépend de d, F, η et δ, vérifiant la propriété suivante : si $x \in \mathbf{R}/\mathbf{Z}$ et $\mathrm{dist}(x,F) \geq \delta$, alors il existe $P \in V_d$ tel que

(a) $P(F) = \{0\}$;
(b) $P(x) = \varepsilon$;
(c) $\|P\| \leq \eta$.

La contrainte (a) définit en effet un sous-espace W_F de dimension ≥ 1 dans V_d. Si $x \in \mathbf{R}/\mathbf{Z}$, l'évaluation en x détermine une forme linéaire $\mathrm{év}_x : W_F \to \mathbf{R}$; cette forme s'annule si, et seulement si $x \in F$; et lorsque $\mathrm{dist}(x,F) \geq \delta$, la norme de $\mathrm{év}_x$ est uniformément minorée. La remarque en découle.

Construction.– Choisissons un entier $k_1 \geq 1$. Posons $F_0 = \{x_n \,;\, n < k_1\}$. Il existe un polynôme trigonométrique $P_1 \in V_{k_1}$, tel que $P_1(F_0) = \{0\}$ et $P_1(x_{k_1}) \neq 0$. Si l'on définit $s_1 = P_1$, alors l'ensemble des temps des passage $n \leq k_1$ de la suite (z_n) sur la courbe $G(s_1)$ coïncide avec $\{k_1\}$.

Supposons maintenant s_i définie en sorte que l'ensemble des temps de passage $\{n \,;\, n \leq k_i \text{ et } z_n \in G(s_i)\}$ coïncide avec $\{k_j \,;\, j \leq i\}$. Considérons l'ensemble $F_i = \{x_n \,;\, n \leq k_i\}$; il comporte k_i éléments distincts. Soit $\delta_i > 0$ suffisamment petit pour qu'il existe un intervalle I de longueur > 0 dans $\{x \in \mathbf{R}/Z \,;\, \mathrm{dist}(x,F_i) \geq \delta_i\}$. Soit η_i un réel > 0 que l'on choisira ultérieurement. Soit ε_i un réel > 0 pour lequel la remarque préliminaire soit valable pour k_i, F_i, δ_i, η_i. Par densité de la suite (z_n), nous pouvons trouver un entier k_{i+1} tel que $k_{i+1} > 2k_i$ et

$$x_{k_{i+1}} \in I \tag{8.11}$$

$$|s_i(x_{k_{i+1}}) - y_{k_{i+1}}| < \varepsilon_i. \tag{8.12}$$

Ainsi, le point z_{k_i+1} est à distance $< \varepsilon_i$ du graphe $G(s_i)$ et sa première coordonnée est à distance $\geq \delta_i$ de F_i. Il existe alors un polynôme trigonométrique $P_{i+1} \in V_{k_{i+1}}$ tel que $P_{i+1}(F_i) = \{0\}$, $P_{i+1}(x_{k_{i+1}}) = s_i(x_{k_{i+1}}) - y_{k_{i+1}}$ et $\|P_{i+1}\| \leq \eta_i$. Posons $s^0_{i+1}(t) = s_i(t) - P_{i+1}(t)$. Les entiers $n \leq k_i$ tels que $z_n \in G(s^0_{i+1})$ sont encore les k_j pour $j \leq i$; par ailleurs, $z_{k_{i+1}}$ est aussi situé sur $G(s^0_{i+1})$. Nous allons modifier s^0_{i+1} pour assurer qu'aucun des z_n ne soit sur le graphe lorsque $k_i < n < k_{i+1}$. Pour cela, on choisit $Q_{i+1} \in V_{k_{i+1}}$ tel que

— $Q_{i+1}(F_i \cup \{x_{k_{i+1}}\}) = \{0\}$;
— si $k_i < n < k_{i+1}$, alors $Q_{i+1}(x_n) = 0$ si, et seulement si $z_n \notin G(s^0_{i+1})$.

Un tel choix est possible car les x_n sont distincts ; en multipliant Q_{i+1} par une constante non nulle, nous imposerons aussi $\|Q_{i+1}\| \leq \eta_i$. Posons

$$s_{i+1} = s_{i+1}^0 + Q_{i+1} = s_i + P_{i+1} + Q_{i+1} \tag{8.13}$$

et $P_{i+1} + Q_{i+1} \in V_{k_{i+1}}$ vérifie $\|P_{i+1} + Q_{i+1}\| \leq 2\eta_i$. Alors

$$\{n \leq k_{i+1} \, ; \, z_n \in G(s_i)\} = \{k_j \, ; \, j \leq i+1\}. \tag{8.14}$$

Si les η_i tendent suffisamment vite vers 0, la suite de fonctions trigonométriques $(s_i)_{i\geq 1}$ converge vers une fonction analytique 1-périodique vérifiant $\{n \, ; \, z_n \in G(s)\} = \{k_i \, ; \, i \geq 1\}$, ce qu'il fallait démontrer.

9. Annexe B : Démonstration du lemme de plongement de Lech

Ecrivons $\mathbf{K}$ comme une extension algébrique d'une extension transcendante pure $\mathbf{L}$ de $\mathbf{Q}$ (voir [12]). En notant ℓ le degré de transcendance de $\mathbf{L}$ sur $\mathbf{Q}$, nous pouvons fixer un isomorphisme $\mathbf{L} \simeq \mathbf{Q}(t_1, \ldots t_\ell)$ où les t_i sont des indéterminées. Le théorème de l'élément primitif (voir [12]) montre qu'il existe $\alpha \in \mathbf{K}$ tel que $\mathbf{K} = \mathbf{L}[\alpha]$. Soit $P_\alpha(\mathbf{x}) \in \mathbf{L}[\mathbf{x}]$ le polynôme minimal (unitaire) de α sur $\mathbf{L}$; quitte à multiplier P_α par un élément non nul de $\mathbf{Z}[t_1, \ldots, t_\ell]$, nous pouvons supposer que P_α appartient à l'anneau $\mathbf{Z}[t_1, \ldots, t_\ell][\mathbf{x}]$ (ce faisant, P_α n'est plus unitaire). Soit D le discriminant de P_α par rapport à la variable $\mathbf{x}$: c'est un élément de $\mathbf{Z}[t_1, \ldots, t_d]$.

Pour chaque élément s de $S \setminus \{0\}$, il existe un polynôme $G_s \in \mathbf{L}[\mathbf{x}]$ tel que $s = G_s(\alpha)$. Nous fixerons G_s, ainsi qu'un polynôme $B_s \in \mathbf{Z}[t_1, \ldots, t_l]$ tel que $B_s \times G_s$ soit un élément de $\mathbf{Z}[t_1, \ldots, t_\ell][\mathbf{x}]$. Le résultant de $P_\alpha(\mathbf{x})$ et de $(B_s G_s)(\mathbf{x})$ sera noté R_s : c'est un élément de $\mathbf{Z}[t_1, \ldots, t_\ell]$.

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

— $D(a_1, \ldots, a_\ell)$ n'est pas nul ;

— $P_\alpha(a_1, \ldots, a_\ell)(\mathbf{x})$ n'est pas un polynôme constant (de la variable $\mathbf{x}$) ;

— pour tout $s \in S$, $B_s(a_1, \ldots, a_\ell)$ et $R_s(a_1, \ldots, a_\ell)$ ne sont pas nuls.

Soit $\mathcal{B}$ l'ensemble des premiers p tels que (a) ces trois propriétés restent valables modulo p et (b) le polynôme $P_\alpha(a_1, \ldots, a_\ell)(\mathbf{x})$ a une racine modulo p. Le lemme 6.2 montre que $\mathcal{B}$ est infini.

Fixons alors un 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 $\mathbf{Q}(\tau_1, \ldots, \tau_\ell)$ soit une extension transcendante pure de $\mathbf{Q}$. Le polynôme $P_\alpha(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell)(\mathbf{x})$ a une racine modulo p ; comme $D(a_1, \ldots, a_\ell)$ n'est pas nul modulo p, le lemme de Hensel assure l'existence d'une racine $\hat{\alpha} \in \mathbf{Z}_p$ de $P_\alpha(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell)(\mathbf{x})$. Il

existe donc un unique homomorphisme $\iota : \mathbf{K} \to \mathbf{Q}_p$ tel que $\iota(t_i) = a_i + p\tau_i$ et $\iota(\alpha) = \hat{\alpha}$.

Soit s un élément de $S \setminus \{0\}$. Le choix de p montre que $\iota(B_s(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell))$ est dans $\mathbf{Z}_p$ et n'est pas nul modulo p ; sa valeur absolue est donc égale à 1. Cet argument s'applique aussi à

$$B_s(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell) G_s(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell)(\hat{\alpha}) \tag{9.1}$$

car $R_s(a_1 + p\tau_1, \ldots, a_\ell + p\tau_\ell)$ n'est pas nul modulo p. Ainsi, $|\iota(s)|_p = 1$, ce qui conclut la démonstration.

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 Pierre Bell. The Skolem-Mahler-Lech theorem. *Doc. Math.*, Extra Volume Mahler Selecta :173–178, 2019.

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

[5] Antoine Chambert-Loir. Balade newtonienne entre analyse et arithmétique. *Ce volume*, pages 1–46, 2023.

[6] Yves Coudène. *Théorie ergodique et systèmes dynamiques*. Savoirs Actuels (Les Ulis). [Current Scholarship (Les Ulis)]. EDP Sciences, Les Ulis ; CNRS Éditions, Paris, 2012.

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

[8] Harm Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.*, 168(1) :175–224, 2007.

[9] William Dunham. *Journey through genius*. Wiley Science Editions. John Wiley & Sons, Inc., New York, 1990. The great theorems of mathematics.

[10] H. Furstenberg. *Recurrence in ergodic theory and combinatorial number theory*. Princeton University Press, Princeton, N.J., 1981. M. B. Porter Lectures.

[11] Harry Furstenberg. Poincaré recurrence and number theory. *Bull. Amer. Math. Soc. (N.S.)*, 5(3) :211–234, 1981.

[12] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.

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

[14] K. Mahler. On the Taylor coefficients of rational functions. *Proc. Cambridge Philos. Soc.*, 52 :39–48, 1956.

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

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

[17] T. Skolem. Ein verfahren zur behandlung gewisser exponentialer gleichungen und diophantischer gleichungen. *Comptes Rendus, 8-ème congrès scandinave à Stockholm*, pages 163–188, 1934.

[18] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2) :26–37, 1996.

[19] T. Tao. Open question : effective skolem-mahler-lech theorem. *What's new, blog of the author*, pages https ://terrytao.wordpress.com/2007/05/25/open–question–effective–skolem–mahler–lech–theorem/, 2007.

UNIV RENNES, CNRS, IRMAR - UMR 6625, F-35000 RENNES, FRANCE
Email address: serge.cantat@univ-rennes1.fr