

# **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 pourrions 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

$$\{ak + b : k \geq 0\} \quad (1)$$

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*

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

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

$$\{n \geq 0 : u_n = 0\} \quad (3)$$

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

Ce théorème fut d'abord démontré par Skolem pour une suite récurrente linéaire sur  $\mathbf{Q}$  en utilisant les nombres  $p$ -adiques. Il fut ensuite généralisé 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

$$f = (f_1, \dots, f_n) : \mathbf{C}^n \rightarrow \mathbf{C}^n \quad (4)$$

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

**EXEMPLE 1.2.** Toute 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  $n \geq 2$ . En effet, regardons par exemple

$$z_1, \dots, z_n \mapsto (z_1 + P(z_2, \dots, z_n), z_2, \dots, z_n) \quad (5)$$

avec  $P(z_2, \dots, z_n) \in \mathbf{C}[z_2, \dots, z_n]$ . 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  $P_1, \dots, P_r \in \mathbf{C}[z_1, \dots, z_n]$  tels que

$$V = \{(z_1, \dots, z_n) \in \mathbf{C}^n : P_1(z_1, \dots, z_n) = \dots = P_r(z_1, \dots, z_n) = 0\}. \quad (6)$$

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

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

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

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

$$\forall n \geq 0, \begin{pmatrix} u_n \\ \vdots \\ u_{n+d-1} \end{pmatrix} = A^n \begin{pmatrix} u_0 \\ \vdots \\ u_{d-1} \end{pmatrix} \quad (8)$$

où

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

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

$$V = \{z_1 = 0\}. \quad (10)$$

## 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

$$x = p^\alpha m' \quad (11)$$

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

$$v_p(x) = \alpha. \quad (12)$$

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

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

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

Ce résultat permet d'interpréter la valuation  $p$ -adique de la façon 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'il existe une unique écriture de  $x \in \mathbf{Q}$  de la forme

$$p^{\alpha} \frac{a}{b} \quad (14)$$

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

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

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

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

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

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

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

Comme  $\beta - \alpha \geq 0$ , 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  $v_p(x+y) \geq \alpha = \min(\alpha, \beta)$ .  $\square$

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

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

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)  $\forall x, y \in \mathbf{Q}, |x+y|_p \leq \max(|x|_p, |y|_p)$ .

EXERCICE 2.6. On définit la fonction suivante :

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

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

$$\forall x, y, z \in \mathbf{Q}, d_p(x, z) \leq \max(d_p(x, y), d_p(y, z)). \quad (20)$$

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

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

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

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

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

$$|x_{n+1} - x_n|_p \leq \frac{1}{p^{n+1}} < \frac{1}{p^n}. \quad (23)$$

Par un argument télescopique on obtient que

$$\forall m \geq n, |x_m - x_n|_p \frac{1}{p^{n+1}} < \frac{1}{p^n}. \quad (24)$$

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

$$x^p = x \quad (25)$$

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

$$|x - a|_p < 1. \quad (26)$$

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 respectivement) des racines de polynômes irréductibles sur  $\mathbf{Q}$  ce qui prouve que  $\mathbf{Q} \neq \mathbf{Q}_2, \mathbf{Q}_3$   $\square$

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

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

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

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

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

$$x_m y_m - x_n y_n = x_m (y_m - y_n) + y_n (x_m - x_n). \quad (29)$$

De sorte que

$$|x_m y_m - x_n y_n| \leq \max \left( \max(|x_k|_p) |y_m - y_n|, \max(|y_l|_p) |x_m - x_n| \right). \quad (30)$$

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

$$|(x_n + y_n) - (x'_n + y'_n)| \leq \max \left( |x_n - x'_n|_p, |y_n - y'_n|_p \right). \quad (31)$$

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

Pour le produit on a

$$x_n y_n - x'_n y'_n = x_n (y_n - y'_n) + y_n (x'_n - x_n). \quad (32)$$

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  $x$ . Montrons d'abord qu'elle est de Cauchy. On a

$$\frac{1}{x_m} - \frac{1}{x_n} = \frac{x_n - x_m}{x_n x_m}. \quad (33)$$

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

$$1 = \lim x_n y_n = xy. \quad (34)$$

D'où  $y = \frac{1}{x}$ .  $\square$

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

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

*de multiplication*

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

*et d'inversion*

$$\text{inv} : x \in \mathbf{Q}_p^\times \mapsto \frac{1}{x} \in \mathbf{Q}_p. \quad (37)$$

*sont continues.*

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

$$\sum u_n \quad (38)$$

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

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  $\forall n \geq n_0, |u_n| < \varepsilon$ . Maintenant, on a pour tout  $m \geq n \geq n_0$

$$|S_m - S_n| = \left| \sum_{k=n+1}^m u_k \right| \leq \varepsilon \quad (39)$$

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.  $\square$

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

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

$$|x + y| = |y|. \quad (40)$$

DÉMONSTRATION. On a que

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

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

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

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

*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  $\log |\mathbf{Q}^\times| = \mathbf{Z} \cdot \log p$ . Comme  $\mathbf{Q}$  est dense dans  $\mathbf{Q}_p$  cela donne le résultat.  $\square$

PROPOSITION 2.17. *On a les propriétés suivantes.*

- (1)  $\mathbf{Z}_p$  est l'adhérence de  $\mathbf{Z}$  dans  $\mathbf{Q}_p$ .
- (2)  $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x| \leq 1\}$ .
- (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  $|x| \leq 1$ . Par la proposition 2.16, cela implique qu'il existe une suite de rationnels  $x_n$  avec  $|x_n| \leq 1$  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

$$x_n = \frac{a_n}{b_n}. \quad (43)$$

Le fait que  $|x_n| \leq 1$  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  $k \geq 1$ , 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

$$um + p^k v = 1. \quad (44)$$

On a alors

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

Et

$$\left| p^k \frac{v}{m} \right| \leq p^{-k} \quad (46)$$

car  $|m| = 1$  et le résultat est démontré. Les assertions (3) et (4) viennent du fait que si  $x \neq 0$ ,  $|\frac{1}{x}| = \frac{1}{|x|}$ . 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  $k \geq 1$  tel que  $|x| = \frac{1}{p^k}$ . Et alors

$$x = p \cdot \frac{1}{p} x \quad (47)$$

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

$$z^N + a_{N-1}z^{N-1} + \cdots + a_1z + a_0 = 0 \quad (48)$$

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

$$z^N = - \sum_{k \leq N-1} a_k z^k \quad (49)$$

et donc

$$|z|^N \leq \max(|a_k| |z|^k). \quad (50)$$

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

$$|z|^N > |z^k| > |a_k| |z^k|. \quad (51)$$

Ce qui est une contradiction.  $\square$

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

$$p^k \mathbf{Z}_p = \left\{ x \in \mathbf{Q}_p : |x| \leq \frac{1}{p^k} \right\} \quad (52)$$

et

$$\mathbf{Z}_p / p^k \mathbf{Z}_p = \mathbf{Z} / p^k \mathbf{Z}. \quad (53)$$

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  $k \geq 1$  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  $v_p(i) \geq k$ , donc  $i/p^k \in \mathbf{Z}_p$  et  $i \in p^k \mathbf{Z}_p$ . Construisons l'application quotient  $\mathbf{Z}_p \rightarrow \mathbf{Z} / p^k \mathbf{Z}$ .

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

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

*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  $x_n = y_n \bmod p^k$ .  $\square$

Ce lemme permet de construire le morphisme d'anneaux

$$\phi_k : \mathbf{Z}_p \rightarrow \mathbf{Z} / p^k \mathbf{Z} \quad (55)$$

par

$$\phi_k(x) = \lim_n x_n \bmod p^k \quad (56)$$

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

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

□

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

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

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

$$x = p^k u \quad (59)$$

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  $x \in \mathbf{Q}_p, r \geq 0$ ,

$$\mathbb{D}(x, r) = \{z \in \mathbf{Q}_p : |x - z|_p < r\}, \overline{\mathbb{D}}(x, r) = \{z \in \mathbf{Q}_p : |x - z|_p \leq r\} \quad (60)$$

and

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

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

DÉMONSTRATION. Il est clair que  $\mathbb{D}(x, r)$  est ouvert et que  $\overline{\mathbb{D}}(x, r)$  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  $\overline{\mathbb{D}}(x, r)$  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  $k \geq 1$  et  $x, y \in \mathbf{Z}_p$ , on a que

$$y \in \overline{D}(x, p^{-k}) \Leftrightarrow |x - y| \leq \frac{1}{p^k} \Leftrightarrow p^k |x - y| \Leftrightarrow x = y \pmod{p^k}. \quad (62)$$

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

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

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  $0, \dots, p^{k+1}$ . Pour savoir dans quel disque de rayon  $\frac{1}{p^k}$  ils sont contenus, il suffit de regarder la congruence modulo  $p^k$ . On a

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

On peut faire le dessin suivant où en bleu on a les  $p$  disques de rayons  $1/p$  indexés par  $0, \dots, p-1$  et dans le disque  $\overline{D}(0, \frac{1}{p})$  on a dessiné en rouge les  $p$  disques de rayons  $\frac{1}{p^2}$  indexés par  $0, p, 2p, \dots, (p-1)p$ . 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  $u \in \{0, \dots, p^k - 1\}$ , alors les  $p$  disques de rayons  $\frac{1}{p^{k+1}}$  contenus dans  $D$  sont

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

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

$$x_1 = x \bmod p. \quad (66)$$

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

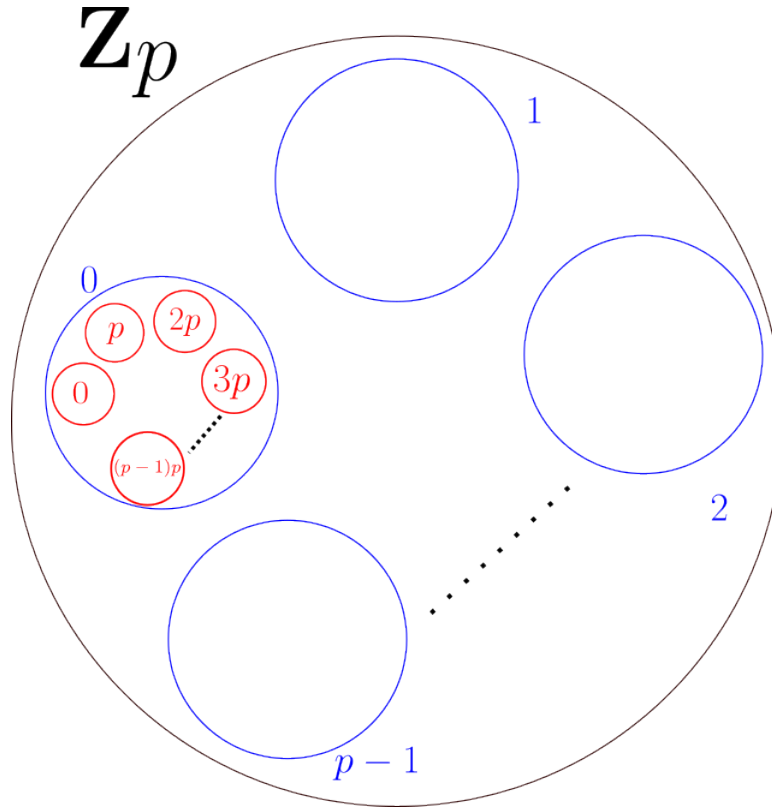
$$x \in D_{u_k, x_{k+1}} = \overline{D}(x_{k+1} \cdot p^k + u_k, \frac{1}{p^{k+1}}). \quad (67)$$

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

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

**EXERCICE 2.23.** Montrer que la topologie induite par cette distance est la topologie produit sur  $0, \dots, p-1$ .

**PROPOSITION 2.24.** L'application  $\phi : \mathbf{Z}_p \rightarrow \{0, \dots, p-1\}^{\mathbf{N}}$  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  $n \geq 0$

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

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

$$|u_m - u_n| \leq \frac{1}{p^{n+1}}. \quad (70)$$

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

$$|x - y| = \frac{1}{p^k} \quad (71)$$

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

$$\forall \ell = 1, \dots, k, x_\ell = y_\ell. \quad (72)$$

□

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

**COROLLAIRE 2.25.** *L'espace  $\mathbf{Z}_p$  est un Cantor : il est totalement 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

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

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  $m \geq n$  on a l'homomorphisme d'anneaux canonique

$$\pi_{m,n} : \mathbf{Z}/p^m\mathbf{Z} \rightarrow \mathbf{Z}/p^n\mathbf{Z}. \quad (74)$$

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

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

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

$$W = \varprojlim_{i \rightarrow +\infty} \mathbf{Z}/p^i\mathbf{Z}. \quad (76)$$

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  $m \geq n' \geq n$ , alors

$$\pi_{m,n} = \pi_{n',n} \circ \pi_{m,n'}. \quad (77)$$

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

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

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

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

*Alors  $\psi$  est un homéomorphisme.*

DÉMONSTRATION. Montrons que  $\psi$  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  $m \geq n$ , on a par construction que

$$z_m = z_n \bmod p^n \quad (80)$$

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

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

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

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

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  $z \in \overline{\mathbb{D}}(x_n, \frac{1}{p^n})$ .  $\square$

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

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  $\phi : \mathbf{N} \rightarrow \mathbf{N}$  strictement croissante telle que

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

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

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

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  $\Lambda_k$  défini par

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

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  $z_{\phi(n+1)} = z_{\phi(n)} \pmod{p^n}$ .

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  $m \geq n$ ,  $z_{\phi(m)} = z_{\phi(n)} \pmod{p^n}$  et donc

$$|z_{\phi(m)} - z_{\phi(n)}|_p \leq \frac{1}{p^n}. \quad (86)$$

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  $P \in \mathbf{Z}_p[X_1, \dots, X_n]$  un polynôme à  $n$  variables, alors les assertions suivantes sont équivalentes.*

- (1)  $P = 0$  admet une solution dans  $\mathbf{Z}_p^n$ .
- (2) pour tout  $k \geq 1$ ,  $P = 0$  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  $\mathbf{R}$ . Soit  $f : \mathbf{R} \rightarrow \mathbf{R}$  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

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

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

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

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

$$|N_f(x) - a| \leq \frac{2M_2}{m_1} |x - a|^2. \quad (89)$$

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

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

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

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

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  $P(x) = 0 \pmod{p^n}$  (donc  $x$  n'est pas trop loin d'une racine de  $P$ ). Si  $k = v(P'(x)) < n/2$ , alors si  $\hat{x} = N_p(x) = x - \frac{P(x)}{P'(x)}$ , alors*

- (1)  $P(\hat{x}) = 0 \pmod{p^{n+1}}$  (on a une meilleure approximation de la racine).
- (2)  $\hat{x} = x \pmod{p^{n-k}}$  ( $\hat{x}$  n'est pas trop loin de  $x$ ).
- (3)  $v(P'(\hat{x})) = v(P'(x)) (= k)$  (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

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

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

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

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

$$|P(\hat{x})| \leq \frac{1}{p^{n+1}}. \quad (94)$$

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

$$P'(\hat{x}) = P'(x + (\hat{x} - x)) = P'(x) + (\hat{x} - x) \cdot s \quad (95)$$

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

$$|P'(\hat{x})| = |P'(x)| = p^{-k}. \quad (96)$$

□

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*

$$P(x) = 0 \pmod{p^n}. \quad (97)$$

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

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

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

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

On voit donc par récurrence avec la proposition 3.2 que

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

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

$$|x_m - x_l| \leq \frac{1}{p^{n+l-k}} \quad (101)$$

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

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

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

Montrons maintenant l'unicité. Si  $\xi_1, \xi_2$  sont deux racines de  $P$  qui vérifient les propriétés énoncées dans le théorème, alors par la formule de Taylor on a

$$P(\xi_2) = P(\xi_1) + P'(\xi_1)(\xi_2 - \xi_1) + (\xi_2 - \xi_1)^2 a \quad (103)$$

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

$$(\xi_1 - \xi_2) (P'(\xi_1) + (\xi_1 - \xi_2)a) = 0. \quad (104)$$

Or

$$|\xi_1 - \xi_2| \leq \max(|\xi_1 - x|, |\xi_2 - x|) \leq \frac{1}{p^{n-k}} < \frac{1}{p^k}. \quad (105)$$

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

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

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

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

$$|x - \xi| \leq \frac{1}{p} \text{ et } P'(\xi) \neq 0 \bmod p. \quad (107)$$

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

$$\mu(\mathbf{Q}_p) \rightarrow \mathbf{F}_p^\times. \quad (108)$$

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

$$P(x) = 0 \pmod{p} \quad (109)$$

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

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

Avec  $\mu_{p-1}$  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  $\mu_{p-1}$ .*

**DÉMONSTRATION.** On a l'application de réduction  $\mu(\mathbf{Q}_p) \rightarrow \mathbf{F}_p^\times$ . 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  $\xi \equiv 1 \pmod{p}$ . On écrit  $\xi = (1 + pt)$  et on a qu'il existe  $n \geq 2$  telle que

$$(1 + pt)^n = 1. \quad (111)$$

Ce qui donne

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

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

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

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

$$\xi^{p^k} = 1. \quad (114)$$

et  $\xi = 1 \pmod{p}$ . On montre que  $\xi = 1$ . Cela découle du lemme suivant.

**LEMME 3.6.** *Si  $\omega \in \mathbf{Z}_p^\times$  est tel que  $\omega^p = 1$  et  $\omega \equiv 1 \pmod{p}$ , alors  $\omega = 1$ .*

**DÉMONSTRATION.** On écrit  $\omega = (1 + pt)$  et on a  $(1 + pt)^p = 1$  ce qui donne

$$t \left( p + \binom{p}{2} pt + \dots + p^{p-1} t^{p-1} \right). \quad (115)$$

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

On montre que cela conclut. On a  $\xi^{p^k} = 1$  et  $\xi = 1 \pmod{p}$ . Si  $k = 0$  ou  $k = 1$  on a bien  $\xi = 1$  par le lemme 3.6. Ensuite si le résultat est vrai pour  $k - 1$  avec  $k \geq 2$ , on a

$$\xi^{p^k} = 1 \Rightarrow (\xi^{p^{k-1}})^p = 1. \quad (116)$$

Par le lemme 3.6 on a que  $\xi^{p^{k-1}} = 1$  et par récurrence cela implique que  $\xi = 1$ .  $\square$

#### 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  $\{|x| \geq 1\}$ . 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

$$f = \sum_{i \geq 0} a_i t^i \quad (117)$$

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

$$\|f\| := \max_i |a_i|. \quad (118)$$

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

$$\mathbf{Z}_p\langle t \rangle = \{f \in \mathbf{Q}_p\langle t \rangle : \|f\| \leq 1\}. \quad (119)$$

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

$$\|fg\| \leq \|f\| \cdot \|g\|. \quad (120)$$

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

$$fg = \sum c_i t^i \quad (121)$$

avec

$$c_i = \sum_{k+l=i} a_k b_l \quad (122)$$

et le lemme suit.  $\square$

On a également que  $\|f + g\| \leq \max(\|f\|, \|g\|) \leq \|f\| + \|g\|$ . 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

$$f_i = \sum_j a_{i,j} t^j. \quad (123)$$

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

$$|a_{i,j} - a_{i',j}| \leq \|f_i - f_{i'}\|. \quad (124)$$

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

$$\forall i \geq i_0, \forall j \geq j_0, |a_{i,j}| \leq \max(|a_{i_0,j}|, |a_{i,j} - a_{i_0,j}|) \leq \varepsilon. \quad (125)$$

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

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

$$\forall j, \forall i, i' \geq i_0, |a_{i,j} - a_{i',j}| \leq \varepsilon. \quad (126)$$

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

$$\forall j \geq 0, \forall i \geq i_0, |a_j - a_{i,j}| \leq \varepsilon. \quad (127)$$

Cela implique que pour tout  $i \geq i_0$ ,  $\|f - f_i\| \leq \varepsilon$  et donc que  $(f_i)$  converge vers  $f$ .  $\square$

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

$$f : \mathbf{Z}_p \rightarrow \mathbf{Q}_p. \quad (128)$$

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

$$a_i |z|^i \xrightarrow{i \rightarrow +\infty} 0. \quad (129)$$

On dira qu'une fonction  $f : \mathbf{Z}_p \rightarrow \mathbf{Q}_p$  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

$$f(t) = \frac{t^p - t}{p}. \quad (130)$$

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

$$f = f(a) + (t - a)g. \quad (131)$$

Si de plus on définit  $N(f)$  par

$$N(f) := \max \{n \geq 0 : |a_n| = \|f\|\}, \quad (132)$$

alors

$$N(g) \leq N(f) - 1. \quad (133)$$

dès lors que  $N(f) \geq 1$ .

DÉMONSTRATION. On a

$$f(t) - f(a) = \sum_{i \geq 0} a_i(t^i - a^i) = \sum_{i \geq 0} a_i(t - a)(t^{i-1} - t^{i-2}a + \dots + (-1)^{i-1}a^{i-1}). \quad (134)$$

Cette somme est égale à

$$(t - a) \sum_{i \geq 0} b_i t^i \quad (135)$$

avec

$$b_i = \sum_{k \geq 1} a_{i+k} (-a)^{i+k-1}. \quad (136)$$

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

$$|b_i| \leq \max_{j \geq i+1} |a_j|. \quad (137)$$

Si  $N(f) \geq 1$ , alors cela implique que  $\|g\| = \|f\|$  et que  $N(g) = N(f) - 1$ . En effet, on a que

$$b_{N(f)-1} = a_{N(f)} + \sum_{k \geq N(f)+1} a_k (-a)^{k-1}. \quad (138)$$

Donc  $|b_{N(f)-1}| = \|f\|$  et pour tout  $l \geq N(f)$ ,  $|b_l| \leq \max_{n > N(f)} |a_n| < \|f\|$ .  $\square$

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  $N(f) = \max \{i \geq 0 : |a_i| = \|f\|\}$ , 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

$$f(t) = a_0 + pg(t) \quad (139)$$

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

$$|f(z)| = |a_0| = 1 \quad (140)$$

et donc  $f$  n'a pas de zéros dans  $\mathbf{Z}_p$ . Supposons le résultat vrai pour  $N(f) = k$  avec  $k \geq 0$  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

$$f(t) = (t - z_0)g(t). \quad (141)$$

avec  $N(g) \leq N(f) - 1$ . 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  $\mathbf{Z}_p$ .  $\square$

**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

$$\|(x_1, \dots, x_d)\| = \max(|x_i|). \quad (142)$$

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

$$\mathbf{x}^I = x_1^{i_1} \cdots x_n^{i_n}. \quad (143)$$

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

$$f = \sum_I a_I \mathbf{x}^I \quad (144)$$

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

$$\|f\| = \max_I |a_I|. \quad (145)$$

**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

$$\|f + g\| \leq \max(\|f\|, \|g\|) \text{ et } \|fg\| \leq \|f\| \|g\|. \quad (146)$$

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

$$|f(z)| \leq \|f\| \|z\|. \quad (147)$$

Et pour tout  $x, y \in \mathbf{Z}_p^d$ , on a

$$|f(x) - f(y)| \leq \|f\| \cdot \|x - y\|. \quad (148)$$

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

DÉMONSTRATION. La première assertion est claire. On montre la deuxième par récurrence sur  $d$ . Si  $d = 1$ , alors

$$|f(x) - f(y)| = \left| \sum_n a_n(x-y) \right| \leq \max_n (|a_n| |x-y|^n) \leq \|f\| |x-y|. \quad (149)$$

Supposons le résultat vrai pour  $d \geq 1$  et montrons le résultat pour  $d+1$ . Soit  $f \in \mathbf{Q}_p\langle x_1, \dots, x_{d+1} \rangle$ , alors par l'exercice 4.12 on peut écrire

$$f = \sum_{n \geq 0} f_n(x_1, \dots, x_d) x_{d+1}^n. \quad (150)$$

On a en particulier que  $\|f_n\| \leq \|f\|$  pour tout  $n \geq 0$ . De sorte que

$$f(x) - f(y) = f_0(x_1, \dots, x_d) - f_0(y_1, \dots, y_d) + \sum_{n \geq 1} f_n(x_1, \dots, x_d) x_{d+1}^n - f_n(y_1, \dots, y_d) y_{d+1}^n. \quad (151)$$

Le premier terme a sa valeur absolue majorée par  $\|f_0\| |x-y|$  par hypothèse de récurrence. On majore ensuite chacun des termes de la somme comme suit. On note  $\hat{x}$  pour  $(x_1, \dots, x_d)$  et de même pour  $\hat{y}$ .

$$f_n(\hat{x}) x_{d+1}^n - f_n(\hat{y}) y_{d+1}^n = f_n(\hat{x})(x_{d+1}^n - y_{d+1}^n) + y_{d+1}^n (f_n(\hat{x}) - f_n(\hat{y})). \quad (152)$$

Comme  $(x_{d+1}^n - y_{d+1}^n) = (x-y)u$  avec  $u \in \mathbf{Z}_p$  on a que le premier terme a une valeur absolue  $\leq \|f_n\| \cdot \|\hat{x}\| \cdot |x_{d+1} - y_{d+1}| \leq \|f\| \cdot \|x-y\|$ . Le second terme a une valeur absolue majorée par hypothèse de récurrence par

$$\leq \|f\| \cdot |y_{d+1}^n| \|\hat{x} - \hat{y}\| \leq \|f\| \cdot \|x-y\|. \quad (153)$$

□

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

$$g \circ f = g(f_1(\mathbf{x}), \dots, f_d(\mathbf{x})) \in \mathbf{Q}_p\langle \mathbf{x} \rangle. \quad (154)$$

Et de plus,

$$\|g \circ f\| \leq \|g\| \cdot \|f\|. \quad (155)$$

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

$$g(f_1, \dots, f_d) = \sum_I a_I f_1^{i_1} \cdots f_d^{i_d}. \quad (156)$$

On pose  $h_k = \sum_{|I| \leq k} a_I f_1^{i_1} \cdots f_d^{i_d}$ . 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  $m \geq n$ , on a

$$\|h_m - h_n\| = \left\| \sum_{n+1 \leq |I| \leq m} a_I f_1^{i_1} \cdots f_d^{i_d} \right\| \leq \max_{|I| \geq n+1} |a_I|. \quad (157)$$

La dernière inégalité vient de l'exercice 4.7 et du fait que pour tout  $j = 1, \dots, d$ ,  $|f_j| \leq 1$ . Comme  $\max_{|I| \geq n+1} |a_I| \rightarrow 0$  quand  $n \rightarrow +\infty$ , c'est bien une suite de Cauchy. L'inégalité sur la norme de Gauss vient du fait que comme  $\|f\| \leq 1$  on a que  $\left\| f_1^{i_1} \cdots f_d^{i_d} \right\| \leq \|f\|$ .  $\square$

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

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

$$f(z_1, \dots, z_r, x_{r+1}, \dots, x_d) = \sum_I a_I z_1^{i_1} \cdots z_r^{i_r} x_{r+1}^{i_{r+1}} \cdots x_d^{i_d}. \quad (158)$$

Montrer également qu'on peut écrire

$$f = \sum_{k \geq 0} f_k(x_1, \dots, x_{d-1}) x_d^k \quad (159)$$

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

PROPOSITION 4.13. Si  $f : \mathbf{Z}_p^d \rightarrow \mathbf{Q}_p$  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  $d \geq 2$  et que le résultat soit vrai pour  $d - 1$ , alors on écrit

$$f = \sum_{k \geq 0} f_k(x_1, \dots, x_{d-1}) x_d^k. \quad (160)$$

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

$$f(z_1, \dots, z_{d-1}, x_d) = \sum_{k \geq 0} f_k(z_1, \dots, z_{d-1}) x_d^k \in \mathbf{Q}_p\langle x_d \rangle. \quad (161)$$

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  $k \geq 0$ ,  $f_k(z_1, \dots, z_{d-1}) = 0$ . On a donc que pour tout  $k \geq 0$ , la fonction analytique  $f_k : \mathbf{Z}_p^{d-1} \rightarrow \mathbf{Z}_p$  est nulle sur le polydisque  $\overline{D}(0, \varepsilon)^{d-1}$ . Par hypothèse de récurrence on a que pour tout  $k \geq 0$ ,  $f_k = 0$  et donc  $f = 0$ .

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

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

$$\mathbf{Z}_p\langle x_1, \dots, x_n \rangle^m \times \mathbf{Z}_p\langle y_1, \dots, y_m \rangle^l \rightarrow \mathbf{Z}_p\langle x_1, \dots, x_n \rangle^l. \quad (162)$$

En prenant  $n = m = l$  on obtient un monoïde pour la loi de composition. Un *difféomorphisme analytique* est un élément inversible dans ce monoïde. C'est à dire que  $f : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  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  $f \circ g = g \circ f = \text{id}$ . On note  $\text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  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)  $\|g \circ f\| \leq \|g\|$ .
- (2) Si  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$ , alors  $\|g \circ f\| = \|g\|$ .
- (3)  $\|g \circ (\text{id} + h) - g\| \leq \|h\|$ .
- (4)  $\|f^{-1} - \text{id}\| = \|f - \text{id}\|$  si  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$ .

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

$$\left\| \frac{g}{\|g\|} \circ f \right\| \leq 1. \quad (163)$$

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  $\|h_i\| \leq \|h\|$  et on a

$$g \circ (\text{id} + h) = g + A_1(h) + \sum_{k \geq 2} A_k(h) \quad (164)$$

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

$$\|g \circ (\text{id} + h) - g\| \leq \|h\|. \quad (165)$$

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

Soit  $c > 0$ , on définit

$$\text{Diff}_c^{\text{an}}(\mathbf{Z}_p^d) = \left\{ f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d) : \|f - \text{id}\| \leq \frac{1}{p^c} \right\}. \quad (166)$$

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

DÉMONSTRATION. Cela découle de la proposition 4.14.  $\square$

PROPOSITION 4.16. Pour tout  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  on a que  $\|f\| = 1$  et pour tout  $x, y \in \mathbf{Z}_p^d$  on a

$$\|f(x) - f(y)\| = \|x - y\|. \quad (167)$$

En particulier,  $\text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  agit par isométrie sur  $\mathbf{Z}_p^d$ .

**4.4. Expansion de Mahler.** Lorsqu'on a une série entière à une variable  $f(z) = \sum_n a_n z^n$ , on sait que

$$a_n = \frac{f^{(n)}(0)}{n!}. \quad (168)$$

Mahler s'est inspiré de cette écriture pour obtenir une formule équivalente en  $p$ -adique. On définit l'opérateur de différentiation discrète de la façon suivante. Pour toute fonction  $f : \mathbf{Z}_p \rightarrow \mathbf{Q}_p$

$$\nabla f(x) = f(x+1) - f(x). \quad (169)$$

Considérons également les fonctions tirés des coefficients binomiaux. On définit

$$\forall x \in \mathbf{Z}_p, \quad \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}. \quad (170)$$

Notez que  $\binom{x}{n} \in \mathbf{Q}_p\langle x \rangle$  car c'est une fonction polynomiale et de plus pour tout  $k \in \mathbf{N}$ , la fonction  $\binom{x}{n}$  évaluée en  $k$  vaut bien  $\binom{k}{n}$ . On a de plus que  $\phi(\mathbf{N}) \subset \mathbf{N}$  pour  $\phi = \binom{x}{n}$ . De plus on a la formule

$$\nabla \binom{x}{i} = \binom{x}{i-1}, \quad i \geq 1 \text{ et } \nabla \binom{x}{0} = 0. \quad (171)$$

En effet, nous sommes en train d'écrire une égalité de fonctions analytiques. Ces relations sont vraies lorsque  $x \in \mathbf{N} \subset \mathbf{Z}_p$ . Comme  $\mathbf{N}$  est infini on a par le principe des zéros isolés que ces deux fonctions analytiques coïncident.

**PROPOSITION 4.17.** *Soit  $M$  un groupe abélien et  $f : \mathbf{N} \rightarrow M$  une fonction quelconque. Il existe une unique suite  $(m_i) \subset M$  telle que*

$$f(x) = \sum_{i \geq 0} m_i \binom{x}{i}. \quad (172)$$

De plus on a  $m_i = \nabla^i f(0)$ .

**DÉMONSTRATION.** Notons tout d'abord que pour tout  $i \geq x$ ,  $\binom{x}{i} = 0$  donc ces sommes sont finies. En évaluant en 0 on a

$$f(0) = m_0. \quad (173)$$

On voit de plus que

$$\nabla^k f(x) = \sum_{i \geq k} m_i \binom{x}{i-k}. \quad (174)$$

De sorte que  $m_k = \nabla^k f(0)$ . Donc les  $m_k$  sont entièrement caractérisés par  $f$ , ceci prouve l'unicité. Réciproquement soit  $f : \mathbf{N} \rightarrow M$ , on pose  $g = \sum_{k \geq 0} \nabla^k f(0) \binom{x}{k}$  et on montre que  $f = g$ . Posons  $\phi = f - g$ . On a par construction que  $\phi(0) = 0$  et pour tout  $k \geq 1$

$$\nabla^k \phi(0) = \nabla^k f(0) - \nabla^k g(0) = 0. \quad (175)$$

On en déduit que  $\phi(1) - \phi(0) = \phi(1) = 0$ . Montrons que  $\phi(k) = 0$  par récurrence sur  $k$ . On montre par récurrence que pour tout  $k \geq 0$ ,

$$\nabla^k \phi(x) = \phi(x+k) + \sum_{l=0}^{k-1} b_l \phi(x+l) \quad (176)$$

avec  $b_l \in \mathbf{Z}$ . En effet, c'est vrai pour  $k = 0, 1$ . Et on a

$$\begin{aligned} \nabla^{k+1} \phi(x) &= \nabla^k \phi(x+1) - \nabla^k \phi(x) = \phi(x+k+1) + \sum_{l=0}^{k-1} b_l \phi(x+1+l) - \phi(x+k) - \sum_{l=0}^{k-1} b_l \phi(x+k) \\ &= \phi(x+k+1) + \sum_{l=0}^k c_k \phi(x+l). \end{aligned} \quad (177)$$

Donc la formule est vraie par récurrence. Supposons avoir montré que pour tout  $l \leq k$ ,  $\phi(l) = 0$ , alors par la formule (176) on a

$$0 = \nabla^{k+1} \phi(0) = \phi(k+1). \quad (178)$$

D'où le résultat.  $\square$

EXERCICE 4.18. Montrer que si  $\phi : \mathbf{N} \rightarrow M$  est une fonction vers un groupe abélien, alors

$$\forall k \geq 0, \nabla^k \phi(0) = \sum_{i=0}^k \binom{k}{i} (-1)^i \phi(k-i). \quad (179)$$

On énonce maintenant les deux théorèmes de Mahler.

THÉORÈME 4.19. Soit  $f : \mathbf{Z}_p \rightarrow \mathbf{Q}_p$  une fonction continue et définissons  $a_k = \nabla^k f(0)$ , on a alors que  $|a_k| \rightarrow 0$  et la série  $\sum_k a_k \binom{\cdot}{k}$  converge uniformément vers  $f$  sur  $\mathbf{Z}_p$ . De plus,

$$\sup_{\mathbf{Z}_p} |f| = \sup_{k \geq 0} |a_k|. \quad (180)$$

THÉORÈME 4.20. Soit  $f : \mathbf{N} \rightarrow \mathbf{Q}_p$  une fonction. On définit  $a_k = \nabla^k f(0)$ . Alors les propriétés suivantes sont équivalentes.

- (1)  $|a_k| \rightarrow 0$  quand  $k \rightarrow +\infty$ .
- (2) La série de Mahler  $\sum_{k \geq 0} a_k \binom{\cdot}{k}$  converge uniformément sur  $\mathbf{Z}_p$ .
- (3)  $f$  admet un prolongement continu  $f : \mathbf{Z}_p \rightarrow \mathbf{Q}_p$ .
- (4)  $f$  est uniformément continue (pour la topologie  $p$ -adique sur  $\mathbf{N}$ ).
- (5)  $\sup_{\mathbf{N}} |\nabla^k f| \rightarrow 0$  quand  $k \rightarrow +\infty$ .

**4.5. Flots et théorème de Bell-Poonen.** On définit maintenant la notion de flot comme en géométrie différentielle. Soit  $d \geq 1$  un entier. Un *flot analytique* sur  $\mathbf{Z}_p^d$  est une fonction analytique  $\Phi \in \mathbf{Z}_p\langle t, \mathbf{x} \rangle^d : \mathbf{Z}_p \times \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  telle que

$$(1) \quad \Phi(0, \cdot) = \text{id}.$$

$$(2) \quad \text{Pour tout } s, t \in \mathbf{Z}_p, \Phi(s+t, \cdot) = \Phi(s, \Phi(t, \cdot)) = \Phi(t, \Phi(s, \cdot)).$$

Pour  $t \in \mathbf{Z}_p$  on notera  $\Phi_t := \Phi(t, \cdot) \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$ . On a en fait pour tout  $t \in \mathbf{Z}_p, \Phi_t \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  car  $\Phi_t \cdot \Phi_{-t} = \text{id}$ . Et si  $f = \Phi_1$ , on a que

$$\forall k \in \mathbf{Z}, \quad f^k = \Phi_k. \quad (181)$$

On va montrer maintenant le théorème de Bell-Poonen qui énonce le fait suivant : si  $f : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  est une fonction analytique qui n'est pas très loin de l'identité, alors  $f$  est un difféomorphisme et il existe un unique flot analytique  $\Phi_1 = f$ .

**THÉORÈME 4.21.** *Soit  $c > \frac{1}{p-1}$  et soit  $f \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$  tel que  $\|f - \text{id}\| \leq |p|^c$ , alors  $f \in \text{Diff}_c^{\text{an}}(\mathbf{Z}_p^d)$  et il existe un unique flot analytique  $\Phi \in \mathbf{Z}_p\langle t, \mathbf{x} \rangle^d$  tel que*

$$\Phi_1 = f. \quad (182)$$

**DÉMONSTRATION.** Montrons tout d'abord l'unicité. Soit  $x \in \mathbf{Z}_p^d$  et soit  $\Phi_1, \Phi_2$  deux flots qui vérifient le théorème. Alors on a pour tout  $k \in \mathbf{N}$

$$\Phi_1(k, x) = \Phi_2(k, x) = f^k(x). \quad (183)$$

Donc la fonction analytique  $t \in \mathbf{Z}_p \mapsto \Phi_1(t, x) - \Phi_2(t, x)$  vaut l'origine une infinité de fois. Par le principe des zéros isolés cette fonction est constante égale à l'origine. Donc pour tout  $t \in \mathbf{Z}_p, x \in \mathbf{Z}_p^d$

$$\Phi_1(t, x) = \Phi_2(t, x). \quad (184)$$

Ceci implique l'égalité des séries associées par la proposition 4.13. Montrons l'existence maintenant. Pour trouver comment construire  $\Phi$  on va se baser sur les séries de Mahler. Si on fixe  $x \in \mathbf{Z}_p^d$ , alors on veut construire une fonction  $\phi : \mathbf{Z}_p \rightarrow \mathbf{Z}_p^d$  telle que pour tout  $k \in \mathbf{N}, \phi(k) = f^k(x)$  et  $\phi(0) = x$ . Par la proposition 4.17 cette fonction a une unique écriture sous la forme

$$\phi(t) = \sum_{k \geq 0} \nabla^k \phi(0) \binom{t}{k}. \quad (185)$$

Analysons les coefficients de cette somme. On a  $\phi(0) = x$ , puis  $\nabla \phi(0) = \phi(1) - \phi(0) = f(x) - x$ . Ensuite  $\nabla^2 \phi(0) = \phi(2) - 2\phi(1) + \phi(0)$ . Définissons l'opérateur  $\Delta$  qui vaut

$$\forall g \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d, \Delta g(\mathbf{x}) = g(f(\mathbf{x})) - g(\mathbf{x}). \quad (186)$$

**LEMME 4.22.** *Pour tout  $x \in \mathbf{Z}_p^d$ , si  $\phi_x : \mathbf{N} \rightarrow \mathbf{Z}_p^d$  est définie par  $\phi_x(l) = f^l(x)$ , alors*

$$\forall k \geq 0, \quad \nabla^k \phi_x(0) = \Delta^k(\text{id})(x). \quad (187)$$

DÉMONSTRATION. En effet, c'est vrai pour  $k = 0, 1$ . Montrons le résultat par récurrence. On a

$$\nabla^k \phi_x(0) = \nabla(\nabla^{k-1} \phi_x)(0) = \nabla^{k-1} \phi_x(1) - \nabla^{k-1} \phi_x(0). \quad (188)$$

Soit  $\psi : \mathbf{N} \rightarrow \mathbf{Z}_p^d$  définie par  $\psi(l) = \phi_x(l+1)$ , alors on a que

$$\nabla^{k-1} \phi_x(1) = \nabla^{k-1} \psi(0). \quad (189)$$

Mais  $\psi = \phi_{f(x)}$  et on a donc par récurrence que

$$\nabla^{k-1} \psi(0) = \Delta^{k-1}(\text{id})(f(x)). \quad (190)$$

Et donc

$$\nabla^k \phi_x(0) = \Delta^{k-1}(\text{id})(f(x)) - \Delta^{k-1}(\text{id})(x) = \Delta^k(\text{id})(x). \quad (191)$$

Ce qui donne le résultat.  $\square$

En définissant  $\Delta^k(\mathbf{x}) := \Delta^k(\text{id})(\mathbf{x})$ , il est donc naturel de poser

$$\Phi(t, \mathbf{x}) = \sum_{k \geq 0} \Delta^k(\mathbf{x}) \binom{t}{k}. \quad (192)$$

Chaque terme est un élément de  $\mathbf{Z}_p\langle t, \mathbf{x} \rangle$ , il faut montrer que la série est convergente.

LEMME 4.23. *On a pour tout  $k \geq 0$ ,*

$$\left\| \Delta^k(\mathbf{x}) \right\| \leq \frac{1}{p^{kc}} \quad (193)$$

DÉMONSTRATION. C'est vrai si  $k = 0, 1$ . Montrons le résultat par récurrence. Posons  $h = \Delta^{k-1}(\mathbf{x})$ . On a alors que  $h = p^m g$  avec  $m \geq (k-1)c$  et  $g \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$ . Et alors

$$\Delta^k(\mathbf{x}) = h(f(\mathbf{x})) - h(\mathbf{x}) = p^m (g(f(\mathbf{x})) - g(\mathbf{x})). \quad (194)$$

Maintenant on peut écrire  $f(\mathbf{x}) = \mathbf{x} + p^a w(\mathbf{x})$  avec  $a \geq c$  et  $w \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$ . Écrivons

$$g(\mathbf{x}) = A_0 + A_1(\mathbf{x}) + \sum_{l \geq 2} A_l(\mathbf{x}) \quad (195)$$

où  $A_i$  est la partie homogène de degré  $i$ . On a alors

$$g(f(\mathbf{x})) = A_0 + A_1(\mathbf{x}) + p^a A_1(w(\mathbf{x})) + \sum_{l \geq 2} A_l(\mathbf{x} + p^a w(\mathbf{x})) = g(\mathbf{x}) + p^a u(\mathbf{x}) \quad (196)$$

avec  $u \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$ . On a donc que  $g(f(\mathbf{x})) - g(\mathbf{x}) = p^a u(\mathbf{x})$  et donc

$$\left\| \Delta^k(\mathbf{x}) \right\| \leq |p^{m+a}| \leq \frac{1}{p^{kc}}. \quad (197)$$

$\square$

On a de plus que pour tout  $k \geq 1$

$$\left| \frac{1}{k!} \right| \leq \frac{1}{p^{-\frac{k}{p-1}}}. \quad (198)$$

En effet, on a vu en exercice que

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k \geq 1} \frac{n}{p^k} = \frac{n}{p-1}. \quad (199)$$

Maintenant si  $\|f - \text{id}\| \leq \frac{1}{p^c}$  avec  $c > \frac{1}{p-1}$  on a par le lemme 4.23 que

$$\left\| \frac{\Delta^k(\mathbf{x})}{k!} \right\| \leq \frac{1}{p^{k(c-\frac{1}{p-1})}} \xrightarrow{k \rightarrow +\infty} 0. \quad (200)$$

On a donc que la série définissant  $\Phi(t, \mathbf{x})$  est convergente et définit bien une fonction analytique de  $\mathbf{Z}_p \times \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$ . Montrons que  $c$  est un flot. Soit  $x \in \mathbf{Z}_p^d$  et  $n \in \mathbf{N}$ , on a que

$$\Phi(n, x) = \sum_{k=0}^n \binom{n}{k} \Delta^k(\text{id})(x) = (\text{id} + \Delta)^n(\text{id})(x) = f^n(x). \quad (201)$$

On a donc que pour tout  $s, t \in \mathbf{N}$  entiers

$$\Phi(s+t, x) = f^{s+t}(x) = f^s(f^t(x)) = f^t(f^s(x)). \quad (202)$$

Donc

$$\Phi(s+t, x) = \Phi(s, \Phi(t, x)) = \Phi(t, \Phi(s, x)). \quad (203)$$

Si on fixe la variable  $s$ , on a deux fonctions analytiques de  $t$  qui coïncident pour tout  $t \in \mathbf{N}$  donc les fonctions sont égales sur  $\mathbf{Z}_p$ . Maintenant à  $t \in \mathbf{Z}_p$  fixé, on a une égalité entre deux fonctions analytiques de la variable  $s$  qui est vraie sur  $\mathbf{N}$  qui est infini donc par les zéros isolés, l'égalité est vraie pour  $s \in \mathbf{Z}_p$ . Et on a bien également que pour tout  $x \in \mathbf{Z}_p^d$ ,  $\Phi(0, x) = x$ . En particulier on obtient que  $f \in \text{Diff}_c^{\text{an}}(\mathbf{Z}_p^d)$  car  $\Phi_1 = f$  et  $\Phi_{-1} = f^{-1}$ .  $\square$

On dira que  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  est contenu dans un flot s'il existe un flot analytique  $\phi_t$  tel que  $\phi_1 = f$ .

REMARQUE 4.24. On remarque que si  $p \geq 3$ , alors la condition est que  $c > \frac{1}{p-1} \geq \frac{1}{2}$ . En particulier,  $c = 1$  vérifie les hypothèses et on a donc que tout élément de  $\text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$  est contenu dans un flot.

COROLLAIRE 4.25. Soit  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  un difféomorphisme contenu dans un flot, si  $f \neq \text{id}$  alors  $f$  est d'ordre infini. En particulier si  $p \geq 3$ , alors  $\text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$  est sans torsion.

DÉMONSTRATION. Soit  $\phi_t$  le flot analytique tel que  $\phi_1 = f$ . Supposons que  $f^N = \text{id}$  pour un certain  $N \neq 0$ . Soit  $x \in \mathbf{Z}_p^d$ , on considère l'application analytique

$$ev_x : t \in \mathbf{Z}_p \mapsto \phi_t(x). \quad (204)$$

On a que  $ev_x(N\mathbf{Z}) = \{x\}$ , par le principe des zéros isolés cela implique que  $ev_x$  est constante égale à  $x$  et donc  $f(x) = ev_x(1) = x$ .

Si  $p \geq 3$ , alors par le théorème de Bell-Poonen on a que tous les éléments de  $\text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$  sont contenus dans un flot et donc sans torsion.  $\square$

On montre maintenant que la condition de congruence n'est pas restrictive.

**PROPOSITION 4.26.** *Soit  $G \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  un sous-groupe, il existe  $G_0 \subset G'$  un sous-groupe d'indice fini tel que  $G_0$  fixe toutes les boules  $U$  de rayons  $1/p$  de  $\mathbf{Z}_p^d$  et de plus pour chaque boule  $U$  on peut trouver des coordonnées sur  $U \simeq \mathbf{Z}_p^d$  tel que  $G_{0|U} \subset \text{Diff}_1^{\text{an}}(U)$ .*

**DÉMONSTRATION.** On a que  $G$  agit sur les boules de rayon  $\frac{1}{p^2}$ . De plus, pour tout  $g \in G$  et pour  $x \in \{0, \dots, p-1\}^d$ , on peut regarder la différentielle  $D_x(g)$  de  $g$  en  $x$ . Cela donne un homomorphisme de groupes

$$G \rightarrow \text{Bij}((\mathbf{Z}/p^2\mathbf{Z})^d) \times \prod_{\{0, \dots, p-1\}^d} \text{GL}_d(\mathbf{Z}/p\mathbf{Z}) \quad (205)$$

dont l'image est un groupe fini. Soit  $G_0$  le noyau de ce morphisme, c'est un sous-groupe d'indice fini et  $G_0$  fixe toutes les boules de rayon  $1/p^2$  et donc aussi celle de rayon  $1/p$ . Soit  $U = B(x_0, \frac{1}{p}) = p\mathbf{Z}_p$  avec  $x_0 \in \{0, \dots, p-1\}^d$ , en conjuguant  $G_0$  par la translation par  $x_0$  et en notant  $y_i + x_0(i) = x_i$  on a que dans les coordonnées  $y_1, \dots, y_d = \mathbf{y}$ , tout  $g \in G_0$  est de la forme

$$g(\mathbf{y}) = p^2 B_0 + A_1(\mathbf{y}) + \sum_{k \geq 2} A_k(\mathbf{y}) \quad (206)$$

avec  $A_i$  la partie homogène de degré  $i$ . On a alors que

$$\frac{1}{p}g(p\mathbf{y}) = pB_0 + A_1(\mathbf{y}) + \sum_{k \geq 2} p^{k-1}A_k(\mathbf{y}). \quad (207)$$

On voit donc que  $g(U) = U$  et de plus si on note  $z_i = py_i$  les coordonnées sur  $U$  on voit que  $g : U \rightarrow U$  est analytique en les coordonnées  $z_1, \dots, z_d$ . On voit de plus que  $g|_U = \text{id}|_U \pmod{p}$ .  $\square$

Ceci conclut la partie du cours sur l'analyse  $p$ -adique ou en tout cas tout a été introduit pour prouver les principaux résultats du cours.

## 5. Des automorphismes polynomiaux aux difféomorphismes analytiques

Les théorèmes qu'on cherche à démontrer concerne les automorphismes polynomiaux de l'espace affine  $\mathbf{C}^n$ . Il faut donc montrer comment on passe de transformations polynomiales sur  $\mathbf{C}$  à des transformations analytiques sur  $\mathbf{Z}_p^d$ . On va tout d'abord montrer que tout corps de type fini sur  $\mathbf{Q}$  se plonge dans  $\mathbf{Q}_p$  pour une infinité de nombres premiers  $p$ . Pour cela on va utiliser le lemme de Hensel, mais nous avons besoin d'introduire la notion de discriminant.

**5.1. Le discriminant d'un polynôme.** Soit  $A$  un anneau et  $P, Q \in A[X]$  de degré  $n$  et  $m$  respectivement. On note  $A[X]_{\leq l}$  l'ensemble des polynômes de degré  $\leq l$ , c'est un  $A$ -module (i.e stable par multiplication par  $A$  et stable par somme). On note  $\phi_{P,Q}$  l'application linéaire

$$\phi_{P,Q} \in (U, V) \in A[X]_{\leq m-1} \times A[X]_{\leq n-1} \mapsto UP + VQ \in A[X]_{n+m-1}. \quad (208)$$

Si on considère au départ la base

$$((X^{m-1}, 0), \dots, (1, 0), (0, X^{n-1}), \dots, (0, 1)) \quad (209)$$

et à l'arrivée la base

$$(X^{n+m-1}, \dots, 1) \quad (210)$$

alors la matrice de  $\phi_{P,Q}$  est donnée par

$$M_{P,Q} := \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & \vdots & b_m & \ddots & \vdots \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & \vdots & \ddots & a_n & b_1 & & & b_m \\ a_0 & & & a_{n-1} & b_0 & \ddots & \vdots & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\ \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{pmatrix}. \quad (211)$$

On définit le *résultant*  $R(P, Q)$  comme le déterminant de cette matrice. On a que

$$R(P, Q) = (-1)^{nm} R(Q, P). \quad (212)$$

**LEMME 5.1.** Soit  $A$  un anneau et  $I$  un idéal de  $A$  et  $P, Q \in A[X]$  de sorte que si on note  $\bar{P}$  et  $\bar{Q}$  leur image dans  $A/I[X]$ , alors  $\deg \bar{P} = \deg P$  et  $\deg \bar{Q} = \deg Q$ . On a la relation suivante entre les résultats et le passage au quotient :

$$R_{A/I}(\bar{P}, \bar{Q}) = R_A(P, Q) \text{ mod } I. \quad (213)$$

**DÉMONSTRATION.** Il est clair que la matrice de  $\phi_{\bar{P}, \bar{Q}}$  est  $\bar{M}_{P,Q}$ . Le résultat vient du fait que le déterminant est un polynôme en les coefficients de la matrice.  $\square$

**PROPOSITION 5.2.** Si  $A$  est un anneau factoriel, on a que  $R(P, Q) \neq 0$  si et seulement si  $P$  et  $Q$  sont premiers entre eux.

DÉMONSTRATION. Notez que si  $A$  est factoriel, alors  $A[x]$  est factoriel on peut donc parler de polynômes premiers entre eux. Si  $P$  et  $Q$  ne sont pas premiers entre eux, alors ils ont un facteur commun  $C$  et on a que

$$\phi_{P,Q}(Q/C, -P/C) = 0. \quad (214)$$

L'application linéaire  $\phi_{P,Q}$  n'est donc pas injective et son déterminant est donc nul. Réciproquement, si le résultant est nul, alors  $\phi_{P,Q}$  n'est pas injective et donc on peut écrire

$$UP = VQ \quad (215)$$

avec  $UV \neq 0$ . Si  $P$  et  $Q$  étaient premiers entre eux, on aurait alors par le lemme de Gauss que  $P$  divise  $V$  mais c'est absurde car  $\deg V < \deg P$ .  $\square$

Soit  $A$  un anneau intègre et soit  $P \in A[X]$  un polynôme de degré  $n$  et tel que  $\deg P' = n - 1$ , on définit le *discriminant* de  $P$  par

$$\Delta(P) := (-1)^{\frac{n(n-1)}{2}} R(P, P') \quad (216)$$

**5.2. Un théorème de changement de base.** On va maintenant montrer que tout corps de type fini sur  $\mathbf{Q}$  se plonge dans une infinité de  $\mathbf{Q}_p$ . On commence par le lemme suivant.

LEMME 5.3. *Soit  $P \in \mathbf{Z}[x]$  un polynôme à coefficients entiers, alors il existe une infinité de nombres premiers  $p$  tel que  $P$  a une racine modulo  $p$ .*

DÉMONSTRATION. En effet si ce n'était pas le cas, alors il existerait un nombre fini de nombres premiers  $p_1, \dots, p_r$  tel que pour tout  $n \in \mathbf{Z}$ ,  $P(n) = (-1)^{\varepsilon(n)} p_1^{\alpha_1(n)} \dots p_r^{\alpha_r(n)}$ . Soit  $M > 0$ , on a alors qu'il existe une constante  $C$  tel que

$$|P(\mathbf{Z}) \cap [-M, M]| \leq C \deg P (\log M)^r. \quad (217)$$

En effet, on a

$$|P(n)| \leq M \Rightarrow \forall i, \alpha_i(n) \leq \frac{1}{p_i} \log M. \quad (218)$$

Comme chaque point  $z \in \mathbf{C}$  a au plus  $\deg P$  préimages cela donne bien la borne voulue. Maintenant  $P$  est de la forme

$$P(x) = cx^{\deg P} + a_1 x^{\deg P - 1} + \dots + a_{\deg P}. \quad (219)$$

On voit donc que lorsque  $M \rightarrow +\infty$ , on a

$$|P(\mathbf{Z}) \cap [-M, M]| \geq \beta M^{1/\deg P} \quad (220)$$

avec  $\beta > 0$  ce qui est absurde.  $\square$

THÉORÈME 5.4. *Soit  $K$  un corps de type fini sur  $\mathbf{Q}$  et  $S \subset K$  une partie finie. Il existe une infinité de nombres premiers  $p$  tels que*

- (1) *Il existe un plongement  $\iota_p : K \hookrightarrow \mathbf{Q}_p$ .*
- (2)  *$\iota_p(S) \subset \mathbf{Z}_p$ .*

DÉMONSTRATION. Soit  $d = \text{tr. deg } K/\mathbf{Q}$ . Par le théorème de l'élément primitif il existe  $t_1, \dots, t_d \in K$  algébriquement indépendant et  $\theta \in K$  tel que

$$K = \mathbf{Q}(t_1, \dots, t_d)(\theta). \quad (221)$$

Soit  $f(x) = f(t_1, \dots, t_d; x) \in \mathbf{Q}(t_1, \dots, t_d)[x]$  le polynôme minimal de  $\theta$  sur  $\mathbf{Q}(t_1, \dots, t_d)$ , quitte à multiplier par les dénominateurs, on peut supposer que  $f(x) \in \mathbf{Z}[t_1, \dots, t_d][x]$ . Soit  $\Delta(t_1, \dots, t_d) \in \mathbf{Z}[t_1, \dots, t_d]$  le discriminant de  $f$  par rapport à la variable  $x$ . Pour tout  $s \in S$ , on a que  $s = g_s(\theta)$  avec  $g_s(x) \in \mathbf{Q}(t_1, \dots, t_d)(x)$ . On choisit des polynômes  $B_s(t_1, \dots, t_d) \in \mathbf{Z}[t_1, \dots, t_d]$  de sorte que  $B_s g_s \in \mathbf{Z}[t_1, \dots, t_d][x]$ . On note également  $A_s \in \mathbf{Z}[t_1, \dots, t_d]$  le résultant  $R(f, B_s g_s)$  par rapport à la variable  $x$ .

On choisit des entiers  $a_1, \dots, a_d$  de sorte que

- (1)  $\Delta(a_1, \dots, a_d) \neq 0$ ;
- (2)  $f(a_1, \dots, a_d, x)$  est un polynôme non constant.
- (3)  $B_s(a_1, \dots, a_d) \neq 0$  pour tout  $s \in S$ .
- (4)  $A_s(a_1, \dots, a_d) \neq 0$  pour tout  $s \in S$ .

On choisit un nombre premier  $p$  tel que

- (1)  $B_s(a_1, \dots, a_d) \neq 0 \pmod p$  pour tout  $s \in S$ .
- (2)  $\Delta(a_1, \dots, a_d) \neq 0 \pmod p$ .
- (3)  $A_s(a_1, \dots, a_d) \neq 0 \pmod p$ .
- (4)  $f(a_1, \dots, a_d; x)$  a une racine modulo  $p$  et a le même degré modulo  $p$ .

Les trois premières conditions sont vérifiées dès que  $p$  est assez grand et la dernière est vérifiée pour une infinité de nombres premiers  $p$  par le lemme précédent.

Comme  $\mathbf{Z}_p$  n'est pas dénombrable on peut trouver  $\mu_1, \dots, \mu_d \in \mathbf{Z}_p$  algébriquement indépendants. Posons alors

$$g(x) = f(a_1 + p\mu_1, \dots, a_d + p\mu_d; x) \in \mathbf{Z}_p[x]. \quad (222)$$

On a que  $g$  a une racine modulo  $p$ . Comme  $\Delta(a_1, \dots, a_d) \neq 0 \pmod p$  et que le degré ne chute pas modulo  $p$  on a par le lemme 5.1 et la proposition 5.2 que  $g \pmod p$  et  $g' \pmod p$  n'ont pas de racine communes. Par le lemme de Hensel on a alors que  $g$  admet une racine  $\tilde{\theta}$ . On définit le plongement  $\iota_p : K \hookrightarrow \mathbf{Q}_p$  par

$$\iota_p(t_i) = a_i + p\mu_i, \quad \iota_p(\theta) = \tilde{\theta}. \quad (223)$$

Enfin les conditions sur  $A_s$  et  $B_s$  impliquent que les éléments de  $s$  sont envoyés dans  $\mathbf{Z}_p$ . En effet, on a

$$s = B_s(t_1, \dots, t_d)^{-1} B_s(t_1, \dots, t_d) g_s(\theta). \quad (224)$$

On a que  $\iota(B_s) \in \mathbf{Z}_p^\times$  car il est  $\neq 0 \pmod p$  et comme  $A_s \neq 0$ , on a que  $\tilde{\theta}$  n'est pas une racine de  $g_s$  ce qui donne bien que  $s \in \mathbf{Z}_p$ .  $\square$

**5.3. Preuve du théorème 1.5.** On peut maintenant démontrer le théorème de Bell, Ghioca et Tucker énoncé au début de ce cours.

**THÉORÈME 5.5.** *Soit  $f \in \text{Aut}(\mathbf{C}^d)$  un automorphisme polynomial, soit  $x \in \mathbf{C}^d$  et  $V \subset \mathbf{C}^d$  une sous-variété. L'ensemble*

$$\{n \in \mathbf{Z} : f^n(x) \in V\} \quad (225)$$

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

**DÉMONSTRATION.** La sous-variété  $V \subset \mathbf{C}^d$  est définie par des polynômes  $P_1, \dots, P_r$ . Soit  $S \subset \mathbf{C}$  l'ensemble fini contenant les coefficients de  $f$  et de  $f^{-1}$ , les coefficients des polynômes  $P_i$  et les coordonnées de  $x$ . On considère un nombre premier  $p \geq 3$  et un plongement du corps  $K = \mathbf{Q}(S)$  dans  $\mathbf{Q}_p$  donné par le théorème 5.4 de sorte que  $S \subset \mathbf{Z}_p$ . On a alors que le sous-groupe engendré par  $f$  est contenu dans  $\text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$ . Par la proposition 4.26, il existe un entier  $N_0$  tel que  $f^{\pm N_0}$  préserve toutes les boules  $U$  de rayon  $1/p$  et tel que en changeant les coordonnées on a que  $\langle f^{N_0} \rangle \subset \text{Diff}_1^{\text{an}}(U)$ . Pour  $k = 0, \dots, N_0 - 1$ , on note  $U_k$  la boule de rayon  $1/p$  contenant  $f^k(x)$ . Soit  $\mathbf{z} = z_1, \dots, z_n$  des coordonnées sur  $U_k$  telles que  $\langle f^{N_0} \rangle \subset \text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$ . Par le théorème de Bell-Poonen, il existe un unique flot analytique  $\Phi_k(t; \mathbf{z})$  qui interpole les itérés de  $f^{N_0}$  sur  $U_k$ . Soit  $\phi_k : t \in \mathbf{Z}_p \mapsto \Phi_k(t, f^k(x))$ , c'est une fonction analytique de  $\mathbf{Z}_p \rightarrow \mathbf{Z}_p^d$ . On a pour tout  $\ell \in \mathbf{Z}$ ,

$$f^{\ell N_0 + k}(x) \in V \Leftrightarrow \forall i = 1, \dots, r, \quad P_i(\phi_k(\ell)) = 0. \quad (226)$$

Mais pour tout  $i = 1, \dots, r$ ,  $t \mapsto P_i(\phi_k(t))$  est une fonction analytique de  $\mathbf{Z}_p$  vers  $\mathbf{Q}_p$  donc elle n'a qu'un nombre fini de zéros ou bien elle est constante égale à zéro par le principe des zéros isolés. On voit donc que

$$\Gamma_k := \{m \in \ell\mathbf{Z} + k : f^m(x) \in V\} \quad (227)$$

est ou bien fini ou bien la progression arithmétique  $\ell\mathbf{Z} + k$ . Comme

$$\{m \in \mathbf{Z} : f^m(x) \in V\} = \bigcup_{k \in 0, \dots, N_0 - 1} \Gamma_k \quad (228)$$

on a le résultat. □

## 6. Application pour l'étude de l'action de groupes sur des variétés algébriques

**6.1. Champs de vecteurs analytiques.** On a vu en exercice l'opérateur de dérivation par rapport à la  $i$ -ème variable  $\partial_i : \mathbf{Q}_p\langle \mathbf{x} \rangle \rightarrow \mathbf{Q}_p\langle \mathbf{x} \rangle$ . Un *champ de vecteurs analytiques* sur  $\mathbf{Z}_p$  est un objet  $X$  de la forme

$$X(\mathbf{x}) = \sum_i u_i(\mathbf{x}) \partial_i \quad (229)$$

avec  $u_i(\mathbf{x}) \in \mathbf{Z}_p\langle \mathbf{x} \rangle$ . On écrit  $\Theta(\mathbf{Z}_p^d)$  pour l'espace des champs de vecteurs analytiques sur  $\mathbf{Z}_p^d$ , c'est un  $\mathbf{Z}_p$ -module (ou un  $\mathbf{Q}_p$ -espace vectoriel). Un champ de vecteurs induit une *dérivation* sur  $\mathbf{Q}_p\langle \mathbf{x} \rangle$

par

$$X(f) = \sum_i u_i(\mathbf{x}) \partial_i f(\mathbf{x}). \quad (230)$$

C'est à dire que

$$X(f+g) = X(f) + X(g) \text{ et } X(fg) = gX(f) + fX(g). \quad (231)$$

EXERCICE 6.1. Montrer que si deux champs de vecteurs induisent la même dérivation, alors ils sont égaux. C'est à dire que si pour tout  $f \in \mathbf{Z}_p\langle \mathbf{x} \rangle^d$ ,  $X(f) = Y(f)$ , alors  $X = Y$ .

EXERCICE 6.2. Montrer que pour tout  $x \in \mathbf{Z}_p^d$ ,

$$X(f)(x) = \frac{d}{dt} \Big|_{t=0} f(x_1 + tu_1(x), \dots, x_d + tu_d(x)). \quad (232)$$

Montrer en fait que pour toute fonction analytique  $\phi : \mathbf{Z}_p \rightarrow \mathbf{Z}_p^d$  telle que  $\phi(0) = x$  et  $\phi'(0) = (u_1(x), \dots, u_d(x))$  on a

$$X(f)(x) = \frac{d}{dt} \Big|_{t=0} f(\phi(t)). \quad (233)$$

6.1.1. *Crochet de Lie.* On définit le *crochet de Lie* de deux champs de vecteurs par si  $X = \sum_i u_i \partial_i$  et  $Y = \sum_i v_i \partial_i$ , alors

$$[X, Y] = \sum_j w_j \partial_j \quad (234)$$

où

$$w_j = \sum_{i=1}^d \left( u_i \frac{\partial v_j}{\partial x_i} - v_i \frac{\partial u_j}{\partial x_i} \right). \quad (235)$$

EXERCICE 6.3. Montrer que si  $f : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p$  est une fonction analytique, alors

$$[X, Y](f) = X(Y(f)) - Y(X(f)). \quad (236)$$

On dit que  $X$  et  $Y$  *commutent* si  $[X, Y] = 0$ . C'est équivalent à ce que les applications de dérivation associées commutent.

6.1.2. *Champs de vecteurs associés à un flot.* Soit  $\Phi : \mathbf{Z}_p \times \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  un flot analytique, on peut définir le *flot* associé à  $\phi$  par

$$X_\Phi(\mathbf{x}) := \frac{\partial \Phi_t}{\partial t} \Big|_{t=0} (\mathbf{x}). \quad (237)$$

Plus précisément si on écrit  $\Phi(t, \mathbf{x}) = (\phi_1(t, \mathbf{x}), \dots, \phi_d(t, \mathbf{x}))$ , alors

$$X_\phi(\mathbf{x}) = \sum_i \partial_i \phi_i(0, \mathbf{x}) \partial_i. \quad (238)$$

On a alors la formule suivante :

$$\forall x \in \mathbf{Z}_p^d, \forall t \in \mathbf{Z}_p, \quad X(\Phi_t(x)) = \frac{\partial}{\partial t} \Phi_t(x). \quad (239)$$

Autrement dit, le long de la courbe analytique  $t \mapsto \Phi_t(x)$ , le champ de vecteur  $X$  en  $\Phi_t(x)$  est donné par le vecteur tangent à la courbe.

Soit  $\varphi \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$ , alors  $\varphi$  agit sur les champs de vecteurs par *tiré-en-arrière* :

$$\varphi^* X(\mathbf{x}) = D_{\varphi(\mathbf{x})} \varphi^{-1}(X(\varphi(\mathbf{x}))). \quad (240)$$

Pour établir cette formule on fait l'identification suivante. On a que  $\Theta(\mathbf{Z}_p^d) = \mathbf{Z}_p \langle \mathbf{x} \rangle^d$  et si  $g \in \mathbf{Z}_p \langle \mathbf{x} \rangle^d$ , l'application différentielle qui à  $x \in \mathbf{Z}_p^d$  associe la matrice  $D_x g$  est donnée par

$$D_x g = (\partial_i f_j(x))_{1 \leq i, j \leq d}. \quad (241)$$

En particulier, c'est une application analytique de  $\mathbf{Z}_p^d$  vers  $M_d(\mathbf{Z}_p) \simeq \mathbf{Z}_p^{d^2}$ .

EXERCICE 6.4. Montrer que pour toute fonction analytique  $f$ ,

$$\varphi^* X(f)(x) = X(f \circ \varphi^{-1})(\varphi(x)). \quad (242)$$

PROPOSITION 6.5. Soit  $\varphi$  un difféomorphisme analytique et  $X, Y$  deux champs de vecteurs, alors

$$\varphi^* [X, Y] = [\varphi^* X, \varphi^* Y]. \quad (243)$$

DÉMONSTRATION. On a vu que pour toute fonction analytique  $f$ , on a

$$\varphi^* X(f) = X(f \circ \varphi^{-1}) \circ \varphi. \quad (244)$$

On a donc

$$\varphi^* [X, Y](f) = [X, Y](f \circ \varphi^{-1}) \circ \varphi = X(Y(f \circ \varphi^{-1})) \circ \varphi - Y(X(f \circ \varphi^{-1})) \circ \varphi. \quad (245)$$

Analysons le premier terme, on a

$$X(Y(f \circ \varphi^{-1})) \circ \varphi = X(Y(f \circ \varphi^{-1}) \circ \varphi \circ \varphi^{-1}) \circ \varphi = X(\varphi^* Y(f) \circ \varphi^{-1}) \circ \varphi = \varphi^* X(\varphi^* Y(f)). \quad (246)$$

De même le second terme vaut  $-\varphi^* Y(\varphi^*(X)(f))$ .  $\square$

PROPOSITION 6.6. Soit  $\varphi$  un difféomorphisme analytique et soit  $X$  un champ de vecteurs associés à un flot  $\Phi$ , alors

$$\forall x \in \mathbf{Z}_p^d, \quad \varphi^* X(x) = \frac{d}{dt} \Big|_{t=0} \varphi^{-1} \circ \Phi_t \circ \varphi(x). \quad (247)$$

Autrement dit le flot associé à  $\varphi^* X$  est le flot  $\varphi^{-1} \circ \Phi_t \circ \varphi$  et on a pour tout  $x, t$ ,

$$\varphi^* X(\varphi^{-1} \circ \Phi_t \circ \varphi) = \frac{d}{dt} \varphi^{-1} \circ \Phi_t \circ \varphi. \quad (248)$$

DÉMONSTRATION. On a

$$\varphi^*X(x) = D_{\varphi(x)}\varphi^{-1}X(\varphi(x)) = D_{\varphi(x)}\varphi^{-1}\left(\frac{d}{dt}\Big|_{t=0}\Phi_t(\varphi(x))\right). \quad (249)$$

Et par la formule de la chaîne cela donne

$$\varphi^*X(x) = \frac{d}{dt}\Big|_{t=0}\varphi^{-1}\circ\Phi_t\circ\varphi(x). \quad (250)$$

□

COROLLAIRE 6.7. *Soit  $\varphi$  un difféomorphisme analytique et  $X$  un champ de vecteur associé à un flot  $\Phi$ , alors*

$$\varphi^*X = X \Leftrightarrow \forall t \in \mathbf{Z}_p, \varphi \circ \Phi_t = \Phi_t \circ \varphi \Leftrightarrow \varphi \circ \Phi_1 = \Phi_1 \circ \varphi. \quad (251)$$

DÉMONSTRATION. L'équivalence entre les deux dernières assertions vient du principe des zéros isolés. Montrons la première, si  $\varphi$  et  $\Phi_t$  commutent, alors  $\varphi^{-1}\circ\Phi_t\circ\varphi = \Phi_t$  et par la proposition 6.6 on a que  $\varphi^*X = X$ . Réciproquement, si  $\varphi^*X = X$  alors soit  $x \in \mathbf{Z}_p^d$ , Par la proposition 6.6 on a que

$$X(\varphi^{-1}\circ\Phi_t\circ\varphi) = \frac{d}{dt}\varphi^{-1}\circ\Phi_t\circ\varphi. \quad (252)$$

Sauf que  $\Phi_t$  est aussi solution de cette équation différentielle. Ainsi les flots  $\Psi_t := \varphi^{-1}\circ\Phi_t\circ\varphi$  et  $\Phi_t$  sont tous les deux des flots de  $X$ . Mais par unicité locale des solutions des équations différentielles cela donne que  $\Psi_t$  et  $\Phi_t$  doivent coïncider pour les petits temps  $t$  mais par le principe des zéros isolés les flots sont égaux pour tout  $t$  et on a bien que

$$\varphi \circ \Phi_t = \Phi_t \circ \varphi. \quad (253)$$

□

PROPOSITION 6.8. *Soit  $\Phi_t$  un flot analytique et  $X_\Phi$  son champ de vecteurs associés, alors pour tout  $t \in \mathbf{Z}_p$*

$$\Phi_t^*X = X. \quad (254)$$

*Et de plus,  $X(x_0) = 0$  si et seulement si  $\Phi_1(x_0) = x_0$ .*

DÉMONSTRATION. Soit  $s \in \mathbf{Z}_p$ , on a

$$(\Phi_s)^*X(x) = D_{\Phi_s(x)}\Phi_{-s}(X(\Phi_s(x))) = D_{\Phi_s(x)}\Phi_{-s}\left(\frac{\partial\Phi}{\partial t}\Big|_{t=0}(t+s,x)\right) \quad (255)$$

$$= \frac{\partial}{\partial t}\Big|_{t=0}\Phi_{-s}(\Phi(t+s,x)) \quad (256)$$

$$= \frac{\partial\Phi_t}{\partial t}\Big|_{t=0}(x) = X(x). \quad (257)$$

Ceci est équivalent à la formule suivante : pour tout  $t \in \mathbf{Z}_p$

$$X(\Phi_t(x)) = D_x\Phi_t(X(x)). \quad (258)$$

On voit donc que si  $X(x_0) = 0$ , alors  $X(\Phi_t(x_0)) = 0$  pour tout  $t \in \mathbf{Z}_p$ , cela signifie que la dérivée de  $t \mapsto \Phi_t(x_0)$  est nulle. Ainsi  $t \mapsto \Phi_t(x_0)$  est constante égale à  $x_0$  car elle vaut  $x_0$  en  $t = 0$ . Ce qui donne bien que  $\Phi_1(x_0) = x_0$ . Réciproquement si  $\Phi_1(x_0) = x_0$ , alors pour tout  $t \in \mathbf{Z}_p$ , on a  $\Phi_t(x_0) = x_0$ , en effet par la propriété du flot c'est vrai pour tout temps  $t \in \mathbf{Z}$  et par les zéros isolés cela doit être vrai pour tout  $t \in \mathbf{Z}_p$ . Et donc la dérivée en  $t$  est nulle pour tout  $t$ .  $\square$

PROPOSITION 6.9. Soit  $\Phi$  un flot analytique et  $X_\Phi$  son champ de vecteurs associés. Soit  $Y$  un champ de vecteur analytique, alors

$$[X, Y] = \frac{\partial}{\partial t} \Big|_{t=0} \Phi_t^* Y. \quad (259)$$

DÉMONSTRATION. Soit  $f$  une fonction analytique, on a

$$\frac{d}{dt} \Big|_{t=0} \Phi_t^* Y(f)(x) = \lim_{t \rightarrow 0} \frac{\Phi_t^* Y(f)(x) - Y(f)(x)}{t} = \lim_{t \rightarrow 0} \frac{Y(f \circ \Phi_{-t})(\Phi_t(x)) - Y(f)(x)}{t}. \quad (260)$$

On ajoute et retranche  $Y(f)(\Phi_t(x))$  pour obtenir

$$\frac{d}{dt} \Big|_{t=0} \Phi_t^* Y(f)(x) = \lim_t \frac{Y(f \circ \Phi_{-t})(\Phi_t(x)) - Y(f)\Phi_t(x)}{t} + \frac{Y(f)\Phi_t(x) - Y(f)(x)}{t}. \quad (261)$$

La deuxième limite converge vers  $X(Y(f))$  et pour la première on a qu'elle vaut

$$\frac{\Phi_t^* Y(f)(x) - \Phi_t^* Y(f \circ \Phi_t)(x)}{t} = -\Phi_t^* Y \left( \frac{f \circ \Phi_t(x) - f(x)}{t} \right). \quad (262)$$

Comme  $\Phi_t^* Y \rightarrow Y$  on a que la limite vaut  $-Y(X(f))$  ce qui donne bien le résultat.  $\square$

EXERCICE 6.10. Soit  $f, g \in \text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$  et  $\Phi_f, \Phi_g$  leurs flots associés et  $X_f, X_g$  les champs de vecteurs associés. Montrer que  $f$  et  $g$  commutent si et seulement si les flots  $\Phi_f, \Phi_g$  commutent si et seulement si les champs de vecteurs  $X_f$  et  $X_g$  commutent.

EXERCICE 6.11. Soit  $X = \sum_i u_i \partial_i$  un champ de vecteurs. Montrer que  $[X, \partial_d] = 0$  si et seulement si pour tout  $i, \partial_d u_i = 0$ , autrement dit  $X$  ne dépend pas de la variable  $x_d$ .

On va maintenant prouver un théorème très important en géométrie différentielle. Le théorème de redressement des champs de vecteurs. Il nous sera utile pour des arguments de récurrence sur la dimension. On doit tout d'abord énoncer le théorème d'existence de flot locaux.

THÉORÈME 6.12. Soit  $f : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  une application analytique et  $m$  un point tel que  $D_m f$  est inversible, alors il existe un ouvert  $U \simeq \mathbf{Z}_p^d$  contenant  $m$  et un ouvert  $V \simeq \mathbf{Z}_p^d$  et des coordonnées analytiques sur ces ouverts tels que  $f : U \rightarrow V$  soit un difféomorphisme local. De plus si  $f(m) = m$  on peut prendre le même ouvert  $U = V$ .

DÉMONSTRATION. On peut supposer que  $m$  et  $f(m)$  sont l'origine de sorte que  $f$  s'écrivent

$$f(\mathbf{x}) = A(\mathbf{x}) + \sum_{k \geq 2} A_k(\mathbf{x}) \quad (263)$$

où  $A = D_0 f$  est une matrice inversible et les  $A_k$  sont les termes homogènes de degré  $k \geq 2$ . On peut montrer que  $g$  admet un inverse dans l'espace des séries formelles et que cet inverse a un rayon de convergence positif. Soit  $\ell \geq 1$  un entier tel que le rayon de convergence de  $g$  soit  $\leq \frac{1}{p^\ell}$ . On a alors que  $g$  a la même forme que  $f$  et alors soit  $U = B(0, \frac{1}{p^\ell}) \simeq \mathbf{Z}_p^d$  et munit des coordonnées  $y_1, \dots, y_d$  de sorte que l'inclusion  $\varphi : U \rightarrow \mathbf{Z}_p^d$  est donnée par

$$\varphi(y_1, \dots, y_d) = (p^\ell y_1, \dots, p^\ell y_d). \quad (264)$$

On a alors que

$$\varphi^{-1} \circ f \circ \varphi(y) = \frac{1}{p^\ell} f(p^\ell y) = A(y) + \sum_{k \geq 2} p^{\ell-1} A_k(y) \in \mathbf{Z}_p \langle y \rangle \quad (265)$$

et de même pour  $\varphi^{-1} \circ g \circ \varphi$ . □

**PROPOSITION 6.13.** *Soit  $X$  un champ de vecteurs analytiques sur  $\mathbf{Z}_p^d$  et  $m \in \mathbf{Z}_p^d$  un point. Il existe un ouvert  $U \simeq \mathbf{Z}_p^d$  contenant  $m$  et un difféomorphisme analytique local  $\varphi : U \rightarrow \mathbf{Z}_p^d$  tel que  $\varepsilon \varphi^* X$  soit un champ de vecteurs analytiques sur  $U$  provenant d'un flot analytique pour un certain  $\varepsilon \in \mathbf{Z}_p \setminus \{0\}$ .*

**DÉMONSTRATION.** On peut supposer que  $m = 0$  est l'origine. Trouver un flot local de  $X$  revient à résoudre l'équation différentielle

$$\frac{d}{dt} \Phi_t(\mathbf{x}) = X(\Phi_t(\mathbf{x})) \text{ et } \Phi_0 = \text{id}. \quad (266)$$

On peut voir  $X$  comme une application analytique de  $\mathbf{Z}_p^d$  vers  $\mathbf{Z}_p^d$ . On a vu en exercice qu'une telle équation différentielle possède une solution  $F(t, \mathbf{x})$  dans l'espace des séries formelles et qu'elle a un rayon de convergence positif vu que  $X$  a un rayon de convergence positif. Soit  $p^k$  avec  $k \geq 1$  telle que le rayon de convergence de  $F$  soit  $\geq \frac{1}{p^k}$ . On sait que  $F$  est de la forme

$$F(t, \mathbf{x}) = \mathbf{x} + tG(t, \mathbf{x}). \quad (267)$$

Et on a alors que

$$\frac{1}{p^k} F(p^k t, p^k y) = y + t \left( G(p^k t, p^k y) \right) \in \mathbf{Z}_p \langle t; y \rangle. \quad (268)$$

Soit  $U = B(0, \frac{1}{p^k}) \simeq \mathbf{Z}_p^d$  avec coordonnées  $y_1, \dots, y_d$ . On pose  $\varphi : U \rightarrow \mathbf{Z}_p^d$  tel que  $\varphi(y_1, \dots, y_d) = (p^k y_1, \dots, p^k y_d)$ . On a alors que pour tout  $y \in U$ ,

$$\varphi^* X(y) = \frac{1}{p^k} X(p^k y). \quad (269)$$

et alors si on pose  $\Phi(t, y) = \frac{1}{p^k} F(p^k t, p^k y) = \varphi^{-1} \circ F(p^k t, p^k x)$  on a bien

$$\frac{d}{dt} \Phi(t, y) = \frac{1}{p^k} \frac{d}{dt} \left( F(p^k t, p^k x) \right) = \left( \frac{d}{dt} F \right) (p^k t, p^k y) \quad (270)$$

$$= X(F(p^k t, p^k y)) = X \left( p^k \Phi(t, y) \right) = p^k \varphi^* X(\Phi(t, y)). \quad (271)$$

Donc  $\Phi_t$  est bien le flot de  $p^k \varphi^* X$ .  $\square$

**THÉORÈME 6.14** (Théorème de redressement). *Soit  $X$  et  $m \in \mathbf{Z}_p^d$  un point tel que  $X(m) \neq 0$ , alors il existe un ouvert  $U \simeq \mathbf{Z}_p^d$  contenant  $m$  et un difféomorphisme analytique local  $\varphi : U \rightarrow \mathbf{Z}_p^d$  tel que  $\lambda \varphi^* X = \partial_d$  avec  $\lambda \in \mathbf{Z}_p$ .*

**DÉMONSTRATION.** Par la proposition 6.13, il existe un ouvert  $U \simeq \mathbf{Z}_p^d$  et un changement de coordonnées analytiques telle que  $\varepsilon \varphi^* X$  proviennent d'un flot  $\Phi$ . On suppose à nouveau que  $m = 0_{\mathbf{Z}_p^d}$  est l'origine. On peut conjuguer  $\Phi$  et  $X$  par une matrice dans  $\mathrm{SL}_d(\mathbf{Z}_p)$  de sorte que  $X(0) = (0, \dots, 0, \lambda)$  avec un certain  $\lambda \in \mathbf{Z}_p$ . Considérons l'application  $\theta : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  définie par

$$\theta(x_1, \dots, x_{d-1}, t) = \Phi_t((x_1, \dots, x_{d-1}, 0)). \quad (272)$$

Comme  $\frac{d}{dt}|_{t=0} \theta(0, \dots, 0, t) = X(0) = \lambda(0, \dots, 0, 1)$  on a que la différentielle de  $\theta$  à l'origine est  $\mathrm{Diag}(1, \dots, 1, \lambda)$  qui est inversible. Par la théorème d'inversion local on peut trouver une boule ouverte  $V \simeq \mathbf{Z}_p$  et des coordonnées locales  $y_1, \dots, y_d$  telles que  $\varphi : V \rightarrow \mathbf{Z}_p^d$  soit donné par  $\varphi(y) = p^k y$ . contenant l'origine tel que  $\theta : V \rightarrow V$  soit un difféomorphisme analytique. Maintenant  $\theta^* X$  n'est peut être pas à coefficient dans  $\mathbf{Z}_p$  mais un de ses multiples l'est. Soit  $Y_d$  le champ de vecteurs  $\partial_d$  on a

$$Y_d(y) = \frac{d}{dt} (y_1, \dots, y_{d-1}, y_d + t) \quad (273)$$

$$= \frac{1}{p^k} \frac{d}{dt} (p^k y_1, \dots, p^k y_{d-1}, p^k y_d + p^k t) \quad (274)$$

$$= \frac{1}{p^k} \frac{d}{dt} \theta^{-1} \circ \Phi_{p^k t} \left( \theta \left( p^k y_1, \dots, p^k y_d \right) \right) \quad (275)$$

$$= \frac{d}{dt} \left( \varphi^{-1} \circ \theta^{-1} \circ \Phi_{p^k t} \circ \theta \circ \varphi \right) (y) \quad (276)$$

$$= \theta^* \varphi^* X. \quad (277)$$

$\square$

**6.2. Groupes nilpotents.** Soit  $G$  un groupe. Si  $a, b \in G$ , on définit le *commutateur* de  $a$  et  $b$  par

$$[a, b] = aba^{-1}b^{-1}. \quad (278)$$

Si  $A, B \subset G$  sont deux sous-groupes on définit  $[A, B]$  comme le sous-groupe engendré par

$$\{[a, b] : a \in A, b \in B\}. \quad (279)$$

On définit la *suite dérivée* d'un groupe comme la suite de sous-groupe  $G_{(k)}$  définie par

$$G_{(0)} = G, \quad G_{(k+1)} = [G_{(k)}, G_{(k)}]. \quad (280)$$

En particulier le *sous-groupe dérivé* de  $G$  est le groupe  $D(G) := G_{(1)} = [G, G]$ .

EXERCICE 6.15. Montrer que si  $a, b, g \in G$ , alors

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]. \quad (281)$$

En déduire que  $D(G)$  est un sous-groupe distingué de  $G$ . Montrer que tout sous-groupe distingué  $H \subset G$  tel que  $G/H$  est abélien contient  $D(G)$ .

On définit la *suite centrale* d'un groupe  $G$  par

$$G^{(0)} = G, \quad G^{(k+1)} = [G, G^{(k)}]. \quad (282)$$

DÉFINITION 6.16. On dit qu'un groupe  $G$  est *résoluble* s'il existe un entier  $e \geq 0$  tel que  $G_{(e)} = 0$ . On définit la *longueur dérivée*  $dl(G)$  de  $G$  comme le plus petit entier  $e \geq 0$  tel que  $G_{(e)} = 0$ .

On dit qu'un groupe  $G$  est *nilpotent* s'il existe un entier  $e \geq 0$  tel que  $G^{(e)} = 0$ . On définit l'*indice de nilpotence*  $nilp(G)$  de  $G$  comme le plus petit entier  $e \geq 0$  tel que  $G^{(e)} = 0$ .

EXERCICE 6.17. Montrer que nilpotent implique résoluble.

Soit  $G$  le groupe des transformations affines sur  $\mathbf{C}$ . Montrer que  $G$  résoluble mais pas nilpotent. (Montrer que  $D(G)$  est le sous-groupe des translations et montrer que toute translation est le commutateur d'une translation avec une homothétie).

EXERCICE 6.18. Montrer qu'un groupe  $G$  est résoluble si et seulement si il existe une suite de sous-groupes  $G_0 = G \supset G_1 \supset \dots \supset G_s = \{0\}$  telle que  $G_{i+1} \subset G_i$  est distingué et  $G_i/G_{i+1}$  est abélien.

EXERCICE 6.19. Soit  $H \subset G$  un sous-groupe distingué. Montrer que  $G$  est résoluble si et seulement si  $H$  et  $G/H$  sont résolubles. Montrer qu'on a de plus que  $dl(G) \leq dl(H) + dl(G/H)$ .

Si maintenant  $G$  est nilpotent, montrer que  $H$  et  $G/H$  sont nilpotents (mais la réciproque est fausse).

EXERCICE 6.20. Soit  $G$  un groupe, le *centre* de  $G$  est défini par

$$Z(G) = \{h \in G : \forall g \in G, \quad gh = hg\}. \quad (283)$$

On dit que  $H$  est *central* si  $H \subset Z(G)$ . Montrer que tout sous-groupe central est distingué. Montrer que si  $H$  est un-sous groupe central et que  $G/H$  est nilpotent alors  $G$  est nilpotent et  $nilp(G) \leq nilp(H) + 1$ .

REMARQUE 6.21. Il est à noter que si  $G$  est un groupe nilpotent non trivial, alors  $Z(G)$  n'est pas trivial. En effet, si  $k = nilp(G)$ , alors  $G^{(k-1)} \subset Z(G)$  et  $G^{(k-1)} \neq 0$  par définition.

On a enfin les formules suivantes :

$$(1) [x, y]^{-1} = [y, x].$$

$$(2) [x, yz] = [x, y][y, [x, z]][x, z].$$

$$(3) [xy, z] = [x, [y, z]][y, z][x, z].$$

**6.3. Algèbre de Lie.** Soit  $K$  un corps, une *algèbre de Lie* sur  $K$  est un espace vectoriel  $\mathfrak{g}$  munit d'une application bilinéaire  $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$  telle que

$$(1) \forall x \in \mathfrak{g}, [x, x] = 0.$$

$$(2) \forall x, y, z \in \mathfrak{g}, [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

En particulier on a que  $[x, y] = -[y, x]$ .

EXEMPLE 6.22. Soit  $K$  un corps et  $M_n(K)$  l'ensemble des matrices carrées de taille  $n \times n$ , alors  $M_n(K)$  est une algèbre de Lie avec le crochet

$$[A, B] = AB - BA. \quad (284)$$

EXEMPLE 6.23. Le  $\mathbf{Q}_p$ -espace vectoriel engendré par les champs de vecteurs analytiques sur  $\mathbf{Z}_p^d$  munit du crochet de Lie de champs de vecteurs est une algèbre de Lie.

On dit qu'une algèbre de Lie  $\mathfrak{g}$  est *abélienne* si son crochet de Lie est trivial : pour tout  $x, y \in \mathfrak{g}$ ,  $[x, y] = 0$ . On peut définir de la même manière la suite dérivée  $\mathfrak{g}^{(k)}$  et la suite centrale  $\mathfrak{g}^{(k)}$  et définir la notion d'algèbre de Lie résoluble et nilpotente. Si  $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{g}$  sont deux sous-algèbres de Lie, alors  $[\mathfrak{a}, \mathfrak{b}]$  est le *sous-espace vectoriel* engendré par

$$\{[a, b], a \in \mathfrak{a}, b \in \mathfrak{b}\}. \quad (285)$$

On définit alors la suite dérivée  $\mathfrak{g}^{(k)}$  par  $\mathfrak{g}^{(0)} = \mathfrak{g}$  et  $\mathfrak{g}^{(k+1)} = [\mathfrak{g}^{(k)}, \mathfrak{g}^{(k)}]$  et la suite centrale  $\mathfrak{g}^{(k)}$  par  $\mathfrak{g}^{(0)} = \mathfrak{g}$  et  $\mathfrak{g}^{(k+1)} = [\mathfrak{g}, \mathfrak{g}^{(k)}]$ . On dit que  $\mathfrak{g}$  est *résoluble* s'il existe  $e \geq 0$  tel que  $\mathfrak{g}^{(e)} = 0$  et *nilpotente* s'il existe  $e \geq 0$  tel que  $\mathfrak{g}^{(e)} = 0$ . Notez que chaque  $\mathfrak{g}^{(k)}$  et  $\mathfrak{g}^{(k)}$  est une sous-algèbre de Lie.

Un *morphisme d'algèbre de Lie* est une application linéaire  $\phi : \mathfrak{g} \rightarrow \mathfrak{h}$  telle que pour tout  $x, y \in \mathfrak{g}$ ,  $\phi([x, y]) = [\phi(x), \phi(y)]$ . On peut définir alors le *noyau* de  $\phi$  par  $\ker \phi$  qui est naturellement une sous-algèbre de Lie.

EXEMPLE 6.24. Soit  $\phi : \mathbf{Z}_p^d \rightarrow \mathbf{Z}_p^d$  un difféomorphisme analytique, l'application de tiré-en-arrière  $\phi^* : \Theta(\mathbf{Z}_p^d) \rightarrow \Theta(\mathbf{Z}_p^d)$  est un morphisme d'algèbre de Lie.

Soit  $\mathfrak{h} \subset \mathfrak{g}$  une sous-algèbre de Lie. On dit que  $\mathfrak{h}$  est un *idéal* de  $\mathfrak{g}$  si  $[\mathfrak{h}, \mathfrak{g}] \subset \mathfrak{h}$ . On a alors que  $\mathfrak{g}/\mathfrak{h}$  possède une unique structure d'algèbre de Lie telle que l'application quotient  $\mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$  soit un morphisme d'algèbres de Lie. C'est l'*algèbre de Lie quotient*.

On dit qu'une algèbre de Lie  $\mathfrak{g}$  est *simple* si elle n'admet pas d'idéaux autre que  $\{0\}$  et  $\mathfrak{g}$ . On verra en exercice que l'algèbre de Lie  $\mathfrak{sl}_n(K)$  est simple pour tout corps  $K$ , où

$$\mathfrak{sl}_n(K) = \{A \in M_n(K) : \text{Tr}(A) = 0\} \quad (286)$$

et le crochet de Lie est donné par  $[A, B] = AB - BA$ .

L'ensemble des exercices sur les groupes résolubles et nilpotents sont également vrais pour les algèbres de Lie.

THÉORÈME 6.25. Soit  $d \geq 1$  et  $\mathfrak{g} \subset \Theta(\mathbf{Z}_p^d)$  une sous-algèbre de Lie nilpotente, alors

$$d \geq \text{dl}(\mathfrak{g}). \quad (287)$$

À noter ici que même si l'algèbre de Lie est nilpotente, c'est bien la longueur dérivée qui permet de minorer.

DÉMONSTRATION. Montrons le résultat par récurrence sur  $d$ . Si  $d = 1$ , alors on montre que l'algèbre de Lie est en fait abélienne. En effet, soit  $X \in \mathfrak{g}$  un champ de vecteur central. Par le théorème 6.14, il existe un ouvert  $U \simeq \mathbf{Z}_p^d$  et des coordonnées analytiques sur  $U$  telle que si  $\varphi : U \rightarrow \mathbf{Z}_p^d$  est le changement de coordonnées, alors  $\varphi^*X = \lambda \partial_x$  avec  $\lambda \in \mathbf{Q}_p$ . Maintenant, par les zéros isolés, l'application linéaire  $\varphi_{|\mathfrak{g}}^*$  est injective. Soit maintenant  $Y \in \mathfrak{g}$ , on a que  $[Y, X] = 0$  et donc  $[\varphi^*Y, \varphi^*X] = 0$ . Mais comme  $d = 1$  cela signifie que  $\varphi^*Y = u(x)\partial_x$  avec  $\partial_x u = 0$ . Donc  $\varphi^*Y$  est un champ de vecteurs constant mais par les zéros isolés cela signifie que  $Y$  est le champ de vecteur constant. Ainsi on a que pour tout  $Y_1, Y_2 \in \mathfrak{g}$ ,  $[\varphi^*Y_1, \varphi^*Y_2] = 0$  et donc l'algèbre de Lie  $\mathfrak{g}$  est abélienne et  $\text{dl}(\mathfrak{g}) = 1$ .

Supposons que le résultat soit vrai en dimension  $d$  avec  $d \geq 1$  et montrons le en dimension  $d + 1$ . Soit  $X \in \mathfrak{g}$  un champ de vecteurs analytique central dans  $\mathfrak{g}$ . Par le théorème 6.14, il existe un ouvert  $V \simeq \mathbf{Z}_p^d$  tel que après un changement de coordonnées on a  $X = \partial_{d+1}$  sur  $V$ . Soit  $Y \in \mathfrak{g}$ , comme  $[Y, \partial_{d+1}] = 0$  on a que  $Y$  est de la forme

$$Y = \sum_{i=1}^{d+1} u_i(x_1, \dots, x_d) \partial_i. \quad (288)$$

Soit  $\mathfrak{h} \subset \mathfrak{g}$  la sous-algèbre de Lie définie par

$$\mathfrak{h} = \mathfrak{g} \cap \{u(x_1, \dots, x_d) \partial_{d+1}\}. \quad (289)$$

C'est une sous-algèbre de Lie abélienne non triviale car  $X = \partial_{d+1} \in \mathfrak{h}$  et c'est un idéal de  $\mathfrak{g}$ . En effet on peut le montrer par le calcul mais aussi parce que c'est le noyau du morphisme d'algèbres de Lie donné par la projection sur les  $d$  premières coordonnées

$$Y = \sum_{i=1}^{d+1} u_i(x_1, \dots, x_d) \partial_i \in \mathfrak{g} \mapsto \sum_{i=1}^d u_i(x_1, \dots, x_d) \partial_i \in \Theta(\mathbf{Z}_p^d). \quad (290)$$

Notons  $\mathfrak{g}'$  l'image de  $\mathfrak{g}$ . C'est une algèbre nilpotente et par récurrence on a que  $d \geq \text{dl}(\mathfrak{g}')$ . Cela donne alors

$$d + 1 \geq \text{dl}(\mathfrak{g}') + 1 = \text{dl}(\mathfrak{g}') + \text{dl}(\mathfrak{h}) \geq \text{dl}(\mathfrak{g}). \quad (291)$$

□

**6.4. Preuve du théorème sur les groupes nilpotents.** On dit que  $f \in \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  est analytique par flot s'il existe un flot analytique  $\Phi$  tel que  $\Phi_1 = f$ . Soit  $G \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$ , on dira que  $G$  est analytique par flot si tous ses éléments le sont. En particulier, tout sous-groupe de  $\text{Diff}_1^{\text{an}}(\mathbf{Z}_p^d)$  est analytique par flot si  $p \geq 3$  par le théorème de Bell-Poonen.

EXERCICE 6.26. Montrer que si  $f$  et  $g$  commutent et sont analytiques par flots, alors  $f \circ g$  est aussi analytique par flot et  $X_{f+g} = X_f + X_g$ .

DÉFINITION 6.27. Si  $G$  est analytique par flot, on définit son *algèbre de Lie*  $\mathfrak{g}$  par l'algèbre de Lie engendrée par les champs de vecteurs analytiques  $X_f$  pour  $f \in G$ .

LEMME 6.28. Soit  $G$  un sous-groupe analytique par flot et  $G' \subset G$  un sous-groupe d'indice fini, alors  $G'$  et  $G$  ont même algèbre de Lie.

DÉMONSTRATION. Soit  $\mathfrak{g}'$  l'algèbre de Lie de  $G'$ . On a  $\mathfrak{g}' \subset \mathfrak{g}$ , réciproquement soit  $f \in G$ , alors il existe un entier  $m$  tel que  $f^m \in G'$  et alors  $X_{f^m} = mX_f \in \mathfrak{g}'$  et donc  $\mathfrak{g} \subset \mathfrak{g}'$ .  $\square$

EXERCICE 6.29. En déduire que si  $G$  est un groupe analytique par flot, alors pour tout  $G' \subset G$  d'indice fini on a

$$Z(G') = Z(G) \cap G'. \quad (292)$$

EXERCICE 6.30. Soit  $G$  un groupe nilpotent et soit  $Z$  son centre, montrer que

$$\text{nilp}(G) = \text{nilp}(G/Z) + 1. \quad (293)$$

EXERCICE 6.31. Montrer que pour tout ouvert  $U \subset \mathbf{Z}_p^d$ , l'application de restriction  $\Theta(\mathbf{Z}_p^d) \rightarrow \Theta(\mathbf{Z}_p^d)|_U$  est injective.

EXERCICE 6.32. On suppose  $d = 1$  et  $G \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p)$ . Montrer que les assertions suivantes sont équivalentes.

- (1)  $G$  est abélien.
- (2)  $G$  est nilpotent.
- (3) Le centre de  $G$  n'est pas trivial.
- (4) Il existe un ouvert  $U \subset \mathbf{Z}_p^d$  telle que  $\mathfrak{g}|_U$  est abélienne.
- (5)  $\mathfrak{g}$  est abélienne.

(Utiliser le théorème de redressement).

PROPOSITION 6.33. Soit  $G$  un groupe analytique par flot, alors  $G$  est abélien si et seulement si  $\mathfrak{g}$  est abélienne.

DÉMONSTRATION. Par l'exercice 6.26, on a que  $f, g \in G$  commutent si et seulement si  $[X_f, X_g] = 0$ . Ce qui donne l'équivalence.  $\square$

Si  $G$  est un groupe résoluble on définit sa *longueur dérivée virtuelle* par

$$\text{vdl}(G) := \min \{ \text{dl}(H) : H \subset G \text{ d'indice fini} \}. \quad (294)$$

THÉORÈME 6.34. Soit  $G \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  un sous-groupe nilpotent et analytique par flot, alors  $\mathfrak{g}$  est nilpotente et

$$d \geq \text{vdl}(G) \quad (295)$$

DÉMONSTRATION. Si  $d = 1$ , alors c'est l'exercice 6.32. On procède maintenant par récurrence et on suppose  $d \geq 2$ . Soit  $f$  dans le centre de  $G$ . Comme pour la proposition précédente, on trouve une boule ouverte  $U$  telle que  $X_f = \partial_d$  sur  $U$ . Soit  $G'$  un sous-groupe d'indice fini de  $G$  qui fixe  $U$ , alors tout élément de  $G'|_U$  est de la forme

$$g = \text{id} + h(x_1, \dots, x_{d-1}). \quad (296)$$

On considère la projection  $\pi : U \rightarrow \mathbf{Z}_p^{d-1}$  sur les  $d - 1$  premières coordonnées. Elle induit un homomorphisme de groupe  $\pi : G \rightarrow G_1$  de noyau un sous-groupe central  $K$ . De même on a un homomorphisme d'algèbres de Lie  $\mathfrak{g} \rightarrow \mathfrak{g}_1$  et de noyau une sous-algèbre de Lie centrale  $\mathfrak{k}$ . Le groupe  $G_1$  est nilpotent et analytique par flot et son algèbre de Lie est  $\mathfrak{g}_1$ . Par hypothèse de récurrence,  $\mathfrak{g}_1$  est nilpotente et  $d - 1 \geq \text{vdl}(G_1)$ . Comme  $\mathfrak{g}_1$  est nilpotente et que  $\mathfrak{k}$  est centrale on a que  $\mathfrak{g}$  est nilpotente et  $\text{dl}(\mathfrak{g}) \leq \text{dl}(\mathfrak{g}_1) + 1$ . Il faut maintenant montrer que  $d \geq \text{vdl}(G)$ . Par hypothèse de récurrence, il existe  $G'_1 \subset G_1$  d'indice fini tel que  $\text{dl}(G'_1) \leq d - 1$ . Soit  $G' = \pi^{-1}(G'_1)$ , c'est un sous-groupe d'indice fini de  $G$ . Si  $k = \text{dl}(G'_1)$ , alors  $D_{(k)}(G') \subset K$  qui est central et donc  $D_{(k+1)}(G') = 0$ . On a donc que

$$\text{dl}(G') \leq \text{dl}(G'_1) + 1 \leq d. \quad (297)$$

C'est ce qu'il fallait démontrer.  $\square$

Pour finir cette partie on montre un dernier résultat qui lie un groupe nilpotent analytique par flot à son algèbre de Lie. On doit d'abord énoncer une version améliorée du théorème de redressement.

THÉORÈME 6.35. *Soit  $X_1, \dots, X_r$  des champs de vecteurs analytiques qui commutent deux à deux, alors pour tout point  $o \in \mathbf{Z}_p^d$ , tel que  $X_1(o), \dots, X_r(o)$  sont linéairement indépendants, il existe une boule ouverte  $U \simeq \mathbf{Z}_p^d$  contenant  $o$  et des coordonnées analytiques sur  $U$  tel que  $X_i|_U = \partial_i$ .*

La preuve se fait de la même manière que pour le théorème de redressement. On peut supposer que  $o$  est l'origine. Si  $\Phi^1, \dots, \Phi^r$  sont les flots associés à  $X_1, \dots, X_r$ , alors on considère l'application

$$(t_1, \dots, t_r, x_{r+1}, \dots, x_d) \mapsto \Phi_{t_1}^1 \circ \dots \circ \Phi_{t_r}^r ((0, \dots, x_{r+1}, \dots, x_d)). \quad (298)$$

On montre que c'est un difféomorphisme local et le résultat suit. La preuve marche car les flots  $\Phi^i$  commutent.

PROPOSITION 6.36. *Soit  $G \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p^d)$  un sous-groupe analytique et soit  $\mathfrak{g}$  son algèbre de Lie. Si  $\mathfrak{g}$  est nilpotente, alors  $G$  est nilpotent et il existe un sous-groupe d'indice fini  $G' \subset G$  tel que  $\text{nilp}(G') = \text{nilp}(G)$ . En particulier,  $\text{nilp}(\mathfrak{g}) = \min \{\text{nilp}(G_0) : G_0 \subset G \text{ d'indice fini}\}$ .*

DÉMONSTRATION. On raisonne par récurrence sur la dimension. Si  $d = 1$ , alors par l'exercice 6.32 le résultat suit. On suppose  $d \geq 2$ . Soit  $\mathfrak{z} \subset \mathfrak{g}$  le centre de  $\mathfrak{g}$ . Soit  $s = \max_{x \in \mathbf{Z}_p^d} \dim \mathfrak{z}(x)$ . Soit  $o$  un point où le max est réalisé. Soit  $X_1, \dots, X_s \in \mathfrak{z}$  tels que  $X_1(o), \dots, X_s(o)$  sont linéairement indépendants. Par le théorème 6.35, il existe une boule ouverte  $U$  et des coordonnées analytiques sur  $U$

telles que  $X_i = \partial_i$ . Par construction de  $s$  on a de plus que  $\mathfrak{z}_{|U} \subset \mathbf{Q}_p\langle \mathbf{x} \rangle X_1 + \cdots + \mathbf{Q}_p\langle \mathbf{x} \rangle X_s$ . Soit  $H \subset G$  un sous-groupe d'indice fini de  $G$  qui fixe  $U$ , tout élément de  $H_{|U}$  est de la forme

$$h(x_1, \dots, x_d) = \text{id} + h'(x_{s+1}, \dots, x_d). \quad (299)$$

La projection sur les  $d - s$  dernières coordonnées donne un morphisme de groupes surjectifs  $H \rightarrow H_1$  avec  $H_1 \subset \text{Diff}^{\text{an}}(\mathbf{Z}_p^{d-s})$  analytique par flot et on a aussi le morphisme d'algèbres de Lie  $\mathfrak{h} \rightarrow \mathfrak{h}_1$  associé. On a que  $\mathfrak{h} = \mathfrak{g}$  car  $H$  est d'indice fini dans  $G$  et donc le centre de  $H$  est contenu dans le noyau de la projection. Autrement dit on a

$$\text{nilp}(H_1) \leq \text{nilp}(H) - 1, \quad \text{nilp}(\mathfrak{h}_1) \leq \text{nilp}(\mathfrak{h}) - 1. \quad (300)$$

Or comme le noyau de la projection est centrale pour le morphisme de groupes et pour le morphisme d'algèbres de Lie on a également que  $\text{nilp}(H) \leq \text{nilp}(H_1) + 1$  et  $\text{nilp}(\mathfrak{h}) \leq \text{nilp}(\mathfrak{h}_1) + 1$ . D'où  $\text{nilp}(H) = \text{nilp}(H_1) + 1$  et  $\text{nilp}(\mathfrak{h}) = \text{nilp}(\mathfrak{h}_1) + 1$ . Par hypothèse de récurrence,  $H_1$  admet un sous-groupe d'indice fini  $H'_1$  tel que  $\text{nilp}(H'_1) = \text{nilp}(\mathfrak{h}_1)$ . Soit  $H'$  la préimage de  $H'_1$  c'est un sous-groupe d'indice fini de  $H$  et on a que  $\text{nilp}(H') \leq \text{nilp}(H'_1) + 1$ . Mais, comme  $H' \subset H$  est d'indice fini, le centre de  $H'$  est le même que le centre de  $H$  et donc  $\text{nilp}(H'_1) \leq \text{nilp}(H_1) - 1$ . D'où l'égalité  $\text{nilp}(H') = \text{nilp}(H'_1) + 1$  et le résultat.  $\square$

<++>

## 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.