ⵜⴰⴳⵍⴷⵉⵜ ⵜⴰⵎⴰⵣⵉⵖⵜ ⵜⴰⵣⵣⴰⵢⵔⵉⵜ ⵜⴰⵏⴰⵙⵙⵉⵔⵜ ⵜⴰⵏⴰⵎⵓⵔⵜ
République Algérienne Démocratique et Populaire
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵏⵜⵣⵣⵍⵎⴷ ⵜⴰⵙⵙⵏⵜⵉⵔⵜ ⵏⵜⵣⵣⵍⵎⴷ ⵜⵎⵓⵔⵜ
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire

Abd elhafid Boussouf Mila

Institut des Sciences et de la Technologie **Département de Mathématiques et Informatique**

Mémoire préparé en vue de l'obtention du diplôme de Master

En: Mathématiques

Spécialité: Mathématiques fondamentales et appliquées

Application des méthodes numériques dans un espace ultramétrique

Préparé par

- **Kecita Rima**
- **Kheloufi Radia**

Soutenue devant le jury

-**Encadré par**: *Kecies Mohamed*……*M.A.A*

- Président *:* *Kaouche Ismail* ……*M.A.A*

- Examinateur *:* *Boudjerida Najet*……*M.A.A*

Année Universitaire: 2015/2016

Remerciements

Nous remercions d'abord et avant tout le bon Dieu qui m'a

donné le courage et la patience pour réaliser ce travail.

Nous remercions vivement monsieur M.Kecies et

assurer d'avoir voulu proposes la direction

de ce mémoire sa disponibilité,son soutien

ses encouragements et ses précieux

conseils tout au long de ce travail.

Sans oublier tous les enseignants qui

ont contribué a notre formation durant notre

vie scolaire surtout les enseignant de l'institut (S- T).

Nous voudrons dire toute notre reconnaissance à nos parents pour

leur dévouement sans limite et pour tout ce qu'ils nous ont donné sur

tous les plants, et remercier nos familles et nos amis pour leur soutien constant.

RADIA & RIMA

Dédicace

Je remercie dieu qui a toujours était à mais côtes.Je dédie cet humble travail :

A mon père Eltahar(Allah yarahmo), et à ma mère

Khadidja qui ma donné la tendresse et l'amour.

A tous mes frères Adel,Soufiane,Daoud.

A mes soeurs Sabrina,Fatima.

Et ma petit ameur : Anes,

Islam,Sohaib

A mon binome : Rima.

A mes amies qui vivaient avec moi des

périodes tant activement que passivement sur tout :

Mariam,Imen,Nihad,Nassima,Rahma,Hakima,Khalida,Rokai,Hada,

Kanza,Amira,karima,Sihame,Khawla,Sara,Souad,Amani,Ibtisam, et d'autres.

RADIA

Dédicace

Je dédie ce modeste travail en signe de reconnaissance et derespect :

A mon exemplaire, mon chère père Mohamed.

A ma source de tendresse, ma chére mère Fatiha.

A mes fréres : Farouk et Yacine

A ma soeur : Faiza

A mon espoire et ma soeur : Salsabil.

A ma chère tante : Samira

A mon binome : Radia

A mes amies qui vivaient avec moi des périodes tant

activement que passivement surtout : Hadjer,Hakima,Rahma,

Nassima,Rokia,Karima,Kanza,Hanan(hada),Amira,khawla,Sihame,Mariam et d'autres.

RIMA

Table des matières

Introduction Générale

L'apparition des nombres p-adiques remonte à la fin du dix-neuvième siècle grâce au mathématicien Allemand Kurt Hensel (1861,1941) qui a tenté de remplacer le complété $\mathbb{R}$ du corps des nombres rationnels par un autre complété noté $\mathbb{Q}_p$, où la norme cette fois, est une norme non archimédienne définie à l'aide du nombre premier p. Depuis ce temps-là, les mathématiciens ont commencé à s'intéresser à ce nouveau domaine de mathématiques. Les recherches dans ce domaine sont souvent faites, soit pour voir les différences et les similitudes par rapport au cas réel, soit pour obtenir des résultats propres aux nombres p-adiques. 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.

L'application des nombres p-adiques et de l'analyse p-adique qui nous intéresse dans ce travail est penchée vers l'informatique. Il s'agit, dans ce travail, d'une application intéressante des outils de l'analyse numérique à la théorie des nombres. On verra comment utiliser les méthodes numériques de bases (Newton, sécante, point fixe) pour calculer le zéro d'une fonction f où

$$\begin{cases} f(x) = \frac{1}{x} - a = 0 \\ a \in \mathbb{Q}_p^* \ , p\text{-premier} \end{cases} \tag{1}$$

Nous avons basé dans ce mémoire sur les travaux de Michael P. Knapp, Christos Xenophontos, où les auteurs ont utilisé les méthodes numériques élémentaires pour trouver le réciproque d'un entier modulo p^n (voir [7] pour plus de détails).

Ce mémoire est composé de l'introduction et trois chapitres. Dans l'introduction, on donne un aperçu historique sur les nombres p-adiques et leur évolution. Dans le premier chapitre, nous donnons quelques notions fondamentales, en particulier, la définition des corps normés ultramétriques, la procédure de complétion pour construire les corps complets.

Dans le deuxième chapitre, il est question de présenter des notions de base de l'analyse p-adique et de théorie des nombres p-adiques. Ils servent comme outils nécessaires au

reste du travail.

Dans le dernier chapitre, principal dans ce mémoire, il est question de calculer le développement de Hensel (les premiers chiffres) de l'inverse d'un nombre p-adique par les méthodes numériques élémentaires, telles que la méthode de Newton, la méthode de la sécante et du point fixe. Autrement dit, chercher l'écriture

$$\frac{1}{a} = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_n p^n + ..., a \in \mathbb{Q}_p^*$$

On termine ce mémoire par une conclusion générale.

Chapitre 1

Corps valués ultramétriques complets

Dans ce chapitre, nous allons donner des notions fondamentales sur les corps normés ultramétriques.

En, mathématiques, un espace métrique M est dit espace complet si toute suite de Cauchy de M a une limite dans M (c'est-à-dire qu'elle converge dans M). La propriété de complétude dépend de la distance. Il est donc important de toujours préciser la distance que l'on prend quand on parle d'espace complet et le procédé de complétion est valable pour un espace métrique quelconque.

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 a dire une norme qui vérifie une condition plus forte que l'inégalité triangulaire.
3. *Une norme constante $||.||$ est dite triviale si et seulement si*

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

Remarque 1.1.1
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* $(R_+^*, .)$ *et donc que* $||1|| = 1$.

Exemple 1.1.1 *La valeur absolue usuelle* $|.|$ *est une norme archimédienne sur* $\mathbb{R}$. *Car*

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

Définition 1.1.2

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 archimèdienne.*

Proposition 1.1.1 *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.
1) Soit K un corps ultramétrique. 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

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

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

$$\begin{aligned}
\left\|(x+y)^n\right\| &= \left\|\sum_{k=0}^{n} C_n^k \cdot x^k \cdot y^{n-k}\right\| \\
&\leq \sum_{k=0}^{n} C_n^k \cdot \left\|x^k\right\| \cdot \left\|y^{n-k}\right\| \\
&\leq \sum_{k=0}^{n} \left\|C_n^k\right\| \cdot \|x\|^k \cdot \left\|y\right\|^{n-k} \quad \text{,avec } \left\|C_n^k\right\| \leq 1 \\
&\leq \sum_{k=0}^{n} \|x\|^k \cdot \left\|y\right\|^{n-k}
\end{aligned}$$

D'autre part, on a

$$\begin{aligned}
\|x\| &\leq \max\left(\|x\|, \left\|y\right\|\right) \\
\left\|y\right\| &\leq \max\left(\|x\|, \left\|y\right\|\right)
\end{aligned}$$

Donc

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

On obtient

$$\begin{aligned}
\forall 0 \leq k \leq n : \quad \|x\|^k \cdot \left\|y\right\|^{n-k} &\leq \left[\max\left(\|x\|, \left\|y\right\|\right)\right]^k \cdot \left[\max\left(\|x\|, \left\|y\right\|\right)\right]^{n-k} \\
&\leq \left[\max\left(\|x\|, \left\|y\right\|\right)\right]^n
\end{aligned}$$

Ce qui donne

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

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

Proposition 1.1.2 *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

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

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 1.1.3 *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 $\lim_{n,m\to\infty} ||x_n - x_m|| = 0$.

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 1.1.2 *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.*

Exemple 1.2.1 *Les nombres rationnels ne forment pas un espace complet. Car si on considère la suite $(x_n)_n$ définie par*

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

$(x_n)_n$ 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 1.2.2 ***(Définition générale de la complétion)***
Soit K un corps normé arbitraire (non complet) muni d'une norme $\|.\|_K$ et $\hat{K}$ un autre corps normé (construit à partir de K) muni d'une norme $\|.\|_{\hat{K}}$. On dit que $\hat{K}$ est le complété de K si

1) $\hat{K}$ contient $K(K \subset \hat{K})$.

2) K est dense dans $\hat{K}$ par rapport à la topologie associé avec $\|.\|_{\hat{K}}$.

3) $\forall x \in K : \|x\|_K = \|x\|_{\hat{K}}$ (la norme $\|.\|_{\hat{K}}$ est définie à partir de $\|.\|_K$).

4) $(\hat{K}, \|.\|_{\hat{K}})$ 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*

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

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

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

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

L'ensemble $(SC(K), +, \cdot)$ est un anneau unitaire, d'élément neutre $1_{SC(K)} = \{1\}_{n \in \mathbb{N}} = \{1, 1, 1, \ldots, 1, \ldots\}$(resp : $0_{SC(K)} = \{0\}_{n \in \mathbb{N}} = \{0, 0, 0, \ldots, 0, \ldots\}$) 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 $K^{\mathbb{N}}$.
En effet, si $A = \{a_n\}_n, B = \{b_n\}_n \in SC(K)$ et $n, m \in \mathbb{N}$, alors

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

Ainsi

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

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

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

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

D'autre part, on a

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

Ainsi

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

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

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

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

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

3)Etape 3 : *On définit sur* $SC(K)$ *une relation* $\mathfrak{R}$ *par*

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

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

$$\lim_{n\to\infty} ||a_n - a_n||_K = 0 \Longrightarrow \{a_n\}_n \mathfrak{R} \{a_n\}_n \text{ (réflexivité)}$$

D'autre part

$$\begin{aligned} \{a_n\}_n \mathfrak{R} \{b_n\}_n &\Longleftrightarrow \lim_{n\to\infty} ||a_n - b_n||_K = 0 \\ &\Longrightarrow \lim_{n\to\infty} ||b_n - a_n||_K = 0 \\ &\Longrightarrow \{b_n\}_n \mathfrak{R} \{a_n\}_n \text{ (symétrie)} \end{aligned}$$

On a

$$\begin{cases} \{a_n\}_n \mathfrak{R} \{b_n\}_n \\ \\ \{b_n\}_n \mathfrak{R} \{c_n\}_n \end{cases} \Longleftrightarrow \begin{cases} \lim_{n\to\infty} ||a_n - b_n||_K = 0 \\ \\ \lim_{n\to\infty} ||b_n - c_n||_K = 0 \end{cases}$$

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* $\lim_{n\to\infty} ||a_n - c_n||_K = 0$. *Donc*

$$\{a_n\}_n \mathfrak{R} \{c_n\}_n \text{(transitivité)}$$

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

$$\{a_n\}_{n\in\mathbb{N}} = \{a, a, a, \cdots\}, a \in K$$

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* $(a_n) \in \hat{K}$*, et nous allons considérer K comme un sous ensemble de* $\hat{K}$*, et nous identifions* $a \in K$ *avec* $\hat{a} = (a) \in \hat{K}$*.*

Théorème 1.2.1 *L'ensemble quotient* $\hat{K} = SC(K)/SN(K)$ *est un corps.*

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

$$\forall \{a_n\}_{n\in\mathbb{N}} \in A \in \hat{K}, \forall \{b_n\}_{n\in\mathbb{N}} \in B \in \hat{K} : \quad \begin{array}{l} A + B = (a_n) + (b_n) = (a_n + b_n) \\ A \cdot B = (a_n) \cdot (b_n) = (a_n \cdot b_n) \end{array}$$

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

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

Soit $A \in \hat{K}$ tel que $A \neq \bar{0} = SN(K)$ 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

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

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

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

On trouve

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

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

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

Alors $A \cdot A^{-1} = \bar{1}$.

Définition 1.2.3 *Pour tout $A = (a_n) \in \hat{K}$, on définit l'application*

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

Proposition 1.2.1 *L'application $\|.\|_{\hat{K}}$ est une norme sur $\hat{K}$. 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 $\{a_n\}_n \in A \in \hat{K}$. 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

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

On obtient, pour tout $\varepsilon > 0, |\|a_m\|_K - \|a_n\|_K| \leq \varepsilon$.
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 $\lim\limits_{n\to+\infty} \|a_n\|_K$ existe.
Supposons que $\{a_n\}_n$ et $\{a_n^{\backprime}\}_n$ sont deux représentants de A. Alors par la même inégalité, nous avons

$$0 \leq \lim_{n\to+\infty} |\|a_n\|_K - \|a_n^{\backprime}\|_K| \leq \lim_{n\to+\infty} \|a_n - a_n^{\backprime}\|_K = 0$$

Alors $\lim\limits_{n\to+\infty} \|a_n\|_K = \lim\limits_{n\to+\infty} \|a_n^{\backprime}\|_K$.
On vérifie les trois propriétés de la norme :

1) Si $A = (a_n) \in \hat{K}$ telle que $A = 0$, alors

$$\begin{aligned} A = (a_n) = 0 &\Longleftrightarrow \{a_n\}_{n\in\mathbb{N}} \in SN(K) \\ &\Longleftrightarrow \lim_{n\to+\infty} \|a_n\|_K = 0 \\ &\Longleftrightarrow \|A\|_{\hat{K}} = 0 \end{aligned}$$

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

$$\begin{aligned} &\exists c \in \mathbb{R}_+^*, \exists N \in \mathbb{N}^* : \|a_n\|_K \geq c > 0, \forall n \geq N \\ &\Longrightarrow \lim_{n\to+\infty} \|a_n\|_K \neq 0 \\ &\Longrightarrow \|A\|_{\hat{K}} > 0 \end{aligned}$$

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

$$\begin{aligned} \|A \cdot B\|_{\hat{K}} &= \lim_{n\to+\infty} \|a_n b_n\|_K = \lim_{n\to+\infty} (\|a_n\|_K \cdot \|b_n\|_K) \\ &= \lim_{n\to+\infty} \|a_n\|_K \cdot \lim_{n\to+\infty} \|b_n\|_K = \|A\|_{\hat{K}} \cdot \|B\|_{\hat{K}} \end{aligned}$$

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

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

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

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

Lemme 1.2.1 *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 $b \neq \lim_{n\to+\infty} a_n$. 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

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

D'autre part, on a

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

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

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

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

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 $\{a_n\}$ est de Cauchy dans K, 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 $\|\ .\ \|_{\hat{K}}$ est non-archimèdienne :
Soient $A = (a_n)_n, B = (b_n)_n \in \hat{K}$ telle que $A \neq B$. Supposons que les deux suites ne sont pas nulles ($b = 0$), d'après le lemme (1.2.1), on obtient

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

Soit $N = \max(N_1, N_2)$. Alors d'après (1,1) et $\|.\|_K$ est ultramétrique, on trouve

$$\|a_n + b_n\|_K \leq \max(\|a_n\|_K, \|b_n\|_K) = \max(\|A\|_{\hat{K}}, \|B\|_{\hat{K}})$$

Donc

$$\begin{aligned} \lim_{n\to+\infty} \|a_n + b_n\|_K &\leq \max(\|A\|_{\hat{K}}, \|B\|_{\hat{K}}) \\ \Longrightarrow \|A + B\|_{\hat{K}} &\leq \max(\|A\|_{\hat{K}}, \|B\|_{\hat{K}}) \end{aligned}$$

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

Théorème 1.2.2 *L'espace $\hat{K}$ muni de la norme $\|.\|_{\hat{K}}$ est complet. De plus K est un sous-ensemble dense dans $\hat{K}$.*

Preuve.

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

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

Soit $A \in \hat{K}$ 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

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

Il vient que K est dense dans $\hat{K}$.

2) **Montrons que $(\hat{K}, \|.\|_{\hat{K}})$ est complet.**
C'est-à-dire toute suites de Cauchy de $\hat{K}$ est convergente dans $\hat{K}$.
Soit $\{A_n\}_{n\in\mathbb{N}} = \{A_1, A_2, \ldots\}$ une suite de Cauchy dans $\hat{K}$, d'après la densité de K dans $\hat{K}$, alors pour tout A_n il existe un élément $a_n \in K$ tel que

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

Donc $\{A_n - (\bar{a}_n)\}_{n\in\mathbb{N}}$ est une suite nulle, d'où elle est de Cauchy dans $\hat{K}$.
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 $\hat{K}$, et comme tous ses éléments appartiennent à K, alors $\{a_n\}_{n\in\mathbb{N}}$ est de Cauchy dans K. On note A la classe d'équivalence de (a_n) ($A = (a_n) \in \hat{K}$).
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 $\hat{K}$. 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 $\hat{K}$, ce qui implique que $\lim\limits_{n\longrightarrow+\infty} \|A - A_n\|_{\hat{K}} = 0$. Il vient que $A = \lim\limits_{n\longrightarrow+\infty} A_n$.

Chapitre 2

Corps des nombres p-adiques

Dans ce chapitre nous allons présenter les différents concepts des corps de nombres p-adiques, en particulier ceux qui concernent la valuation p-adique, la norme p-adique, les entiers p-adiques, et quelques propriétés topologiques et analytiques.

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.*

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

Dans ce cas x s'écrit

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

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*

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

Remarque 2.1.1 *0 est divisible une infinité de fois par p, alors $v_p(0) = +\infty$.*

Exemple 2.1.1 *Soit $a \in \mathbb{Q}$. Alors*

1) *$a = p^2 + p^3 + 2p^4, v_p(a) = 2, \forall p \geq 2$.*

2) $a = 24 = 3.8, (3, 8) = 1, v_p(a) = 1$, *pour* $p = 3$.

3) $a = 14 = 2.7, (2, 7) = 1, v_p(a) = 1$, *pour* $p = 2$.

Proposition 2.1.1 *La valuation p-adique vérifie les propriétés suivantes :*

1) Si $x = \dfrac{a}{b} \in \mathbb{Q}^*$, *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 $x = \dfrac{a}{b} \in \mathbb{Q}^*$ telles que

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

Ce qui donne

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

Alors

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

2) Soient $x, y \in \mathbb{Q}$, alors

i) Si $x = 0$ ou $y = 0$, on a alors $x \cdot y = 0$, donc $v_p(x \cdot y) = +\infty$ et $v_p(x) + v_p(y) = +\infty$. D'où l'égalité.

ii) Si $x, y \in \mathbb{Q}^*$ telles que

$$x = c \cdot p^{v_p(x)}, (c, p) = 1$$
$$y = d \cdot p^{v_p(y)}, (d, p) = 1$$

On obtient

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

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

$$x = p^r \cdot \frac{a}{b}, v_p(x) = r, (a, p) = (b, p) = 1$$

$$y = p^s \cdot \frac{c}{d}, v_p(y) = s, (c, p) = (d, p) = 1$$

On obtient

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

Supposons que $s \geq r$, donc

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

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

$$\begin{array}{rcl} |.|_p : \mathbb{Q} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & |x|_p = \left\{ \begin{array}{ll} p^{-v_p(x)} & , si \quad x \neq 0 \\ 0 & , si \quad x = 0 \end{array} \right. \end{array}$$

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

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

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

Exemple 2.2.1 .

1) Pour $x = \dfrac{99}{140} = \dfrac{3^2 \times 11}{2^2 \times 5 \times 7} = 2^{-2} \times 5^{-1} \times 7^{-1} \times 3^2 \times 11 \in \mathbb{Q}$. 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) 0 est divisible une infinité de fois par p, donc on a $|0|_p = \dfrac{1}{+\infty} = 0$.

3) 1 n'est divisible aucune fois par p, donc $|1|_p = \dfrac{1}{p^0} = 1$.

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

$$d_5(252, 2) = |252 - 2|_5 = |250|_5 = |5^3.2|_5 = \frac{1}{5^3}$$

Proposition 2.2.1 *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

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

Remarque 2.2.1 *On peut définir sur le corps des nombres rationnels* $\mathbb{Q}$ *trois types de valeurs absolues :*
1) Valeur absolue triviale

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

2) Valeur absolue ordinaire

$$|x|_\infty = \max(x, -x) = \begin{cases} x \ , si\ x \geq 0 \\ \\ -x \ , si\ x < 0 \end{cases}$$

3) Valeur absolue p-adique $|.|_p$.

Proposition 2.2.2 *La norme p-adique définie sur* $\mathbb{Q}$ *prend ses images dans l'ensemble discret défini par*

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

Autrement dit

$$|\mathbb{Q}|_p = \{0\} \cup \{p^n : n \in \mathbb{Z}\}$$

Preuve. Soit $x \in \mathbb{Q}, x \neq 0$. Alors d'après la définition de la norme p-adique, on a

$$|\mathbb{Q}^*|_p \subset \{p^n : n \in \mathbb{Z}\}$$

D'autre part, pour tout $m \in \mathbb{Z}$, on a

$$p^m = p^{v_p(p^m)-v_p(1)} = \left|\frac{1}{p^m}\right|_p$$

Alors

$$\{p^n : n \in \mathbb{Z}\} \subset |\mathbb{Q}^*|_p$$

Remarque 2.2.2 *$\mathbb{Z}$ est un ensemble borné selon cette norme.*

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

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

Théorème 2.2.1 (*La formule du 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

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

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 2.2.2 *On a pour tout $p \notin \{2, 3, \infty\}$: $\left|\frac{3}{2}\right|_p = 1$, alors*

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

2.3 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 $(\mathbb{Q}, |.|_p)$ 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*

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

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

$$\Longrightarrow x_{n+1} - x_n \equiv 0 \bmod 7^n$$

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

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

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

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

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 2.3.1 *Soit p un nombre premier.*

1) *Le corps des nombres p-adiques est la complétion de l'espace métrique $(\mathbb{Q}, d_p)$. Ses éléments sont les classes d'équivalence des suites de Cauchy des nombres rationnels $\{a_n\}_n$ muni de la relation suivante*

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

2) *On prolonge la norme p-adique définie 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) est une suite de Cauchy d'éléments de $\mathbb{Q}$ qui représente le nombre p-adique a.

Remarque 2.3.1

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 ultramétrique.*

Lemme 2.3.1 *Soit $x \in \mathbb{Q}$ avec $|x|_p \leq 1$. Alors pour tout $n \in \mathbb{N}$, il existe un entier unique $\alpha \in \{0, 1, \ldots, p^n - 1\}$ 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. Or $|x|_p \leq 1$, alors

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

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

D'autre part, on pose $\alpha = a \cdot m_1$

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

Finalement, nous pouvons ajouter un multiple de p^n à α pour obtenir un entier entre 0 et p^n à l'aide de l'inégalité forte pour que $|\alpha - x|_p \leq p^{-n}$. En effet :

Soit

$$am_1 = \alpha + kp^n$$

Alors

$$\begin{aligned} |\alpha - x|_p &= \left|\alpha - \frac{a}{b}\right|_p \\ &= \left|am_1 - kp^n - \frac{a}{b}\right|_p \\ &= \left|-\frac{a}{b}(1 - m_1 b) - kp^n\right|_p \\ &= \left|\frac{a}{b}(1 - m_1 b) + kp^n\right|_p \\ &= \left|\frac{a}{b}.m_2 p^n + kp^n\right|_p \leq \max\left\{\left|\frac{a}{b}.m_2 p^n\right|_p, \left|kp^n\right|_p\right\} = \max\{p^{-n}, p^{-n}\} = p^{-n} \end{aligned}$$

Théorème 2.3.1 *(Théorème 1.4.3 [9]) 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*

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

Conclusion 2.3.1

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 $a = \sum_{k=n}^{\infty} \beta_k \cdot p^k$ où $\beta_k \in \{0, 1, 2, \ldots, p-1\}, n \in \mathbb{Z}$ sont appelés des digits (ou chiffres) et $|a|_p = p^{-n}$.*

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

$$\forall a \in \mathbb{Q}_p : [a] = \sum_{k=0}^{\infty} \beta_k p^k = \cdot\beta_0\beta_1\beta_2...$$

4) *On note par* $\langle a \rangle$ *la partie fractionnelle (irrégulière) de a, telle que*

$$\forall a \in \mathbb{Q}_p : \langle a \rangle = \sum_{n \leq k < 0} \beta_k p^k = \beta_n...\beta_{-3}\beta_{-2}\beta_{-1}\cdot$$

donc, on obtient la décomposition suivante

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

5) *On note par* $a = \beta_n\beta_{n+1}... \cdot \beta_0\beta_1 \ldots$ *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) $a = \beta_n\beta_{n+1} \ldots \beta_{-1} \cdot \beta_0\beta_1 \ldots$*, si* $n < 0$
   (b) $a = \cdot\beta_0\beta_1\beta_2 \ldots$*, si* $n = 0$
   (c) $a = \cdot 00 \ldots 0\beta_0\beta_1 \ldots$*, si* $n > 0$

Exemple 2.3.2 *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) *Développement formel de* -1 *en série de puissances de p :*
   On a

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

Par conséquent

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

Exemple 2.3.3 *On considère le développement p-adique suivant*

$$\begin{aligned} x &= 2 + 3p + p^2 + 3p^3 + p^4 + 3p^5 + ... \\ &= 2 + 3p(1 + p^2 + p^4 + ...) + p^2(1 + p^2 + p^4 + ...) \\ &= 2 + (3p + p^2)(1 + p^2 + p^4 + ...) \\ &= 2 + (3p + p^2).\frac{1}{1-p^2} \end{aligned}$$

En particulier pour $p = 5$*, on obtient* $x = \frac{1}{3} = \cdot 23131313...$

Proposition 2.3.1 *L'image de la norme p-adique sur $\mathbb{Q}_p^*$ est définie par*

$$\left|\mathbb{Q}_p^*\right|_p = \{p^n : n \in \mathbb{Z}\}$$

Preuve. Soient $x \in \mathbb{Q}_p, x \neq 0$ et $(x_n)_n \subset \mathbb{Q}$ une suite de nombres rationnels converge vers x selon la norme p-adique. Alors

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

Maintenant par la proposition (2.2.2), $|\mathbb{Q}|_p = \{0\} \cup \{p^n : n \in \mathbb{Z}\}$, donc $(|x_n|_p)_n$ doit converger à quelque élément dans

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

Or $x \neq 0$, alors on a $|x|_p \neq 0$. On obtient

$$\left|\mathbb{Q}_p^*\right|_p \subset \{p^n : n \in \mathbb{Z}\}$$

D'autre part, d'après la preuve de la proposition (2.2.2), on a

$$p^m = \left|\frac{1}{p^m}\right|_p$$

Alors

$$\{p^n : n \in \mathbb{Z}\} \subset \left|\mathbb{Q}_p^*\right|_p$$

Théorème 2.3.2 *(Théorème 2.2 [3]) Un nombre p-adique $x \in \mathbb{Q}_p$ est un nombre rationnel si et seulement si son développement p-adique $\sum_{n=m}^{\infty} \alpha_n p^n$ est périodique. Autrement dit la suite $(\alpha_n)_n$ est périodique au de la d'un certain rang.*

$$\exists k, n_0 \in \mathbb{N} : \alpha_{n+k} = \alpha_n, \forall n \geqslant n_0$$

et l'entier k est appelé la période de la suite.

Exemple 2.3.4 *On a*

$$\begin{aligned} \frac{1}{3} &= 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + ... \\ &= \cdot 231313131 \\ &= \cdot 2\overline{31} \end{aligned}$$

Le développement 5-adique de $\frac{1}{3}$ est périodique, donc $x = \frac{1}{3} \in \mathbb{Q}$.

2.4 Entiers p-adiques

Une partie intéressante de $\mathbb{Q}_p$ est l'ensemble des éléments 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*

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

2. *On note par $\mathbb{Z}_p$ l'ensemble des entiers p-adiques, 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 2.4.1 .

1) $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\} = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$. 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 $\mathbb{Z}_p$

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

Proposition 2.4.1 *$\mathbb{Z}_p$ est un sous anneau de $\mathbb{Q}_p$.*

Preuve.

i) On a $|0|_p = 0$, donc $0 \in \mathbb{Z}_p$.

ii) Soient $x, y \in \mathbb{Z}_p$, alors

$$\left|x + y\right|_p \leq \max\left\{ |x|_p, \left|y\right|_p \right\} \leq 1$$
$$\Longrightarrow x + y \in \mathbb{Z}_p$$

iii) Soit $x \in \mathbb{Z}_p$, alors

$$|-x|_p = |x|_p \leq 1$$
$$\Longrightarrow -x \in \mathbb{Z}_p$$

iiii) Soient $x, y \in \mathbb{Z}_p$, alors

$$\left|x \cdot y\right|_p = |x|_p \cdot \left|y\right|_p \leq 1$$
$$\Longrightarrow x \cdot y \in \mathbb{Z}_p$$

Définition 2.4.2 *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

$$a = \alpha_0 + \alpha_1 \cdot p + \alpha_2 \cdot p^2 + \cdots + \alpha_n \cdot p^n + \cdots = \sum_{n=0}^{\infty} \alpha_n \cdot p^n, 0 < \alpha_n < p, \ \forall n \in \mathbb{N}$$

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

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

Proposition 2.4.2 *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

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

donc

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

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

$$\alpha = u_1 \cdot p^{m_1}, u_1 \in \mathbb{Z}_p^*, m_1 \in \mathbb{Z}$$

$$\alpha = u_2 \cdot p^{m_2}, u_2 \in \mathbb{Z}_p^*, m_2 \in \mathbb{Z}$$

Alors

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

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

Exemple 2.4.1 *Soient*

$$\begin{cases} p = 5 \\ \alpha^{(1)} = \cdot 4\overline{13} = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \dots \\ \alpha^{(2)} = \cdot 4\overline{2} = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 \dots \end{cases}$$

Alors $\alpha^{(1)}$ et $\alpha^{(2)}$ sont des nombres de $\mathbb{Z}_5^*$. Par contre

$$\begin{cases} \beta^{(1)} = \cdot 01\overline{40} = 0 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + 4 \cdot 5^4 + 0 \cdot 5^5 \dots \notin \mathbb{Z}_5^* \\ \beta^{(2)} = 42 \,.\, 1\overline{331} = 4 \cdot 5^{-2} + 2 \cdot 5^{-1} + 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \dots \notin \mathbb{Z}_5^* \end{cases}$$

puisque le premier chiffre dans $\beta^{(1)}$ est nul et $\beta^{(2)} \notin \mathbb{Z}_5^*$ et le développement 5-adique de $\beta^{(2)}$ contient des puissances négatives de 5*.*

Tout nombre p-adique x possède un unique opposé $(-x)$ tel que $x + (-x) = 0$. La relation entre les expansions p-adiques du x et $(-x)$ peut être vu dans le résultat suivant.

Proposition 2.4.3 *(Recherche des opposés) Si $x = \sum_{k=n}^{\infty} \alpha_k p^k = \alpha_n p^n + \alpha_{n+1} p^{n+1} + \alpha_{n+2} p^{n+2} + ...$, alors $-x = \sum_{k=n}^{\infty} \beta_k p^k = \beta_n p^n + \beta_{n+1} p^{n+1} + \beta_{n+2} p^{n+2} + ...$, où $\beta_n = p - \alpha_n$ et $\beta_i = (p-1) - \alpha_i$ pour $i > n$.*

Preuve. Nous allons montrer que $x + (-x) = 0$. On écrit

$$-x = (p - \alpha_n)p^n + (p - 1 - \alpha_{n+1})p^{n+1} + (p - 1 - \alpha_{n+2})p^{n+2} + ...$$

Si nous formons $x + (-x)$, nous obtenons

$$\begin{aligned} 0 &= p \cdot p^n + (p-1) \cdot p^{n+1} + (p-1) \cdot p^{n+2} + ... \\ &= 0 + p \cdot p^{n+1} + (p-1) \cdot p^{n+2} + ... \\ &= 0 + 0 + p \cdot p^{n+2} + ... \\ &= 0 + 0 + 0 + ... \end{aligned}$$

□

Exemple 2.4.2 *Rappelons que l'expansion 5-adique pour $x = \frac{1}{3}$ dans l'exemple* (2.3.3) *est*

$$x = \frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + ...$$

Alors

$$y = -x = -\frac{1}{3} = 3 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 1 \cdot 5^5 + ...$$

En effet

$$\begin{aligned} x+y &= 5+4\cdot 5+4\cdot 5^2+4\cdot 5^3+... \\ &= 0+5\cdot 5+4\cdot 5^2+4\cdot 5^3+... \\ &= 0+0\cdot 5+5\cdot 5^2+4\cdot 5^3+... \\ &\quad . \\ &\quad . \\ &\quad . \\ &= 0+0\cdot 5+0\cdot 5^2+0\cdot 5^3+... \\ &= 0 \end{aligned}$$

Lemme 2.4.1 *Si $x \in \mathbb{Q}_p^*$, alors x est inversible dans $\mathbb{Q}_p$.*

Preuve. On a

$$\forall x \in \mathbb{Q}_p^* : x = p^n \cdot u, u \in \mathbb{Z}_p^*, n \in \mathbb{Z}$$

On pose

$$u = \sum_{k=0}^{\infty} a_k \cdot p^k, a_0 \neq 0$$

Alors

$$\begin{aligned} u &= a_0 + \sum_{k=1}^{\infty} a_k \cdot p^k = a_0 + p \cdot \sum_{k=1}^{\infty} a_k \cdot p^{k-1} \\ &= a_0 + p \cdot \sum_{k=0}^{\infty} a_{k+1} \cdot p^k = a_0 - p \cdot y \text{ où } y = -\sum_{k=0}^{\infty} a_{k+1} \cdot p^k \in \mathbb{Z}_p \end{aligned}$$

Comme $a_0 \neq 0$, alors on peut prend $a_0 = 1$, on obtient

$$u = 1 - p \cdot y$$

Donc

$$u^{-1} = (1 - p \cdot y)^{-1} = 1 + y \cdot p + y^2 \cdot p^2 + \ldots \in \mathbb{Z}_p^*$$

Ce qui donne

$$x^{-1} = p^{-n} \cdot u^{-1} \in \mathbb{Q}_p^*$$

Puisque $u^{-1} \in \mathbb{Z}_p^*, n \in \mathbb{Z}$. Alors x est inversible dans $\mathbb{Q}_p$.

Le résultat suivant est central à notre étude.

Lemme 2.4.2 *Soient $x, y \in \mathbb{Q}_p$ et $m \in \mathbb{Z}$, alors $x \equiv y \bmod p^m$ si et seulement si $\left|x-y\right|_p \leq p^{-m}$*

Preuve. On a

$$x \equiv y \bmod p^m \iff \frac{x-y}{p^m} \in \mathbb{Z}_p \iff \left|\frac{x-y}{p^m}\right|_p \leq 1 \iff \left|x-y\right|_p \leq p^{-m}$$

2.5 Fonctions p-adiques

Définition 2.5.1
1) Soit $X \subset \mathbb{Q}_p$. Une fonction $f : X \longrightarrow \mathbb{Q}_p$ est dite continue au point $a \in X$ si

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x : |x - a|_p < \delta \Longrightarrow \left|f(x) - f(a)\right|_p < \varepsilon \tag{2.1}$$

2) La fonction $f : X \longrightarrow \mathbb{Q}_p$ est dite continue sur X si elle est continue en tout point de X.

Exemple 2.5.1 *Les fonctions polynomiales $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n$ à coefficients dans $\mathbb{Q}_p$ sont continues sur tout sous-ensemble de $\mathbb{Q}_p$ comme dans le cas réel.*

Définition 2.5.2
1) Soit X un sous ensemble de $\mathbb{Q}_p$ et $a \in X$. La fonction $f : X \longrightarrow \mathbb{Q}_p$ est dite différentiable au point a, si la dérivée de f à a définie par $f'(a) = \lim\limits_{x \longrightarrow a} \frac{f(x)-f(a)}{x-a}$ existe.
2) La fonction f est différentiable sur X si $f'(a)$ existe pour tout $a \in X$.

Exemple 2.5.2 *Avec cette définition de la dérivée, si $f(x) = \sum\limits_{i=0}^{n} \alpha_i x^i$, $\alpha_i \in \mathbb{Q}_p$, alors $f'(x) = \sum\limits_{i=1}^{n} i\alpha_i x^{i-1}$.*

2.6 Arithmétique dans $\mathbb{Q}_p$

Les opérations d'addition, soustraction, multiplication dans $\mathbb{Q}_p$ sont assez similaires aux opérations correspondantes sur les nombres décimaux. Cependant, la principale différence est que ces opérations sont faites chiffre à chiffre, on part de la gauche vers la droite.

2.6.1 Addition

En règle générale, lorsqu'on additionne des nombres entiers usuels, exprimés en base 10, on additionne terme à terme. Par exemple, soient deux nombres A et B, 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 nombre. Pour l'addition des nombres p-adiques, on procède de la même manière, on les additionne terme à terme, tout en appliquant le **système des retenues**. Les calculs se faisant de gauche à droite, on peut ainsi effectuer une addition.

Supposons que nous avons deux nombres p-adiques arbitraires

$$\begin{aligned} x &= \alpha_n p^n + \alpha_{n+1} p^{n+1} + \alpha_{n+2} p^{n+2} + ... \\ y &= \beta_n p^n + \beta_{n+1} p^{n+1} + \beta_{n+2} p^{n+2} + ... \end{aligned}$$

les chiffres (digits) α_n et β_n formant les nombres p-adiques x et y seront donc compris entre 0 et $p-1$. Alors

$$\alpha_n, \beta_n \in \{0, 1, 2, ..., p-1\}$$

On obtient

$$\begin{aligned} x+y &= (\alpha_n+\beta_n)p^n + (\alpha_{n+1}+\beta_{n+1})p^{n+1} + (\alpha_{n+2}+\beta_{n+2})p^{n+2} + ... \\ &= c_n p^n + c_{n+1}p^{n+1} + c_{n+2}p^{n+2} + ... \end{aligned}$$

Où

$$c_i = \alpha_i + \beta_i, i = n, n+1, ...$$

Supposons $c_n, c_{n+1}, ..., c_{k-1}$ sont des **digits** (ils sont inférieurs à p) mais c_k n'est pas. Alors

$$c_k = p + d_k$$

Où $0 \leq d_k < p$. Dans ce cas

$$\begin{aligned} x+y &= c_n p^n + ... + c_{k-1}p^{k-1} + (p+d_k)p^k + c_{k+1}p^{k+1} + ... \\ &= c_n p^n + ... + c_{k-1}p^{k-1} + d_k p^k + (c_{k+1}+1)p^{k+1} + ... \end{aligned}$$

et d_k est un digit associé à p^k. Notons que "la retenue" a été généré et ainsi c_{k+1} est augmenté d'une unité. À ce stade $(c_{k+1}+1)$ doit être examiné pour voir s'il est inférieure à p ou non. Dans le cas contraire $(\geq p)$, nous avons "une retenue" propagée à c_{k+2} et ainsi de suite.

Exemple 2.6.1 *Soient* $x = \frac{2}{3}, y = \frac{5}{6} \in \mathbb{Q}_5$ *tels que*

$$\begin{aligned} x &= \cdot 4131313... = \cdot 4\overline{13} \\ y &= \cdot 0140404... = \cdot 01\overline{404} \end{aligned}$$

Alors

$$\begin{array}{cccccccccc} & & & & & \overset{R_0}{} & & \overset{R_1}{} & & \\ + & \cdot & 4 & 1 & 3 & 1 & 3 & 1 & 3 & ... \\ & \cdot & 0 & 1 & 4 & 0 & 4 & 0 & 4 & ... \\ \hline = & \cdot & 4 & 2 & 2 & 2 & 2 & 2 & 2 & ... \end{array}$$

Donc

$$x + y = \cdot 4222222 = \cdot 4\overline{2} = \frac{3}{2}$$

Où la retenue $R_0 = 1$ *correspond à la retenue éventuelle de la somme* $(3+4)$*, elle est additionnée à la somme* $(1+0)$.
$R_1 = 1$ *correspond à la retenue éventuelle de la somme* $(3+4)$*, elle est additionnée à la somme* $(1+0)$*, et ainsi de suite.*

2.6.2 Soustraction

Pour faire la soustraction de deux nombres p-adiques $x, y \in \mathbb{Q}_p$, en utilisant "l'addition complétée". C'est-à-dire, on calcule $(-y)$, en utilisant la proposition (2.4.3), puis on fait l'addition (au lieu d'effectuer $x - y$ on fait $x + (-y)$).

Exemple 2.6.2 *Soient* $x = \frac{2}{3} = \cdot 4131313... = \cdot 4\overline{13}, y = \frac{1}{6} = \cdot 1404040... = \cdot 1\overline{40} \in \mathbb{Q}_5$.
Calculons $(-y)$, *on a*

$$\begin{cases} b_0 = p - a_0 \\ b_j = (p-1) - a_j, j \geq 1 \end{cases}$$

Où a_j *(resp :* b_j*) sont des digits de* y *(resp :* $-y$*). On trouve*

$$b_0 = 4, b_1 = 0, b_2 = 4, b_3 = 0, b_4 = 4, b_5 = 0$$

Donc

$$-y = -\frac{1}{6} = \cdot 40404040... = \cdot 4\overline{04}$$

On obtient

$$x - y = \cdot 4131313... + \cdot 4040404... = \cdot 3222222... = \cdot 3\overline{2} = \frac{1}{2}$$

2.6.3 Multiplication

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-adiques se fait suivant la technique habituelle de la multiplication de deux nombres entiers, comme on sait le faire habituellement.

Soient $x, y \in \mathbb{Q}_p$, tels que

$$\begin{aligned} x &= p^n.u = p^n(a_0 + a_1 p + a_2 p^2 + ...), u \in \mathbb{Z}_p^* \\ y &= p^m v = p^n(b_0 + b_1 p + b_2 p^2 + ...), v \in \mathbb{Z}_p^* \end{aligned}$$

Alors

$$x.y = p^{n+m} u.v$$

Ainsi, sans perte de généralité, on restreint notre discussion sur la multiplication des nombres p-adiques à une discussion sur la multiplication des nombres p-adiques **unitaires**. Alors

$$\begin{aligned} u.v &= (a_0 + a_1 p + a_2 p^2 + ...).(b_0 + b_1 p + b_2 p^2 + ...) \\ &= c_0 + c_1 p + c_2 p^2 + c_3 p^3 + ... \end{aligned}$$

avec

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 \\ . \\ . \\ . \\ c_k = a_0b_k + a_1b_{k-1} + ... + a_kb_0 \\ . \\ . \\ . \end{cases}$$

On remarque que même si les digits p-adiques a_i et b_i sont dans l'ensemble $\{0, 1, ..., p-1\}$, on ne peut pas supposer que les entiers c_i se trouvent dans cet ensemble. Alors nous ne pouvons pas supposer qu'ils sont des digits. (En général, ils ne sont pas). Par conséquent, nous écrivons

$$c_0 = a_0b_0 = d_0 + t_1p$$

Où $0 \leq d_0 < p$. Alors d_0 est le digit (chiffre) dans l'expansion p-adique de $u.v$ et t_1 est «la retenue» que nous devons ajouter à c_1. Ensuite, nous écrivons

$$\begin{aligned} c_1 + t_1 &= (a_0b_1 + a_1b_0) + t_1 \\ &= d_1 + t_2p \end{aligned}$$

Où $0 \leq d_1 < p$. Alors d_1 est le deuxième digit dans l'expansion p-adique de $u.v$ et t_2 est «la retenue» que nous devons ajouter à c_2. Si nous continuons de cette procédure, nous obtenons l'expansion (unique) p-adique

$$u.v = d_0 + d_1p + d_2p^2 + ...$$

Tel que $0 \leq d_i < p$ pour tout i.

Exemple 2.6.3 *Soient* $x = \frac{2}{3} = \cdot 4131313... = \cdot 4\overline{13}$, $y = \frac{1}{6} = \cdot 1404040... = \cdot 1\overline{40} \in \mathbb{Q}_5$. *Alors*

$$\begin{array}{cccccccccccc} * & \cdot & 4 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & . & . & . \\ & \cdot & 1 & 4 & 0 & 4 & 0 & 4 & 0 & 4 & . & . & . \\ & & 4 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & . & . & . \\ & & & 1 & 2 & 3 & 1 & 3 & 1 & 3 & . & . & . \\ & & & & 0 & 0 & 0 & 0 & 0 & 0 & . & . & . \\ & & & & & 1 & 2 & 3 & 1 & 3 & . & . & . \\ & & & & & & 0 & 0 & 0 & 0 & . & . & . \\ & & & & & & & 1 & 2 & 3 & . & . & . \\ & & & & & & & & 0 & 0 & . & . & . \\ & & & & & & & & & 1 & . & . & . \\ = & \cdot & 4 & 2 & 0 & 1 & 2 & 4 & 3 & 2 & . & . & . \end{array}$$

Donc

$$x.y = \cdot 42012432... = \cdot 4\overline{2012432} = \frac{1}{9}$$

2.7 Propriétés topologiques et analytiques des nombres p-adiques

2.7.1 Quelques propriétés analytiques

Théorème 2.7.1 *Une suite $(a_n)_n$ de $\mathbb{Q}_p$ est de Cauchy et par conséquent convergente si et seulement si*

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

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

$$\lim_{n,m\longrightarrow\infty} |a_m - a_n|_p = 0$$

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

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

D'autre part, supposons que

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

Par définition

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

Prenons $\varepsilon > 0, m > n \geq n_0$ et examinons $|a_m - a_n|_p$, en utilisant l'inégalité triangulaire forte, on obtient

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

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

Proposition 2.7.1 *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

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

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

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

Remarque 2.7.1 *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* $\sum_{n\geq 1} \frac{1}{n}$.

Proposition 2.7.2 *(Suites stationnaires)*
Soit $(a_n)_n$ *est une suite des nombres p-adiques, telle que* $\lim_{n\longrightarrow\infty} a_n = a \neq 0$*. Autrement dit* $(a_n)_n$ *est une suite non nulle, alors*

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

C'est à dire la suite de normes $\left(|a_n|_p\right)_n$ *doit stationnaire (constante) pour n suffisamment grand.*

Preuve. Cela découle du lemme (1.2.1). □

2.7.2 Quelques propriétés topologiques

Définition 2.7.1 *(Topologie p-adique). On définit la topologie p-adique par la famille des boules*

$$V_n(a) = \left\{x \in \mathbb{Q}_p : |x-a|_p \leq p^{-n}\right\} = \left\{x \in \mathbb{Q}_p : v_p(x-a) \geq n\right\}$$

où $a \in \mathbb{Q}_p$ *et* $|x|_p = p^{-v_p(x)}$.

Proposition 2.7.3 *Soient* $x, a \in \mathbb{Q}_p$*. Si* $|a-x|_p < |a|_p$*, alors* $|x|_p = |a|_p$*. Autrement dit, tous les triangles dans l'espace* $(\mathbb{Q}_p, |.|_p)$ *sont isocèles et la longueur de sa base ne dépasse pas les longueurs des côtés.*

Preuve. Cela découle de la proposition (1.1.2).

Définition 2.7.2 *On appelle :*

1. *La boule ouverte dans* $\mathbb{Q}_p$*, de rayon* $r \in \mathbb{R}^+$ *et de centre* $a \in \mathbb{Q}_p$ *l'ensemble donné par*

$$B(a,r) = \{x \in \mathbb{Q}_p : d_p(a,x) < r\} = \{x \in \mathbb{Q}_p : |x-a|_p < r\} \tag{2.2}$$

2. *La boule fermée dans* $\mathbb{Q}_p$*, de rayon* $r \in \mathbb{R}^+$ *et de centre* $a \in \mathbb{Q}_p$ *l'ensemble donné par*

$$\bar{B}(a,r) = \{x \in \mathbb{Q}_p : d_p(a,x) \leq r\} = \{x \in \mathbb{Q}_p : |x-a|_p \leq r\} \tag{2.3}$$

3. *La sphère dans* $\mathbb{Q}_p$ *l'ensemble défini par*

$$S(a,r) = \{x \in \mathbb{Q}_p : d_p(a,x) = r\} = \{x \in \mathbb{Q}_p : |x-a|_p = r\} \tag{2.4}$$

Remarque 2.7.2 *La norme p-adique* $|.|_p$ *prend ses valeurs dans l'ensemble discret* $\{0, p^n : n \in \mathbb{Z}\}$*, donc on peut prend* $r = p^n, n \in \mathbb{Z}$.

Proposition 2.7.4 *La sphère $S(a,r)$ est un ensemble ouvert dans $\mathbb{Q}_p$.*

Preuve. Il faut montrer que $S(a,r)$ est voisinage de tous ses points, c'est à dire que pour tout $x \in S(a,r)$, il existe une boule ouverte de centre x et de rayon s inclus dans $S(a,r)$. Cela signifie

$$\forall x \in S(a,r), \exists s > 0 : B(x,s) \subset S(a,r)$$

Soient $x \in S(a,r)$ et $s < r$. Montrons que $B(x,s) \subset S(a,r)$.
Supposons que $y \in B(x,s)$, alors

$$\begin{cases} |x-y|_p < s \\ \\ |x-a|_p = r \end{cases} \Longrightarrow |x-y|_p < |x-a|_p = r$$

D'après la proposition (2.7.3), on a

$$|y-a|_p = |x-a|_p = r$$

Alors

$$y \in S(a,r)$$

Proposition 2.7.5 *Toute boule $B(a,r)$ de $(\mathbb{Q}_p, |.|_p)$ est un ensemble à la fois ouvert et fermé.*

Preuve. On sait que toute boule $B(a,r)$ est ouverte dans tout espace métrique. Pour montrer que $B(a,r)$ est fermée dans $\mathbb{Q}_p$, on va montrer que son complémentaire

$$C = \{x \in \mathbb{Q}_p : |x-a|_p \geq r\}$$

est un ensemble ouvert.
On a

$$C = S(a,r) \cup D$$

Où

$$D = \{x \in \mathbb{Q}_p : |x-a|_p > r\}$$

L'ensemble

$$D = \{x \in \mathbb{Q}_p : |x-a|_p > r\}$$

est un ouvert. En effet :
Supposons que $y \in D$ et posons

$$|y-a|_p = r_1 > r$$

Montrons que la boule $B(y, r_1 - r)$ est incluse dans D.
Pour cela, supposons que $B(y, r_1 - r)$ n'est pas incluse dans D, alors on peut trouver $x_0 \in B(y, r_1 - r), x_0 \notin D$ telle que

$$\begin{cases} |y-x_0|_p < r_1 - r \\ \\ |x_0 - a|_p \leq r \end{cases}$$

On trouve

$$\begin{aligned} r_1 = |y-a|_p &= |y-x_0+x_0-a|_p \\ &\leq |y-x_0|_p + |x_0-a|_p \\ &< r_1 - r + r = r_1 \end{aligned}$$

Contradiction. Comme l'union de deux ouverts est un ouvert, donc C est un ouvert.

Proposition 2.7.6 *Tout point d'une boule est le centre de cette boule. C'est-à-dire*

$$\forall b \in B(a,r) \Longrightarrow B(a,r) = B(b,r)$$

Preuve. Soient $b \in B(a,r)$ et $x \in B(a,r)$, alors

$$|x-b|_p = |x-a+a-b|_p \leq \max\{|x-a|_p, |a-b|_p\} < \max\{r,r\} = r$$

on obtint $B(a,r) \subset B(b,r)$.
D'autre part, Maintenant si nous échangeons les rôles de a et b, alors on trouve $B(b,r) \subset B(a,r)$.

Proposition 2.7.7 *Deux boules sont soit disjointes soit l'une est contenue dans l'autre. Autrement dit si $B(a,r)$ et $B(b,s)$ deux boules de $(\mathbb{Q}_p, |.|_p)$, alors*

$$B(a,r) \cap B(b,s) \neq \varnothing \Longrightarrow B(a,r) \subset B(b,s) \text{ ou } B(b,s) \subset B(a,r) \tag{2.5}$$

Preuve. Supposons que $r \leq s$, et $y \in B(a,r) \cap B(b,s)$. Alors $y \in B(a,r)$ et $y \in B(b,s)$. D'après la proposition (2.7.6)

$$\begin{cases} B(a,r) = B(y,r) \\ \\ B(b,s) = B(y,s) \end{cases}$$

D'autre part, on a $B(y,r) \subset B(b,s)$, on obtient

$$B(a,r) \subset B(b,s)$$

De même, si on suppose que $s \leq r$, alors on trouve

$$B(b,s) \subset B(a,r)$$

Remarque 2.7.3 *Toutes les propriétés qui sont démontrées au-dessus pour les boules ouvertes, restent vraies pour les boules fermées dans $\mathbb{Q}_p$.*

Chapitre 3

Application des méthodes numériques - Calcul de l'inverse d'un nombre p-adique -

La connaissance des propriétés arithmétiques et algébriques des nombres p-adiques est utile à l'étude de leurs propriétés diophantiennes et des problèmes d'approximation. Il s'agit, dans ce chapitre, d'une application intéressante des outils de l'analyse numérique à la théorie des nombres. On verra comment appliquer les méthodes numériques de bases (Newton, sécante, point fixe) pour calculer le zéro d'une fonction f.

L'objet essentiel de ce chapitre est de calculer les développements finis p-adiques (les premiers chiffres) de l'inverse de $a \in \mathbb{Q}_p^*$ à l'aide à de détermination de la solution de l'équation

$$\begin{cases} f(x) = \frac{1}{x} - a = 0 \\ a \in \mathbb{Q}_p^* \ , p\text{-premier} \end{cases} \tag{3.1}$$

par une méthode d'approximation. La solution de (3.1) est approchée par une suite de nombres p-adiques $(x_n)_n \in \mathbb{Q}_p^*$ construite soit par la méthode de Newton, de la sécante ou par la méthode du point fixe.

Principe général de calcul, est le suivant :
Soit a un nombre p-adique non nul tel que

$$\begin{cases} a = p^m \cdot u, v_p(a) = m \in \mathbb{Z}, u \in \mathbb{Z}_p^* \\ |a|_p = p^{-m}, m \in \mathbb{Z} \end{cases}$$

Il est clair que si $b \in \mathbb{Q}_p^*$ est l'inverse de a, alors

$$|b|_p = |a^{-1}|_p = p^m, m \in \mathbb{Z}$$

Donc la suite des nombres p-adiques $(x_n)_n$ devrait tendre vers $b \in \mathbb{Q}_p^*$. Ainsi à partir d'un certain rang (d'après le lemme (2.7.2)) , on a

$$|x_n|_p = |b|_p = p^m, m \in \mathbb{Z} \tag{3.2}$$

3.1 Méthode de Newton

La méthode de Newton est une méthode basée sur la construction d'une suite de points $(x_n)_n \in \mathbb{Q}_p^*$ qui converge vers le zéro de f. La fonction d'itération de Newton est définie par

$$g(x) = x - \frac{f(x)}{f'(x)} \tag{3.3}$$

La suite des itérés associée à la fonction g est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = g(x_n) = x_n - \frac{f(x_n)}{f'(x_n)} \tag{3.4}$$

Sachant que

$$f(x) = \frac{1}{x} - a, f'(x) = \frac{-1}{x^2} \tag{3.5}$$

La suite des itérés de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - a \cdot x_n) \tag{3.6}$$

Remarque 3.1.1 *Pour mesurer la vitesse de convergence d'une méthode itérative, on mesure l'évolution de la suite $(e_{n+n_0})_n$ de écarts $e_{n+n_0} = x_{n+n_0} - x_{n+n_0-1}$ entre les itérés de la suite $(x_n)_n$ obtenue à chaque étape d'itération.*

Définition 3.1.1 *Soit $a \in \mathbb{Q}_p^*$. On dit que $b \in \mathbb{Q}_p$ est l'inverse de a d'ordre r si et seulement si $a \cdot b \equiv 1 \bmod p^r$.*

Théorème 3.1.1 *Si x_{n_0} est l'inverse de a d'ordre r, alors x_{n+n_0} est l'inverse de a d'ordre $(\eta_n)_n$, tel que la suite $(\eta_n)_n$ est définie par*

$$\forall n \in \mathbb{N} : \eta_n = 2^n \cdot r \tag{3.7}$$

et la suite des écarts est définie par

$$x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\eta_n'}$$

Où la (η_n') est donnée par

$$\forall n \in \mathbb{N} : \eta_n' = \eta_n - m = 2^n \cdot r - m$$

Preuve. Soit $(x_n)_n$ la suite définie par la formule (3.6). On a x_{n_0} est l'inverse de a d'ordre r, c'est-à-dire

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r$$

Tels que n_0 représente un rang quelconque et $r \in \mathbb{N}^*$. On obtient

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r \Longrightarrow |a \cdot x_{n_0} - 1|_p \leq p^{-r}$$

D'autre part, on a

$$\forall n \in \mathbb{N} : a \cdot x_{n+1} - 1 = -(ax_n - 1)^2 \tag{3.8}$$

Par conséquent

$$\left|a \cdot x_{n_0+1} - 1\right|_p = \left|a \cdot x_{n_0} - 1\right|_p^2 \implies \left|a \cdot x_{n_0+1} - 1\right|_p \leq p^{-2r}$$

D'après le lemme (2.4.2), on obtient

$$a \cdot x_{n_0+1} - 1 \equiv 0 \bmod p^{2r}$$

De cette façon, on obtient

$$a \cdot x_{n_0} - 1 \equiv 0 \bmod p^r \Longrightarrow \begin{cases} a \cdot x_{n_0+1} - 1 \equiv 0 \bmod p^{2r} \\ a \cdot x_{n_0+2} - 1 \equiv 0 \bmod p^{4r} \\ a \cdot x_{n_0+3} - 1 \equiv 0 \bmod p^{8r} \\ a \cdot x_{n_0+4} - 1 \equiv 0 \bmod p^{16r} \end{cases}$$

Donc

$$\forall n \in \mathbb{N} : a \cdot x_{n+n_0} - 1 \equiv 0 \bmod p^{\eta_n} \tag{3.9}$$

La suite $(\eta_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \eta_n = 2^n \cdot r \tag{3.10}$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n(1 - a \cdot x_n) \tag{3.11}$$

Ce qui donne

$$\begin{array}{rcl} |x_{n+n_0+1} - x_{n+n_0}|_p & = & |x_{n+n_0} \cdot (1 - a \cdot x_{n+n_0})|_p \\ & \Longrightarrow & |x_{n+n_0+1} - x_{n+n_0}|_p = |x_{n+n_0}|_p \cdot |1 - a \cdot x_{n+n_0}|_p \\ & \Longrightarrow & |x_{n+n_0+1} - x_{n+n_0}|_p \leq p^m \cdot p^{-\eta_n} \\ & \Longrightarrow & |x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{-(\eta_n - m)} \\ & \Longrightarrow & x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\eta_n'} \end{array}$$

Où la suite (η_n') est définie par

$$\forall n \in \mathbb{N} : \eta_n' = \eta_n - m = 2^n \cdot r - m \tag{3.12}$$

Conclusion 3.1.1

1. *La vitesse de convergence de la suite $(x_n)_n$ est d'ordre η_n'.*

2. *Pour déterminer le nombre des itération n pour une précision donnée M qui représente le nombre de chiffres p-adiques dans le développement p-adique de a^{-1}, on pose*

$$\eta_n^{'} \geq M \Longleftrightarrow 2^n \cdot r - m \geq M \Longrightarrow n = \left\lceil \frac{\ln \frac{M+m}{r}}{\ln 2} \right\rceil$$

Exemple 3.1.1 *(Application de la méthode de Newton)*
Supposons que

$$p = 5, a = 3, M = 8$$

Alors

$$|a|_5 = |3|_5 = 1 = 5^0 \Rightarrow m = 0$$

On prend $x_0 = 2$, car

$$a \cdot x_0 = 2 \cdot 3 = 6 \equiv 1 \bmod 5$$

Ce qui donne $r = 1, n_0 = 0$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln \frac{M+m}{r}}{\ln 2} \right\rceil = \left\lceil \frac{\ln \frac{8+0}{1}}{\ln 2} \right\rceil = \left\lceil \frac{3 \ln 2}{\ln 2} \right\rceil = 3$$

La suite d'itération de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - 3x_n) \tag{3.13}$$

Alors

$$x_1 = 2 \cdot (2 - 2 \cdot 3) = -8 \equiv 17 = 2 + 3 \cdot 5 \bmod 5^2$$

$$x_2 = -8 \cdot (2 - 3 \cdot (-8)) = -208 \equiv 417 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 \bmod 5^4$$

$$x_3 = -208 \cdot (2 - 3 \cdot (-208)) = -130208 \equiv 260417 = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 \bmod 5^8$$

Donc

$$\begin{cases} \frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 \bmod 5^8 \\ \frac{1}{3} = \cdot 23131313 = \cdot 2\overline{31} \end{cases}$$

Exemple 3.1.2 *Supposons que*

$$p = 2, a = 3, M = 8$$

Alors

$$|a|_2 = |3|_2 = 1 = 2^0 \Rightarrow m = 0$$

On prend $x_0 = 1$, car

$$a \cdot x_0 = 3 \cdot 1 = 3 \equiv 1 \bmod 2$$

Ce qui donne $r = 1, n_0 = 0$.
Le nombre des itérations est

$$n = 3$$

La suite d'itération de Newton est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(2 - 3x_n) \tag{3.14}$$

Alors

$$x_1 = -1 \equiv 3 \bmod 4 = 1 + 1 \cdot 2 \bmod 2^2$$
$$x_2 = -5 \equiv 11 \bmod 16 = 1 + 1 \cdot 2 + 1 \cdot 2^3 \bmod 2^4$$
$$x_3 = -85 \equiv 171 \bmod 256 = 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^5 + 1 \cdot 2^7 \bmod 2^8$$

Donc

$$\begin{cases} \frac{1}{3} \equiv 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^5 + 1 \cdot 2^7 \bmod 2^8 \\ \frac{1}{3} = \cdot 11010101 = \cdot 11\overline{01} \end{cases}$$

3.2 Méthode de la sécante

Une méthode élémentaire pour déterminer le zéro d'une fonction est la méthode de la sécante. Cette méthode permet de pallier les cas où l'on peut pas calculer facilement la dérivée de f. Dans ce cas, on remplace $f'(x_n)$ par le taux d'accroissement de f enter x_n et x_{n-1}. ie :

$$f'(x_n) = \frac{f(x_n) - f(x_{n-1})}{x_n - x_{n-1}}$$

La relation de récurrence est donnée par

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n - \frac{f(x_n) \cdot (x_n - x_{n-1})}{f(x_n) - f(x_{n-1})}$$

Par conséquent

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n - x_{n-1} - a \cdot x_n \cdot x_{n-1} \tag{3.15}$$

Théorème 3.2.1 *Si x_{n_0-1} (resp : x_{n_0}) est l'inverse de a d'ordre α (resp : β), alors x_{n+n_0-1} est l'inverse de a d'ordre F_n. Telle que la suite F_n est définie par*

$$\begin{aligned} \forall n \in \mathbb{N} : F_n &= \left[\frac{1}{\sqrt{5}} \left(\beta - \frac{1 - \sqrt{5}}{2} \alpha \right) \cdot \left(\frac{1 + \sqrt{5}}{2} \right)^n + \frac{1}{\sqrt{5}} \left(-\beta + \frac{1 + \sqrt{5}}{2} \alpha \right) \cdot \left(\frac{1 - \sqrt{5}}{2} \right)^n \right] \\ &= \left[\frac{1}{\sqrt{5}} ((\beta - \alpha(1 - \Phi)) \cdot \Phi^n + (-\beta + \alpha\Phi) \cdot (1 - \Phi)^n) \right] \end{aligned}$$

Sachant que $\Phi = \dfrac{1 + \sqrt{5}}{2}$.

Preuve.
Soit $(x_n)_n$ la suite définie par la formule (3,15). On a x_{n_0-1} (resp : x_{n_0}) est l'inverse de a d'ordre α (resp :β), alors

$$\begin{cases} a \cdot x_{n_0-1} - 1 \equiv 0 \bmod p^{\alpha} \\ \\ a \cdot x_{n_0} - 1 \equiv 0 \bmod p^{\beta} \end{cases} \qquad \alpha, \beta \in \mathbb{N}$$

Donc

$$\begin{cases} |a \cdot x_{n_0-1} - 1|_p \leq p^{-\alpha} \\ |a \cdot x_{n_0} - 1|_p \leq p^{-\beta} \end{cases}$$

On a

$$\forall n \in \mathbb{N}^* : a \cdot x_{n+1} - 1 = (a \cdot x_n - 1) \cdot (1 - a \cdot x_{n-1})$$

Alors

$$\left|ax_{n_0+1} - 1\right|_p = \left|ax_{n_0} - 1\right|_p . \left|1 - ax_{n_0-1}\right|_p$$

Ce qui donne

$$\left|ax_{n_0+1} - 1\right|_p \leq p^{-\beta} \cdot p^{-\alpha} = p^{-(\alpha+\beta)}$$

On obtient

$$ax_{n_0+1} - 1 \equiv 0 \bmod p^{\alpha+\beta}$$

De cette manière, on obtient

$$\begin{cases} a \cdot x_{n_0-1} - 1 \equiv 0 \bmod p^{\alpha} \\ \\ a \cdot x_{n_0} - 1 \equiv 0 \bmod p^{\beta} \end{cases} \Longrightarrow \begin{cases} a \cdot x_{n_0+1} - 1 \equiv 0 \bmod p^{\alpha+\beta} \\ a \cdot x_{n_0+2} - 1 \equiv 0 \bmod p^{\alpha+2\beta} \\ a \cdot x_{n_0+3} - 1 \equiv 0 \bmod p^{2\alpha+3\beta} \\ a \cdot x_{n_0+4} - 1 \equiv 0 \bmod p^{3\alpha+5\beta} \\ \vdots \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : a \cdot x_{n+n_0-1} - 1 \equiv 0 \bmod p^{F_n}$$

Où $(F_n)_n$ est une suite linéaire récurrente définie par

$$\begin{cases} F_0 = \alpha, F_1 = \beta \\ \forall n \in \mathbb{N}^* : F_{n+1} = F_{n-1} + F_n \end{cases}$$

Dont le terme général est

$$\begin{aligned} \forall n \in \mathbb{N} : F_n &= \left[\frac{1}{\sqrt{5}} \left(\beta - \frac{1 - \sqrt{5}}{2} \alpha \right) \cdot \left(\frac{1 + \sqrt{5}}{2} \right)^n + \frac{1}{\sqrt{5}} \left(-\beta + \frac{1 + \sqrt{5}}{2} \alpha \right) \cdot \left(\frac{1 - \sqrt{5}}{2} \right)^n \right] \\ &= \left[\frac{1}{\sqrt{5}} ((\beta - \alpha(1 - \Phi)) \cdot \Phi^n + (-\beta + \alpha\Phi) \cdot (1 - \Phi)^n) \right] \end{aligned}$$

Tel que $\Phi = \dfrac{1 + \sqrt{5}}{2}$ est appelé "le nombre d'or".
D'autre part, on a

$$\forall n \in \mathbb{N}^* : x_{n+1} - x_n = x_{n-1}(1 - ax_n) \tag{3.16}$$

On trouve

$$\left|x_{n+n_0} - x_{n+n_0-1}\right|_p = \left|x_{n+n_0-2}\right|_p \cdot \left|1 - a \cdot x_{n+n_0-1}\right|_p = p^m \cdot \left|1 - a x_{n+n_0-1}\right|_p$$

Ce qui donne

$$\left|x_{n+n_0} - x_{n+n_0-1}\right|_p \leq p^m \cdot p^{-F_n} = p^{-(F_n - m)}$$

On obtient

$$x_{n+n_0} - x_{n+n_0-1} \equiv 0 \bmod p^{F_n - m}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0} - x_{n+n_0-1} \equiv 0 \bmod p^{F'_n}$$

Telle que la suite $(F'_n)_n$ est définie par

$$\forall n \in \mathbb{N} : F'_n = F_n - m = \left[\frac{1}{\sqrt{5}}((\beta - \alpha(1-\Phi)) \cdot \Phi^n + (-\beta + \alpha\Phi) \cdot (1-\Phi)^n)\right] - m$$

Conclusion 3.2.1

1. *La vitesse de convergence de la suite $(x_n)_n$ est de l'ordre F'_n.*
2. *Comme $|1 - \Phi| < 1$, alors*

$$F'_n \simeq \frac{1}{\sqrt{5}} (\beta - \alpha (1 - \Phi)) \cdot \Phi^n - m$$

3. *On peut déterminer le nombre des itérations n pour M chiffres donnés comme suit*

$$F'_n \geq M \Longrightarrow \frac{1}{\sqrt{5}} (\beta - \alpha (1 - \Phi)) \cdot \Phi^n - m \geq M$$

On obtient

$$n = \left[\frac{\ln \frac{\sqrt{5}(M+n)}{\beta - (1-\Phi)\alpha}}{\ln \Phi}\right]$$

Exemple 3.2.1 *(Application de la méthode de la sécante)*
Soient $p = 5$, $a = 3$, $M = 8$. On a

$$|3|_5 = 1 = 5^0 \Longrightarrow m = 0$$

On prend $x_0 = x_1 = 2$ puisque $2 \cdot 3 \equiv 1 \bmod 5$. On obtient $\alpha = \beta = 1$, $n_0 = 0$.
Le nombre des itérations est

$$n = \left[\frac{\ln \frac{\sqrt{5}(8+0)}{1-(1-\Phi)}}{\ln \Phi}\right] = \left[\frac{\ln \frac{8\sqrt{5}}{\Phi}}{\ln \Phi}\right] = 5$$

En effet

$$\begin{aligned}
x_0 &\equiv 2 \bmod 5 \\
x_1 &\equiv 2 \bmod 5 \\
x_2 &= 2+2-3\cdot 2\cdot 2 \equiv 17 = 2+3\cdot 5 \bmod 5^2 \\
x_3 &= 17+2-3\cdot 2\cdot 17 \equiv -83 \equiv 42 = 2+3\cdot 5+1\cdot 5^2 \bmod 5^3 \\
x_4 &= 42+17-3\cdot 17\cdot 42 \equiv -2083 \equiv 1042 = 2+3\cdot 5+1\cdot 5^2+3\cdot 5^3+1\cdot 5^4 \bmod 5^5 \\
x_5 &= 1042+42-3\cdot 1042\cdot 42 \equiv -130208 \equiv 260417 \\
&= 2+3\cdot 5+1\cdot 5^2+3\cdot 5^3+1\cdot 5^4+3\cdot 5^5+1\cdot 5^6+3\cdot 5^7 \bmod 5^8
\end{aligned}$$

Alors

$$\begin{cases} \frac{1}{3} \equiv 2+3\cdot 5+1\cdot 5^2+3\cdot 5^3+1\cdot 5^4+3\cdot 5^5+1\cdot 5^6+3\cdot 5^7 \bmod 5^8 \\ \frac{1}{3} = \cdot 23131313 = \cdot 2\overline{31} \end{cases}$$

Exemple 3.2.2 *Soient $p = 2, a = 3, M = 8$. Alors $m = 0$.*
On prend $x_0 = x_1 = 1$, puisque

$$a \cdot x_0 = a \cdot x_1 = 3 \cdot 1 \equiv 1 \bmod 2$$

On obtient $\alpha = \beta = 1$, $n_0 = 0$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln \frac{\sqrt{5}(8+0)}{1-(1-\Phi)}}{\ln \Phi} \right\rceil = \left\lceil \frac{\ln \frac{8\sqrt{5}}{\Phi}}{\ln \Phi} \right\rceil = 5$$

D'autre part, on a

$$\forall n \in \mathbb{N}^* : x_{n+1} = x_n + x_{n-1} - 3x_n x_{n-1} \tag{3.17}$$

On trouve

$$x_0 \equiv 1 \bmod 2$$

$$x_1 \equiv 1 \bmod 2$$

$$x_2 = -1 \equiv 3 \bmod 4 = 1+1\cdot 2 \bmod 2^2$$

$$x_3 = 3 \equiv 3 \bmod 8 = 1+1\cdot 2 \bmod 2^3$$

$$x_4 = 11 \equiv 11 \bmod 2^5 = 1+1\cdot 2+1\cdot 2^3 \bmod 2^5$$

$$x_5 = -88 \equiv 171 \bmod 2^8 = 1+1\cdot 2+1\cdot 2^3+1\cdot 2^5+1\cdot 2^7 \bmod 2^8$$

On écrit

$$\begin{cases} \frac{1}{3} \equiv 1+1\cdot 2+1\cdot 2^3+1\cdot 2^5+1\cdot 2^7 \bmod 2^8 \\ \frac{1}{3} = \cdot 11010101 = \cdot 11\overline{01} \end{cases}$$

3.3 Méthode du point fixe

Nous donnons dans cette section un procédé général pour trouver les racines d'une équation non linéaire. La méthode est fondée sur le fait qu'il est toujours possible, pour f, de transformer le problème $f(x) = 0$ en un problème équivalent $x - g(x) = 0$, où la fonction auxiliaire g a été choisie de manière à ce que $g(\alpha) = \alpha$ quand $f(\alpha) = 0$. Approcher les zéros de f se ramène donc au problème de la détermination des points fixes de g, ce qui se fait en utilisant l'algorithme itératif suivant.

Etant donné une valeur initiale x_0, on pose

$$x_{n+1} = g(x_n), \forall n \geq 0 \tag{3.18}$$

On dit que (3.18) est une itération de point fixe et g la fonction d'itération associée. On appelle parfois (3.18) itération de Picard ou itération fonctionnelle pour la résolution de $f(x) = 0$. Le choix de g n'est pas unique. Par exemple, toute fonction de la forme $g(x) = x + F(f(x))$, où F est une fonction continue telle que $F(0) = 0$, est une fonction d'itération possible.

Le résultat suivant donne des conditions pour que la méthode du point fixe (3.18) converge vers la racine α du problème $f(x) = 0$.

Sous des hypothèses convenables sur la fonction g (voir théorème 3.7 , page 133 – 134 dans [6]), l'itération (3.18) converge vers α pour toute valeur initiale x_0 suffisamment proche de α, avec une vitesse de convergence égale à **s**. Telles que

$$g(\alpha) = \alpha, g^{(1)}(\alpha) = g^{(2)}(\alpha) = ... = g^{(s-1)}(\alpha) = 0, g^{(s)}(\alpha) \neq 0, s \in \mathbb{N}^* \tag{3.19}$$

Notre objectif est d'améliorer la vitesse de convergence de la suite $(x_n)_n$. Pour cela, on cherche une fonction g telles que

1. La fonction g doit être vérifier les conditions de (3.19) pour $\alpha = \frac{1}{a}$.
2. La fonction g ne doit pas avoir de l'inverse de a dans ses coefficients.

On choisit g sous la forme

$$g(x) = x + x\gamma(x) = x(1 + \gamma(x)) \tag{3.20}$$

On obtient

$$\begin{cases} g^{(1)}(x) &= 1 + \gamma(x) + x\gamma^{(1)}(x) \\ g^{(k)}(x) &= k\gamma^{(k-1)}(x) + x\gamma^{(k)}(x), k \geq 2 \end{cases} \tag{3.21}$$

On distingue les cas suivants :

3.3.1 Cas 1 : *s=2*

Si g vérifie la relation

$$g\left(\frac{1}{a}\right) = \frac{1}{a}, g^{(1)}\left(\frac{1}{a}\right) = 0, g^{(2)}\left(\frac{1}{a}\right) \neq 0 \tag{3.22}$$

Alors, la fonction γ vérifie

$$\gamma\left(\frac{1}{a}\right) = 0, \gamma^{(1)}\left(\frac{1}{a}\right) = -a \tag{3.23}$$

On cherche la fonction γ de manière à faire disparaître l'inverse de a dans les coefficients de g. Pour cela, on prend

$$\gamma(x) = \alpha_0 + \alpha_1 x \tag{3.24}$$

D'après (3.23), on obtient

$$\begin{cases} \alpha_0 + \alpha_1 \cdot \frac{1}{a} = 0 \\ \alpha_1 = -a \end{cases} \Longrightarrow \begin{cases} \alpha_0 = 1 \\ \alpha_1 = -a \end{cases}$$

Par conséquent

$$\gamma(x) = 1 - ax \tag{3.25}$$

Ce qui donne

$$g(x) = x(1 + (1 - ax))$$

La suite associée à la fonction g est définie par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - ax_n)) = x_n \cdot (2 - ax_n) \tag{3.26}$$

Cette suite représente la suite de la méthode de Newton.

Remarque 3.3.1 *Dans le cas où $s = 1$, on prend $\gamma(x) = \alpha_0$, on trouve $\alpha_0 = 0$ et $g(x) = x$.*

3.3.2 Cas 2 : *s=3*

Supposons que

$$g\left(\frac{1}{a}\right) = \frac{1}{a}, g^{(1)}\left(\frac{1}{a}\right) = g^{(2)}\left(\frac{1}{a}\right) = 0, g^{(3)}\left(\frac{1}{a}\right) \neq 0 \tag{3.27}$$

Alors

$$\gamma\left(\frac{1}{a}\right) = 0, \gamma^{(1)}\left(\frac{1}{a}\right) = -a, \gamma^{(2)}\left(\frac{1}{a}\right) = 2a^2 \tag{3.28}$$

On prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 \tag{3.29}$$

D'après (3.28), on obtient

$$\begin{cases} \alpha_0 + \alpha_1 \frac{1}{a} + \alpha_2 \frac{1}{a^2} = 0 \\ \alpha_1 + 2\alpha_2 \frac{1}{a} + a = 0 \\ 2\alpha_2 - 2a^2 = 0 \end{cases}$$

On résout ce système, on trouve

$$\alpha_0 = 2, \alpha_1 = -3a, \alpha_2 = a^2 \tag{3.30}$$

Donc

$$\gamma(x) = 2 - 3ax + a^2x^2 = (1 - ax) + (1 - ax)^2 \tag{3.31}$$

On écrit

$$g(x) = x\left(1 + (1 - ax) + (1 - ax)^2\right) \tag{3.32}$$

La suite des itérations $(x_n)_n$ associée à g est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n \cdot \left(1 + (1 - ax_n) + (1 - ax_n)^2\right) \tag{3.33}$$

Théorème 3.3.1 *Si x_{n_0} est l'inverse de a d'ordre r, alors x_{n+n_0} est l'inverse de a d'ordre ω_n, telle que*

$$\forall n \in \mathbb{N} : \omega_n = 3^n \cdot r$$

La suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\omega'_n}$$

Où

$$\forall n \in \mathbb{N} : \omega'_n = \omega_n - m = 3^n \cdot r - m$$

Preuve.
Soit $(x_n)_n$ la suite définie par (3.33). On a

$$\forall n \in \mathbb{N} : ax_{n+1} - 1 = (ax_n - 1)^3 \tag{3.34}$$

Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^r$$

Alors

$$ax_{n_0+1} - 1 \equiv 0 \bmod p^{3r}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{\omega_n}$$

Où $(\omega_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \omega_n = 3^n \cdot r$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n((1 - ax_n) + (1 - ax_n)^2) \tag{3.35}$$

On déduit

$$\begin{aligned} \left|x_{n+n_0+1} - x_{n+n_0}\right|_p &\leq \left|x_{n+n_0}\right| . \max\left(\left|1 - ax_{n+n_0}\right|, \left|1 - ax_{n+n_0}\right|^2\right) \\ &\leq p^m . \max\left\{p^{-\omega_n}, p^{-2\omega_n}\right\} = p^{-(\omega_n - m)} \end{aligned}$$

Alors

$$x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\omega_n - m}$$

On obtient

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\omega'_n}$$

Telle que

$$\forall n \in \mathbb{N} : \omega'_n = \omega_n - m = 3^n \cdot r - m$$

Conclusion 3.3.1

1. *La vitesse de convergence de la suite $(x_n)_n$ est d'ordre ω'_n.*
2. $n = \left\lceil \dfrac{\ln\left(\frac{M+m}{r}\right)}{\ln 3} \right\rceil$ *est le nombre nécessaire des itérations.*

Exemple 3.3.1 *Soient $a = 3$, $M = 9$, $p = 5$. On a $|3|_5 = 1$, $m = 0$. On prend $x_0 = 2$ puisque*

$$ax_0 = 2 \cdot 3 = 6 \equiv 1 \bmod 5$$

Alors $n_0 = 0$, $r = 1$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln\left(\frac{M+m}{r}\right)}{\ln 3} \right\rceil = \left\lceil \frac{\ln 9}{\ln 3} \right\rceil = 2$$

La formule d'itération est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - 3x_n) \cdot (2 - 3x_n))$$

On obtient

$$\begin{aligned}
x_0 &\equiv 2 \bmod 5 \\
x_1 &= 2 \cdot (1 + (1 - 3 \cdot 2) \cdot (2 - 3 \cdot 2)) = 42 \equiv 2 + 3 \cdot 5 + 1 \cdot 5^2 \bmod 5^3 \\
x_2 &= 42 \cdot (1 + (1 - 3 \cdot 42) \cdot (2 - 3 \cdot 42)) \\
&= 651042 \equiv 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 + 1 \cdot 5^8 \bmod 5^9
\end{aligned}$$

On écrit

$$\begin{cases} \frac{1}{3} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + 1 \cdot 5^6 + 3 \cdot 5^7 + 1 \cdot 5^8 \bmod 5^9 \\ \frac{1}{3} = \cdot 231313131 = \cdot 2\overline{31} \end{cases}$$

Exemple 3.3.2 *Soient $a = 3$, $M = 8$, $p = 2$. On a $|3|_2 = 1$, $m = 0$. On prend $x_0 = 1$ puisque*

$$ax_0 = 3 \cdot 1 \equiv 1 \bmod 2$$

Alors $n_0 = 0$, $r = 1$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln 8}{\ln 3} \right\rceil \simeq 2$$

La formule d'itération est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n \left(1 + (1 - 3x_n) + (1 - 3x_n)^2\right)$$

On obtient

$$x_0 \equiv 1 \bmod 2$$

$$x_1 = 3 \equiv 3 \bmod 8 = 1 + 1 \cdot 2 \bmod 2^3$$

$$x_2 = 171 \equiv 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^5 + 1 \cdot 2^7 \bmod 2^8$$

On écrit

$$\begin{cases} \frac{1}{3} = 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^5 + 1 \cdot 2^7 \bmod 2^8 \\ \frac{1}{3} = \cdot 11010101 = \cdot 11\overline{01} \end{cases}$$

Remarque 3.3.2 *Dans cet exemple, on remarque que cette méthode nécessite seulement deux itérations pour une précision donnée* ($M = 8$)*, ce qui est un grand avantage dans le calcul.*

3.3.3 Cas 3 : *s=4*

Supposons que

$$g\left(\frac{1}{a}\right) = \frac{1}{a}, g^{(1)}\left(\frac{1}{a}\right) = g^{(2)}\left(\frac{1}{a}\right) = g^{(3)}\left(\frac{1}{a}\right) = 0, g^{(4)}\left(\frac{1}{a}\right) \neq 0 \tag{3.36}$$

Alors

$$\gamma\left(\frac{1}{a}\right) = 0, \gamma^{(1)}\left(\frac{1}{a}\right) = -a, \gamma^{(2)}\left(\frac{1}{a}\right) = 2a^2, \gamma^{(3)}\left(\frac{1}{a}\right) = -6a^3 \tag{3.37}$$

On prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 \tag{3.38}$$

D'après (3.37), on obtient

$$\begin{cases} \alpha_0 + \alpha_1 \cdot \frac{1}{a} + \alpha_2 \cdot \frac{1}{a^2} + \alpha_3 \cdot \frac{1}{a^3} = 0 \\ \alpha_1 + 2 \cdot \alpha_2 \cdot \frac{1}{a} + 3 \cdot \alpha_3 \cdot \frac{1}{a^2} + a = 0 \\ 2 \cdot \alpha_2 + 6 \cdot \alpha_3 \cdot \frac{1}{a} - 2 \cdot a^2 = 0 \\ 6 \cdot \alpha_3 + 6 \cdot a^3 = 0 \end{cases}$$

On trouve

$$\alpha_0 = 3, \alpha_1 = -6a, \alpha_2 = 4a^2, \alpha_3 = -a^3. \tag{3.39}$$

Donc

$$\gamma(x) = 3 - 6ax + 4a^2x^2 - a^3x^3 = (1 - ax) + (1 - ax)^2 + (1 - ax)^3 \tag{3.40}$$

On écrit

$$g(x) = x(1 + (1 - ax) + (1 - ax)^2 + (1 - ax)^3) \tag{3.41}$$

La suite des itération $(x_n)_n$ associée à g est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - ax_n) + (1 - ax_n)^2 + (1 - ax_n)^3) \tag{3.42}$$

Théorème 3.3.2 *Si x_{n_0} est l'inverse de a d'ordre t, alors x_{n+n_0} est l'inverse de a d'ordre μ_n, telle que*

$$\forall n \in \mathbb{N} : \mu_n = 4^n \cdot t$$

La suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\mu'_n}$$

Où

$$\forall n \in \mathbb{N} : \mu'_n = \mu_n - m = 4^n \cdot t - m$$

Preuve.
Soit $(x_n)_n$ la suite définie par (3.42). On a

$$\forall n \in \mathbb{N} : ax_{n+1} - 1 = -(ax_n - 1)^4 \tag{3.43}$$

Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^t$$

Alors

$$ax_{n_0+1} - 1 \equiv 0 \bmod p^{4t}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{\mu_n}$$

Où $(\mu_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \mu_n = 4^n \cdot t$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n((1 - ax_n) + (1 - ax_n)^2 + (1 - ax_n)^3) \tag{3.44}$$

On déduit

$$\begin{aligned} |x_{n+n_0+1} - x_{n+n_0}|_p &\leq |x_{n+n_0}|_p \cdot \max\left\{|1 - ax_{n+n_0}|_p, |1 - ax_{n+n_0}|_p^2, |1 - ax_{n+n_0}|_p^3\right\} \\ &\leq p^m \cdot \max\left\{p^{-\mu_n}, p^{-2\mu_n}, p^{-3\mu_n}\right\} = p^{-(\mu_n - m)} \\ &\Longrightarrow x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{(\mu_n - m)} \end{aligned}$$

On obtient

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{\mu'_n}$$

Telle que

$$\forall n \in \mathbb{N} : \mu'_n = \mu_n - m = 4^n \cdot t - m$$

Conclusion 3.3.2

1. *La vitesse de convergence de la suite $(x_n)_n$ est d'ordre μ'_n.*

2. $n = \left\lceil \dfrac{\ln\left(\frac{M+m}{t}\right)}{\ln 4} \right\rceil$ *est le nombre nécessaire des itérations.*

Exemple 3.3.3 *Soient* $a = 3$, $M = 16$, $p = 2$. *On a* $|3|_2 = 1$, $m = 0$. *On prend* $x_0 = 1$ *puisque*

$$ax_0 = 3 \cdot 1 \equiv 1 \bmod 2$$

Alors $n_0 = 0$, $t = 1$.
Le nombre des itérations est

$$n = \left\lceil \frac{\ln 16}{\ln 4} \right\rceil = 2$$

La formule d'itération est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n \left(1 + (1 - 3x_n) + (1 - 3x_n)^2 + (1 - 3x_n)^3\right)$$

On obtient

$$x_0 \equiv 1 \bmod 2$$

$$x_1 = -5 \equiv 11 \bmod 16 = 1 + 1 \cdot 2 + 1 \cdot 2^3 \bmod 2^4$$

$x_2 = -21845 \equiv 43691 \bmod 65536 = 1+1\cdot 2+1\cdot 2^3+1\cdot 2^5+1\cdot 2^7+1\cdot 2^9+1\cdot 2^{11}+1\cdot 2^{13}+1\cdot 2^{15} \bmod 2^{16}$

On écrit

$$\begin{cases} \frac{1}{3} = 1 + 1 \cdot 2 + 1 \cdot 2^3 + 1 \cdot 2^5 + 1 \cdot 2^7 + 1 \cdot 2^9 + 1 \cdot 2^{11} + 1 \cdot 2^{13} + 1 \cdot 2^{15} \bmod 2^{16} \\ \frac{1}{3} = \cdot 1101010101010101 = \cdot 1\overline{101} \end{cases}$$

3.3.4 Généralisation

Supposons que g vérifie la relation

$$g\left(\frac{1}{a}\right) = \frac{1}{a}, g^{(1)}\left(\frac{1}{a}\right) = g^{(2)}\left(\frac{1}{a}\right) = \cdots = g^{(s-1)}\left(\frac{1}{a}\right) = 0, g^{(s)}\left(\frac{1}{a}\right) \neq 0, s \in \mathbb{N}^* \tag{3.45}$$

Alors

$$\gamma\left(\frac{1}{a}\right) = 0, \gamma^{(k)}\left(\frac{1}{a}\right) = (-1)^k \cdot k! \cdot a^k, k = \overline{1, s-1} \tag{3.46}$$

On prend

$$\gamma(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{s-1} x^{s-1} \tag{3.47}$$

On écrit

$$g(x) = x(1 + (1 - ax) + (1 - ax)^2 + \cdots + (1 - ax)^{(s-1)}) \tag{3.48}$$

La suite des itérations $(x_n)_n$ associée à g est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n(1 + (1 - ax_n) + (1 - ax_n)^2 + \cdots + (1 - ax_n)^{(s-1)}) \tag{3.49}$$

Théorème 3.3.3 *Si x_{n_0} est l'inverse de a d'ordre t, alors x_{n+n_0} est l'inverse de a d'ordre l_n, telle que*

$$\forall n \in \mathbb{N} : l_n = s^n \cdot t$$

La suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{l'_n}$$

Où

$$\forall n \in \mathbb{N} : l'_n = l_n - m = s^n \cdot t - m$$

Preuve.
Soit $(x_n)_n$ la suite définie par (3.49). On a

$$\forall n \in \mathbb{N} : ax_{n+1} - 1 = -(ax_n - 1)^s \tag{3.50}$$

Supposons que

$$ax_{n_0} - 1 \equiv 0 \bmod p^t$$

Alors

$$ax_{n_0+1} - 1 \equiv 0 \bmod p^{st}$$

Par conséquent

$$\forall n \in \mathbb{N} : ax_{n+n_0} - 1 \equiv 0 \bmod p^{l_n}$$

Où $(l_n)_n$ est définie par

$$\forall n \in \mathbb{N} : l_n = s^n \cdot t$$

D'autre part, on a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = x_n((1 - ax_n) + (1 - ax_n)^2 + \cdots + (1 - ax_n)^{(s-1)}) \tag{3.51}$$

On déduit

$$\begin{aligned} |x_{n+n_0+1} - x_{n+n_0}|_p &\leq |x_{n+n_0}|_p \cdot \max\left\{|1 - ax_{n+n_0}|_p, |1 - ax_{n+n_0}|_p^2, \cdots, |1 - ax_{n+n_0}|_p^{(s-1)}\right\} \\ &\leq p^m \cdot \max\left\{p^{-l_n}, p^{-2l_n}, \cdots, p^{(1-s)l_n}\right\} = p^{-(l_n - m)} \\ &\Longrightarrow x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{(l_n - m)} \end{aligned}$$

On obtient

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \bmod p^{l'_n}$$

Telle que

$$\forall n \in \mathbb{N} : l'_n = l_n - m = s^n \cdot t - m$$

Conclusion 3.3.3

1. *La vitesse de convergence de la suite $(x_n)_n$ est d'ordre l'_n.*
2. $n = \left[\dfrac{\ln\left(\frac{M+m}{t}\right)}{\ln s}\right]$ *est le nombre nécessaire des itérations.*

Conclusion Générale

Pour tout nombre premier p, on considère les ensembles suivants :

$$B_1 = \{a \in \mathbb{Q}_p : |a|_p = 1\} \text{ si } m = 0$$

$$B_2 = \{a \in \mathbb{Q}_p : |a|_p < 1\} \text{ si } m > 0$$

$$B_3 = \{a \in \mathbb{Q}_p : |a|_p > 1\} \text{ si } m < 0$$

1) Si $m < 0$, alors pour tout nombre p-adique appartient à B_3, la vitesse de convergence est plus rapide que celle de B_1.
2) Si $m > 0$, alors pour tout nombre p-adique appartient à B_2, la vitesse de convergence est moins rapide que celle de B_1.

Bibliographie

[1] Alain M. Robert, *A Course in p-adic Analysis*. Graduate Texts in Mathematics, 198. Springer-Verlag New York, Inc. 2000.

[2] Alfio Quarteroni, Riccardo Sacco,Fausto Saleri, *Méthodes Numériques Algorithmes, analyse et applications.* Springer-Verlag Italia, Milano 2004.

[3] Bachman, G. *Introduction to p-adic Numbers and Valuation Theory*. Academic Press, New York, 1964.

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

[5] Fredrik Bajers. Vej, *P-adic Numbers*. Aalborg University. Departement Of Mathematical Sciences. 7E 9222 Aalborg ∅st. Groupe E3-104, 18-12-2000.

[6] J. Epperson, *An Introduction to Numerical Methods and Analysis*. Wiley and Sons, 2002.

[7] Michael P. Knapp, Christos Xenophontos, *Numerical analysis meets number theory : using rootfinding methods to calculate inverses modp^n*. Appl. Anal. Discrete Math. (4) 23-31, 2010.

[8] N. Koblitz, p-adic numbers, *p-adic analysis and zeta functions*. Second edition, Springer-Verlag, 1984.

[9] S. Katok, *Real and p-adic analysis*. Course notes for Math 497C, Mass Program, Fall 2000. University Park, PA 16802, U.S.A.

[10] R. T. Gregory, E. V. Krishnamurthy, *Methods and Applications of Error-Free Computation*. Springer-Verlag New York Inc. 1984.

[11] Schikhof W.H, *Ultrametric calculus, An introduction to p-adic analysis*. Combridge university press (1984).

Résumé

Ce travail est une application très intéressante des outils de l'analyse de numérique à un espace ultramétrique noté $(\mathbb{Q}_p, |.|_p)$. Nous avons utilisé les méthodes numériques élémentaires, telles que la méthode de newton, sécante et du point fixe pour calculer le développement de Hensel (les premiers chiffres) de l'inverse d'un nombre p-adique non nul $a \in \mathbb{Q}_p^*$. Autrement dit, chercher l'écriture

$$\frac{1}{a} = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_k p^k$$

Nous avons étudié le coût de chaque méthode, dont la vitesse de convergence, le nombre nécessaire des itérations pour une précision donnée. Nous avons également présentés des tests numériques pour chaque méthode.

Mots clés : espace ultramétrique, Norme p-adique, nombre p-adique, méthode de Newton, sécante, point fixe, ordre de convergence.

Abstract

This work is a very interesting application of tools from numerical analysis to ultrametric space denoted by $(\mathbb{Q}_p, |.|_p)$. We used the basic numerical methods such as Newton, secant and fixed point method to calculate the development of Hensel (the first digits) the inverse of a nonzero p-adic number $a \in \mathbb{Q}_p^*$. In other words, find the writing

$$\frac{1}{a} = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_k p^k$$

We studied the cost of each method, such as the rate of convergence, the necessary number of iterations for a given precision. We also presented numerical tests for each method.

Keywords: ultrametric space, p-adic norm, p-adic number, Newton's method, secant, fixed point, rate of convergence.