Introduction à l'analyse p-adique

Marc Abboud

Ce texte correspond aux notes du cours donné à l'université de Neuchâtel au premier semestre 2025-2026. La référence principal du cours est le livre d'Alain Robert, a course in p-adic analysis ([**Rob00**]).

1. Introduction

1.1. Les nombres p-adiques. Les nombres p-adiques ont été introduit par Kurt Hensel au début du 20ème siècle. Il s'agit d'un espace topologique obtenus à partir des nombres entiers en utilisant une métrique provenant de l'arithmétique qui dépend d'un nombre premier p. Bien que la topologie de ces espaces est très différente de la topologie réelle, on peut faire de l'analyse dessus. Les espaces p-adiques sont maintenant fondamentaux en théorie algébrique des nombres et en géométrie arithmétique.

Notons $\mathbf{Z}_p$ l'espace des nombres p-adiques. Il est en particulier totalement discontinu. On peut par exemple sur $\mathbf{Z}_p$ avoir des fonctions localement constante qui ne sont pas constantes ! Il faudra donc définir la bonne notion de fonctions analytiques sur cette espace. Une fois cela fait nous pourrons retrouver des théorèmes classiques de l'analyse complexe comme par exemple le théorème des zéros isolés. Un avantage essentiel des nombres p-adiques est que sur cet espace, une série converge si et seulement si son terme général tend vers zéro. Cela permet de démontrer les théorèmes d'analyse du type Cauchy-Lipschitz ou inversion locale de façon beaucoup plus simple que dans le cas réel ou complexe.

1.2. Arithméticité des temps de passages. Dans ce cours, nous allons introduire la notion de nombres p-adiques et la théorie analytique que l'on peut faire dessus. Nous verrons des applications de cette théorie à des problèmes de dynamique algébrique. Commençons par énoncer le résultat suivant. Une progression arithmétique dans $\mathbf{N}$ est un ensemble de la forme

$$\{ak+b : k \geqslant 0\} \tag{1}$$

où $a, b \in \mathbf{N}$ et $a \neq 0$.

THÉORÈME 1.1 (Skolem, Mahler, Lech, [**Lec53**]). *Soit (u_n) une suite récurrente linéaire sur $\mathbf{C}$, i.e qui vérifie une relation de la forme*

$$\forall n \geqslant 0, \quad u_{n+d} = \sum_{k=0}^{d-1} a_k u_{n+k} \tag{2}$$

où $a_k \in \mathbf{C}$ et $a_0 \neq 0$, alors l'ensemble

$$\{n \geqslant 0 : u_n = 0\} \tag{3}$$

est une union finie de progressions arithmétiques et d'un ensemble fini.

Ce théorème fut d'abord démontrer par Skolem pour une suite récurrente linéaire sur $\mathbf{Q}$ en utilisant les nombres p-adiques. Il fut ensuite généraliser par Mahler pour tout corps de nombre (c'est à dire une extension finie de $\mathbf{Q}$) et enfin par Lech pour $\mathbf{C}$. Nous allons démontrer dans ce cours une généralisation de ce résultat dû à Bell, Ghioca et Tucker. Définissons quelques objets d'abord. Une *transformation polynomiale* de $\mathbf{C}^n$ est une application

$$f = (f_1, \ldots, f_n) : \mathbf{C}^n \to \mathbf{C}^n \tag{4}$$

telle que chaque f_i est un polynôme complexe à n variables. Un *automorphisme polynomial* de $\mathbf{C}^n$ est une application polynomiale $f : \mathbf{C}^n \to \mathbf{C}^n$ inversible et telle que l'inverse est également polynomial.

EXEMPLE 1.2. Tout application affine $x \in \mathbf{C}^n \mapsto Ax+b$ avec $A \in M_n(\mathbf{C}), b \in \mathbf{C}^n$ est une transformation polynomiale. C'est un automorphisme polynomial si et seulement si A est inversible.

EXERCICE 1.3. Montrer que un automorphisme polynomial de $\mathbf{C}$ est nécessairement une application affine.

EXEMPLE 1.4. Il existe des automorphismes polynomiaux de $\mathbf{C}^n$ qui ne sont pas affines pour $n \geqslant 2$. En effet, regardons par exemple

$$z_1, \ldots, z_n \mapsto (z_1 + P(z_2, \ldots, z_n), z_2, \ldots, z_n) \tag{5}$$

avec $P(z_2, \ldots, z_n) \in \mathbf{C}[z_2, \ldots, z_n]$. C'est un automorphisme polynomial pour tout polynôme P.

Une *sous-variété algébrique* de $\mathbf{C}^n$ est un ensemble $V \subset \mathbf{C}^n$ défini par un ensemble d'équations polynomiales. C'est à dire qu'il existe $P_1, \ldots, P_r \in \mathbf{C}[z_1, \ldots, z_n]$ tels que

$$V = \{(z_1, \ldots, z_n) \in \mathbf{C} : P_1(z_1, z_n) = \cdots = P_r(z_1, \ldots, z_n) = 0\}. \tag{6}$$

On peut maintenant énoncer le théorème de Bell, Ghioca, Tucker.

THÉORÈME 1.5 (Bell, Ghioca, Tucker, [**BGT08**]). *Soit $f : \mathbf{C}^n \to \mathbf{C}^n$ un automorphisme polynomial, $V \subset \mathbf{C}^n$ une sous variété algébrique et $x \in \mathbf{C}^n$. L'ensemble*

$$\{n \in \mathbf{Z} : f^n(x) \in V\} \tag{7}$$

est une union finie de progressions arithmétiques et d'un ensemble fini.

Ce théorème généralise bien le résultat de Skolem-Mahler-Lech car si (u_n) est une suite récurrente linéaire d'ordre d et $x = (u_0, \dots, u_{d-1})$ est le vecteur des conditions initiales, alors on a

$$\forall n \geqslant 0, \begin{pmatrix} u_n \\ \vdots \\ u_{n+d-1} \end{pmatrix} = A^n \begin{pmatrix} u_0 \\ \vdots \\ u_{d-1} \end{pmatrix} \tag{8}$$

où

$$A = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ a_0 & a_1 & \cdots & & a_{d-1} \end{pmatrix}. \tag{9}$$

La matrice A est bien inversible car son polynôme caractéristique est donné par $X^d - \sum_{i=0}^{d-1} a_i X^i$ et $a_0 \neq 0$. Donc l'application $f : p \in \mathbf{C}^n \mapsto Ap$ est un automorphisme polynomial et on regarde l'intersection de l'orbite de x sous f avec la sous-variété

$$V = \{z_1 = 0\}. \tag{10}$$

2. Les nombres p-adiques

2.1. Distance p-adique. Soit p un nombre premier. Pour tout entier $x \in \mathbf{Z} \setminus \{0\}$, on définit la *valuation p-adique* de x de la façon suivante. Par le théorème de factorisation des entiers, on peut écrire de façon unique

$$x = p^\alpha m' \tag{11}$$

avec $\alpha \geqslant 0$ et $p \nmid m'$. On définit alors

$$v_p(x) = \alpha. \tag{12}$$

Et par convention on définit $v_p(0) = +\infty$.

EXERCICE 2.1. Montrer que pour tout $x \in \mathbf{Z}$,

$$v_p(x) = \max\left\{k \geqslant 0 : p^k \mid x\right\}. \tag{13}$$

Ce résultat permet d'interpréter la valuation p-adique de la facon suivante.

COROLLAIRE 2.2. *L'écriture en base p d'un entier x se termine par exactement $v_p(x)$ zéros.*

De même pour les nombres rationnels, le théorème de factorisation des entiers dit qu'iol existe une unique écriture de $x \in \mathbf{Q}$ de la forme

$$p^{\alpha}\frac{a}{b} \tag{14}$$

avec a et b premiers entre eux et non divisible par p. On définit alors $v_p(x) := \alpha$. C'est bien compatible avec la définition pour les entiers.

LEMME 2.3. *On a les propriétés suivantes.*

(1) $\forall x, y \in \mathbf{Q}, v_p(xy) = v_p(x) + v_p(y)$.

(2) $\forall x, y \in \mathbf{Q}, v_p(x+y) \geqslant \min(v_p(x), v_p(y))$.

DÉMONSTRATION. Si $x = 0$ ou $y = 0$, alors les deux propriétés sont évidentes donc on suppose $x, y \neq 0$. Soit $\alpha = v_p(x)$ et $\beta = v_p(y)$. Écrivons

$$x = p^{\alpha}\frac{a_x}{b_x}, \quad y = p^{\beta}\frac{a_y}{b_y} \tag{15}$$

avec $p \nmid a_x b_x a_y b_y$. Alors

$$xy = p^{\alpha+\beta}\frac{a_x a_y}{b_x b_y}. \tag{16}$$

Ce qui prouve la première propriété. Pour la deuxième, on peut supposer quitte à intervertir x et y que $\beta \geqslant \alpha$, on a alors

$$x + y = p^{\alpha}(\frac{a_x}{b_x} + p^{\beta-\alpha}\frac{a_y}{b_y}) = p^{\alpha}\left(\frac{a_x b_y + p^{\beta-\alpha}a_y}{b_y b_x}\right). \tag{17}$$

Comme $\beta - \alpha \geqslant 0$, le numérateur est bien un entier. La fraction n'est peut être pas sous forme réduite mais le dénominateur n'est pas divisible par p ce qui implique bien que $v_p(x+y) \geqslant \alpha = \min(\alpha, \beta)$. □

REMARQUE 2.4. Il est possible que $v_p(x+y) > \min(v_p(x), v_p(y))$. Par exemple si $x = -y$, alors $v_p(x+y) = +\infty$.

On définit la *valeur absolue p-adique* de $x \in \mathbf{Q}$ par

$$|x|_p := p^{-v_p(x)}. \tag{18}$$

Par le lemme 2.3, elle vérifie les propriétés suivantes.

PROPOSITION 2.5. *(1)* $|x|_p = 0 \Leftrightarrow x = 0$.

(2) $\forall x, y \in \mathbf{Q}, |x \cdot y|_p = |x|_p \cdot |y|_p$.

(3) $\forall x, y \in \mathbf{Q}, |x+y|_p \leqslant \max\left(|x|_p, |y|_p\right)$.

EXERCICE 2.6. On définit la fonction suivante :

$$\forall x, y \in \mathbf{Q}, d_p(x,y) = |x-y|. \tag{19}$$

Montrer que d_p est une distance et qu'elle vérifie l'inégalité suivante

$$\forall x, y, z \in \mathbf{Q}, \quad d_p(x,z) \leqslant \max\left(d_p(x,y), d_p(y,z)\right). \tag{20}$$

On appelle cette inégalité, *l'inégalité ultramétrique*. On appelle d_p la distance p-adique.

EXERCICE 2.7. Montrer que la suite (p^n) converge vers 0 pour la distance p-adique.

2.2. Complétion.

DÉFINITION 2.8. Soit (X,d) un espace métrique. Une suite (x_n) dans X est *de Cauchy* si

$$\forall \varepsilon > 0, \exists n_0 \geqslant 0, \forall n, m \geqslant n_0, \quad d(x_n, x_m) < \varepsilon. \tag{21}$$

On dit que X est *complet* si toute suite de Cauchy est convergente.

THÉORÈME 2.9. *Soit (X,d) un espace métrique, il existe un unique espace métrique complet $\widehat{X}$ tel que*

(1) Il existe une isométrie injective $\iota : X \hookrightarrow \widehat{X}$.

(2) $\iota(X)$ est dense dans $\widehat{X}$.

On dit que $\widehat{X}$ est le complété *de X pour la distance d.*

PROPOSITION 2.10. *L'espace métrique $(\mathbf{Q}, d_p)$ n'est pas complet pour tout p premier.*

DÉMONSTRATION. Supposons $p \geqslant 5$ impair. Soit $1 < a < p-1$ une entier. Considérons la suite $x_n = a^{p^n}$. Cette suite est de Cauchy car

$$x_{n+1} - x_n = a^{p^{n+1}} - a^{p^n} = a^{p^n}\left(a^{p^n(p-1)} - 1\right). \tag{22}$$

Or $p^n(p-1)$ est le cardinal du groupe $(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$ donc on a que $a^{p^n(p-1)} - 1$ est divisible par p^{n+1} et donc

$$|x_{n+1} - x_n|_p \leqslant \frac{1}{p^{n+1}} < \frac{1}{p^n}. \tag{23}$$

Par un argument téléscopique on obtient que

$$\forall m \geqslant n, |x_m - x_n|_p \frac{1}{p^{n+1}} < \frac{1}{p^n}. \tag{24}$$

Donc, c'est une suite de Cauchy. Supposons qu'elle converge vers un nombre rationnel $x \in \mathbf{Q}$. On a par construction que

$$x^p = x \tag{25}$$

et donc que $x^{p-1} = 1$. Donc x est une racine $p-1$-ième de l'unité. On a donc que $x = \pm 1$. De plus, en appliquant (24) avec $n = 0$ et en faisant tendre m vers $+\infty$, on obtient que

$$|x - a|_p < 1. \tag{26}$$

Ce qui implique que $x \neq \pm 1$ car $a \neq 1, p-1$.

Pour $p = 2, 3$, On verra plus tard le lemme de Hensel qui permettra de construire dans $\mathbf{Q}_2$ et $\mathbf{Q}_3$ (les complétés de $\mathbf{Q}$ pour la distance 2 et 3-adique respectrivement) des racines de polynômes irréductibles sur $\mathbf{Q}$ ce qui prouve que $\mathbf{Q} \neq \mathbf{Q}_2, \mathbf{Q}_3$ □

On définit $\mathbf{Q}_p$ comme le complété de $\mathbf{Q}$ pour la distance p-adique. La valeur absolue p-adique $|\cdot|_p$ s'étend de façon naturelle à $\mathbf{Q}_p$ en effet, on a $|x|_p = d_p(x,0)$. Par définition, tout élément $x \in \mathbf{Q}_p$ est une limite d'entiers x_n. Les propriétés énoncées dans 2.5 sont encore vraies dans $\mathbf{Z}_p$. On définit

$$\forall x, y \in \mathbf{Q}_p, \quad x + y = \lim_n x_n + y_n, \quad xy = \lim x_n y_n. \tag{27}$$

On définit également $\mathbf{Z}_p$ comme le complété de $\mathbf{Z}$ pour la distance p-adique. On a $\mathbf{Z}_p \subset \mathbf{Q}_p$.

PROPOSITION 2.11. *L'addition et la multiplication définies par* (27) *sont bien définies. En particulier, elle ne dépend pas du choix des suites* (x_n, y_n). *En particulier,* $\mathbf{Q}_p$ *est un corps et* $\mathbf{Z}_p$ *est un anneau.*

DÉMONSTRATION. On montre tout d'abord que les suites $(x_n + y_n)$ et $(x_n y_n)$ sont de Cauchy. On a

$$\forall n, m, \quad (x_m + y_m) - (x_n + y_n) = (x_m - x_n) + (y_m - y_n) \tag{28}$$

De sorte que si (x_n) et (y_n) sont de Cauchy, leur somme aussi. Maintenant pour le produit

$$x_m y_m - x_n y_n = x_m(y_m - y_n) + y_n(x_n - x_m). \tag{29}$$

De sorte que

$$|x_m y_m - x_n y_n| \leqslant \max\left(\max(|x_k|_p)\,|y_m - y_n|\,, \max(|y_l|_p)\,|x_m - x_n|_p\right). \tag{30}$$

De sorte que cette suite est également de Cauchy (les suites $(x_k), (y_l)$ sont convergentes donc les suites $(|x_k|), (|y_l|)$ le sont aussi et les deux maximums sont bien définis). On peut donc prendre la limite de ces suites. On montre maintenant que le résultat ne dépend pas des suites choisies. Si $(x_n), (x'_n), (y_n), (y'_n)$ sont des suites d'entiers qui approximent x et y respectivement, alors on a

$$\left|(x_n + y_n) - (x'_n + y'_n)\right| \leqslant \max\left(\left|x_n - x'_n\right|_p, \left|y_n - y'_n\right|_p\right). \tag{31}$$

Comme $x_n - x'_n$ et $y_n - y'_n$ tendent vers zero on a bien que $\lim_n x_n + y_n = \lim_n x'_n + y'_n$.

Pour le produit on a

$$x_n y_n - x'_n y'_n = x_n(y_n - y'_n) + y_n(x'_n - x_n). \tag{32}$$

Encore une fois, cette suite tend vers zéro. On a donc à ce stade que $\mathbf{Q}_p$ et $\mathbf{Z}_p$ sont des anneaux. Pour montrer que $\mathbf{Q}_p$ est un corps il faut montrer que tout élément non nul a un inverse. Soit $x \in \mathbf{Q}_p \setminus \{0\}$ et (x_n) une suite de rationnels convergeant vers x. Comme $|x| \neq 0$, à partir d'un certain rang, tous les x_n sont non nuls. Montrons que la suite $\frac{1}{x_n}$ converge vers l'inverse de x. Montons d'abord qu'elle est de Cauchy. On a

$$\frac{1}{x_m} - \frac{1}{x_n} = \frac{x_n - x_m}{x_n x_m}. \tag{33}$$

Ce qui montre que la suite est de Cauchy car pour tout n assez grand $|x_n| > \frac{|x|}{2} > 0$. On définit $y_n = \frac{1}{x_n}$ et $y = \lim y_n$. On a alors

$$1 = \lim x_n y_n = xy. \tag{34}$$

D'où $y = \frac{1}{x}$. □

COROLLAIRE 2.12 (Corollaire de la preuve). *Les applications d'addition*

$$+ : (x,y) \in \mathbf{Q}_p \times \mathbf{Q}_p \mapsto x+y \in \mathbf{Q}_p, \tag{35}$$

de multiplication

$$\times : (x,y) \in \mathbf{Q}_p \times \mathbf{Q}_p \mapsto xy \in \mathbf{Q}_p \tag{36}$$

et d'inversion

$$inv : x \in \mathbf{Q}_p^\times \mapsto \frac{1}{x} \in \mathbf{Q}_p. \tag{37}$$

sont continues.

PROPOSITION 2.13. *Soit (u_n) une suite de $\mathbf{Q}_p$, alors*

$$\sum u_n \tag{38}$$

converge dans $\mathbf{Q}_p$ si et seulement si $u_n \to 0$.

DÉMONSTRATION. Soit $S_n = \sum_{k=0}^n u_k$. On a $u_n = S_{n+1} - S_n$ donc si S_n converge alors u_n tend vers 0. Réciproquement, supposons que u_n converge vers 0. Cela signifie que pour tout $\varepsilon > 0$ il existe n_0 tel que $\forall n \geqslant n_0, |u_n| < \varepsilon$. Maintenant, on a pour tout $m \geqslant n \geqslant n_0$

$$|S_m - S_n| = \left| \sum_{k=n+1}^{m} u_k \right| \leqslant \varepsilon \tag{39}$$

où la dernière inégalité est obtenue par l'inégalité ultramétrique. On a donc que la suite (S_n) est de Cauchy et donc elle converge. □

EXERCICE 2.14. Soit $u \in \mathbf{Q}_p$ tel que $|u| < 1$. Montrer que $|1-u| = 1$. (Indice : écrire $\frac{1}{1-u} = \sum_{k \geqslant 0} u^k$ et montrer que la série est convergente.)

COROLLAIRE 2.15. *Si $x, y \in \mathbf{Q}_p$ avec $|x| < |y|$, alors*

$$|x+y| = |y|. \tag{40}$$

DÉMONSTRATION. On a que

$$|x+y| = |y| \cdot \left| 1 + \frac{x}{y} \right|. \tag{41}$$

Or par construction on a que $\left|\frac{x}{y}\right| < 1$ donc par l'exercice, on a que $\left|1 + \frac{x}{y}\right| = 1$. □

PROPOSITION 2.16. *L'image du morphisme de groupes*

$$x \in \mathbf{Q}_p^\times \mapsto \log |x|_p \in \mathbf{R} \tag{42}$$

est le sous-groupe discret $\mathbf{Z} \cdot \log p$.

DÉMONSTRATION. Pour tout $x \in \mathbf{Q}$, on a $|x_p| = p^{-v_p(x)}$. Donc l'image $\log \left|\mathbf{Q}^\times\right| = \mathbf{Z} \cdot \log p$. Comme $\mathbf{Q}$ est dense dans $\mathbf{Q}_p$ cela donne le résultat. □

PROPOSITION 2.17. *On a les propriétés suivantes.*

(1) $\mathbf{Z}_p$ *est l'adhérence de* $\mathbf{Z}$ *dans* $\mathbf{Q}_p$.

(2) $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x| \leqslant 1\}$.

(3) $\mathbf{Z}_p^\times = \{x \in \mathbf{Q}_p : |x| = 1\}$.

(4) $\mathbf{Q}_p$ *est le corps des fractions de* $\mathbf{Z}_p$.

(5) $\{x \in \mathbf{Z}_p : |x| < 1\}$ *est l'unique idéal maximal de* $\mathbf{Z}_p$*, c'est l'idéal engendré par* p.

(6) $\mathbf{Z}_p$ *est intégralement clos dans* $\mathbf{Q}_p$.

DÉMONSTRATION. L'assertion (1) vient du fait que $\mathbf{Z}_p$ est le complété de $\mathbf{Z}$. Montrons (2), soit $x \in \mathbf{Q}_p$ avec $|x| \leqslant 1$. Par la proposition 2.16, cela implique qu'il existe une suite de rationnels x_n avec $|x_n| \leqslant 1$ qui converge vers x (le seul cas où on doit utiliser la proposition est si $|x| = 1$). On va montrer qu'on peut remplacer x_n par une suite d'entiers. On écrit

$$x_n = \frac{a_n}{b_n}. \tag{43}$$

Le fait que $|x_n| \leqslant 1$ signifie que b_n est premier avec p. Il suffit alors de montrer que pour tout entier $m \in \mathbf{Z}$ premier avec p, il existe une suite d'entiers m_k qui converge vers $1/m$ pour la distance p-adique. Montrons ce résultat à l'aide du théorème de Bézout. Soit $k \geqslant 1$, comme m et p^k sont premiers entre eux il existe par le théorème de Bézout des entiers $u, v \in \mathbf{Z}$ tels que

$$um + p^k v = 1. \tag{44}$$

On a alors

$$u - \frac{1}{m} = p^k \frac{v}{m}. \tag{45}$$

Et

$$\left| p^k \frac{v}{m} \right| \leqslant p^{-k} \tag{46}$$

car $|m| = 1$ et le résultat est démontré. Les assertions (3) et(4) viennent du fait que si $x \neq 0, \left|\frac{1}{x}\right| = \frac{1}{|x|}$. Pour (5), il est clair par l'inégalité ultramétrique que $\{|x| < 1\}$ est un idéal de $\mathbf{Z}_p$. Il est maximal car par (3), tout élément en dehors de cet idéal est inversible dans $\mathbf{Z}_p$. Par la proposition 2.16, si $|x| < 1$ et $x \neq 0$, il existe $k \geqslant 1$ tel que $|x| = \frac{1}{p^k}$. Et alors

$$x = p \cdot \frac{1}{p} x \tag{47}$$

et $\frac{1}{p}x \in \mathbf{Z}_p$. D'où le fait que cet idéal est principal, engendré par p.

Montrons enfin que $\mathbf{Z}_p$ est intégralement clos dans $\mathbf{Q}_p$. Soit $z \in \mathbf{Q}_p$ tel que z est solution d'une équation

$$z^N + a_{N-1}z^{N-1} + \cdots + a_1 z + a_0 = 0 \tag{48}$$

avec $a_i \in \mathbf{Z}_p$. On a alors

$$z^N = -\sum_{k \leqslant N-1} a_k z^k \tag{49}$$

et donc

$$|z|^N \leqslant \max(|a_k|\,|z|^k). \tag{50}$$

Or si $|z| > 1$, alors pour tout $k = 0, \ldots, N-1$, comme $a_k \leqslant 1$, on a

$$|z|^N > \left|z^k\right| > |a_k|\left|z^k\right|. \tag{51}$$

Ce qui est une contradiction. □

PROPOSITION 2.18. *Tout idéal de $\mathbf{Z}_p$ est principal, engendré par une puissance de p. De plus, on a*

$$p^k\mathbf{Z}_p = \left\{x \in \mathbf{Q}_p : |x| \leqslant \frac{1}{p^k}\right\} \tag{52}$$

et

$$\mathbf{Z}_p/p^k\mathbf{Z}_p = \mathbf{Z}/p^k\mathbf{Z}. \tag{53}$$

DÉMONSTRATION. Soit $I \subset \mathbf{Z}_p$ un idéal. Si $I = \mathbf{Z}_p$, alors $I = (1)$ et il n'y a rien à démontrer. Sinon, soit $k = \min\{v_p(i) : i \in I\}$. On a que $k \geqslant 1$ car tout élément de valuation p-adique zéro est inversible dans $\mathbf{Z}_p$. Soit $u \in I$ tel que $v_p(u) = k$, alors $u/p^k \in \mathbf{Z}_p$ et donc $p^k = p^k \cdot u/p^k \in I$. Ainsi, $p^k\mathbf{Z}_p \subset I$. Réciproquement, si $i \in I$, alors $v_p(i) \geqslant k$, donc $i/p^k \in \mathbf{Z}_p$ et $i \in p^k\mathbf{Z}_p$. Construisons l'application quotient $\mathbf{Z}_p \to \mathbf{Z}/p^k\mathbf{Z}$.

LEMME 2.19. *Soit $x \in \mathbf{Z}_p$, pour toute suite d'entiers x_n convergeant vers x, on a que la suite*

$$\left(x_n \bmod p^k\right) \subset \mathbf{Z}/p^k\mathbf{Z} \tag{54}$$

est stationnaire et sa limite ne dépend que de x.

DÉMONSTRATION. Par construction la suite $x_n - x_m$ est de Cauchy. Donc pour n, m assez grand, p^k divise $x_n - x_m$ et donc $x_n = x_m \bmod p^k$. Si y_n est une autre suite d'entiers convergeant vers x, alors $x_n - y_n$ converge vers zéro et donc pour n assez grand on a que $x_n = y_n \bmod p^k$. □

Ce lemme permet de construire le morphisme d'anneaux

$$\phi_k : \mathbf{Z}_p \to \mathbf{Z}/p^k\mathbf{Z} \tag{55}$$

par

$$\phi_k(x) = \lim_n x_n \bmod p^k \tag{56}$$

avec x_n une suite d'entiers. On a que le morphisme est surjectif car $\phi_k(\mathbf{Z}) = \mathbf{Z}/p^k\mathbf{Z}$. Montrons que son noyau est $p^k\mathbf{Z}_p$. On a que

$$\phi_k(x) = 0 \Leftrightarrow \lim_n \phi_k(x_n) = 0 \Leftrightarrow \forall n \gg 1, p^k | x_n \Leftrightarrow |x| \leqslant \frac{1}{p^k} \Leftrightarrow x \in p^k\mathbf{Z}_p. \tag{57}$$

□

On peut parler de divisibilité dans $\mathbf{Z}_p$ et on a alors à nouveau

$$\forall x \in \mathbf{Z}_p, \quad v_p(x) = \max\left\{k \geqslant 0, p^k | x\right\}. \tag{58}$$

De même, la valuation p-adique d'un élément $x \in \mathbf{Q}_p$ et l'unique entier k tel que

$$x = p^k u \tag{59}$$

avec $u \in \mathbf{Z}_p^\times$.

2.3. Topologie de $\mathbf{Q}_p$. Comme vous avez pu le voir en exercice, la topologie de $\mathbf{Q}_p$ est très différente de la topologie de $\mathbf{R}$.

DÉFINITION 2.20. On définit les disques ouverts, fermés et les cercles comme ceci. Soit $x \in \mathbf{Q}_p, r \geqslant 0$,

$$\mathbb{D}(x,r) = \left\{z \in \mathbf{Q}_p : |x-z|_p < r\right\}, \overline{\mathbb{D}}(x,r) = \left\{z \in \mathbf{Q}_p : |x-z|_p \leqslant r\right\} \tag{60}$$

and

$$C(x,r) = \{z \in \mathbf{Q}_p : |x-z| = r\}. \tag{61}$$

PROPOSITION 2.21. *Pour tout $x \in \mathbf{Q}_p, r > 0$, les espaces $\mathbb{D}(x,r), \overline{D}(x,r), C(x,r)$ sont ouverts et fermés.*

DÉMONSTRATION. Il est clair que $\mathbb{D}(x,r)$ est ouvert et que $\overline{D}(x,r)$ et $C(x,r)$ sont fermés car ils sont définis par des conditions respectivement ouvertes et fermés. Le disque ouvert $\mathbb{D}(x,r)$ est fermé car si $k \in \mathbf{Z}$ est le plus petit entier tel que $p^{-k} < r$, alors $\mathbb{D}(x,r) = \overline{\mathbb{D}}(x,p^{-k})$. Il est à noter que k est bien défini car l'ensemble des valeurs de la valeur absolue p-adique est discret par la proposition 2.16.

Le fait que $\overline{D}(x,r)$ et $C(x,r)$ soient fermés vient du corollaire 2.15. □

On dira d'un espace qui est à la fois ouvert et fermé qu'il est *clopen* (contraction de closed et open).

REMARQUE 2.22. Attention cela signifie que l'adhérence de $\mathbb{D}(x,r)$ est lui-même et non pas $\overline{\mathbb{D}}(x,r)$.

On va s'intéresser maintenant plus particulièrement à la topologie de $\mathbf{Z}_p$. Soit $k \geqslant 1$ et $x, y \in \mathbf{Z}_p$, on a que

$$y \in \overline{D}(x, p^{-k}) \Leftrightarrow |x-y| \leqslant \frac{1}{p^k} \Leftrightarrow p^k | x-y \Leftrightarrow x = y \bmod p^k. \tag{62}$$

Mais on a vu que $\mathbf{Z}_p/p^k\mathbf{Z}_p = \mathbf{Z}/p^k\mathbf{Z}$ est fini. Il y a donc exactement p^k disques de rayon $\frac{1}{p^k}$ dans $\mathbf{Z}_p$ et ils sont tous disjoints. Autrement dit

$$\mathbf{Z}_p = \bigsqcup_{t=0}^{p^k-1} \overline{D}(t, p^{-k}). \tag{63}$$

Que se passe-t-il si on passe de k à $k+1$? On sait que les p^{k+1} disques de rayons $p^{-(k+1)}$ sont paramétrés par les entiers $0, \ldots, p^{k+1}$. Pour savoir dans quel disque de rayon $\frac{1}{p^k}$ ils sont contenus, il suffit de regarder la congurence modulo p^k. On a

$$\forall t \in \left\{0, \ldots, p^{k+1}-1\right\}, \quad \overline{D}(t, p^{-(k+1)}) \subsetneq \overline{D}(t \bmod p^k, p^{-k}). \tag{64}$$

On peut faire le dessin suivant où en bleu on a les p disques de rayons $1/p$ indexés par $0, \ldots, p-1$ et dans le disque $\overline{\mathbb{D}}(0, \frac{1}{p})$ on a dessiné en rouge les p disques de rayons $\frac{1}{p^2}$ indexés par $0, p, 2p, \ldots, (p-1)p$. On voit donc que chaque disque de rayon $\frac{1}{p^k}$ il y a exactement p disques de rayon $\frac{1}{p^k}$. Plus précisément si $D = \overline{D}(u, p^{-k}$ avec $u \in \left\{0, \ldots, p^k-1\right\}$, alors les p disques de rayons $\frac{1}{p^{k+1}}$ contenus dans D sont

$$D_{t,u} := \overline{\mathbb{D}}(t \cdot p^k + u, \frac{1}{p^{k+1}}) \tag{65}$$

pour $t = 0, \ldots, p-1$. On peut donc définir l'application $\phi : \mathbf{Z}_p \to \left\{0, \ldots, p^-1\right\}^{\mathbf{N}}$ qui à toute $x \in \mathbf{Z}_p$ définie la suite (x_i) de la façon suivante.

$$x_1 = x \bmod p. \tag{66}$$

On peut noter que $x \in \overline{\mathbb{D}}(x_1, \frac{1}{p})$. Supposons avoir construit x_k pour $k \geqslant 1$ tel que si on définit $u_k = \sum_{l=1}^{k} x_l p^{l-1}$, alors $x \in \overline{\mathbb{D}}(u_k, \frac{1}{p^k})$. On définit alors x_{k+1} par la propriété

$$x \in D_{u_k, x_{k+1}} = \overline{D}(x_{k+1} \cdot p^k + u_k, \frac{1}{p^{k+1}}). \tag{67}$$

On peut noter que pour tout $k \geqslant 0, |x - u_k| \leqslant \frac{1}{p^k}$, de sorte que $u_k \to x$. On munit l'espace $\{0, \ldots, p-1\}^{\mathbf{N}}$ de la métrique définie par

$$d\left((x_k), y_k\right) = p^{-(\min(l \geqslant 0 : x_l \neq y_l) - 1)}. \tag{68}$$

EXERCICE 2.23. Montrer que la topologie induite par cette distance est la topologie produit sur $0, \ldots, p-1^{\mathbf{N}}$.

PROPOSITION 2.24. *L'application* $\phi : \mathbf{Z}_p \to \{0, \ldots, p-1\}^{\mathbf{N}}$ *est une isométrie bijective.*

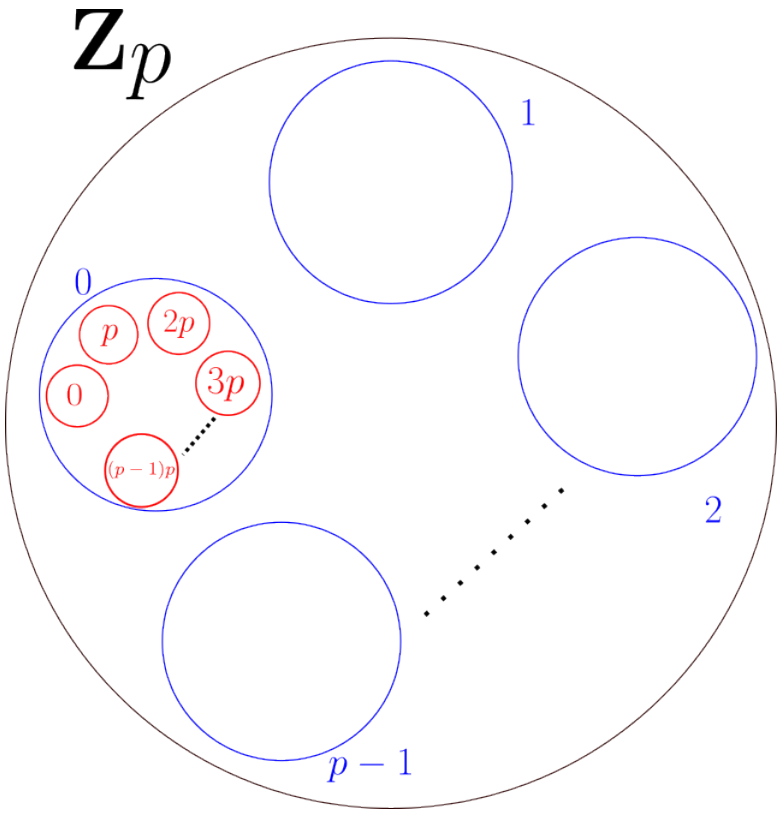

FIGURE 1. Les disques de rayons $1/p$ et $1/p^2$ dans $\mathbf{Z}_p$

DÉMONSTRATION. Montrons d'abord que c'est une bijection. Si (x_k) est une suite, alors on définit pour tout $n \geqslant 0$

$$u_n = \sum_{k=0}^{n} x_k p^k \in \mathbf{Z}_p. \tag{69}$$

On a que (u_n) est une suite de Cauchy car pour tout $m \geqslant n$

$$|u_m - u_n| \leqslant \frac{1}{p^{n+1}}. \tag{70}$$

Soit x sa limite, on a bien que $\phi(x) = x_k$. C'est une isométrie car si $x, y \in \mathbf{Z}_p$ telle que

$$|x - y| = \frac{1}{p^k} \tag{71}$$

alors x et y appartiennent au même boule de rayons $\frac{1}{p^l}$ pour $\ell = 1, \ldots, k$ et donc on a

$$\forall l = 1, \ldots, k, x_l = y_l. \tag{72}$$

□

En particulier, pour les entiers $z \in \mathbf{N}$, on retrouver l'écriture en base p de x.

COROLLAIRE 2.25. *L'espace $\mathbf{Z}_p$ est un Cantor : il est totatement discontinu et a la même cardinalité que $\mathbf{R}$.*

DÉMONSTRATION. Le fait que $\mathbf{Z}_p$ est totalement discontinu vient du fait que l'image de la valeur absolue est discrète et a été vu en exercice. Le fait que $\mathbf{Z}_p$ a la même cardinalité que $\mathbf{R}$ vient du fait que $\{0,\dots,p-1\}^{\mathbf{N}}$ a la cardinalité de $\mathbf{R}$. En effet, cela vient du fait que tout nombre $y \in [0,1[$ peut être écrit de façon unique sous la forme

$$y = \sum_{k=1}^{+\infty} \frac{y_k}{p^k} \tag{73}$$

où $y_k \in 0,\dots,p-1$ et (y_k) ne stationne pas à la valeur $p-1$. □

On peut également définir un autre homéomorphisme. Pour tout $m \geqslant n$ on a l'homomorphisme d'anneaux canonique

$$\pi_{m,n} : \mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}. \tag{74}$$

Soit $W \subset \prod_{i=1}^{+\infty} \mathbf{Z}/p^i\mathbf{Z}$ tel que

$$W = \left\{(x_i) \in \mathbf{Z}/p^i/Z : \forall m \geqslant n, \pi_{m,n}(x_m) = x_n\right\}. \tag{75}$$

On dit que W est la *limite projective* des $\mathbf{Z}/p^i\mathbf{Z}$. On note traditionnellemment

$$W = \varprojlim_{i \to +\infty} \mathbf{Z}/p^i\mathbf{Z}. \tag{76}$$

On peut munir l'espace produit $\prod_i \mathbf{Z}/p^i\mathbf{Z}$ de la topologie produit (en prenant la topologie discrète pour chacun des $\mathbf{Z}/p^i\mathbf{Z}$). Et on peut restreindre cette topologie à W.

EXERCICE 2.26. Montrer que si $m \geqslant n' \geqslant n$, alors

$$\pi_{m,n} = \pi_{n',n} \circ \pi_{m,n'}. \tag{77}$$

En déduire que dans la définition de W, on peut se contenter d'imposer

$$\pi_{n+1,n}(x_{n+1}) = x_n. \tag{78}$$

PROPOSITION 2.27. *On définit l'application $\psi : \mathbf{Z}_p \to W$ par*

$$\forall x \in \mathbf{Z}_p, \quad \psi(x) = (x \ mod \ p^i). \tag{79}$$

Alors ψ est un homéomorphisme.

DÉMONSTRATION. Montrons que ψ est bijective. Soit $(x_k) \in W$. On définit $z_k \in \mathbf{Z}_p$ de la façon suivante : z_k est l'unique entier dans $\{0, \dots, p^k - 1\}$ tel que $x_k = z_k \bmod p$. Montrons que la suite z_k est de Cauchy et converge vers $z \in \mathbf{Z}_p$ tel que $\psi(z) = (x_k)$. Pour tout $m \geqslant n$, on a par construction que

$$z_m = z_n \bmod p^n \tag{80}$$

et donc $|z_m - z_n| \leqslant \frac{1}{p^n}$. Donc la suite est de Cauchy et a une limite z. Pour tout $n \geqslant 1$, on a $|z - z_n| \leqslant \frac{1}{p^n}$. Donc $z \bmod p^n = z_n \bmod p^n = x_n$. D'où $\psi(z) = x$. Montrons que ψ est continue. Une base de la topologie sur W est donné par les ouverts de la forme

$$\forall n \geqslant 1, \forall x_n \in \{0, \dots, p^n - 1\}, \quad W_{n,x_n} = \{(y_k) \in W : y_n = x_n \bmod p^n\}. \tag{81}$$

En effet, la condition $y_n = x_n \bmod p^n$ fixe les n-premières valeurs par la compatibilité des projections. Or on a

$$\psi^{-1}(W_{n,x_n}) = \overline{\mathbb{D}}(x_n, \frac{1}{p^n}). \tag{82}$$

En effet, $\psi(z) \in W_{n,x_n}$ si et seulement si $z = x_n \bmod p^n$ si et seulement si $p^n | z - x_n$ si et seulement si $z \in \overline{\mathbb{D}}(x_n, \frac{1}{p^n})$. □

EXERCICE 2.28. Écrire une formule pour l'application $\phi \circ \psi^{-1} : W \to \{0, \dots, p-1\}^{\mathbf{N}}$.

PROPOSITION 2.29. *L'espace $\mathbf{Z}_p$ est compact, l'espace $\mathbf{Q}_p$ est localement compact.*

DÉMONSTRATION. On sait par la proposition 2.17 que $\mathbf{Z}_p = \overline{\mathbb{D}}(0,1)$. Maintenant une base de la topologie de $\mathbf{Q}_p$ est donné par les disques $\overline{\mathbb{D}}(x, \frac{1}{p^k}) = x + p^k \mathbf{Z}_p$ donc si on montre que $\mathbf{Z}_p$ est compact on a que $\mathbf{Q}_p$ est localement compact.

Comme $\mathbf{Z}_p$ est un espace métrique, pour montrer qu'il est compact il suffit de montrer que toute suite admet une valeur d'adhérence. Notons que par la proposition 2.24, on a que $\mathbf{Z}_p$ est homéomorphe à un produit d'espaces compacts donc est compact par le théorème de Tychonoff. Cependant nous donnons une preuve plus élémentaire ici. Soit (z_n) une suite de $\mathbf{Z}_p$. On construit par récurrence une fonction $\phi : \mathbf{N} \to \mathbf{N}$ strictement croissante telle que

$$\forall n \geqslant 1, \{m > \phi(n) : z_m = z_{\phi(n)} \bmod p^n\} \tag{83}$$

est infini et pour tout $n' \leqslant n, z_{\phi(n)} = z_{\phi(n')} \bmod p^{n'}$. est infini. Commencons par $\phi(1)$. La suite $(z_n \bmod p)_{n \geqslant 1}$ est une suite de $\mathbf{Z}/p\mathbf{Z}$ donc il existe $k \in \mathbf{Z}/p\mathbf{Z}$ telle que $\Lambda_k = \{n \geqslant 1 : z_n \bmod p = k\}$ est infini. On pose $\phi(1) = \min \Lambda_k$. Supposons avoir construit $\phi(1), \dots, \phi(n)$ qui vérifie les propriétés énoncées précedemment et construisons $\phi(n+1)$. Par hypothèse, l'ensemble

$$A_n = \{m > \phi(n) : z_m = z_{\phi(n)} \bmod p^n\} \tag{84}$$

est infini. Considérons la suite $(z_m \bmod p^{n+1})_{m \in A_n}$. C'est une suite de $\mathbf{Z}/p^{n+1}\mathbf{Z}$ donc il existe $k \in \mathbf{Z}/p^{n+1}\mathbf{Z}$ tel que l'ensemble Λ_k défini par

$$\Lambda_{k,n} = \{m \in A_n : k = z_m \bmod p^{n+1}\} \tag{85}$$

est infini. On définit $\phi(n+1) := \min \Lambda_{k,n}$, on a bien $\phi(n+1) > \phi(n)$. Toutes les propriétés sont bien vérifiées car $\phi(n+1) \in A_n$ donc $z_{\phi(n+1)} = z_{\phi(n)} \bmod p^n$.

Montrons que la sous-suite $(z_{\phi(n)})$ est convergente. Il suffit de montrer qu'elle est de Cauchy. Par construction on a que pour tout $m \geqslant n, z_{\phi(m)} = z_{\phi(n)} \bmod p^n$ et donc

$$\left|z_{\phi(m)} - z_{\phi(n)}\right|_p \leqslant \frac{1}{p^n}. \tag{86}$$

C'est bien une suite de Cauchy. □

EXERCICE 2.30. Refaire la preuve de la compacité de $\mathbf{Z}_p$ mais en utilisant plutôt l'homéomorphisme de la proposition 2.24. Quels devraient être les équivalents des ensembles $\Lambda_{k,n}$ et A_n ?

3. Le lemme d'Hensel

Ce dont Hensel s'est rendu compte est qu'on pouvait utiliser l'algorithme itératif de Newton sur les nombres p-adiques pour construire des solutions d'équations polynomiales. Avant cela, énonçons le premier principe d'Hensel.

PROPOSITION 3.1. *Soit $P \in \mathbf{Z}_p[X_1, \ldots, x_n]$ un polynôme à n variables, alors les assertions suivantes sont équivalentes.*

(1) $P = 0$ admet une une solution dans $\mathbf{Z}_p^n$.

(2) pour tout $k \geqslant 1, P = 0$ admet une solution dans $\mathbf{Z}/p^k\mathbf{Z}$.

DÉMONSTRATION. La preuve sera faite en exercice. □

Rappelons brièvement comment fonctionne l'algorithme de Newton sur R. Soit $f : \mathbf{R} \to \mathbf{R}$ une fonction C^1. On cherche à trouver une solution de $f(x) = 0$. On part d'un point $x_0 \in \mathbf{R}$. On définit par induction la suite (x_n) par

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{87}$$

On définit la fonction $N_f(x) = x - \frac{f(x)}{f'(x)}$. L'idée est que si a est un zéro de f et que f est C^2, alors on a par Taylor-Lagrange

$$0 = f(a) = f(x) + f'(x)(a-x) + f''(\xi)\frac{(a-x)^2}{2} \tag{88}$$

pour $\xi \in]a,x[$. Soit $M_2 = \max_{[a,x]} |f''|$ et $m_1 = \min_{[a,x]} |f'|$, alors

$$\left|N_f(x) - a\right| \leqslant \frac{2M_2}{m_2} |x-a|^2. \tag{89}$$

De sorte que par récurrence, on a si $K = \frac{2M_2}{m_1}$ que

$$K|x_n - a| \leqslant (K|x_0 - a|)^{2^n}. \tag{90}$$

C'est donc un algorithme qui converge très rapidement. On voit que si on cherche la solution sous forme dyadique, on double le nombre de décimales connues après chaque itération. Hensel applique l'équivalent de l'algorithme de Newton pour les nombres p-adiques. Rappelons que si P est un polynôme, on peut toujours écrire

$$P(X+h) = P(X) + hP_1(X,h) = P(X) + hP'(X) + h^2P_2(X,h) \tag{91}$$

où P_1, P_2 sont des polynômes à deux variables à coefficients dans $\mathbf{Z}_p$.

PROPOSITION 3.2. *Soit $P \in \mathbf{Z}_p[X]$ un polynôme et $x \in \mathbf{Z}_p$ tel que $P(x) = 0$ mod p^n (donc x n'est pas trop loin d'une racine de P). Si $k = v(P'(x)) < n/2$, alors si $\widehat{x} = N_P(x) = x - \frac{P(x)}{P'(x)}$, alors*

(1) $P(\widehat{x}) = 0$ mod p^{n+1} (on a une meilleure approximation de la racine).

(2) $\widehat{x} = x$ mod p^{n-k} ($\widehat{x}$ n'est pas trop loin de x).

(3) $v(P'(\widehat{x})) = v(P'(x))(= k)$ (on peut itérer).

DÉMONSTRATION. On écrit $P(x) = p^n y$ avec $y \in \mathbf{Z}_p$ et $P'(x) = p^k u$ avec $u \in \mathbf{Z}_p^\times$, alors

$$\widehat{x} - x = -\frac{P(x)}{P'(x)} = -p^{n-k}\frac{y}{u}. \tag{92}$$

Ce qui montre bien que $|\widehat{x} - x| \leqslant \frac{1}{p^{n-k}}$. Ensuite, on a par (91) que

$$P(\widehat{x}) = P(x + (\widehat{x} - x)) = P(x) - \frac{P(x)}{P'(x)}P'(x) + (\widehat{x} - x)^2 t = (\widehat{x} - x)^2 t. \tag{93}$$

Comme $k < n/2$, on a que $2(n-k) > n$ donc $2(n-k) \geqslant n+1$ et

$$|P(\widehat{x})| \leqslant \frac{1}{p^{n+1}}. \tag{94}$$

Enfin on applique la formule d'expansion de Taylor pour P' :

$$P'(\widehat{x}) = P'(x + (\widehat{x} - x)) = P'(x) + (\widehat{x} - x) \cdot s \tag{95}$$

avec $s \in \mathbf{Z}_p$. Comme $n - k > n/2$, on a que

$$\left|P'(\widehat{x})\right| = \left|P'(x)\right| = p^{-k}. \tag{96}$$

□

On peut maintenant énoncer le théorème de Hensel.

THÉORÈME 3.3. *Soit $P \in \mathbf{Z}_p[X]$ et $x \in \mathbf{Z}_p$ tel que*

$$P(x) = 0 \text{ mod } p^n. \tag{97}$$

Si $k = v_p(P'(x)) < n/2$, alors il existe une unique racine ξ de P dans $\mathbf{Z}_p$ tel que

$$\xi = x \text{ mod } p^{n-k} \text{ et } v_p(P'(\xi)) = v(P'(x)). \tag{98}$$

DÉMONSTRATION. Commençons par l'existence. On définit une suite (x_l) de $\mathbf{Z}_p$ par $x_0 = x$ et $x_{l+1} = N_P(x_l)$. Montrons que cette suite est bien définie. Par la proposition 3.2, on a que

$$x_1 = x_0 \bmod p^{n-k}, \quad P(x_1) = 0 \bmod p^{n+1}, \quad v_p(P'(x_1)) = v_p(P'(x_0)) = k < n/2. \tag{99}$$

On voit donc par récurrence avec la proposition 3.2 que

$$x_{l+1} = x_l \bmod p^{n+l-k}, \quad P(x_{l+1}) = 0 \bmod p^{n+l+1}, \quad v_p(P'(x_{l+1})) = k. \tag{100}$$

On a donc que pour tout $m \geqslant l$

$$|x_m - x_l| \leqslant \frac{1}{p^{n+l-k}} \tag{101}$$

C'est donc une suite de Cauchy et si ξ et sa limite, on a que

$$|P(x_l)|_p \leqslant \frac{1}{p^{n+1+l}} \tag{102}$$

et donc $P(\xi) = 0$.

Montrons maintenant l'unicité. Si ξ_1, ξ_2 sont deux racines de P qui vérifient les propriétés énoncées dans le théorème, alors par la formule de Taylor on a

$$P(\xi_2) = P(\xi_1) + P'(\xi_1)(\xi_2 - \xi_1) + (\xi_2 - \xi_1)^2 a \tag{103}$$

avec $a \in \mathbf{Z}_p$. Ce qui donne

$$(\xi_1 - \xi_2)\left(P'(x_1) + (\xi_1 - \xi_2)a\right) = 0. \tag{104}$$

Or

$$|\xi_1 - \xi_2| \leqslant \max\left(|\xi_1 - x|, |\xi_2 - x|\right) \leqslant \frac{1}{p^{n-k}} < \frac{1}{p^k}. \tag{105}$$

Donc le terme entre parenthèse dans (104) n'est pas nul ce qui impose $\xi_1 = \xi_2$. □

On réénonce la version du théorème de Hensel avec $n = 1$, car c'est celle plus utilisée en pratique.

THÉORÈME 3.4. *Soit $P \in \mathbf{Z}_p[X]$ un polynôme et $x \in \mathbf{Z}_p$ tel que*

$$P(x) = 0 \text{ mod } p \text{ et } P'(x) \neq 0 \text{ mod } p \tag{106}$$

alors il existe une unique racine $\xi \in \mathbf{Z}_p$ de P telle que

$$|x - \xi| \leqslant \frac{1}{p} \text{ et } P'(\xi) \neq 0 \text{ mod } p. \tag{107}$$

3.0.1. *Application aux racines de l'unité.* Soit p un nombre premier. Supposons que $\xi \in \mathbf{Q}_p$ soit une racine de l'unité. On a donc que $\xi^n = 1$ pour un certain entier n et alors $|\xi|^n = 1 \Rightarrow |\xi| = 1$ donc $\xi \in \mathbf{Z}_p^\times$. Ceci implique qu'on a une application de réduction modulo p bien définie

$$\mu(\mathbf{Q}_p) \to \mathbf{F}_p^\times. \tag{108}$$

Supposons p impair et prenons le polynôme $P = X^{p-1} - 1$. Pour tout $x \in \mathbf{Z}_p^\times$ on a que

$$P(x) = 0 \bmod p \tag{109}$$

et $P'(X) = (p-1)X^{p-2}$ donc $P'(x) \neq 0 \bmod p$. On peut donc appliquer le théorème de Hensel avec tout $x \in \mathbf{Z}_p^\times$. En particulier, en l'appliquant avec $1, \ldots, p-1$ on construit les $(p-1)$-racines de P. On a donc que

$$\mu_{p-1} \subset \mathbf{Z}_p^\times \subset \mathbf{Q}_p^\times. \tag{110}$$

Avec μ_{p-1} le groupe des racines $(p-1)$-ième de l'unité qui est un groupe cyclique de taille $p-1$.

PROPOSITION 3.5. *Soit p un nombre premier impair, alors le groupe $\mu(\mathbf{Q}_p)$ des racines de l'unité de $\mathbf{Q}_p$ est exactement μ_{p-1}.*

DÉMONSTRATION. On a l'application de réduction $\mu(\mathbf{Q}_p) \to \mathbf{F}_p^\times$. On a vu qu'elle était surjective par le théorème de Hensel. Montrons qu'elle est injective. Soit $\xi \in \mu(\mathbf{Q}_p)$ une racine de l'unité telle que $\xi = 1 \bmod p$. On écrit $\xi = (1 + pt)$ et on a qu'il existe $n \geqslant 2$ telle que

$$(1 + pt)^n = 1. \tag{111}$$

Ce qui donne

$$t\left(n + \binom{n}{2}pt + \binom{n}{3}p^2t^2 \cdots + p^{n-1}t^{p-1}\right) = 0. \tag{112}$$

Si $p \nmid n$, alors le terme entre parenthèse est $\neq 0$ et donc $t = 0$ et $\xi = 1$. Sinon, on a que n est divisible par p. On écrit donc $n = pn'$ et on a

$$\xi^n = (\xi^p)^{n'} = 1 \tag{113}$$

et $\xi^p = 1 \bmod p$. En réitérant on voit que si on écrit $n = p^k n'$ avec $p \nmid n'$, alors on a que

$$\xi^{p^k} = 1. \tag{114}$$

et $\xi = 1 \bmod p$. On montre que $\xi = 1$. On écrit $\xi = (1 + pt)$ et on a $(1 + pt)^{p^k} = 1$ ce qui donne

$$t\left(p + \binom{p^k}{2}pt + \cdots + p^{p^k}t^{p^k-1}\right) = 0. \tag{115}$$

Or le terme entre parenthèse est $\neq 0$ car les coefficients binomiaux sont tous divisibles par p donc le terme entre parenthèse est de la forme $p + up^2$ avec $u \in \mathbf{Z}_p$. Donc $t = 0$ et on a le résultat. $\square$

4. Analyse p-adique

On peut maintenant commencer à faire de l'analyse p-adique. Il faut d'abord définir la bonne notion de fonctions analytiques. En effet, la définition traditionnelle est la suivante : Une fonction analytique est une fonction localement développable en série entière avec un rayon de convergence strictement positif. Cette définition fonctionne bien sur $\mathbf{R}$ ou $\mathbf{C}$ car ce sont des espaces connexes. Mais sur $\mathbf{Q}_p$ cette définition ne va pas. En effet, prenons la fonction qui vaut zéro sur $\{|x| < 1\}$ et 1 sur $\{|x| \geqslant 1\}$. C'est une fonction localement constante, donc localement développable en série entière mais qui n'est pas constante. Or sur $\mathbf{C}$ ou $\mathbf{R}$ on sait qu'une fonction analytique localement constante doit être constante. On veut le même genre de résultats sur $\mathbf{Q}_p$. C'est à dire qu'on veut un *théorème des zéros isolés*.

4.1. L'algèbre de Tate. On définit *l'algèbre de Tate* à 1 variable sur $\mathbf{Q}_p$ comme l'ensemble des séries formelles à une variable

$$f = \sum_{i \geqslant 0} a_i t^i \tag{116}$$

avec $a_i \in \mathbf{Q}_p$ et $a_i \to 0$ pour $i \to +\infty$. On la note $\mathbf{Q}_p\langle t\rangle$. On la munit de la norme de Gauss :

$$||f|| := \max_i |a_i| \,. \tag{117}$$

On notera également $\mathbf{Z}_p\langle t\rangle \subset \mathbf{Q}_p\langle t\rangle$ le sous-ensemble composé des séries formelles à coefficients dans $\mathbf{Z}_p$. On a en particulier que

$$\mathbf{Z}_p\langle t\rangle = \{f \in \mathbf{Q}_p\langle x\rangle : ||f|| \leqslant 1\} \,. \tag{118}$$

LEMME 4.1. *Pour tout $f, g \in \mathbf{Q}_p\langle t\rangle$, on a*

$$||fg|| \leqslant ||f|| \cdot ||g|| \,. \tag{119}$$

DÉMONSTRATION. Si $f = \sum a_i t^i$ et $g = \sum b_i t^i$, alors

$$fg = \sum c_i t^i \tag{120}$$

avec

$$c_i = \sum_{k+l=i} a_k bl \tag{121}$$

et le lemme suit. □

On a également que $||f+g|| \leqslant \max(||f||, ||g||) \leqslant ||f|| + ||g||$. Ainsi, $\mathbf{Q}_p\langle x\rangle$ munit de la norme de Gauss est une algèbre de Banach grâce au lemme suivant.

LEMME 4.2. *L'algèbre $\mathbf{Q}_p\langle x\rangle$ muni de la norme de Gauss est complète.*

DÉMONSTRATION. Soit (f_i) une suite de Cauchy dans $\mathbf{Q}_p\langle x\rangle$. On écrit

$$f_i = \sum_j a_{i,j} t^j. \tag{122}$$

Montrer que pour tout j, la suite $(a_{i,j})_i$ est de Cauchy. En effet, on a

$$\left|a_{i,j} - a_{i',j}\right| \leqslant |f_i - f_{i'}|. \tag{123}$$

C'est donc une suite de Cauchy. On note $a_j = \lim_i a_{i,j}$ et $f = \sum_j a_j t$. Montrons que $f \in \mathbf{Q}_p\langle x\rangle$. Il faut montrer que $a_j \to 0$ quand $j \to +\infty$. Soit $\varepsilon > 0$. Il existe i_0, tel que pour tout $i, i' \geqslant i_0, ||f_i - f_{i'}|| \leqslant \varepsilon$. Maintenant, il existe j_0 tel que pour tout $j \geqslant j_0$, on a $|a_{i_0,j}| \leqslant \varepsilon$. Ce qui implique que

$$\forall i \geqslant i_0, \forall j \geqslant j_0, \left|a_{i,j}\right| \leqslant \max\left(|a_{i_0,j_0}|, \left|a_{i,j} - a_{i_0,j_0}\right|\right) \leqslant \varepsilon. \tag{124}$$

En effet, la dernière inégalité vient du fait que $\left|a_{i,j} - a_{i_0,j_0}\right| \leqslant ||f_i - f_{i_0}|| \leqslant \varepsilon$.

Maintenant, comme la suite (f_i) est de Cauchy on a

$$\forall j, \forall i, i' \geqslant i_0, \left|a_{i,j} - a_{i',j}\right| \leqslant \varepsilon. \tag{125}$$

En faisant tendre $i' \to +\infty$ on a que

$$\forall j \geqslant 0, \forall i \geqslant i_0, \left|a_j - a_{i,j}\right| \leqslant \varepsilon. \tag{126}$$

Cela implique que pour tout $i \geqslant i_0, ||f - f_i|| \leqslant \varepsilon$ et donc que (f_i) converge vers f. □

Pour tout $f \in \mathbf{Q}_p\langle x\rangle$, on a que $f = \sum_i a_i t^i$ définit une fonction

$$f : \mathbf{Z}_p \to \mathbf{Q}_p. \tag{127}$$

En effet, si $z \in \mathbf{Z}_p$, alors $|z| \leqslant 1$ et alors

$$a_i |z|^i \xrightarrow[i \to +\infty]{} 0. \tag{128}$$

On dira qu'une fonction $f : \mathbf{Z}_p \to \mathbf{Q}_p$ est *analytique* si elle est donnée par un élément de $\mathbf{Q}_p\langle x\rangle$.

REMARQUE 4.3. Attention, il est vrai que si $f \in \mathbf{Z}_p\langle x\rangle$, alors $f(\mathbf{Z}_p) \subset \mathbf{Z}_p$ mais la réciproque n'est pas vrai. Prenez par exemple

$$f(t) = \frac{t^p - t}{p}. \tag{129}$$

On a que $f(\mathbf{Z}_p) = \mathbf{Z}_p$ car dans $\mathbf{Z}/p\mathbf{Z}, x^p = x$.

PROPOSITION 4.4. *Soit $f \in \mathbf{Z}_p\langle x\rangle$ et $a \in \mathbf{Z}_p$, alors il existe $g \in \mathbf{Z}_p\langle x\rangle$ tel que*

$$f = f(a) + (t - a)g. \tag{130}$$

Si de plus on définit $N(f)$ par

$$N(f) := \max\{n \geqslant 0 : |a_n| = ||f||\}, \tag{131}$$

alors

$$N(g) \leqslant N(f) - 1. \tag{132}$$

dès lors que $N(f) \geqslant 1$.

DÉMONSTRATION. On a

$$f(t) - f(a) = \sum_{i \geqslant 0} a_i(t^i - a^i) = \sum_{i \geqslant 0} a_i(t-a)\left(t^{i-1} - t^{i-2}a + \cdots + (-1)^{i-1}a^{i-1}\right). \tag{133}$$

Cette somme est égale à

$$(t-a)\sum_{i \geqslant 0} b_i t^i \tag{134}$$

avec

$$b_i = \sum_{k \geqslant 1} a_{i+k}(-a)^{i+k-1}. \tag{135}$$

et on a que $b_i \in \mathbf{Z}_p$ et que

$$|b_i| \leqslant \max_{j \geqslant i+1} |a_i|. \tag{136}$$

Si $N(f) \geqslant 1$, alors cela implique que $||g|| = ||f||$ et que $N(g) \leqslant N(f) - 1$. □

On va retrouver maintenant un des résultats classiques d'analyse complexe. Le principe des zéros isolés.

THÉORÈME 4.5 (Strassman, principe des zéros isolés). *Soit* $f \in \mathbf{Q}_p\langle x \rangle \setminus \{0\}$. *On définit* $N(f) = \max(i \geqslant 0 : |a_i| = ||f||)$, *alors* f *a au plus* $N(f)$ *zéros dans* $\mathbf{Z}_p$ *(comptés avec multiplicités).*

DÉMONSTRATION. On montre le résultat par récurrence sur $N(f)$. On peut supposer que $||f|| = 1$ quitte à multiplier f par la bonne puissance de p. Cela ne change pas la valeur de $N(f)$. Si $N(f) = 0$, alors

$$f(t) = a_0 + pg(t) \tag{137}$$

avec $|a_0| = 1$ et $g \in \mathbf{Z}_p\langle x \rangle$. Ainsi, pour tout $z \in \mathbf{Z}_p$, on a que

$$|f(z)| = |a_0| = 1 \tag{138}$$

et donc f n'a pas de zéros dans $\mathbf{Z}_p$. Supposons le résultat vrai pour $N(f) = k$ avec $k \geqslant 0$ et prenons $f \in \mathbf{Z}_p\langle x \rangle$ tel que $N(f) = k+1$. On suppose toujours que $||f|| = 1$. Si f n'a pas de zéros dans $\mathbf{Z}_p$, alors il n'y a rien à démontrer. Soit z_0 un zéro de f dans $\mathbf{Z}_p$. On a par la proposition 4.4 que

$$f(t) = (t - z_0)g(t). \tag{139}$$

avec $N(g) \leqslant N(f) - 1$. Par hypothèse de récurrence, g a au plus $N(g)$ zéros dans $\mathbf{Z}_p$ et f a donc au plus $N(f)$ zéros dans $\mathbf{Z}_p$. □

COROLLAIRE 4.6. *Soit* $f, g \in \mathbf{Q}_p\langle x \rangle$. *On a que si les fonctions induites par* f *et* g *sont égales, alors* $f = g$ *dans* $\mathbf{Q}_p\langle x \rangle$.

4.2. À plusieurs variables. Sur $\mathbf{Q}_p^d$ on définit la norme par

$$||(x_1,\dots,x_d)|| = \max\left(|x_i|\right). \tag{140}$$

On a en particulier que $\mathbf{Z}_p^d$ est la boule unité sur $\mathbf{Q}_p^d$ et $\mathbf{Q}_p^d$ est également complet pour cette norme.

Soient $x_1,\dots,x_n$ des variables. On note $\mathbf{x}$ l'ensemble de ces variables et on définit la notation suivante : si $I=(i_1,\dots,i_n)$ est un n-uplet d'entiers alors on pose

$$\mathbf{x}^I = x_1^{i_1}\cdots x_n^{i_n}. \tag{141}$$

On note $|I| = \max i_j$ et on définit l'algèbre de Tate à n variables $\mathbf{Q}_p\langle x_1,\dots,x_n\rangle =: \mathbf{Q}_p\langle \mathbf{x}\rangle$ comme l'ensemble des séries formelles

$$f = \sum_I a_I \mathbf{x}^I \tag{142}$$

où $a_I \in \mathbf{Q}_p$ et $a_I \to 0$ lorsque $|I| \to +\infty$. On définit de même l'ensemble $\mathbf{Z}_p\langle x\rangle$. On la munit également de la norme de Gausse donné par

$$||f|| = \max_I |a_I|. \tag{143}$$

EXERCICE 4.7. Montrer que $\mathbf{Q}_p\langle \mathbf{x}\rangle$ est une algèbre de Banach. C'est à dire qu'elle est complète et que

$$||f+g|| \leqslant \max\left(||f||,||g||\right) \text{ et } ||fg|| \leqslant ||f||\,||g||. \tag{144}$$

DÉFINITION 4.8. Une fonction $\mathbf{Z}_p^d \to \mathbf{Q}_p$ est *analytique* si elle est donnée par un élément de $\mathbf{Q}_p\langle \mathbf{x}\rangle$. Une fonction $\mathbf{Z}_p^d \to \mathbf{Q}_p^m$ est *analytique* si chaque projection sur les coordonnées est analytique.

PROPOSITION 4.9. *Soit $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle$, alors pour tout $z \in \mathbf{Z}_p^d$ on a*

$$|f(z)| \leqslant ||f||\,||z||. \tag{145}$$

En particulier, $f : \mathbf{Z}_p^d \to \mathbf{Q}_p$ est $||f||$-Lipschitz.

PROPOSITION 4.10. *Soit $g \in \mathbf{Q}_p\langle x\rangle$ et $f=(f_1,\dots,f_d) \in \mathbf{Z}_p\langle \mathbf{x}\rangle$, alors*

$$g\circ f = g(f_1(\mathbf{x}),\dots,f_d(\mathbf{x})) \in \mathbf{Q}_p\langle \mathbf{x}\rangle. \tag{146}$$

DÉMONSTRATION. On écrit $g=\sum_I a_I\mathbf{x}^I$, alors on a formellement

$$g(f_1,\dots,f_r) = \sum_I a_I f_1^{i_1}\cdots f_d^{i_d}. \tag{147}$$

On pose $h_k = \sum_{|I|\leqslant k} a_I f_1^{i_1}\cdots f_d^{i_d}$. C'est un élément de $\mathbf{Q}_p\langle \mathbf{x}\rangle$ car c'est un polynôme en les $f_1,\dots,f_d$ et $\mathbf{Q}_p\langle \mathbf{x}\rangle$ est une algèbre de Banach. Comme l'algèbre est complète il suffit de montrer que h_k est

une suite de Cauchy. Or, pour tout $m \geqslant n$, on a

$$||h_m - h_n|| = \left|\left| \sum_{n+1 \leqslant |I| \leqslant m} a_I f_1^{i_1} \cdots f_d^{i_d} \right|\right| \leqslant \max_{|I| \geqslant n+1} |a_I| . \tag{148}$$

La dernière inégalité vient de l'exercice 4.7 et du fait que pour tout $j = 1, \ldots, d, \left|f_j\right| \leqslant 1$. Comme $\max_{|I| \geqslant n+1} \to 0$ quand $n \to +\infty$, c'est bien une suite de Cauchy. □

EXERCICE 4.11. Montrer que la proposition est fausse si par exemple f est la translation par un élément de norme > 1.

EXERCICE 4.12. Montrer que si $z_1, \ldots, z_r \in \mathbf{Z}_p$ avec $r \leqslant d$, alors on a une application d'évaluation $\mathbf{Q}_p\langle x_1, \ldots, x_d\rangle \to \mathbf{Q}_p\langle x_{r+1}, \cdots, x_d\rangle$ donnée par

$$f(z_1, \ldots, z_r, x_{r+1}, \ldots, x_d) = \sum_I a_I z_1^{i_1} \cdots z_r^{i_r} x_{r+1}^{i_{r+1}} \cdots x_d^{i_d}. \tag{149}$$

Montrer également qu'on peut écrire

$$f = \sum_{k \geqslant 0} f_k(x_1, \ldots, x_{d-1}) x_d^k \tag{150}$$

avec $f_k \in \mathbf{Q}_p\langle x_1, \ldots, x_{d-1}\rangle$.

PROPOSITION 4.13. *Si $f : \mathbf{Z}_p^d \to \mathbf{Q}_p$ est analytique et nulle sur un ouvert, alors $f = 0$. En particulier, si deux éléments $f, g \in \mathbf{Q}_p\langle \mathbf{x}\rangle$ induisent la même fonction sur $\mathbf{Z}_p^d$, alors $f = g$.*

DÉMONSTRATION. Soit $f \in \mathbf{Q}_p\langle \mathbf{x}\rangle$. On montre le résultat par récurrence. Soit U un ouvert sur lequel f s'annule. Soit $d = 1$, on peut supposer quitte à translater que $0 \in U$ par la proposition 4.10. On a alors que $f(t) = 0$ pour tout t de valeur absolue assez petite et par le théorème 4.5 on a que $f = 0$. Maintenant supposons $d \geqslant 2$ et que le résultat soit vrai pour $d - 1$, alors on écrit

$$f = \sum_{k \geqslant 0} f_k(x_1, \ldots, x_{d-1}) x_d^k. \tag{151}$$

On peut supposer quitte à translater que $(0, \ldots, 0) \in U$. Il existe donc $\varepsilon > 0$ tel que que $f(z_1, \ldots, z_d) = 0$ pour tout $z_i \in \mathbf{Z}_p$ tel que $|z_i| \leqslant \varepsilon$. Prenons $z_1, \ldots, z_{d-1} \in \mathbf{Z}_p$ de valeur absolue $\leqslant \varepsilon$. On a

$$f(z_1, \ldots, z_{d-1}, x_d) = \sum_{k \geqslant 0} f_k(z_1, \ldots, z_{d-1}) x_d^k \in \mathbf{Q}_p\langle x_d\rangle. \tag{152}$$

Cette fonction analytique va de $\mathbf{Z}_p$ dans $\mathbf{Z}_p$ et est nulle sur le disque $\overline{\mathbb{D}}(0, \varepsilon)$. Par Strassman on a que pour tout $k \geqslant 0, f_k(z_1, \ldots, z_{d-1}) = 0$. On a donc que pour tout $k \geqslant 0$, la fonction analytique $f_k : \mathbf{Z}_p^{k-1} \to \mathbf{Z}_p$ est nulle sur le polydisque $\overline{D}(0, \varepsilon)^{d-1}$. Par hypothèse de récurrence on a que pour tout $k \geqslant 0, f_k = 0$ et donc $f = 0$.

La deuxième assertion de la proposition vient du fait que $f - g$ induit la fonction nulle sur $\mathbf{Z}_p^d$. □

4.3. Difféomorphismes analytiques. Par la proposition 4.10 on a une application de composition bien définie

$$\mathbf{Z}_p\langle x_1,\dots,x_n\rangle^m \times \mathbf{Z}_p\langle y_1,\dots,y_m\rangle^l \to \mathbf{Z}_p\langle x_1,\dots,x_n\rangle^l. \tag{153}$$

En prenant $n = m = l$ on obtient un monoide pour la loi de composition. Un *difféomorphisme analytique* est un élément inversible dans ce monoide. C'est à dire que $f : \mathbf{Z}_p^d \to \mathbf{Z}_p^d$ est un difféomorphisme analytique si $f \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$ et il existe $g \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$ tel que $f \circ g = g \circ f = \mathrm{id}$. On note $\mathrm{Diff}^{\mathrm{an}}(\mathbf{Z}_p^d)$ l'ensemble des difféomorphismes analytiques de $\mathbf{Z}_p^d$.

PROPOSITION 4.14. *Soient $f, g, h \in \mathbf{Z}_p\langle x\rangle^d$, alors*

(1) $||g \circ f|| \leqslant ||g||$.

(2) Si $f \in \mathrm{Diff}^{\mathrm{an}}(\mathbf{Z}_p^d)$, alors $||g \circ f|| = ||g||$.

(3) $||g \circ (\mathrm{id} + h) - g|| \leqslant ||h||$.

(4) $\left|\left|f^{-1} - \mathrm{id}\right|\right| = ||f - \mathrm{id}||$ *si* $f \in \mathrm{Diff}^{\mathrm{an}}(\mathbf{Z}_p^d)$.

DÉMONSTRATION. On a que si $g \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$, alors $\frac{g}{||g||} \in \mathbf{Z}_p\langle \mathbf{x}\rangle^d$ et donc

$$\left|\left|\frac{g}{||g||} \circ f\right|\right| \leqslant 1. \tag{154}$$

On a donc la première assertion. La deuxième assertion vient du fait que $g = g \circ f \circ f^{-1}$. Pour l'assertion (3), on écrit $h = (h_1, \dots, h_d)$ avec $||h_i|| \leqslant ||h||$ et on a

$$g \circ (\mathrm{id} + h) = g + A_1(h) \sum_{k \geqslant 2} A_k(h) \tag{155}$$

où A_k est un polynôme homogène de degré k à d variables à coefficients dans $\mathbf{Z}_p$. D'où

$$||g \circ (\mathrm{id} + h) - g|| \leqslant ||h||. \tag{156}$$

Enfin pour la dernière assertion on a par (2) que $\left|\left|f^{-1} - \mathrm{id}\right|\right| = ||\mathrm{id} - f||$. □

Soit $c > 0$, on définit

$$\mathrm{Diff}_c^{\mathrm{an}}(\mathbf{Z}_p^d) = \left\{ f \in \mathrm{Diff}^{\mathrm{an}}(\mathbf{Z}_p^d) : ||f - \mathrm{id}|| \leqslant \frac{1}{p^c} \right\}. \tag{157}$$

PROPOSITION 4.15. *Pour tout $c > 0$, on a que $\mathrm{Diff}_c^{\mathrm{an}}(\mathbf{Z}_p^d)$ est un sous-groupe distingué de $\mathrm{Diff}^{\mathrm{an}}(\mathbf{Z}_p^d)$.*

DÉMONSTRATION. Cela découle de la proposition 4.14. □

Bibliographie

[BGT08] Jason Bell, Dragos Ghioca, and Thomas Tucker. The dynamical Mordell-Lang problem for etale maps. *American Journal of Mathematics*, 132, September 2008.

[Lec53] Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2(5) :417–421, August 1953.

[Rob00] Alain M. Robert. *A Course in P-Adic Analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2000.