الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. /11

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

QUELQUES PROPRIETES DU CORPS DE NOMBRES P-ADIQUES

Dirigé par : Ismail Kaouache

Presenté par : 1. Safa Boukouira
2. Nassima Souilah

Année universitaire
2010-2011

دعاء

دعاء

اللهم لا تجعلنا نصاب بالغرور إذا نجحنا

و باليأس

إذا أخفقنا و ذكرنا أن

الإخفاق هو التجربة التي تسبق النجاح

اللهم إذا أعطيتنا نجاحا فلا تأخذ تواضعنا

و إذا أعطيتنا تواضعا فلا تأخذ

اعتزازنا بكرامتنا .

اللهم اختم بالسعادة أحلامنا و حقق بالزيادة أمالنا

ربنا تقبل دعائنا

إنك أنت السميع العليم

Remerciements

Nos remerciements vont tout premièrement à dieu tout puissant pour la volonté, la santé et la patience qu'il ma Donnée pour terminer ce mémoire.

Nous adressons mes remerciements d'abord à mon encadreur monsieur S. kaouache qui a accepté l'encadrement sa disponibilité, ses encouragements et ses précieux conseils tout au Long de ce travail.

Nous adressons aussi mes remerciements à tous les Enseignants et a tout l'ensemble des collègues de l'équipe de Mathématique.

Table des matières

Introduction Générale

Dans ce mémoire, nous allons déterminer une nouvelle valeur absolue p-adique sur le corps $\mathbb{Q}$ et nous allons essayer de compléter $\mathbb{Q}$ par ca valeur absolue. Finalement, nous donnerons une procédure générale pour les corps ultra-métriques.
On sait que le corps de nombres réels $\mathbb{R}$ est complété de $\mathbb{Q}$ pour la valeur absolue et qu'à chaque nombre premier p, on peut associer une valeur absolue (que l'on appelle valeur absolue p-adique). Les questions que l'on se pose sont :

*Est-ce qu'il y a d'autres valeurs absolues sur ?

*Si oui, quels sont les autres complets de pour ces valeurs absolues ?

Ce mémoire comporte deux chapitres. Il est structuré de la manière suivante :
Le premier chapitre de ce mémoire tentera de rependre à la première question. Quand à la seconde question, elle sera au sujet des valeurs absolues ultra-métriques et des corps ultra-métrique. Comme cas particulier, nous parlerons de la valeur absolue p-adique et $\mathbb{Q}_p$
Dans le deuxième chapitre, on présente quelques résultats classiques sur l'analyse p-adique, notamment les propriétés analytiques, topologiques et algébriques.du corps de nombres p-adique.

Chapitre 1

Corps de nombres p-adiques

La présente partie consiste à donner un nouveau corps dit le corps de *nombres* $p-$ *adiques*, que l'on munit d'une norme ultra-métrique de telle sorte qu'on peut le considérer comme une complétion de $\mathbb{Q}$ par rapport à cette norme.

1.1 Corps de nombres ultra-métriques

Définition 1.1.1 *Soit $\mathbb{k}$ un corps munit d'une norme $\|.\|$.*
On dit que la norme $\|.\|$ est ultra-métrique (ou non-Archimédiènne) , si et seulement si

$$\forall x,\ y \in \mathbb{k} : \|x + y\| \leq \max\{\|x\|, \|y\|\} \tag{1.1}$$

Définition 1.1.2 *Tout corps munit d'une norme non-archimédiènne s'appel corps $ulta-$ $métrique$.*

Remarque 1.1.3 *Si $d_{\|.\|}$ est la distance induite par la norme $\|.\|$, alors la relation précédente peut s'écrire sou la forme :*

$$\forall x,\ y,\ z \in \mathbb{k} : d_{\|.\|}(x, z) \leq \max\left\{d_{\|.\|}(x, y), d_{\|.\|}(y, z)\right\} \tag{1.2}$$

Proposition 1.1.4 *La norme $\|.\|$ est ultramétrique si et seulement si*

$$\forall n \in \mathbb{N} : \|n\| \leq 1 \tag{1.3}$$

Preuve. Supposons que $\|.\|$ est ultramétrique et montrons par récurrence que

$$\forall n \in \mathbb{N} : \|n\| \leq 1$$

Pour $n = 1$, on a

$$\|1\| = 1 \leq 1$$

Supposons maintenant que $\|n\| \leq 1$.
Alors

$$\|n+1\| \leq \max\{\|i\|, \|1\|\} = 1$$

Inversement : Supposons que

$$\forall n \in \mathbb{N} : \|n\| \leq 1$$

et montrons que $\|.\|$ est ultramétrique.
ie :

$$\forall x,\, y \in \Bbbk : \|x+y\| \leq \max\{\|x\|, \|y\|\}$$

Si $y = 0$, alors

$$\|x+y\| = \|x\| \leq \max\{\|x\|, 0\}$$

Si $y \neq 0$, il suffit de démontrer que

$$\forall x,\, y \in \Bbbk : \left\|\frac{x}{y} + 1\right\| \leq \max\left\{\left\|\frac{x}{y}\right\|, \|1\| = 1\right\}$$

C'est-à-dire

$$\forall x \in \mathbb{Q} : \|x+1\| \leq \max\{\|x\|, \|1\|\}$$

On a

$$\|x+1\|^n = \|(x+1)^n\|$$

$$\begin{aligned} &= \left\|\sum_{k=0}^{n} C_n^k\, x^k\right\| \leq \sum_{k=0}^{n} \|C_n^k\| . \|x^k\| \\ &\leq \sum_{k=0}^{n} \|x^k\| \end{aligned}$$

Si $\|x\| \leq 1$, alors

$$\|x\|^n \leq 1, \forall n \in \mathbb{N}$$

Si $\|x\| \succ 1$, alors

$$\max\{\|x\|^n, 1\} = \|x\|^n$$

D'où

$$\|x+1\|^n \leq \sum_{k=0}^{n} \max\{\|x\|^n, 1\}$$

$$\Rightarrow \|x+1\|^n \leq (n+1).\max\{\|x\|^n, 1\}$$

On en déduit le résultat en prenant la racine$n-$ième des deux membreset en passant à lal imite quand n tend vers $+\infty$ ■

Lemme 1.1.5 *Si $\|\|$est ultra-métrique et $\|x\| \neq \|y\|$, alors*

$$\|x+y\| = \max\{\|x\|, \|y\|\} \tag{1.4}$$

Preuve. On peut supposer $\|x\| \succ \|y\|$. On a alors

$$\begin{aligned} \|x+y\| &\leq \max\{\|x\|, \|y\|\} = \|x\| = \|(x+y)-y\| \\ &\leq \max\{\|x+y\|, \|y\|\} \\ &\leq \|x+y\|, \text{ (car } \|y\| \prec \|x\| \text{)} \end{aligned}$$

D'où

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

■

1.2 Les nombres p-adiques

1.2.1 Valuations $p-$adiques

Définition 1.2.1 ***(Valuation p-adique)*** *La valuation p-adique est une fonction de $\mathbb{Z}_p$ dans $\mathbb{N} \cup \{+\infty\}$ vérifiant*

$$V_p(x) = \begin{cases} \max\{r \in \mathbb{Z}_+ \text{ tel que } p^r/x\}, & si\ x \neq 0 \\ +\infty, & si\ x = 0 \end{cases} \tag{1.5}$$

La relation précédente, peut s'écrire sous la forme

$$x = p^{V_p(x)}.x' \text{ avec } (p, x') = 1 \tag{1.6}$$

Remarque 1.2.2 *Si $x = \frac{a}{b} \in \mathbb{Q}^*$, alors*

$$V_p(x) = V_p(a) - V_p(b) \tag{1.7}$$

Preuve. En effet

$$\frac{a}{b} \in \mathbb{Q}^* \Rightarrow (a,b) \in \mathbb{Z}^{*2}$$

$$\Longrightarrow \begin{cases} a = a_1.p^{V_p(a)}, (a_1, p) = 1 \\ b = b_1.p^{V_p(b)}, (b_1, p) = 1 \end{cases}$$

$$\begin{aligned} \Rightarrow \quad \frac{a}{b} &= \frac{a_1.p^{V_p(a)}}{b_1.p^{V_p(b)}} \\ &= \frac{a_1}{b_1}.p^{V_p(a)-V_P(b)} \text{ avec } (a_1, b_1, p) = 1 \end{aligned}$$

On en déduit que

$$V_p(x) = V_p(\frac{a}{b}) = V_p(a) - V_p(a)$$

■

Proposition 1.2.3 *Soient x, $y \in \mathbb{Q}$, Alors la valuation V_p vérifie*

$$1) V_p(x.y) = V_p(x) + V_p(y) \tag{1.8}$$

$$2) V_p(x + y) \geq \min\{V_p(x), V_p(y)\} \tag{1.9}$$

Preuve.

1) Soient

$$\begin{cases} x = p^{V_p(x)}.x' \\ y = y'.p^{V_p(y)} \end{cases} \text{, avec } p \nmid x' \text{ et } p \nmid y'$$

C'est-à-dire

$$x'.y' \neq k.p \ (k \in \mathbb{Z})$$

Alors

$$x.y = x'.y'.p^{V_p(x)+V_p(y)}$$

Donc

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

2) Soient

$$x = p^r \frac{a}{b} ety = p^s \frac{c}{d}, \text{ tels que } r \leq s$$

Alors

$$\begin{aligned} V_p(x + y) &= V_p\left(p^r \frac{a}{b} + p^s \frac{c}{d}\right) \\ &= V_p p^r \left[\frac{a}{b} + p^{s-r} \frac{c}{d}\right] \\ &= V_p\left(p^r \left[\frac{da + p^{s-r}cb}{bd}\right]\right), \text{ avec } p \nmid bd. \end{aligned}$$

Donc

$$\begin{aligned} V_p(x+y) &= V_p(p^r) + V_p\left(\left[\frac{da + p^{s-r}cb}{bd}\right]\right) \\ &\geq r = \min\{V_p(x), V_p(y)\} \end{aligned}$$

■

Lemme 1.2.4 *Soit $p > 2$ un nombre premier, alors pour tout $n \in \mathbb{N}$, nous avons*

$$v_p\left(\frac{p^n}{n!}\right) \geq n\ \frac{p-2}{p-1} \tag{1.10}$$

Preuve. Pour tout $n \in \mathbb{N}$, on a

$$v_p\left(\frac{p^n}{n!}\right) = v_p(p^n) - v_p(n!) = n - v_p(n!)$$

D'autre part

$$\begin{aligned} v_p(n!) &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... \\ &\leq \frac{n}{p} + \frac{n}{p^2} + ... = \frac{n}{p-1} \end{aligned}$$

Donc

$$v_p\left(\frac{p^n}{n!}\right) \geq n - \frac{n}{p-1} = n\ \frac{p-2}{p-1}$$

■

1.2.2 Norme p-adique

Définition 1.2.5 ***(norme p-adique)*** *Soit p un nombre premier.*
La norme p-adique est une application de $\mathbb{Q}$ dans $\mathbb{R}_+$ vérifiant

$$\|x\|_p = \begin{cases} p^{-V_p(x)},\ si\ x \neq 0 \\ 0,\ si\ x = 0 \end{cases} \tag{1.11}$$

Proposition 1.2.6 *$\|.\|_p$ est une norme ultra-métrique sur $\mathbb{Q}$.*

Preuve. Il est facile de montrer que $\|.\|_p$ est une norme sur $\mathbb{Q}$.
Pour montrer que $\|.\|_p$ est une norme ultra-métrique sur $\mathbb{Q}$, il suffit de prouver l'inégalité triangulaire forte (1.1).

Si $x = 0$ ou $y = 0$, l' inégalité (1.1) est évidente.
Supposons maintenant que

$$x, y \neq 0, \text{ tels que } x = \frac{a}{b}, y = \frac{c}{d}$$

Alors

$$V_p(x+y) = V_p(ad+bc) - V_p(b) - V_p(d)$$

$$\begin{aligned} &= \min\{V_p(a) - V_p(b), V_p(c) - V_p(d)\} \\ &= \min\{V_p(x), V_p(y)\} \end{aligned}$$

Donc

$$\|x+y\|_p = p^{-V_p(x+y)} \leq \max\{p^{-V_p(x)},\ p^{-V_p(y)}\}$$
$$= \max\left\{\|x\|_p, \|y\|_p\right\}$$

Alors $\|.\|_p$ est ultra-métrique. ■

Remarque 1.2.7 *L'application $\|.\|_p$ est appellée norme p-adique (valeur absolue p-adique). La distance sur $\mathbb{Q}$ induite par la norme p-adique $\|.\|_p$ est notée par d_p et définie par*

$$d_p(x, y) = \|x - y\|_p$$

Exemple 1.2.8 *Pour la distance usuelle, on a $|10 - 3| = 7$. Tandis que pour la norme $5 -$ adique on a*

$$\|10 - 3\|_5 = \|7\|_5$$

Or

$$7 = 2 + 1.5$$
$$\Rightarrow V_5(7) = 0$$
$$\Rightarrow \|7\|_5 = 5^0 = 1$$

Remarque 1.2.9 *La norme p-adique $\|.\|_p$ prend les valeurs discrètes, et on a*

$$\|\mathbb{Q}\|_p = \{0,\ p^n\ ;\ n \in \mathbb{Z}\} \tag{1.12}$$

Désignons maintenant par $\|.\|_\infty$ la valeur absolue usuelle sur $\mathbb{Q}$. Il est clair que $\|.\|_\infty$ est une norme Archimédiènne, et donc $\mathbb{Z}$ n'est pas bornée pour la distance usuelle $d_{\|.\|_\infty}$ sur $\mathbb{R}$.

Si p est premier, tout entier n s'écrit sous la forme $n = p^r.m$ où $p \nmid m$ et r est la valuation p-adique de n. Donc

$$\forall n \in \mathbb{Z} : \|n\|_p \leq p^{-r} \leq 1$$

Alors $\mathbb{Z}$ est bornée pour toute valeur absolue p-adique $\|.\|_p$.
Le théorème suivant donne la relation entre les différentes normes p-adiques.

1.2.3 Formule de produit

Théorème 1.2.10 *Pour tout nombre rationnel non nul x, on a*

$$\prod_{p \text{ premier ou } p=\infty} \|x\|_p = 1 \tag{1.13}$$

Preuve. Soit $x \in \mathbb{Q}^*$, alors

$$x = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdot .... \cdot p_k^{r_k} \ (\text{ factorisation canonique de } x\ ), \text{où } u = \pm 1$$

Soit p un nombre premier quelconque.
Si $p \neq p_i$, $\forall i = \overline{1, k}$. Alors

$$\|x\|_p = p^{-0} = 1$$

Si $p = p_i$, on aura

$$\|x\|_p = p_i^{-r_i}$$

D'autre part

$$\|x\|_\infty = |x| = p_1^{r_1} \cdot p_2^{r_2} \cdot .... \cdot p_k^{r_k}$$

Ce qui donne

$$\begin{aligned}\prod_{p \text{ premier ou } p=\infty} \|x\|_p &= \prod_{p \neq p_i} \|x\|_p \cdot \prod_{i=1}^{k} \|x\|_{p_i} \cdot \|x\|_\infty \\ &= 1 \cdot \left(p_1^{-r_1} \cdot p_2^{-r_2} \cdot .... \cdot p_k^{-r_k}\right) \cdot p_1^{r_1} \cdot p_2^{r_2} \cdot .... \cdot p_k^{r_k} \quad = 1\end{aligned}$$

■

Exemple 1.2.11 *Pour tout $p \notin \{2, 3, \infty\}$, on a*

$$\left\|\frac{3}{2}\right\|_p = \frac{\|3\|_p}{\|2\|_p} = \frac{1}{1} = 1$$

D'où

$$\begin{aligned}\left\|\frac{3}{2}\right\|_\infty \cdot \prod_{p \text{ premier}} \left\|\frac{3}{2}\right\|_p &= \left\|\frac{3}{2}\right\|_\infty \cdot \left\|\frac{3}{2}\right\|_2 \cdot \left\|\frac{3}{2}\right\|_3 \cdot \prod_{\substack{p \text{ premier} \\ p\notin\{2,3,\infty\}}} \left\|\frac{3}{2}\right\|_p \\ &= \frac{3}{2}.2.\frac{1}{3}.1 = 1\end{aligned}$$

Corollaire 1.2.12 *Deux valeurs absolues p-adiques $\|.\|_{p_1}$, $\|.\|_{p_2}$ sont équivalentes si et seulement si $p_1 = p_2$.*

Preuve. Il suffit de considérer la suite $(p_1^n)_{n\in\mathbb{N}}$.
Il est évident que cette suite converge vers 0 pour $\|.\|_{p_1}$.
Car

$$\|p_1^n\|_{p_1} = p_1^{-n} \longrightarrow 0; \text{quand } n \longrightarrow +\infty$$

Et si $p_1 \neq p_2$, on a

$$\|p_1^n\|_{p_2} = p_2^{-0} = 1.$$

Donc $(p_1^n)_{n\in\mathbb{N}}$ ne converge pas vers 0 pour $\|.\|_{p_2}$ ■

1.2.4 Les nombres p-adiques

On sait que le corps $\mathbb{R}$ est la complétion de $\mathbb{Q}$ par rapport la valeur absolue usuelle, et dans ce cas les éléments de $\mathbb{R}$ sont les classes d'équivalences des suites de Cauchy de $\mathbb{Q}$. La même procédure se fait pour une valeur absolue ultra-métrique $\|.\|_p$. La complétion de $\mathbb{Q}$ par rapport cette valeur absolue, donne un corps ultra-métrique appelé corps des *nombres* $p-$*adiques* et se note par $\mathbb{Q}_p$. Ainsi les éléments de $\mathbb{Q}_p$ sont les classes d'équivalences des suites de Cauchy dans $\mathbb{Q}$, muni de la relation suivante :

$$(a_n)\ R\ (b_n) \iff \lim_{n\longrightarrow\infty} \|a_n - b_n\|_p = 0 \tag{1.14}$$

Remarque 1.2.13 *La valeur absolue $\|.\|_p$ peut être prolonger de $\mathbb{Q}$ sur tout $\mathbb{Q}_p$ de la façon suivante :*
Soit $x \in \mathbb{Q}_p$ et $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{Q}$ de limite x pour la distance p-adique $d_{\|.\|_p}$; alors

$$\|x\|_p = \lim_{n\longrightarrow\infty} \|x_n\|_p \tag{1.15}$$

ie :

$$\forall x \in \mathbb{Q}_p,\ \exists x_n \in \mathbb{Q} : x = \lim_{n \longrightarrow \infty} x_n$$

1.2.5 Développement p-adique de Hensel du corps de nombres p-adiques

Dans cette partie, on va montrer que tous les élément de $\mathbb{Q}_p$ admet une représentation canonique unique. Pour cela, on a besoin du lemme suivant.

Lemme 1.2.14 *Si $x \in \mathbb{Q}$ avec $\|x\|_p \leq 1$, alors*

$$\forall n \in \mathbb{N}\ ,\ \exists \alpha \in \mathbb{Z} : \|\alpha - x\|_p \leq p^{-n} \tag{1.16}$$

Preuve. Soient p un nombre premier et $x = \frac{a}{b}$ tel que :

$$(a, b) = 1$$

Nous avons

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

Donc p ne divise pas b, car si p divise $b \Rightarrow (a, b) \neq 1$.
De plus

$$(p, b) = 1 \Rightarrow (p^n, b) = 1, \forall n \in \mathbb{N}$$

$$\stackrel{\text{Bezout}}{\Longrightarrow} \exists m_1, m_2 \in \mathbb{Z} : m_1 b + m_2 p^n = 1$$

Posons $\alpha = a.m_1$, alors

$$\begin{aligned} \|\alpha - x\|_p &= \left\| a m_1 - \frac{a}{b} \right\|_p \\ &= \left\| \frac{a}{b} \right\|_p . \|(m_1 b - 1)\|_p \\ &\leq \|(m_1 b - 1)\|_p = \|m_2 p^n\|_p \\ &\leq p^{-n} \end{aligned}$$

■

Remarque 1.2.15 *Le lemme précédent peut s'écrire sous la forme uivante*
Si $x \in \mathbb{Q}$ avec $\|x\|_p \leq 1$, alors

$$\forall n \in \mathbb{N}\ ,\ \exists \alpha_n \in \mathbb{Z} : \|x - \alpha_n\|_p \leq p^{-n} \tag{1.17}$$

où $\alpha_n \in \{0, 1, ...p^n - 1\}$

Preuve. En effet. D'aprés le lemme précédent, si $x \in \mathbb{Q}$ où $\|x\|_p \leq 1$, alors

$$\forall n \in \mathbb{N} \ , \exists \alpha_n \in \mathbb{Z} : \|\alpha_n - x\|_p \leq p^{-n}$$

où $\alpha_n \in \{0, 1, ...p^n - 1\}$ et $k \in \mathbb{Z}$.
Il suffit de prendre

$$\alpha = kp^n + \alpha_n$$

Donc

$$\begin{aligned}
\|\alpha_n - x\|_p &= \|\alpha - kp^n - x\|_p \\
&\leq \max\left[\|kp^n\|_p , \|\alpha - x\|_p\right] \\
&\leq p^{-n}
\end{aligned}$$

■

Théorème 1.2.16 *Si la classe d'équivalence* $a \in \mathbb{Q}_p$ *vérifie la condition* $\|a\|_p \leq 1$*, alors, elle possède une seule représentation* $(a_n)_n$ *qui vérifie les conditions suivantes*

$$\begin{cases} (a_n) \in \mathbb{Z},\ 0 \leq a_n < p^n,\ \textit{tout}\ n \in \mathbb{N} \\ a_{n+1} \equiv a_n (\operatorname{mod} p^{n+1}),\ \textit{tout}\ n \in \mathbb{N} \\ \|a - a_n\|_p < p^{-n} \ ,\ \textit{pour}\ ,\ \textit{tout}\ n \in \mathbb{N} \end{cases} \tag{1.18}$$

Preuve. Existance.
Soit $a \in \mathbb{Q}_p$ tel que $\|a\|_p \leq 1$
Alors, d'après la remarque précédente, il existe $\lambda_0 = \alpha_1 \in \mathbb{Z}$ tel que

$$\|a - \lambda_0\|_p \leq p^{-1} < p^0 = 1$$

où $0 \leq \lambda_0 = \alpha_1 < p$.
Poson $x = a - \lambda_0$
Toujours, d'aprés la remarque précédente, il existe $\alpha_2 \in \mathbb{Z}$:

$$\|x - \alpha_2\|_p \leq p^{-2} < p^{-1}$$

où $0 \leq \alpha_2 < p^2$.
Ce qui assurer l'éxistance de $\lambda_1 = \frac{\alpha_1}{p}\,(\alpha_1 \in \mathbb{Z})$, tel que

$$\|a - (\lambda_0 + p\lambda_1)\|_p < p^{-1}$$

où $0 \leq \lambda_i \prec p.$, pour tout $i = \overline{1,2.}$
Par récurrence, on peut assurer l'existance de $\lambda_{n-1} = \frac{\alpha_n}{p^{n-1}}$ $(\alpha_n \in \mathbb{Z})$ tel que

$$\left\| a - (\lambda_0 + p\lambda_1 + ... + p^{n-1}\lambda_{n-1}) \right\|_p \leq p^{-n} < p^{-(n-1)}$$

où $0 \leq \lambda_i < p.$, pour tout $i = \overline{1, n-1.}$
Comme l'entier positif n est quelconque, alors on peut construire une suite d'entiers $(a_n) \in \mathbb{Z}$ telle que

$$a_n = \lambda_0 + p\lambda_1 + ... + p^n\lambda_n$$

où $0 \leq \lambda_i < p.$, pour tout $i = \overline{1, n.}$
qui vérifie

$$\begin{cases} (a_n) \in \mathbb{Z},\ 0 \leq a_n < p^n, \text{ tout } n \in \mathbb{N} \\ a_{n+1} \equiv a_n (\operatorname{mod} p^{n+1}), \text{ tout } n \in \mathbb{N} \\ \|a - a_n\|_p < p^{-n}\ ,\ \ pour\ , \text{ tout } n \in \mathbb{N} \end{cases}$$

Unicité.
Supposons qu'il existe deux suites de Cauchy (α'_d) et (α_d) vérifiant les conditions de la représentation précédente, telle que $\alpha'_d \neq \alpha_d$
Soit

$$\beta_n = \alpha_0 + \alpha_1 p + ... + \alpha_n p^n, où\ 0 \leq \alpha_n \leq p - 1$$

et

$$\beta'_n = \alpha'_0 + \alpha'_1 p + ...\alpha'_n p^n, \text{ où } 0 \leq \alpha'_n \leq p - 1$$

Alors

$$\begin{aligned} v_p(\beta_n - \beta'_n) &= v_p \left[\sum_{n=0}^{n} (\alpha'_n - \alpha_n) p^n \right] = v_p(\alpha'_d - \alpha_d) p^d \\ &= d, \text{ (car } 1 \leq \alpha'_d - \alpha_d \leq p - 1 \end{aligned}$$

Par suite

$$\|\beta'_n - \beta_n\|_p = p^{-d}$$

D'autre part

$$\begin{aligned} \|\beta'_n - \beta_n\|_p &= \|\beta'_d - \beta_d\|_p = \|\beta'_d - a + a - \beta_d\|_p \\ &\leq \max \left\{ \|\beta'_d - a\|_p , \|a - \beta_d\|_p \right\} < p^{-d} \end{aligned}$$

qui est une contradiction. ■

Remarque 1.2.17 *Supposons maintenant que $a \in \mathbb{Q}_p$ tel que $\|a\|_p \succ 1$, alors*

$$\exists m \in \mathbb{Z}_+ : \|a\|_p = p^m \tag{1.19}$$

Et soit $a' = p^m a$, avec $a' \in \mathbb{Q}$.
Alors

$$\begin{aligned} \|a'\|_p &= \|p^m.a\|_p \\ &= \|p^m\|_p . \|a\|_p \\ &= p^{-m}.p^m = 1 \\ &\Longrightarrow \|a'\|_p \leq 1 \end{aligned}$$

D'après le théorème précédent, on déduit que

$$\begin{aligned} a' &= \sum_{n=0}^{\infty} d_n p^n \\ &\Longrightarrow p^m.a = \sum_{n=0}^{\infty} d_n p^n \\ &\Longrightarrow a = \sum_{n=0}^{\infty} d_n p^{n-m} \\ &\Rightarrow a = \sum_{k=-m}^{\infty} \beta_k p^k \end{aligned}$$

Remarque 1.2.18 *La suite de Cauchy $(a_n)_n$ qui vérifie les conditions (18.1), s'appelle représentation canonique de a..*
C'est-à-dire

$$\forall a \in \mathbb{Q}_p \text{ où } \|a\|_p \leq 1, \ \exists (a_n) \in \mathbb{Z}, \text{ telle que } a_n = \alpha_0 + \alpha_1 p + ... + \alpha_n p^n$$

Et

$$a = \lim_{n \longrightarrow \infty} a_n = \sum_{n=0}^{\infty} \alpha_n p^n = \alpha_0 \alpha_1 .... \tag{1.20}$$

Les α_j représentent les chiffres p-adiques et $\sum_{n=0}^{\infty} \alpha_n p^n$ s'appelle la série (ou développement $p-adique$) de Hensel de a.

Remarque 1.2.19 1) *Si $\beta_{-m} \neq 0$; alors $\|a\|_p = p^m$.*

2) *On note par* $[x]$ *la partie entière d'un nombre p-adique* $x \in \mathbb{Q}_p$, *telle que*

$$\forall x \in \mathbb{Q}_p : [x] = \sum_{k=0}^{\infty} \beta_k p^k = \beta_0 \beta_1 ....$$

Et on note par $\langle x \rangle$ *la partie fractionnaire de* x, *telle que*

$$\forall x \in \mathbb{Q}_p : \langle x \rangle = \sum_{k \prec 0} \beta_k p^k = ... \beta_{-2} \beta_{-1}$$

On obtient, alors

$$\forall x \in \mathbb{Q}_p : x = [x] + \langle x \rangle \tag{1.21}$$

1.2.6 Développement de Hensel des nombres rationnels

Définition 1.2.20 *Le développement p-adique de* $x = \sum_{n=-m}^{\infty} \alpha_n p^n$ *représente un nombre rationnel si et seulement si la suite* $(\alpha_n)_{n \geq 0}$ *est périodique à partir d'un certain rang .*

Exemple 1.2.21 *Soit* $x = \frac{1}{3} \in \mathbb{Q}_5$. *Alors*

$$\frac{1}{3} = 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5$$

C'est-à-dire

$$\frac{1}{3} = 231313131 = \overline{231}$$

Le développement $5-adique$ *de* $\frac{1}{3}$ *est périodique. Ce qui signifie que* $\frac{1}{3} \in \mathbb{Q}$.

Définition 1.2.22 *On dit que a est un entier p-adique si son développement p-adique ne contient que des puissances positives de p . Autrement dit*

$$a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_n p^n +$$

Notation 1.2.23 *On note par* $\mathbb{Z}_p$ *l'ensemble des entiers p-adiques .*

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : a = \sum_{n=0}^{\infty} \alpha_n p^n \right\} \tag{1.22}$$

Puisque dans le cas d'un entier p-adique a, $V_p(x)$ *est positive . On a la caractérisation suivante*

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : \|a\|_p = p^{-V_p(x)} \leq 1 \right\}$$

C'est-à-dire : $\mathbb{Z}_p$ *représente le disque d'unité de rayon* 1 *et de centre* 0 *.*

Remarque 1.2.24 1) *Tout nombre p-adique* $a \in \mathbb{Q}_p$ *est une limite d'une suite de cauchy de nombres rationnels .*
2) *Le corps* $\mathbb{Q}_p$ *est l'ensemble des fractions de* $\mathbb{Z}_p$ *. ie :*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \text{ ; } (a,b) \in \mathbb{Z}_p.\mathbb{Z}_p^* \right\}$$

1.2.7 Unités p-adiques

Définition 1.2.25 ***(unité p-adique)*** *Soit* $a = \sum_{n=0}^{\infty} \alpha_n p^n$ *un entier* $p-$*adique.*
On dit que a est une unité dans $\mathbb{Z}_p$*, si et seulement si* $\alpha_0 \neq 0$
Soit U_p *l'ensemble des unités* $p-$*adiques, alors*

$$\begin{aligned} U_p &= \left\{ \sum_{n=0}^{\infty} \alpha_n p^n, \ \alpha_0 \neq 0 \right\} \\ &= \{a \in \mathbb{Z}_p, \ \alpha_0 \neq 0\} = \mathbb{Z}_p^* \end{aligned}$$

Théorème 1.2.26

$$U_p = \left\{ a \in \mathbb{Z}_p, tel \text{ } que \ \|a\|_p = 1 \right\} \tag{1.23}$$

Preuve. Nous avons

$$\begin{aligned} a &\in U_p \Longrightarrow a_0 \neq 0 \\ &\Leftrightarrow V_p(\alpha) = 0 \\ &\Leftrightarrow \|a\|_p = p^{-0} = 1 \end{aligned}$$

■

Proposition 1.2.27 *Soit* $\alpha \in \mathbb{Q}_p$ *tel que* $\|\alpha\|_p = p^{-n}$*, alors* α *admet une représentation unique définie par*

$$\alpha = p^n u, \ n \in \mathbb{Z} \text{ et } u \in U_p \tag{1.24}$$

Preuve.
1) **Existense** :
Soit $\alpha \in \mathbb{Q}_p$, alors

$$\alpha = \frac{a}{b}; (a,b) \in \mathbb{Z}_p \ .\mathbb{Z}_p^*$$

Par définition

$$\left\{\begin{array}{l} a = u_1 p^{m_1}\ ;\ u_1 \in U_p \\ b = u_2 p^{m_2}\ ;\ u_2 \in U_p \end{array}\right.$$

$$\begin{aligned} \Longrightarrow \quad & \alpha = \frac{a}{b} = \frac{u_1}{u_2} p^{m_1 - m_2} \\ \Rightarrow \quad & \alpha = u p^n \text{ où } u = \frac{u_1}{u_2} \text{ et } n = m_1 - m_2 \end{aligned}$$

Reste à montrer que $u \in U_p$

En effet

$$\begin{aligned} u_2 \in U_p \Rightarrow \frac{1}{u_2} \in U_p \\ \Rightarrow u = \frac{u_1}{u_2} \in U_p \end{aligned}$$

2) **Unicité** :

Supposons que α admet deux représentations

$$\left\{\begin{array}{l} \alpha = u_1 p^{m}\ ;\ u_1 \in U_p,\ m \in \mathbb{Z} \\ \alpha = u_2 p^{m'}\ ;\ u_2 \in U_p,\ m' \in \mathbb{Z} \end{array}\right.$$

Alors

$$\frac{u_1}{u_2} = p^{m' - m}$$

Comme $\frac{u_1}{u_2} \in U_p$; on en déduit que

$$\begin{aligned} V_p\left(\frac{u_1}{u_2}\right) &= 0 \\ &\Longrightarrow u_1 = u_2 \\ &\Rightarrow m = m' \end{aligned}$$

D'où l'unicité de la représentation. ∎

Lemme 1.2.28 *Soient $x \in \mathbb{Q}_p$ et $k \in \mathbb{Z}$. Alors*

$$\left\{ y \in \mathbb{Q}_p \textit{ tel que } \|y - x\|_p \leq p^k \right\} = x + p^{-k}\mathbb{Z}_p \subset \mathbb{Q}_p$$

Preuve. On a

$$\begin{aligned} x + p^{-k}\mathbb{Z}_p &= \{x + p^{-k}a, \text{ où } a \in \mathbb{Z}_p\} \\ &= \left\{x + \mu, \text{ tel que } \|\mu\|_p \leq p^k\right\} \\ &= \left\{y \in \mathbb{Q}_p \text{ tel que } \|y - x\|_p \leq p^k\right\} \end{aligned}$$

Comme $x \in \mathbb{Q}_p$, et $p^{-k}\mathbb{Z}_p \subset \mathbb{Q}_p$, alors

$$x + p^{-k}\mathbb{Z}_p \subset \mathbb{Q}_p$$

■

Chapitre 2

Propriétés du corps de nombres p-adiques

Dans cette partie, on étudie seulement les propriétés élémentaires des nombres $p-adiques$.

2.1 propriétés analytiques

En général, les propriétés analytiques de $\mathbb{Q}_p$ sont analogues à celles de $\mathbb{R}$. Mais la différence est remarquable entre ses deux corps , notamment dans les critères de convergence des suites et des séries de puissances.

Théorème 2.1.1 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite de $\mathbb{Q}_p$, alors $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy convergente si et seulement si*

$$\lim_{n\longrightarrow\infty} \|a_{n+1} - a_n\|_p = 0 \tag{2.1}$$

Preuve. Supposons à présent que $\lim\limits_{n\longrightarrow\infty} \|a_{n+1} - a_n\|_p = 0$.
Alors

$$\forall\varepsilon \succ 0, \exists N \in \mathbb{N}\,; \forall n \geq N : \|a_{n+1} - a_n\|_p \prec \varepsilon$$

En tenant compte maintenant des inégalités

$$\|a_m - a_n\|_p = \|a_m - a_{m-1} + a_{m-1} - a_{m-2} + a_{m-2} - \ \ldots\ldots - a_n\|_p$$

$$\leq \max\left\{\|a_m - a_{m-1}\|_p, \|a_{m-1} - a_{m-2}\|_p, \ldots., \|a_{n+1} - a_n\|_p\right\} \prec \varepsilon$$

On déduit que (a_n) est une suite de Cauchy . ■

Remarque 2.1.2 *En générale, la dernière propriété n'est pas vérifiée dans* $\mathbb{R}$ *.*
C'est-a-dire

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

n'implique pas que $(a_n)_{n\in\mathbb{N}}$ *est une suite de Cauchy.*

Proposition 2.1.3 *Si la série* $\sum_{i=0}^{\infty} \|a_i\|_p$ *converge dans* $\mathbb{R}$*, alors* $\sum_{i=0}^{\infty} a_i$ *converge dans* $\mathbb{Q}_p$ *.*

Preuve. Puisque $\sum_{i=0}^{\infty} \|a_i\|_p$converge, alors la suite des sommes partielles

$$\left(S_n = \sum_{i=0}^{n} \|a_i\|_p\right)_{n\in\mathbb{N}}$$

est de Cauchy.
ie :

$$\forall\varepsilon \succ 0,\ \exists N \in \mathbb{N}\ ;\ \forall m \succ n \geq N :\ \sum_{i=n+1}^{m} \|a_i\|_p < \varepsilon$$

Soit $\left(\overline{S}_n = \sum_{i=0}^{n} \|a_i\|_p\right)_{n\in\mathbb{N}}$ la suite des sommes partielles de la série $\sum_{i=0}^{\infty} a_i$. Alors

$$\begin{aligned} \left\|\overline{S}_m - \overline{S}_n\right\|_p &= \left\|\sum_{i=n+1}^{m} a_i\right\|_p \\ &\leq \sum_{i=n+1}^{m} \|a_i\|_p < \varepsilon \end{aligned}$$

Ce qui implique que $\left(\overline{S_n} = \sum_{i=0}^{n} a_i\right)_{n\in\mathbb{N}}$ est une suite de Cauchy.
Par suite $\sum_{i=0}^{\infty} a_i$ converge dans $\mathbb{Q}_p$. ■

Proposition 2.1.4 *Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite de* $\mathbb{Q}_p$ *.*
Si $\lim_{n\longrightarrow\infty} a_n = a$ *dans* $\mathbb{Q}_p$*, alors*

$$\exists\ N \in \mathbb{N}\ ,\ \forall n \geq N\ :\ \|a_n\|_p = \|a\|_p \tag{2.2}$$

Preuve. Supposons que $(a_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{Q}_p$, telle que

$$\lim_{n\longrightarrow\infty} a_n = a$$

$(a_n)_{n\in\mathbb{N}}$ est convergente dans $\mathbb{Q}_p$; et donc elle est de Cauchy .
C'est-à-dire

$$\forall\varepsilon \succ 0\ ,\ \exists n_0 \in \mathbb{N}\ ;\ \forall m \succ n \geq n_0 \Rightarrow \|a_m - a_n\|_p < \varepsilon$$

D'autre part

$$\left| \|a_m\|_p - \|a_n\|_p \right| \leq \|a_m - a_n\|_p < \varepsilon$$

Alors $\left(\|a_n\|_p\right)_n$ est une suite de Cauchy dans $\mathbb{R}$, donc elle est convergente.
Posons

$$\lim_{n\longrightarrow\infty} \|a_n\|_p = l = \|a\|_p$$

Si $\|a\|_p \neq 0 \implies \|a\|_p > 0$.
Alors, pour $\varepsilon = \frac{l}{2} > 0$, il vient

$$\exists n_1 \in \mathbb{N},\ \forall n \geq n_1 :\ \left| \|a_n\|_p - l \right| < \frac{l}{2}$$

Ce qui implique

$$\|a_n\|_p > \frac{l}{2}$$

De même, puisque $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{Q}_p$, alors, pour $\varepsilon = \frac{l}{2}$

$$\exists n_2 \in \mathbb{N} \text{ tel que } \forall m \succ n \geq n_2 \implies \|a_m - a_n\|_p < \frac{l}{2}$$

Donc, si $n \succ n_3 = \max\{n_1, n_2\}$, on a

$$\begin{aligned} \|a_m\|_p &= \|a_m - a_n + a_n\|_p \\ &= \max\left\{ \|a_m - a_n\|_p , \|a_n\|_p \right\},\ (\text{car } \ \|\| \ \text{ est ultra-métrique et } \ \|a_m - a_n\|_p \neq \|a_n\|_p \\ &= \|a_n\|_p \end{aligned}$$

Faisons m tends vers $+\infty$, on aura

$$\|a_n\|_p = \|a\|_p\ \ ,\ \forall n > n_3$$

■

Proposition 2.1.5 *Soit* $\sum\limits_{n=0}^{\infty} a_n$ *une série dans* $\mathbb{Q}_p$ *; alors*

$$\sum_{n=0}^{\infty} a_n \text{ converge dans } \mathbb{Q}_p \iff \lim_{n\longrightarrow\infty} a_n = 0 \tag{2.3}$$

De plus

$$\left\| \sum_{n=0}^{\infty} a_n \right\|_p \leq \max_{n \geq 0} \left\{ \|a_n\|_p \right\} \tag{2.4}$$

Preuve.

1) *On sait que la série* $\sum_{n=0}^{\infty} a_n$ *converge si la suite des sommes partielles* $\left(S_n = \sum_{i=0}^{n} a_i \right)_{n \in \mathbb{N}}$ *est convergente .*

Et comme

$$S_n - S_{n-1} = a_n$$

Alors, d'après le théorème (**??**), *la série* $\sum_{n=0}^{\infty} a_n$ *converge si et seulement si* a_n *tend vers* 0*, quand* n *tend vers* $+\infty$

2) *Supposons que* $\sum_{n=0}^{\infty} a_n$ *converge . Puisque* a_n *tend vers* 0*, alors*

$$\exists N \in \mathbb{N} : \left\| \sum_{n=0}^{\infty} a_n \right\|_p = \left\| \sum_{n=0}^{N} a_n \right\|_p$$

De plus

$$\max \left\{ \|a_n\|_p \, , \, 0 \leq n \leq N \right\} = \max_{n \geq 0} \left\{ \|a_n\|_p \right\}$$

D'où

$$\left\| \sum_{n=0}^{N} a_n \right\|_p \leq \max \left\{ \|a_n\|_p \, , \, 0 \leq n \leq N \right\} = \max_{n \geq 0} \left\{ \|a_n\|_p \right\}$$

■

Théorème 2.1.6 *(Théorème de permutation)*

Soit $b_{i,j} \in \mathbb{Q}_p$*,* $i, j = 1, 2, ...$*vérifie le critère de convergence suivant*

$$\forall \varepsilon > 0, \ \exists n_0 = n_0(\varepsilon), \ \textit{tel que} \ \max(\ i, \ j \ ) \geq n_0 \Rightarrow ||b_{i,j}||_p < \varepsilon \tag{2.5}$$

Alors, les deux séries $\sum_i \left(\sum_j b_{i,j} \right)$ *et* $\sum_j \left(\sum_i b_{i,j} \right)$ *sont convergentes.*

De plus

$$\sum_i \left(\sum_j b_{i,j} \right) = \sum_j \left(\sum_i b_{i,j} \right) \tag{2.6}$$

Preuve. En effet. Nous avons

$$\sum_j b_{i,j} \leq \max_j ||b_{i,j}||_p < \varepsilon, \text{ pour tout } j \ \geq n_0$$

De même

$$\sum_i b_{i,j} \leq \max_i ||b_{i,j}||_p < \varepsilon, \text{ pour tout } i \geq n_0$$

D'aprés la proposition (2.1.15), les deux séries $\sum\limits_i \left(\sum\limits_j b_{i,j} \right)$ et $\sum\limits_j \left(\sum\limits_i b_{i,j} \right)$ sont convergentes.

D'autre part

$$\begin{aligned}
\left| \sum_{i=1}^{+\infty} \left(\sum_{j=1}^{+\infty} b_{i,j} \right) - \sum_{i=1}^{N} \left(\sum_{j=1}^{N} b_{i,j} \right) \right| &= \left| \sum_{i=1}^{N} \left(\sum_{j=N+1}^{+\infty} b_{i,j} \right) + \sum_{i=N+1}^{+\infty} \left(\sum_{j=1}^{+\infty} b_{i,j} \right) \right| \\
&\leq \max_{\max(\ i,\ j\ ) \geq N} ||b_{i,j}||_p \leq \max_{\max(\ i,\ j\ ) \geq n_0} ||b_{i,j}||_p < \varepsilon
\end{aligned}$$

Ce qui implique que

$$\sum_{i=1}^{+\infty} \left(\sum_{j=1}^{+\infty} b_{i,j} \right) \overset{N \to +\infty}{\to} \sum_{i=1}^{N} \left(\sum_{j=1}^{N} b_{i,j} \right)$$

Et comme

$$\sum_{i=1}^{N} \left(\sum_{j=1}^{N} b_{i,j} \right) = \sum_{j=1}^{N} \left(\sum_{i=1}^{N} b_{i,j} \right)$$

On déduit que

$$\sum_i \left(\sum_j b_{i,j} \right) = \sum_j \left(\sum_i b_{i,j} \right)$$

■

Théorème 2.1.7 *(théorème de Strassman* [5] *Soit*

$$F(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p [x] \tag{2.7}$$

une série de puissances non nulle.

Si $\lim\limits_{n \longrightarrow +\infty} a_n = 0$*, alors* $F(x)$ *converge pour tout* x *de* $\mathbb{Z}_p$*.*

De plus, s'il existe un entier positif N*, tel que*

$$\begin{cases} i\ )\ \|a_N\|_p = \max\limits_{n \geq 0} \left\{ \|a_n\|_p \right\} \\ ii\ )\ \|a_n\|_p < \|a_N\|_p, \text{pour } n > N \end{cases} \tag{2.8}$$

Alors $F : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ *admet au maximum* N *zéros.*

Preuve. Par récurrence .
Si $N=0$, notre hypothèse signifie que $\|a_0\|_p > \|a_n\|_p$, $\forall n>0$.
On va montrer que dans ce cas $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$.
Supposons le contraire. C'est-à-dire

$$F(x) = a_0 + a_1 x + ... + ... = 0$$

On en déduit que

$$\begin{aligned} \|a_0\|_p &= \left\|a_1 x + a_2 x^2 + \ ...+ \ ....\right\|_p \\ &\leq \max_{n\geq 1}\left\{\|a_n\|_p\right\} \end{aligned}$$

$$< \|a_0\|_p$$

Qui est une contradiction.
Donc $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$.
Supposons maintenant qu'il existe $N>0$ et que les deux hypothèses du théorème sont satisfaites.
Cest-à-dire

$$\|a_N\|_p = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

et que

$$\|a_n\|_p < \|a_N\|_p \text{, pour tout } n > N$$

Montrons que $F(x)$ admet au maximum N zéros dans $\mathbb{Z}_p$.
Soit $\alpha \in \mathbb{Z}_p$, tel que $F(\alpha)=0$, alors

$$\begin{aligned} \forall x &\in \mathbb{Z}_p : F(x) = F(x) - F(\alpha) \\ &= \sum_{n=0}^{\infty} a_n (x^n - \alpha^n) \end{aligned}$$

$$\begin{aligned} &= (x-\alpha)\sum_{n\geq 1}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j} \\ &= (x-\alpha)\sum_{j=0}^{\infty} b_j x^j, \text{ où } b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k \\ &= (x-\alpha)\, g(x) \text{ , où } g(x) = \sum_{j=0}^{\infty} b_j x^j, \end{aligned}$$

Nous avons

$$\|b_j\|_p \leq \max\left\{\|a_{j+1+k}\|_p\right\} \leq \|a_N\|_p \text{ ; } \forall j = o, ...$$

En particulier

$$\begin{aligned}\|b_{N-1}\|_p &= \left\|a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \ \ldots + \ \ldots\right\|_p \\ &= \|a_N\|_p = \max_j \|b_j\|_p\end{aligned}$$

Et si $j \succ N-1$, on a

$$\begin{aligned}\|b_j\|_p &\leq \max_{k\geq 0}\left\{\|a_{j+1+k}\|_p\right\} \leq \max_{i\geq N+1}\left\{\|a_i\|_p\right\} \\ &\prec \|a_N\|_p = \|b_{N-1}\|_p\end{aligned}$$

Par l'hypothèse de récurrence, on déduit que $g(x)$ admet au maximum $N-1$ zéros.
Par suite, g admet au maximum N zéros. ■

2.2 Propriétés topologiques

On défini la topologie $p - adique$ par la famille des boules

$$\begin{aligned}V_n(a) &= \left\{x \in \mathbb{Q}_p \text{ tel que } \|x-a\|_p \leq p^{-n}, \text{ pour tout } a \in \mathbb{Q}_p\right\} \\ &= \{x \in \mathbb{Q}_p \text{ tel que } v_p(x-a) \geq n\}\end{aligned}$$

Proposition 2.2.1 *Toute boule de l'espace ultra-métrique* $\left(\mathbb{Q}_p,\ \|.\|_p\right)$ *est à la fois ouverte et fermée.*

Preuve. 1) Soit $B(a,r)$ une boule ouverte de $\mathbb{Q}_p$ de centre a et de rrayon r. Alors, par définition, il existe $n \in \mathbb{Z}$, tel que

$$p^n < r \leq p^{n+1}$$

Soit $x \in B(a,r)$, alors

$$\|x-a\|_p < r \leq p^{n+1}$$

D'où

$$x \in B(a, p^{n+1})$$

Ce qui implique que

$$B(a,r) \subset B(a, p^{n+1})$$

Supposons maintenant que $x \in \overline{B}(a, p^n)$, alors

$$\|x - a\|_p \leq p^n < r$$

D'où

$$x \in B(a, r)$$

Donc

$$\overline{B}(a, p^n) \subset B(a, r) \subset B(a, p^{n+1})$$

Supposons encore que $x \in B(a, p^{n+1})$, alors

$$\begin{array}{rcl} \|x - a\|_p & < & p^{n+1} \\ & \Rightarrow & v_p(x - a) > -(n + 1) \\ v_p(x - a) & \geq & -n \\ & \Rightarrow & \|x - a\|_p \leq p^n \end{array}$$

D'où

$$x \in B(a, p^n)$$

Alors

$$\overline{B}(a, p^n) \subset B(a, r) \subset B(a, p^{n+1}) \subset B(a, p^n)$$

Ce qui implique

$$B(a, r) = B(a, p^{n+1}) = B(a, p^n)$$

Donc, $B(a, r)$ est à la fois ouverte et fermée.
2) Pour une boule fermée $\overline{B}(a, r)$, on prend

$$p^n \leq r < p^{n+1}$$

et de même on montre que

$$\overline{B}(a, r) = \overline{B}(a, p^n) = B(a, p^{n+1})$$

■

Proposition 2.2.2 *Tous point d'une boulle en est le centre. C'est-à-dire*

$$x \in B(a, r) \Rightarrow B(a, r) = B(x, r)$$

Preuve. En effet. Soit

$$y \in B(a,r) \Rightarrow \|x-a\|_p < r$$

Nous avons

$$\begin{aligned} \|x-y\|_p &\leq \max\ (\ \|a-y\|_p\,,\ \ \|a-x\|_p) < r \\ &\Rightarrow y \in B(x,r) \end{aligned}$$

D'où

$$B(a,r) \subset B(x,r)$$

De même

$$B(x,r) \subset B(a,r)$$

Par suite

$$B(a,r) = B(x,r)$$

■

Proposition 2.2.3 *Si deux boules de l'espace ultra-métrique* $\left(\mathbb{Q}_p,\ \ \|.\|_p\right)$ *se rencontrent, alors l'une d'elles est forcément contenue dans l'autre.*

Preuve. Soient $B(x_1,r_1)$ et $B(x_2,r_2)$ deux boules de $\mathbb{Q}_p$, tels que $r_1 < r_2$.
Et soit

$$x \in B(x_1,r_1) \cap B(x_2,r_2)$$

Alors, d'aprés la proposition précédente, on a

$$B(x,r_1) = B(x_1,r_1)$$

et

$$B(x,r_2) = B(x_2,r_2)$$

Comme $r_1 \prec r_2$, on troiuve

$$B(x,r_1) \subset B(x,r_2)$$

Par suite

$$B(x_1,r_1) \subset B(x_2,r_2)$$

■

Proposition 2.2.4 *Tous les triangles de l'espace ultra-métrique* $\left(\mathbb{Q}_p,\ \ \|.\|_p\right)$ *sont isoceles.*

Preuve. *En effet. Soient x, y et $z \in \mathbb{Q}_p$, tels que*

$$\|x-z\|_p \neq \|y-z\|_p$$

Supposons par exemple que

$$\|x-z\|_p < \|y-z\|_p$$

Alors

$$\|x-y\|_p \leq \max\ (\ \|x-z\|_p\,,\ \ \|y-z\|_p) = \|y-z\|_p$$

D'autre part

$$\|z-y\|_p \leq \max\ (\ \|z-x\|_p\,,\ \ \|x-y\|_p) = \|x-y\|_p$$

■

2.3 Propriétés algébriques

Définition 2.3.1 *On dit que le corps $\Bbbk$ est algébriquement clos, si chaque polynôme $p(x) \in \Bbbk[x]$, admet des racines dans $\Bbbk$. Autrement dit chacun de ces polynômes se divise en facteur linéaire dans $\Bbbk[x]$.*

Proposition 2.3.2 *Le corps $\mathbb{Q}_p$ n'est pas algébriquement clos pour tout p premier*

Preuve. On considère le polynôme

$$p(x) = x_2 - p \in \mathbb{Q}_p[x]$$

Supposons que $p(x)$ admet des racines dans $\mathbb{Q}_p$
Alors

$$\begin{aligned} \left\|x^2\right\|_p &= \|x\|_p^2 \\ &= \|p\|_p = p^{-1} \end{aligned}$$

Ce qui implique

$$\begin{aligned} \|x\|_p &= p^{\frac{-1}{2}} \\ &\Rightarrow\ v_p(x) = \frac{1}{2}, \end{aligned}$$

Qui est contredit le fait que $v_p(x) \in \mathbb{Z}$.
Donc $p(x)$ n'a pas des racines dans $\mathbb{Q}_p$. ■

Proposition 2.3.3 *Tout nombre p-adique non nul, est inversible dans* $\mathbb{Q}_p$.

Preuve. Soit $x \in \mathbb{Q}_p^*$.tel que $x = p^n \mu$; $n \in \mathbb{Z}$ et $\mu \in U_p$
Alors

$$\mu \in U_p \Rightarrow \mu = \sum_{n=0}^{\infty} \alpha_n p^n \text{ ; } \alpha_0 \neq 0$$

$$\begin{aligned} \Longrightarrow \quad & \mu = \alpha_0 + p\sum_{n=1}^{\infty} \alpha_n p^{n-1} = \alpha_0 + p\sum_{n=0}^{\infty} \alpha_{n+1} p^n \\ \Longrightarrow \quad & \mu = \alpha_0 - py \text{ où } y = -\sum_{n=0}^{\infty} \alpha_{n+1} p^n \in \mathbb{Z}_p \end{aligned}$$

Comme $\alpha_0 \neq 0$; alors, on peut prendre $\alpha_0 = 1$
Donc

$$\begin{aligned} \mu &= 1 - py \Rightarrow \mu^{-1} = (1 - py)^{-1} \\ &= 1 + py + p^2 y^2 + \; \ldots\ldots \in U_p \end{aligned}$$

D'où

$$\begin{aligned} x^{-1} &= p^{-n} u^{-1} \text{tel que } n \in \mathbb{Z} \text{ et } u^{-1} \in U_p \\ &\Longrightarrow x^{-1} \in \mathbb{Q}_p^* \end{aligned}$$

■

Conclusion 2.3.4 *Le corps $\mathbb{Q}_p$ muni de la topologie induite par l'extension de la valeur absolue p-adique est donc de corps ultramétriques.*
Toutes les propriétés qui se transmettent de $\mathbb{Q}_p$ au corps $\mathbb{k}$ sont une raison suffisante pour dire des corps $\mathbb{k}$ qu'ils sont des corps de nombres p-adiques. Contrairement à $\mathbb{R}$, les corps $\mathbb{Q}_p$ admettent une infinité d'extensions finies (donc algébriques). Autrementp dit, les extensions finies de $\mathbb{Q}_p$ ne sont pas algébriquement closes.
Il est possible de montrer que la totalité des corps complets localement compact non-discrets sont donnés ('a isomorphisme prés) par les extensions finies des corps : $\mathbb{Q}_2, \mathbb{Q}_3, .., \mathbb{Q}_{+\infty} = \mathbb{R}$.

Bibliographie

[1] Z. I . Borevitch et I .R . Chafarevitch, Théorie des nombres, Gauthier-Villars, Paris. 1967.

[2] A. M. Robert, A Course in p-adic s Program, Fall 2000(2001).Analysis, Springer-Verlag Berlin Heidelbery New York, 2000.)

[3] Y. Amice, Les nombres p-adiques .Colledtion sup, no 14, Les presses universitaires de France, Paris

1975.

[4] S. Katok, real and p-adic analysis, course notes for Math 497C, Mass Program, Fall 2000(2001) .

[5] R. Strassman, Uber den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen, J. furbMath. 159 (1928), 13-2