الجمهورية الجزائرية الديموقراطية 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. ***/***

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

Licence Académique

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

Thème

Les opérations arithmétiques dans le corps Qp

Présenté par :
1- Daas nawal
2- Kerrouche saliha

Dirigé par :
Kecies Mohamed

Année universitaire 2011-2012

*** Remerciements ***

Nous tenons à remercier en premier et avant tout, notre créateur <<ALLAH>>, qui nous aide à réaliser ce travail.

Nos sincères gratitudes et remerciements à notre encadreur Mohamed Kecies pour le grand soutient moral et leur aides précieuses qui nous apportez durant tout ce travail.

Nousadressons, également, mes remerciements chaleureux aux membres de l'institut des sciences et de la technologie et à tous ceux qui ont pris part de près ou de loin, à la réalisation de ce travail.

Nawal et Saliha

Table des matières

Introduction Générale

Les notions des nombres p-adiques et de l'analyse p-adique sont apparues pour la première fois, au début du vingtième siècle grâce au mathématicien K.Hensel considère comme l'inventeur des nombres p-adiques.

Pour tout p un nombre premier, le corps $\mathbb{Q}_p$ des nombres p-adiques est obtenu suite à la complétion du corps des rationnels $\mathbb{Q}$ par rapport à une certaine norme spécifique appelée norme p-adique qui est non-archimédienne, comme elle induit une distance ultramétrique appelée distance p-adique.

Parmi les propriétés spécifiques de l'analyse p-adique, on peut citer par exemple le fait qu'une série converge si et seulement si son terme général tend vers zéro.

L'utilisation des nombres p-adiques est fréquente en théorie des nombres et en Géométrie. D'autre part, depuis quelques années plusieurs auteurs en Physique Mathématique prennent comme corps de base, au lieu des corps des nombres réels et complexes, les corps p-adiques.

Ce mémoire est réparti sur l'introduction générale, et trois chapitres.

Dans le premier chapitre, on a commencé par donner quelques rappels des notions fondamentales du corps normés ultramétriques muni d'une norme non Archimédienne. En suite, on a appliqué ces notions et la procédure de complétion pour construire les corps complets.

Dans le deuxième chapitre, on a construit pour chaque p premier de "nouveaux nombres" selon le procédé de complétion par rapport à la norme p-adique, appelés nombres p-adiques noté $\mathbb{Q}_p$ qui étend le corps des nombres rationnels $\mathbb{Q}$. Nous avons présenté aussi la valuation p-adique, la norme p-adique et le corps des entiers p-adiques $\mathbb{Z}_p$.

Enfin, dans le dernier chapitre, On a exposé les règles des opérations arithmétiques, dont l'addition et la recherche d'opposés, ainsi que les règles de multiplication et de recherche des inverses, en utilisant les codes de Hensel.

Chapitre 1

Corps valués ultramétriques complets

Le but de ce chapitre est de présenter la construction des corps normés complets. On va donner des notions fondamentales sur les corps normés ultramètriques et la procédure de complétion pour construire les corps normés complet.

1.1 Corps normés

Définition 1.1.1 *Soit K un corps.*
1) On appelle une norme sur K toute application $\|.\|$ de K dans $\mathbb{R}^+$ telles que :
i) $\forall x \in K : \|x\| = 0 \Longleftrightarrow x = 0$.
ii) $\forall x, y \in K : \|x \cdot y\| = \|x\| \cdot \|y\|$.
iii) $\forall x, y \in K : \|x + y\| \leq \|x\| + \|y\|$ *(l'inégalité triangulaire).*
2) On dit que la norme $\|.\|$ est ultramétrique ou non archimédienne si

$$\forall x, y \in K : \|x + y\| \leq \max(\|x\|, \|y\|) \textit{(Inégalité triangulaire forte)}$$

c'est à dire une norme qui vérifie une condition plus forte que l'inégalité triangulaire.
3) Une norme constante $\|.\|$ est dite triviale si est seulement si

$$\|x\| = \begin{cases} 1, si\ x \neq 0 \\ 0, si\ x = 0 \end{cases}$$

Remarque 1.1.2
1) On dit parfois valeur absolue au lieu de norme de corps.
2) La norme est une extension de la valeur absolue des nombres aux vecteurs.

3) La norme $\|.\|$ est un morphisme de groupes entre les groupes multiplicatifs $(K^*,.)$ et $(\mathbb{R}_+^*,.)$ et donc que $\|1\| = 1$.

Exemple 1.1.3 *La valeur absolue usuelle $|.|$ est une norme archimédienne sur $\mathbb{R}$. Car*

$$|(-1) - 4| = 5 > \max(|(-1)|, |4|) = 4$$

Définition 1.1.4
1) On appelle corps valué, tout couple de la forme $(K, \|.\|)$ ou K est un corps et $\|.\|$ est une norme sur K.
2) On appelle la distance induite sur K par $\|.\|$, la distance $d_{\|.\|}$ sur K définie par

$$\forall x, y \in K : d_{\|.\|}(x, y) = \|x - y\|$$

3) Si $\|.\|$ est une norme ultramétrique, alors

$$\forall x, y, z \in K : d_{\|.\|}(x, z) \leq \max(d_{\|.\|}(x, y), d_{\|.\|}(y, z))$$

et la distance induite par cette norme appelée distance ultramétrique.
4) Lorsque K muni de la distance ultramétrique, on dit que K est un corps valué ultramétrique. Dans le cas contraire, on dit que K est un corps valué archimédien.

Proposition 1.1.5 *K est un corps ultramétrique si et seulement si*

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

Autrement dit $\mathbb{N}$ est borné selon $\|.\|$.

Preuve. Supposons que K 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 que$\|i\| \leq 1$ pour tout $i \leq n$ et montrons que $\|n + 1\| \leq 1$.
On a

$$\begin{aligned} \|n + 1\| &\leq \max\{\|n\|, \|1\|\} = 1 \\ &\Rightarrow \|n + 1\| \leq 1 \end{aligned}$$

Pour l'implication réciproque. On suppose que $\forall n \in \mathbb{N} : \|n\| \leq 1$.
Soient $x, y \in K$, alors

$$\|(x+y)^n\| = \left\| \sum_{k=0}^{n} C_n^k \cdot x^k \cdot y^{n-k} \right\| \leq \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \left\|x^k\right\| \cdot \left\|y^{n-k}\right\|$$

$$\leq \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \|x\|^k \cdot \|y\|^{n-k} \ , \text{ avec } \left\|C_n^k\right\| \leq 1$$

$$\Longrightarrow \|(x+y)^n\| \leq \sum_{k=0}^{n} \|x\|^k \cdot \|y\|^{n-k}$$

On sait que $\|x\| \leq \max(\|x\|, \|y\|), \|y\| \leq \max(\|x\|, \|y\|)$. Par conséquent

$$\forall K = \overline{0,n} \ : \begin{cases} \|x\|^k \leq [\max(\|x\|, \|y\|)]^k \\ \|y\|^{n-k} \leq [\max(\|x\|, \|y\|)]^{n-k} \end{cases}$$

On obtient

$$\|x\|^k . \|y\|^{n-k} \leq [\max(\|x\|, \|y\|)]^k . [\max(\|x\|, \|y\|)]^{n-k} = [\max(\|x\|, \|y\|)]^n , \forall K = \overline{0,n}$$

Ce qui donne

$$\begin{aligned} \|(x+y)^n\| &\leq \sum_{k=0}^{n} [\max(\|x\|, \|y\|)]^n \\ &\leq (n+1) . [\max(\|x\|, \|y\|)]^n \end{aligned}$$

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

On sait que $\lim_{n\to\infty} (n+1)^{\frac{1}{n}} = 1$, alors $\|x+y\| \leq \max(\|x\|, \|y\|)$. Par conséquent $\|.\|$ est une norme ultramétrique. ■

Proposition 1.1.6
Soit K un corps non-archimédien, $a, x \in K$, on a si $\|a-x\| < \|a\|$, alors $\|x\| = \|a\|$. Autrement dit, tous les triangles de $(K, \|.\|)$ sont isocèles.

Preuve.
Soient $x, a \in K$, alors

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

$$\Longrightarrow \|x\| \leq \|a\|$$

D'autre part, on a

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

Si $\|x - a\| > \|x\|$, alors $\|a\| \leq \|x - a\|$. Contradiction avec l'hypothèse.
Donc $\|x - a\| < \|x\|$, ce qui donne $\|a\| \leq \|x\|$ .On déduit que $\|a\| = \|x\|$. ■

Définition 1.1.7 *Soit $(x_n)_n \subset (K, \|.\|)$. Alors*
1) On dit que $(x_n)_n$est une suite de Cauchy si elle vérifie la propriété suivante, appelée critère de Cauchy

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n, m \geq n_0 : \|x_n - x_m\| \leq \varepsilon$$

Ceci est équivalent à $\underset{n,m \to +\infty}{Lim} \|x_n - x_m\| = 0$.
2) On dit que $(x_n)_n$ est une suite converge vers $x \in K$ si et seulement si

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : \|x_n - x\| \leq \varepsilon$$

3) On dit que $(x_n)_n$ est une suite bornée si et seulement si

$$\exists c > 0, \forall n \in \mathbb{N} : \|x_n\| \leq c$$

Remarque 1.1.8 *Dans un espace métrique :*
1) Toute suite converge est de Cauchy et la réciproque est fausse dans le cas général.
2) Toute suite de Cauchy est bornée.

1.2 Construction d'un corps normé complet

Définition 1.2.1 *Un espace métrique M est dit complet si toute suite de Cauchy de M a une limite dans M. C'est-à-dire qu'elle converge dans M. Autrement dit l'espace M n'a pas de trou ou n'a aucun point manquant.*

Exemple 1.2.2 *Les nombres rationnels ne forment pas un espace complet. Car si on considére la suite $(x_n)_n$ définie par*

$$x_0 = 1, x_1 = \frac{14}{10}, x_2 = \frac{141}{100}, ...$$

$(x_n)_n$ est une suite des nombres rationnels, de plus elle est de Cauchy dans $\mathbb{Q}$. Cependant, elle ne converge pas dans $\mathbb{Q}$, puisque elle a une limite $\sqrt{2}$ dans le corps complet $\mathbb{R}$.

Définition 1.2.3 ***(Définition générale de la complétion)***
Soit K un corps normé arbitraire (non complet) muni d'une norme $\|.\|_K$ et $\widehat{K}$ un autre

corps normé (construit à partir de K) muni d'une norme $\|.\|_{\widehat{K}}$ .On dit que $\widehat{K}$ est le complété de K si
1) $\widehat{K}$ contient K ($K \subset \widehat{K}$).
2) K est dense dans $\widehat{K}$ par rapport à la topologie associé avec $\|.\|_{\widehat{K}}$.
3) $\forall x \in K : \|x\|_K = \|x\|_{\widehat{K}}$ (la norme $\|.\|_{\widehat{K}}$ est définie à partir de $\|.\|_K$).
4) $(\widehat{K}, \|.\|_{\widehat{K}})$ est complet.

Si un espace métrique n'est pas complet, nous pouvons toujours le compléter en lui ajoutant les limites de toutes les suites de Cauchy modulo une relation d'équivalence. Dans le cas où le corps $\mathbb{Q}$ est muni de la norme euclidienne $|.|$, la procédure de complétion donne le corps $\mathbb{R}$. La construction d'un espace métrique complet est donnée selon les étapes suivantes :
1) **Etape 1 :** On note par

$$SC(K) = \left\{ A = \{a_n\}_n \in K^{\mathbb{N}} : \lim_{n,m \longrightarrow \infty} \|a_n - a_m\|_K = 0 \right\}$$

L'ensemble des suites de Cauchy défini dans $(K, \|.\|)$.
On définit sur $SC(K)$ les lois suivantes :

$$\text{Addition : } \begin{cases} + : & SC(K) \times SC(K) & \longrightarrow & SC(K) \\ & ((a_n)_n, (b_n)_n) & \longmapsto & (a_n + b_n)_n \end{cases}$$

$$\text{Multiplication : } \begin{cases} \cdot : & SC(K) \times SC(K) & \longrightarrow & SC(K) \\ & ((a_n)_n, (b_n)_n) & \longmapsto & (a_n \cdot b_n)_n \end{cases}$$

L'ensemble $(SC(K), +, \cdot)$ est un anneau unitaire, d'élément neutre $1_{SC(K)} = \{1\}_{n \in N} = \{1, 1, 1, ..., 1, ...\}$ (resp : $0_{SC(K)} = \{0\}_{n \in N} = \{0, 0, 0, ..., 0, ...\}$) par rapport à la multiplication (resp : à l'addition).

Pour cela, il suffit de vérifier que $SC(K)$ est un sous anneau de l'anneau produit K^N. En effet, si $A = \{a_n\}_n, B = \{b_n\}_n \in SC(K)$ et $n, m \in N$, alors

$$a_n \cdot b_n - a_m \cdot b_m = (a_n - a_m) \cdot b_n + a_m (b_n - b_m)$$

Ainsi

$$\begin{aligned} \|a_n \cdot b_n - a_m \cdot b_m\| &= \|(a_n - a_m) \cdot b_n + a_m (b_n - b_m)\| \\ &\leq \|(a_n - a_m) \cdot b_n\| + \|a_m (b_n - b_m)\| \\ &\leq \|b_n\| \cdot \|a_n - a_m\| + \|a_m\| \cdot \|b_n - b_m\| \\ &\leq \beta \|a_n - a_m\| + \alpha \|b_n - b_m\| \end{aligned}$$

Telles que $\alpha = \sup_n \|a_n\|, \beta = \sup_n \|b_n\|$, car $\{a_n\}_n$ et $\{b_n\}_n$ sont bornées. On déduit que

$$\lim_{n,m\to\infty} \|a_n \cdot b_n - a_m \cdot b_m\| = 0$$

$$\Longrightarrow A \cdot B \in SC(K)$$

D'autre part, on a

$$(a_n - b_n) - (a_m - b_m) = (a_n - a_m) + (b_m - b_n)$$

Ainsi

$$\|(a_n - b_n) - (a_m - b_m)\| = \|(a_n - a_m) + (b_m - b_n)\| \leq \|a_n - a_m\| + \|b_n - b_m\|$$

Comme $\{a_n\}_n$ et $\{b_n\}_n$ sont de Cauchy, alors $\lim_{n,m\longrightarrow\infty} \|(a_n - b_n) - (a_m - b_m)\| = 0$.
On déduit que $A - B \in SC(K)$.
De plus $SC(K)$ n'est pas un corps puisqu'il contient un diviseur de Zéro

$$\{1,0,0,0,...\} \cdot \{0,1,0,0,...\} = \{0,0,0,...,0,...\} = \{0\}_{n\in N^*}$$

2) **Etape 2 :** On définit l'ensemble des suites nulles de Cauchy

$$SN(K) = \left\{A = \{a_n\} \in SC(K) : \lim_{n\longrightarrow\infty} \|a_n\|_K = 0\right\}$$

3)**Etape 3 :** On définit sur $SC(K)$ une relation $\Re$ par

$$\forall \{a_n\}_n, \{b_n\}_n \in SC(K) : \{a_n\}_n \Re \{b_n\}_n \Longleftrightarrow \lim_{n\longrightarrow\infty} \|a_n - b_n\|_K = 0 \Longleftrightarrow \{a_n - b_n\} \in SN(K)$$

$\Re$ est une relation équivalence. En effet :
Soient $\{a_n\}_n, \{b_n\}_n, \{c_n\}_n \in SC(K)$. Alors

$$\lim_{n\longrightarrow\infty} \|a_n - a_n\|_K = 0 \Longrightarrow \{a_n\}_n \Re \{a_n\}_n \quad \text{(réflexivité)}$$

D'autre part

$$\{a_n\}_n \Re \{b_n\}_n \Longleftrightarrow \lim_{n\longrightarrow\infty} \|a_n - b_n\|_K = 0$$

$$\Longrightarrow \lim_{n\longrightarrow\infty} \|b_n - a_n\|_K = 0$$

$$\Longrightarrow \{b_n\}_n \Re \{a_n\}_n \quad \text{(symétrie)}$$

On a

$$\begin{cases} \{a_n\}_n \Re \{b_n\}_n \\ \{b_n\}_n \Re \{c_n\}_n \end{cases} \Longleftrightarrow \begin{cases} \lim\limits_{n\longrightarrow\infty} \|a_n - b_n\|_K = 0 \\ \lim\limits_{n\longrightarrow\infty} \|b_n - c_n\|_K = 0 \end{cases}$$

Alors

$$\|a_n - c_n\|_K = \|(a_n - b_n) + (b_n - c_n)\|_K \leq \|a_n - b_n\|_K + \|b_n - c_n\|_K$$

Pour $n \to \infty$, on obtient $\lim_{n\longrightarrow\infty} \|a_n - c_n\|_K = 0$. Donc

$$\{a_n\}_n \Re \{c_n\}_n \quad \text{(transitivité)}$$

4) **Etape 4 :** Soit $\widehat{K} = SC(K)/SN(K)$ l'ensemble des classes d'équivalence des suites de Cauchy $\{a_n\}_n$ pour la relation $\Re$ définie précédente. On note par $(a_n) \in \widehat{K}$ la classe d'équivalence de suite de Cauchy $\{a_n\}_n \in SC(K)$ et la suite constante

$$\{a\}_{n\in N} = \{a, a, a, ...\}, a \in K$$

appartient à des classes différentes pour différents éléments a.

Notons par (a_n) la classe d'équivalence qui représente la suite de Cauchy $\{a\}_n$. Ainsi $(a_n) \in \widehat{K}$, et nous allons considérer K comme un sous ensemble de $\widehat{K}$, et nous identifions $a \in K$ avec $\widehat{a} = (a) \in \widehat{K}$.

Théorème 1.2.4 *L'ensemble quotient $\widehat{K} = SC(K)/SN(K)$ est un corps.*

Preuve. Il est facile de vérifier que $\widehat{K}$ muni des deux opérations suivantes :

$$\forall \{a_n\}_{n\in\mathbb{N}} \in A \in \widehat{K}, \forall \{b_n\}_{n\in\mathbb{N}} \in B \in \widehat{K} : \begin{cases} A + B = (a_n) + (b_n) = (a_n + b_n) \\ A.B = (a_n).(b_n) = (a_n.b_n) \end{cases}$$

est un anneau commutatif, tel que son élément neutre par rapport à l'addition (resp : à la multiplication) est $\overline{0}$ (resp : $\overline{1}$).
Il reste à montrer que tout élément de $\widehat{K}$ admet un inverse par rapport à la multiplication. C'est-à-dire

$$\forall A \in \widehat{K}^*, \exists \grave{A} \in \widehat{K} : A.\grave{A} = \overline{1}$$

Soit $A \in \widehat{K}$ tel que $A \neq \overline{0} = SN(K)$ et $\{a_n\}_{n\in\mathbb{N}}$ un représentant de A (une suite de Cauchy dans K). Tant qu'elle n'est pas nulle, alors

$$\exists C \in \mathbb{R}_+^*, \exists N \in \mathbb{N}^* : \|a_n\| > C, \forall n \geq N$$

On définit une autre suite $\{a_n^*\}_{n\in\mathbb{N}}$ par

$$a_n^* = \begin{cases} 0 & , \text{si } 1 \leq n \leq N-1 \\ \frac{1}{a_n} & , \text{si } n \geq N \end{cases}$$

La suite $\{a_n^*\}_{n\in\mathbb{N}}$ est de Cauchy. En effet :
Pour tous $n, m \geq N$, on a

$$0 \leq \|a_m^* - a_n^*\| = \|\frac{1}{a_m} - \frac{1}{a_n}\| = \frac{\|a_m - a_n\|}{\|a_m\|\|a_n\|} \leq C^{-2}\|a_m - a_n\| \longrightarrow 0, n, m \longrightarrow \infty$$

Notons la classe d'équivalence de $\{a_n^*\}_{n\in\mathbb{N}}$ par A^{-1}. On a

$$\{a_n\}_{n\in\mathbb{N}} . \{a_n^*\}_{n\in\mathbb{N}} = \{a_n.a_n^*\}_{n\in\mathbb{N}} = \left\{ \underbrace{0, 0, \ldots, 0}_{(N-1)terme}, 1, 1, \ldots \right\}$$

On trouve

$$\{a_n a_n^*\}_{n\in\mathbb{N}} - \{1\}_{n\in\mathbb{N}} = \left\{ \underbrace{-1, -1, \ldots, -1}_{(N-1)terme}, 0, 0, \ldots \right\} \in SN(K)$$

Ceci implique que $\{a_n \cdot a_n^*\}_{n\in\mathbb{N}} \in \bar{1}$, c'est à dire que

$$(a_n a_n^*) = A.B = \bar{1}$$

Alors $A.A^{-1} = \bar{1}$. ■

Définition 1.2.5 *Pour tout $A = (a_n) \in \widehat{K}$, on définit l'application*

$$\begin{array}{rccl} \|.\|_{\widehat{K}} : & \widehat{K} & \longrightarrow & \mathbb{R}^+ \\ & A & \longrightarrow & \|A\|_{\widehat{K}} = \lim\limits_{n\to+\infty} \|a_n\|_K \end{array}$$

Proposition 1.2.6 *L'application $\|.\|_{\widehat{K}}$ est une norme sur $\widehat{K}$. Elle est non-archimédienne si la norme de K est non-archimédienne aussi.*

Preuve. Cette norme est bien définie. Pour cela, nous devons montrer que la limite existe et indépendante du représentant $\{a_n\}_n \in A \in \widehat{K}$. On a $\{a_n\}_n$ est une suite de Cauchy, alors

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n, m \geq n_0 : \|a_m - a_n\|_K \leq \varepsilon$$

D'autre part, on sait que

$$\left|\|a_m\|_K - \|a_n\|_K\right| \leq \|a_m - a_n\|_K$$

On obtient, pour tout $\varepsilon > 0, \left|\|a_m\|_K - \|a_n\|_K\right| \leq \varepsilon$.
La suite de nombres réels $\{\|a_n\|\}_{n\in\mathbb{N}}$ est de Cauchy dans $(\mathbb{R}, |.|)$ complet, alors elle a une limite $l \in \mathbb{R}^+$. Donc $\lim\limits_{n\longrightarrow+\infty} \|a_n\|_K$ existe.
Supposons que $\{a_n\}_n$ et $\{a'_n\}_n$ sont deux représentants de A. Alors par la même inégalité, nous avons

$$0 \leq \lim_{n\longrightarrow+\infty} \left|\|a_n\|_K - \|a'_n\|_K\right| \leq \lim_{n\longrightarrow+\infty} \|a_n - a'_n\|_K = 0$$

Alors $\lim\limits_{n\longrightarrow+\infty} \|a_n\|_K = \lim\limits_{n\longrightarrow+\infty} \|a'_n\|_K$.
On vérifie les trois propriétés de la norme :
1) Si $A = (a_n) \in \widehat{K}$ telle que $A = 0$, alors

$$A = (a_n) = 0 \Longleftrightarrow \{a_n\}_{n\in\mathbb{N}} \in SN(K)$$

$$\Longleftrightarrow \lim_{n\to+\infty} \|a_n\|_K = 0$$

$$\Longleftrightarrow \|A\|_{\widehat{K}} = 0$$

Si $A = (a_n) \neq 0$, alors $\{a_n\}_{n\in\mathbb{N}} \notin SN(K)$, on obtient

$$\exists c \in \mathbb{R}^*_+, \exists N \in \mathbb{N}^* : \|a_n\|_K \geq c > o, \forall n \geq N$$

$$\Longrightarrow \lim_{n\to+\infty} \|a_n\|_K \neq 0$$

$$\Longrightarrow \|A\|_{\widehat{K}} > 0$$

2) Soient $A = (a_n) \in \widehat{K}$, $B = (b_n) \in \widehat{K}$, alors

$$\|A \cdot B\|_{\widehat{K}} = \lim_{n\to+\infty} \|a_n b_n\|_K = \lim_{n\to+\infty} (\|a_n\|_K \cdot \|b_n\|_K)$$

$$= \lim_{n\to+\infty} \|a_n\|_K \cdot \lim_{n\to+\infty} \|b_n\|_K = \|A\|_{\widehat{K}} \cdot \|B\|_{\widehat{K}}$$

3) Pour $A = (a_n) \in \widehat{K}$, $B = (b_n) \in \widehat{K}$, on a

$$\|A + B\|_{\widehat{K}} = \lim_{n\to+\infty} \|a_n + b_n\|_K \leq \lim_{n\to+\infty} (\|a_n\|_K + \|b_n\|_K)$$

$$\leq \lim_{n\to+\infty} \|a_n\|_K + \lim_{n\to+\infty} \|b_n\|_K = \|A\|_{\widehat{K}} + \|B\|_{\widehat{K}}$$

l'application $\|.\|_{\widehat{K}}$ est une norme. ■

Lemme 1.2.7 *Soient K un corps muni de la norme non-archimédienne $\|.\|_K$, et $(a_n)_{n\in\mathbb{N}}$ une suite de Cauchy et $b \in K$ possède la propriété $b \neq \lim\limits_{n\longrightarrow+\infty} a_n$. Alors*

$$\exists M \in \mathbb{N}, \forall n, m > M : \|a_n - b\|_K = \|a_m - b\|_K$$

On dit que la suite des nombres réels $(\|a_n - b\|_K)_{n\in\mathbb{N}}$ est stationnaire. En particulier, si $(a_n)_{n\in\mathbb{N}}$ n'est pas une suite nulle, alors la suite $(\|a_n\|_K)_{n\in\mathbb{N}}$ est stationnaire.

Preuve. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de Cauchy

$$\forall \varepsilon > 0, \exists M > 0 : \forall m, n > M \Longrightarrow \|a_m - a_n\|_K < \varepsilon$$

D'autre part, on a

$$\| (a_m - b) + (b - a_n) \|_K = \|a_m - a_n\|_K \geq |\|a_m - b\|_K - \|b - a_n\|_K|$$

$$\Longrightarrow |\|a_m - b\|_K - \|b - a_n\|_K| < \varepsilon$$

Donc la suite $(\|a_n - b\|_K)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$, d'où elle est convergente. Soit l sa limite et

$$b \neq \lim_{n\longrightarrow+\infty} a_n \Longrightarrow \|a_n - b\|_K > 0 \Longrightarrow l > 0$$

Nous avons, par définition

$$\forall \varepsilon > 0, \ \exists M_1 \in \mathbb{N} : \forall n > M_1 \Longrightarrow |\|a_n - b\|_K - l| < \varepsilon$$

Donc pour $\varepsilon = \frac{l}{2} > 0$, on a $\frac{l}{2} < \|a_n - b\|_K < \frac{3l}{2}$. On obtient

$$\exists M_1 \in \mathbb{N} \ : \forall n > M_1 \Longrightarrow \|a_n - b\|_K > \frac{l}{2}$$

De même, puisque $(a_n)_n$ est de Cauchy dans $\mathbb{Q}_p$, alors pour $\varepsilon = \frac{l}{2}$, il existe $M_2 \in \mathbb{N}$ tel que

$$\forall n, m > M_2 \Longrightarrow \|a_m - a_n\|_K < \frac{l}{2}$$

On prend $M = \max(M_1, M_2)$. Alors pour tout $n, m \geq M$, on obtient

$$\|a_m - b\|_K = \|a_n - b + a_m - a_n\|_K = \max\{\|a_n - b\|_K, \|a_m - a_n\|_K\} = \|a_n - b\|_K$$

Montrons que $\| .\|_{\widehat{K}}$ est non-archimédienne :
Soient $A = (a_n)_n, B = (b_n)_n \in \widehat{K}$ telle que $A \neq B$. Supposons que les deux suites ne sont

pas nulles ($b = 0$), D'après le lemme (1.2.7), on obtient

$$\begin{aligned} \exists N_1 \in \mathbb{N}, \forall n > N_1 &\Longrightarrow \|A\|_{\widehat{K}} = \|a_n\|_K \\ \exists N_2 \in \mathbb{N}, \forall n > N_2 &\Longrightarrow \|B\|_{\widehat{K}} = \|b_n\|_K \end{aligned} \tag{1.1}$$

Soit $N = \max(N_1, N_2)$. Alors d'après (1.1) et $\|.\|_K$ est ultramétrique, on trouve

$$\|a_n + b_n\|_K = \max\left(\|a_n\|_K, \|b_K\|_K\right) = \max\left(\|A\|_{\widehat{K}}, \|B\|_{\widehat{K}}\right)$$

Donc

$$\begin{aligned} \lim_{n \longrightarrow +\infty} \|a_n + b_n\|_K &= \max\left(\|A\|_{\widehat{K}}, \|B\|_{\widehat{K}}\right) \\ \Longrightarrow \|A + B\|_{\widehat{K}} &= \max\left(\|A\|_{\widehat{K}}, \|B\|_{\widehat{K}}\right) \end{aligned}$$

Alors $\|.\|_{\widehat{K}}$ est une norme ultramétrique. ■

Théorème 1.2.8 *L'espace $\widehat{K}$ muni de la norme $\| \ .\|_{\widehat{K}}$ est complet. De plus K est un sous-ensemble dense dans $\widehat{K}$.*

Preuve. 1) Montrons que K est dense dans $\widehat{K}$.
On sait qu'on peut identifier la suite constante $\{c\}_{n \in N} = \{c, c, c, ...\}, c \in K$ avec sa classe d'équivalence

$$\bar{c} = \{c, c, c, ...\}$$

Soit $A \in \widehat{K}$ et $\{a_m\}_{m \in \mathbb{N}}$ est une suite de K qui représente A.
Pour tout entier positif fixé "n", nous considérons la suite constante $\bar{a}_n$, donc la suite $\{a_m - a_n\}_{m \in \mathbb{N}}$ représente la classe $A - (\bar{a}_n)$, et comme $\{a_n\}_{n \in \mathbb{N}}$ est de Cauchy, on peut écrire

$$\lim_{n \longrightarrow +\infty} \| \ A - (\bar{a}_n)\|_{\widehat{K}} \ = \lim_{n \to +\infty} \left(\lim_{m \to +\infty} \| \ a_m - a_n\|_K \ \right) = 0 \tag{1.2}$$

Il vient que K est dense dans $\widehat{K}$.
2) **Montrons que $(\widehat{K}, \|.\|_{\widehat{K}})$ est complet**
C'est-à-dire toute suites de Cauchy de $\widehat{K}$ est convergente dans $\widehat{K}$.

Soit $\{A_n\}_{n \in \mathbb{N}} = \{A_1, A_2, ...\}$ une suite de Cauchy dans $\widehat{K}$, d'après la densité de K dans $\widehat{K}$, alors pour tout A_n il existe un élément $a_n \in K$ tel que

$$\| \ A_n - (\bar{a}_n)\|_{\widehat{K}} \leq \frac{1}{n} \tag{1.3}$$

Donc $\{A_n - (\bar{a}_n)\}_{n \in \mathbb{N}}$ est une suite nulle, d'où elle est de Cauchy dans $\widehat{K}$.

Nous avons

$$\{(\bar{a}_n)\}_{n \in \mathbb{N}} = \{A_n\}_{n \in \mathbb{N}} - \{A_n - (\bar{a}_n)\}_{n \in \mathbb{N}}$$

Alors $\{(\bar{a}_n)\}_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\widehat{K}$, et comme tous ses éléments appartiennent à K, alors $\{a_n\}_{n\in\mathbb{N}}$ est de Cauchy dans K.

De (1.2) et (1.3), on déduit que $\{A-(\bar{a}_n)\}_{n\in\mathbb{N}}$ et $\{A_n-(\bar{a}_n)\}_{n\in\mathbb{N}}$ sont des suites nulles dans $\widehat{K}$. Donc sa différence

$$\{A-A_n\}_{n\in\mathbb{N}}=\{A-(\bar{a}_n)\}_{n\in\mathbb{N}}-\{A_n-(\bar{a}_n)\}_{n\in\mathbb{N}}$$

est une suite nulle dans $\widehat{K}$, ce qui implique que $\lim\limits_{n\to+\infty}\parallel A-A_n\parallel_{\widehat{K}}=0$. Il vient que $A=\lim\limits_{n\to+\infty}A_n$. ■

Chapitre 2

Corps des nombres p-adique

Dans ce chapitre nous allons présenter le corps des nombres p-adiques où p désigne un nombre premier. Nous allons appliqués la procédure de complétion que nous avons vu dans le chapitre précédent sur le corps des nombres rationnels, en utilisant une norme spécifique appelée norme p-adique. On va donner quelques notions et résultats importants concernant la valutaion, la norme et les entiers p-adiques.

2.1 Valuation et norme p-adique sur $\mathbb{Q}$

Définition 2.1.1 *Soit p un nombre premier. Alors*
1) On appelle valuation p-adique d'un entier rationnel non nul $x \in \mathbb{Z}^*$ notée $v_p(x)$ le plus grand entier positif tel que $p^{v_p(x)}$ divise x.

$$\begin{array}{rccl} v_p: & \mathbb{Z}^* & \to & \mathbb{Z}^+ \\ & x & \longmapsto & v_p(x) = \max\{r \in \mathbb{Z}^+ : p^r \ divise \ x\} \end{array}$$

Dans ce cas x s'écrit

$$x = u.p^{v_p(x)} \ \text{où } u \in \mathbb{Z}^*, (u,p) = 1$$

tel que (u,p) désigne le pgcd de u et de p. Autrement dit la valuation p-adique compte le nombre de fois que l'on peut diviser un nombre par p.
2) La valuation p-adique d'un nombre rationnel non nul $x \in \mathbb{Q}^*$ est définie par

$$\begin{array}{rccl} v_p: & \mathbb{Q}^* & \to & \mathbb{Z} \\ & x & \longmapsto & v_p(x) = \max\{r \in \mathbb{Z} : p^r divise \ x\} \end{array}$$

Remarque 2.1.2 *0 est divisible une infinité de fois par p, alors $v_p(0) = +\infty$.*

Exemple 2.1.3 *Soit $a \in \mathbb{Q}$. Alors*
1) $a = p^2 + p^3 + 2p^4$, $v_p(a) = 2, \forall p \geq 2$
2) $a = 24 = 3 \cdot 8$, $(3, 8) = 1$, $v_p(a) = 1$, *pour* $p = 3$
3) $a = 14 = 2 \cdot 7$, $(2, 7) = 1$, $v_p(a) = 1$, *pour* $p = 2$

Proposition 2.1.4 *La valuation p-adique vérifie les propriétés suivantes :*
1) si $x = \frac{a}{b} \in \mathbb{Q}^*$, *alors* $v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$
2) $v_p(x \cdot y) = v_p(x) + v_p(y)$,$\forall x, y \in \mathbb{Q}$
3) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$,.$\forall x, y \in \mathbb{Q}$

Preuve.
1) Soit $x = \frac{a}{b} \in \mathbb{Q}^*$ telles que

$$\begin{cases} a = a_1.p^{v_p(a)}, (a, a_1) \in \mathbb{Z}^2, (a_1, p) = 1 \\ b = b_1.p^{v_p(b)}, (b, b_1) \in \mathbb{Z}^{*2}, (b_1, p) = 1 \end{cases}$$

Ce qui donne

$$x = \frac{a}{b} = \frac{a_1.p^{v_p(a)}}{b_1.p^{v_p(b)}} = \frac{a_1}{b_1} p^{v_p(a) - v_p(b)}, (a_1, p) = (b_1, p) = 1$$

Alors

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

2) Soient $x, y \in \mathbb{Q}$, alors il y a trois cas à étudier :
i) Si $x = 0$ ou $y = 0$, on a alors $xy = 0$, donc $v_p(xy) = +\infty$ et $v_p(x) + v_p(y) = +\infty$. D'où l'égalité.
ii) Si $xy = 0$, alors $v_p(xy) = +\infty$. C'est à dire

$$\forall n \in \mathbb{N} : p^n \mid xy \Longrightarrow \forall k, m \in \mathbb{N}, k + m = n : \begin{cases} p^k \mid x \\ p^m \mid y \end{cases}$$

$$\Longrightarrow \begin{cases} v_p(x) \geq k, \forall k \in \mathbb{N} \\ v_p(y) \geq m, \forall m \in \mathbb{N} \end{cases}$$

$$\Longrightarrow v_p(x) = +\infty \text{ et } v_p(y) = +\infty$$

Par la convention $(+\infty) + (+\infty) = +\infty$. Donc $v_p(x) + v_p(y) = +\infty$. D'où l'égalité.
iii) Soient $x, y \in \mathbb{Q}^*$ telles que

$$\begin{aligned} x &= c.p^{v_p(x)}, (c, p) = 1 \\ y &= d.p^{v_p(y)}, (d, p) = 1 \end{aligned}$$

On obtient

$$x.y = cd.p^{v_p(x)+v_p(y)}, (cd, p) = 1$$
$$\Longrightarrow v_p(x.y) = v_p(x) + v_p(y)$$

3) Soient $x, y \in \mathbb{Q}$ telles que

$$\begin{aligned} x &= p^r.\frac{a}{b}, v_p(x) = r, (a, p) = (b, p) = 1 \\ y &= p^s.\frac{c}{d}, v_p(y) = s, (c, p) = (d, p) = 1 \end{aligned}$$

On obtient

$$v_p(x + y) = v_p(p^r.\frac{a}{b} + p^s.\frac{c}{d})$$

Supposons que $s \geq r$, donc

$$\begin{aligned} v_p(x + y) &= v_p\left(p^r.(\frac{a}{b} + p^{s-r}.\frac{c}{d})\right) = v_p\left(p^r.(\frac{ad + p^{s-r}.cd}{bd})\right) \\ &= v_p(p^r) + v_p(\frac{ad + p^{s-r}.cd}{bd}) = r + v_p\left(ad + p^{s-r}.cd\right) - v_p(bd) \end{aligned}$$

Tant que $(bd, p) = 1$, alors $v_p(bd) = 0$. Comme $ad + p^{s-r}.cd \in \mathbb{Z}$.
Donc $v_p(ad + p^{s-r}.cd) \geq 0$. On conclut que

$$v_p(x + y) \geq r = \min(v_p(x), v_p(y))$$

■

2.2 Norme p-adique

Définition 2.2.1 *Soit p un nombre premier.*
1) On considère l'application $|.|_p$ définie par

$$|.|_p : \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{R}^+ \\ x & \longrightarrow & |x|_p = \begin{cases} p^{-v_p(x)} & , si\ x \neq 0 \\ 0 & , si\ x = 0 \end{cases} \end{array}$$

avec $v_p(x)$ représente la valuation p-adique de x. L'application $|.|_p$ est appelé la norme p-adique (la valeur absolue p-adique) de $\mathbb{Q}$.

2) La distance sur $\mathbb{Q}$ induite par cette norme notée d_p est définie par

$$\begin{array}{rccl} d_p: & \mathbb{Q}\times\mathbb{Q} & \to & \mathbb{R}^+ \\ & (x,y) & \to & d_p(x,y)=|x-y|_p \end{array}$$

Remarque 2.2.2
1) 0 est divisible une infinité de fois par p, donc on a $|0|_p = \frac{1}{+\infty} = 0$.
2) 1 n'est divisible aucune fois par p, donc $|1|_p = \frac{1}{p^0} = 1$.

Proposition 2.2.3 *Pour tout p premier l'application* $x \mapsto |x|_p$ *est une norme ultramétrique sur* $\mathbb{Q}$.

Preuve.
1) Soit $x \in \mathbb{Q}$, alors

$$|x|_p = 0 \Leftrightarrow p^{-v_p(x)} = 0 \Leftrightarrow -v_p(x) = -\infty \Leftrightarrow v_p(x) = +\infty \Leftrightarrow x = 0$$

2) Soient $x, y \in \mathbb{Q}$. Alors, si $x = 0$ ou $y = 0$, on a l'égalité.
Si $x \neq 0$ et $y \neq 0$, on trouve

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

3) Soient $x, y \in \mathbb{Q}$. Alors

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

$$\Rightarrow -v_p(x+y) \leq -\min(v_p(x), v_p(y)) = \max(-v_p(x), -v_p(y))$$

$$\Rightarrow p^{-v_p(x+y)} \leq p^{-\min(v_p(x),v_p(y))} = p^{\max(-v_p(x),-v_p(y))} = \max\left(p^{-v_p(x)}, p^{-v_p(y)}\right)$$

$$\Rightarrow |x+y|_p \leq \max\left\{|x|_p, |y|_p\right\}$$

■

Remarque 2.2.4
1) La norme p-adique $|.|_p$ *prend ses valeurs dans l'ensemble discret* $\{0\} \cup \{p^n : n \in \mathbb{Z}\}$.
2) $\mathbb{Z}$ *est un ensemble borné selon cette norme.*

$$\forall x \in \mathbb{Z} : |x|_p \leq 1$$

Exemple 2.2.5
1) Pour $x = \frac{99}{140} = \frac{3^2 \times 11}{2^2 \times 5 \times 7} = 2^{-2} \times 5^{-1} \times 7^{-1} \times 3^2 \times 11 \in \mathbb{Q}$. *Alors*

$$|x|_2 = 4, |x|_3 = \frac{1}{9}, |x|_5 = 5, |x|_7 = 7, |x|_{11} = \frac{1}{11}, |x|_p = 1, \forall p > 11$$

2) La distance usuelle de 252 *à* 2*est* $d(252, 2) = |252 - 2| = 250$. *Par contre, la distance 5-adique de* 252 *à* 2 *que la note* $d_5(252, 2)$ *est*

$$d_5(256, 2) = |252 - 2|_5 = |250|_5 = \left|5^3 \cdot 2\right|_5 = \frac{1}{5^3}$$

Le théorème suivant donne la relation entre les différentes normes p-adiques.

Théorème 2.2.6 *(La formule de produit)*
Pour tout nombre rationnel non nul $a \in \mathbb{Q}^*$, *on a*

$$|a|_\infty \cdot \prod_{p\ premier} |a|_p = 1$$

Autrement dit, pour tout a non nul de $\mathbb{Q}$, $|a|_p$ *est égal à* 1 *sauf pour un nombre fini de valeurs de p.*

Preuve. Soit $a \in \mathbb{Q}^*$. Alors la factorisation primaire de a s'écrit

$$a = \mp p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot \ldots \cdot p_k^{m_k}$$

Alors

$$|a|_\infty = \left|\mp p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot \ldots p_k^{mk}\right| = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot \ldots \cdot p_k^{mk}$$

Telles que

$$\forall i \in \{1, \ldots, k\} : |a|_p = p_i^{-m_i}$$

D'autre part, si $p \notin \{p_1, p_2, \ldots, p_k\}$, alors $|a|_p = 1$.
On obtient

$$|a|_\infty \cdot \prod_{p\ premier} |a|_p = |a|_\infty \cdot \prod_{i=1}^{k} |a|_{p_i} = (p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3} \cdot \ldots \cdot p_k^{m_k}) \cdot \prod_{i=1}^{k} p_i^{-m_i} = 1$$

■

Exemple 2.2.7 *Pour tout $p \notin \{2,3,\infty\}$, on a $\left|\frac{2}{3}\right|_p = 1$, ce qui donne*

$$\left|\frac{2}{3}\right|_\infty \cdot \prod_{p\ premier} \left|\frac{2}{3}\right|_p = \left|\frac{2}{3}\right|_\infty \cdot \left|\frac{2}{3}\right|_2 \cdot \left|\frac{2}{3}\right|_3 = \frac{3}{2} \cdot 2 \cdot \frac{1}{3}$$

Notons que la propriété remarquable suivante n'est pas vraie pour la valeur absolue ordinaire (vraie seulement pour les espaces ultramétriques)

Théorème 2.2.8 *Soit $(a_n)_n$ suite de $\mathbb{Q}$. Alors $(a_n)_n$est une suite de Cauchy si et seulement si*

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

Preuve.
1) Si$(a_n)_n$ est une suite de Cauchy. Alors

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n, m \geq n_0 : |a_m - a_n|_p \leq \varepsilon$$

En particulier, pour $m = n + 1 \geq n_0$, on a

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : |a_{n+1} - a_n|_p \leq \varepsilon$$

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

2) D'autre part, supposons que $\lim_{n\longrightarrow+\infty} |a_{n+1} - a_n|_p = 0$. Alors d'après la définition de la limite

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N}; \forall n \geq n_0 : |a_{n+1} - a_n|_p \leq \varepsilon$$

Prenons $\varepsilon > 0, m > n \geq n_0$et examinons $|a_m - a_n|_p$. On a

$$|a_m - a_n|_p = |a_m - a_{m-1} + a_{m-1} - a_{m-2} + ... + a_{n+1} - a_n|_p$$

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

$$\leq \max(\varepsilon, \varepsilon, \varepsilon, ..., \varepsilon) = \varepsilon$$

Alors $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy. ■

2.3 Les nombres p-adiques

L'espace métrique associé à la distance p-adique n'est pas un espace complet, tout comme $\mathbb{Q}$ n'est pas complet pour la valeur absolue ordinaire. Lorsqu'on complète $\mathbb{Q}$ par

rapport à la distance associée à la valeur absolue $|.|$,on obtient $\mathbb{R}$, de la même façon, on complète $\mathbb{Q}$ par rapport à la distance associée à la norme p-adique, on obtient un espace complet que l'on note $\mathbb{Q}_p$. L'exemple suivant nous montre que l'espace métrique $\left(\mathbb{Q}, ||_p\right)$ n'est pas complet.

Exemple 2.3.1 *On considère pour $p = 7$ les deux suites $(a_n)_n$et $(x_n)_n$ de $\mathbb{Q}$ définies par*

$$\begin{aligned} a_0 &= 3 \\ x_1 &= a_0 = 3 \\ x_2 &= x_1 + a_1 \cdot 7 = a_0 + a_1 \cdot 7 \\ &\vdots \\ x_n &= a_0 + a_1 \cdot 7 + ... + a_{n-1} \cdot 7^{n-1}, \forall n \geq 1 \end{aligned}$$

$$\Longrightarrow x_{n+1} = x_n + a_n \cdot 7^n$$

$$\Longrightarrow x_{n+1} - x_n \equiv 0 \bmod 5^n$$

On détermine $a_n \in \{0, 1, 2, 3, 4, 5, 6\}$ et x_n par la suite de congruence

$$\forall n \geq 1 : x_n^2 - 2 \equiv 0 \bmod 7^n$$

On obtient la relation de récurrence

$$x_{n+1} \equiv x_n + x_n^2 - 2 \bmod 7^{n+1}$$

La suite $(x_n)_n$est de Cauchy dans $\mathbb{Q}$ car

$$|x_{n+1} - x_n|_p \leq |7^n|_7 = \frac{1}{7^n} \longrightarrow 0, n \to \infty$$

Cependant, elle ne peut converger vers $x \in \mathbb{Q}$, puisque dans ce cas, on aurait $x^2 - 2 = 0$ dans $\mathbb{Q}$. Il n'existe pas d'entier x vérifiant cette dernière équation. Ce qui est impossible.

Définition 2.3.2 *Soit p un nombre premier.*
1) Le corps des nombres p-adiques est la commplétion de l'espace mètrique $(\mathbb{Q}, d_p)$. Ses èlèments sont les classes d'èquivalence des suites de Cauchy des nombre rationnels $\{a_n\}_n$ muni de la relation suivante

$$\{a_n\} \Re \{b_n\} \Leftrightarrow \lim_{n \longrightarrow +\infty} |a_n - b_n|_p = 0$$

2) On prolonge la norme p-adique dèfinie sur $\mathbb{Q}$ à tout $\mathbb{Q}_p$ par

$$\forall a \in \mathbb{Q}_p : |a|_p = \lim_{n \longrightarrow \infty} |\alpha_n|_p$$

où (α_n) ets une suite de Cauchy d'èlèments de $\mathbb{Q}$ qui reprèsente le nombre p-adique a.

Remarque 2.3.3
1) $\mathbb{Q}$ est inclus dans $\mathbb{Q}_p$ de plus il est dense dans $\mathbb{Q}_p$.
2) $\mathbb{Q}_p$ est un corps valué complet ultramètrique.

Lemme 2.3.4
Soit $x \in \mathbb{Q}$ avec $|x|_p \leq 1$. Alors pour tout $n \in \mathbb{N}$, il existe un entier unique $\alpha \in \{0, 1, ..., p^n - 1\}$ tel que

$$|\alpha - x|_p \leq p^{-n}$$

Preuve. Soient $x = \frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$ et p un nombre premier. On a

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

$$\Longrightarrow p^{-v_p(a)+v_p(b)} \leq 1$$

$$\Longrightarrow v_p(b) = 0$$

pour assurer que $|x|_p \leq 1$. Alors

$$\begin{aligned} (p, b) &= 1 \Longrightarrow (p^n, b) = 1, \forall n \in \mathbb{N} \\ &\Longrightarrow \exists m_1, m_2 \in \mathbb{Z} : m_1 b + m_2 . p^n = 1 \end{aligned}$$

Soit

$$a.m_1 \equiv \alpha \bmod p^n \text{ (par la division euclidienne où } 0 \leq \alpha \leq p^n - 1)$$

Alors

$$|\alpha - x|_p = \left|\alpha - \frac{a}{b}\right|_p = \left|a.m_1 - kp^n - \frac{a}{b}\right|_p = \left|\frac{-a}{b}.(1 - m_1 b) - kp^n\right|_p = \left|\frac{a}{b}.(1 - m_1 b) + kp^n\right|_p$$

$$\Longrightarrow |\alpha - x|_p = \left|\frac{a}{b}.(m_2 p^n) + kp^n\right|_p \leq \max\left\{\left|\frac{a}{b}.(m_2 p^n)\right|_p, |kp^n|_p\right\} = \max\left\{p^{-n}, p^{-n}\right\} = p^{-n}$$

■

Théorème 2.3.5 *Si la classe d'équivalence $a \in \mathbb{Q}_p$ vérifie la condition $|a|_p \leq 1$, alors*

elle possède un seul représentant (λ_n) *qui satisfait*

$$\begin{cases} \lambda_n \in \mathbb{Z}, 0 \leq \lambda_n \leq p^n - 1 \\ \lambda_{n+1} \equiv \lambda_n \bmod p^n \end{cases}$$

Preuve. Voir [9] . ■

Conclusion 2.3.6
1) La suite de Cauchy (λ_n) *qui vérifie les condition du théorème précédent s'appelle représentant canonique de a.*
2) Tout nombre p-adique $a \in \mathbb{Q}_p$ *admet un développement p-adique unique sous forme d'une série convergente (série de Hensel) s'écrit sous la forme* $a = \sum_{k=n}^{\infty} \beta_k \cdot p^k$ *ou* $\beta_k \in \{0, 1, 2, ..., p-1\}, n \in \mathbb{Z}$ *et* $|a|_p = p^{-n}$.
3) On note par $a = \beta_n \beta_{n+1} ... \cdot \beta_0 \beta_1 ...$*la forme canonique de a ou* $\cdot$ *est appelé le point p-adique qui nous permet de déterminer le signe de n, tels que :*
(a) $a = \beta_n \beta_{n+1} ... \beta_{-1} . \beta_0 \beta_1 ...$, *si* $n < 0$
(b) $a = \cdot \beta_0 \beta_1 \beta_2 ...$, *si* $n = 0$
(c) $a = \cdot 00...0 \beta_0 \beta_1 ...$, *si* $n > 0$.

Exemple 2.3.7 *Soient les nombres 5-adiques suivants :*
1) $a_1 = 13 \cdot 41 = 1 \cdot 5^{-2} + 3 \cdot 5^{-1} + 4 \cdot 5^0 + 1 \cdot 5^1 +, n = -2$
2) $a_2 = \cdot 1341 = 1 \cdot 5^0 + 3 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3, n = 0$
3) $a_3 = \cdot 01341 = 0 \cdot 5^0 + 1 \cdot 5^1 + 3 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4, n = 1$
4) Le développement 5-adique de $b = \frac{1}{3}$

$$\frac{1}{3} = 2 \cdot 5^0 + 3 \cdot 5^1 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + ... = \cdot 231313131... = \cdot 2\overline{31} \text{ (périodique)}$$

5) Pour tout p premier, le développement p-adique de -1 *est*

$$-1 = (p-1) + (p-1) \cdot p + (p-1) \cdot p^2 + (p-1) \cdot p^3 ... + (p-1) \cdot p^n + ... = (p-1) \cdot \sum_{n=0}^{\infty} p^n$$

Par conséquent $\frac{1}{1-p} = \sum_{n=0}^{\infty} p^n = \cdot 11111$.

2.4 Les entiers p-adiques

Une partie intéressante de $\mathbb{Q}_p$ est l'ensemble des élément de la norme p-adique inférieure ou égale à 1 que l'on note $\mathbb{Z}_p$.

Définition 2.4.1 *1) On dit que le nombre p-adique $a \in \mathbb{Q}_p$est un entier p-adique si le développement canonique de a ne contient que les puissances positives de p. Autrement dit $v_p(a) \geq 0$. On écrit*

$$a = \alpha_0 + \alpha_1 \cdot p + \alpha_2 \cdot p^2 + ... + \alpha_n \cdot p^n + ... = \sum_{n=0}^{\infty} \alpha_n \cdot p^n, 0 \leq \alpha_n < p$$

2) On note par $\mathbb{Z}_p$ l'ensemble des entier p-adique, où

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : a = \sum_{n=0}^{\infty} \alpha_n \cdot p^n \right\} = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\}$$

Remarque 2.4.2
1) $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\} = \left\{a \in \mathbb{Q}_p : |a|_p \leq 1\right\}$. Autrement dit $\mathbb{Z}_p$ représente le disque de l'unité de rayon 1 et de centre 0.
2) Le corps $\mathbb{Q}_p$ est l'ensemble des fractions de $\mathbb{Z}_p$

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

Définition 2.4.3 *Soit a un nombre p-adique,*
1) On dit que a est unitaire ou inversible si le développement canonique p-adique de a ne contient que les puissances positives de p et le premier chiffre différent de zéro. On écrit

$$a = \alpha_0 + \alpha_1 \cdot p + \alpha_2 \cdot p^2 + ... + \alpha_n \cdot p^n + ... = \sum_{n=0}^{\infty} \alpha_n \cdot p^n, 0 < \alpha_n < p$$

2) Notons par $\mathbb{Z}_p^*$(ou U_p) l'ensemble de nombre p-adique inversibles (unitaires) défini par

$$\mathbb{Z}_p^* = \left\{ \sum_{n=0}^{\infty} \alpha_n \cdot p^n : \alpha_0 \neq 0 \right\} = \{a \in \mathbb{Q}_p : v_p(a) = 0\} = \left\{\alpha \in \mathbb{Z}_p : |\alpha|_p = 1\right\}$$

Proposition 2.4.4 *Tout nombre p-adique $\alpha \in \mathbb{Q}_p$ s'écrit de façon unique sous la forme*

$$\alpha = p^n \cdot u, u \in \mathbb{Z}_p^*, n \in \mathbb{Z}$$

Preuve.
1) Existence de la représentation : Soit $\alpha \in \mathbb{Q}_p$, alors α s'écrit sous la forme

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

On sait que

$$\begin{aligned} a &= u_1 \cdot p^{m_1}, u_1 \in \mathbb{Z}_p^*, m_1 = v_p(a) \\ b &= u_2 \cdot p^{m_2}, u_2 \in \mathbb{Z}_p^*, m_2 = v_p(b) \end{aligned}$$

Donc

$$\alpha = \frac{a}{b} = \frac{u_1 \cdot p^{m_1}}{u_2 \cdot p^{m_2}} = \frac{u_1}{u_2} \cdot p^{m_1 - m_2} = u \cdot p^n, n = m_1 - m_2, u = \frac{u_1}{u_2} \in \mathbb{Z}_p^* \text{ (puisque } \mathbb{Z}_p^* \text{ un corps)}$$

2) Unicité de la représentation :
Supposons que α admet deux représentations

$$\begin{aligned} \alpha &= u_1 \cdot p^{m_1}, u_1 \in \mathbb{Z}_p^*, m_1 \in \mathbb{Z} \\ \alpha &= u_2 \cdot p^{m_2}, u_2 \in \mathbb{Z}_p^*, m_2 \in \mathbb{Z} \end{aligned}$$

Alors

$$u_1 \cdot p^{m_1} = u_2 \cdot p^{m_2}$$

$$\Rightarrow u_1 \cdot u_2^{-1} = p^{m_2 - m_1}$$

$$\Rightarrow v_p\left(u_1 \cdot u_2^{-1}\right) = m_2 - m_1$$

Or $v_p\left(u_1 \cdot u_2^{-1}\right) = 0$ (car$u_1 \cdot u_2^{-1} \in \mathbb{Z}_p^*$), alors $m_1 = m_2$ et $u_1 = u_2$. ■

Exemple 2.4.5 *Soient* $p = 5$, $\alpha^{(1)} = \cdot 4\overline{13} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 ...$, *et* $\alpha^{(2)} = \cdot 4\overline{2} = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 ....$ *Alors* $\alpha^{(1)}$ *et* $\alpha^{(2)}$ *sont des nombres de* $\mathbb{Z}_5^*$. *Par contre* $\beta^{(1)} = \cdot 01\overline{40} = 0 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + 4 \cdot 5^4 + 0 \cdot 5^5 ... \notin \mathbb{Z}_5^*$ *puisque le premier chiffre est nul, et* $\beta^{(2)} = 42 \cdot 13\overline{31} = 4 \cdot 5^{-2} + 2 \cdot 5^{-1} + 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 ... \notin \mathbb{Z}_5^*$ *puisque son développement 5-adique contient des puissances négatives de* 5.

Théorème 2.4.6 *Une suite* $(a_n)_n$ *de* $\mathbb{Q}_p$ *est de Cauchy et par conséquent convergente si et si seulement si*

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

Preuve. De la même façon où $||_p$est définie sur $\mathbb{Q}$. ■

Proposition 2.4.7 *Une série* $\sum_{n \geq 0} a_n$ *avec* $a_n \in \mathbb{Q}_p$ *converge dans* $\mathbb{Q}_p$ *si et seulement si* $\lim_{n \to +\infty} a_n = 0$.

Preuve. On note par $\sum_{i=0}^{n} a_i = s_n$ la suite des sommes partielles. Alors

$$\sum_{n\geq 0} a_n \text{ converge dans } \mathbb{Q}_p \Longleftrightarrow (s_n)_n = (\sum_{i=0} a_i)_n \text{ converge dans } \mathbb{Q}_p$$

$$\Longleftrightarrow s_n - s_{n-1} = a_n \text{ converge vers } 0 \text{ dans } \mathbb{Q}_p$$

$$\Longleftrightarrow \lim_{n\to+\infty} a_n = 0 \text{ dans } \mathbb{Q}_p$$

■

Remarque 2.4.8 *Cette proposition est fausse dans* $(\mathbb{R}, |.|)$ *, L'exemple le plus évident d'une série dans* $(\mathbb{R}, |.|)$ *dont le terme général tend vers* 0*, mais qui ne converge par, est la série harmonique*$\sum_{n\geq 1} \frac{1}{n}$.

Chapitre 3

Les opérations arithmétiques dans le corps des nombres p-adiques

3.1 Codes de Hensel

Les opérations arithmétiques dans le corps des nombres p-adique $\mathbb{Q}_p$ sont faites chiffre à chiffre. On part de la gauche vers la droite comme dans les calculs arithmétiques dans la base p. Donc pour les calculs arithmétiques p-adiques, le problème dépend du nombre (la longueur) de suite des chiffres p-adiques. La solution consiste à introduire une arithmétique p-adique de longueur finie (les codes de Hensel).

Définition 3.1.1 *Soit p un nombre premier, le code de Hensel noté $H(p, M, \alpha)$ de longueur M pour tout nombre p-adique $\alpha = p^m.\frac{a}{b}$ est le couple*

$$(mant_\alpha, \exp_\alpha) = (a_m a_{m+1}... \cdot a_0 a_1 ... a_t, m), M = |m| + t + 1$$

où les chiffres (a_i) (resp : m) sont (la mantisse) les mantisses de α (resp : exposant), on écrit

$$H(p, M, \alpha) = (mant_\alpha, \exp_\alpha) = (a_m a_{m+1}... \cdot a_0 a_1 ... a_t, m)$$

Autrement dit le code de Hensel est un segment fini (une approximation) de son développement p-adique infini et M un entier positif qui spécifie le nombre de chiffres signéficatifs dans le développement p-adique de α.
Notons $H_{p,M}$ l'ensemble des codes de Hensel d'un nombre p-adique.

3.2 Calcul de code de Hensel

Soit $\alpha = \frac{a}{b} \in \mathbb{Q}_p$ un nombre p-adique et p un nombre premier, divisons a et b par le nombre p autant de fois que possible jusqu'à obtenir $\alpha = p^m.\frac{c}{d}, (cd, p) = 1$.
Supposons que le code de Hensel de $\frac{c}{d}$ est $H(p, M, \frac{c}{d}) = (\cdot a_0 a_1 ... a_{M-1}, 0)$, où $(a_{M-1}...a_1 a_0)$ est la représentation de $\frac{c}{d} (\mathrm{mod}\, p^M)$ dans la base p.

$$cd^{-1} \equiv a_{M-1}p^{M-1} + ... + a_1 p + a_0 (\mathrm{mod}\, p^M)$$

On distingue les cas suivants :
1) **Si** $m = 0$, alors premièrement on écrit le nombre $\frac{c}{d}$ dans la base p, i.e :

$$cd^{-1} \equiv a_{M-1}p^{M-1} + ... + a_1 p + a_0 (\mathrm{mod}\, p^M) = (a_{M-1}...a_1 a_0)_p$$

puis en versant les chiffres $(a_i)_{i=\overline{0,M-1}}$ pour obtenir le code de Hensel de α.

$$H(p, M, \alpha) = (\cdot a_0 a_1 ... a_{M-1}, 0)$$

2) **Si** $m < 0$, alors dans ce cas $\alpha = p^m.\frac{c}{d}, m < 0$. Pour trouver $H(p, M, \alpha)$, il suffit de trouver $H(p, M, \frac{c}{d})$ comme dans le cas précédent, en suite on change le point p-adique $(-m)$ fois à droite.

$$H(p, M, \alpha) = (a_0 a_1 ... a_{m-1} \cdot ... a_{M-1}, m)$$

3) **Si** $m > 0$, alors $\alpha = p^m.\frac{c}{d}, m > 0$.Pour calculer $H(p, M, \alpha)$, il suffit de calculer $H(p, M, \frac{c}{d})$ comme dans le premier cas, en suite on change le point p-adique m fois à gauche.

$$H(p, M, \alpha) = (\cdot 0...00000 a_0 a_1 ... a_{M-(m+1)}, m)$$

Exemple 3.2.1
1) Soient $\alpha = \frac{2}{3}, p = 5, M = 4, p^M = 625$. *Alors* $\alpha = \frac{2}{3} = 5^0.\frac{2}{3}$, $m = 0$ *et*

$$2.3^{-1} = 2.417 \equiv 209 \,\mathrm{mod}\, 625$$

Exprimons le nombre 209 *dans la base* 5. *On trouve*

$$209 = 1.5^3 + 3.5^2 + 1.5^1 + 4.5^0 = (1314)_5$$

Le code de Hensel de $\alpha = \frac{2}{3}$ *est* $H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$.
2) Si $\alpha = \frac{2}{15}$, *alors* $\alpha = \frac{2}{15} = 5^{-1}.\frac{2}{3}$, $m = -1 < 0$. *On obtient* $H(5, 4, \frac{2}{3}) = (\cdot 4131, 0)$ *et on*

change le point 5-adique une fois à droite, on obtient

$$H(5, 4, \frac{2}{15}) = (4 \cdot 131, -1)$$

3) Si $\alpha = \frac{10}{3}$, *alors* $\alpha = \frac{10}{3} = 5^{+1}.\frac{2}{3}$, $m = 1 > 0$. *On change le point p-adique une fois à gauche, on trouve*

$$H(5, 4, \frac{10}{3}) = (\cdot 0413, +1)$$

Remarque 3.2.2 *Les règles pour obtenir les codes de Hensel des nombres négatifs sont les mêmes.*

3.2.1 Addition :

En règle générale, lorsqu'on additionne des nombres entiers usuels, exprimés en base 10. On additionne terme à terme. On additionne les unités avec les unités, les dizaines avec les dizaines avec la retenue éventuelle provenant de la colonne précédente,... et ainsi de suite pour les autres termes du nombres. Pour l'addition des nombres p-adique, on procède de la même manière : on les additionnes terme à termes (Les calculs se faisant de gauche à droite), tout en appliquant le système des retenues (les quotients de la division euclidiennes).

Soient α, β deux nombres p-adiques telles que :

$$H(p, M, \alpha) = (mant_\alpha, \exp_\alpha) = (\cdot a_0 a_1 ... a_{M-1}, \exp_\alpha)$$
$$H(p, M, \beta) = (mant_\beta, \exp_\beta) = (\cdot b_0 b_1 ... b_{M-1}, \exp_\beta)$$

Donc pour trouver le nombre p-adique $H(p, M, \alpha) + H(p, M, \beta)$:

Premièrement, on normalise le code qui a le plus grand exposant selon les cas I, II, III précédents pour obtenir $\exp_\beta = \exp_\alpha$.

Deuxièmement, On fait l'addition gauche à droite par rapport aux mantisses comme suit :

$$\begin{array}{cccccccc} & a_0 & & a_1 & & a_2 & . \ . \ . \ . & a_{M-1} \\ + & b_0 & & b_1 & & b_2 & . \ . \ . \ . & b_{M-1} \\ = & a_0 + b_0 & a_1 & + b_1 + r_0 & a_2 & + b_2 + r_1 & . \ . \ . \ . & a_{M-1} + b_{M-1} + r_{M-2} \end{array}$$

la retenue r_0 correspond à la retenue éventuelle de la somme $(a_0 + b_0)$, elle est additionnée à la somme $(a_1 + b_1)$. Le $M - 1$ rang correspond à la somme de $a_{M-1} + b_{M-1} + r_{M-2}$, l'éventuelle retenue de la colonne précédente.

La formule générale pour trouver la somme est

$$\gamma = \alpha + \beta = \cdot\gamma_0\gamma_1\gamma_2.....\gamma_{M-1}$$

telles que

$$\begin{aligned}
\gamma_0 &\equiv a_0 + b_0 \bmod p, r_0 = \left[\frac{a_0 + b_0}{p}\right] \\
\gamma_1 &\equiv a_1 + b_1 + r_0 \bmod p, r_1 = \left[\frac{a_1 + b_1 + r_0}{p}\right] \\
&\vdots \\
\gamma_{M-1} &\equiv a_{M-1} + b_{M-1} + r_{M-2} \bmod p, r_{M-1} = \left[\frac{a_{M-1} + a_{M-1} + r_{M-2}}{p}\right]
\end{aligned}$$

Ceci est équivalent à

$$\forall i = \overline{0, M-2} : \begin{cases} \gamma_0 \equiv a_0 + b_0 \bmod p, r_0 = \left[\frac{a_0+b_0}{p}\right] \\ \gamma_{i+1} \equiv a_{i+1} + b_{i+1} + r_i \bmod p, r_{i+1} = \left[\frac{a_{i+1}+b_{i+1}+r_i}{p}\right] \end{cases}$$

et

$$H(p, M, \alpha) + H(p, M, \beta) = H(p, M, \gamma) = (mant_\alpha + mant_\beta, \exp_\gamma)$$

Exemple 3.2.3 *Soient* $\alpha = \frac{3}{10}, \beta = \frac{1}{2}, p = 5, M = 4$ *tels que*

$$H(5, 4, \frac{3}{10}) = (\cdot 4222, -1), H(5, 4, \frac{1}{2}) = (\cdot 3222, 0)$$

Remarquons que les exposants sont différents, donc nous devons normaliser le code qui a le plus grand exposant

$$(\cdot 3222, 0) \longrightarrow (\cdot 0322, -1)$$

On fait l'addition entre les mantisses

$$\begin{aligned}
\gamma_0 &\equiv a_0 + b_0 = 4 + 0 \equiv 4 \bmod 5, r_0 = \left[\frac{a_0 + b_0}{5}\right] = \left[\frac{4+0}{5}\right] = 0 \\
\gamma_1 &\equiv a_1 + b_1 + r_0 = 2 + 3 + 0 \equiv 0 \bmod 5, r_1 = \left[\frac{a_1 + b_1 + r_0}{5}\right] = \left[\frac{2+3+0}{5}\right] = 1 \\
\gamma_2 &\equiv a_2 + b_2 + r_1 = 2 + 2 + 1 \equiv 0 \bmod 5, r_2 = \left[\frac{a_2 + b_2 + r_1}{5}\right] = \left[\frac{2+2+1}{5}\right] = 1 \\
\gamma_3 &\equiv a_3 + b_3 + r_2 = 2 + 2 + 1 \equiv 0 \bmod 5
\end{aligned}$$

C'est à dire $\gamma_0 = 4, \gamma_1 = 0, \gamma_2 = 0, \gamma_3 = 0$. *Ceci est équivalent à*

$$\begin{array}{cccccccc} + & \cdot & 4 & 2 & 2 & 2 & , & -1 \\ = & \cdot & 0 & 3 & 2 & 2 & , & -1 \\ \hline & \cdot & 4 & 0 & 0 & 0 & , & -1 \end{array}$$

On obtient $H(5, 4, \frac{3}{10}) + H(5, 4, \frac{1}{2}) = (\cdot 4000, -1) = H(5, 4, \frac{4}{5})$.

3.2.2 La Soustraction (recherche des opposés) :

Tout nombre p-adique A possède un unique opposé B tel que $A+B = 0$. Pour faire la soustraction $H(p, M, \alpha) - H(p, M, \beta)$ où α, β sont deux nombres p-adiques, en utilisant "l' addition complétée". C'est-à-dire, on calcule le code $H(p, M, -\beta)$, puis on fait l'addition comme dans le cas précédent (au lieu d'effectuer $A - B$, on fait $A + (-B)$).

$$H(p, M, \alpha) - H(p, M, \beta) = H(p, M, \alpha) + H(p, M, -\beta) = (mant_\alpha, \exp_\alpha) + (mant_{-\beta}, \exp_{-\beta})$$

Trouvons $H(p, M, -\beta)$. Pour cela, on pose

$$A = mant_\beta = \cdot b_0 b_1 ... b_{M-1}, B = mant_{-\beta} = \cdot b'_0 b'_1 ... b'_{M-1}$$

On obtient

$$A + B = 0 \Longleftrightarrow \begin{cases} b_0 + b'_0 = p, b'_0 = p - b_0 \\ b_1 + b'_1 + 1 = p, b'_1 = p - 1 - b_1 \\ \vdots \\ b_{M-1} + b'_{M-1} + 1 = p, b'_{M-1} = p - 1 - b_{M-1} \end{cases}$$

Alors

$$\forall i = \overline{1, M-1} : \begin{cases} b'_0 = p - b_0 \\ b'_i = (p-1) - b_i \end{cases} \tag{3.1}$$

Par cette formule, on trouve que -1 est $-1 = \cdot (p-1)(p-1)(p-1)...(p-1)$.

Exemple 3.2.4 *Calculons la soustraction suivante* $\frac{3}{4} - \frac{3}{2}, p = 5, M = 4$. *On a*

$$H(5, 4, \frac{3}{4}) = (\cdot 2111, 0), H(5, 4, \frac{3}{2}) = (\cdot 4222, 0)$$

On remarque que les exposants sont égaux.

Alors d'après (3.1)*, on obtient* $H(5,4,\frac{-3}{2}) = (\cdot 1222, 0)$ *et*

$$H(5,4,\frac{3}{4}) - H(5,4,\frac{3}{2}) = H(5,4,\frac{3}{4}) + H(5,4,\frac{-3}{2}) = (\cdot 2111,0) + (\cdot 1222,0) = (\cdot 3333,0) = H(5,4,\frac{-3}{4})$$

3.2.3 Multiplication des nombres p-adiques :

Par définition, la multiplication est une opération produit associant à deux nombres, l'un appelé multiplicande, l'autre multiplicateur, un troisième nombre appelé produit. La multiplication de deux nombres p-adique se fait suivant la technique habituelle de la multiplication de deux nombres entiers, comme on sait le faire habituellement. Pour faire la multiplication, on multiplie les mantisses et on additionne les exposants. En effet, si $\alpha_1 = p^{m_1}.u_1$, $\alpha_2 = p^{m_2}.u_2 \in \mathbb{Q}_p$, alors

$$\alpha_1.\alpha_2 = p^{m_1}.p^{m_2}.u_1u_2 = p^{(m_1+m_2)}.u_3$$

D'autre part, soient $H(p,M,\alpha_1) = (\cdot a_0a_1...a_{M-1}, m_1)$, $H(p,M,\alpha_2) = (\cdot b_0b_1...b_{M-1}, m_2)$. Alors

$$H(p,M,\alpha_3) = H(p,M,\alpha_1).H(p,M,\alpha_2) = (\cdot s_0s_1...s_{M-1}, m_1+m_2)$$

Le tableau (la grille de multiplication) suivant donne la multiplication dans $H_{p,M}$:

$$\begin{array}{cccccccccccc}
* & \cdot & a_0 & a_1 & a_2 & a_3 & . & . & . & . & . & a_{M-1} \\
= & \cdot & b_0 & b_1 & b_2 & b_3 & . & . & . & . & . & b_{M-1} \\
 & & P_{0,0} & P_{0,1} & P_{0,2} & P_{0,3} & . & . & . & . & . & P_{0,M-1} \\
 & & & P_{1,0} & P_{1,1} & P_{1,2} & . & . & . & . & . & P_{1,M-2} \\
 & & & & P_{2,0} & P_{2,1} & . & . & . & . & . & P_{2,M-3} \\
 & & & & & P_{3,0} & . & . & . & . & . & P_{3,M-4} \\
 & & & & & & . & . & . & . & . & . \\
 & & & & & & & . & . & . & . & . \\
 & & & & & & & & . & . & . & . \\
 & & & & & & & & & . & . & . \\
 & & & & & & & & & & . & . \\
 & & & & & & & & & & & P_{M-1,0} \\
= & \cdot & s_0 & s_1 & s_2 & s_3 & . & . & . & . & . & s_{M-1}
\end{array}$$

tels que ($P_{i,j} = b_i a_j$ sont les produits croisés) définis par

$$\begin{aligned}
&P_{0,0} \equiv b_0.a_0 \bmod p, r_{0,0} = \left[\tfrac{b_0.a_0}{p}\right] \\
&P_{0,1} \equiv b_0.a_1 + r_{0,0} \bmod p, r_{0,1} = \left[\tfrac{b_0.a_1+r_{0,0}}{p}\right] \\
&P_{0,2} \equiv b_0.a_2 + r_{0,1} \bmod p, r_{0,2} = \left[\tfrac{b_0.a_2+r_{0,1}}{p}\right] \\
&\vdots \\
&P_{0,M-1} \equiv b_0.a_{M-1} + r_{0,M-2} \bmod p, r_{0,M-2} = \left[\tfrac{b_0.a_{M-2}+r_{0,M-3}}{p}\right]
\end{aligned}$$

On écrit

$$\forall j = \overline{1, M-1} : \begin{cases} P_{0,0} \equiv b_0.a_0 \bmod p, r_{0,0} = \left[\tfrac{b_0.a_0}{p}\right] \\ P_{0,j} \equiv b_0.a_j + r_{0,j-1} \bmod p, r_{0,j} = \left[\tfrac{b_0.a_j+r_{0,j-1}}{p}\right] \end{cases}$$

et

$$\begin{aligned}
&P_{1,0} \equiv b_1.a_0 \bmod p, r_{1,0} = \left[\tfrac{b_1.a_0}{p}\right] \\
&P_{1,1} \equiv b_1.a_1 + r_{1,0} \bmod p, r_{1,1} = \left[\tfrac{b_1.a_1+r_{1,0}}{p}\right] \\
&P_{1,2} \equiv b_1.a_2 + r_{1,1} \bmod p, r_{1,2} = \left[\tfrac{b_1.a_2+r_{1,1}}{p}\right] \\
&\vdots \\
&P_{1,M-2} \equiv b_1.a_{M-2} + r_{1,M-3} \bmod p, r_{1,M-3} = \left[\tfrac{b_1.a_{M-3}+r_{1,M-4}}{p}\right]
\end{aligned}$$

On écrit

$$\forall j = \overline{1, M-2} : \begin{cases} P_{1,0} \equiv b_1.a_0 \bmod p, r_{1,0} = \left[\tfrac{b_1.a_0}{p}\right] \\ P_{1,j} \equiv b_1.a_j + r_{1,j-1} \bmod p, r_{1,j} = \left[\tfrac{b_1.a_j+r_{1,j-1}}{p}\right] \end{cases}$$

et ainsi de suite.
D'autre part, on pose

$$\begin{aligned}
&s_0 \equiv P_{0,0} \bmod p, r_0 = 0 \\
&s_1 \equiv P_{0,1} + P_{1,0} \bmod p, r_1 = \left[\tfrac{P_{0,1}+P_{1,0}}{p}\right] \\
&s_2 \equiv P_{0,2} + P_{1,1} + P_{2,0} + r_1 \bmod p, r_2 = \left[\tfrac{P_{0,2}+P_{1,1}+P_{2,0}+r_1}{p}\right] \\
&\vdots \\
&s_{M-1} = P_{0,M-1} + P_{1,M-2} + ... + P_{M-1,0} + r_{M-2} \bmod p, r_{M-2} = \left[\tfrac{P_{0,M-2}+P_{1,M-3}+...+P_{M-2,0}+r_{M-3}}{p}\right]
\end{aligned}$$

Exemple 3.2.5 *Soient* $H(5, 4, \frac{4}{15}) = (\cdot a_0 a_1 a_2 a_3) = (\cdot 3313, -1)$ *et* $H(5, 4, \frac{5}{2}) = (\cdot b_0 b_1 b_2 b_3)(\cdot 3222, 1)$.

Alors

$$\begin{array}{cccccc} * & \cdot & 3 & 3 & 1 & 3 \\ = & \cdot & 3 & 2 & 2 & 2 \\ & & P_{0,0} & P_{0,1} & P_{0,2} & P_{0,3} \\ & & & P_{1,0} & P_{1,1} & P_{1,2} \\ & & & & P_{2,0} & P_{2,1} \\ & & & & & P_{3,0} \\ \\ = & \cdot & s_0 & s_1 & s_2 & s_3 \end{array}$$

La première étape

$$\begin{array}{l} P_{0,0} \equiv b_0.a_0 = 3 \times 3 \equiv 4 \bmod 5, r_{0,0} = \left[\frac{b_0.a_0}{5}\right] = \left[\frac{3\times 3}{5}\right] = 1 \\ P_{0,1} \equiv b_0.a_1 + r_{0,0} = 3 \times 3 + 1 \equiv 0 \bmod 5, r_{0,1} = \left[\frac{b_0.a_1 + r_{0,0}}{5}\right] = \left[\frac{3\times 3+1}{5}\right] = 2 \\ P_{0,2} \equiv b_0.a_2 + r_{0,1} = 3 \times 1 + 2 \equiv 0 \bmod 5, r_{0,2} = \left[\frac{b_0.a_2 + r_{0,1}}{5}\right] = \left[\frac{3\times 1+2}{5}\right] = 1 \\ P_{0,3} \equiv b_0.a_3 + r_{0,2} = 3 \times 3 + 1 \equiv 0 \bmod 5 \end{array}$$

La deuxième étape

$$\begin{array}{l} P_{1,0} \equiv b_1.a_0 = 2 \times 3 \equiv 1 \bmod 5, r_{1,0} = \left[\frac{b_1.a_0}{5}\right] = \left[\frac{6}{5}\right] = 1 \\ P_{1,1} \equiv b_1.a_1 + r_{1,0} = 2 \times 3 + 1 \equiv 2 \bmod 5, r_{1,1} = \left[\frac{b_1.a_1 + r_{1,0}}{5}\right] = \left[\frac{2\times 3+1}{5}\right] = 1 \\ P_{1,2} \equiv b_1.a_2 + r_{1,1} = 2 \times 1 + 1 \equiv 3 \bmod 5, r_{1,2} = \left[\frac{b_1.a_2 + r_{1,1}}{5}\right] = \left[\frac{3}{5}\right] = 0 \end{array}$$

La troisième étape

$$\begin{array}{l} P_{2,0} \equiv b_2.a_0 = 2 \times 3 \equiv 1 \bmod 5, r_{2,0} = \left[\frac{b_2.a_0}{5}\right] = \left[\frac{6}{5}\right] = 1 \\ P_{2,1} \equiv b_2.a_1 + r_{2,0} = 2 \times 3 + 1 \equiv 2 \bmod 5 \end{array}$$

La quatrième étape

$$P_{3,0} \equiv b_3.a_0 = 2 \times 3 \equiv 1 \bmod 5$$

On obtient

$$\begin{array}{l} s_0 \equiv P_{0,0} \equiv 4 \bmod 5, r_0 = 0 \\ s_1 \equiv P_{0,1} + P_{1,0} = 0 + 1 \equiv 1 \bmod 5, r_1 = \left[\frac{P_{0,1}+P_{1,0}}{p}\right] = \left[\frac{0+1}{5}\right] = 0 \\ s_2 \equiv P_{0,2} + P_{1,1} + P_{2,0} + r_1 = 0 + 2 + 1 + 0 \equiv 3 \bmod 5, r_2 = \left[\frac{P_{0,2}+P_{1,1}+P_{2,0}+r_1}{p}\right] = \left[\frac{0+2+1+0}{5}\right] = 0 \\ s_3 \equiv P_{0,3} + P_{1,2} + P_{2,1} + P_{3,0} + r_2 = 0 + 3 + 2 + 1 + 0 \equiv 1 \bmod 5 \end{array}$$

Alors

$$\begin{array}{cccccccc} * & \cdot & 3 & 3 & 1 & 3 & , & -1 \\ = & \cdot & 3 & 2 & 2 & 2 & , & +1 \\ + & & 4 & 0 & 0 & 0 & & \\ & & & 1 & 2 & 3 & & \\ & & & & 1 & 2 & & \\ & & & & & 1 & & \\ = & \cdot & 4 & 1 & 3 & 1 & , & 0 \end{array}$$

On obtient $H(5,4,\frac{4}{15}.\frac{5}{2}) = H(5,4,\frac{2}{3}) = (\cdot 4131, 0)$.

3.2.4 La Division :

L'opération de la division est similaire à l'opération de la multiplication car diviser par un nombre A, revient à multiplier par son inverse. Pour effectuer la division entre deux nombres p-adiques A et B , on trouve l'inverse de B modulo p^M, en suite on fait la multiplication comme dans le cas précédent. Si le nombre p-adique A admet un inverse B, alors B est unique et $A.B = 1$.

Pour effectuer la division nous devons diviser les mantisses et soustraire les exposants de ces codes.
Soient $\alpha_1 = p^{m_1}.u_1, \alpha_2 = p^{m_2}.u_2 \in \mathbb{Q}_p$. Alors $\frac{\alpha_1}{\alpha_2} = \frac{p^{m_1}.u_1}{p^{m_2}.u_2} = p^{m_1-m_2}.\frac{u_1}{u_2}$.
Supposons que

$$H(p,M,\alpha_1) = (\cdot c_0c_1...c_{M-1}, m_1)$$
$$H(p,M,\alpha_2) = (\cdot a_0a_1...a_{M-1}, m_2), \;\; a_0 \neq 0$$

Donc $H(p,M,\alpha_3 = \frac{\alpha_1}{\alpha_2}) = (\cdot t_0t_1...t_{M-1}, m_1 - m_2)$ où $\cdot t_0t_1...t_{M-1} = \frac{\cdot c_0c_1...c_{M-1}}{\cdot a_0a_1...a_{M-1}}$.
D'autre part, on a $\alpha_3 = \frac{\alpha_1}{\alpha_2} = \alpha_1.\alpha_2^{-1}$. Supposons que $\alpha_2^{-1} = \cdot b_0b_1...b_{M-1}$. Alors

$$\alpha_2.\alpha_2^{-1} = 1 \Longleftrightarrow (\cdot a_0a_1...a_{M-1}).(\cdot b_0b_1...b_{M-1}) = \cdot 100...0$$

D'après la formule de multiplication, on trouve

$$\begin{array}{l} s_0 \equiv P_{0,0} \equiv 1 \bmod p, r_0 = 0 \\ s_1 \equiv P_{0,1} + P_{1,0} \equiv 0 \bmod p, r_1 = \left[\frac{P_{0,1}+P_{1,0}}{p}\right] \\ s_2 \equiv P_{0,2} + P_{1,1} + P_{2,0} + r_1 \equiv 0 \bmod p, r_2 = \left[\frac{P_{0,2}+P_{1,1}+P_{2,0}+r_1}{p}\right] \\ \vdots \\ s_{M-1} = P_{0,M-1} + P_{1,M-2} + ... + P_{M-1,0} + r_{M-2} \equiv 0 \bmod p, r_{M-2} = \left[\frac{P_{0,M-2}+P_{1,M-3}+...+P_{M-2,0}+r_{M-3}}{p}\right] \end{array}$$

Exemple 3.2.6 *Soient* $H(7,4,A) = (\cdot 3221, 0)$. *On va trouver l'inverse de* A *dans le corps*

$\mathbb{Q}_7$.
Pour cela, on pose

$$H(7,4,A) = (\cdot 3221, 0) = (\cdot a_0a_1a_2a_3, 0), H(7,4,A^{-1}) = (\cdot b_0b_1b_2b_3, 0)$$

Où $b_0, b_1, b_2, b_3 \in \{0,1,2,3,4,5,6\}$. *Alors*

$$\begin{aligned} A.A^{-1} &= 1 \Longleftrightarrow (\cdot a_0a_1a_2a_3) \times (\cdot b_0b_1b_2b_3) = \cdot 1000 \\ &\Longrightarrow \cdot 3221 \times \cdot b_0b_1b_2b_3 = \cdot 1000 \end{aligned}$$

On écrit

$*$	$\cdot$	3	2	2	1
$=$	$\cdot$	b_0	b_1	b_2	b_3
		$3b_0$	$2b_0$	$2b_0$	b_0
			$3b_1$	$2b_1$	$2b_1$
				$3b_2$	$2b_2$
					$3b_3$

$$3b_0 \quad 2b_0 + 3b_1 + r_1 \quad 2b_0 + 2b_1 + 3b_2 + r_2 \quad b_0 + 2b_1 + 2b_2 + 3b_3 + r_3$$

On obtient

$$\begin{aligned} &3b_0 \equiv 1 \bmod 7 \\ &2b_0 + 3b_1 + r_1 \equiv 0 \bmod 7, r_1 = \left[\tfrac{3b_0}{7}\right] \\ &2b_0 + 2b_1 + 3b_2 + r_2 \equiv 0 \bmod 7, r_2 = \left[\tfrac{2b_0+3b_1+r_1}{7}\right] \\ &b_0 + 2b_1 + 2b_2 + 3b_3 + r_3 \equiv 0 \bmod 7, r_3 = \left[\tfrac{2b_0+2b_1+3b_2+r_2}{7}\right] \end{aligned}$$

On trouve

$$\begin{aligned} &b_0 = 5, r_1 = \left[\tfrac{15}{7}\right] = 2 \\ &12 + 3b_1 \equiv 0 \bmod 7 \Longrightarrow 5 + 3b_1 \equiv 0 \bmod 7 \Longrightarrow b_1 = 3 \\ &r_2 = \left[\tfrac{21}{7}\right] = 3 \\ &19 + 3b_2 \equiv 0 \bmod 7 \Longrightarrow 5 + 3b_2 \equiv 0 \bmod 7 \Longrightarrow b_2 = 3 \\ &r_3 = \left[\tfrac{28}{7}\right] = 4 \\ &21 + 3b_3 \equiv 0 \bmod 7 \Longrightarrow 3b_3 \equiv 0 \bmod 7 \Longrightarrow b_3 = 0 \end{aligned}$$

Ce qui donne

$$H(7,4,A^{-1}) = (\cdot b_0b_1b_2b_3, 0) = \cdot 5330$$

Bibliographie

[1] A.J. Baker, *An Introduction to p-adic Numbers and p-adic Analysis*. Department of Mathematics, University of Glasgow, Scotland (2004).

[2] B. Diarra, *Analyse p-adique. Cours DEA- Algèbre Commutative FAST*. Université du Mali. Décembre 1999- Mars (2000).

[3] C. Berger, *Topologie pour la Licence*. Université de Nice-Sophia Antipolis, Laboratoire J.-A. Dieudonné, 06108 Nice Cedex (2004).

[4] C. K. Koc, *A Tutorial on P-adic Arithmetic*. Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon 97331. Technical Report (2002).

[5] F. B. Vej, *P-adic Numbers*. Aalborg University, Department Of Mathematical Sciences. 7E 9222 Aalborg Øst. Groupe E3-104 (2000).

[6] F.Q. Gouvéa, *P-adic Numbers : An Introduction.* Second Edition. New York : Springer-Verlag, (1997).

[7] G. Christol, A. Cot, C. M Marle, *Topologie, Mathématiques pour le deuxième cycle.* Ellipses (1997).

[8] J.P Bézivin, *Dynamique des fractions rationnelles p-adiques*. Université de Caen (2005).

[9] S. Katok : *Real and p-adic analysis.* Course notes for Math 497C, Mass Program, Fall 2000
(2001).

[10] W.H. Schiko, *Ultrametric Calculus*, *An Introduction to p-adic Analysis*, Cambridge Studies in Adv. Math. 4, Cambridge University Press, (1984).

[11] Y. Amice, *Les nombres p-adiques*. Presses universitaires de France (1975).