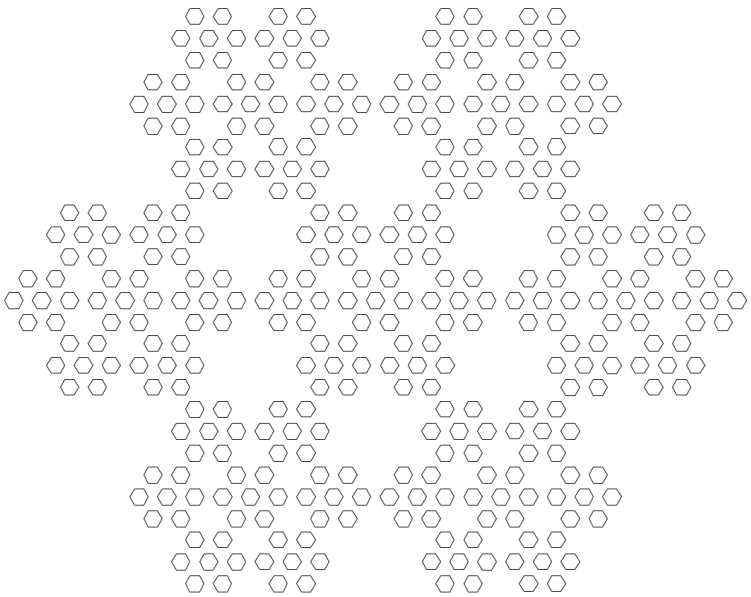
Travail Encadré de Recherche
4ème année de Mathématiques

SUR LA DYNAMIQUE DES AUTOMORPHISMES POLYNOMIAUX AFFINES EN CARACTÉRISTIQUE ZÉRO

Cyril Falcon

Résumé. Dans ce dossier, on montrera qu'en caractéristique zéro, l'ensemble des indices en lesquels une suite récurrente linéaire s'annule est l'union d'un ensemble fini et d'un nombre fini de progressions arithmétiques. On donnera une version algébriquo-géométrique de ce résultat qui précisera le comportement des itérés des automorphismes linéaires en dimension finie. Les techniques employées pour établir ce théorème nous permettront d'en énoncer une généralisation aux automorphismes polynomiaux affines.



Sous la direction de : François Charles

Date: Janvier-Juin 2016.

Table des matières

Remerciements

Je témoigne tout d'abord mon entière reconnaissance à la direction des études du département de Mathématiques de l'Université Paris-Sud qui est à l'initiative des travaux encadrés de recherche. Ils favorisent l'instauration d'échanges privilégiés avec les chercheurs et valorisent de fait notre formation.

Je tiens ensuite à exprimer ma profonde gratitude à François Charles qui a accepté de me superviser dans un sujet de son initative. Je suis sincérement reconnaissant de la qualité de son encadrement, c'est en effet grâce à la pertinence de ses remarques et de ses conseils que j'ai pu pleinement m'épanouir dans ce travail. Je le remercie enfin de sa disponibilité et de sa gentillesse et ce malgré mes visites impromptues dans son bureau.

Je manifeste toute ma sympathie à Amadou Bah avec qui nous avons étudié le même thème et dont le travail de relecture m'a permi de corriger une preuve de l'annexe qui n'était initialement pas exhaustive.

Je souhaite finalement remercier mon lecteur dont la curiosité l'aura amené à s'intéresser au texte maladroit d'un étudiant. Je m'excuse d'ailleurs auprès de lui pour les éventuelles longueurs de ma rédaction.

Introduction et motivations

Commençons par introduire la notion de suite récurrente linéaire sur un corps, il s'agira de l'objet central de notre étude :

Définition 1. Soit k un corps, une suite $(u_n)_{n\in\mathbb{N}}$ est dite récurrente linéaire si et seulement s'il existe un entier naturel d non nul et $a_0, \cdots, a_{d-1}$ dans k avec $a_0 \neq 0_k$ tels que la suite $(u_n)_{n\in\mathbb{N}}$ satisfasse à la relation de récurrence suivante :

$$\forall n \in \mathbb{N}, u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i}.$$

On peut légitimement s'interroger sur la nature des zéros d'une telle suite, autrement dit, sur la répartition des indices en lesquels elle s'annule ; notamment, est-ce qu'un ensemble quelconque d'entiers naturels est systématiquement l'ensemble des zéros d'une suite récurrente linéaire ? Ou au contraire, est-ce que les zéros des suites récurrentes linéaires ont une structure rigide et se distribuent selon des motifs réguliers ? Le cas échéant, quelles sont les obstructions et les conditions nécessaires pour qu'un ensemble d'indices soit l'ensemble des zéros d'une suite récurrente linéaire ? Dans le suite de notre étude, on supposera que le corps k est de caractéristique zéro ; la situation en caractéristique positive est quant à elle plus subtile, on verra notamment l'article de H. Derksen [5].

Afin de mieux appréhender la nature des zéros des suites récurrentes linéaires en caractéristique zéro et de se construire une intuition sur leur répartition, considérons sans plus attendre un exemple. Nous nous plaçons dans $\mathbb{Q}$ et nous rappelons alors que tout corps de caractéristique zéro est une extension de $\mathbb{Q}$. On s'intéresse à la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 := 0, u_1 := 0, u_2 := 1, u_3 := 0$ et satisfaisant à la relation de récurrence suivante :

$$\forall n \in \mathbb{N}, u_{n+4} = u_{n+2} + u_n.$$

Par récurrence, on montre que u_n est nul si et seulement si $n = 0$ ou est impair. En d'autres termes, l'ensemble des indices en lesquels $(u_n)_{n\in\mathbb{N}}$ s'annule est :

$$\{0\} \cup \{2n + 1; n \in \mathbb{N}\}.$$

Il s'agit de l'union d'un ensemble fini et d'une progression arithmétique, ce que l'on peut reformuler en disant qu'à partir du rang 1, l'écart entre deux zéros consécutifs est constant égal à 2. Cette observation témoigne d'une très grande rigidité de la structure de l'ensemble des indices où $(u_n)_{n\in\mathbb{N}}$ s'annule. Plus généralement, la distribution des zéros d'une suite récurrente linéaire en caractéristique zéro est donnée par l'énoncé suivant :

Théorème 1. (Skolem [15], Mahler [11], Lech [10]) Soient k un corps de caractéristique 0 et $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire sur k, alors l'ensemble :

$$\{n \in \mathbb{N} \text{ t.q. } u_n = 0\}$$

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

Étant donné une telle suite, ce résultat exprime qu'à partir d'un certain rang les indices en lesquels elle s'annule se disposent selon un même motif de longueur finie qui se repète indéfiniment, on dit également que l'ensemble de ses zéros est ultimement périodique ; on verra notamment la figure 1.

FIGURE 1. Un motif fini dans les zéros d'une suite récurrente linéaire.

Le théorème 1 constitue en particulier une obstruction à ce que l'ensemble des nombres premiers, respectivement l'ensemble des carrés parfaits, soit l'ensemble des zéros d'une suite récurrente linéaire en caractéristique zéro.

Historiquement, la première version de ce théorème est due à T. Skolem qui en 1933 avait établi le résultat pour les suites récurrentes linéaires sur sur le corps des nombres rationnels. Par la suite, K. Mahler a généralisé en 1935 la preuve de T. Skolem aux corps de nombres, c'est-à-dire aux extensions finies du corps des nombres rationnels. Cependant, il aura fallu attendre 1954 pour que C. Lech démontre la version du théorème sur tout corps de caractéristique zéro.

Même dans sa variante sur $\mathbb{Q}$, ce théorème présente un véritable intérêt et ce plus particulièrement lorsque les relations de récurrence sont d'ordre au moins égal à 2. En effet, les zéros des suites récurrentes linéaires contiennent une profonde complexité et il est notamment extrêmement difficile d'identifier de manière effective leurs zéros. À titre d'exemple, le problème suivant est ouvert :

Problème ouvert 1. Soient k un corps de caractéristique zéro et $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire sur k. Est-ce que le statut de l'assertion suivante :

$$\forall n \in \mathbb{N}, u_n \neq 0$$

est vérifiable en temps fini ?

On donne désormais une formulation du théorème 1 en termes d'algèbre linéaire :

Théorème 2. Soient k un corps de caractéristique zéro, $x \in k^d$ et σ un automorphisme linéaire de k^d. Si H est un hyperplan de k^d, alors l'ensemble :

$$\{n \in \mathbb{N} \text{ t.q. } \sigma^n(x) \in H\}$$

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

Avant d'établir l'équivalence annoncée, rappelons la terminologie suivante :

Définition 2. Soient R un anneau commutatif et d un entier naturel non nul, on appelle matrice compagnon de taille d, toute matrice de la forme suivante :

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{d-1} \end{pmatrix},$$

où $a_0, \cdots, a_{d-1}$ sont dans R.

Il est aisé de constater que si k est un corps, A est une matrice compagnon de taille $d \geqslant 2$ et $x \in k^d$, alors les composantes de $(A^n x)_{n\in\mathbb{N}}$ sont des suites récurrentes linéaires sur k. Il suffit pour cela de comprendre l'action de A sur x.

Nous pouvons désormais montrer que les théorèmes 1 et 2 sont équivalents.

Preuve. On procède par double implication.

- On suppose le théorème 1 acquis. En vertu du théorème de décomposition de Frobenius [6], il existe une base de k^d dans laquelle la matrice de σ, que l'on note A, soit constituée d'une diagonale de matrices compagnons. Par ailleurs, H étant de codimension 1 dans k^d, il existe $v \in k^d$ tel que :
$$H = \left\{ y \in k^d \text{ t.q. } {}^t v y = 0 \right\}.$$
Par conséquent, on en déduit que l'on a :
$$\{n \in \mathbb{N} \text{ t.q. } \sigma^n(x) \in H\} = \{n \in \mathbb{N} \text{ t.q. } {}^t v A^n x = 0\}. \tag{1}$$
σ étant un automorphisme, la matrice A est inversible et les matrices compagnons qui la composent sont toutes de taille au moins égale à 2. Ainsi, puisqu'une combinaison linéaire de suites récurrentes linéaires est encore récurrente linéaire, $({}^t v A^n x)_{n\in\mathbb{N}}$ est elle aussi récurrente linéaire. Finalement, d'après (1) et le théorème 1, on a établi le théorème 2.

- On suppose le théorème 2 acquis. Par définition, il existe $d \in \mathbb{N}_{\geqslant 1}$ et $a_0, \cdots, a_{d-1}$ dans k avec $a_0 \neq 0_k$ tels que l'on ait :
$$\forall n \in \mathbb{N}, u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i}.$$
On introduit alors A la matrice compagnon associée aux $a_0, \cdots, a_{d-1}$; en développant le déterminant de A par rapport à sa première colonne, on constate que A est inversible. Ainsi, en notant σ l'unique endomorphisme de k^d dont la matrice dans la base canonique est A, on définit un automorphisme de k^d. En outre, on introduit les éléments de k^d suivants :
$$x := \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{d-1} \end{pmatrix} \text{ et } w := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$
De cette manière, en comprenant l'action de σ sur x, on montre que :
$$\forall n \in \mathbb{N}, u_n = {}^t w \sigma^n(x). \tag{2}$$
On définit alors l'hyperplan de k^d suivant :
$$H := \{y \in k^d \text{ t.q. } {}^t w y\}.$$
Dès lors, d'après (2), on en déduit que l'on a :
$$\{n \in \mathbb{N} \text{ t.q. } u_n = 0\} = \{n \in \mathbb{N} \text{ t.q. } \sigma^n(x) \in H\}. \tag{3}$$
Finalement, d'après (3) et le théorème 2, on a établi le théorème 1.

□

Avant de pouvoir donner une généralisation significative de la version algébriquo-géométrique du théorème de Skolem-Mahler-Lech (théorème 2), nous avons besoin d'introduire la notion d'automorphisme polynomial affine :

Définition 3. Soient R un anneau commutatif et d un entier naturel non nul, on appelle espace affine de rang d sur R et l'on note $\mathbb{A}_R^d$, le R-module R^d. Alors, les automorphismes de $\mathbb{A}_R^d$ sont les inversibles de $R[X_1, \cdots, X_d]^d$.

Théorème 3. (Bell [1]) Soient k un corps de caractéristique zéro, $x \in \mathbb{A}_k^d$ et σ un automorphisme de $\mathbb{A}_k^d$. Si X est une sous-variété de $\mathbb{A}_k^d$, alors l'ensemble :

$$\{m \in \mathbb{Z} \text{ t.q. } \sigma^m(x) \in X\}$$

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

Le théorème 2 apparait comme une version linéaire du théorème 3 ; en effet, un automorphisme linéaire est un automorphisme polynomial dont les composantes de lui-même et son inverse sont des polynômes homogènes de degré 1.

Le contexte et les enjeux ayant été introduits, détaillons désormais l'approche que nous adopterons pour obtenir les résultats annoncés ci-dessus.

Veuillez tout d'abord noter que nous nous contenterons seulement d'établir intégralement le théorème 1. Cependant, nous insistons sur le fait que le cheminement suivi permettrait d'obtenir avec un moindre effort le théorème 3. En effet, il s'agirait essentiellement de vérifier que le résultat d'interpolation p-adique utilisé pour démontrer le théorème 1 s'applique encore.

Comme nous venons de le laisser sous-entendre, nous montrerons qu'il suffit d'établir les théorèmes 1 et 3 sur les corps de nombres p-adiques, notamment en montrant que toute extension finiment engendrée de $\mathbb{Q}$ se plonge dans une infinité de $\mathbb{Q}_p$ (partie 3.1). Cette restriction ayant été faite, nous utiliserons un résultat général d'interpolation p-adique pour les itérés de fonctions polynomiales (partie 2), ce qui nous permettra d'inclure l'ensemble qui intervient dans le théorème 1, respectivement dans le théorème 3, dans l'ensemble de zéros d'une fonction p-analytique. Finalement, nous conclurons grâce à un résultat sur la répartition dans $\mathbb{Z}_p$ des zéros des séries entières p-adiques (partie 1.3).

Ce dossier a été construit de telle manière à ce que chaque partie puisse être lue indépendamment des autres. En effet, nous nous sommes dans la mesure du possible efforcés de montrer chaque résultat utile au moment venu et nous faisons systématiquement mention des énoncés exploités. De cette manière, le lecteur pourra parcourir ce rapport à son entière convenance et s'il est familier à l'analyse p-adique, il pourra se laisser tenter de passer à la partie 2.

1. Quelques rudiments d'analyse p-adique

Soit p un nombre premier quelconque, l'objectif final de cette partie est la compréhension de la répartition dans l'anneau des entiers p-adiques des zéros de séries entières à coefficients p-adiques. Ce résultat sera crucial pour établir les théorèmes 1 et 3 énoncés en introduction. Notre cheminement débutera par une construction algébrique des entiers et des nombres p-adiques et se poursuivra par l'élaboration d'une topologie sur ces ensembles.

1.1. Arithmétique élémentaire des entiers et des nombres p-adiques.

Quels que soient m et n des entiers naturel au moins égaux à 1 et tels que $m \leqslant n$, on introduit le morphisme d'anneaux suivant :

$$\varphi_m^n : \left\{ \begin{array}{ccc} \mathbb{Z}/(p^n) & \to & \mathbb{Z}/(p^m) \\ x \mod p^n & \mapsto & x \mod p^m \end{array} \right. .$$

Soit $(x, y) \in \mathbb{Z}^2$ tel que $x \equiv y \mod p^n$, alors comme $p^m | p^n$, il vient :

$$x \equiv y \mod p^m.$$

Ainsi, φ_m^n est constante sur les classes d'équivalence de $\mathbb{Z}$ modulo p^n.

Définition 1.1. L'ensemble des entiers p-adiques, noté $\mathbb{Z}_p$, est défini par :

$$\left\{ (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n) \text{ t.q. } \forall (m,n) \in {\mathbb{N}_{\geqslant 1}}^2, m \leqslant n \Rightarrow \varphi_m^n(x_n) = x_m \right\}.$$

Remarque 1.2. C'est l'étude des équations diophantiennes qui a motivé K. Hensel à définir les entiers p-adiques dans son article fondateur [7] de 1897.

Remarque 1.3. Soient $(I, \preceq)$ un ensemble ordonné, $(E_i)_{i\in I}$ une famille d'ensembles indexée par I et $\left(f_i^j : E_j \to E_i\right)_{\substack{(i,j)\in I^2 \\ i\preceq j}}$ une famille d'application satisfaisant aux deux propriétés suivantes :

$$\forall i \in I, f_i^i = \mathrm{id}_{E_i},$$
$$\forall (i,j,k) \in I^2, i \preceq j \preceq k \Rightarrow f_i^k = f_i^j \circ f_j^k.$$

Une telle donnée constitue un système projectif d'ensembles. On appelle alors limite projective des E_i et on note $\varprojlim E_i$ l'ensemble suivant :

$$\left\{ (a_i)_{i\in I} \in \prod_{i\in I} E_i \text{ t.q. } \forall (i,j) \in I^2, i \preceq j \Rightarrow f_i^j(a_j) = a_i \right\}.$$

Selon le formalisme décrit ci-dessus, $\mathbb{Z}_p$ est la limite projective du système :

$$\left\{ \left(\mathbb{Z}/(p^n)\right)_{n\in\mathbb{N}_{\geqslant 1}}, \left(\varphi_m^n\right)_{\substack{(m,n)\in {\mathbb{N}_{\geqslant 1}}^2 \\ m\leqslant n}} \right\}.$$

Par conséquent, la grande majorité des résultats que nous établirons dans cette partie s'inscrivent dans le cadre d'une théorie plus large et s'étendent en particulier naturellement aux limites projectives d'anneaux topologiques.

Définition-Proposition 1.4. Quels que soient $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}}$ et $y := (y_n)_{n\in\mathbb{N}_{\geqslant 1}}$ des éléments de $\mathbb{Z}_p$, on définit :

$$x + y := (x_n + y_n)_{n\in\mathbb{N}_{\geqslant 1}},$$
$$x \times y := (x_n y_n)_{n\in\mathbb{N}_{\geqslant 1}}.$$

$\mathbb{Z}_p$ muni de $+$ et $\times$ est un anneau commutatif unitaire.

Preuve. Quel que soit $(m, n) \in {\mathbb{N}_{\geqslant 1}}^2$ satisfaisant à $m \leqslant n$, φ_m^n est un morphisme d'anneaux. Par conséquent, $+$ et $\times$ sont des lois de compositions internes sur $\mathbb{Z}_p$ et les deux éléments définis ci-dessous sont dans $\mathbb{Z}_p$:

$$0_{\mathbb{Z}_p} := \left(0_{\mathbb{Z}/(p^n)}\right)_{n\in\mathbb{N}_{\geqslant 1}}, 1_{\mathbb{Z}_p} := \left(1_{\mathbb{Z}/(p^n)}\right)_{n\in\mathbb{N}_{\geqslant 1}}.$$

Quel que soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p$, on définit l'élément de $\mathbb{Z}_p$ suivant :

$$-x := (-x_n)_{n\in\mathbb{N}_{\geqslant 1}}.$$

À partir des propriétés de l'addition et de la multiplication sur chacun des anneaux $\mathbb{Z}/(p^n), n \in \mathbb{N}_{\geqslant 1}$, on vérifie que quel que soit $(x, y, z) \in {\mathbb{Z}_p}^3$, on a :

- $x + (y + z) = (x + y) + z$ (associativité de $+$),
- $x + y = y + x$ (commutativité de $+$),
- $x + 0_{\mathbb{Z}_p} = x$ (élément neutre pour $+$),
- $x + (-x) = 0_{\mathbb{Z}_p}$ (inverse pour $+$),
- $x \times (y \times z) = (x \times y) \times z$ (associativité de $\times$),
- $x \times y = y \times x$ (commutativité de $\times$),
- $x \times 1_{\mathbb{Z}_p} = x$ (élément neutre pour $\times$),
- $x \times (y + z) = x \times y + x \times z$ (distributivité à gauche de $+$ sur $\times$).

Finalement, $\mathbb{Z}_p$ est un anneau commutatif unitaire.

□

Proposition 1.5. On définit l'application suivante :

$$i : \left\{ \begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ x & \mapsto & (x \mod p^n)_{n\in\mathbb{N}_{\geqslant 1}} \end{array} \right. .$$

i est un morphisme d'anneaux injectif.

Preuve. On vérifie sans peine que i est à valeurs dans $\mathbb{Z}_p$ et que $i(1) = 1_{\mathbb{Z}_p}$. Par ailleurs, quel que soit $(x, y) \in \mathbb{Z}^2$, on a :

- $i(x + y) = i(x) + i(y)$.
- $i(xy) = i(x)i(y)$.

Enfin, on observe que pour tout $x \in \mathbb{Z}$, on a :

$$i(x) = 0_{\mathbb{Z}_p} \Leftrightarrow \forall n \in \mathbb{N}, p^n | x \Leftrightarrow x = 0.$$

D'où le résultat annoncé.

□

Remarque 1.6. D'après la proposition 1.5, $\mathbb{Z}_p$ est de caractéristique 0.

Proposition 1.7. Le groupe des unités des entiers p-adiques, noté ${\mathbb{Z}_p}^\times$, est :

$$ {\mathbb{Z}_p}^\times = \{(x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p \text{ t.q. } x_1 \in (\mathbb{Z}/p\mathbb{Z})^*\}. $$

Preuve. On procède par double inclusion.

- Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in {\mathbb{Z}_p}^\times$, il existe $y := (y_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p$ satisfaisant à :
$$ xy = 1_{\mathbb{Z}_p}. $$
Dès lors, en examinant les termes d'indice 1, il vient :
$$ x_1 y_1 = 1_{\mathbb{Z}/(p)}. $$
Finalement, on a $x_1 \in (\mathbb{Z}/p\mathbb{Z})^*$.
- Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p$ avec $x_1 \in (\mathbb{Z}/p\mathbb{Z})^*$, il existe $y_1 \in \mathbb{Z}/(p)$ tel que :
$$ x_1 y_1 = 1_{\mathbb{Z}/(p)}. $$
Soit $n \in \mathbb{N}_{\geqslant 2}$, supposons avoir construit $(y_k)_{k\in[\![1,n-1]\!]}$ dans $\displaystyle\prod_{k=1}^{n-1} \mathbb{Z}/(p^k)$ satisfaisant aux deux propriétés suivantes :

$$ \forall k \in [\![1, n-1]\!], x_k y_k = 1_{\mathbb{Z}/(p^k)}, \tag{1} $$

$$ \forall (q,r) \in {\mathbb{N}_{\geqslant 1}}^2, q \leqslant r \leqslant n-1, \Rightarrow \varphi_q^r(y_r) = y_q. \tag{2} $$

Soit $\widetilde{x_n}$ un représentant de x_n modulo p^n, comme $\varphi_1^n(x_n) = x_1$, on a :
$$ \widetilde{x_n} \not\equiv 0 \mod p. $$
On en déduit que $\widetilde{x_n}$ et p sont premiers entre-eux. Dès lors, $\widetilde{x_n}$ et p^n sont premiers entre-eux et il existe $\widetilde{y_n} \in \mathbb{Z}$ tel que l'on ait :
$$ \widetilde{x_n}\widetilde{y_n} \equiv 1 \mod p^n. $$
En d'autres termes, il existe $y_n \in \mathbb{Z}/(p^n)$ satisfaisant à l'égalité suivante :

$$ x_n y_n = 1_{\mathbb{Z}/(p^n)}. \tag{3} $$

Soit $m \in \mathbb{N}_{\geqslant 1}, m \leqslant n$, en appliquant le morphisme d'anneaux φ_m^n à (3), on obtient l'égalité suivante :

$$ \varphi_m^n(x_n)\varphi_m^n(y_n) = 1_{\mathbb{Z}/(p^m)}. \tag{4} $$

Par ailleurs, en prenant l'égalité (1) en $k = m$, il vient $x_m y_m = 1_{\mathbb{Z}/(p^m)}$. Dès lors, en rapprochant cette égalité avec (4), il vient :

$$ \varphi_m^n(x_n)\varphi_m^n(y_n) = x_m y_m. \tag{5} $$

Or, $\varphi_m^n(x_n) = x_m$ et injectant cette information dans l'égalité (5), on a :

$$ x_m \varphi_m^n(y_n) = x_m y_m. \tag{6} $$

Finalement, d'après l'égalité (1) prise en $k = m$ ou d'après l'égalité (3), selon que $m < n$ ou $m = n$, en multipliant (6) par y_m, il vient :

$$ \varphi_m^n(y_n) = y_m. \tag{7} $$

En résumé, d'après (1), (2), (3) et (7), on a construit $(y_k)_{k\in[\![1,n]\!]}$ dans $\prod_{k=1}^{n}\mathbb{Z}/(p^k)$ satisfaisant aux deux propriétés suivantes :

$$\forall k \in [\![1,n]\!], x_k y_k = 1_{\mathbb{Z}/(p^k)},$$
$$\forall (q,r) \in {\mathbb{N}_{\geqslant 1}}^2, q \leqslant r \leqslant n, \Rightarrow \varphi_q^r(y_r) = y_q.$$

Finalement, on construit par récurrence un inverse à x dans $\mathbb{Z}_p$.

D'où l'égalité annoncée.

□

Remarque 1.8. Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p$, on a :

$$\forall n \in \mathbb{N}_{\geqslant 2}, \varphi_{n-1}^n(x_n) = x_{n-1}.$$

Par conséquent, p divise x_1 si et seulement si pour tout $n \in \mathbb{N}_{\geqslant 1}$, p divise x_n. En accord avec la proposition 1.7, on a alors :

$${\mathbb{Z}_p}^{\times} = \mathbb{Z}_p \setminus p\mathbb{Z}_p.$$

Proposition 1.9. Quel que soit $x \in {\mathbb{Z}_p}^*$, il existe m un unique entier naturel et ε une unique unité de $\mathbb{Z}_p$ tels que l'on ait la décomposition suivante :

$$x = p^m \varepsilon.$$

Preuve. On montre l'existence et l'unicité séparément.

- Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in {\mathbb{Z}_p}^*$, on distingue les deux cas suivants :
  - Supposons que $x \in {\mathbb{Z}_p}^{\times}$, alors $m = 0$ et $\varepsilon = x$ conviennent.
  - Supposons que $x \notin {\mathbb{Z}_p}^{\times}$, il existe $k \in \mathbb{N}_{\geqslant 1}$ tel que l'on ait $x_k \neq 0_{\mathbb{Z}/(p^k)}$. Soit $\ell \in \mathbb{N}_{\geqslant k}$, comme $\varphi_k^\ell(x_\ell) = x_k$, on a $x_\ell \neq 0_{\mathbb{Z}/(p^\ell)}$ et l'ensemble des indices $n \in \mathbb{N}_{\geqslant 1}$ tels que $x_n = 0_{\mathbb{Z}/(p^n)}$ est majoré par k. Or, d'après la proposition 1.7, $x_1 = 0_{\mathbb{Z}/(p)}$ et on peut alors introduire :

    $$m := \max\left\{n \in \mathbb{N}_{\geqslant 1} \text{ t.q. } x_n = 0_{\mathbb{Z}/(p^n)}\right\}.$$

    Quel que soit $n \in \mathbb{N}_{\geqslant 1}$, on fixe $\widetilde{x_n}$ un représentant de x_n modulo p^n. Soit $n \in \mathbb{N}_{\geqslant 1}$, on constate que l'on a :

    $$\varphi_m^{m+n}(x_{m+n}) = x_m = 0_{\mathbb{Z}/(p^m)}.$$

    Dès lors, p^m divise $\widetilde{x_{n+m}}$ et on introduit l'élément de $\mathbb{Z}/(p^n)$ suivant :

    $$\varepsilon_n := \frac{\widetilde{x_{m+n}}}{p^m} \mod p^n.$$

    On pose $\varepsilon := (\varepsilon_n)_{n\in\mathbb{N}_{\geqslant 1}}$, quel que soit $(q,r) \in {\mathbb{N}_{\geqslant 1}}^2, q \leqslant r$, on a :

    $$\varphi_q^r(\varepsilon_r) = \frac{\widetilde{x_{m+r}}}{p^m} \mod p^q. \tag{8}$$

    Or, comme $\varphi_q^{m+r}(x_{m+r}) = x_q = \varphi_q^{m+q}(x_{m+q})$, il vient :

    $$\widetilde{x_{m+q}} \equiv \widetilde{x_{m+r}} \mod p^q.$$

Dès lors, en réinjectant cette information dans l'égalité (8), on a :

$$\varphi_q^r(\varepsilon_r) = \varepsilon_q.$$

On a $\varepsilon \in \mathbb{Z}_p$ et supposons par l'absurde que $\varepsilon_1 = 0_{\mathbb{Z}/(p)}$, alors on a :

$$x_{m+1} = 0_{\mathbb{Z}/(p^{m+1})}.$$

Dès lors, par définition de m, il vient $m+1 \leqslant m$, ce qui n'est pas. Par conséquent, d'après la proposition 1.7, on a :

$$\varepsilon \in {\mathbb{Z}_p}^{\times}.$$

Enfin, quel que soit $n \in \mathbb{N}_{\geqslant 1}$, on observe que l'on a :

$$p^m \varepsilon_n = \widetilde{x_{m+n}} \mod p^n. \tag{9}$$

Or, comme $\varphi_n^{m+n}(x_{m+n}) = x_n$, il vient :

$$\widetilde{x_{m+n}} \equiv \widetilde{x_n} \mod p^n.$$

En réinjectant cette information dans (9), on a :

$$p^m \varepsilon_n = x_n.$$

Finalement, on a l'égalité suivante avec $m \in \mathbb{N}$ et $\varepsilon \in {\mathbb{Z}_p}^{\times}$:

$$p^m \varepsilon = x.$$

- Soit $x \in {\mathbb{Z}_p}^*$, supposons que l'on dispose de m_1 et m_2 dans $\mathbb{N}$, ainsi que de $\varepsilon_1 := (\varepsilon_{1,n})_{n \in \mathbb{N}_{\geqslant 1}}$ et $\varepsilon_2 := (\varepsilon_{2,n})_{n \in \mathbb{N}_{\geqslant 1}}$ dans ${\mathbb{Z}_p}^{\times}$ tels que l'on ait :

$$x = p^{m_1}\varepsilon_1 \text{ et } x = p^{m_2}\varepsilon_2.$$

Dès lors, on a les égalités suivantes :

$$\forall n \in \mathbb{N}_{\geqslant 1}, p^{m_1}\varepsilon_{1,n} = p^{m_2}\varepsilon_{2,n}. \tag{10}$$

Par conséquent, en prenant $n = m_1$ dans (10), on a :

$$p^{m_2}\varepsilon_{2,m_1} = 0_{\mathbb{Z}/(p^{m_1})}. \tag{11}$$

Or, si $\widetilde{\varepsilon_{2,m_1}}$ est un représentant de ε_{2,m_1} modulo p^{m_1}, alors d'après la remarque 1.8, p ne divise pas $\widetilde{\varepsilon_{2,m_1}}$. On en déduit que p^{m_1} et $\widetilde{\varepsilon_{2,m_1}}$ sont premiers entre eux et que $\varepsilon_{2,m_1} \in (\mathbb{Z}/p^{m_1}\mathbb{Z})^{\times}$. Ainsi, d'après (11), on a :

$$m_2 \geqslant m_1.$$

En reproduisant le même argument en prenant $n = m_2$ dans (10), on a :

$$m := m_1 = m_2.$$

Quel que soit $n \in \mathbb{N}_{\geqslant 1}$, en prenant (10) en $n = n + m$, il vient :

$$p^m \varepsilon_{1,n+m} = p^m \varepsilon_{2,n+m}.$$

On en déduit que les représentants de $\varepsilon_{1,n+m}$ et $\varepsilon_{1,n+m}$ modulo p^{n+m} sont congruents modulo p^n, c'est-à-dire que l'on a :

$$\varphi_n^{m+n}(\varepsilon_{1,n+m}) = \varphi_n^{m+n}(\varepsilon_{2,n+m}).$$

Finalement, on a $\varepsilon_{1,n} = \varepsilon_{2,n}$. D'où l'unicité de la décomposition.

D'où le résultat annoncé.

□

Corollaire 1.10. $\mathbb{Z}_p$ est un anneau intègre.

Preuve. Chacun des $\mathbb{Z}/(p^n), n \in \mathbb{N}_{\geqslant 1}$ étant non nul, on a :

$$0_{\mathbb{Z}_p} \neq 1_{\mathbb{Z}_p}.$$

Soient x et y dans ${\mathbb{Z}_p}^*$, d'après la proposition 1.9, il existe m_x et m_y dans $\mathbb{N}$, ainsi que ε_x et ε_y dans ${\mathbb{Z}_p}^\times$ tels que l'on ait :

$$x = p^{m_x}\varepsilon_x \text{ et } y = p^{m_y}\varepsilon_y.$$

Dès lors, il vient :

$$xy = p^{m_x+m_y}\varepsilon_x\varepsilon_y.$$

On en déduit que $xy \neq 0_{\mathbb{Z}_p}$, sinon on aurait $p^{m_x+m_y} = 0_{\mathbb{Z}_p}$, ce qui n'est pas. Par contraposition, on a alors :

$$\forall (x, y) \in {\mathbb{Z}_p}^2, xy = 0_{\mathbb{Z}_p} \Rightarrow x = 0_{\mathbb{Z}_p} \text{ ou } y = 0_{\mathbb{Z}_p}.$$

Finalement, $\mathbb{Z}_p$ est un anneau intègre.

□

Définition 1.11. On appelle corps des nombres p-adiques et l'on note $\mathbb{Q}_p$ le corps des fractions de l'anneau intègre $\mathbb{Z}_p$.

Remarque 1.12. D'après la remarque 1.6, $\mathbb{Q}_p$ est de caractéristique 0.

Proposition 1.13. Il existe un unique morphisme d'anneaux injectif de $\mathbb{Q}$ dans $\mathbb{Q}_p$ qui prolonge i, on le note $j : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Preuve. On note $i_1 : \mathbb{Z} \hookrightarrow \mathbb{Q}$, respectivement $i_2 : \mathbb{Z}_p \hookrightarrow \mathbb{Q}_p$, le plongement canonique de l'anneau $\mathbb{Z}$, respectivement de $\mathbb{Z}_p$, dans son corps des fractions. Dès lors, d'après la proposition 1.5, on a le diagramme suivant :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad i \quad} & \mathbb{Z}_p \\ \downarrow{\scriptstyle i_1} & \searrow & \downarrow{\scriptstyle i_2} \\ K(\mathbb{Z}) = \mathbb{Q} & & K(\mathbb{Z}_p) = \mathbb{Q}_p \end{array} .$$

Finalement, par propriété universelle du corps des fractions de $\mathbb{Z}$, il existe un unique morphisme d'anneaux injectif $j : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$ tel que :

$$j \circ i_1 = i_2 \circ i.$$

En pensant à i_1 et i_2 comme à des inclusions, on a le résultat annoncé.

□

Proposition 1.14. $\mathbb{Q}_p$ est engendré par $\dfrac{1}{p}$ sur $\mathbb{Z}_p$, c'est-à-dire que l'on a :

$$\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right].$$

Preuve. D'après la remarque 1.8, un élément de $\mathbb{Z}_p$ est non inversible si et seulement s'il appartient à $p\mathbb{Z}_p$. Dès lors, $\mathbb{Q}_p$ est le localisé de $\mathbb{Z}_p$ en $p\mathbb{Z}_p$. Finalement, $p\mathbb{Z}_p$ étant engendré par p, on a l'égalité annoncée.

□

Proposition 1.15. Quel que soit $x \in {\mathbb{Q}_p}^*$, il existe m un unique entier relatif et ε une unique unité de $\mathbb{Z}_p$ tels que l'on ait la décomposition suivante :

$$x = p^m \varepsilon.$$

Preuve. On montre l'existence et l'unicité séparément.

- Soit $x \in {\mathbb{Q}_p}^*$, d'après la proposition 1.14, il existe $P \in \mathbb{Z}_p[X]$ de degré n satisfaisant à l'égalité suivante :

  $$x = P\left(\frac{1}{p}\right).$$

  En réduisant chaque fraction de cette identité au même dénominateur, on obtient $a \in \mathbb{Z}_p$ tel que l'on ait :

  $$x = \frac{a}{p^n}.$$

  Comme $x \in {\mathbb{Q}_p}^*$, $a \in {\mathbb{Z}_p}^*$ et d'après la proposition 1.9, il existe $n' \in \mathbb{N}$ et $\varepsilon \in {\mathbb{Z}_p}^\times$ tel que $a = p^{n'}\varepsilon$. Finalement, en posant $m := n' - n \in \mathbb{Z}$, on a :

  $$x = p^m \varepsilon.$$

- Soit $x \in {\mathbb{Q}_p}^*$, supposons qu'il existe m_1 et m_2 dans $\mathbb{Z}$, ainsi que ε_1 et ε_2 dans ${\mathbb{Z}_p}^\times$ satisfaisants à :

  $$x = p^{m_1}\varepsilon_1 \text{ et } x = p^{m_2}\varepsilon_2.$$

  On commence par observer que m_1 et m_2 ont même signe ; en effet, sinon x serait à la fois dans $\mathbb{Z}_p$ et $\mathbb{Q}_p \setminus \mathbb{Z}_p$, ce qui ne peut être.

  - Supposons que m_1 et m_2 soient tous les deux positifs, alors d'après la proposition 1.9, on a $m_1 = m_2$ et $\varepsilon_1 = \varepsilon_2$.
  - Supposons que m_1 et m_2 soient tous les deux négatifs, alors, on a :

    $$p^{-m_2}\varepsilon_1 = p^{-m_2}\varepsilon_2.$$

    $-m_1$ et $-m_2$ étant tous les deux positifs, d'après la proposition 1.9, on a $-m_1 = -m_2$ et $\varepsilon_1 = \varepsilon_2$.

D'où le résultat annoncé.

□

1.2. **Topologie élémentaire du corps des nombres p-adiques.**

Définition 1.16. On appelle valuation p-adique et on note $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ l'application définie par :

- $v_p(0) := \infty$.
- Si $x \in {\mathbb{Q}_p}^*$, d'après la proposition 1.15, il existe m un unique entier relatif et ε une unique unité de $\mathbb{Z}_p$ tels que l'on ait :

  $$x = p^m \varepsilon.$$

  On pose alors $v_p(x) := m$.

Remarque 1.17. Soit $x \in {\mathbb{Q}_p}^*$, il existe $\varepsilon \in {\mathbb{Z}_p}^\times$ satisfaisant à $x = p^{v_p(x)}\varepsilon$. La valuation p-adique de x est le plus grand entier relatif m tel que $x \in p^m\mathbb{Z}_p$. En effet, on a $x \in p^{v_p(x)}\mathbb{Z}_p$ et si l'on avait $x \in p^{v_p(x)+1}\mathbb{Z}_p$, alors $\varepsilon \in p\mathbb{Z}_p$, ce qui d'après la proposition 1.7 et la remarque 1.8 contredirait que ε soit dans ${\mathbb{Z}_p}^\times$. On en déduit les interprétations suivantes de la valuation p-adique :

- Si $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in {\mathbb{Z}_p}^*$, alors $v_p(x) = \max\left\{n \in \mathbb{N}_{\geqslant 1} \text{ t.q. } x_n = 0_{\mathbb{Z}/(p^n)}\right\}$.
- Si $x \in \mathbb{Z}^*$, alors avec la proposition 1.5, $v_p(x) = \max\left\{n \in \mathbb{N}_{\geqslant 1} \text{ t.q. } p^n | x\right\}$.

Proposition 1.18. Quels que soient x et y dans $\mathbb{Q}_p$, on a :

i. $v_p(x) = \infty$ si et seulement si $x = 0$.

ii. $v_p(xy) = v_p(x) + v_p(y)$.

iii. $v_p(x + y) \geqslant \min(v_p(x), v_p(y))$ avec égalité si $v_p(x) \neq v_p(y)$.

Preuve. On montre indépendamment chaque propriété.

i. Cette propriété découle immédiatement de la définition 1.16.

ii. On distingue les deux cas suivants sur x et y :
   - Supposons que x ou y soit nul, alors l'égalité est vraie.
   - Supposons que x et y soient non nuls, il existe $\varepsilon_x, \varepsilon_y \in {\mathbb{Z}_p}^\times$ tels que :
   $$x = p^{v_p(x)}\varepsilon_x \text{ et } y = p^{v_p(y)}\varepsilon_y.$$
   Par conséquent, on a :
   $$xy = p^{v_p(x)+v_p(y)}\varepsilon_x\varepsilon_y.$$
   Comme $\varepsilon_x\varepsilon_y \in {\mathbb{Z}_p}^\times$, d'après la définition 1.16, il vient :
   $$v_p(xy) = v_p(x) + v_p(y).$$

iii. On distingue les deux cas suivants sur x et y :
   - Supposons que x ou y soit nul, alors la propriété est vraie.
   - Supposons que x et y soient non nuls, il existe $\varepsilon_x, \varepsilon_y \in {\mathbb{Z}_p}^\times$ tels que :
   $$x = p^{v_p(x)}\varepsilon_x \text{ et } y = p^{v_p(y)}\varepsilon_y.$$
   On suppose sans perte de généralité que $v_p(x) \leqslant v_p(y)$, on a alors :
   $$x + y = p^{v_p(x)}\left(\varepsilon_x + p^{v_p(y)-v_p(x)}\varepsilon_y\right). \tag{12}$$
   Or, on a $p^{v_p(y)-v_p(x)}\varepsilon_y \in \mathbb{Z}_p$ et d'après (12), il vient :
   $$x + y \in p^{v_p(x)}\mathbb{Z}_p. \tag{13}$$
   Dès lors, d'après la remarque 1.17, on a :
   $$v_p(x + y) \geqslant v_p(x).$$
   Supposons désormais que $v_p(x) < v_p(y)$, alors on a :
   $$p^{v_p(y)-v_p(x)}\varepsilon_y \in p\mathbb{Z}_p. \tag{14}$$

Si par l'absurde $x+y \in p^{v_p(x)+1}\mathbb{Z}_p$, alors d'après (12), on a :

$$\varepsilon_x + p^{v_p(y)-v_p(x)}\varepsilon_y \in p\mathbb{Z}_p.$$

Ainsi, d'après (14), on a $\varepsilon_x \in p\mathbb{Z}_p$, ce qui d'après la proposition 1.15 contredit $\varepsilon_x \in {\mathbb{Z}_p}^\times$ et on en déduit que l'on a :

$$x+y \notin p^{v_p(x)+1}\mathbb{Z}_p. \tag{15}$$

Finalement, d'après (13), (15) et la remarque 1.17, on a :

$$v_p(x+y) = v_p(x).$$

D'où le résultat annoncé.

□

Définition 1.19. On appelle norme p-adique et on note $|\cdot|_p : \mathbb{Q}_p \to [0,+\infty[$ l'application définie par :

- $\left|0_{\mathbb{Q}_p}\right|_p = 0$.
- Si $x \in {\mathbb{Q}_p}^*$, on pose $|x|_p := p^{-v_p(x)}$.

Remarque 1.20. D'après la proposition 1.9 et la définition 1.19, on a :

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \text{ t.q. } |x|_p \leqslant 1\}.$$

Proposition 1.21. Quels que soient x et y dans $\mathbb{Q}_p$, on a :

i. $|x|_p = 0$ si et seulement si $x = 0$.

ii. $|xy|_p = |x|_p|y|_p$.

iii. $|x+y|_p \leqslant \max(|x|_p, |y|_p)$ avec égalité si $|x|_p \neq |y|_p$.

Preuve. Ses propriétés se déduisent de la proposition 1.18 par exponentiation et en remarquant que quel que soit $(a,b) \in \mathbb{R}^2$, on a :

$$-\min(a,b) = \max(-a,-b),$$
$$p^{\max(a,b)} = \max(p^a, p^b).$$

□

Définition 1.22. On appelle distance p-adique et on note $\delta_p : {\mathbb{Q}_p}^2 \to [0,+\infty[$ l'application définie par :

$$\forall (x,y) \in {\mathbb{Q}_p}^2, \delta_p(x,y) := |x-y|_p.$$

Proposition 1.23. $\mathbb{Q}_p$ muni de δ_p est un espace ultramétrique.

Preuve. Quel que soit $(x,y,z) \in {\mathbb{Q}_p}^3$, on a :

- (séparation) D'après le point i. de la proposition 1.21, on a :
$$\delta_p(x,y) = 0 \Leftrightarrow x = y.$$
- (symétrie) D'après le point ii. de la proposition 1.21, on a :
$$\delta_p(x,y) = \delta_p(y,x).$$

- (inégalité ultramétrique) On commence par écrire :

$$x - z = (x - y) + (y - z).$$

D'après le point iii. de la proposition 1.21 et le point précédent, on a :

$$\delta_p(x, z) \leqslant \max(\delta_p(x, y), \delta_p(y, z)).$$

Finalement, $(\mathbb{Q}_p, \delta_p)$ est un espace ultramétrique.

□

Proposition 1.24. On note $\mathscr{T}$ la topologie produit sur $\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)$ associée aux topologies discrètes sur chacun des $\mathbb{Z}/(p^n), n \in \mathbb{N}_{\geqslant 1}$. La topologie induite par $\mathscr{T}$ sur $\mathbb{Z}_p$ et la topologie associée à la restriction de δ_p sur $\mathbb{Z}_p$ sont égales.

Preuve. Soient $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p, \varepsilon \in \mathbb{R}_{>0}$ et $y := (y_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \mathbb{Z}_p$, on a :

$$y \in B_{\delta_p}(x, \varepsilon) \Leftrightarrow v_p(x - y) > -\log_p(\varepsilon). \tag{16}$$

Or, en posant $m := \lfloor -\log_p(\varepsilon) \rfloor$, d'après la remarque 1.17, on a :

$$v_p(x - y) > -\log_p(\varepsilon) \Leftrightarrow \forall n \in \mathbb{N}_{\geqslant 1}, n \leqslant m \Rightarrow x_n = y_n. \tag{17}$$

Dès lors, d'après (16) et (17), il vient :

$$y \in B_{\delta_p}(x, \varepsilon) \Leftrightarrow \forall n \in \mathbb{N}_{\geqslant 1}, n \leqslant m \Rightarrow x_n = y_n.$$

Finalement, on en déduit que l'on a :

$$B_{\delta_p}(x, \varepsilon) = \left(\prod_{n=1}^{m} \{x_n\} \times \prod_{n\geqslant n_0} \mathbb{Z}/(p^n) \right) \cap \mathbb{Z}_p.$$

Or, l'ensemble suivant constitue une base de voisinages ouverts de $\left(\mathbb{Z}_p, \mathscr{T}_{|\mathbb{Z}_p}\right)$:

$$\left\{ \left(\prod_{n=1}^{m} \{x_n\} \times \prod_{n\geqslant m} \mathbb{Z}/(p^n) \right) \cap \mathbb{Z}_p, m \in \mathbb{N}_{\geqslant 1}, (x_n)_{n\in[\![1,m]\!]} \in \prod_{n=1}^{m} \mathbb{Z}/(p^n) \right\}$$

et celui ci-dessous est quant à lui une base de voisinages ouverts de $(\mathbb{Z}_p, \delta_p)$:

$$\left\{ B_{\delta_p}(x, \varepsilon), x \in \mathbb{Z}_p, \varepsilon \in \mathbb{R}_{>0} \right\}.$$

D'où le résultat annoncé.

□

Proposition 1.25. $i(\mathbb{N})$ est une partie dense de $\mathbb{Z}_p$.

Preuve. Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}}$ dans $\mathbb{Z}_p$, quel que soit $n \in \mathbb{N}_{\geqslant 1}$, on se donne y_n un représentant positif de x_n modulo p^n, en accord avec la proposition 1.5, on a :

$$x_n - i(y_n)_n = 0_{\mathbb{Z}/(p^n)}.$$

Or, d'après la remarque 1.17, on a :

$$v_p(x - i(y_n)) = \max \left\{ m \in \mathbb{N}_{\geqslant 1} \text{ t.q. } x_m - i(y_n)_m = 0_{\mathbb{Z}/(p^m)} \right\}.$$

Par conséquent, $v_p(x - i(y_n)) \geqslant n$ et on en déduit l'inégalité suivante :

$$\delta_p(x, i(y_n)) \leqslant p^{-n}.$$

En passant à la limite quand n tend vers $+\infty$, il vient :

$$\lim_{n\to+\infty} \delta_p(x, i(y_n)) = 0.$$

Finalement, on a $\lim_{n\to+\infty} i(y_n) = x$. D'où le résultat annoncé.

□

Proposition 1.26. $j(\mathbb{Q})$ est une partie dense de $\mathbb{Q}_p$.

Preuve. Soit $x \in \mathbb{Z}_p$, il existe $(a, b) \in \mathbb{Z}_p \times {\mathbb{Z}_p}^*$ satisfaisant à :

$$x = ab^{-1}. \tag{18}$$

D'après la proposition 1.25, il existe $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ dans ${\mathbb{Z}_p}^{\mathbb{N}}$ telles que :

$$\lim_{n\to+\infty} i(a_n) = a \text{ et } \lim_{n\to+\infty} i(b_n) = b. \tag{19}$$

En particulier, il existe $N \in \mathbb{N}$ tel que l'on ait :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow i(b_n) \in B_{\delta_p}(b, \varepsilon). \tag{20}$$

Or, b étant non nul, il existe $\varepsilon \in \mathbb{R}_{>0}$ satisfaisant à :

$$0 \notin B_{\delta_p}(b, \varepsilon). \tag{21}$$

Ainsi, i étant injectif (proposition 1.5), d'après (20) et (21), on a :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow b_n \neq 0.$$

Quel que soit $n \in \mathbb{N}_{\geqslant N}$ on est alors en mesure de définir l'élément de $\mathbb{Q}$ suivant :

$$x_n := \frac{a_n}{b_n}.$$

Dès lors, d'après la proposition 1.13, on a :

$$\forall n \in \mathbb{N}_{\geqslant N}, j(x_n) = j(a_n)j(b_n)^{-1} = i(a_n)i(b_n)^{-1}. \tag{22}$$

Finalement, d'après (18), (19) et (22), on a :

$$\lim_{n\to+\infty} j(x_n) = x.$$

D'où le résultat annoncé.

□

Lemme 1.27. $\mathbb{Z}_p$ est fermé dans $\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)$ muni de $\mathscr{T}$.

Preuve. Soit $x := (x_n)_{n\in\mathbb{N}_{\geqslant 1}} \in \left(\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)\right) \setminus \mathbb{Z}_p$, on dispose de m et n des entiers naturels au moins égaux à 1 tels que $m \leqslant n$ et satisfaisants à :

$$\varphi_m^n(x_n) \neq x_m.$$

On introduit alors l'ensemble suivant :

$$V := \prod_{k=1}^{n} \{x_n\} \times \prod_{k\geqslant n+1} \mathbb{Z}/(p^k).$$

V est un ouvert de $\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)$ qui contient x et tel que $V \cap \mathbb{Z}_p = \varnothing$. Finalement, V est un voisinage ouvert de x dans $\left(\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)\right) \setminus \mathbb{Z}_p$ et $\left(\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)\right) \setminus \mathbb{Z}_p$ est ouvert dans $\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)$, d'où le résultat annoncé.

□

Proposition 1.28. $\mathbb{Z}_p$ est compact dans $\mathbb{Q}_p$.

Preuve. Quel que soit $n \in \mathbb{N}_{\geqslant 1}$, $\mathbb{Z}/(p^n)$ étant fini, il est compact pour la topologie discrète. Dès lors, d'après le théorème de Tychonoff, $\prod_{n\in\mathbb{N}_{\geqslant 1}} \mathbb{Z}/(p^n)$ muni de $\mathscr{T}$ est compact. Ainsi, d'après le lemme 1.27, $\left(\mathbb{Z}_p, \mathscr{T}_{|\mathbb{Z}_p}\right)$ est compact. Finalement, d'après la proposition 1.24, $(\mathbb{Z}_p, \delta_p)$ est compact.

□

Corollaire 1.29. L'espace métrique $\mathbb{Z}_p$ est complet.

Proposition 1.30. L'espace métrique $\mathbb{Q}_p$ est complet.

Preuve. Soit $(x_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{\mathbb{N}}$ une suite de Cauchy, il existe $N \in \mathbb{N}$ tel que :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow |x_n - x_N| \leqslant 1.$$

Dès lors, d'après la remarque 1.20, on a :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow x_n - x_N \in \mathbb{Z}_p.$$

Comme $(x_n)_{n\in\mathbb{N}}$ est une suite de Cauchy, $(x_n - x_N)_{n\geqslant N} \in {\mathbb{Z}_p}^{\mathbb{N}}$ l'est également. Par conséquent, d'après la proposition 1.29, $(x_n - x_N)_{n\geqslant N}$ converge vers $x \in \mathbb{Z}_p$. Finalement, $(x_n)_{n\in\mathbb{N}}$ converge vers $x + x_N$ dans $\mathbb{Q}_p$. D'où le résultat annoncé.

□

Remarque 1.31. En accord avec les propositions 1.26 et 1.30, $\mathbb{Q}_p$ est obtenu par complétion de $\mathbb{Q}$ pour la distance δ_p.

1.3. Étude des zéros des séries entières à coefficients p-adiques.

Définition 1.32. Soit $(a_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{\mathbb{N}}$, on appelle série entière formelle en l'indéterminée X de terme général $(a_n)_{n\in\mathbb{N}}$ la série $\sum a_n X^n$.

Notation 1.33. L'ensemble des séries entières formelles en l'indéterminée X et à coefficients dans $\mathbb{Q}_p$ est noté $\mathbb{Q}_p[[X]]$.

Définition 1.34. Soient $f \in \mathbb{Q}_p[[X]]$ de terme général $(a_n)_{n\in\mathbb{N}}$ et $x \in \mathbb{Q}_p$, on dit que f est convergente en x si et seulement si la série $\sum a_n x^n$ est convergente.

Proposition 1.35. Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{Q}_p$, la série $\sum a_n$ est convergente si et seulement si $(a_n)_{n\in\mathbb{N}}$ converge vers 0. Le cas échéant, on a :

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p \leqslant \max_{n\in\mathbb{N}} |a_n|_p.$$

Preuve. On introduit la suite des sommes partielles de $\sum a_n$:

$$(A_n)_{n\in\mathbb{N}} := \left(\sum_{k=0}^{n} a_k\right)_{n\in\mathbb{N}}.$$

On procède alors par double implication.

- Supposons que la série $\sum a_n$ soit convergente, alors $(A_n)_{n\in\mathbb{N}}$ converge. Or, on observe que l'on a :

$$\forall n \in \mathbb{N}, a_n = A_n - A_{n-1}.$$

  Finalement, en passant à la limite quand n tend vers $+\infty$, il vient :

$$\lim_{n\to+\infty} a_n = 0.$$

- Supposons que la suite $(a_n)_{n\in\mathbb{N}}$ converge vers 0, on observe que l'on a :

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}_{\geqslant 1}, \delta_p(A_m, A_{m+n}) \leqslant \left|\sum_{k=m+1}^{m+n} a_k\right|_p. \tag{23}$$

  Or, d'après la proposition 1.23, on a :

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}_{\geqslant 1}, \left|\sum_{k=m+1}^{m+n} a_k\right|_p \leqslant \max_{k\in[\![m+1,m+n]\!]} |a_k|_p \tag{24}$$

  Dès lors, d'après (23) et (24), il vient :

$$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}_{\geqslant 1}, \delta_p(A_m, A_{m+n}) \leqslant \max_{k\in[\![m+1,n]\!]} |a_k|_p. \tag{25}$$

  Soit $\varepsilon \in \mathbb{R}_{>0}$, comme $(a_n)_{n\in\mathbb{N}}$ converge vers 0, il existe $N \in \mathbb{N}$ tel que :

$$\forall m \in \mathbb{N}, m \geqslant N \Rightarrow |a_k|_p \leqslant \varepsilon.$$

  En particulier, on en déduit que l'on a :

$$\forall m \in \mathbb{N}, m \geqslant N, \forall n \in \mathbb{N}_{\geqslant 1}, \max_{k\in[\![m+1,m+n]\!]} |a_k|_p \leqslant \varepsilon. \tag{26}$$

  Dès lors, d'après (25) et (26), il vient :

$$\forall m \in \mathbb{N}, m \geqslant N, \forall n \in \mathbb{N}_{\geqslant 1}, \delta_p(A_m, A_{m+n}) \leqslant \varepsilon.$$

  $(A_n)_{n\in\mathbb{N}}$ est de Cauchy et d'après la proposition 1.30, $(A_n)_{n\in\mathbb{N}}$ converge. Finalement, $\sum a_n$ est convergente.

Supposons que $(a_n)_{n\in\mathbb{N}}$ converge vers 0, alors d'après ce qui précède $\sum a_n$ est convergente. Or, d'après le point iii. de la proposition 1.21, $|\cdot|_p$ est continue (1-lipschitzienne) et l'on en déduit l'égalité suivante :

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p = \lim_{n\to+\infty} \left|\sum_{k=0}^{n} a_k\right|_p. \tag{27}$$

Or, d'après la proposition 1.23, on a :

$$\forall n \in \mathbb{N}, \left|\sum_{k=0}^{n} a_k\right|_p \leqslant \max_{k\in[\![0,n]\!]} |a_k|_p. \tag{28}$$

$(a_n)_{n\in\mathbb{N}}$ convergeant vers 0, elle est bornée et il existe $N \in \mathbb{N}$ tel que l'on ait :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow |a_n|_p \leqslant \max_{k\in\mathbb{N}} |a_k|_p.$$

Par conséquent, on en déduit que l'on a :

$$\max_{k\in\mathbb{N}} |a_k|_p = \max_{k\in[\![0,N]\!]} |a_k|_p.$$

Dès lors, d'après (28), on a :

$$\forall n \in \mathbb{N}, n \geqslant N \Rightarrow \left|\sum_{k=0}^{n} a_k\right|_p \leqslant \max_{n\in\mathbb{N}} |a_n|_p. \tag{29}$$

Finalement, d'après (27) et par passage à la limite dans (29), on a :

$$\left|\sum_{n=0}^{+\infty} a_n\right|_p \leqslant \max_{n\in\mathbb{N}} |a_n|_p.$$

□

Proposition 1.36. Soit $(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ une suite double d'éléments de $\mathbb{Q}_p$ telle que $\lim\limits_{\max(i,j)\to+\infty} a_{i,j} = 0$, alors les séries $\sum\limits_i \sum\limits_j a_{i,j}$ et $\sum\limits_j \sum\limits_i a_{i,j}$ sont convergentes dans $\mathbb{Q}_p$ et convergent vers la même limite.

Preuve. Soit $i \in \mathbb{N}$, comme $\lim\limits_{j\to+\infty} \max(i,j) = +\infty$, on a :

$$\lim_{j\to+\infty} a_{i,j} = 0.$$

Par conséquent, d'après la proposition 1.35, $\sum\limits_j a_{i,j}$ est convergente et l'on a :

$$\left|\sum_{j=0}^{+\infty} a_{i,j}\right|_p \leqslant \max_{j\in\mathbb{N}} |a_{i,j}|_p.$$

Or, quel que soit $j \in \mathbb{N}$, $\lim\limits_{i\to+\infty} \max(i,j) = +\infty$, d'où $\lim\limits_{i\to+\infty} |a_{i,j}| = 0$ et l'on a :

$$\lim_{i\to+\infty} \max_{j\in\mathbb{N}} |a_{i,j}|_p = 0.$$

Dès lors, $\lim\limits_{i\to+\infty} \sum\limits_{j=0}^{+\infty} a_{i,j} = 0$ et d'après la proposition 1.35, $\sum\limits_i \sum\limits_j a_{i,j}$ converge.
De la même manière, on montre que $\sum\limits_j \sum\limits_i a_{i,j}$ est convergente.

Soit $\varepsilon \in \mathbb{R}_{>0}$, il existe $N \in \mathbb{N}$ tel que l'on ait :

$$\forall (i,j) \in \mathbb{N}^2, \max(i,j) \geqslant N \Rightarrow |a_{i,j}|_p \leqslant \varepsilon.$$

Dès lors, d'après la proposition 1.35, on a :

$$\left|\sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty}a_{i,j}-\sum_{i=0}^{N}\sum_{j=0}^{N}a_{i,j}\right|_p=\left|\sum_{\substack{i\\ \max(i,j)>N}}\sum_{j}a_{i,j}\right|_p\leqslant\max_{\substack{(i,j)\in\mathbb{N}^2\\ \max(i,j)>N}}|a_{i,j}|_p\leqslant\varepsilon, \tag{30}$$

$$\left|\sum_{j=0}^{+\infty}\sum_{i=0}^{+\infty}a_{i,j}-\sum_{j=0}^{N}\sum_{i=0}^{N}a_{i,j}\right|_p=\left|\sum_{\substack{j\\ \max(i,j)>N}}\sum_{i}a_{i,j}\right|_p\leqslant\max_{\substack{(i,j)\in\mathbb{N}^2\\ \max(i,j)>N}}|a_{i,j}|_p\leqslant\varepsilon. \tag{31}$$

L'ordre de sommation des sommes finies n'ayant pas d'importance, on a :

$$\left|\sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty}a_{i,j}-\sum_{j=0}^{+\infty}\sum_{i=0}^{+\infty}a_{i,j}\right|_p=\left|\sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty}a_{i,j}-\sum_{i=0}^{N}\sum_{j=0}^{N}a_{i,j}-\sum_{j=0}^{+\infty}\sum_{i=0}^{+\infty}a_{i,j}+\sum_{j=0}^{N}\sum_{i=0}^{N}a_{i,j}\right|_p.$$

Ainsi, d'après le point iii. de la proposition 1.21, (30) et (31), il vient :

$$\left|\sum_{i=0}^{+\infty}\sum_{j=0}^{+\infty}a_{i,j}-\sum_{j=0}^{+\infty}\sum_{i=0}^{+\infty}a_{i,j}\right|_p\leqslant\varepsilon.$$

D'où le résultat annoncé.

□

Théorème 1.37. (Strassmann [16]) Soit $f\in\mathbb{Q}_p[[X]]$ de terme général $(a_n)_{n\in\mathbb{N}}$. Si $(a_n)_{n\in\mathbb{N}}$ est non nulle et converge vers 0, alors f converge sur $\mathbb{Z}_p$ et l'on a :

$$\#\{x\in\mathbb{Z}_p\text{ t.q. }f(x)=0\}\leqslant\max\left\{n\in\mathbb{N}\text{ t.q. }|a_n|_p=\max_{k\in\mathbb{N}}|a_k|_p\right\}<\infty.$$

Preuve. D'après la remarque 1.20 et le point ii. de la proposition 1.21, on a :

$$\forall x\in\mathbb{Z}_p,\forall n\in\mathbb{N},|a_nx^n|_p\leqslant|a_n|_p.$$

Dès lors, on en déduit que l'on a :

$$\forall x\in\mathbb{Z}_p,\lim_{n\to+\infty}a_nx^n=0.$$

Finalement, d'après la définition 1.34 et la proposition 1.35, f converge sur $\mathbb{Z}_p$.

$(a_n)_{n\in\mathbb{N}}$ convergeant vers 0, elle est bornée et il existe $N\in\mathbb{N}$ tel que :

$$\forall n\in\mathbb{N},n\geqslant N\Rightarrow|a_n|_p\leqslant\max_{k\in\mathbb{N}}|a_k|_p.$$

On peut alors définir l'entier naturel suivant :

$$M:=\max\left\{n\in\mathbb{N}\text{ t.q. }|a_n|_p=\max_{k\in\mathbb{N}}|a_k|_p\right\}.$$

On procède alors par récurrence sur M.

- **Initialisation.** Si $M = 0$, alors par construction de M, on a :

$$\forall n \in \mathbb{N}, n \geqslant 1 \Rightarrow |a_n|_p < |a_0|_p. \tag{32}$$

S'il existait $x \in \mathbb{Z}_p$ tel que $f(x) = 0$, on aurait l'égalité suivante :

$$a_0 = -\sum_{n=1}^{+\infty} a_n x^n.$$

Dès lors, d'après la remarque 1.20, le point ii. de la proposition 1.21, la proposition 1.35 et l'inégalité (32), il viendrait :

$$|a_0|_p \leqslant \max_{n \in \mathbb{N}_{\geqslant 1}} |a_n|_p < |a_0|_p,$$

ce qui ne peut être. Finalement, f ne s'annule pas dans $\mathbb{Z}_p$.

- **Hérédité.** Si $M \geqslant 1$, on distingue les deux cas suivants sur f :
  - Si f ne s'annule pas dans $\mathbb{Z}_p$, alors f a au plus M zéros dans $\mathbb{Z}_p$.
  - S'il existe $y \in \mathbb{Z}_p$ tel que $f(y) = 0$, alors, on a :

$$\forall x \in \mathbb{Z}_p, f(x) = f(x) - f(y) = \sum_{n=1}^{+\infty} a_n (x^n - y^n). \tag{33}$$

Or, on rappelle que quel que soit $x \in \mathbb{Z}_p$, on a l'identité suivante :

$$\forall n \in \mathbb{N}_{\geqslant 1}, x^n - y^n = (x - y) \sum_{k=0}^{n-1} x^k y^{n-k-1}. \tag{34}$$

Dès lors, quel que soit $x \in \mathbb{Z}_p$, on définit $\alpha(x) \in {\mathbb{Q}_p}^{\mathbb{N}^2}$ par :

$$\forall (i,j) \in \mathbb{N}^2, \alpha(x)_{i,j} = \begin{cases} a_i x^j y^{i-j-1} & \text{, si } i \geqslant 1 \text{ et } j < i \\ 0 & \text{, sinon.} \end{cases}.$$

De cette manière, d'après (33) et (34), on a l'égalité suivante :

$$\forall x \in \mathbb{Z}_p, f(x) = (x - y) \sum_{m=0}^{+\infty} \sum_{n=0}^{+\infty} \alpha(x)_{m,n}. \tag{35}$$

D'après la remarque 1.20 et le point ii. de la proposition 1.21, on a :

$$\forall x \in \mathbb{Z}_p, \forall (i,j) \in \mathbb{N}^2, |\alpha(x)_{i,j}|_p \leqslant |a_i|_p.$$

Dès lors, quel que soit $x \in \mathbb{Z}_p$, on a :

$$\forall j \in \mathbb{N}, \lim_{i \to +\infty} |\alpha(x)_{i,j}|_p = 0.$$

Par ailleurs, on constate que quel que soit $x \in \mathbb{Z}_p$, on a :

$$\forall i \in \mathbb{N}, \lim_{j \to +\infty} |\alpha(x)_{i,j}|_p = 0.$$

Par conséquent, d'après la proposition 1.36 et l'égalité (35), il vient :

$$f(x) = (x - y) \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} \alpha(x)_{m,n}.$$

On en déduit l'égalité suivante :

$$\forall x \in \mathbb{Z}_p, f(x) = (x-y)\sum_{n=1}^{+\infty} x^n \sum_{m=n+1}^{+\infty} a_m y^{m-n-1}. \tag{36}$$

On pose $b_0 := 0$ et quel que soit $n \in \mathbb{N}_{\geqslant 1}$, on définit l'élément suivant :

$$b_n := \sum_{m=n+1}^{+\infty} a_m y^{m-n-1}.$$

Soit g la série entière de terme général $(b_n)_{n\in\mathbb{N}}$, d'après (36), on a :

$$\forall x \in \mathbb{Z}_p, f(x) = (x-y)g(x). \tag{37}$$

En outre, d'après la remarque 1.20, le point ii. de la proposition 1.21, la proposition 1.35 et par construction de M, on a :

$$\forall n \in \mathbb{N}, |b_n|_p \leqslant \max_{m\geqslant n+1} |a_m|_p \leqslant |a_M|_p. \tag{38}$$

Par ailleurs, par construction de M, on a également :

$$\forall n \in \mathbb{N}, n \geqslant M+1 \Rightarrow |a_n|_p < |a_M|_p. \tag{39}$$

Dès lors, d'après la remarque 1.20, le point ii. de la proposition 1.21, la proposition 1.35 et l'inégalité (39), on a :

$$\left|\sum_{m=M+1} a_m y^{m-M}\right|_p \leqslant \max_{m\geqslant M+1} |a_n|_p < |a_M|_p.$$

Par conséquent, d'après le point iii. de la proposition 1.21, il vient :

$$|b_{M-1}|_p = \max\left(|a_M|_p, \left|\sum_{m=M+1} a_m y^{m-M}\right|_p\right) = |a_M|_p. \tag{40}$$

Enfin, d'après les inégalités (38) et (39), on a :

$$\forall n \in \mathbb{N}, n > M-1 \Rightarrow |b_n|_p < |a_M|_p. \tag{41}$$

Dès lors, d'après (38), (40) et (41), on a :

$$\max\left\{n \in \mathbb{N} \text{ t.q. } |b_n|_p = \max_{k\in\mathbb{N}} |b_k|_p\right\} = M-1.$$

Ainsi, par hypothèse de récurrence, g a au plus $M-1$ zéros dans $\mathbb{Z}_p$. Finalement, d'après (37), f a au plus M zéros dans $\mathbb{Z}_p$.

D'où le résultat annoncé.

□

Remarque 1.38. Le théorème 1.37 est l'analogue p-adique du théorème de Rouché sur les zéros des fonctions holomorphes dans un disque.

2. Interpolation p-adique des itérés de fonctions polynomiales

Soient p un nombre premier quelconque, $d \in \mathbb{N}_{\geqslant 1}$ et $f \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$. On introduit $I := (X_1, \cdots, X_d)$ et on montre que s'il existe une puissance de p suffisamment grande divisant les coefficients de chacune des composantes polynomiales de $f - I$, alors on peut interpoler à $\mathbb{Z}_p$ les itérés de f prises en un point fixé de ${\mathbb{Z}_p}^d$. Autrement dit, sous ces hypothèses, quel que soit $x \in {\mathbb{Z}_p}^d$, on exhibera $g \in \mathbb{Q}_p[[X]]^d$ qui converge sur $\mathbb{Z}_p$ et satisfaisant à :

$$\forall n \in \mathbb{N}, g(n) = f^n(x).$$

L'unicité d'un telle fonction est assurée par la proposition suivante :

Proposition 2.1. Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'élements de $\mathbb{Q}_p$, il existe au plus une fonction continue $f : \mathbb{Z}_p \to \mathbb{Q}_p$ satisfaisant à :

$$\forall n \in \mathbb{N}, f(n) = u_n.$$

Preuve. $\mathbb{N}$ étant dense dans $\mathbb{Z}_p$ (proposition 1.25), une fonction continue est entièrement déterminée par les valeurs qu'elle prend sur $\mathbb{N}$.

□

2.1. Quelques préliminaires techniques.

On commence par donner un minorant de la norme p-adique de la factorielle d'un entier naturel.

Proposition 2.2. Quel que soit $m \in \mathbb{N}$, on a :

$$v_p(m!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{m}{p^k} \right\rfloor.$$

Preuve. On rappelle que l'on a :

$$m! = \prod_{\ell=1}^{m} \ell.$$

Dès lors, d'après le point ii. de la proposition 1.18, il vient :

$$v_p(m!) = \sum_{\ell=1}^{m} v_p(\ell). \tag{1}$$

On introduit l'ensemble suivant :

$$A_m := \left\{(k, \ell) \in \mathbb{N}_{\geqslant 1} \times [\![1, m]\!] \text{ t.q. } p^k | \ell\right\}.$$

D'une part, on constate que l'on a :

$$\#A_m = \sum_{k=1}^{+\infty} \#\left\{\ell \in [\![1, m]\!] \text{ t.q. } p^k | \ell\right\}.$$

Or, quel que soit $k \in \mathbb{N}_{\geqslant 1}$, $[\![1, m]\!]$ contient $\left\lfloor \frac{m}{p^k} \right\rfloor$ multiple de p^k, d'où :

$$\#\left\{\ell \in [\![1, m]\!] \text{ t.q. } p^k | \ell\right\} = \left\lfloor \frac{m}{p^k} \right\rfloor.$$

Par conséquent, on a l'égalité suivante :

$$\#A_m = \sum_{k=1}^{+\infty} \left\lfloor \frac{m}{p^k} \right\rfloor. \tag{2}$$

D'autre part, on observe que l'on a :

$$\#A_m = \sum_{\ell=1}^{m} \#\left\{k \in \mathbb{N}^* \text{ t.q. } p^k | \ell\right\}.$$

Or, d'après la remarque 1.17, quel que soit $\ell \in [\![1, m]\!]$, on a :

$$v_p(\ell) = \#\left\{k \in \mathbb{N}^* \text{ t.q. } p^k | \ell\right\}.$$

Par conséquent, on a également l'égalité suivante :

$$\#A_m = \sum_{\ell=1}^{m} v_p(\ell). \tag{3}$$

En rapprochant les égalités (1), (2) et (3), on a l'égalité annoncée.

□

Corollaire 2.3. Quel que soit m entier naturel, on a :

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

Preuve. On rappelle que l'on a :

$$\forall x \in \mathbb{R}, \lfloor x \rfloor \leqslant x.$$

Par conséquent, d'après la proposition 2.2, on a :

$$v_p(m!) \leqslant \sum_{k=1}^{+\infty} \frac{m}{p^k} = \frac{m}{p-1}.$$

Finalement, d'après la définition 1.19, on a l'inégalité annoncée.

□

Afin de vérifier que la fonction construite est donné par une série entière, on aura besoin de la proposition suivante :

Proposition 2.4. Soient $(a_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{\mathbb{N}}$ qui converge vers 0 et $(b_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{(\mathbb{N})}$. Les séries $\sum_i a_i \sum_j b_j X^j$ et $\sum_j a_i \sum_i b_j X^j$ sont convergentes et égales sur $\mathbb{Z}_p$.

Preuve. Quel que soit $x \in \mathbb{Z}_p$, on définit $\alpha(x) \in {\mathbb{Q}_p}^{\mathbb{N}^2}$ de la manière suivante :

$$\forall (i,j) \in \mathbb{N}^2, \alpha(x)_{i,j} := a_i b_j x^j.$$

D'après le point ii. de la proposition 1.18 et la remarque 1.20, on a :

$$\forall x \in \mathbb{Z}_p, \forall (i,j) \in \mathbb{N}^2, |\alpha(x)_{i,j}|_p \leqslant |a_i|_p |b_j|_p. \tag{4}$$

Or, comme par hypothèse $\lim_{i\to+\infty} a_i = 0$, d'après (4), il vient :

$$\forall x \in \mathbb{Z}_p, \lim_{i\to+\infty} \alpha(x)_{i,j} = 0. \tag{5}$$

Par ailleurs, comme $(b_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{(\mathbb{N})}$, on a $\lim\limits_{j\to+\infty} b_j = 0$ et d'après (4), il vient :

$$\forall x \in \mathbb{Z}_p, \lim_{j\to+\infty} \alpha(x)_{i,j} = 0. \tag{6}$$

Par conséquent, d'après (5) et (6), il vient :

$$\forall x \in \mathbb{Z}_p, \lim_{\max(i,j)\to+\infty} \alpha(x)_{i,j} = 0.$$

Dès lors, d'après la proposition 1.36, quel que soit $x \in \mathbb{Z}_p$, les séries $\sum\limits_i \sum\limits_j \alpha(x)_{i,j}$ et $\sum\limits_j \sum\limits_i \alpha(x)_{i,j}$ sont convergentes dans $\mathbb{Q}_p$ et convergent vers la même limite. Finalement, on en déduit que l'on a :

$$\sum_i a_i \sum_j b_j X^j = \sum_j \left(b_j \sum_i a_i \right) X^j \in \mathbb{Q}_p[[X]].$$

D'où le résultat annoncé.

□

Remarque 2.5. Quels que soient $(a_n)_{n\in\mathbb{N}} \in {\mathbb{Q}_p}^{\mathbb{N}}$ qui converge vers 0 et $(P_n)_{n\in\mathbb{N}} \in \mathbb{Q}_p[X]^{\mathbb{N}}$, d'après la proposition 2.4, la série $\sum a_n P_n$ converge en chaque point de $\mathbb{Z}_p$ et définit un élément de $\mathbb{Q}_p[[X]]$.

Afin de vérifier que la fonction construite interpole bien les itérés de f en un point fixé, on aura besoin de l'égalité combinatoire suivante :

Lemme 2.6. Quel que soit $n \in \mathbb{N}$ et quel que soit $\ell \in [\![0, n]\!]$, on a :

$$\sum_{m=\ell}^{n} \binom{n}{m}\binom{m}{\ell}(-1)^{m-\ell} = \delta_{n,\ell}.$$

Preuve. Quel que soit $m \in [\![\ell, n]\!]$, on remarque que l'on a :

$$\binom{n}{m}\binom{m}{\ell} = \frac{n!}{\ell!(n-\ell)!}\frac{(n-\ell)!}{(m-\ell)!(n-m)!} = \binom{n}{\ell}\binom{n-\ell}{m-\ell}.$$

En sommant sur $m \in [\![\ell, n]\!]$ et en changeant d'indice, il vient :

$$\sum_{m=\ell}^{n} \binom{n}{m}\binom{m}{\ell}(-1)^{m-\ell} = \binom{n}{\ell}\sum_{m=0}^{n-\ell}\binom{n-\ell}{m}(-1)^m.$$

Dès lors, d'après la formule du binôme de Newton, on a :

$$\sum_{m=\ell}^{n} \binom{n}{m}\binom{m}{\ell}(-1)^{m-\ell} = \binom{n}{\ell}(1-1)^{n-\ell} = \delta_{n,\ell}.$$

D'où l'égalité annoncé.

□

2.2. **Étude sommaire d'un opérateur de différence finie.**

Définition 2.7. On définit $\Delta : \mathbb{Z}_p[X_1, \cdots, X_d]^d \to \mathbb{Z}_p[X_1, \cdots, X_d]^d$ par :

$$\forall h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d, \Delta(h) := h \circ f - h.$$

Remarque 2.8. Pour $h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$, on notera parfois Δh pour $\Delta(h)$.

Proposition 2.9. Soit $(h_1, h_2) \in \mathbb{Z}_p[X_1, \cdots, X_d]^d \times \mathbb{Z}_p[X_1, \cdots, X_d]^d$, on a :

i. $\Delta(h_1 + h_2) = \Delta h_1 + \Delta h_2$.

ii. $\Delta(h_1 h_2) = (h_2 \circ f)\Delta h_1 + h_1 \Delta h_2$.

Preuve. On montre indépendamment chaque propriété.

i. D'après la définition 2.7, on a :

$$\begin{aligned}\Delta(h_1 + h_2) &= (h_1 + h_2) \circ f - (h_1 + h_2),\\ &= h_1 \circ f + h_2 \circ f - h_1 - h_2,\\ &= \Delta h_1 + \Delta h_2.\end{aligned}$$

ii. D'après la définition 2.7, on a :

$$\begin{aligned}\Delta(h_1 h_2) &= (h_1 h_2) \circ f - h_1 h_2,\\ &= (h_1 \circ f)(h_2 \circ f) - h_1 h_2,\\ &= (h_1 \circ f)(h_2 \circ f) - h_1(h_2 \circ f) + h_1(h_2 \circ f) - h_1 h_2,\\ &= (h_2 \circ f)(h_1 \circ f - h_1) + h_1(h_2 \circ f - h_2),\\ &= (h_2 \circ f)\Delta h_1 + h_1 \Delta h_2.\end{aligned}$$

D'où le résultat annoncé.

□

Proposition 2.10. Quels que soient $h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$ et $m \in \mathbb{N}$, on a :

$$\Delta^m h = \sum_{l=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} h \circ f^\ell.$$

Preuve. On procède par récurrence sur m.

- **Initialisation.** Si $m = 0$, quel que soit $h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$, on a :

$$\Delta^m h = h = \sum_{\ell=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} h \circ f^\ell.$$

- **Hérédité.** Soit $m \geqslant 1$, on suppose que l'on a :

$$\forall h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d, \Delta^{m-1} h = \sum_{\ell=0}^{m} \binom{m-1}{\ell} (-1)^{m-\ell-1} h \circ f^\ell.$$

Soit $h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$, d'après la définition 2.7, on a :

$$\Delta^m h = \Delta^{m-1}(h \circ f - h).$$

Dès lors, d'après le point i. de la proposition 2.9, il vient :

$$\Delta^m h = \Delta^{m-1}(h \circ f) - \Delta^{m-1} h.$$

Ainsi, par hypothèse de récurrence, on a :

$$\begin{aligned}\Delta^m h &= \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^{m-\ell-1} h \circ f^{\ell+1} \\ &\quad - \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^{m-\ell-1} h \circ f^{\ell}, \\ &= \sum_{\ell=1}^{m} \binom{m-1}{\ell-1} (-1)^{m-\ell} h \circ f^{\ell} \\ &\quad + \sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^{m-\ell} h \circ f^{\ell}.\end{aligned}$$

Dès lors, d'après la formule du triangle de Pascal, il vient :

$$\Delta^m h = h + \sum_{\ell=1}^{m-1} \binom{m}{\ell} (-1)^{m-\ell} h \circ f^{\ell} + h \circ f^m.$$

Finalement, on a :

$$\Delta^m h = \sum_{\ell=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} h \circ f^{\ell}.$$

D'où l'égalité annoncée.

□

2.3. **Construction de la fonction p-analytique d'interpolation.** On munit ${\mathbb{Q}_p}^d$ de la norme infini associée à $|\cdot|_p$ que l'on note $\|\cdot\|_p$, on a :

$$\forall x := (x_1, \cdots, x_d) \in {\mathbb{Q}_p}^d, \|x\|_p := \max_{i \in [\![1,d]\!]} |x_i|_p.$$

On rappelle qu'une suite d'éléments de ${\mathbb{Q}_p}^d$ est convergente si et seulement si chacune de ses composantes converge dans $\mathbb{Q}_p$. Ainsi, en accord avec la proposition 1.35, une série d'éléments de ${\mathbb{Q}_p}^d$ est convergente si et seulement si chacune des composantes de son terme général converge vers 0 dans $\mathbb{Q}_p$, c'est-à-dire si et seulement si son terme général converge vers 0.

Définition 2.11. Soit $n \in \mathbb{N}$, on appelle $n^{\text{ème}}$ polynôme binomial et on note $\binom{\cdot}{n} : \mathbb{Z}_p \to \mathbb{Q}_p$ l'application définie par :

- Quel que soit $x \in \mathbb{Z}_p$, $\binom{x}{0} := 1$.
- Quel que soit $x \in \mathbb{Z}_p$, $\binom{x}{n} := \dfrac{1}{n!} \displaystyle\prod_{k=0}^{n-1} (x-k)$, si $n \geqslant 1$.

Remarque 2.12. Quels que soient $n \in \mathbb{N}$ et $x \in \mathbb{N}$, le $n^{\text{ème}}$ polynôme binomial évalué en x coïncide avec le coefficient binomial usuel $\binom{x}{n}$.

Théorème 2.13. (Poonen [12]) On définit l'entier suivant :

$$c := \begin{cases} 2 & \text{, si } p = 2 \\ 1 & \text{, sinon} \end{cases}.$$

Si $f - I \in p^c\mathbb{Z}_p[X_1, \cdots, X_d]^d$, alors quel que soit $x \in {\mathbb{Z}_p}^d$, il existe $g \in \mathbb{Q}_p[[X]]^d$ qui converge en chaque point de $\mathbb{Z}_p$ et satisfaisant à :

$$\forall n \in \mathbb{N}, g(n) = f^n(x).$$

Preuve. Quel que soit $i \in [\![1, d]\!]$, on introduit l'élément de ${\mathbb{Z}_p}^d$ suivant :

$$\varepsilon_i := (\delta_{i,j})_{j \in [\![1,d]\!]}.$$

Soit $(i, j) \in [\![1, d]\!]^2$, comme par hypothèse $f_i - X_i \in p^c\mathbb{Z}_p[X_1, \cdots, X_d]$, on a :

$$\Delta(X_i\varepsilon_j) = (f_i - X_i)\varepsilon_j \in p^c\mathbb{Z}_p[X_1, \cdots, X_d]^d. \tag{7}$$

Tout élément de $\mathbb{Z}_p[X_1, \cdots, X_d]^d$ étant une somme de produits de $(X_i\varepsilon_j)_{(i,j)\in[\![1,d]\!]^2}$, d'après la proposition 2.9 et (7), il vient :

$$\Delta : \mathbb{Z}_p[X_1, \cdots, X_d]^d \to p^c\mathbb{Z}_p[X_1, \cdots, X_d]^d. \tag{8}$$

Or, on constate que l'on a :

$$\forall \lambda \in \mathbb{Q}_p, \forall h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d, \Delta(\lambda h) = \lambda \Delta h. \tag{9}$$

Dès lors, d'après (8) et (9), par récurrence immédiate, il vient :

$$\forall m \in \mathbb{N}, \Delta^m I \in p^c\mathbb{Z}_p[X_1, \cdots, X_d]^d.$$

Soit $x \in {\mathbb{Z}_p}^d$, on en déduit que l'on a :

$$\forall m \in \mathbb{N}, (\Delta^m I)(x) \in p^c{\mathbb{Z}_p}^d.$$

Dès lors, par construction de $\|\cdot\|_p$ et d'après la remarque 1.17, on a :

$$\forall m \in \mathbb{N}, \|(\Delta^m I)(x)\|_p \leqslant p^{-c}.$$

Ainsi, d'après le corollaire 2.3, il vient :

$$\forall m \in \mathbb{N}, \left\| \frac{(\Delta^m I)(x)}{m!} \right\|_p \leqslant p^{-m\left(c - \frac{1}{p-1}\right)}.$$

En particulier, comme $c - \frac{1}{p-1} > 0$, on en déduit que l'on a :

$$\lim_{m \to +\infty} \frac{(\Delta^m I)(x)}{m!} = 0.$$

Par conséquent, d'après les remarques 1.20 et 2.5, quel que soit $n \in \mathbb{Z}_p$, $\sum_m \binom{n}{m}(\Delta^m I)(x)$ est convergente et définit alors un élément de $\mathbb{Q}_p[[n]]^d$. Ainsi, la fonction g définie comme suit est la somme d'un élément de $\mathbb{Q}_p[[X]]^d$:

$$\forall n \in \mathbb{Z}_p, g(n) := \sum_{m=0}^{+\infty} \binom{n}{m}(\Delta^m I)(x).$$

Soit $n \in \mathbb{N}$, quel que soit $m \in \mathbb{N}_{\geqslant m}$, d'après la remarque 2.12, on a :

$$\binom{n}{m} = 0.$$

En particulier, on en déduit que l'on a :

$$g(n) = \sum_{m=0}^{n} \binom{n}{m} (\Delta^m I)(x).$$

Dès lors d'après la proposition 2.10 appliquée en $h = I$, il vient :

$$\begin{aligned} g(n) &= \sum_{m=0}^{n} \binom{n}{m} \sum_{\ell=0}^{m} \binom{m}{\ell} (-1)^{m-\ell} f^{\ell}(x), \\ &= \sum_{\ell=0}^{n} f^{\ell}(x) \sum_{m=\ell}^{n} \binom{n}{m} \binom{m}{\ell} (-1)^{m-\ell}. \end{aligned}$$

Finalement, d'après le lemme 2.6, on a :

$$g(n) = \sum_{\ell=0}^{n} f^{\ell}(x) \delta_{n,\ell} = f^n(x).$$

D'où le résultat annoncé.

□

3. Une généralisation du théorème de Skolem-Mahler-Lech

On montre en préliminaire que l'on peut plonger toute extension finiment engendrée de $\mathbb{Q}$ dans une infinité de $\mathbb{Q}_p$ et que l'on peut même choisir ces plongements de telle manière à ce qu'ils envoient un nombre fini d'éléments prescrits sur des entiers p-adiques. Ce résultat nous permettra enfin d'établir les théorèmes 1 et 3, nous exploiterons les théorèmes 1.37 et 2.13.

3.1. Plongement dans un corps de nombres p-adiques.

Lemme 3.1. Soit d un entier naturel non nul, quels que soient $N \in \mathbb{N}_{\geqslant 1}$ et $(f_n)_{n\in[\![1,N]\!]} \in \mathbb{Z}[X_1, \cdots, X_d]^N$ tous non nuls, il existe $(a_i)_{i\in[\![1,d]\!]} \in \mathbb{Z}^d$ tel que :

$$\forall n \in [\![1, N]\!], f_n(a_1, \cdots, a_d) \neq 0.$$

Preuve. On définit l'élément de $\mathbb{Z}[X_1, \cdots, X_d]$ suivant :

$$f := \prod_{n=1}^{N} f_n.$$

On distingue alors les deux cas suivants sur d :

- Si $d = 1$, on suppose par l'absurde que f s'annule en chaque point de $\mathbb{Z}$. Dès lors, f a une infinité de racines dans le corps $\mathbb{Q}$ et on a alors $f = 0$. Par intégrité de $\mathbb{Z}[X_1]$, il existe $n \in [\![1, N]\!]$ tel que $f_n = 0$, contradiction. Finalement, il existe $a_1 \in \mathbb{Z}$ tel que $f(a_1) \neq 0$ et en particulier, on a :
$$\forall n \in [\![1, N]\!], f_n(a_1) \neq 0.$$
- Si $d \geqslant 2$, on suppose par l'absurde que f s'annule en chaque point de $\mathbb{Z}^d$. On définit alors l'anneau intègre suivant :
$$A := \mathbb{Z}[X_1, \cdots, X_{d-1}].$$
Ainsi, f vu comme élément de $A[X_d]$ s'annule en chaque point de $\mathbb{Z} \subseteq A$. f a une infinité de racines dans le corps des fractions de A et l'on a $f = 0$. Par intégrité de $\mathbb{Z}[X_1, \cdots, X_d]$, il existe $n \in [\![1, N]\!]$ tel que $f_n = 0$, ce qui n'est pas. Finalement, il existe $(a_i)_{i\in[\![1,d]\!]} \in \mathbb{Z}^d$ tel que $f(a_1, \cdots, a_d) \neq 0$ et en particulier, on a :
$$\forall n \in [\![1, N]\!], f_n(a_1, \cdots, a_n) \neq 0.$$

D'où le résultat annoncé.

□

Proposition 3.2. Soit $P \in \mathbb{Z}[X]$ non constant, il existe une infinité de nombres premiers p tel que l'équation $P(x) \equiv 0 \mod p$ ait une solution.

Preuve. On note d le degré de P, il existe $(a_i)_{i\in[\![0,d]\!]} \in \mathbb{Z}^{d+1}$ telle que :

$$P = \sum_{i=0}^{d} a_i X^i.$$

On distingue les deux cas suivants :

- Si $a_0 = 0$, alors quel que soit p premier, on a $P(0) \equiv 0 \mod p$.

- Si $a_0 \neq 0$, on définit le polynôme à coefficients dans $\mathbb{Z}$ suivant :

$$R := 1 + \sum_{i=1}^{d} a_i {a_0}^{i-1} X^i.$$

On commence par constater que l'on a :

$$P(a_0 X) = a_0 R. \tag{1}$$

Soit E l'ensemble des p premiers tel que $R(x) \equiv 0 \mod p$ soit résoluble. On suppose par l'absurde que E est fini et l'on définit alors :

$$x := \prod_{p \in E} p.$$

Quels que soient $p \in E$ et $N \in \mathbb{N}$, p divise Nx et l'on a :

$$R(Nx) \mod p \equiv 1 \mod p. \tag{2}$$

P étant non constant et a_0 étant non nul, d'après (1), R est non constant. Ainsi, il existe $N \in \mathbb{N}$ tel que $R(Nx) \in \mathbb{Z} \setminus \{\pm 1\}$; sinon, $R-1$ ou $R+1$ aurait une infinité de racines et R serait constant, d'où une contradiction. Dès lors, il existe un nombre premier p_0 tel que :

$$R(Nx) \equiv 0 \mod p_0. \tag{3}$$

Ainsi, $p_0 \in E$ et d'après (2), on a :

$$R(Nx) \equiv 1 \mod p_0. \tag{4}$$

(3) et (4) étant incompatibles, E est infini, c'est-à-dire qu'il existe une infinité de nombre premiers p tel que $R(x) \equiv 0 \mod p$ ait une racine. Finalement, a_0 étant non nul, d'après (1), $P(x) \equiv 0 \mod p$ a une solution pour une infinité de nombre premiers p.

D'où le résultat annoncé.

□

Proposition 3.3. Soit p un nombre premier, $\mathbb{Z}_p$ est non dénombrable.

Preuve. Supposons par l'absurde que $\mathbb{Z}_p$ soit dénombrable, il existe alors une énumération de $\mathbb{Z}_p$ que l'on note $(x_n)_{n \in \mathbb{N}_{\geqslant 1}}$ et quel que soit $n \in \mathbb{N}_{\geqslant 1}$, on écrit :

$$x_n := (x_{n,i})_{i \in \mathbb{N}_{\geqslant 1}}.$$

On construit récursivement un élément de $\mathbb{Z}_p$ distinct de chaque $x_n, n \in \mathbb{N}_{\geqslant 1}$.

- **Initialisation.** Comme $\mathbb{Z}/(p)$ est de cardinal $p \geqslant 2$, on dispose d'un élément y_1 de $\mathbb{Z}/(p)$ qui soit distinct de $x_{1,1}$.
- **Hérédité.** Soit $n \geqslant 2$, on suppose avoir construit :

$$(y_k)_{k \in [\![1, n-1]\!]} \in \prod_{k=1}^{n-1} \mathbb{Z}/(p^k) \text{ t.q. } \forall k \in [\![1, n-1]\!], y_k \neq x_{k,k}.$$

Si $n \geqslant 3$, on suppose de plus que l'on a :

$$\forall m \in [\![2, n-1]\!], \varphi_{m-1}^m(y_m) = y_{m-1}.$$

Comme $[\![0, p^n - 1]\!]$ contient p multiples de p^{n-1} et que le noyau de φ_{n-1}^n est constitué des classes modulo p^n des multiples de p^{n-1}, il vient :

$$\#\ker(\varphi_{n-1}^n) = p.$$

Par conséquent, y_{n-1} possède $p \geqslant 2$ antécédents par φ_{n-1}^n et il existe alors y_n dans $\mathbb{Z}/(p^n)$ distinct de $x_{n,n}$ satisfaisant à $\varphi_{n-1}^n(y_n) = y_{n-1}$. Finalement, on a construit :

$$(y_k)_{k\in[\![1,n]\!]} \in \prod_{k=1}^{n} \mathbb{Z}/(p^k) \text{ t.q. } \forall k \in [\![1, n]\!], y_k \neq x_{k,k},$$

et tel que pour tout $m \in [\![2, n]\!]$, on ait $\varphi_{m-1}^m(y_m) = y_{m-1}$.

On a construit $y \in \mathbb{Z}_p$ qui n'est pas dans $\{x_n, ; n \in \mathbb{N}_{\geqslant 1}\}$, ce qui ne peut être. D'où le résultat annoncé.

□

Corollaire 3.4. Soit p un nombre premier, toutes les bases de transcendance de $\mathbb{Q}_p/\mathbb{Q}$ ont un cardinal infini.

Preuve. Supposons par l'absurde qu'il existe $\{x_1, \cdots, x_n\}$ une base de transcendance finie de $\mathbb{Q}_p/\mathbb{Q}$, alors $\mathbb{Q}_p$ est algébrique sur $\mathbb{Q}(x_1, \cdots, x_n)$ et l'on a :

$$\forall x \in \mathbb{Q}_p, \exists P \in \mathbb{Q}(x_1, \cdots, x_n)[X] \setminus \{0\} \text{ t.q. } P(x) = 0. \tag{5}$$

On introduit alors l'ensemble suivant :

$$E := \bigcup_{\substack{P\in\mathbb{Q}(x_1,\cdots,x_n)[X]\\ P\neq 0}} \{x \in \mathbb{Q}_p \text{ t.q. } P(x) = 0\}.$$

En particulier, d'après (5), on a l'inclusion suivante :

$$\mathbb{Q}_p \subseteq E. \tag{6}$$

Or, $\mathbb{Q}$ étant dénombrable, $\mathbb{Q}(x_1, \cdots, x_n)$ et $\mathbb{Q}(x_1, \cdots, x_n)[X]\setminus\{0\}$ le sont aussi. Par ailleurs, $\mathbb{Q}_p$ étant un corps, pour tout $P \in \mathbb{Q}(x_1, \cdots, x_n)[X] \setminus \{0\}$, on a :

$$\#\{x \in \mathbb{Q}_p \text{ t.q. } P(x) = 0\} < \infty.$$

Dès lors, E est dénombrable comme union dénombrable d'ensembles finis. Finalement, d'après (6), $\mathbb{Q}_p$ est dénombrable, ce qui contredit la proposition 3.3. D'où le résultat annoncé.

□

Corollaire 3.5. Quel que soit $n \in \mathbb{N}_{\geqslant 1}$, il existe $\{\mu_1, \cdots, \mu_n\} \subseteq \mathbb{Q}_p$ qui soit algébriquement indépendant sur $\mathbb{Q}$.

Preuve. Soit S une base de transcendance de $\mathbb{Q}_p/\mathbb{Q}$, d'après le corollaire 3.4, S est de cardinal infini, si bien que pour tout $n \in \mathbb{N}_{\geqslant 1}$, S contient un ensemble de cardinal n, disons $\{\mu_1, \cdots, \mu_n\}$. Comme S est algébriquement indépendant, $\{\mu_1, \cdots, \mu_n\}$ l'est également. D'où le résultat annoncé.

□

Lemme 3.6. Soient d un entier naturel non nul et (x, y) un élément de $\left(\mathbb{Z}_p{}^d\right)^2$. Si $x - y \in p\mathbb{Z}_p{}^d$, alors quel que soit $f \in \mathbb{Z}_p[X_1, \cdots, X_d]$, on a $f(x) - f(y) \in p\mathbb{Z}_p$.

Preuve. Soit $(h_1, h_2) \in \mathbb{Z}_p[X_1, \cdots, X_d]^2$ tel que :

$$\forall i \in \{1, 2\}, h_i(x) - h_i(y) \in p\mathbb{Z}_p.$$

On constate alors que $h_1 + h_2$ et $h_1 h_2$ satisfont aussi à cette même propriété. En effet, on remarque que l'on a les deux égalités suivantes :

$$(h_1 + h_2)(x) - (h_1 + h_2)(y) = (h_1(x) - h_1(y)) + (h_2(x) - h_2(y)),$$
$$(h_1 h_2)(x) - (h_1 h_2)(y) = g(x)(h_1(x) - h_1(y)) + f(y)(h_2(x) - h_2(y)).$$

Or, par hypothèse sur (x, y), on a :

$$\forall i \in [\![1, d]\!], X_i(x) - X_i(y) \in p\mathbb{Z}_p.$$

Ainsi, tout élément de $\mathbb{Z}_p[X_1, \cdots, X_d]$ étant une somme de produits de $(X_i)_{i \in [\![1,d]\!]}$, on a le résultat annoncé.

□

Proposition 3.7. Soit $f \in \mathbb{Z}_p[X]$, supposons qu'il existe $\alpha_0 \in \mathbb{Z}_p$ tel que :

$$f(\alpha_0) \in p\mathbb{Z}_p \text{ et } f'(\alpha_0) \notin p\mathbb{Z}_p,$$

alors il existe un unique $\alpha \in \mathbb{Z}_p$ satisfaisant à $f(\alpha) = 0$ et $\alpha - \alpha_0 \in p\mathbb{Z}_p$.

Preuve. D'après la formule de Taylor, il existe $g \in \mathbb{Z}_p[X, Y]$ tel que l'on ait :

$$\forall (x, y) \in {\mathbb{Z}_p}^2, f(y) = f(x) + (y - x)f'(x) + (y - x)^2 g(x, y). \tag{7}$$

On montre alors l'existence et l'unicité séparément.

- **Existence.** On construit par récurrence $(\alpha_n)_{n \in \mathbb{N}} \in {\mathbb{Z}_p}^{\mathbb{N}}$ telle que :

  $$\forall n \in \mathbb{N}, f(\alpha_n) \in p^{n+1}\mathbb{Z}_p \text{ et } f'(\alpha_n) \notin p\mathbb{Z}_p.$$

  On exige de plus que $(\alpha_n)_{n \in \mathbb{N}}$ satisfasse à :

  $$\forall n \in \mathbb{N}_{\geqslant 1}, \alpha_n - \alpha_{n-1} \in p^n\mathbb{Z}_p.$$

  - **Initialisation.** Si $n = 0$, α_0 convient par hypothèse.
  - **Hérédité.** Soit $n \geqslant 1$, on suppose avoir construit α_{n-1}, alors comme $f'(\alpha_{n-1}) \notin p\mathbb{Z}_p$, d'après la proposition 1.7 et la remarque 1.8, il vient :

    $$f'(\alpha_{n-1}) \in {\mathbb{Z}_p}^{\times}.$$

    Ainsi, nous sommes en mesure de définir l'élément de $\mathbb{Z}_p$ suivant :

    $$\alpha_n := \alpha_{n-1} - f(\alpha_{n-1})f'(\alpha_{n-1})^{-1}.$$

    Par construction $f(\alpha_{n-1}) \in p^n\mathbb{Z}_p$ et on a alors :

    $$\alpha_{n-1} - \alpha_n \in p^n\mathbb{Z}_p. \tag{8}$$

    Par ailleurs, en appliquant (7) en $(x, y) = (\alpha_{n-1}, \alpha_n)$, il vient :

    $$f(\alpha_n) = (\alpha_n - \alpha_{n-1})^2 g(\alpha_{n-1}, \alpha_n).$$

    Dès lors, d'après (8), $f(\alpha_n) \in p^{2n}\mathbb{Z}_p$ et comme $n \geqslant 1$, on a :

    $$f(\alpha_n) \in p^{n+1}\mathbb{Z}_p. \tag{9}$$

    En outre, comme $n \geqslant 1$, d'après (8) et le lemme 3.6, il vient :

    $$f'(\alpha_n) - f'(\alpha_{n-1}) \in p\mathbb{Z}_p.$$

Par conséquent, comme $f'(\alpha_{n-1}) \notin p\mathbb{Z}_p$, on en déduit que l'on a :

$$f'(\alpha_n) \notin p\mathbb{Z}_p. \tag{10}$$

Finalement, d'après (8), (9) et (10), le α_n construit convient.

Soit $(m,n) \in \mathbb{N}^2$, d'après le point iii. de la proposition 1.21, on a :

$$|\alpha_{n+m} - \alpha_n|_p \leqslant \max_{k \in [\![1,m]\!]} |\alpha_{n+k} - \alpha_{n+k-1}|_p. \tag{11}$$

Or, par construction de $(\alpha_n)_{n\in\mathbb{N}}$, quel que soit $k \in [\![1,m]\!]$, on a :

$$|\alpha_{n+k} - \alpha_{n+k-1}|_p \leqslant p^{-(n+k)}.$$

Dès lors, d'après (11), on en déduit que l'on a :

$$|\alpha_{n+m} - \alpha_n|_p \leqslant p^{-n}.$$

Par conséquent, on a montré que $(\alpha_n)_{n\in\mathbb{N}}$ satisfaisait à :

$$\forall n \in \mathbb{N}^2, \sup_{m\in\mathbb{N}} |\alpha_{n+m} - \alpha_n|_p \leqslant p^{-n}.$$

Ainsi, $\lim\limits_{n\to+\infty} \sup\limits_{m\in\mathbb{N}} |\alpha_{n+m} - \alpha_n|_p = 0$ et $(\alpha_n)_{n\in\mathbb{N}}$ est une suite de Cauchy. D'après la proposition 1.29, $(\alpha_n)_{n\in\mathbb{N}}$ est convergente, disons vers $\alpha \in \mathbb{Z}_p$. Par construction de $(\alpha_n)_{n\in\mathbb{N}}$ et d'après la remarque 1.17, on a :

$$\forall n \in \mathbb{N}, |f(\alpha_n)|_p \leqslant p^{-n}.$$

Dès lors, par passage à la limite quand n tend vers $+\infty$, il vient :

$$\lim_{n\to+\infty} f(\alpha_n) = 0.$$

Comme f est continue en $\alpha = \lim\limits_{n\to+\infty} \alpha_n$, on en déduit que l'on a :

$$f(\alpha) = 0. \tag{12}$$

En outre, par construction de $(\alpha_n)_{n\in\mathbb{N}}$ et d'après la remarque 1.17, on a :

$$\forall n \in \mathbb{N}, |\alpha_n - \alpha_0|_p \leqslant p^{-1}.$$

Dès lors, par passage à la limite quand n tend vers $+\infty$, on a :

$$\lim_{n\to+\infty} |\alpha_n - \alpha_0|_p \leqslant p^{-1}.$$

$|\cdot|_p$ étant continue (1-lipschitzienne) en $\alpha = \lim\limits_{n\to+\infty} \alpha_n$, on en déduit que $|\alpha - \alpha_0|_p \leqslant p^{-1}$ et d'après la remarque 1.17, il vient :

$$\alpha - \alpha_0 \in p\mathbb{Z}_p. \tag{13}$$

Finalement, d'après (12) et (13), le α construit convient.

- **Unicité.** On suppose qu'il existe $(\alpha_1, \alpha_2) \in {\mathbb{Z}_p}^2$ tel que :

$$\forall i \in \{1,2\}, f(\alpha_i) = 0 \text{ et } \alpha_i - \alpha_0 \in p\mathbb{Z}_p.$$

Par conséquent, d'après (7) appliqué en $(x,y) = (\alpha_1, \alpha_2)$, on a :

$$(\alpha_2 - \alpha_1) f'(\alpha_1) + (\alpha_2 - \alpha_1)^2 g(\alpha_1, \alpha_2) = 0. \tag{14}$$

Comme $\alpha_1 - \alpha_0 \in p\mathbb{Z}_p$, d'après le lemme 3.6, on a $f'(\alpha_1) - f'(\alpha_0) \in p\mathbb{Z}_p$. Dès lors, comme $f'(\alpha_0) \notin p\mathbb{Z}_p$, on en déduit que l'on a $f'(\alpha_1) \notin p\mathbb{Z}_p$ et d'après la proposition 1.7 et la remarque 1.8, il vient :

$$f'(\alpha_1) \in {\mathbb{Z}_p}^{\times}.$$

En particulier, d'après (14), on a :

$$\alpha_2 - \alpha_1 = -(\alpha_2 - \alpha_1)^2 g(\alpha_1, \alpha_2) f'(\alpha_1)^{-1}.$$

En prenant la norme p-adique de cette égalité, d'après le point ii. de la proposition 1.21 et la remarque 1.20, il vient :

$$|\alpha_2 - \alpha_1|_p \leqslant {|\alpha_2 - \alpha_1|_p}^2. \tag{15}$$

Or, comme $\alpha_2 - \alpha_1 \in p\mathbb{Z}_p$, d'après la remarque 1.17, on a :

$$|\alpha_2 - \alpha_1|_p < 1. \tag{16}$$

Finalement, d'après (15) et (16), $|\alpha_2 - \alpha_1|_p = 0$ et d'après le point i. de la proposition 1.21, il vient $\alpha_1 = \alpha_2$.

D'où le résultat annoncé.

□

Théorème 3.8. (Cassels [3]) Soit $K/\mathbb{Q}$ une extension finiment engendrée et soit S un sous-ensemble fini de K, il existe alors une infinité de nombres premiers p tel qu'il existe un plongement $\alpha : K \hookrightarrow \mathbb{Q}_p$ satisfaisant à :

$$\forall s \in S, \alpha(s) \in \mathbb{Z}_p.$$

Preuve. $K/\mathbb{Q}$ admet une base de transcendance finie, notons la $\{x_1, \cdots, x_m\}$. Dans le cas contraire, K ne serait pas finiment engendré sur $\mathbb{Q}$, contradiction. On introduit alors le corps suivant :

$$k := \mathbb{Q}(x_1, \cdots, x_m).$$

Par ailleurs, K/k est une extension séparable de degré fini ; en effet, k est de caractéristique zéro et l'extension K/k est algébrique et finiment engendrée. Par conséquent, d'après le théorème de l'élément primitif [13], il existe $y \in K$ algébrique sur k satisfaisant à :

$$K = k[y]. \tag{17}$$

Dès lors, quel que soit $s \in S$, il existe $(U_s, V_s) \in \mathbb{Z}[X_1, \cdots, X_m, Y] \times \mathbb{Z}[X_1, \cdots, X_m]$ avec $V_s \neq 0$ tels que l'on ait l'égalité suivante :

$$s = \frac{U_s(x_1, \cdots, x_m, y)}{V_s(x_1, \cdots, x_m)}. \tag{18}$$

Quitte à multiplier le polynôme minimal de y dans K/k par le produit des dénominateurs de ses coefficients, on dispose d'un polynôme annulateur de y qui est irréductible sur k et à coefficients dans $\mathbb{Z}[x_1, \cdots, x_m]$, notons le G. Notamment, il existe $H \in \mathbb{Z}[X_1, \cdots, X_m, Y]$ satisfaisant à :

$$H(x_1, \cdots, x_m, Y) = G(Y). \tag{19}$$

Soit $H_0 \in \mathbb{Z}[X_1, \cdots, X_n]$ le coefficient dominant de H en l'indéterminée Y. Comme G est irréductible sur k de caractéristique 0, on en déduit que G est

séparable, c'est-à-dire que son discriminant est non nul. Plus précisément, le discriminant de G est de la forme $\Delta(x_1, \cdots, x_n)$, où $\Delta \in \mathbb{Z}[X_1, \cdots, X_n] \setminus \{0\}$. Ainsi, $\{V_s\}_{s\in S} \cup \{H_0, \Delta\}$ forme un sous-ensemble fini de $\mathbb{Z}[X_1, \cdots, X_m] \setminus \{0\}$ et d'après le lemme 3.1, il existe $(a_1, \cdots, a_m) \in \mathbb{Z}^m$ tel que l'on ait :

$$H_0(a_1, \cdots, a_m) \neq 0, \tag{20}$$

$$\Delta(a_1, \cdots, a_m) \neq 0, \tag{21}$$

$$\forall s \in S, V_s(a_1, \cdots, a_m) \neq 0. \tag{22}$$

Comme G est irréductible sur k, on déduit de l'égalité (19) que H est de degré au moins égal à 1 en l'indéterminée Y. Ainsi, d'après (20), $H(a_1, \cdots, a_n, Y)$ est non constant et d'après la proposition 3.2, il existe une infinité de nombres premiers p tels que $H(a_1, \cdots, a_m, Y)$ ait une racine modulo p. Or, d'après (21) et (22), les diviseurs premiers de $\Delta(a_1, \cdots, a_m)$ et $V_s(a_1, \cdots, a_m), s \in S$ sont en nombre fini. Dès lors, il existe un infinité de nombres premiers p tel que :

$$\exists b \in \mathbb{Z} \text{ t.q. } H(a_1, \cdots, a_m, b) \equiv 0 \mod p, \tag{23}$$

$$\Delta(a_1, \cdots, a_m) \not\equiv 0 \mod p, \tag{24}$$

$$\forall s \in S, V_s(a_1, \cdots, a_m) \not\equiv 0 \mod p. \tag{25}$$

Par ailleurs, d'après le corollaire 3.5, il existe $\{\mu_1, \cdots, \mu_m\} \subseteq \mathbb{Q}_p$ un ensemble algébriquement indépendant sur $\mathbb{Q}$, quitte à multiplier chacun des $\mu_i, i \in [\![1, m]\!]$ par l'entier naturel p^n, où $n := \max\limits_{i\in[\![1,m]\!]} v_p(\mu_i) + 1$, on suppose que l'on a :

$$\forall i \in [\![1, m]\!], \mu_i \in p\mathbb{Z}_p. \tag{26}$$

Quel que soit $i \in [\![1, m]\!]$, on définit l'élément de $\mathbb{Z}_p$ suivant :

$$\xi_i := \mu_i + a_i.$$

Dès lors, par construction des $\xi_i, i \in [\![1, m]\!]$, d'après le lemme 3.6, il vient :

$$H(\xi_1, \cdots, \xi_m, b) - H(a_1, \cdots, a_m, b) \in p\mathbb{Z}_p,$$
$$\Delta(\xi_1, \cdots, \xi_m) - \Delta(a_1, \cdots, a_m) \in p\mathbb{Z}_p.$$

Par conséquent, d'après (23) et (24), on en déduit que l'on a :

$$H(\xi_1, \cdots, \xi_m, b) \in p\mathbb{Z}_p, \tag{27}$$

$$\Delta(\xi_1, \cdots, \xi_m) \notin p\mathbb{Z}_p. \tag{28}$$

Par construction, $\Delta(\xi_1, \cdots, \xi_m)$ est le discriminant de $H(\xi_1, \cdots, \xi_m, Y)$ et avec (24), on en déduit que les racines de $H(\xi_1, \cdots, \xi_m, Y)$ modulo $p\mathbb{Z}_p$ sont simples. En particulier, d'après (27), il vient :

$$H'(\xi_1, \cdots, \xi_m, b) \notin p\mathbb{Z}_p. \tag{29}$$

Ainsi, d'après (27), (29) et la proposition 3.7, il existe $z \in \mathbb{Z}_p$ satisfaisant à :

$$H(\xi_1, \cdots, \xi_m, z) = 0.$$

Supposons par l'absurde que $\{\xi_1, \cdots, \xi_m\} \subseteq \mathbb{Q}_p$ ne soit pas algébriquement indépendant sur $\mathbb{Q}$, alors il existe $P \in \mathbb{Q}[X_1, \cdots, X_m] \setminus \{0\}$ tel que l'on ait :

$$P(\mu_1 + a_1, \cdots, \mu_m + a_m) = 0.$$

Alors, comme les $a_i, i \in [\![1, m]\!]$ sont des entiers relatifs, le binôme de Newton appliqué à $P(\mu_1 + a_1, \cdots, \mu_m + a_m)$ fournit $Q \in \mathbb{Q}[X_1, \cdots, X_m] \setminus \{0\}$ tel que :

$$Q(\mu_1, \cdots, \mu_m) = 0,$$

ce qui contredit l'indépendance algébrique de l'ensemble $\{\mu_1, \cdots, \mu_m\}$ sur $\mathbb{Q}$. Dès lors, nous sommes en mesures de définir le morphisme d'anneaux suivant :

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{Q}(x_1, \cdots, x_m)[y] & \to & \mathbb{Q}(\xi_i, \cdots, \xi_m)[z] \\ x_i & \mapsto & \xi_i \\ y & \mapsto & z \end{array} \right. .$$

Comme on a $\mathbb{Q}(\xi_i, \cdots, \xi_m)[z] \subseteq \mathbb{Q}_p$, α réalise un plongement de K dans $\mathbb{Q}_p$. En outre, d'après la remarque 1.20, on a :

$$\forall s \in S, |U_s(\xi_1, \cdots, \xi_m, z)|_p \leqslant 1. \tag{30}$$

De plus, d'après le lemme 3.6, on a :

$$\forall s \in S, V_s(\xi_1, \cdots, \xi_m) - V_s(a_1, \cdots, a_m) \in p\mathbb{Z}_p.$$

Dès lors, d'après (25), on en déduit que l'on a :

$$\forall s \in S, V_s(\xi_1, \cdots, x_m) \notin p\mathbb{Z}_p$$

Ainsi, d'après la remarque 1.17, il vient :

$$\forall s \in S, |V_s(\xi_1, \cdots, \xi_m)|_p = 1. \tag{31}$$

Finalement, d'après (18), (30) et (31), on a :

$$\forall s \in S, \alpha(s) \in \mathbb{Z}_p.$$

D'où le résultat annoncé.

□

3.2. **Le cas des automorphismes linéaires.**

Lemme 3.9. Soit p premier, les anneaux $\mathbb{Z}_p/p\mathbb{Z}_p$ et $\mathbb{Z}/(p)$ sont isomorphes.

Preuve. L'application suivante est un morphisme d'anneaux :

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}_p & \to & \mathbb{Z}/(p) \\ (x_n)_{n \in \mathbb{N}_{\geqslant 1}} & \to & x_1 \end{array} \right. .$$

Soient $x \in \mathbb{Z}/(p)$ et $\overline{x} \in \mathbb{Z}$ satisfaisant à $x = \overline{x} \mod p$, alors on a :

$$\varphi(i(\overline{x})) = x.$$

Ainsi, φ est surjectif. Or, d'après la proposition 1.7 et la remarque 1.8, on a :

$$\ker(\varphi) = p\mathbb{Z}_p.$$

Par conséquent d'après le théorème de factorisation, il vient :

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/(p).$$

D'où le résultat annoncé.

□

Remarque 3.10. D'après le lemme 3.9, $\mathbb{Z}_p/p\mathbb{Z}_p$ est un corps.

Corollaire 3.11. Soient p un nombre premier et d un entier naturel non nul, alors tout élément de $\mathrm{GL}_d(\mathbb{Z}_p/p\mathbb{Z}_p)$ est d'ordre fini.

Preuve. D'après le lemme 3.9, $\mathbb{Z}_p/p\mathbb{Z}_p$ est fini, ainsi $\mathrm{GL}_d(\mathbb{Z}_p/p\mathbb{Z}_p)$ est aussi fini. D'où le résultat annoncé.

□

Remarque 3.12. L'ordre d'un élément de $\mathrm{GL}_d(\mathbb{Z}_p/p\mathbb{Z}_p)$ divise

$$\#\mathrm{GL}_d(\mathbb{Z}_p/p\mathbb{Z}_p) = \prod_{i=0}^{d-1} \left(p^d - p^i\right).$$

Théorème 3.13. (Skolem [15], Mahler [11], Lech [10]) Soient k un corps de caractéristique 0 et $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire sur k, alors l'ensemble :

$$\{n \in \mathbb{N} \text{ t.q. } u_n = 0\}$$

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

Preuve. Il existe $d \in \mathbb{N}_{\geqslant 1}$ et $a_0, \cdots, a_{d-1}$ dans k avec $a_0 \neq 0_k$ tels que :

$$\forall n \in \mathbb{N}, u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i}. \tag{32}$$

Soit K l'extension de $\mathbb{Q}$ engendrée par $u_0, \cdots, u_{d-1}$ et $a_0, \cdots, a_{d-1}$, d'après le théorème 3.8, il existe $p \geqslant 3$ premier et un plongement $\alpha : K \hookrightarrow \mathbb{Q}_p$ tels que :

$$\alpha(u_0), \cdots, \alpha(u_{d-1}), \alpha(a_0), \alpha(a_0)^{-1}, \alpha(a_1), \cdots, \alpha(a_{d-1}) \in \mathbb{Z}_p.$$

Par conséquent, en pensant à α comme à une inclusion, nous sommes en mesure de supposer que $a_0, {a_0}^{-1}, a_1, \cdots, a_{d-1} \in \mathbb{Z}_p$ et que $(u_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{Z}_p$. On note A la matrice compagnon associée aux $a_0, \cdots, a_{d-1}$ et on introduit :

$$\forall n \in \mathbb{N}, v_n := \begin{pmatrix} u_n \\ \vdots \\ u_{n+d-1} \end{pmatrix}.$$

À l'aide de (32), on montre par récurrence que l'on a :

$$\forall n \in \mathbb{N}, v_n = A^n v_0. \tag{33}$$

Soit f l'élément de $\mathbb{Z}_p[X_1, \cdots, X_d]^d$ obtenu par multiplication à droite de A par le vecteur colonne constitué des $X_1, \cdots, X_d$, Ainsi, d'après (33) il vient :

$$v_n = f^n(v_0). \tag{34}$$

En développant le déterminant de A par rapport à sa première colonne, on a :

$$\det(A) = (-1)^{d+1} a_0. \tag{35}$$

On note $\overline{A}$ la matrice obtenue en réduisant modulo $p\mathbb{Z}_p$ les coefficients de A. De cette manière, d'après (35), il vient :

$$\det\left(\overline{A}\right) = (-1)^{d+1} a_0 \mod p\mathbb{Z}_p. \tag{36}$$

Or, comme $a_0 \in {\mathbb{Z}_p}^\times$, d'après la proposition 1.7 et la remarque 1.8, on a :

$$a_0 \mod p\mathbb{Z}_p \neq 0. \tag{37}$$

Ainsi, d'après (36), (37) et la remarque 3.10, on en déduit que l'on a :

$$\overline{A} \in \mathrm{GL}_d(\mathbb{Z}_p/p\mathbb{Z}_p).$$

Dès lors, en notant I_d l'élément neutre de $\mathscr{M}_d(\mathbb{Z}_p)$, d'après le corollaire 3.11, il existe $m \in \mathbb{N}_{\geqslant 1}$ tel que l'on ait l'égalité suivante dans $\mathscr{M}_d(\mathbb{Z}_p/p\mathbb{Z}_p)$:

$$\left(\overline{A}\right)^m = \overline{I_d}.$$

En d'autres termes, il existe $B \in \mathscr{M}_d(Z_p)$ satisfaisant à l'égalité suivante :

$$A^m = I_d + pB. \tag{38}$$

Soit $I := (X_1, \cdots, X_d)$, en multipliant (38) par le vecteur colonne constitué des $X_1, \cdots, X_d$, on obtient l'existence de $h \in \mathbb{Z}_p[X_1, \cdots, X_d]^d$ tel que :

$$f^m = I + ph.$$

Autrement dit, on a $f^m - I \in p\mathbb{Z}_p[X_1, \cdots, X_d]^d$ et d'après le théorème 2.13, quel que soit $i \in [\![0, m-1]\!]$, il existe $g_i \in \mathbb{Q}_p[[X]]^d$ qui converge en chaque point de $\mathbb{Z}_p$ et satisfaisant à la relation suivante :

$$\forall n \in \mathbb{N}, g_i(n) = f^{mn}(v_i). \tag{39}$$

Par conséquent, d'après (34) et (39), il vient :

$$\forall n \in \mathbb{N}, v_{mn+i} = g_i(n). \tag{40}$$

Cependant, d'après le théorème 1.37, quel que soit $(i, j) \in [\![0, m-1]\!] \times [\![1, d]\!]$, on a la dichotomie suivante :

- La $j^{\text{ème}}$ composante de g_i est nulle, ce qui avec (40) implique que l'on a :

$$\forall n \in \mathbb{N}, u_{mn+i+j-1} = 0.$$

- La $j^{\text{ème}}$ composante de g_i ne s'annule qu'un nombre fini de fois dans $\mathbb{Z}_p$, ce qui avec (40) implique que l'on a :

$$\#\{n \in \mathbb{N} \text{ t.q. } u_{mn+i+j-1} = 0\} < \infty.$$

$\{mn + i + j - 1; n \in \mathbb{N}\}_{\substack{i \in [\![0,m-1]\!] \\ j \in [\![1,d]\!]}}$ recouvrant $\mathbb{N}$, on a le résultat annoncé.

□

Compte tenu de la discussion faite lors de l'introduction, nous venons également d'établir le théorème suivant :

Théorème 3.14. Soient k un corps de caractéristique zéro, $x \in k^d$ et σ un automorphisme linéaire de k^d. Si H est un hyperplan de k^d, alors l'ensemble :

$$\{n \in \mathbb{N} \text{ t.q. } \sigma^n(x) \in H\}$$

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

3.3. **Le cas des automorphismes polynomiaux affines.**

Définition 3.15. Soit X un sous-ensemble de k^d, X est une sous-variété de $\mathbb{A}_k^d$ si et seulement s'il existe $P_1, \cdots, P_m \in k[X_1, \cdots, X_d]$ tels que l'on ait :

$$X := \left\{(x_1, \cdots, x_d) \in k^d \text{ t.q. } \forall i \in [\![1, m]\!], P_i(x_1, \cdots, x_d) = 0\right\}.$$

Remarque 3.16. Autrement dit, une sous-variété de $\mathbb{A}_k^d$ est l'ensemble des zéros communs sur k d'un ensemble fini de polynômes à d variables.

Théorème 3.17. (Bell [1]) Soient k un corps de caractéristique zéro, $x \in \mathbb{A}_k^d$ et σ un automorphisme de $\mathbb{A}_k^d$. Si X est une sous-variété de $\mathbb{A}_k^d$, alors l'ensemble :

$$\{m \in \mathbb{Z} \text{ t.q. } \sigma^m(x) \in X\}$$

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

Soient $x_1, \cdots, x_d$ les coordonnées de x dans k et $f_1, \cdots, f_d$, respectivement $g_1, \cdots, g_d$, les coordonnées de σ, respectivement de σ^{-1}, dans $k[X_1, \cdots, X_d]$. Par ailleurs, il existe $P_1, \cdots, P_m$ dans $k[X_1, \cdots, X_d]$ tels que X soit l'ensemble des zéros communs dans k de $P_1, \cdots, P_m$. On pose alors S l'ensemble constitué des $x_1, \cdots, x_d$ et des coefficients dans k de $f_1, \cdots, f_d, g_1, \cdots, g_d, P_1, \cdots, P_m$. Dès lors, en notant K le corps engendré par S sur $\mathbb{Q}$, d'après le théorème 3.8, il existe un nombre premier $p \geqslant 3$ et un plongement $\alpha : K \hookrightarrow \mathbb{Q}_p$ tels que :

$$\forall s \in S, \alpha(s) \in \mathbb{Z}_p.$$

Par conséquent, en pensant à α comme à une inclusion, nous sommes en mesure de supposer que $x \in \mathbb{A}_{\mathbb{Z}_p}^d$, que σ est un automorphisme de $\mathbb{A}_{\mathbb{Z}_p}^d$ et que X est définie par des polynômes à coefficients dans $\mathbb{Z}_p$. Finalement, pour établir complètement le théorème 3.17, il resterait à montrer que le théorème 2.13 s'applique à une itérée de σ et l'on conclurait en utilisant le théorème 1.37.

Annexe A. Base de transcendance d'une extension de corps

Soit L/K une extension de corps.

Définition A.1. Soit S un sous-ensemble de L, S est algébriquement indépendant sur K si et seulement si pour toute partie finie $\{x_1, \cdots, x_n\}$ de S, on a :

$$\forall P \in K[X_1, \cdots, X_n], P(x_1, \cdots, x_n) = 0 \Rightarrow P = 0.$$

Définition A.2. Soit S un sous-ensemble de L, S est une base de transcendance de L/K si et seulement si S satisfait aux propriétés suivantes :

i. S est algébriquement indépendant sur K.

ii. L est algébrique sur $K(S)$.

Proposition A.3. Soit S un sous-ensemble de L, alors les deux propriétés suivantes sont équivalentes :

i. S est une base de transcendance de L/K.

ii. S est algébriquement indépendant sur K et maximal pour cette propriété, ainsi pour tout $x \in L$, $S \cup \{x\}$ est algébriquement dépendant sur K.

Preuve. On procède par double implication.

- Supposons que S soit une base de transcendance de L/K, alors S est algébriquement indépendant sur K. Par ailleurs, si $x \in L$, comme L est algébrique sur $K(S)$, il existe $F \in K(S)[X] \setminus \{0\}$ tel que l'on ait :
$$F(x) = 0.$$
F ayant un nombre fini de coefficients dans $K(S)$ et les éléments de $K(S)$ étant des fractions rationnelles en un nombre fini d'éléments de S, il existe $x_1, \cdots, x_n \in S$ tels que $F \in K(x_1, \cdots, x_n)[X] \setminus \{0\}$. Ainsi, en multipliant F par le produit des dénominateurs de ses coefficients, on obtient $P \in K[x_1, \cdots, x_n][X] \setminus \{0\}$ satisfaisant à :
$$P(x) = 0.$$
En d'autres termes, il existe $\widetilde{P} \in K[X_1, \cdots, X_{n+1}] \setminus \{0\}$ tel que l'on ait :
$$\widetilde{P}(x_1, \cdots, x_n, x) = 0.$$
Dès lors, $S \cup \{x\}$ est algébriquement dépendant sur K. Finalement, S est algébriquement indépendant sur K et est maximal pour cette propriété.
- Supposons que S soit algébriquement indépendant sur K et maximal pour cette propriété, supposons par l'absurde que L ne soit pas algébrique sur $K(S)$, il existe alors $x \in L$ transcendant sur $K(S)$, on obtiendra une contradiction en montrant que $S \cup \{x\}$ est algébriquement indépendant. Pour ce faire, comme S est algébriquement indépendant sur K, il suffit de montrer que pour tout $x_1, \cdots, x_n \in S$, $\{x_1, \cdots, x_n, x\}$ est algébriquement indépendant sur K. Or, puisque x est transcendant sur $K(S)$, il vient :
$$\forall P \in K(S)[X], P(x) \Rightarrow P = 0.$$

En particulier, on en déduit que pour tous $x_1, \cdots, x_n \in S$, on a :

$$\forall P \in K[X_1, \cdots, X_n, X], P(x_1, \cdots, x_n, x) = 0 \Rightarrow P = 0.$$

Ainsi, $S \cup \{x\}$ est algébriquement indépendant sur K, ce qui contredit la maximalité de S. Finalement, S est une base de transcendance de L/K.

D'où le résultat annoncé.

□

Lemme A.4. Soient I un ensemble de parties de L et $\{x_1, \cdots, x_n\} \subseteq \bigcup_{S \in I} S$. Si $(I, \subseteq)$ est totalement ordonné, alors il existe $S \in I$ contenant $\{x_1, \cdots, x_n\}$.

Preuve. On procède par récurrence sur n.

- **Initialisation.** Si $n = 1$, $x_1 \in \bigcup_{S \in I} S$ et il existe $S \in I$ contenant x_1.
- **Hérédité.** Soit $n \geqslant 2$, on suppose qu'il existe $S_{n-1} \in I$ tel que l'on ait :

  $$\{x_1, \cdots, x_{n-1}\} \subseteq S_{n-1}.$$

  Par ailleurs, d'après l'étape d'initialisation, il existe $S_n \in I$ contenant x_n. Or, $(I, \subseteq)$ étant totalement ordonné, on suppose sans perte de généralité que S_{n-1} est contenu dans S_n, si bien que S_n contient $\{x_1, \cdots, x_{n-1}\}$. Finalement, on a $\{x_1, \cdots, x_n\} \subseteq S_n$.

D'où le résultat annoncé.

□

Proposition A.5. Il existe au moins une base de transcendance de L/K.

Preuve. Soit E l'ensemble des parties algébriquement indépendantes de L/K. On commence par constater que l'ensemble E est non vide, en effet, $\varnothing \in E$. Soit I une partie de E totalement ordonnée pour l'inclusion, alors $\bigcup_{S \in I} S \in E$. En effet, sinon il existerait $\{x_1, \cdots, x_n\} \subseteq \bigcup_{S \in I} S$ et $P \in K[X_1, \cdots, X_n]$ non nul satisfaisant à l'égalité suivante :

$$P(x_1, \cdots, x_n) = 0.$$

D'après le lemme A.4, il existerait alors $S \in I \subseteq E$ tel que l'on ait :

$$\{x_1, \cdots, x_n\} \subseteq S.$$

Dès lors, S serait algébriquement dépendant sur K et $S \notin E$, ce qui n'est pas. Par conséquent, d'après le lemme de Zorn [4], E contient un élément maximal. Finalement, d'après la proposition A.3, L/K admet une base de transcendance. D'où le résultat annoncé.

□

Remarque A.6. On pourrait montrer que toutes les bases de transcendance de L/K ont même cardinal [9], on l'appelle le degré de transcendance de L/K.

Références

[1] J.P. Bell. A generalised Skolem-Mahler-Lech theorem for affine varieties. *Journal of the London Mathematical Society*, 73 :367–379, 2006.

[2] Z.I. Borevitch et I.R. Chafarevitch. *Number Theory*, pages 18–32. Academic Press, 1966.

[3] J.W.S. Cassels. An embedding theorem for fields. *Bulletin of the Australian Mathematical Society*, 14 :193–198, 1976.

[4] K. Ciesielski. *Set Theory for the Working Mathematician*, pages 53–54. London Mathematical Society, 1997.

[5] H. Derksen. A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Inventiones Mathematicae*, 168 :175–224, 2007.

[6] X. Gourdon. *Les maths en tête, Algèbre*, pages 279–281. Ellipses, 2009.

[7] K. Hensel. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 6 :83–88, 1897.

[8] S. Katok. *p-adic Analysis Compared with Real*, pages 53–60, 75–86 et 98–102. American Mathematical Society, 2007.

[9] S. Lang. *Algebra*, pages 355–356. Springer, 2002.

[10] C. Lech. A note on recurring series. *Arkiv för Matematik*, 2 :417–421, 1954.

[11] K. Mahler. Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen. *Akadamie van Wetenschappen Amsterdam*, 38 :50–60, 1935.

[12] B. Poonen. p-adic interpolation of iterates. *Bulletin of the London Mathematical Society*, 46 :525–527, 2014.

[13] P. Samuel. *Théorie algébrique des nombres*, pages 39–41. Hermann, 1967.

[14] J.-P. Serre. *Cours d'arithmétique*, pages 23–30. PUF, 1995.

[15] T. Skolem. Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen. *Skrifter Norske Vitenskapsakademiet Oslo*, 6 :1–61, 1933.

[16] R. Strassmann. Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen. *Journal für die reine und angewandte Mathematik*, 159 :13–28, 1928.