République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université Mohammed Seddik Ben Yahia - Jijel

Faculté des Sciences Exactes et Informatique

Département de Mathématique

Mémoire

Présenté pour l'obtention du diplôme de : ***Master***

Spécialité : *Mathématiques*

Option : *Analyse Fonctionnelle*

Thème

Théorème des Accroissements Finis p-adique

Présenté par :

Ghalia Samia

Lahoula Khadidja

Devant le jury :

Président :	*D. AFFANE*	*M.C.A*	*Univ. Jijel*
Encadreur :	*R. BELHADEF*	*M.C.B*	*Univ. Jijel*
Examinateur :	*B. SAOUDI*	*M.A.A*	*Univ. Jijel*

Promotion **2018/2019**

Remerciements

Nous tenons tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui nous a donné la force, la volonté, le courage et la patience d'accomplir ce Modeste travail.

La première personne que nous tenons à remercier est notre encadrant **Dr. Belhadef Rafik** *pour la patience, l'orientation et ses bonnes explications qui nous ont éclairé le chemin de la recherche et sa collaboration avec nous dans l'accomplissement de ce modeste travail.*

Nos vifs remerciements vont également aux membres du jury : Madame **Affane Doria M.C.A** *à l'université de Jijel, et Monsieur* **Saoudi Bilal M.A.A** *à l'université de Jijel, pour l'intérêt qu'ils ont porté à notre mémoire en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.*

Nous tenons à exprimer nos sincères remerciements à tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Nous adressons nos remerciements les plus chaleureux à nos familles et nos amis pour leur aoutien, encouragements et tout ce qu'ils ont fait pour nous pendant cette période.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Table des matières

Introduction

Dans ce mémoire, nous présentons le théorème des accroissements finis p-adique, et quelques applications de ce théorème.

Le théorème des accroissements finis réel est un théorème trés important dans l'analyse mathématique, eu égard au nombre de simplifications techniques qu'il permet. Il est utilisé pour démontrer de nombreuses théorèmes, par exemple : théorème de Schwarz, théorème de l'inverse locale,...etc. Ce théorème n'est pas valable toujours dans le cas p-adique, la condition $|h|_p \leq r_p = p^{-\frac{1}{p-1}}$ limite le domaine de validité de la version p-adique du théorème des accroissements finis. Donc on doit modifier les conditions sur la fonction en question pour avoir une inégalité ressemble a celle dans le cas réel.

Le théorème des accroissements finis p-adique à été obtenu en 1991 par **Alain Robert** dans l'article "A note on the numerators of the Bernoulli numbers" [16], puis il a détaillé ce théorème en 1995 dans le deuxième article "le théorème des accroissements finis p-adique" [18] et dans son livre "A course in p-adic analysis" [15] éditer en 2000.

En 1992, **Maxime Zuber** a utilisé dans sa thèse de doctorat [22], le théorème des accroissements finis p-adique établit par **Robert** pour démontrer des résultats concernant les polynômes de Bernoulli, Euler et Chebyshev,...etc.

En 2003, dans sa thèse de doctorat [10], **Alexandre Junod** a fait aussi des démonstrations de congruence en utilisant le théorème des accroissements finis p-adique.

En 2014, **Bertin Diara et Djeidi Sylla** [7], ont généralisé le travail de **Maxime Zuber** [22] sur les polynômes de Chebyshev T_q, avec $q = p^\nu$ telle que $\nu \geq 1$ et $p > 2$.

Ce mémoire autour de trois chapitres précède par une introduction, qui sont organisés comme suit :

Dans le premier chapitre, on va rappeler les outils nécessaire de base pour l'analyse p-adique dont on aura besoin. Nous commençons par la construction du corps des nombres p-adique $\mathbb{Q}_p$, qui est la complétion de $\mathbb{Q}$ par rapport à la norme p-adique $|.|_p$. Nous terminons par la construction du corps des nombres complexe p-adiques $\mathbb{C}_p$, qui est la complétion de la clôture algébrique de $\mathbb{Q}_p$ muni de la norme p-adique.

Le deuxième chapitre, commence par l'étude des propriétés de convergence des suites et des séries dans $\mathbb{Q}_p$, ensuite l'étude des sériers entières et des fonctions p-adiques (continuité, différentiabilité,...). En termine le chapitre par les définitions et les propriétés de la fonction exponentielle et logarithme p-adique, puis quelques définitions de l'analyse dans $\mathbb{C}_p$.

Dans le dernier chapitre, nous rappelons le théorème des accroissements finis dans un espace vectoriel normé, puis nous présentons ce théorème dans le cas p-adique. Dans la dernière partie du chapitre, on donne la façon d'utiliser le théorème des accroissements finis p-adique pour démontrer, le théorème du point fixe p-adique, le théorème de Wolstenholme, les propriétés des polynômes connus, et pour établir des congruences sur les coefficients binomiaux.

Enfin, nous finissons ce mémoire par une liste des références approuvé dans ce travail.

Notations

Nous utilisons les notations suivantes :

$\mathbb{K}$: Un corps.

E, F : Deux espaces vectoriels normés.

$\|.\|_{\mathbb{K}}$: La norme sur un corps $\mathbb{K}$.

p : Un nombre premier, $p = 2, 3, 5, 7, ...$

$\mathbb{Z}$: L'ensemble des entiers relatifs réels.

$\mathbb{Z}^*$: L'ensemble des entiers relatifs réels non nuls.

$\mathbb{R}$: L'ensemble des nombres réels.

$\mathbb{N}$: L'ensemble des entiers naturels.

$\mathbb{N}^*$: L'ensemble des entiers naturels non nuls.

$\mathbb{Q}$: L'ensemble des nombres rationnels.

$\mathbb{Q}^*$: L'ensemble des nombres rationnels non nuls.

$\mathbb{Q}_p$: L'ensemble des nombres p-adiques.

$\mathbb{Q}_p^*$: L'ensemble des nombres p-adiques non nuls.

$\overline{\mathbb{Q}}_p$: La clôture algébrique du corps $\mathbb{Q}_p$.

$\mathbb{Z}_p$: L'ensemble des entiers p-adique.

$\mathbb{Z}_p^\times$: L'ensemble des éléments inversibles dans $\mathbb{Z}_p$.

$\mathbb{C}_p$: L'ensemble des nombres complexes p-adiques.

$(a, b) = 1$: a et b sont premiers entre eux.

$v_p(x)$: La valuation p-adique de x.

$|.|_p$: La norme p-adique.

$\mathbb{K}[.]$: L'ensemble des polynômes sur le corps $\mathbb{K}$.

$\mathbb{K}[[.]]$: L'ensemble des séries entières sur le corps $\mathbb{K}$.

$B_{\leq 1}(\mathbb{C}_p)$: La boule fermé de centre 0 et de rayon 1 sur $\mathbb{C}_p$.

$\mathbb{K}\{.\}$: L'ensemble des séries formelles restreintes sur $\mathbb{K}$.

$\mathcal{L}(E, F)$: L'ensemble des applications linéaires continues de E dans F.

r_f : Le rayon de convergence d'une série entière p-adique.

r_p : Le rayon de convergence de l'exponentielle p-adique.

$[x]$: La partie entière réel de x.

$\|.\|$: La norme de Gauss d'une série entière.

CHAPITRE 1

Préliminaires sur les nombres p-adiques

Le but de ce chapitre est de présenter la base du domaine p-adique. Nous commençons par quelques définitions et propriétés concernant la valuation et la norme p-adique, ensuite nous présentons la construction du corps des nombres p-adique et le développement de Hensel. Enfin, nous donnons quelques définitions sur le corps $\mathbb{C}_p$.

1.1 Norme p-adique sur $\mathbb{Q}$

Définition 1.1. *Soit $\mathbb{K}$ un corps. On appelle norme sur $\mathbb{K}$ une application $\|.\|_{\mathbb{K}}$ de $\mathbb{K}$ dans $\mathbb{R}_+$ vérifiant les conditions suivantes :*

1) $\|x\|_{\mathbb{K}} = 0 \Leftrightarrow x = 0$.

2) $\|xy\|_{\mathbb{K}} = \|x\|_{\mathbb{K}}.\|y\|_{\mathbb{K}} \quad \forall x, y \in \mathbb{K}$.

3) $\|x+y\|_{\mathbb{K}} \leq \|x\|_{\mathbb{K}} + \|y\|_{\mathbb{K}} \quad \forall x, y \in \mathbb{K}$ *(inégalité triangulaire).*

On dit que $\mathbb{K}$ est un corps non-archimédien et la norme $\|.\|_{\mathbb{K}}$ est non-archimédienne si en peut remplacé la troisième condition par l'inégalité triangulaire forte, i.e.,

$$\|x+y\|_{\mathbb{K}} \leq \max(\|x\|_{\mathbb{K}}, \|y\|_{\mathbb{K}}) \quad \forall x, y \in \mathbb{K}.$$

Définition 1.2 (Valuation p-adique)**.**

Soit p un nombre premier et $\alpha \in \mathbb{Z}$. La valuation p-adique de α, notée $v_p(\alpha)$; est le plus grand entier $n \in \mathbb{N}$ tel que p^n divise α, i.e., $\alpha = p^n n_1$ avec p ne divise pas n_1.
De plus, pour $x \in \mathbb{Q}$ tel que $x = \dfrac{a}{b}$ où $a \in \mathbb{Z}, b \in \mathbb{Z}^*$, on a

$$v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Par convention, on a $v_p(0) = +\infty$.

Exemple 1.3.

1) $v_p(1) = 0, \forall p \geq 2$.

2) Soit $\alpha = 1 + 2p + 2p^2$, $\forall p > 2$, *alors* $v_p(\alpha) = 0$.

3) Si $24 = 2.3 + 2.3^2$, *alors* $v_3(24) = 1$.

Proposition 1.4. *Pour tout $a, b \in \mathbb{Q}$, on a*

1) $v_p(a) = +\infty \Leftrightarrow a = 0$.

2) $v_p(ab) = v_p(a) + v_p(b)$.

3) $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

Démonstration.

1) Par définition, on a

$$v_p(a) = +\infty \Leftrightarrow v_p(a) = v_p(0) \Leftrightarrow a = 0.$$

2) Soient $a, b \in \mathbb{Z}^*$ tel que : $a = p^\alpha n_1$, $b = p^\beta n_2$ et $(n_1, p) = 1$, $(n_2, p) = 1$, alors

$$v_p(a) = \alpha \ \ et \ \ v_p(b) = \beta$$

On a

$$ab = p^\alpha p^\beta n_1 n_2 = p^{\alpha+\beta} n_1 n_2$$

Comme p ne divise pas $n_1 n_2$, alors

$$v_p(ab) = \alpha + \beta = v_p(a) + v_p(b).$$

▶ Dans le cas $a, b \in \mathbb{Q}^*$, soit $a = \frac{a_1}{a_2}$, $b = \frac{b_1}{b_2}$ où $a_1, a_2, b_1, b_2 \in \mathbb{Z}^*$, on a

$$\begin{aligned} v_p(ab) &= v_p\left(\frac{a_1 b_1}{a_2 b_2}\right) \\ &= v_p(a_1 b_1) - v_p(a_2 b_2) \\ &= v_p(a_1) + v_p(b_1) - v_p(a_2) - v_p(b_2) \\ &= v_p\left(\frac{a_1}{a_2}\right) + v_p\left(\frac{b_1}{b_2}\right) \\ &= v_p(a) + v_p(b). \end{aligned}$$

3) Soient $a, b \in \mathbb{Z}^*$ tel que : $a = p^\alpha n_1$, $b = p^\beta n_2$ et $(n_1, p) = 1$, $(n_2, p) = 1$.

• Si $\alpha \leq \beta$, on a

$$a + b = p^\alpha n_1 + p^\beta n_2 = p^\alpha (n_1 + p^{\beta-\alpha} n_2)$$

Comme $(n_1', p) = 1$ tel que $n_1' = (n_1 + p^{\beta-\alpha} n_2)$, alors

$$v_p(a+b) = \alpha = \min(v_p(a), v_p(b)).$$

• Si $\alpha \geq \beta$, on a

$$a + b = p^\alpha n_1 + p^\beta n_2 = p^\beta (n_1 p^{\alpha-\beta} + n_2)$$

Comme $(n_2', p) = 1$ tel que $n_2' = (n_1 p^{\alpha-\beta} + n_2)$, alors

$$v_p(a+b) = \beta = \min(v_p(a), v_p(b)).$$

▶ Dans le cas $a, b \in \mathbb{Q}^*$, soit $a = \frac{a_1}{a_2}$, $b = \frac{b_1}{b_2}$ où $a_1, a_2, b_1, b_2 \in \mathbb{Z}^*$, on a

$$\begin{aligned} v_p(a+b) &= v_p\left(\frac{a_1}{a_2} + \frac{b_1}{b_2}\right) \\ &= v_p\left(\frac{a_1 b_2 + a_2 b_1}{a_2 b_2}\right) \\ &= v_p(a_1 b_2 + a_2 b_1) - v_p(a_2) - v_p(b_2) \\ &\geq \min\left(v_p(a_1 b_2), v_p(a_2 b_1)\right) - v_p(a_2) - v_p(b_2) \\ &= \min\left(vp(a_1) + vp(b_2) - vp(a_2) - vp(b_2), vp(a_2) + vp(b_1) - vp(a_2) - vp(b_2)\right) \\ &= \min(v_p(a), v_p(b)) \end{aligned}$$

□

Remarque. *Pour tout $a, b \in \mathbb{Q}$, on a*

$$v_p(a) \neq v_p(b) \Rightarrow v_p(a+b) = \min(v_p(a), v_p(b)).$$

Définition 1.5. *On définit la norme p-adique $|.|_p$ sur $\mathbb{Q}$ comme suit :*

$$|x|_p = \begin{cases} p^{-v_p(x)} & si \quad x \neq 0 \\ 0 & si \quad x = 0 \end{cases}$$

Proposition 1.6. *L'application $|.|_p$ définit une norme non archimédienne sur $\mathbb{Q}$.*

Démonstration.

1) $|x|_p = 0 \Leftrightarrow x = 0$

   On a $|x|_p = 0$, alors

$$p^{-v_p(x)} = 0 \Rightarrow v_p(x) = +\infty \Rightarrow x = 0$$

   On a $x = 0$, alors $|0|_p = 0$ (par définition).

2) $|xy|_p = |x|_p |y|_p \quad \forall x, y \in \mathbb{Q}$

   Pour tout $x, y \in \mathbb{Q}$, on a

$$|xy|_p = p^{-v_p(xy)}$$

   D'après la proposition 1.4, nous avons

$$v_p(xy) = v_p(x) + v_p(y)$$
$$-v_p(xy) = -v_p(x) - v_p(y)$$

   Donc

$$|xy|_p = p^{-v_p(x)-v_p(y)} = p^{-v_p(x)} p^{-v_p(y)} = |x|_p |y|_p.$$

3) $|x+y|_p \leq \max(|x|_p, |y|_p) \quad \forall x, y \in \mathbb{Q}$

   Pour tout $x, y \in \mathbb{Q}$, on a

$$|x+y|_p = p^{-v_p(x+y)}$$

   On sait que

$$v_p(x+y) \geq \min(v_p(x), v_p(y))$$
$$-v_p(x+y) \leq -\min(v_p(x), v_p(y))$$

Alors

$$\begin{aligned} p^{-v_p(x+y)} &\leq p^{-\min(v_p(x),v_p(y))} \\ &= p^{\max(-v_p(x),-v_p(y))} \\ &= \max(p^{-v_p(x)}, p^{-v_p(y)}) \\ &= \max(|x|_p, |y|_p) \end{aligned}$$

D'où

$$|x+y|_p \leq \max(|x|_p, |y|_p).$$

$\square$

Remarque. *Les valeurs de la norme p-adique sont donnée par l'ensemble suivant :*

$$\{p^n, n \in \mathbb{Z}\} \cup \{0\}.$$

Proposition 1.7. *Soit $x, y \in \mathbb{Q}$. Si $|x|_p \neq |y|_p$, alors $|x+y|_p = \max\{|x|_p, |y|_p\}$.*

Démonstration. On pose $|x|_p < |y|_p$, alors

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} = |y|_p \tag{1.1}$$

Et d'autre part

$$|y|_p = |y+x-x|_p \leq \max\{|x+y|_p, |x|_p\} = |x+y|_p$$

Donc

$$\max\{|x|_p, |y|_p\} \leq |x+y|_p \tag{1.2}$$

De (1.1) et (1.2), on a

$$|x+y|_p = \max\{|x|_p, |y|_p\}$$

(De la même manière pour $|x|_p > |y|_p$). $\square$

Proposition 1.8. *Si $a, b \in \mathbb{Z}$, alors*

$$a \equiv b \pmod{p^n} \Leftrightarrow |a-b|_p \leq p^{-n}, \ \forall n \geq 0.$$

Démonstration. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$.

$\Rightarrow$) Montrons que $|a-b|_p \leq p^{-n}, \forall n \geq 0$

Si $a \equiv b \pmod{p^n}$, $\forall n \geq 0$, alors

$$\exists k \in \mathbb{Z} \ \textit{tel que} \ a - b = kp^n$$

D'où

$$\begin{aligned} |a-b|_p &= |k|_p |p^n|_p \\ &\leq p^{-n}, \ \forall n \end{aligned}$$

$\Leftarrow$) Montrons que $a \equiv b \pmod{p^n}$

Si $|a-b|_p \leq p^{-n}$, $\forall n$, alors

$$\begin{aligned} |a-b|_p \leq p^{-n} &\Leftrightarrow p^{-v_p(a-b)} \leq p^{-n} \\ &\Leftrightarrow n \leq v_p(a-b) \\ &\Leftrightarrow v_p(a-b) - n \geq 0 \end{aligned}$$

Par définition, on a

$$\begin{aligned} a - b &= p^{v_p(a-b)}.n_1, \ \textit{où} \ (n_1, p) = 1, \ n_1 \in \mathbb{N} \\ &= p^{v_p(a-b)} p^n p^{-n}.n_1 \\ &= p^{v_p(a-b)-n} p^n.n_1 \\ &= kp^n, \ \textit{tel que} \ k = p^{v_p(a-b)-n}.n_1 \in \mathbb{N} \end{aligned}$$

Alors

$$a \equiv b \pmod{p^n}.$$

□

1.2 Construction du corps des nombres p-adiques

Il est bien connu que le corps $\mathbb{Q}$ n'est pas complet par rapport à la valeur absolue usuelle $|.|$, on complète ce corps par la méthode de complétion connu dans la topologie on trouve le corps des nombres réels $\mathbb{R}$ associée à la valeur absolue usuelle $|.|$. En appliquant le même théorème sur le corps $\mathbb{Q}$ mais par rapport à la norme p-adique $|.|_p$, nous obtenons

le corps des nombres p-adiques associée à la norme p-adique $|.|_p$ on le note $\mathbb{Q}_p$.
Dans l'exemple suivant on va démontrer que le corps $\mathbb{Q}$ n'est pas complet par rapport à la norme p-adique $|.|_p$.

Exemple 1.9.

Soit $y \in \mathbb{Q}$ et $1 \leq y < p$, soit la suite de terme général $\alpha_n = y^{p^n}$.
D'après le théorème de Fermat-Euler, on a

$$y^{p^n(p-1)} - 1 \equiv 0 (\mathrm{mod}\, p^n)$$

Alors

$$\begin{aligned} |\alpha_{n+1} - \alpha_n|_p &= |y^{p^n}(y^{p^n(p-1)} - 1)|_p \\ &= |y^{p^n}|_p |(y^{p^n(p-1)} - 1)|_p \\ &\leq p^{-n} \end{aligned}$$

Donc

$$\lim_{n \to +\infty} |\alpha_{n+1} - \alpha_n|_p = 0$$

Donc la suite $(\alpha_n)_n$ est de Cauchy dans $\mathbb{Q}$ muni de la norme $|.|_p$.
Pour montrer que le corps $\mathbb{Q}$ n'est pas complet par rapport à la valeur absolue p-adique $|.|_p$, il suffit de montrer que la suite $(\alpha_n)_n$ n'est pas converge dans $\mathbb{Q}$.
On suppose que α_n converge vers $\alpha \in \mathbb{Q}$, c'est-à-dire

$$\begin{aligned} \alpha &= \lim_{n \to +\infty} \alpha_n = \lim_{n \to +\infty} \alpha_{n+1} \\ &= \lim_{n \to +\infty} (\alpha_n)^p \\ &= \alpha^p \end{aligned}$$

Alors

$$\begin{aligned} \alpha - \alpha^p = 0 &\Rightarrow \alpha(\alpha^{p-1} - 1) = 0 \\ &\Rightarrow \alpha^{p-1} = 1 \end{aligned}$$

Cela signifie que α est une $(p-1)^{ieme}$ racine de l'unité dans $\mathbb{Q}$, donc égale à 1.
D'autre part, on a

$$\begin{aligned} |\alpha - y|_p &= |\alpha - y^{p^n} + y^{p^n} - y|_p \\ &\leq max(|\alpha - y^{p^n}|_p, |y^{p^n} - y|_p) \\ &\leq |y^{p^n - 1} - 1|_p < 1 \end{aligned}$$

Alors $p^{-v_p(\alpha-y)} < 1$*, d'où* $v_p(\alpha - y) \geq 1$*, ainsi* p *divise* $\alpha - y$*, cela signifie que* $\alpha = y$*.*
Si $y \neq 1$ *on aura une contradiction, donc* $\alpha \notin \mathbb{Q}$*.*
Alors le corps $\mathbb{Q}$ *n'est pas complet par rapport à la valeur absolue* p*-adique* $|.|_p$*.*

Proposition 1.10. $(\mathbb{Q}_p, +, .)$ *est un corps.*

Démonstration.

Pour montrons que $\mathbb{Q}_p$ est un corps, il suffit de montrer que $(\mathbb{Q}_p, +, .)$ est un anneau commutatif et pour tout $\alpha \in \mathbb{Q}_p$ non nul admet un inverse dans $\mathbb{Q}_p$.

1. Il est clair que $(\mathbb{Q}_p, +, .)$ est un anneau commutatif.
2. Soit $(\alpha_n) \in \mathbb{Q}$ une suite de Cauchy de limite α alors :

$$\lim_{n\to+\infty} |\alpha_n|_p = |\alpha|_p \neq 0$$

Donc $|\alpha_n|_p$ est aussi non nul pour n assez grand. Pour $N \in \mathbb{N}$, on définit une suite γ_n d'élément de $\mathbb{Q}$ par :

$$\gamma_n = \begin{cases} 0 & si \quad n < N \\ \frac{1}{\alpha_n} & si \quad n \geq N \end{cases}$$

Pour tout $n, m \geq N$, on a

$$|\gamma_n - \gamma_m|_p = \frac{|\alpha_n - \alpha_m|_p}{|\alpha_n|_p |\alpha_m|_p}$$

On a la suite (α_n) est de cauchy dans $\mathbb{Q}$, donc $|\alpha_n - \alpha_m|_p \to 0$, quand $n \to +\infty$
Alors $|\gamma_n - \gamma_m|_p \to 0$, quand $n \to +\infty$.
C'est-à-dire γ_n est une suite de Cauchy dans $\mathbb{Q}$, donc elle converge vers $\gamma \in \mathbb{Q}_p$, et comme $\alpha_n \gamma_n = 1$, alors $\alpha\gamma = 1$.
Donc pour tout $\alpha \in \mathbb{Q}_p$ non nul admet un inverse dans $\mathbb{Q}_p$.

□

Remarque. *Comme* $|.|_p$ *est une norme non-archimédienne sur* $\mathbb{Q}$*, alors* $\mathbb{Q}_p$ *est un corps complet non-archimédienne.*

Définition 1.11. *L'ensemble des entiers* p*-adiques est le disque unitaire suivant :*

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

Définition 1.12. *On peut aussi définir le corps des nombres p-adique $\mathbb{Q}_p$ par :*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \; ; \; a \in \mathbb{Z}_p \; et \; b \in \mathbb{Z}_p^* \right\}.$$

Définition 1.13. *L'ensemble $\mathbb{Z}_p^\times$ des éléments inversibles dans $\mathbb{Z}_p$ est défini par :*

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p : |a|_p = 1\}.$$

Les éléments de $\mathbb{Z}_p^\times$ s'appelant les unités, et $\mathbb{Z}_p^\times$ est le groupe des unités.

Définition 1.14. *Soit $x \in \mathbb{Q}_p$. On définit $p^n\mathbb{Z}_p$ par l'ensemble suivant :*

$$\begin{aligned} p^n\mathbb{Z}_p &= \{x \in \mathbb{Q}_p : x = p^n a; a \in \mathbb{Z}_p\} \\ &= \left\{ x \in \mathbb{Q}_p : |x|_p \leq \frac{1}{p^n} \right\}. \end{aligned}$$

Proposition 1.15. *Soit $x \in \mathbb{Q}$, $|x|_p \leq 1$, alors*

$$\forall i \geq 1, \exists \alpha \in \mathbb{Z} \quad \textit{tel que } 0 \leq \alpha \leq p^i - 1 \quad \textit{et} \quad |x - \alpha|_p \leq p^{-i}.$$

Démonstration. Soit $x \in \mathbb{Q}$ tel que $x = \frac{a}{b}$ et $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $(a, b) = 1$.
Nous avons

$$\begin{aligned} |x - \alpha|_p &= |x - am + am - \alpha|_p \\ &\leq \max(|x - am|_p, |am - \alpha|_p) \end{aligned}$$

On a

$$\begin{aligned} |x|_p \leq 1 &\Rightarrow \frac{|a|_p}{|b|_p} \leq 1 \\ &\Rightarrow \frac{p^{v_p(b)}}{p^{v_p(a)}} \leq 1 \end{aligned}$$

D'où $(b, p) = 1$, alors $v_p(b) = 0$.
Donc

$$(b, p^i) = 1, \; \forall i \geq 1$$

Alors, d'après le théorème de Bézout il existe $m, n \in \mathbb{Z}$ tel que $mb + np^i = 1$, $\forall i \geq 1$.
Donc

$$|x - am|_p = \left| \frac{a}{b} - am \right|_p = \left| \frac{a}{b} \right|_p |1 - mb|_p \leq |p^i|_p \tag{1.3}$$

D'autre part, par division euclidienne, on a : $am = \alpha + kp^i$ avec $0 \leq \alpha \leq p^i - 1$ et

$$|am - \alpha|_p = |p^i|_p |k|_p \leq p^{-i} \tag{1.4}$$

De (1.3) et (1.4), on a

$$\forall i \geq 1, \exists \alpha \in \mathbb{Z} \quad \textit{tel que } 0 \leq \alpha \leq p^i - 1 \quad \textit{et} \quad |x - \alpha|_p \leq p^{-i}.$$

□

Proposition 1.16. *[11] Soit $x \in \mathbb{Z}_p$ tel que $|x|_p = p^{-n}$, $n \in \mathbb{Z}$, on peut écrire x sous la forme*

$$x = p^n u \;, \;\; \textit{où} \;\; u \in \mathbb{Z}_p^{\times}.$$

Puisque si on pose $u = p^{-v_p(x)}x$ alors $|u|_p = 1$ et on a $x = p^{v_p(x)}u$.

Proposition 1.17. *Tout $a \in \mathbb{Q}_p \setminus \{0\}$ admet une unique représentation $a = p^n u$ où $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^{\times}$ et $v_p(u) = 0$.*

Démonstration.

a) **Existence de la représentation :**
Soit $a \in \mathbb{Q}_p \setminus \{0\}$ alors $a = \frac{x}{y}$ où $x \in \mathbb{Z}_p$, $y \in \mathbb{Z}_p^*$.
On sait que $x = x_0 p^n$ et $y = y_0 p^m$ où x_0, y_0 des unités dans $\mathbb{Z}_p$, alors $n = v_p(x)$ et $m = v_p(y)$, d'où

$$a = \frac{x_0 p^n}{y_0 p^m} = \frac{x_0}{y_0} p^{n-m}$$

On met $u = \frac{x_0}{y_0}$, on a $|u|_p = 1$, donc $v_p(u) = 0$.

b) **Unicité de la représentation :**
Supposons que $a \in \mathbb{Q}_p^*$ admet deux représentation $a = up^n = wp^m$ avec u, w des unités dans $\mathbb{Z}_p$ et $n, m \in \mathbb{Z}$, alors

$$up^n = wp^m \Rightarrow uw^{-1} = p^{m-n} \Rightarrow v_p(uw^{-1}) = v_p(p^{m-n}) = m - n$$

Et on a uw^{-1} est une unité, alors $v_p(uw^{-1}) = 0 \Rightarrow n = m$.

□

1.3 Développement de Hensel

On va démontrer dans cette section que chaque élément dans $\mathbb{Q}_p$ s'écrit sous forme d'une série.

Proposition 1.18. *Soit $a \in \mathbb{Q}_p$ et $j_0 = v_p(a) \in \mathbb{Z}$. Il existe une unique suite $(a_n)_{n\in\mathbb{Z}}$, avec $0 \leq a_n \leq p-1$, pour tout $n \geq j_0$ tel que la série $\sum\limits_{n\geq j_0} a_n p^n$ converge vers a.*

Démonstration.

• Soit $a \in \mathbb{Q}_p$, $a \neq 0$; posons $b = p^{-v_p(a)}a$, alors $v_p(b) = 0$, i.e., $|b|_p = 1$.

Comme $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$, il existe $r \in \mathbb{Q}$ tel que $|b-r|_p \leq |p|_p$. On déduit de la proposition(1.15) qu' il existe $a_0 \in \mathbb{Z}$ tel que

$$0 < a_0 \leq p-1 \ et \ |r-a_0| \leq |p|_p$$

Ainsi $|b-a_0|_p \leq |p|_p$ et $b - a_0 = p^{n_1}b_1$, avec $n_1 \geq 1$ et $|b_1|_p = 1$.

De même, il existe a_1, $0 < a_1 \leq p-1$ tel que

$$b_1 - a_1 = p^{n_2'}b_2, \ n_2' \geq 1, \ |b_2|_p = 1$$

Ainsi

$$b = a_0 + a_1p^{n_1} + p^{n_1+n_2'}b_2 = a_0 + a_1p^{n_1} + p^{n_2}b_2$$

où $n_2 = n_1 + n_2' > n_1$.

Supposons par hypothèse de récurrence, avoir déterminer $a_0, a_1, ..., a_k$ et $n_1, n_2..., n_k$ tel que $0 < a_j \leq p-1$, $1 \leq j \leq k$, $n_1 < n_2 < ... < n_k$.

Et

$$b = a_0 + a_1p^{n_1} + ... + a_{k-1}p^{k-1} + p^{n_k}b_k, \ avec \ |b_k|_p = 1;$$

alors, il existe a_k, $0 < a_k \leq p-1$ et $n_k' \geq 1$ tel que

$$b_k - a_k = p^{n_k'}b_{k+1}, \ |b_{k+1}| = 1$$

Posons $n_k + n_k' = n_{k+1}$, on obtient

$$b = a_0 + a_1p^{n_1} + ... + a_kp^k + p^{n_{k+1}}b_{k+1}$$

Comme la suite $(n_k)_{k\geq 1}$ est strictement croissante, on a $\lim\limits_{k\to+\infty} n_k = +\infty$ et

$$\lim_{k\to+\infty} |p^{n_{k+1}}b_{k+1}|_p = 0$$

D'où

$$\lim_{k\to+\infty}\left(a_0+\sum_{j=1}^{k}a_jp^{n_j}\right)=\sum_{n\geq 0}a_np^n$$

où l'on a posé $a_n = 0$ lorsque $n \notin \{0, n_j, j \geq 1\}$.

• Si l'on a pour $|a|_p = 1$, un autre développement de forme

$$a=\sum_{n\geq 0}a'_np^n,\ 0\leq a'_n\leq p-1,\ alors\ |a'_0-a_0|_p\leq |p|_p$$

Ainsi, $a_0 \equiv a'_0\ (mod\ p)$ comme ces deux entiers sont compris entre 0 et $p-1$, ils sont égaux.

On voit alors de proche en proche que $a_n = a'_n,\ \forall n \geq 0$.

Sachant que tout $a \in \mathbb{Q}_p$ tel que $a = p^{v_p(a)}b = p^{j_0}b$, $|b|_p = 1$, on a le développement en série

$$a=\sum_{n\geq j_0}\alpha_np^n,\ où\ \ \alpha_n=a_{n-j_0},\ \ n\geq j_0.$$

$\square$

Définition 1.19. *Soit $a \in \mathbb{Q}_p$, on appel "**développement de Hensel**" de "a" la série suivante :*

$$a=\sum_{n\geq n_0}a_np^n$$

où $n_0 \in \mathbb{Z}$ et $0 \leq a_n \leq p-1$, $\forall n \geq n_0$, en particulier $a_{n_0} \neq 0$ et $v_p(a) = n_0$.

Définition 1.20. *Soit $a \in \mathbb{Z}_p$, son développement de Hensel est donné par :*

$$a=\sum_{n\geq 0}a_np^n\ \ où\ \ 0\leq a_n\leq p-1$$

1.4 Construction du corps des nombres complexes p-adiques

Définition 1.21. *Une extension d'un corps commutatif $\mathbb{K}$ est un corps E qui contient $\mathbb{K}$ comme sous-corps.*

Définition 1.22. *On dit qu'un corps $\mathbb{K}$ est algébriquement clôs si chaque polynôme $p(x)$ dans $\mathbb{K}[x]$ de degré n admet n racines dans $\mathbb{K}$.*

Définition 1.23. *Soit E une extension de $\mathbb{K}$. On dit que E est une extension algébrique de $\mathbb{K}$ lorsque tout élément de E est algébrique sur $\mathbb{K}$.*

Définition 1.24. *Soit E une extension de $\mathbb{K}$. On dit que E est une clôture algébrique de $\mathbb{K}$ si E est une extension algébrique de $\mathbb{K}$ qui est algébriquement clôs.*

On veut construire une extension complète algébriquement clôs de $\mathbb{Q}_p$. Comme le corps $\mathbb{Q}_p$ n'est pas algébriquement clôs (voir l'exemple 1.25), alors on peut considérer une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ et qui n'est pas complet.
Dans l'exemple suivant on va démontrer que le corps $\mathbb{Q}_p$ n'est pas algébriquement clôs.

Exemple 1.25. *On considère le polynôme $P(x) = x^2 - p^3 \in \mathbb{Q}_p[x]$.*
Supposons que les racines de $P(x)$ sont dans $\mathbb{Q}_p$, donc

$$\begin{aligned} P(x) = 0 &\Leftrightarrow x^2 = p^3 \\ &\Leftrightarrow |x^2|_p = |p^3|_p \\ &\Leftrightarrow |x|_p^2 = p^{-3} \\ &\Rightarrow |x|_p = p^{-\frac{3}{2}} \end{aligned}$$

c'est-à-dire que $v_p(x) = \frac{3}{2} \notin \mathbb{Z}$, contradiction avec $v_p(x) \in \mathbb{Z}$, pour tout $x \in \mathbb{Q}_p$.
Donc les racines de $P(x)$ ne sont pas dans $\mathbb{Q}_p$. Alors $\mathbb{Q}_p$ n'est pas algébriquement clôs.

Définition 1.26. *La complétion de la clôture algébrique $\overline{\mathbb{Q}}_p$ est appelé le corps des nombres complexes p-adique et est noté $\mathbb{C}_p$.*

Définition 1.27. *Soit $x \in \mathbb{C}_p^*$. On définit la norme p-adique dans $\mathbb{C}_p^*$ comme suit :*

$$|x|_p = \frac{1}{p^\alpha}\ , \ \ \alpha \in \mathbb{Q}.$$

CHAPITRE 2

Analyse élémentaire p-adique

Nous commençons ce chapitre par les définitions et les propriétés de la convergence des suites et des séries dans $\mathbb{Q}_p$, ensuite nous étudions les séries entières et ses propriétés, puis les fonctions élémentaires p-adiques (exponentielle et logarithme). Enfin, nous redéfinissons quelques propriétés dans $\mathbb{C}_p$.

2.1 Suites et séries p-adiques

Théorème 2.1. *Soit $(a_n)_{n\geq 0}$ une suite dans $\mathbb{Q}_p$. Alors $(a_n)_{n\geq 0}$ est de Cauchy et donc convergente si et seulement si*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Démonstration. $\Rightarrow$) Supposons que $(a_n)_{n\geq 0}$ est une suite de Cauchy, i.e.,

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n, m \in \mathbb{N},\ m > n \geq N \ \Rightarrow |a_m - a_n|_p < \varepsilon$$

En particulier, pour $m = n + 1$, on a

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

$\Leftarrow$) Supposons que $\lim_{n\to\infty} |a_{n+1}-a_n|_p = 0$ et montrons que $(a_n)_{n\geq 0}$ est une suite de Cauchy. On a

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq N\ \Rightarrow |a_{n+1} - a_n|_p < \varepsilon$$

Pour tout $m > n \geq N$, on a

$$\begin{aligned} |a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + ... - a_n|_p \\ &\leq \max(|a_m - a_{m-1}|_p, ..., |a_{n+1} - a_n|_p) < \varepsilon. \end{aligned}$$

□

Lemme 2.2. *Soit $(a_n)_{n\geq 0}$ une suite dans $\mathbb{Q}_p$, et $\lim_{n\to\infty} a_n = a \in \mathbb{Q}_p^*$, alors*

$$\exists N \in \mathbb{N},\ \forall n \geq N\ :\ |a_n|_p = |a|_p.$$

Définition 2.3. *Soit $\sum_{n\geq 0} u_n$ une série dans $\mathbb{Q}_p$. On définit la somme partielle de cette série par la suite $(S_N)_{N\geq 0}$ tel que*

$$S_N = u_0 + u_1 + ... + u_N = \sum_{n=0}^{N} u_n.$$

Définition 2.4. *Soit $\sum_{n=0}^{\infty} u_n$ une série dans $\mathbb{Q}_p$. On dit que cette série converge si la suite des sommes partielles converge dans $\mathbb{Q}_p$,i.e.,(d'après le théorème 2.1)*

$$\lim_{N\to\infty} |S_{N+1} - S_N|_p = 0 \ \ \textit{avec}\ S_N = \sum_{n=0}^{N} u_n.$$

Proposition 2.5. *La série $\sum_{n=0}^{\infty} u_n$ converge dans $\mathbb{Q}_p$ si et seulement si $\lim_{n\to\infty} u_n = 0$, de plus, on a*

$$\left|\sum_{n=0}^{\infty} u_n\right|_p \leq \max_n |u_n|_p.$$

Démonstration. On a d'après la définition 2.4 : La série $\sum_{n=0}^{\infty} u_n$ converge si et seulement si la suite des sommes partielles $S_n = \sum_{i=0}^{n} u_i$ converge.

Soit $u_n = S_n - S_{n-1}$, alors d'après le théorème 2.1 la série $\sum_{n=0}^{\infty} u_n$ converge si et seulement si u_n tend vers 0.

Maintenant, supposons que $\sum\limits_{n=0}^{\infty} u_n$ converge. Si $\sum\limits_{n=0}^{\infty} u_n = 0$ la preuve est triviale. Sinon, d'après le lemme 2.2, il existe $N \in \mathbb{N}$ et pour tout $n \geq N$, on a

$$\left|\sum_{n=0}^{\infty} u_n\right|_p = \left|\sum_{n=0}^{N} u_n\right|_p \leq \max_{0\leq n\leq N} |u_n|_p \leq \max_n |u_n|_p.$$

□

2.2 Séries entières p-adiques

Définition 2.6. *Soit $(a_n)_n \subset \mathbb{Q}_p$ et X une indéterminé. On définit une série entière formelle dans $\mathbb{Q}_p$ sous la forme :*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

On note $\mathbb{Q}_p[[X]]$ l'ensemble des séries entières formelles sur $\mathbb{Q}_p$.

Remarque. *En cas de convergence pour $x \in \mathbb{Q}_p$, on écrit*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \text{ tel que } f \in \mathbb{Q}_p[[x]].$$

Définition 2.7. *On définit l'ensemble des séries formelles restreintes dans $\mathbb{Q}_p$ par :*

$$\mathbb{Q}_p\{X\} = \left\{ f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]], \lim_{n\to+\infty} a_n = 0 \right\}.$$

Définition 2.8. *Soit $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p\{x\}$. On définit la norme de Gauss de f par :*

$$\|f\| = \sup_{|x|_p\leq 1} |f(x)|_p = \max_{n\geq 0} |a_n|_p.$$

Proposition 2.9. *Soit $f(x) = \sum\limits_{n\geq 0} a_n x^n \in \mathbb{Q}_p\{x\}$. Si $|s|_p \leq 1$ et $|t|_p \leq 1$, on a*

$$\|f(s) - f(t)\| \leq |s-t|_p.\|f\|.$$

Démonstration. On a

$$\begin{aligned} f(s) - f(t) &= \sum_{n\geq 0} a_n s^n - \sum_{n\geq 0} a_n t^n \\ &= \sum_{n\geq 0} a_n (s^n - t^n) \\ &= (s-t) \sum_{n\geq 1} a_n (s^{n-1} + s^{n-2}t + ... + t^{n-1}) \end{aligned}$$

Pour $|s|_p \leq 1$ et $|t|_p \leq 1$, on a

$$|s^{n-1} + s^{n-2}t + ... + t^{n-1}|_p \leq \max_{1 \leq i \leq n} |s^{n-i}t^{i-1}|_p \leq 1$$

D'où

$$\|f(s) - f(t)\| \leq |s-t|_p.\|f\| .$$

□

Remarque. *On peut réecrire l'inégalité de la proposition précédente sous la forme équivalente :*

$$|f(t+h) - f(t)|_p \leq |h|_p.\|f\| \textit{ tel que } |h|_p \leq 1.$$

Proposition 2.10. *Soit $x \in \mathbb{Q}_p$ et $r \geq 0$ tel que $|a_n|_p r^n \to 0$ donc la série $\sum\limits_{n=0}^{\infty} a_n x^n$ converge si $|x|_p \leq r$.*

Démonstration.

Pour montrer que $\sum\limits_{n=0}^{\infty} a_n x^n$ converge, il suffit de montrer que $|a_n x^n|_p \to 0$ quand $n \to +\infty$.

On a

$$|a_n x^n|_p = |a_n|_p |x|_p^n \leq |a_n|_p r^n \to 0$$

D'où

$$|a_n x^n|_p \to 0, \textit{ quand } n \to +\infty.$$

□

Définition 2.11. *Le rayon de convergence d'une série entière $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$ est le nombre réel $0 \leq r_f \leq \infty$ définie par :*

$$r_f = sup\{r \geq 0 : |a_n|_p r^n \to 0\}.$$

Remarque. *Pour calculer r_f, on applique par exemple le critère de Hadamard ,i.e.,*

$$r_f = \frac{1}{\limsup |a_n|_p^{\frac{1}{n}}} .$$

Proposition 2.12. *Soit $x \in \mathbb{Q}_p$, alors la série $\sum\limits_{n \geq 0} a_n x^n$ converge si $|x|_p < r_f$ et diverge si $|x|_p > r_f$.*

Démonstration. Si $|x|_p > r_f$ (cela ne peut arriver que si $r_f < \infty$), on a

$$\begin{aligned}\lim_{n\to\infty}\sup_{k\geq n}|x|_p|a_k|_p^{\frac{1}{k}} &= |x|_p \lim_{n\to\infty}\sup_{k\geq n}|a_k|_p^{\frac{1}{k}} \\ &= |x|_p\,\frac{1}{r_f} > 1\end{aligned}$$

Donc pour tout $k \geq 0$, on a $|a_k|_p|x|_p^k > 1$. À savoir, le terme général a_kx^k de la série ne tend pas vers 0, alors la série $\sum a_kx^k$ diverge.

Inversement, si $|x|_p < r_f$ (cela ne peut arriver que si $r_f > 0$).

On peut choisir : $|x|_p < r < r_f$, on a

$$\lim_{n\to\infty}\sup_{k\geq n} r|a_k|_p^{\frac{1}{k}} = r\lim_{n\to\infty}\sup_{k\geq n}|a_k|_p^{\frac{1}{k}} < 1$$

Nous en déduisons que pour certain grand N

$$\sup_{k\geq N} r|a_k|_p^{\frac{1}{k}} < 1$$

Par conséquent, $|a_k|_pr^k < 1$ pour tous $k \geq N$, et

$$|a_kx^k|_p = |a_k|_pr^k\left(\frac{|x|_p}{r}\right)^k < \frac{|x|_p^k}{r^k} \to 0 \ \ (k \to \infty)$$

Cela montre que le terme général de la série $\sum a_kx^k$ tend vers zéro, et la série converge.

□

Proposition 2.13. *Le domaine de convergence d'une série entière p-adique $f(x) \in \mathbb{Q}_p[[x]]$ est la boule fermée*

$$B_f(0,R) = \{x \in \mathbb{Q}_p : |x|_p \leq R\}$$

Pour $R \in \{p^k : k \in \mathbb{Z}\}\bigcup\{0\}\bigcup\{\infty\}$.

Démonstration. Soit r_f le rayon de convergence de $f(x)$. On sait que $f(x)$ converge dans la boule ouvert $\{|x|_p < r_f\}$.

Dans la frontière (i.e $|x|_p = r_f$) cette série converge si et seulement si $|a_nx^n|_p \to 0$, ce qui ne dépend que de la norme $|x|_p$, et pas de sa valeur exacte de x.

Donc si la série converge en tout points x tel que $|x|_p = r_f$ alors $R = r_f$, et si la série diverge en tous points tels que $|x|_p = r_f$ alors $R = p^{-1}r_f$. □

Exemple 2.14. *Soit la série* $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n} \in \mathbb{Q}_p[[x]]$, *on a*

$$|a_n|_p = p^{v_p(n)} \ \textit{et} \ \lim_{n\to\infty} |a_n|_p^{\frac{1}{n}} = 1$$

La série converge pour $|x|_p < 1$ *et diverge pour* $|x|_p > 1$.

Si $|x|_p = 1$, *on a*

$$|a_n x^n|_p = p^{v_p(n)} \geq 1$$

Par conséquent la série diverge pour tous x, *et le domaine de convergence de cette série est*

$$\{x \in \mathbb{Q}_p : |x|_p \leq p^{-1}\}.$$

Proposition 2.15. $f(x) \in \mathbb{Z}_p[[x]]$ *converge dans* $\{x \in \mathbb{Q}_p : |x|_p < 1\}$.

Démonstration. Soit $|x|_p < 1$ et $f(x) = \sum_{n=0}^{\infty} a_n x^n$, où $a_n \in \mathbb{Z}_p$.

Pour tout $n \geq 0$, $|a_n|_p \leq 1$, on a

$$|a_n x^n|_p \leq |x|_p^n \to 0 \ \textit{quand}\, n \to \infty$$

D'où la série converge. □

Exemple 2.16. *Soit* $f(x) = \sum_{n=0}^{\infty} p^n x^n \in \mathbb{Z}_p[[x]]$. *En utilisant le critère de Cauchy, on a*

$$\begin{aligned}
\lim_{n\to+\infty} \sqrt[n]{|p^n x^n|_p} < 1 &\Rightarrow \lim_{n\to+\infty} |px|_p < 1 \\
&\Rightarrow |px|_p < 1 \\
&\Rightarrow |p|_p |x|_p < 1 \\
&\Rightarrow |x|_p < p = r_f
\end{aligned}$$

- *Si* $|x|_p = p$

$$\lim_{n\to+\infty} |p|_p^n |x|_p^n = \lim_{n\to+\infty} |p|_p^n p^n = \lim_{n\to+\infty} p^{-n} p^n = 1 \neq 0$$

Alors

$$R = r_f p^{-1} = pp^{-1} = 1$$

Donc le domaine de convergence de cette série est :

$$\{x \in \mathbb{Q}_p \ : \ |x|_p \leq 1\}.$$

Définition 2.17. *Soit $f : \mathbb{Q}_p \to \mathbb{Q}_p$, et $x_0 \in \mathbb{Q}_p$. La fonction f est dite continue en x_0 si :*

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in \mathbb{Q}_p\ :\ |x - x_0|_p < \delta \Rightarrow |f(x) - f(x_0)|_p < \varepsilon.$$

Proposition 2.18. *Soit $f(x) = \sum\limits_{n \geq 0} a_n x^n$, $a_n \in \mathbb{Q}_p$, une série entière dont le domaine de convergence est $D \subset \mathbb{Q}_p$.*
Alors $f : D \longrightarrow \mathbb{Q}_p$ est une fonction continue sur D.

Démonstration. On a f continue sur $D \Leftrightarrow f$ continue en x_0, $\forall x_0 \in D$.

i) Si $x_0 = 0$

$$f \textit{ continue en } 0 \Leftrightarrow \forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in D\ :\ |x|_p < \delta \Rightarrow |f(x) - f(0)|_p < \varepsilon$$

$$\begin{aligned} |f(x) - f(0)|_p &= \left| \sum_{n=0}^{\infty} a_n x^n - a_0 \right|_p = \left| \sum_{n=1}^{\infty} a_n x^n \right|_p \\ &= |x|_p \left| \sum_{n=1}^{\infty} a_n x^{n-1} \right|_p \\ &\leq |x|_p . \max\{|a_n|_p |x^{n-1}|_p\ ,\ n \geq 1\} \end{aligned}$$

On a $\max\{|a_n|_p |x^{n-1}|_p\ ,\ n \geq 1\}$ existe car

$$|a_n|_p |x^{n-1}|_p \longrightarrow 0$$

On pose $M = \max\{|a_n|_p |x^{n-1}|_p\ ,\ n \geq 1\}$, donc

$$|f(x) - f(0)|_p \leq |x|_p M < \delta M < \varepsilon$$

On prend

$$\delta = \frac{\varepsilon}{M}.$$

ii) Si $x_0 \neq 0$

$$f \textit{ continue en } x_0 \Leftrightarrow \forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in D\ :\ |x - x_0|_p < \delta \Rightarrow |f(x) - f(x_0)|_p < \varepsilon$$

Soit $\delta < |x_0|_p$, on a

$$|x - x_0|_p < \delta < |x_0|_p \Rightarrow |x|_p = |x_0|_p \ \textit{(triangle isocèle)}$$

On a

$$
\begin{aligned}
|f(x) - f(x_0)|_p &= \left| \sum_{n=0}^{\infty} (a_n x^n - a_n x_0^n) \right|_p \\
&\leq \max_{n\in\mathbb{N}} (|a_n x^n - a_n x_0^n)|_p) \\
&= \max_{n\in\mathbb{N}} \left(|a_n|_p |x - x_0|_p |x^{n-1} + x^{n-2}x_0 + ... + x^{n-i}x_0^{i-1} + ... + x_0^{n-1}|_p \right)
\end{aligned}
$$

Comme

$$
\begin{aligned}
|x^{n-1} + x^{n-2}x_0 + ... + x^{n-i}x_0^{i-1} + ... + x_0^{n-1}|_p &\leq \max_{1\leq i\leq n} (|x^{n-i}x_0^{i-1}|_p) \\
&= \max_{1\leq i\leq n} (|x|_p^{n-i}|x_0|_p^{i-1}) = |x_0|_p^{n-1}
\end{aligned}
$$

D'où

$$
\begin{aligned}
|f(x) - f(x_0)|_p &\leq \max_{n\in\mathbb{N}} (|a_n|_p |x_0|_p^{n-1})\delta \\
&= \frac{\delta}{|x_0|_p} \max_{n\in\mathbb{N}} (|a_n|_p |x_0|_p^n)
\end{aligned}
$$

Comme la série converge en x_0, on a $a_n x_0^n \to 0$ dans $\mathbb{Q}_p$.

Alors $(a_n x_0^n)_{n\in\mathbb{N}}$ bornée, donc

$$
\exists M \geq 0, \textit{ tel que } |a_n|_p |x_0^n|_p \leq M
$$

D'où

$$
|f(x) - f(x_0)|_p \leq \frac{\delta}{|x_0|_p} M < \varepsilon
$$

Donc il suffit de prendre

$$
\delta = \min \left(|x_0|_p \,, \frac{|x_0|_p.\varepsilon}{M} \right).
$$

□

Définition 2.19 (Différentiabilité des fonctions dans le corps $\mathbb{Q}_p$)**.**

Soit $D \subset \mathbb{Q}_p$ et $a \in D$. Une fonction $f : D \to \mathbb{Q}_p$ est différentiable en a si la dérivée $f'(a)$ de f en a existe et fini, tel que

$$
f'(a) = \lim_{x\to a} \frac{f(x) - f(a)}{x - a}.
$$

Remarque.

1) f est différentiable sur $D \Leftrightarrow f$ différentiable en x, $\forall x \in D$.

2) La dérivée d'un polynôme $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}_p[x]$ est

$$p'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Définition 2.20. *Soit $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$. On définit la dérivée de f sous la forme suivante :*

$$f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

Définition 2.21. *Soit $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$. On note "$\mathbf{D^k}$" l'opérateur de dérivation d'ordre k de f, i.e.,*

$$D^k f(x) = f^{(k)}(x)\ ,\ \ k \geq 1$$

Définition 2.22. *Soit $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$. On définit la formule de Taylor sous la forme :*

$$f(x+h) = f(x) + \sum_{k \geq 1} h^k \frac{D^k f(x)}{k!}.$$

Proposition 2.23. *La série entière $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$ et sa dérivée $f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$ ont le même rayon de convergence, i.e.,*

$$r_f = r_{f'}.$$

Démonstration. On a $|n|_p \leq 1$ pour tout $n \in \mathbb{N}$, alors

$$\begin{aligned} r_{f'}^{-1} &= \limsup_{n\to\infty} |n a_n|_p^{\frac{1}{n-1}} = \limsup_{n\to\infty} |n a_n|_p^{\frac{1}{n}} \\ &= \limsup_{n\to\infty} |a_n|_p^{\frac{1}{n}} = r_f^{-1}. \end{aligned}$$

□

Exemple 2.24. *Soit $f(x) = \sum_{n=0}^{\infty} x^{p^n}$, $a_n = 1$, $\forall n \in \mathbb{N}$.*

On a

$$r_p^{-1} = \limsup_{n\to\infty} |a_n|_p^{\frac{1}{p^n}} = \limsup_{n\to\infty} |1|_p^{\frac{1}{p^n}} = \limsup_{n\to\infty} 1 = 1$$

Alors

$$r_f = 1$$

i) f est diverge si $|x|_p = 1$ car

$$\left|x^{p^n}\right|_p = 1 \nrightarrow 0 \quad \textit{quand } n \to \infty.$$

ii) $f'(x) = \sum\limits_{n=1}^{\infty} p^n x^{p^n-1}$ converge si $|x|_p = 1$ car

$$|p^n x^{p^n-1}|_p = |p^n|_p |x^{p^n-1}|_p = |p^n|_p = p^{-n} \longrightarrow 0 \quad \textit{quand } n \to \infty.$$

2.3 Exponentielle et logarithme p-adique

Dans cette section, on donne les définitions de l'exponentielle p-adique et du logarithme p-adique, qu'on aurra besoin dans le chapitre 3.

Définition 2.25. *Soit $r_p > 0$ et $D_p = B(0, r_p) = \{x \in \mathbb{Q}_p : |x|_p < r_p\}$. La fonction exponentielle dans le corps $\mathbb{Q}_p$, notée "$\mathbf{exp_p}$" ; est définie de D_p dans $\mathbb{Q}_p$ par :*

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Pour déterminer le rayon de convergence de "$\mathbf{exp_p}$", nous avons besoin de connaître la norme p-adique de $n!$, pour cela on a la définition et le lemme suivants :

Définition 2.26. *Soit $n \in \mathbb{N}^*$. La somme des coefficients de n dans la base p, notée "$\mathbf{S_p(n)}$" ; définie comme suit :*

$$S_p(n) = \sum_{i=1}^{t} \alpha_i \ , \ \textit{tel que} \ : \ n = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_t p^t.$$

Lemme 2.27. *Soit $n \geq 1$. La valuation p-adique de $n!$ est donnée par :*

$$v_p(n!) = \frac{n - S_p(n)}{p-1}.$$

Démonstration. Soit $j \in \mathbb{N}^*$, le développement de Hensel de j est :

$$j = \alpha_k p^k + \alpha_{k+1} p^{k+1} + ... + \alpha_s p^s, \ \textit{où } 0 \leq \alpha_i \leq p-1$$

i) Montrons que $j - 1 = (p-1) \sum\limits_{\ell=0}^{k-1} p^\ell + (\alpha_k - 1)p^k + \sum\limits_{\ell=k+1}^{s} \alpha_\ell p^\ell$

On a

$$\begin{aligned}(p-1)\sum_{\ell=0}^{k-1}p^\ell+(\alpha_k-1)p^k+\sum_{\ell=k+1}^{s}\alpha_\ell p^\ell &= (p-1)\frac{1-p^k}{1-p}+\alpha_k p^k-p^k+\sum_{\ell=k+1}^{s}\alpha_\ell p^\ell\\ &= -(1-p^k)+\alpha_k p^k-p^k+\sum_{\ell=k+1}^{s}\alpha_\ell p^\ell\\ &= \sum_{\ell=k}^{s}\alpha_\ell p^\ell-1=j-1.\end{aligned}$$

ii) Montrons que $S_p(j-1)=k(p-1)+S_p(j)-1$

D'après i), on a

$$\begin{aligned}S_p(j-1) &= S_p\left((p-1)\sum_{\ell=0}^{k-1}p^\ell+(\alpha_k-1)p^k+\sum_{\ell=k+1}^{s}\alpha_\ell p^\ell\right)\\ &= S_p\left((p-1)\sum_{\ell=0}^{k-1}p^\ell\right)+S_p\left(\alpha_k p^k-p^k+\sum_{\ell=k+1}^{s}\alpha_\ell p^\ell\right)\\ &= k(p-1)+S_p\left(\sum_{\ell=k}^{s}\alpha_\ell p^\ell\right)-S_p(p^k)\\ &= k(p-1)+S_p(j)-1.\end{aligned}$$

iii) D'après ii), on a $S_p(n-1)=v_p(n)(p-1)+S_p(n)-1$, alors

$$v_p(n)=\frac{S_p(n-1)-S_p(n)+1}{p-1}$$

D'autre part, on a

$$v_p(n!)=v_p\left(n(n-1)(n-2)...1\right)=v_p(n)+v_p(n-1)+...+v_p(1)$$

Alors

$$\begin{aligned}v_p(n!) &= \frac{S_p(n-1)-S_p(n)+1}{p-1}+\frac{S_p(n-2)-S_p(n-1)+1}{p-1}+....+\frac{S_p(1)-S_p(2)+1}{p-1}\\ &= \frac{-S_p(n)+1+1+...+1}{p-1}\\ &= \frac{n-S_p(n)}{p-1}\end{aligned}$$

D'où

$$v_p(n!)=\frac{n-S_p(n)}{p-1}.$$

$\square$

Lemme 2.28. *[11] Pour tout $n \in \mathbb{N}$; $\dfrac{S_p(n)}{n} \longrightarrow 0$ quand $n \to \infty$.*

Dans le théorème suivant on donne la valeur du rayon de convergence de l'exponentielle p-adique et bien sûr son disque de convergence.

Théorème 2.29. *L'exponentiel p-adique converge dans le disque*

$$D_p = \{x \in \mathbb{Z}_p \ ; \ |x|_p < p^{\frac{-1}{p-1}}\}$$

et diverge si $|x|_p > p^{\frac{-1}{p-1}}$.

Démonstration. Nous avons

$$r_p^{-1} = \limsup_{n\to\infty} |a_n|_p^{\frac{1}{n}} = \limsup_{n\to\infty} \left|\frac{1}{n!}\right|_p^{\frac{1}{n}}$$

Alors d'après le lemme 2.27

$$r_p^{-1} = \limsup_{n\to\infty} \left(p^{\frac{n-S_p(n)}{p-1}}\right)^{\frac{1}{n}} = \limsup_{n\to\infty} \left(p^{\frac{1}{p-1}(1-\frac{S_p(n)}{n})}\right) = p^{\frac{1}{p-1}}$$

D'où

$$r_p = p^{\frac{-1}{p-1}}.$$

□

Propriétés 2.30. *[11] Si $x, y \in D_p$, alors $x + y \in D_p$ et*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y).$$

Définition 2.31. *Soit $B = B(1,1) = \{x \in \mathbb{Z}_p : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$. La fonction logarithme dans le corps $\mathbb{Q}_p$, notée "$\mathbf{ln_p}$" ; est définie de B dans $\mathbb{Q}_p$ par :*

$$\ln_p(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}.$$

Proposition 2.32. *Le logarithme p-adique converge sur*

$$1 + p\mathbb{Z}_p = \{x \in \mathbb{Z}_p ; |x-1|_p < 1\}.$$

Démonstration. On a

$$r_p^{-1} = \limsup_{n\to\infty} |a_n|_p^{\frac{1}{n}}$$

Donc

$$\begin{aligned} r_p^{-1} &= \limsup_{n\to\infty} \left|\frac{(-1)^{n+1}}{n}\right|_p^{\frac{1}{n}} \\ &= \limsup_{n\to\infty} \left|\frac{1}{n}\right|_p^{\frac{1}{n}} = 1 \end{aligned}$$

D'où

$$r_p = 1.$$

□

Propriétés 2.33. *[11] Si $x, y \in 1 + p\mathbb{Z}_p$, alors $xy \in 1 + p\mathbb{Z}_p$ et*

$$\ln_p(x) + \ln_p(y) = \ln_p(xy).$$

Proposition 2.34.

1) La fonction $\exp_p$ est différentiable sur D_p et $\exp_p'(x) = \exp_p(x)$.

2) La fonction $\ln_p$ est différentiable sur $1 + p\mathbb{Z}_p$ et $\ln_p'(x) = \dfrac{1}{x}$.

Démonstration. 1) Pour tout $x \in D_p$, on a

$$\exp_p'(x) = \left(\sum_{n=0}^{\infty} \frac{x^n}{n!}\right)' = \sum_{n=0}^{\infty} \left(\frac{x^n}{n!}\right)' = \sum_{n=1}^{\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$

2) Pour tout $x \in 1 + p\mathbb{Z}_p$, on a

$$\begin{aligned} \ln_p'(x) &= \left(\sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}\right)' \\ &= \sum_{n=1}^{\infty} n(-1)^{n+1} \frac{(x-1)^{n-1}}{n} \\ &= \sum_{n=0}^{\infty} (-1)^n (x-1)^n = \frac{1}{1+(x-1)} = \frac{1}{x}. \end{aligned}$$

□

Lemme 2.35. *Pour tout $0 < |x|_p < r_p$ et $n \geq 2$, on a*

$$\left|\frac{x^n}{n}\right|_p \leq \left|\frac{x^n}{n!}\right|_p < |x|_p < r_p.$$

Démonstration. On a $v_p(n) \leq v_p(n!)$, alors

$$|n|_p \geq |n!|_p$$

Et comme $|x|_p > 0$, donc

$$\left|\frac{x^n}{n}\right|_p \leq \left|\frac{x^n}{n!}\right|_p$$

D'autre part, on a

$$\begin{aligned}\frac{|x^n|_p}{|n!|_p} &= |x^n|_p.p^{\frac{n-S_p(n)}{p-1}} \\ &\leq |x^n|_p.p^{\frac{n-1}{p-1}} = \left(|x|_p.p^{\frac{1}{p-1}}\right)^{n-1}.|x|_p\end{aligned}$$

Comme $|x|_p < p^{\frac{-1}{p-1}}$ c'est-à-dire $|x|_p.p^{\frac{1}{p-1}} < 1$, donc

$$\left(|x|_p.p^{\frac{1}{p-1}}\right)^{n-1} < 1 \ , \ \ \forall n \geq 2$$

Alors

$$\frac{|x^n|_p}{|n!|_p} < |x|_p < r_p$$

D'où

$$\left|\frac{x^n}{n}\right|_p \leq \left|\frac{x^n}{n!}\right|_p < |x|_p < r_p.$$

□

Proposition 2.36. *Pour $x \in D_p$, on a*

1) $|\exp_p(x) - 1|_p = |x|_p$.

2) $|\ln_p(1 + x)|_p = |x|_p$.

Démonstration. 1) On a

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Donc

$$\exp_p(x) - 1 = x + \sum_{n=2}^{\infty} \frac{x^n}{n!}$$

Et comme

$$\left|\sum_{n=2}^{\infty} \frac{x^n}{n!}\right|_p \leq \sup_{n\geq 2} \frac{|x^n|_p}{|n!|_p} = \max_{n\geq 2} \frac{|x^n|_p}{|n!|_p} < |x|_p$$

Alors

$$|\exp_p(x) - 1|_p = \left|x + \sum_{n=2}^{\infty} \frac{x^n}{n!}\right|_p = |x|_p.$$

2) On a

$$\ln_p(1+x) = x + \sum_{n=2}^{\infty}(-1)^{n-1}\frac{x^n}{n}$$

Donc

$$|\ln_p(1+x)|_p = \left| x + \sum_{n=2}^{\infty}(-1)^{n-1}\frac{x^n}{n} \right|_p = |x|_p.$$

□

2.4 Analyse dans $\mathbb{C}_p$

La plupart des propriétés analytique sont valables lorsque nous remplaçons le corps $\mathbb{Q}_p$ par le corps des nombres complexes p-adiques $\mathbb{C}_p$. Par exemple, on peut citer les propriétés suivantes :

i) Une suite $(a_n)_{n\geq 0}$ dans $\mathbb{C}_p$ est de Cauchy si et seulement si

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

ii) Une série $\sum\limits_{n\geq 0} u_n$ dans $\mathbb{C}_p$ converge si et seulement si son terme général tend vers zéro.

iii) Une série entière dans $\mathbb{C}_p$ est donnée par :

$$f(x) = \sum_{n\geq 0} a_n x^n \quad où \;\; x \in \mathbb{C}_p$$

On note $\mathbb{C}_p[[x]]$ l'ensemble des séries entières sur $\mathbb{C}_p$.

iv) La série $f(x) = \sum\limits_{n\geq 0} a_n x^n \in \mathbb{C}_p[[x]]$ possède un rayon de convergence r_f, qui est donné par :

$$0 \leq r_f = sup\{r \geq 0 : |a_n|_p r^n \to 0\} \leq \infty.$$

Par exemple, le rayon de convergence de :

• La série du logarithme p-adique

$$\ln_p(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n$$

est égal à 1.

• La série de l'exponentielle p-adique

$$\exp_p(x) = \sum_{n\geq 0} \frac{x^n}{n!}$$

est égal à $p^{-\frac{1}{p-1}}$.

v) Une série entière restreinte sur $\mathbb{C}_p$ est donnée par :

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}_p[[x]] \ \ avec \ \ \lim_{n \to +\infty} a_n = 0.$$

CHAPITRE 3

Théorème des accroissements finis (TAF)

Dans ce chapitre, on va présenter le théorème des accroissements finis dans des espaces vectoriels normés et comme cas particulier dans $\mathbb{R}$, puis on présente la version p-adique de ce théorème. On insistant sur le cas p-adique, nous donnons des applications sur le théorème du point fixe, le théorème de Wolstenholme, et les congruences des coefficients binomiaux, et des polynômes connus comme le polynôme de Chebyshev, le polynôme de Bernoulli.

3.1 Rappel sur le théorème des accroissements finis dans un espace vectoriel normé

Dans cette section, E et F deux espaces vectoriels normés (e.v.n).

Définition 3.1. *Soit $a, b \in E$*

- *Le segment [a,b] est le sous-ensemble de E défini par :*

$$[a, b] = \{x \in E \ ; \ \exists t \in [0, 1] \ \ \textit{tel que} \ \ x = a + t(b - a)\}.$$

- *Un sous-ensemble $U \subset E$ est dit convexe si pour tout $a, b \in U$ le segment $[a, b] \subset U$.*

Théorème 3.2. *[21] (Inégalité de **TAF** dans le cas général)*
Soient E et F deux e.v.n, U un ouvert de E et f une application de U dans F différentiable sur U. Soient $a, b \in U$ tels que le segment $[a, b] \subset U$. On suppose qu'il existe $M \geq 0$ telle que $\|d_{a+t(b-a)}f\|_{\mathcal{L}(E,F)} \leq M$ pour tout $t \in]0, 1[$.
Alors on a :

$$\|f(b) - f(a)\|_F \leq \|b - a\|_E \sup_{x\in[a,b]} \|d_x f\|_{\mathcal{L}(E,F)}$$

Dans le cas réel, le théorème précédent est écrite comme suit :

Théorème 3.3. *[21] Soit f une fonction continue sur un intervalle $[a, b]$ à valeurs dans $\mathbb{R}$, dérivable sur $]a, b[$. Soit $M \geq 0$ telle que $|f'(x)| \leq M$, pour tout $x \in [a, b]$, alors*

$$|f(y) - f(x)| \leq M|y - x| \quad \text{pour tout } x, y \in [a, b].$$

Applications

Théorème 3.4. *Soient E et F deux e.v.n et U un ouvert convexe de E.*
Tout application définie de U dans F, différentiable sur U et dont la différentielle sur U est identiquement nulle, est constante.

Démonstration. Soient a, b deux points de U. Puisque U est convexe, le segment $[a, b]$ est contenu dans U, et d'après le **TAF**, on a

$$\|f(b) - f(a)\|_F \leq \|b - a\|_E \sup_{x\in[a,b]} \|d_x f\|_{\mathcal{L}(E,F)}$$

Puisque $d_x f$ est identiquement nulle sur U, on a

$$\sup_{x\in[a,b]} \|d_x f\|_{\mathcal{L}(E,F)} = 0$$

Il en résulte que

$$\|f(b) - f(a)\|_F = 0$$

D'où le résultat. □

Définition 3.5. *Soient E et F deux e.v.n, et $k \geq 0$. Une application $f : U \longrightarrow F$ est dit k-lipschitzienne si pour tout $x, y \in U$, on a*

$$\|f(x) - f(y)\|_F \leq k\|x - y\|_E.$$

Corollaire 3.6. *Soient E et F deux e.v.n, U ouvert convexe de E.*
Soit $f : E \longrightarrow F$ une application différentiable, on suppose qu'il existe $k \geq 0$, tel que $\|d_x f\|_{\mathcal{L}(E,F)} \leq k$, $\forall x \in U$. Alors f est k-lipschitzienne.

3.2 Théorème des accroissements finis p-adique

La forme du théorème des accroissements finis définie dans la section précédente est valable pour les fonctions différentiables avec des conditions sur l'ouvert. Mais, ce théorème n'est pas toujours valable pour des fonctions p-adique. Il y a des fonctions non constantes dont les dérivées sont identiquement nulles.
Dans l'exemple suivant on va démentrer que ce théorème n'est pas valable dans le cas p-adique.

Exemple 3.7. *Soit la fonction $f(t) = t^p$.*
*Nous avons $f^{'}(t) = p\, t^{p-1}$, donc $\|f^{'}\| = |p|_p = p^{-1} < 1$, on applique le **TAF** dans le cas d'un **e.v.n** sur f pour $a = 0$ et $h = b - a = 1$, on trouve*

$$1 = |f(1) - f(0)|_p \leq |h|_p.\|f^{'}\| = p^{-1}$$

*Donc nous ne pouvons pas appliquer le **TAF** dans ce cas.*

• On montre ci-dessons que le théorème des accroissements finis soit valable pour $|h| \leq r_p < 1$, avec $r_p = |p|_p^{\frac{1}{p-1}}$.
Dans le but d'avoir

$$|f(h) - f(0)|_p \leq |h|_p.\|f^{'}\|$$

On a

$$|h|_p^p \leq |h|_p.\|f^{'}\| = |h|_p|p|_p$$

D'où

$$|h|_p \leq |p|_p^{\frac{1}{p-1}} \text{ tel que } r_p = |p|_p^{\frac{1}{p-1}}.$$

Comme on a dit dans l'introduction, le théorème des accroissements finis p-adique à été obtenu en 1991 par **Alain Robert**, il a démontré ce théorème pour un espace de Banach ultramétrique, tandis que dans notre travail nous avons utilisé le cas particulier de l'espace $\mathbb{C}_p$.

3.2.1 Théorème des accroissements finis d'ordre 1

Théorème 3.8. *Soit* $f(t) = \sum_{n\geq 0} a_n t^n \in \mathbb{C}_p\{t\}$. *Pour tout* $t, h \in \mathbb{C}_p$, *avec* $|t|_p \leq 1$ *et* $|h|_p \leq r_p = p^{-\frac{1}{p-1}}$, *on a*

$$|f(t+h) - f(t)|_p \leq |h|_p \|f^{'}\|.$$

Démonstration. i) En utilisant la formule de Taylor qui permet de calculer la différence $f(t+h) - f(t)$ comme

$$\begin{aligned} f(t+h) - f(t) &= \sum_{k\geq 1} h^k . \frac{D^k f(t)}{k!} \\ &= h \sum_{k\geq 1} \frac{h^{k-1}}{k!} . D^{k-1} f^{'}(t) \end{aligned}$$

avec $f^{'}(t) = \sum_{k\geq 1} n a_n t^{n-1}$.

La condition $|t|_p \leq 1$ implique que

$$|f(t+h) - f(t)|_p \leq |h|_p \sup_{k\geq 1} \left| \frac{h^{k-1}}{k!} \right|_p \|D^{k-1} f^{'}\|$$

D'autre part, on a

$$\|Df\| = \|f^{'}\| = \sup_{k\geq 1} |k a_k|_p \leq \sup_{k\geq 0} |a_k|_p = \|f\|$$

Il est facile de montrer par récurrence que

$$\|D^{k-1} f^{'}\| \leq \|f^{'}\|, \ \forall k \geq 1$$

Le résultat sera prouvé si nous pouvons montrer que $\left| \frac{h^{k-1}}{k!} \right|_p \leq 1$, $(k \geq 1)$.

La condition $|h|_p \leq r_p = |p|_p^{\frac{1}{p-1}}$ implique que

$$|h|_p^{k-1} \leq |p|_p^{\frac{k-1}{p-1}} \leq |k!|_p$$

Puisque

$$v_p(k!) = \frac{k - S_p(k)}{p-1} \leq \frac{k-1}{p-1}.$$

ii) Considérons maintenant le cas général d'une série restreinte $f(t) = \sum_{k\geq 0} a_k t^k$. Sans perte de généralité, on peut supposer $|f(t+h) - f(t)|_p \neq 0$, donc f n'est pas constant.

Considérons les polynômes $f_n(t) = \sum\limits_{k \leq n} a_k t^k$. On a

$$\|f - f_n\| = \sup_{k>n} |a_k|_p \longrightarrow 0$$

Aussi bien que

$$\|f_n\| = \sup_{k \leq n} |a_k|_p = \|f\|$$

Et

$$\|f_n^{'}\| = \sup_{k \leq n} |k a_k|_p = \|f^{'}\|$$

Pour n assez grand, prenons t et h comme dans la première partie. La convergence

$$f_n(t+h) - f_n(t) \longrightarrow f(t+h) - f(t) \neq 0, \; quand\ n \to +\infty$$

Implique

$$|f_n(t+h) - f_n(t)|_p = |f(t+h) - f(t)|_p \;\; pour\ n\ assez\ grand.$$

Par conséquent, en utilisant une valeur assez grand de l'entier n, et en utilisant le résultat précédent pour les polynômes, on a

$$\begin{aligned} |f(t+h) - f(t)|_p &= |f_n(t+h) - f_n(t)|_p \\ &\leq |h|_p . \|f_n^{'}\| \\ &= |h|_p . \|f^{'}\| \end{aligned}$$

□

Exemple 3.9. *L'application du* ***TAF*** *à la fonction $f(t) = t^p$, en $t = 1$, montre que*

$$|(1+h)^p - 1|_p \leq |h|_p . |p|_p \;\; tel\ que\ |h|_p \leq r_p$$

Mais cette inégalité doit être remplacée par :

$$|(1+h)^p - 1|_p \leq |h|_p^p \;\; lorsque\ r_p < |h|_p \leq 1 \;\; (avec\ égalité\ si\ p = 2)$$

En effet,

- *Si $p \neq 2$, il existe $q(h) \in \mathbb{Z}_p[h]$ tel que*

$$(1+h)^p = 1 + h^p + phq(h)$$

Donc pour $r_p < |h|_p \leq 1$, *on a*

$$|(1+h)^p - 1|_p = \max\{|h|_p^p, |p|_p|q(h)|_p\} \leq \max\{|h|_p^p, |p|_p|\} = |h|_p^p$$

- *Si* $p = 2$, *il existe* $q(h) = 1 \in \mathbb{Z}_2[h]$ *tel que*

$$(1+h)^2 = 1 + h^2 + 2h$$

Donc pour $r_2 < |h|_2 \leq 1$, *on a*

$$|(1+h)^2 - 1|_2 = \max\{|h|_2^2, |2|_2\} = |h|_2^2.$$

Remarque. *Le théorème des accroissements finis p-adique est plus fort que la proposition* 2.9 *puisque on a* $\|f'\| \leq \|f\|$.

3.2.2 Théorème des accroissements finis d'ordre 2

Théorème 3.10. *Soit* $f(t) = \sum\limits_{n\geq 0} a_n t^n \in \mathbb{C}_p\{t\}$, *on a*

$$|f(t+h) - f(t) - f'(t)h|_p \leq \left|\frac{h^2}{2}\right|_p . \|f''\|$$

pour tout $t, h \in \mathbb{C}_p$, *avec* $|t|_p \leq 1$ *et* $|h|_p \leq |p|_p^{\frac{1}{p-2}}$ *si* $p \geq 3$, $|h|_2 \leq \left|\sqrt{2}\right|_2$ *si* $p = 2$.

Démonstration. On écrit la formule de Taylor de f au point t comme suit :

$$f(t+h) = f(t) + \sum_{k\geq 1} h^k \ \frac{D^k f(t)}{k!} = f(t) + f'(t)h + \sum_{k\geq 2} h^k \ \frac{D^k f(t)}{k!}$$

Alors

$$\begin{aligned} f(t+h) - f(t) - f'(t)h &= \sum_{k\geq 2} h^k \ \frac{D^k f(t)}{k!} \\ &= h^2 \left(\sum_{k\geq 2} \frac{h^{k-2}}{k!} \ D^{k-2} f''(t) \right) \\ &= h^2 \left(\sum_{k\geq 2} \frac{h^{k-2}}{k(k-1)} \cdot \frac{D^{k-2} f''(t)}{(k-2)!} \right) \end{aligned}$$

Comme dans la démonstration du théorème précédent, on a par récurrence :

$$\left\| \frac{D^{k-2} f''(t)}{(k-2)!} \right\| \leq \|f''\| \ (k \geq 2).$$

• Pour $p \neq 2$, il reste à vérifier

$$\left|\frac{h^{k-2}}{k(k-1)}\right|_p \leq 1 \quad (k \geq 2) \tag{3.1}$$

La formule (3.1) est satisfaite :

Si $u = v_p(k) \geq 1$. On a $k \geq p^u$ et $v_p(k-1) = 0$, d'où

$$\left|\frac{h^{k-2}}{k(k-1)}\right|_p \leq \frac{|h|_p^{p^u-2}}{|p|_p^u} \leq |p|_p^e$$

avec

$$e = \frac{p^u - 2}{p-2} - u \geq \frac{p^u - 1}{p-1} - u \geq 0$$

Si $v_p(k) = 0$ et $u = v_p(k-1) \geq 1$, on a $k \geq p^u + 1$ et les estimations précédentes sont satisfaites.

Finalement, si $v_p(k-1) = v_p(k) = 0$, on a

$$|k(k-1)|_p = 1$$

Et la démonstration est terminée.

• Pour $p = 2$, il reste à montrer

$$\left|\frac{h^{k-2}}{k(k-1)/2}\right|_2 \leq 1 \tag{3.2}$$

La formule (3.2) est satisfaite :

Si k pair : $u = v_2(k) \geq 1$, alors $k \geq 2^u$ et $v_2(k-1) = 0$, donc

$$\left|\frac{k(k-1)}{2}\right|_2 \geq |2|_2^{u-1}$$

D'où

$$\left|\frac{h^{k-2}}{k(k-1)/2}\right|_2 \leq \frac{|h|_2^{2^u-2}}{|2|_2^{u-1}} \leq |2|_2^{2^{u-1}-1-(u-1)} = |2|_2^e$$

avec $e = 2^{u-1} - u \geq 0$.

La même maniére pour k impair : $u = v_2(k-1) \geq 1$ et $v_2(k) = 0$.

□

3.3 Applications du théorème des accroissements finis p-adique

3.3.1 Coefficients binomiaux

Proposition 3.11. *Soit $n, k \in \mathbb{N}$. Les coefficients binomiaux satisfont les congruences suivantes :*

$$\binom{np}{kp} \equiv \binom{n}{k} \bmod np\mathbb{Z}_p, \text{ et } \binom{np}{k} \equiv 0 \bmod np\mathbb{Z}_p \text{ si } p \text{ ne divise pas } k.$$

Démonstration. On considère le polynôme $(1+x)^p = 1 + p.g(x) + x^p$.
On suppose $f(T) = (1 + T.g(x) + x^p)^n$, alors

$$f(p) = (1 + p.g(x) + x^p)^n = (1+x)^{pn}, \quad f(0) = (1+x^p)^n$$

Donc

$$f(p) - f(0) = (1+x)^{pn} - (1+x^p)^n = \sum_{k=0}^{pn} \binom{np}{k} x^k - \sum_{k=0}^{n} \binom{n}{k} x^{pk}$$

On applique le **TAF** sur f, on obtient

$$|f(p) - f(0)|_p \leq |p|_p \|f'\| \leq |pn|_p$$

On déduit que

$$\binom{np}{kp} \equiv \binom{n}{k} \bmod np\mathbb{Z}_p$$

D'autre part, quand k ne divise pas p, le coefficient de x^k satisfait

$$\binom{np}{k} \equiv 0 \bmod np\mathbb{Z}_p.$$

□

Corollaire 3.12. *Soit $n \in \mathbb{N}$, on a*

$$(1+x)^n \equiv 1 + nx (\bmod pnx\mathbb{Z}_p)$$

tel que $x \in 2p\mathbb{Z}_p$.

Démonstration. On considère $f(x) = (1+x)^n$, donc

$$f''(x) = n(n-1)(1+x)^{n-2}$$

Alors

$$\|f''\| = |n(n-1)|_p \,,\ \forall n \geq 2$$

• Pour $|x|_p \leq |p|_p^{\frac{1}{p-2}}$ si $p \neq 2$, on applique le **TAF** d'ordre 2 à $f(x)$, on trouve

$$\begin{aligned} |(1+x)^n - 1 - nx|_p &\leq \left|\frac{x^2}{2}\right|_p .\|f''\| \\ &= \left|\frac{x^2}{2}\right|_p |n(n-1)|_p \\ &\leq \left|\frac{x^2}{2}\right|_p |n|_p \\ &\leq |nx|_p \left|\frac{x}{2}\right|_p \end{aligned}$$

Et comme $x \in 2p\mathbb{Z}_p$, donc $\left|\frac{x}{2}\right|_p \leq |p|_p$. Alors

$$|(1+x)^n - 1 - nx|_p \leq |nx|_p |p|_p = |nxp|_p$$

D'où

$$(1+x)^n \equiv 1 + nx (\bmod\, pnx\mathbb{Z}_p)$$

• Pour $|x|_2 \leq |\sqrt{2}|_2$ si $p = 2$, on applique le **TAF** d'ordre 2 à $f(x)$, on trouve

$$|(1+x)^n - 1 - nx|_2 \leq \left|\frac{x^2}{2}\right|_2 .\|f''\| \leq \left|\frac{x^2}{2}\right|_2 |n|_2 \leq |nx|_2 \left|\frac{x}{2}\right|_2$$

Et comme $x \in 2.2\mathbb{Z}_2$, donc $\left|\frac{x}{2}\right|_2 \leq |2|_2$. Alors

$$|(1+x)^n - 1 - nx|_2 \leq |nx|_2 |2|_2 = |2nx|_2$$

D'où

$$(1+x)^n \equiv 1 + nx (\bmod\, 2nx\mathbb{Z}_2).$$

□

3.3.2 Théorème du point fixe p- adique

Théorème 3.13. *Soit $f(x) \in \mathbb{C}_p\{x\}$ avec $\|f\| \leq 1$. Alors f définit une application continue sur la boule unité $B = B_{\leq 1}(\mathbb{C}_p)$. De plus, si*

$$\|f'\| < 1 \text{ et } \inf \|f(x) - x\| \leq r_p = |p|_p^{\frac{1}{(p-1)}}$$

f possède un point fixe.

Démonstration. Par continuité de f sur la boule unité B, on peut trouver $x_0 \in B$ tel que $|f(x_0) - x_0|_p \leq r_p$.

On pose $x_1 = f(x_0), x_2 = f(x_1), ..., x_{n+1} = f(x_n)$ pour tout $n \geq 0$.

En utilisant le **TAF**, on trouve

$$\begin{aligned} |x_{n+1} - x_n|_p &= |f(x_n) - f(x_{n-1})|_p \\ &\leq |x_n - x_{n-1}|_p \|f'\| \\ &< |x_n - x_{n-1}|_p \leq r_p \end{aligned}$$

La suite $|x_{n+1} - x_n|_p$ est strictement décroissante et $|x_{n+1} - x_n|_p \to 0$, alors elle est de Cauchy. Donc la limite de cette suite est un point fixe de f. □

3.3.3 Théorème de Wolstenholme

Définition 3.14. *On définit les nombres harmoniques par :*

$$h_n = 1 + \frac{1}{2} + ... + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}.$$

Théorème 3.15. *Soit $p \geq 5$ un nombre premier, alors le numérateur de h_{p-1} est divisible par p^2.*

Démonstration. On va montrer que $h_{p-1} \in p^2\mathbb{Z}_p$.

On considère le polynôme :

$$f(t) = (t-1)(t-2)...(t-(p-1)) \equiv t^{p-1} - 1 (\text{mod}\, p\mathbb{Z}_p[t])$$

Soit $f(t) = f(p-t)$, alors $f'(t) = -f(p-t)$.

D'où

$$f'(0) = -f'(p)$$

D'autre part,

$$\ln f(t) = \ln(t-1) + \ln(t-2) + ... + \ln(t-(p-1))$$

En dérivant l'expression précédente, on obtient

$$\frac{f'}{f}(t) = \frac{1}{t-1} + \frac{1}{t-2} + ... + \frac{1}{t-(p-1)} = \sum_{k=1}^{p-1} \frac{1}{t-k}$$

On pose $g(t) = \sum\limits_{k=1}^{p-1} \frac{1}{t-k}$, de sorte que

$$g(0) = \sum_{k=1}^{p-1} -\frac{1}{k}$$

Alors

$$-g(0) = \sum_{k=1}^{p-1} \frac{1}{k} = h_{p-1}$$

D'autre part, on a

$$g(p) = \sum_{k=1}^{p-1} \frac{1}{p-k} = h_{p-1}$$

Alors

$$-g(p) = g(0)$$

Donc

$$|h_{p-1}|_p = \left|\frac{f'}{f}(0)\right|_p = |f'(0)|_p = |2f'(0)|_p = |f'(p) - f'(0)|_p$$

On applique le **TAF** d'ordre 2, on obtient

$$\begin{aligned} |f'(p) - f'(0) - pf''(0)|_p &\leq |p^2|_p.\|f'''\| \\ &\leq |p^2|_p \end{aligned}$$

Comme $f(t) \equiv t^{p-1} - 1 (\bmod p\mathbb{Z}_p[t])$, alors

$$f''(t) \equiv (p-1)(p-2)t^{p-3} (\bmod p\mathbb{Z}_p[t])$$

D'où

$$f''(0) \equiv 0 (\bmod p\mathbb{Z}_p)$$

Pour tout $p \geq 5$, on a

$$f'(p) - f'(0) - pf''(0) \equiv f'(p) - f'(0)$$

Alors

$$f'(p) - f'(0) \equiv 0 (\bmod p^2\mathbb{Z}_p)$$

D'où ce qu'on veut. $\square$

Exemple 3.16.

$$h_4 = \frac{25}{12}, \;\; h_6 = \frac{49}{20}, \;\; h_{10} = \frac{7381}{2520}$$

3.3.4 Polynômes de Chebyshev

Définition 3.17. *On définit les polynômes de Chebyshev T_n du premier espèce de degré n par la formule suivante :*

$$T_n(x) = \cos n\theta \; (n \geq 0)$$

avec $x = \cos\theta$ tel que $x \in [-1, 1]$ et $\theta \in [0, \pi]$.

Exemple 3.18.

$$\begin{array}{ll} T_0(x) = 1 & , T_4(x) = 8x^4 - 8x^2 + 1 \\ T_1(x) = x & , T_5(x) = 16x^5 - 20x^3 + 5x \\ T_2(x) = 2x^2 - 1 & , T_6(x) = 36x^6 - 48x^4 + 18x^2 - 1 \\ T_3(x) = 4x^3 - 3 & , T_7(x = 64x^7 - 112x^5 + 56x^3 - 7x \end{array}$$

Définition 3.19. *On définit les polynômes de Chebyshev U_n du deuxième espèce de degré n par la formule suivante :*

$$U_n(x) = \frac{\sin(n+1)\theta}{\sin\theta} \; (n \geq 0)$$

avec $x = \cos\theta$ tel que $x \in [-1, 1]$ et $\theta \in [0, \pi]$.

Exemple 3.20.

$$U_0(x) = 1$$

$$U_1(x) = 2x$$

$$U_2(x) = 4x^2 - 1$$

$$U_3(x) = 8x^3 - 4x...$$

Propriétés 3.21. *[22] La suite des polynômes de Chebyshev du premier espèce satisfait les propriétés suivantes :*

1) $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$, $(n \geq 1)$.

2) $T_n \circ T_m = T_{nm} = T_m \circ T_n$, $(n, m \geq 0)$.

3) $T'_n(x) = nU_{n-1}(x)$, $(n \geq 1)$.

Définition 3.22 (Pseudo-puissances)**.** *On dit qu'un polynôme $f(x) \in \mathbb{Z}_p[x]$ est une pseudo-puissance n si sa dérivée $f'(x) \in n\mathbb{Z}_p[x]$.*

Exemple 3.23.

- $g(x) = x^n$ *alors* $g'(x) = nx^{n-1} \in n\mathbb{Z}_p[x]$.
- $g(x) = h(n)^n$ *tel que* $h(x) \in \mathbb{Z}_p[x]$ *alors* $g'(x) = nh'(x)h(x)^{n-1} \in n\mathbb{Z}_p[x]$.
- $g(x) = T_n(\cos\theta)$ *alors* $T_n'(\cos\theta) = n\frac{\sin n\theta}{\sin\theta} \in n\mathbb{Z}_p[x]$.

Dans la proposition suivante on va utiliser le **TAF** pour démontrer des congruences pour des polynômes.

Proposition 3.24. *Soit $f \in \mathbb{Z}_p[x]$, si f est une pseudo-puissance n, alors*

$$a \equiv b (\operatorname{mod} p\mathbb{Z}_p) \Rightarrow f(a) \equiv f(b) (\operatorname{mod} pn\mathbb{Z}_p).$$

Démonstration. Pour montrer que $f(a) \equiv f(b)(\operatorname{mod} pn\mathbb{Z}_p)$, il suffit de montrer que

$$|f(a) - f(b)|_p \leq |pn|_p$$

En effet, on a

$$|f(a) - f(b)|_p = |f(b + (a - b)) - f(b)|_p$$

Avec $a, b \in \mathbb{Z}_p$ tel que $|b|_p \leq 1$ et $|a - b|_p \leq |p|_p \leq |p|_p^{\frac{1}{p-1}}$.

Les conditions du **TAF** sont vérifiées, donc on applique ce théorème, on obtient

$$\begin{aligned} |f(b + (a - b)) - f(b)|_p &\leq |a - b|_p . \|f'\| \\ &\leq |p|_p . |n|_p = |pn|_p \end{aligned}$$

D'où

$$|f(a) - f(b)|_p \leq |pn|_p.$$

□

Proposition 3.25. *Soit $(f_n)_{n\geq 1}$ une suite de polynômes vérifiant les congruences*

$$f_{np}(x) \equiv f_n(x^p)(\operatorname{mod} pn\mathbb{Z}_p[x]),\ (n \geq 1)$$

Alors $f_n(x)$ est une pseudo-puissance n, $\forall n \geq 1$.

Démonstration. On va montrer que $f_n'(x) \in n\mathbb{Z}_p[x]$.

On peut écrit $n = mp^k$ tel que $k \geq 1$ et $(p, m) = 1$, alors

$$f_{mp^k}(x) \equiv f_{mp^{k-1}}(x^p)(\operatorname{mod} mp^k\mathbb{Z}_p[x])$$

Après dérivation de la congruence, on a

$$f'_{mp^k}(x) \equiv pf'_{mp^{k-1}}(x^p).x^{p-1}(\bmod mp^k\mathbb{Z}_p[x])$$

Par hypothèse, on a

$$f'_{mp^{k-1}}(x) \in mp^{k-1}\mathbb{Z}_p[x]$$

i.e.,

$$f'_{mp^{k-1}}(x) \equiv 0(\bmod mp^{k-1}\mathbb{Z}_p[x])$$

Alors

$$pf'_{mp^{k-1}}(x) \equiv 0(\bmod mp^k\mathbb{Z}_p[x])$$

Donc

$$f'_{mp^k}(x) \equiv 0(\bmod mp^k\mathbb{Z}_p[x]).$$

□

Lemme 3.26. *Les polynômes de Chebyshev de premier espèce vérifient la congruence :*

$$T_p(x) \equiv x^p(\bmod p\mathbb{Z}_p[x]),\ (n \geq 0).$$

Démonstration. Soit $T_n(\cos\theta) = \cos n\theta$.
On a $\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2}$, alors

$$T_n\left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right) = \frac{e^{in\theta}+e^{-in\theta}}{2}$$

On utilisant le changement de variable $t = e^{i\theta}$, donc

$$T_n\left(\frac{t+t^{-1}}{2}\right) = \frac{t^n+t^{-n}}{2}$$

On pose $n = p$ impair et on effectue le changement de variable $x = \frac{t+t^{-1}}{2}$, on obtient

$$T_p\left(\frac{t+t^{-1}}{2}\right) = \frac{t^p+t^{-p}}{2} \equiv \left(\frac{t+t^{-1}}{2}\right)^p (\bmod p\mathbb{Z}_p[x])$$

D'où

$$T_p(x) \equiv x^p(\bmod p\mathbb{Z}_p[x]).$$

□

Théorème 3.27. *Les polynômes de Chebyshev du premier espèce vérifient la congruence :*

$$T_{np}(x) \equiv T_n(x^p)\ (\bmod\ np\mathbb{Z}_p[x]),\ (n \geq 0).$$

Démonstration. Nous montrons que $|T_{np}(x) - T_n(x^p)|_p \leq |np|_p$.
On pose $n = mp^k$, avec $k \geq 0$ et $(m,p) = 1$, alors

$$\begin{aligned}|T_{np}(x) - T_n(x^p)|_p &= |T_{mp^{k+1}}(x) - T_{mp^k}(x^p)|_p \\ &= |T_{mp^k}(T_p(x)) - T_{mp^k}(x^p)|_p \\ &= |T_{mp^k}(x^p + pr(x)) - T_{mp^k}(x^p)|_p\end{aligned}$$

avec $|x|_p^p \leq 1$ et $r(x) \in \mathbb{Z}_p[x]$, alors $|pr(x)|_p \leq |p|_p \leq |p|_p^{\frac{1}{p-1}}$.
Les conditions du **TAF** sont vérifiées, donc on applique ce théorème, on obtient

$$\begin{aligned}|T_{mp^k}(x^p + pr(x)) - T_{mp^k}(x^p)|_p &\leq |pr(x)|_p.\|T'_{mp^k}\| \\ &\leq |p|_p.|mp^k|_p = |mp^k p|_p\end{aligned}$$

(car $\|T'_{mp^k}\| = |mp^k|_p.\|U_{mp^k-1}\| \leq |mp^k|$)
Alors

$$|T_{mp^{k+1}}(x) - T_{mp^k}(x^p)|_p \leq |mp^k p|_p$$

D'où

$$|T_{np}(x) - T_n(x^p)|_p \leq |np|_p.$$

□

Définition 3.28. *Pour tout $n \geq 0$, le n-ème polynôme de Chebyshev est défini comme suit :*

$$T_n(x) = \sum_{k=0}^{[\frac{n}{2}]} (-1)^k \frac{n}{n-k} \binom{n-k}{k} 2^{n-2k-1} x^{n-2k}.$$

Lemme 3.29. *Dans l'anneau des polynômes $\mathbb{Z}_p[x]$, on a la congruence*

$$T_q(x) \equiv x^q \pmod{p\mathbb{Z}_p[x]},\ \textit{tel que}\ q = p^\nu,\ \nu \geq 1\ \textit{et}\ p > 2.$$

Démonstration. D'après la formule des polynômes de Chebychev, on a

$$\begin{aligned}T_q(x) &= \sum_{k=0}^{[\frac{q}{2}]} (-1)^k \frac{q}{q-k} \binom{q-k}{k} 2^{q-2k-1} x^{q-2k} \\ &= 2^{q-1} x^q + \sum_{k=1}^{[\frac{q}{2}]} (-1)^k \frac{q}{q-k} \binom{q-k}{k} 2^{q-2k-1} x^{q-2k}\end{aligned}$$

Pour $1 \leq k \leq [\frac{q}{2}] < q$, on a $v_p(k) < v_p(q) = \nu$.

Donc

$$v_p\left(\frac{q}{q-k}\right) = v_p(q) - v_p(q-k) = \nu - v_p(k) > 0$$

Alors

$$\left|(-1)^k 2^{q-2k-1} \frac{q}{q-k}\binom{q-k}{k}\right|_p = \left|\frac{q}{q-k}\right|_p = |p|_p^{\nu - v_p(k)} < 1$$

D'où

$$(-1)^k 2^{q-2k-1} \frac{q}{q-k}\binom{q-k}{k} \equiv 0 (\text{mod } p) \tag{3.3}$$

D'autre part, d'après le théoème de Fermat, on a

$$2^{q-1} \equiv 1 (\text{mod } p) \tag{3.4}$$

De (3.3) et (3.4), on sorte que

$$T_q(x) \equiv x^q \ (\text{mod } p\mathbb{Z}_p[x]).$$

$\square$

Proposition 3.30. *Soit $q = p^\nu$, $\nu \geq 1$ et $L_q = \{a \in \mathbb{C}_p : |a|_p \leq 1$ et $|a^q - a|_p \leq |p|_p^{\frac{1}{p-1}}\}$. Soit $m > 0$, pour tout $a \in L_q$ la suite $(T_{mq^k}(a))_{k \geq 0}$ converge dans $\mathbb{C}_p$.*

Démonstration. Pour montrer que $(T_{mq^k}(a))_{k\geq 0}$ définit une suite converge dans $\mathbb{C}_p$, il suffit de montrer que

$$|T_{mq^{k+1}}(a) - T_{mq^k}(a)|_p \to 0 \ \ \textit{quand } k \to +\infty$$

On a $T_q(x) \equiv x^q$ (mod $p\mathbb{Z}_p[x]$) donc $T_q(x) = x^q + pr_q(x)$, avec $r_q(x) \in \mathbb{Z}_p[x]$.
Donc pour tout $x \in L_q$ tel que $|x|_p \leq 1$, on a $|r_q(x)|_p \leq 1$, et $|pr_q(x)|_p \leq |p|_p \leq |p|_p^{\frac{1}{p-1}}$.
On applique le **TAF**, on obtient

$$\begin{aligned}
|T_{mq^{k+1}}(x) - T_{mq^k}(x^q)|_p &= |T_{mq^k}(x^q + pr_q(x)) - T_{mp^k}(x^q)|_p \\
&\leq |pr_q(x)|_p.\|T'_{mq^k}\| \\
&\leq |p|_p.|q|_p^k
\end{aligned}$$

D'autre part, pour $a \in L_q$, alors on applique le **TAF** de nouveau, on trouve

$$\begin{aligned}
|T_{mq^k}(a^q) - T_{mq^k}(a)|_p &= |T_{mq^k}(a + (a^q - a)) - T_{mq^k}(a)|_p \\
&\leq |a^q - a|_p.\|T'_{mq^k}\|
\end{aligned}$$

on sait que $|a^q - a|_p \leq |p|_p^{\frac{1}{p-1}}$, alors

$$|T_{mq^k}(a^q) - T_{mq^k}(a)|_p \leq |p|_p^{\frac{1}{p-1}} |q|_p^k$$

Donc pour tout $a \in L_q$, on a

$$\begin{aligned} |T_{mq^{k+1}}(a) - T_{mq^k}(a)|_p &= |T_{mq^k}(a^q + pr(a)) - T_{mq^k}(a^q) + T_{mq^k}(a^q) - T_{mq^k}(a)|_p \\ &\leq \max(|T_{mq^k}(a^q + pr(a)) - T_{mq^k}(a^q)|_p, |T_{mq^k}(a^q) - T_{mq^k}(a)|_p) \\ &\leq \max(|p|_p, |p|_p^{\frac{1}{p-1}})|q|_p^k = |p|_p^{\frac{1}{p-1}} |q|_p^k \end{aligned}$$

D'où pour tout élément $a \in L_q$, on a $|T_{mq^{k+1}}(a) - T_{mq^k}(a)|_p \to 0$ quand $k \to \infty$, et $(T_{mq^k}(a))_{k \geq 0}$ est une suite de Cauchy, alors elle converge dans $\mathbb{C}_p$. □

3.3.5 Nombres et polynômes de Bernoulli

M. Zuber dans sa thèse [22], a utilisé le **TAF** pour donner des nouvelles démonstrations des résultats connu sur les nombres et les polynômes de Bernoulli.

Définition 3.31. *On définit les polynômes de Bernoulli $B_k(x)$ par le développement en série*

$$\frac{te^{xt}}{e^t - 1} = \sum_{k \geq 0} B_k(x) \frac{t^k}{k!}.$$

Exemple 3.32.

$$\begin{aligned} &B_0(x) = 1 &&, B_3(x) = x^3 - \tfrac{3}{2}x^2 + \tfrac{1}{2}x \\ &B_1(x) = x - \tfrac{1}{2} &&, B_4(x) = x^4 - 2x^3 + x^2 - \tfrac{1}{30} \\ &B_2(x) = x^2 - x + \tfrac{1}{6} &&, B_5(x) = x^5 - \tfrac{5}{2}x^4 + \tfrac{5}{3}x^3 - \tfrac{1}{6}x \end{aligned}$$

Définition 3.33. *On définit les nombres de Bernoulli b_k par le développement en série*

$$\frac{t}{e^t - 1} = \sum_{k \geq 0} b_k \frac{t^k}{k!}.$$

Remarque. *Les nombres de Bernoulli ne sont que les termes constants des polynômes de Bernoulli, i.e., $b_k = B_k(0)$.*

Exemple 3.34. *On peut calculer facilement les premières valeurs des nombres de Bernoulli :*

$$b_0 = 1,\ b_1 = -\frac{1}{2},\ b_2 = \frac{1}{6},\ b_3 = 0,\ b_4 = -\frac{1}{30}, \ldots$$

Définition 3.35. *Soient $k, n \in \mathbb{N}^*$. On définit les sommes de Bernoulli comme suit :*

$$S_k(n) = \sum_{i=1}^{n-1} i^k.$$

Propriétés 3.36. *[22] Les nombres et polynômes de Bernoulli vérifient les propriétés suivantes :*

1) $b_{2k+1} = 0,\ (k \geq 1)$.

2) $B_k(x) = \sum\limits_{i=0}^{k} \binom{k}{i} b_{k-i} x^i,\ (k \geq 0)$.

3) $B'_n(x) = nB_{n-1}(x)$.

4) $S_k(n) = \sum\limits_{0 \leq i < n} i^k = \frac{B_{k+1}(n) - b_{k+1}}{k+1},\ (n \geq 1)$.

Théorème 3.37. *Les nombres de Bernoulli ont les propriétés suivantes :*

1) Si $p-1$ ne divise pas $k \geq 1$, alors il existe $r_k \in \mathbb{Z}_p$ tel que

$$b_k = k \cdot r_k\ .$$

2) Si p est impair et si $p-1$ divise $k \geq 1$, alors il existe $r_k \in \mathbb{Z}_p$, tel que

$$b_k = \frac{p-1}{p} + k \cdot r_k\ .$$

Démonstration. D'après la définition (3.35), nous avons

$$S_k(p) = \sum_{i=1}^{p-1} i^k,\ (k \geq 1)$$

Soit $\mu_{p-1} = \{\zeta \in \mathbb{C}_p,\ \zeta^{p-1} = 1\} \subset \mathbb{Z}_p$, nous remplaçons dans la somme précédente chaque entier i par la racine de l'unité $\zeta_i \in \mu_{p-1}$ qui lui est congrue modulo p

$$i \equiv \zeta_i \pmod{p\mathbb{Z}_p}$$

Donc

$$S_k(p) \equiv \sum_{i=1}^{p-1} \zeta_i^k = \sum_{\zeta \in \mu_{p-1}} \zeta^k \pmod{kp\mathbb{Z}_p}.$$

En effet,

pour démontrer cette congruence en appliquant le **TAF** à $f(x) = x^k$ au voisinage de $x = i$, nous avons

$$|\zeta_i^k - i^k|_p \leq |\zeta_i - i|_p\ \|f'\| \leq |p|_p\ \|f'\| \leq |pk|_p$$

Donc

$$i^k \equiv \zeta_i^k \pmod{pk}$$

D'où

$$S_k(p) = \sum_{\zeta \in \mu_{p-1}} \zeta^k + pk \cdot u \quad avec\ u \in \mathbb{Z}_p. \tag{3.5}$$

D'autre part, on a

$$S_k(n) = \frac{B_{k+1}(n) - b_{k+1}}{k+1}$$

D'après de propriétés 3.36, on trouve

$$\begin{aligned} S_k(n) &= \frac{1}{k+1} \sum_{i=1}^{k+1} \binom{k+1}{i} n^i b_{k+1-i} \\ &= \sum_{i=1}^{k+1} \frac{1}{i} \binom{k}{i-1} n^i b_{k+1-i} \\ &= nb_k + \sum_{i=2}^{k+1} \frac{1}{i} \binom{k}{i-1} n^i b_{k+1-i} \end{aligned}$$

Nous remplaçons dans l'expression précédente n par $p > 2$, on obtient

$$\begin{aligned} S_k(p) &= pb_k + \sum_{i=2}^{k+1} \frac{1}{i} \binom{k}{i-1} p^i b_{k+1-i} \\ &= pb_k + pk \left(\sum_{i=2}^{k+1} \frac{1}{i(i-1)} \binom{k-1}{i-2} p^{i-2}\ pb_{k+1-i} \right) \end{aligned}$$

ou encore

$$S_k(p) = pb_k + pk \left(\sum_{i=2}^{k+1} \frac{(k-1)!}{(k-i+1)!} \cdot \frac{p^{i-2}}{i!}\ pb_{k+1-i} \right)$$

Le terme $\frac{(k-1)!}{(k-i+1)!}$ est entier et le terme $\frac{p^{i-2}}{i!} \in \mathbb{Z}_p$, pour $p \neq 2$.

En effet,

$$v_p\left(\frac{p^{i-2}}{i!}\right) = v_p\left(p^{i-2}\right) - v_p(i!) = i - 2 - \left(\frac{i - S_p(i)}{p-1}\right) > -1$$

D'où

$$S_k(p) = pb_k + pk.v \quad avec\ v \in \mathbb{Z}_p. \tag{3.6}$$

De (3.5) et (3.6), on a

$$S_k(p) = \begin{cases} \sum_{\zeta\in\mu_{p-1}} \zeta^k + pk.u \\ pb_k + pk.v \end{cases}$$

on trouve

$$pb_k = \sum_{\zeta\in\mu_{p-1}} \zeta^k + pk.r_k \quad \textit{où } r_k = u - v \in \mathbb{Z}_p$$

• Si k n'est pas multiple de $p-1$, alors $b_k = k \cdot r_k$ avec $r_k \in \mathbb{Z}_p$.

• Si $p-1$ divise k, alors

$$b_k = \frac{p-1}{p} + k \cdot r_k \quad \textit{avec} \quad r_k \in \mathbb{Z}_p \ (p \neq 2).$$

En effet, on considère le polynôme $f(x) = \frac{B_{k+1}(x)}{k+1} \in \mathbb{Q}_p[x]$.

Donc

$$f'(x) = B_k(x) \textit{ et } f''(x) = kB_{k-1}(x)$$

D'après le **TAF** d'ordre 2, on peut écrire

$$\begin{aligned} \left| \frac{B_{k+1}(p) - b_{k+1}}{k+1} - pb_k \right|_p &= |f(p) - f(0) - pf'(0)|_p \\ &\leq \left| \frac{p^2}{2} \right|_p .\|f''\| \\ &= \left| \frac{kp}{2} \right|_p .\|pB_{k-1}(x)\| \\ &\leq |kp|_p \end{aligned}$$

Alors

$$pb_k \equiv \frac{B_{k+1}(p) - b_{k+1}}{k+1} (\bmod kp\mathbb{Z}_p)$$

avec

$$\frac{B_{k+1}(p) - b_{k+1}}{k+1} = \sum_{i=1}^{p-1} i^k$$

► Si $(p-1)$ ne divise pas k, alors

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} \zeta_i^k = \sum_{i=0}^{p-2} (\zeta^k)^i = \frac{1-\zeta^{k(p-1)}}{1-\zeta^k} \equiv 0 (\bmod p)$$

Puisque

$$\zeta^{p-1} \equiv 1 (\bmod p) \ \textit{ et } \ \zeta^k \not\equiv 1 (\bmod p).$$

► Si $(p-1)$ divise k, alors

Pour $1 \leq i \leq p-1$, d'aprés le théorème de Fermat, on a

$$i^k \equiv 1 (\bmod p)$$

Donc

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} 1 \equiv p-1 (\bmod p).$$

□

Bibliographie

[1] **Y. AMICE :** Les nombres p-adiques. Presses universitaires de France, 1975.

[2] **G. BACHMAN :** Introduction to p-adic numbers and valuation theory. Academic Press. Inc, 1964.

[3] **A.J. BAKER :** An Introduction to p-adic Numbers and p-adic Analysis, Departement of mathematics, University of Glasgow, G128QW, Scotland, 2004.

[4] **P. BORWEIN et T. ERDÉLYI :** Polynomials and polynomial inequalities. Springer Science et Business Media, 1995.

[5] **A. CHAMBERT-LOIR :** Algebre corporelle. Éditions École Polytechnique, 2005.

[6] **B. DIARRA :** Analyse p-adique. Cours de DEA-Algèbre Commutative, FAST-Université du Mali, 1999.

[7] **B. DIARRA et D. SYLLA :** p-Adic dynamical systems of Chebyshev polynomials. P-Adic Numbers, Ultrametric Analysis, and Applications, vol. 6, no 1, p. 21-32, 2014.

[8] **F.Q. GOUVÊA :** p-adic Numbers. An Introduction, Springer Verlag, Berlin Heidelberg, New York, Second Edition, Universitext, 2000.

[9] **G.H. HARDY, E.M. WRIGHT :** An introduction to the theory of numbers. Oxford university press, 1979.

[10] **A. JUNOD :** Congruences par l'analyse p-adique et le calcul symbolique. Thèse de doctorat. Université de Neuchâtel, 2003.

[11] **S. KATOK :** p-adic Analysis Compared with Real. American Mathematical Soc, 2007.

[12] **D.S. KIM, T. KIM, et S.H. LEE :** Some identities for Bernoulli polynomials involving Chebyshev polynomials. arXiv preprint arXiv :1211.1582, 2012.

[13] **N. KOBLITZ :** p-adic Numbers, p-adic Analysis, and Zeta-Functions. Springer Science et Business Media, 2012.

[14] **J.C. MASON, D.C. HANDSCOMB :** Chebyshev polynomials. Chapman and Hall/CRC, 2002.

[15] **A. ROBERT :** A course in p-adic analysis. Springer Science et Business Media, 2000.

[16] **A. ROBERT :** A Note on the Numerators of the Bernoulli Numbers. Expositiones Mathematicae, vol. 9, p. 189-191, 1991.

[17] **A. ROBERT :** Cours d'analyse ultramétrique. Troisi eme cycle romand de math ematiques, Lausanne et Berne, 1990, vol. 1991.

[18] **A. ROBERT :** Le théorème des accroissements finis p-adique. In : Annales mathématiques Blaise Pascal. p. 245-258, 1995.

[19] **A. ROBERT :** Polynômes de Legendre mod p. Publication du Département de Mathématiques Pures, Université Blaise Pascal, Clermont, vol. 2, 1990.

[20] **A. ROBERT :** Systèmes de Polynômes, Queen's papers in pure and applied Mathematics, No. 35, Queen's University, Kingston, Ontario, Canada, 1973.

[21] **L. TODJIHOUNDE :**. Calcul différentiel : cours et exercices corrigés. Cepadues, 2004.

[22] **M. ZUBER :** Propriétés p-adiques de polynômes classiques. Thèse de doctorat. Université de Neuchâtel, 1992.