الجمهوريـة الجزائـريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire
وزارة التعليـم العالـي والبحـث العلمـي
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

Méthode de Householder pour résoudre les équations polynomiales p-adiques.

Préparé par :
Aissaoui Ilham
Bouarnouna Chaima

Soutenue devant le jury

Halim Yacine	**M C A**	**C. U. Abdelhafid Boussouf, Mila**	**Président**
Kecies Mohamed	**M C B**	**C. U. Abdelhafid Boussouf, Mila**	**Rapporteur**
Bourourou Siham	**M C B**	**C. U. Abdelhafid Boussouf, Mila**	**Examinatrice**

Année universitaire :2022/2023

Remerciements

Chaque fois qu'on achève une étape importante dans notre vie, on fait une pose pour regarder en arrière et se rappeler toutes ces personnes qui ont partagé avec nous tous les bons moments de notre existence, mais surtout les mauvais.

Avant.tout Nos remerciements s'adressent en premier lieu à Allah le tout puissant pour la volonté, la santé et la patience qu'il nous a donné durant la réalisation de ce modeste mémoire, ainsi que le long de notre cursus d'étude.

Ainsi, nous tenons également à exprimer nos profondes gratitudes à notre encadreur Monsieur MOHAMED KECIES, dont on a profité de son expérience et de son savoir dans la science d'algèbre et d'analyse. Il nous a consacré tout le temps qu'on lui avait demandé et assurer d'avoir voulu proposes la direction de ce mémoire sa disponibilité, son soutien ses encouragement et ses précieux. On a tellement appris de son dévouement exemplaire et son point positif face à tout obstacle.

Nos remerciements vont aussi à tous nos enseignants qui ont contribué à notre formation et à tous les membres du jury qui ont accepté de juger notre modeste travail, à tous responsables, ingénieurs et techniciens de l'institut des sciences et de technologie et de l'univers

Enfin, nous tenons à exprimer notre sincère salutation à tous nos collègues et amis pour le soutien moral.

Dédicace

Je voudrais dédier cet humble mémoire

mes très chers parents :

Rabia et Rafika , Fatima et Abdelwheb, Pour leur dévouement et leur présence permanente. Ils n'ont cessé de me soutenir pendant tout mon parcours. Je leur exprime toute ma gratitude pour leur soutien qui m'a permis d'être à ce niveau. Puisse Dieu, le tout puissant, vous préserver et vous accorder santé, longue vie.

A mes adorables frères et soeurs :

plein de joie, de réussite et de sérénité. Je vous exprime à travers ce mémoire mes sentiments de fraternité et d'amour.

Á toute ma promotion · · ·

En témoignage des souvenirs de tous les moments que nous avons passé ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur. Puisse ce diplôme nous réserver à tous des lendemains meilleurs.

Les études sont avant tout · · · Notre unique et seul atout

TABLE DES MATIÈRES

INTRODUCTION GÉNÉRALE

Pour tout p premier, les nombres p-adiques ont été inventés, aux alentours de 1900 par le 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 est non archimédienne nommée valeur absolue p-adique. On obtient sur ce corps une analyse différente de l'analyse usuelle sur les réels, que l'on appelle analyse p-adique. Lorsque ces nombres ont été introduits, ils étaient considérés comme une partie exotique des mathématiques pures sans aucune application. Néanmoins, diverses applications à d'autres domaines des mathématiques, en particulier en analyse, en géométrie algébrique et dans des domaines connexes des sciences appliquées par exemple, la physique, la bioinformatique, la théorie des nombres et la Géométrie. 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 et pour plus de détails nous renvoyons les lecteurs à [2, 3, 4, 5, 13, 17, 18].

D'un point de vue théorique, la création de ces nombres ouvre la voie à la construction du corps des nombres p-adiques $\mathbb{Q}_p$ comme complétion de $\mathbb{Q}$ radicalement différente du corps des réels $\mathbb{R}$. Le lemme de Hensel, qui est un résultat important en théorie des nombres, joue un rôle important dans l'étude du corps $\mathbb{Q}_p$ et l'ensemble des entiers p-adiques $\mathbb{Z}_p$ en fournissant des conditions suffisantes pour l'existence de racines en $\mathbb{Z}_p$ de polynômes de $\mathbb{Z}_p[x]$. Une application classique de ce lemme, qui a récemment retenu l'attention des mathématiciens, traite du problème de la recherche des racines d'un nombre p-adique a dans $\mathbb{Q}_p$. De nombreux efforts ont été faits pour trouver des solutions d'équations p-adiques, mais il était difficile de le trouver tout de suite, alors les gens ont commencé à rechercher des moyens de calculer les solutions approchées en utilisant des méthodes numériques. En fait, plusieurs études ont été faites en ce qui concerne la recherche de racines carrées et de racines cubiques de nombres p-adiques en utilisant les méthodes numériques de base (Sécante, Newton, point fixe, Halley) (par exemple [7, 9, 10, 11, 15, 16]).

Dans ce travail, nous allons présenter une dérivation simple de la méthode de Newton, nommée méthode de Householder. Cette méthode a été découverte par Alston Scott Householder (un mathématicien Américain 1904-1993), elle s'applique à une fonction de

C^2 (i.e, f' et f'' sont continues) pour trouver la racine approchée de l'équation $f(x) = 0$. En particulier, nous considérons le problème de recherche de racine de $f(x) = x^2 - a$, où $a \in \mathbb{Q}_p$ dans le cadre p-adique, et cherchons à trouver une racine de cette équation en utilisant l'analogue p-adique de la méthode bien connue de Householder. On verra comment utiliser cette méthode pour calculer les développements finis p-adiques des racines carrées de $a \in \mathbb{Q}_p$ à l'aide de suites de nombres p-adiques construite par cette méthode. On va étudier aussi la performance cette méthode dont la vitesse de convergence et le nombre nécessaire des itérations pour que la suite $(x_n)_n$ soit proche de la racine avec une précision donnée M qui représente le nombre de chiffres p-adiques dans le développement de $\sqrt{a}$.

Ce mémoire est composé de l'introduction générale et trois chapitres. 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 les premiers chiffres du développement p-adique des racines carrées d'un nombre p-adique à l'aide de suite de nombres p-adiques construite par la méthode de Householder. On termine ce mémoire par une conclusion générale.

CHAPITRE 1

CORPS VALUÉS ULTRAMÉTRIQUES COMPLETS

Le but de ce chapitre est d'exposer les différents concepts et notions indispensables à l'étude des autres chapitres qui viennent ultérieurement. On va rappeler quelques définitions et propriétés élémentaires qui concernent les espaces complets ultramétriques muni d'une valeur absolue elle-même ultramétrique qui vérifie une condition plus forte que l'inégalité triangulaire. Les espaces pour lesquels le critère de Cauchy est une condition nécessaire et suffisante de convergence (c'est-à-dire, dans lesquels toutes les suites de Cauchy convergent) sont appelés espaces complets. L'étude des espaces complets qui est l'objet de ce chapitre a une place centrale dans l'analyse d'aujourd'hui. La complétude est une propriété qui dépend de la distance, donc il est 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. Dans le procédé de complétion, le rôle principal sera joué par les suites de Cauchy. L'intérêt des suites de Cauchy est que dans des espaces métriques convenables (les espaces complets), on peut vérifier la convergence de certaines suites sans avoir à connaître a priori la limite.

1.1 Corps normés

Définition 1.1.1. *Soit K un corps.*
(1) On appelle une norme sur K toute application $\|\cdot\|$ 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 $\|\cdot\|$ est ultramétrique ou non archimédienne si :

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

c'est à dire une norme qui vérifie une condition plus forte que l'inégalité triangulaire.
(3) Une norme constante $\|\cdot\|$ 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 $\|\cdot\|$ est un morphisme de groupes entre les groupes multiplicatifs $(K^*, \cdot)$ et $(\mathbb{R}_+^*, \cdot)$ et donc que $\|1\| = 1$.*

Définition 1.1.2. *Soit K un corps, on dit que la norme $\|\cdot\|$ est archimédienne si*

$$\forall x, y \in K, x \neq 0, \exists n \in \mathbb{N} : \|nx\| > \left\|y\right\|.$$

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

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

Définition 1.1.3.

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

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

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

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

   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 archimédienne.*

Nous donnons maintenant un critère pour qu'une norme soit non-archimédienne.

Proposition 1.1.1. *K est un corps ultramétrique si et seulement si*

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

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

Preuve. Pour la démonstration de cette proposition, nous renvoyons le lecteur à [14]. □

Corollaire 1.1.1. *Soit K un corps, alors la norme $\|\cdot\|$ est archimédienne si et seulement si* $\sup\{\|n\|, n \in \mathbb{Z}\} = \infty$.

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 $(K, \|\cdot\|)$ 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 1.1.4. *Soit $(x_n)_n \subset (K, \|\cdot\|)$. 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 $\lim\limits_{n,m\to\infty} \|x_n - x_m\| = 0$.
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.*

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

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

$(x_n)_n$ 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 $\|\cdot\|_K$ et $\widehat{K}$ un autre corps normé (construit à partir de K) muni d'une norme $\|\cdot\|_{\widehat{K}}$. On dit que $\widehat{K}$ est le complété de K si

1. *$\widehat{K}$ contient $K(K \subset \widehat{K})$.*
2. *K est dense dans $\widehat{K}$ par rapport à la topologie associé avec $\|\cdot\|_{\widehat{K}}$.*
3. *$\forall x \in K : \|x\|_K = \|x\|_{\widehat{K}}$ (la norme $\|\cdot\|_{\widehat{K}}$ est définie à partir de $\|\cdot\|_K$).*
4. *$(\widehat{K}, \|\cdot\|_{\widehat{K}})$ est complet.*

Si un espace métrique n'est pas complet, nous pouvons toujours le compléter en lui ajoutant les limites de toutes les suites de Cauchy modulo une relation d'équivalence. Dans le cas où le corps $\mathbb{Q}$ est muni de la norme euclidienne $|\cdot|$, 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 $(K, \|\cdot\|)$.
On définit sur $SC(K)$ les lois suivantes :

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

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

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

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

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

$$\leq \|b_n\| \cdot \|a_n - a_m\| + \|a_m\| \cdot \|b_n - b_m\|$$

$$\leq \beta\|a_n - a_m\| + \alpha\|b_n - b_m\|.$$

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

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

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

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

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

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

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

Théorème 1.2.1. *[13] L'ensemble quotient $\widehat{K} = SC(K)/SN(K)$ est un corps.*

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

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

Proposition 1.2.1. *L'application $\|\cdot\|_{\widehat{K}}$ est une norme sur $\widehat{K}$. Elle est non-archimédienne si la norme de K est non-archimédienne aussi.*

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

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

D'autre part, on sait que

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

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 $(\mathbb{R}, |\cdot|)$ complet, alors elle a une limite $l \in \mathbb{R}^+$. Donc $\lim_{n\to+\infty} \|a_n\|_K$ existe.
Supposons que $\{a_n\}_n$ et $\{a'_n\}_n$ sont deux représentants de A. Alors par la même inégalité, nous avons

$$0 \leq \lim_{n\to+\infty} |\|a_n\|_K - \|a'_n\|_K| \leq \lim_{n\to+\infty} \|a_n - a'_n\|_K = 0.$$

Alors $\lim_{n\to+\infty} \|a_n\|_K = \lim_{n\to+\infty} \|a'_n\|_K$.
On vérifie les trois propriétés de la norme :

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

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

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

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

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

$$\exists c \in \mathbb{R}_+^*, \exists N \in \mathbb{N}^* : \|a_n\|_K \geq c > 0, \forall n \geq N$$

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

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

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

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

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

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

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

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

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

Supposons maintenant que $\|\cdot\|_K$ est ultramétrique, pour montrer que $\|\cdot\|_{\widehat{K}}$ est ultramétrique sur $\widehat{K}$, on a besoin du résultat suivant.

Lemme 1.2.1. *[14] Soient K un corps muni de la norme non-archimédienne $\|\cdot\|_K$, 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.

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

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

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

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

Donc

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

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

Théorème 1.2.2. *[13]*
L'espace $\widehat{K}$ muni de la norme $\|\cdot\|_{\widehat{K}}$ est complet. De plus K est un sous-ensemble dense dans $\widehat{K}$.

CHAPITRE 2

CORPS DES NOMBRES $P-$ADIQUES

Dans ce chapitre, nous allons construire les corps des nombres p-adiques en complétant $\mathbb{Q}$ muni de ses valeurs absolues ultramétriques. Nous allons présenter aussi les propriétés du corps $\mathbb{Q}_p$, à savoir, le développement de Hensel qui est une autre façon de représenter un nombre p-adique, quelques propriétés analytiques et topologiques de ce corps et le lemme de Hensel, qui est un résultat fondamental et certainement l'un des plus importants.

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.*

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

Ceci est équivalent à

$$v_p(x) = \max\left\{r \in \mathbb{Z}^+ : x \equiv 0 \mod p^r\right\}.$$

Dans ce cas x s'écrit

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

tel que (u,p) désigne le pgcd de u et de p.

2. *La valuation p−adique d'un nombre rationnel non nul $x \in \mathbb{Q}^*$ est définie par*

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

Remarque 2.1.1.
1) *La valuation p−adique compte le nombre de fois que l'on peut diviser un nombre par p.*

2) 0 *est divisible une infinité de fois par p, alors* $v_p(0) = +\infty$.
3) *Soit r un nombre rationnel. Alors r est entier si et seulement si* $v_p(r) \geq 0$ *pour tout nombre premier p.*
4) *On a* $v_p(1) = 0$ *et pour tout* $k \in \mathbb{Z}^*, v_p(p^k) = k$, *et* $v_p(0) = +\infty$. *Ceci garantit que* v_p *est une application surjective. Par contre* v_p *n'est pas injective puisque par exemple* $v_p(p) = v_p(-p) = 1$.

Exemple 2.1.1.
1)*Si n non nul se décompose sous la forme* $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$, *alors* $v_{p_i}(n) = m_i$ *pour tout* $1 \leq i \leq k$, *et* $v_p(n) = 0$ *si p est distinct des* p_i. *Ainsi,* $v_p(n) = 0$ *sauf pour un nombre fini de p premiers.*
2) ***Formule de Legendre*** *: Il est possible de déterminer les valuations p−adiques d'une factorielle ; Si p est un nombre premier. Pour tout entier positif* $n \in \mathbb{N}$, *soit* $n = \sum_{i=0}^{k} a_i p^i$ *son expansion dans la base p. Nous avons alors*

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

Où $S_p(n) = \sum_{i=0}^{k} a_i$ *la somme des chiffres de n en base p.*
Par exemple, soit $n = 1000$, *alors*

$$n = 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 = 1000.$$

Ce qui donne

$$v_2(1000!) = \frac{1000 - S_2(1000)}{2-1} = 1000 - 6 = 994.$$

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

1. *Si* $x = \frac{a}{b} \in \mathbb{Q}^*$, *alors* $v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.
2. $v_p(x \cdot y) = v_p(x) + v_p(y), \forall x, y \in \mathbb{Q}$.
3. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}, \forall x, y \in \mathbb{Q}$.

Preuve.

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

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

   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

(a) 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.

(b) 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 $|\cdot|_p$ définie par*

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

avec $v_p(x)$ représente la valuation $p-$adique de x. L'application $|\cdot|_p$ 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*

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

Exemple 2.2.1. .

1. *Pour* $x = \dfrac{99}{140} = \dfrac{3^2 \cdot 11}{2^2 \cdot 5 \cdot 7} = 2^{-2} \cdot 5^{-1} \cdot 7^{-1} \cdot 3^2 \cdot 11 \in \mathbb{Q}$. *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

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

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

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

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

□

Remarque 2.2.1.
1) Si dans la définition (2.2.1) *au lieu d'un nombre premier* p, *nous utilisons un nombre entier arbitraire* $m > 1$, *alors l'axiome* (*ii*) *de la définition* (1.1.1) *peut échouer. Par exemple, soit* $m = 4$.

Alors $|2|_4 = 1$, *mais* $|2.2|_4 = \frac{1}{4} \neq |2|_4 . |2|_4 = 1$.
2) Selon la proposition (1.1.2), *si* $|x|_p \neq \left|y\right|_p$ *alors*

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

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

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

b) Valeur absolue ordinaire

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

c) Valeur absolue p−adique $|\cdot|_p$.

4) Les normes $|\cdot|_{p_1}$ *et* $|\cdot|_{p_2}$ *ne sont pas équivalentes si* p_1 *et* p_2 *sont des nombres premiers différents. En effet, pour la suite* $x_n = \left(\frac{p_1}{p_2}\right)^n$, *on a* $|x_n|_{p_1} \longrightarrow$ *mais* $|x_n|_{p_2} \longrightarrow \infty$, *lorsque* $n \longrightarrow \infty$.

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. *Il est clair que l'ensemble des entiers relatifs* $\mathbb{Z}$ *est un ensemble non borné pour la distance usuelle sur* $\mathbb{R}$ *induite par la valeur absolue archimédienne* $|\cdot|_\infty$. *Par contre, si p désigne un nombre premier, tout entier n s'écrit sous la forme* mp^r *où r est un entier positif et m un entier relatif premier à p donc*

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

ce qui implique que l'ensemble $\mathbb{Z}$ est borné pour toute valeur absolue $p-$adique $|\cdot|_p$.

Le résultat suivant est une conséquence immédiate de l'unicité de la décomposition d'un entier en produit de facteurs premiers, mais est très important ; c'est ce qui justifie la normalisation utilisée pour $|\cdot|_p$. Il donne aussi la relation entre les différentes normes $p-$adiques.

Théorème 2.2.3 (*Formule du produit*)**.**
Pour tout nombre rationnel non nul $a \in \mathbb{Q}^*$, on a

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

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

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

□

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

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

2.3 Nombres $p-$adiques

L'espace métrique $\left(\mathbb{Q}, d_p\right)$ 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 $|\cdot|$, 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 $\mathbb{Q}_p$. On définit $\mathbb{Q}_p$, corps des nombres $p-$adiques, comme le complété de $\mathbb{Q}$ pour la norme $p-$adique $|\cdot|_p$, c'est-à-dire que l'on prend, comme pour définir $\mathbb{R}$, l'anneau des suites de Cauchy (pour la norme $|\cdot|_p$) d'éléments de $\mathbb{Q}$, et on quotiente par l'ensemble des suites tendant vers 0.

On va donner un exemple de suite de Cauchy non convergente pour $p = 5$.

Exemple 2.3.1. *On définit deux suites $(a_n)_n$ et $(x_n)_n$ de $\mathbb{Q}$ par $x_0 = a_0 = 2$ et si $x_{n-1} = a_0 + a_1 5 + \cdots + a_{n-1}5^{n-1}$ est définie, on détermine $a_n \in \{0,1,2,3,4\}$ et $x_n = x_{n-1} + a_n 5^n$ par la congruence $x_n^2 + 1 \equiv 0 \mod 5^n$.*
Il est très facile de voir que la suite $(x_n)_n$ est bien définie, et qu'elle est de Cauchy (car $|x_n - x_{n-1}|_p \leq |5^n|_5 = \frac{1}{5} \longrightarrow 0, n \longrightarrow \infty$). Cependant, elle ne peut converger vers $x \in \mathbb{Q}$. En effet, supposons qu'elle converge p−adiquement vers $r \in \mathbb{Q}$, alors

$$x_n^2 + 1 \longrightarrow r^2 + 1.$$

D'autre part, par notre construction, $x_n^2 + 1 \longrightarrow 0$. D'où $r^2 + 1 \longrightarrow 0$ ce qui est impossible dans $\mathbb{Q}$.

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.*
3. *Si $a \in \mathbb{Q}_p$ et $a \equiv 0 \mod p^n, \forall n \geq 1$, alors $a = 0$.*
4. *Pour tout $x \in \mathbb{R}$, on a*
$$|x| \leq |x + x|.$$
5. *Pour tout $x \in \mathbb{Q}_p$, on a*
$$|x + x|_p \leq |x|_p,$$
car
$$\forall x, y \in \mathbb{Q}_p : \left|x + y\right|_p \leq \max\left\{|x|_p, \left|y\right|_p\right\}$$
$$\Longrightarrow |x + x|_p \leq |x|_p.$$

Lemme 2.3.1. *Soit $a \in \mathbb{Q}$ tel que $|a|_p = 1$. Il existe $\alpha \in \mathbb{N}$ tel que $0 \leq \alpha \leq p-1$ et $|a - \alpha|_p \leq \left|p\right|_p = p^{-1}$.*

Preuve. Soit $a \in \mathbb{Q}$, a peut s'écrire sous la forme $a = p^{v_p(a)}\frac{m}{n}$, avec $(m,n) = 1$ et $v_p(m) = 0 = v_p(n)$. Alors
$$|a|_p = \left|p\right|_p^{v_p(a)} = 1 \Longleftrightarrow v_p(a) = 0.$$

Ainsi, $a = \frac{m}{n}$ avec $(n,p) = 1 = (m,p)$ et il existe $s,t \in \mathbb{Z}$ tels que $pt + sn = 1$. On en déduit que $a - sm = \frac{m(1-sn)}{n}$ et que

$$|a - sm|_p = \frac{|m|_p}{|n|_p}.|1 - sn|_p = \left|pt\right|_p \leq \left|p\right|_p = p^{-1}.$$

Par division euclidienne, on a $sm = pk + \alpha$, avec $0 \leq \alpha \leq p-1$ et

$$|sm - \alpha|_p = \left|p\right|_p . |k|_p \leq \left|p\right|_p = p^{-1}.$$

D'où

$$|a - \alpha|_p = |a - sm + sm - \alpha|_p \leq \max\left\{|a - sm|_p , |sm - \alpha|_p\right\} \leq \left|p\right|_p = p^{-1}.$$

De plus $|a|_p = |\alpha|_p = 1$. □

La bonne façon de voir $\mathbb{Q}_p$ est décrite dans le théorème suivant :

Théorème 2.3.2. *[13] 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*

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

Corollaire 2.3.1. *Soit $x \in \mathbb{Q}_p$, alors il existe une unique suite $(\alpha_n)_n$ où $0 \leq \alpha_n < p$ et un entier n_0 tels que pour $n < n_0, \alpha_n = 0$ et que $x = \sum_{n \geq n_0} \alpha_n p^n$. Cette série est appelée développement de Hensel de x.*

Conclusion 2.3.1.

1. *La suite de Cauchy (λ_n) qui vérifie les conditions 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 $a = \beta_n\beta_{n+1}\cdots\beta_0\beta_1\ldots$ 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) *$a = \cdot 00\ldots0\beta_0\beta_1\ldots$, si $n > 0$.*
4. *On note par $[a]$ la partie entière (régulière) d'un nombre p−adique $a \in \mathbb{Q}_p$, telle que*

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

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

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

donc, on obtient la décomposition suivante

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

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

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

Par conséquent

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

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

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

□

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 la boule unité fermée de $\mathbb{Q}_p$.*
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. *L'ensemble $(\mathbb{Z}_p, +, .)$ est un sous-anneau de $\mathbb{Q}_p$ fermé et intègre qui contient $\mathbb{Z}$.*

Preuve. La multiplicativité de $|\ |_p$ montre que $\mathbb{Z}_p$ est stable par multiplication et l'inégalité ultramétrique montre que $\mathbb{Z}_p$ est stable par addition, de plus $0 \in \mathbb{Z}_p$. C'est donc un sous-anneau de $\mathbb{Q}_p$ qui contient $\mathbb{Z}$ de manière évidente et qui est fermé puisque c'est l'image inverse de $[0, 1]$ par l'application $x \longrightarrow |x|_p$.

D'autre part, soient $x, y \in \mathbb{Z}_p : x.y = 0$. Alors

$$\begin{aligned} \left|x.y\right|_p &= 0 \Longrightarrow |x|_p \,.\, \left|y\right|_p = 0 \\ &\Longrightarrow \begin{cases} |x|_p = 0 \\ ou \\ \left|y\right|_p = 0 \end{cases} \\ &\Longrightarrow \begin{cases} x = 0 \\ ou \\ y = 0. \end{cases} \end{aligned}$$

De plus, on sait que

$$\begin{aligned} &\forall x \in \mathbb{Z} : v_p(x) \geq 0 \\ &\Longrightarrow \left|x_p\right| \leq 1 \\ &\Longrightarrow x \in \mathbb{Z}_p. \end{aligned}$$

□

Remarque 2.4.2. *Les nombres p-adiques dépendent réellement du choix du nombre premier p. En effet, pour $p_1 \neq p_2$ deux nombres premiers distincts, les anneaux $\mathbb{Z}_{p_1}$ et $\mathbb{Z}_{p_2}$ sont différents et de même pour $\mathbb{Q}_{p_1}$ et $\mathbb{Q}_{p_2}$.*

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

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

Remarque 2.4.3. *$(\mathbb{Z}_p^{\times}, .)$ est un groupe (groupe des éléments inversibles de $\mathbb{Z}_p$)*

Proposition 2.4.2. *Tout entier p-adique $x \in \mathbb{Z}_p$ peut être représenté de manière canonique unique sous la forme $x = p^v.u$, où $v = v_p(x)$ est la valuation p-adique de x et $u \in \mathbb{Z}_p^{\times}$ est une unité p-adique.*

Preuve.

1) **Existence :** Soit $x \in \mathbb{Z}_p$, alors x s'écrit sous la forme

$$\begin{cases} x = p^{v_p(x)} \cdot u \\ (u, p) = 1 \\ v_p(x) \geq 0. \end{cases}$$

Alors $u = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$ avec $0 \leq \alpha_i \leq p-1$, on obtient

$$|u|_p = 1.$$

2) **Unicité :** Supposons que x admet deux représentations

$$\begin{cases} x = u_1.p^{m_1}, u_1 \in \mathbb{Z}_p^\times, m_1 \in \mathbb{N} \\ \quad\quad et \\ x = u_2.p^{m_2}, u_2 \in \mathbb{Z}_p^\times, m_2 \in \mathbb{N}. \end{cases}$$

Alors

$$u_1 u_2^{-1} = p^{m_2 - m_1}.$$

Or

$$u_1 u_2^{-1} \in \mathbb{Z}_p^\times.$$

Donc

$$v_p(u_1 u_2^{-1}) = 0.$$

Ce qui donne

$$v_p(u_1) = v_p(u_2).$$

Autrement dit

$$m_1 = m_2.$$

Ce qui donne $u_1 = u_2$. Donc l'unicité de la représentation. □

Corollaire 2.4.1. *Nous pouvons encore remarquer que tout nombre p-adique non nul peut s'écrire de manière unique comme $x = p^n \cdot u$ avec $n \in \mathbb{Z}$ et u une unité de $\mathbb{Z}_p$.*

Exemple 2.4.1. *Soient*

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

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

$$\begin{cases} \beta^{(1)} = \cdot 01\overline{40} = 0 + 1 \cdot 5 + 4 \cdot 5^2 + 0 \cdot 5^3 + 4 \cdot 5^4 + 0 \cdot 5^5 \ldots \notin \mathbb{Z}_5^* \\ \beta^{(2)} = 42 \cdot 13\overline{31} = 4 \cdot 5^{-2} + 2 \cdot 5^{-1} + 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \ldots \notin \mathbb{Z}_5^*. \end{cases}$$

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.

On peut se demander comment caractériser les nombres rationnels au sein des nombres p−adiques. Dans le cas réel, les rationnels sont les nombres dont le développement décimal est périodique à partir d'un certain rang. Dans le cas p−adique, le critère est le

même. Le corps $\mathbb{Q}_p$ est la complétion des nombres rationnels $\mathbb{Q}$ et contient $\mathbb{Q}$ comme sous-ensemble dense. Le résultat suivant donne une description des nombres rationnels en tant que nombres $p-$adiques.

Théorème 2.4.4. *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.

Preuve.
i) Pour l'implication réciproque, sans perte de généralité, nous pouvons considérer le cas dans lequel $x \in \mathbb{Z}_p$ (car si $x \in \mathbb{Q}_p$ avec $|x|_p = p^{-m}$, alors on pose $y = p^{-m}.x$ qui dans $\mathbb{Z}_p$) et a une expansion périodique de la forme

$$x = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{k-1} p^{k-1} + \alpha_0 p^k + \alpha_1 p^{k+1} + \alpha_2 p^{k+2} + \cdots$$

Alors le nombre

$$a = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{k-1} p^{k-1}.$$

est un entier rationnel et x peut être exprimé comme suit

$$x = a.\left(1 + p^k + p^{2k} + \cdots\right) = a.\sum_{i=0}^{\infty} \left(p^k\right)^i = a.\frac{1}{1-p^k}.$$

Par conséquent, nous obtenons que x est un nombre rationnel.
ii) Pour l'implication directe, cette partie est assez technique. Une preuve peut être trouvée dans [14]. □

Exemple 2.4.2. *On a*

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

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

Le résultat suivant est un peu magique et très utile pour notre travail.

Lemme 2.4.1. *Soient $x, y \in \mathbb{Q}_p$, alors $x \equiv y \mod p^n$ si et seulement si $\left|x - y\right|_p \leq p^{-n}$.*

Preuve. Soient $x, y \in \mathbb{Q}_p$. Alors

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

□

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 $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ 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 Propriétés topologiques et analytiques des nombres $p-$adiques

2.6.1 Quelques propriétés analytiques

Nous traitons dans cette section quelques propriétés spéciales (analytiques et topologiques) des nombres p-adiques. A propos de suite de Cauchy, noter la propriété remarquable suivante (qui n'est pas vraie pour la valeur absolue ordinaire) :

Théorème 2.6.1. *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 $\lim\limits_{n,m \longrightarrow \infty} |a_m - a_n|_p = 0$. En particulier, pour $m = n + 1$, on obtient $\lim\limits_{n \longrightarrow \infty} |a_{n+1} - a_n|_p = 0$.
D'autre part, supposons que $\lim\limits_{n \longrightarrow +\infty} |a_{n+1} - a_n|_p = 0$. 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

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

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

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

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

Proposition 2.6.1. *[13] (Suites stationnaires) Soit $(x_n)_n$ une suite des nombres p-adiques. Si*

$$\lim_{n\longrightarrow+\infty} x_n = x, x \in \mathbb{Q}_p \text{ et } |x|_p \neq 0.$$

Alors la suite des normes p−adiques $\left\{|x_n|_p : n \in \mathbb{N}\right\}$ doit se stabiliser (ou stationnaire) pour n assez grand, c'est-à-dire qu'il existe N tel que

$$|x_n|_p = |x|_p \,, \forall \geq N.$$

Le fait qu'une série convergente a son terme général qui tend vers 0 est clair, et est partagé par le cas des séries réelles. C'est sa réciproque qui est réellement intéressante (ou plutôt : $p-$adiquement intéressante), et fausse dans le cas réel, par exemple la série harmonique diverge, bien que son terme général tende vers 0. Le théorème(2.6.1) devient un outil important pour déterminer si une série de nombres $p-$adiques converge dans $\mathbb{Q}_p$ ou non.

Définition 2.6.1. *(Séries de nombres p−adiques)*
Soit $\sum_{n=0}^{+\infty} a_n$ une série p−adique (c'est-à-dire, dont le terme général est un nombre p−adique), alors
1) *La série converge si et si la suite de ses sommes partielles converge dans $\mathbb{Q}_p$. Autrement dit*

$$\lim_{n\longrightarrow+\infty} |S_{n+1} - S_n|_p = 0.$$

où $S_n = \sum_{k=0}^{n} a_k$.
2) *La série converge absolument si $\sum_{n=0}^{+\infty} |a_n|_p$ converge dans $\mathbb{R}$.*

Proposition 2.6.2. *Une série p−adique $\sum_{n=0}^{+\infty} a_n$ converge si, et seulement si son terme général tend vers 0 et dans ce cas*

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

Cette propriété peut être considérée comme la propriété la plus forte pour la convergence des séries.

Preuve. On sait que la série converge si et seulement si la suite des sommes partielles $S_n = \sum_{k=0}^{n} a_k$ converge. Mais $a_n = S_{n+1} - S_n$, alors ll résulte du théorème (2.6.1) que a_n tend vers 0 si et seulement si la série converge.
Pour la deuxième partie, nous supposons que $\sum_{n=0}^{+\infty} a_n$ converge ($\sum_{n=0}^{+\infty} a_n = S$). Si $S = 0$, alors il n'y a rien à prouver (ou la preuve est triviale). Sinon, il découle de la proposition (2.6.1) qu'il existe un entier N tel que

$$|S|_p = |S_N|_p \,.$$

D'autre part, comme $a_n \longrightarrow 0$, alors pour N pour assez grand, on a

$$\max_n |a_n|_p = \max\left\{|a_i|_p\,, 1 \leq i \leq N\right\}.$$

Par inégalité triangulaire forte, on obtient

$$|S_N|_p = \left|\sum_{n=0}^{N} a_n\right|_p \leq \max\left\{|a_i|_p\,, 1 \leq i \leq N\right\} = \max_n |a_n|_p\,.$$

ce qui achève la preuve de la proposition. □

Remarque 2.6.2. *Cette propriété est fausse dans* $(\mathbb{R}, |\cdot|)$*, c'est à dire une suite nulle n'implique pas la convergence de la série* $\sum_{n=0}^{\infty} a_n$*. L'exemple le plus évident d'une série dans* $(\mathbb{R}, |\cdot|)$ *dont le terme général tend vers* 0*, mais qui ne converge pas, est la série harmonique* $\sum_{n\geq 1} \frac{1}{n}$*.*

Exemple 2.6.1.

1) *La série de terme général* p^n *converge trivialement, sa somme vaut* $\sum_{n=0}^{+\infty} p^n = \frac{1}{1-p}$*. On a pour* $p = 2$*, on trouve* $\sum_{n=0}^{+\infty} 2^n = -1 = \cdot 11111...$

2) *Si* $(u_n)_{n\in\mathbb{N}}$ *est une suite d'entiers, alors la série de terme général* $a_n = u_n \cdot n!$ *converge dans* $\mathbb{Q}_p$ *pour tout p, et même dans* $\mathbb{Z}_p$ *(car* $\mathbb{Z}_p$ *est fermé). En effet, on a évidemment* $|u_n \cdot n!|_p \leq |n!|_p$ *et* $n! \longrightarrow 0$ *quand* $n \longrightarrow \infty$*.*

2.6.2 Quelques propriétés topologiques

Soit r un réel strictement positif, et a un nombre p-adique. Comme l'espace topologique $\mathbb{Q}_p$ est muni d'une distance, on peut définir des boules ouvertes et fermées : on pose

$$\begin{aligned} B(a,r) &= \left\{x \in \mathbb{Q}_p : d_p(a,x) = |a-x|_p < r\right\} \\ \bar{B}(a,r) &= \left\{x \in \mathbb{Q}_p : d_p(a,x) = |a-x|_p \leq r\right\}. \end{aligned}$$

respectivement les boules ouvertes et fermées en a et de rayon r. Comme l'ensemble des valeurs possibles de $\|_p$ est $p^m, m \in \mathbb{Z}$, on peut considérer uniquement des boules de rayon p^k, où k est un entier relatif. Ces boules sont assez simples à décrire : x_0 est dans la boule fermée de centre a et de rayon p^k si p^k divise $(a - x_0)$.

On note

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

La sphère centrée en a et de rayon r.

Définition 2.6.2. *(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 2.6.3. *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* $(\mathbb{Q}_p, |\cdot|_p)$ *sont isocèles et la longueur de sa base ne dépasse pas les longueurs des côtés.*

Preuve. Cela découle de la proposition (1.1.2). □

Proposition 2.6.4. *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 (2.6.3), on a

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

Alors

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

□

Proposition 2.6.5. *Toute boule* $B(a, r)$ *de* $(\mathbb{Q}_p, |\cdot|_p)$ *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 2.6.6. *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 2.6.7. *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 $(\mathbb{Q}_p, |\cdot|_p)$, alors*

$$B(a,r) \cap B(b,s) \neq \varnothing \Longrightarrow B(a,r) \subset B(b,s) \text{ ou } B(b,s) \subset B(a,r). \tag{2.2}$$

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 (2.6.6)

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

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

2.7 Lemme de Hensel

Dans cette section, nous présentons un résultat classique connu sous le nom de Lemme de Hensel et qui permet, sous certaines conditions, de déduire l'existence d'une racine d'un polynôme à partir de l'existence d'une solution approchée. Ce résultat est très utile pour localiser les zéros des polynômes à coefficients dans $\mathbb{Z}_p$.

Théorème 2.7.1. *[14] (Lemme de Hensel)*
Soit $F(x) = c_0 + c_1x + \cdots + c_nx^n$ *un polynôme dont les cœfficients sont des entiers p-adiques* $\left(c_i \in \mathbb{Z}_p\right)$. *Soit* $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$ *la dérivée de* $F(x)$. *Soit* $\bar{a}_0$ *un entier p-adique tel que* $F(\bar{a}_0) \equiv 0 \mod p$ *et* $F'(\bar{a}_0) \not\equiv 0 \mod p$. *Alors il existe un entier p-adique unique a tel que* $F(a) = 0$ *et* $a \equiv \bar{a}_0 \mod p$.

Remarque 2.7.2.
1) *Les hypothèses de ce théorème peuvent s'écrire aussi en utilisant la norme p−adique sous la forme :* $|F(\bar{a}_0)|_p < 1$, $|F'(\bar{a}_0)|_p = 1$ *et la conclusion* $F(a) = 0$, $|a - \bar{a}_0|_p < 1$.
2) *Pour verifier la condition* $F(\bar{a}_0) \equiv 0 \mod p$ *et* $F'(\bar{a}_0) \not\equiv 0 \mod p$ *il suffit que* $\bar{a}_0$ *soit une racine simple de* $F(x) \mod p$.
3) *On peut choisir* $\bar{a}_0$ *sous la forme* $\bar{a}_0 = d_0 + d_1p + ... + d_np^n + ..., d_i \in \{0, 1, \cdots, p-1\}$.

Exemple 2.7.1. *Soient* $F(x) = x^3 - 2$ *et* $p = 5$. *Alors nous avons* $F(3) = 25 \equiv 0 \mod 5$ *et* $F'(3) = 27 \not\equiv 0 \mod 5$. *Le lemme de Hensel avec approximation initiale* 3, *nous dit qu'il y a une racine cubique unique de* 2 *dans* $\mathbb{Z}_5$ *qui est congruente à* $3 \mod 5$.

Exemple 2.7.2. *Soient* $F(x) = x^2 - 7$ *et* $p = 3$. *Alors nous avons* $F(1) = -6 \equiv 0 \mod 3$ *et* $F'(1) = 2 \not\equiv 0 \mod 3$. *Le lemme de Hensel avec approximation initiale* 1, *nous dit qu'il y a une racine carrée de* 7 *dans* $\mathbb{Z}_3$ *qui est congruente à* $1 \mod 3$.

2.7.1 Carrés de $\mathbb{Q}_p^*$

Nous allons présenter ici une application du lemme de Hensel qui nous permet de déterminer les éléments de $\mathbb{Q}_p$ qui sont des carrés.

Proposition 2.7.1.
1) Supposons que $p \neq 2$. *Soit* $a = p^{v_p(a)} \cdot u \in \mathbb{Q}_p$ *un nombre p-adique non nul avec* $u \in \mathbb{Z}_p^\times$. *Alors a*

est un carré dans $\mathbb{Q}_p$ si et seulement si $v_p(a)$ est paire ($n \equiv 0 \mod 2$) et l'image de u dans $\mathbb{Z}_p^\times$ est un carré. ie $x = p^{2n}y^2$
2) Supposons que $p = 2$, alors pour qu'un élément $a = 2^{v_2(a)}.u \in \mathbb{Q}_2^*$ soit un carré, il faut et il suffit que $v_2(a)$ soit paire et $u \equiv 1 \mod 8$.

Preuve.
Soit $a \in \mathbb{Q}_p^*$, alors a s'écrit sous la forme

$$\begin{cases} a = p^{v_p(a)}.u, u \in \mathbb{Z}_p^\times \\ u = a_0 + a_1 p + a_2 p^2 + \cdots, a_0 \neq 0. \end{cases}$$

Soit

$$b = p^{v_p(b)}(x_0 + x_1 p + x_2 p^2 + \cdots) \in \mathbb{Q}_p^*, x_0 \neq 0.$$

Alors

$$b^2 = a \Longleftrightarrow p^{2v_p(b)} \cdot (x_0 + x_1 p + x_2 p^2 + ...)^2 = p^{v_p(a)} \cdot u.$$

On obtient

$$\begin{cases} v_p(a) = 2v_p(b) \\ (x_0 + x_1 p + x_2 p^2 + ...)^2 = u = a_0 + a_1 p + a_2 p^2 \cdot \cdot \end{cases}$$

Ce qui nous donne

$$x_0^2 \equiv a_0 \mod p \Longleftrightarrow x_0^2 - a_0 \equiv \mod p.$$

On distingue deux cas :
1) Si $p \neq 2$, alors soit le polynôme

$$F(x) = x^2 - u.$$

Alors

$$F(x_0) = x_0^2 - u \equiv 0 \mod p.$$

D'autre part, or $F'(x) = 2x$, alors

$$F'(x_0) \not\equiv 0 \mod p.$$

Alors nous appliquons le lemme de Hensel pour $F(x) = x^2 - u$ avec une approximation initiale $\bar{a}_0 = x_0$. Donc il existe b tel que $b^2 - u = 0$ (u est un carré) et $b \equiv \bar{a}_0 \mod p$.
2) Si $p = 2$, alors

$$\begin{cases} x_0^2 - a_0 \equiv 0 \mod 2 \\ 0 < x_0 < 2. \end{cases}$$

On obtient

$$x_0 = a_0 = 1.$$

On a

$$b^2 = a \Longleftrightarrow 2^{2v_2(b)}(1 + x_1 2 + x_2 2^2 + \cdots)^2 = 2^{v_2(a)}(1 + a_1 2 + a_2 2^2 + \cdots) = 2^{v_2(a)} \cdot u.$$

D'autre part, on peut écrire

$$(1 + x_1 2 + x_2 2^2 + \cdots)^2 = 1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + \cdots.$$

Donc

$$2^{2v_2(b)}(1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + \cdots) = 2^{v_p(a)}(1 + a_1 2 + a_2 2^2 + \cdots).$$

Ce qui donne

$$\begin{cases} v_2(a) = 2v_2(b) \\ x_0 = 1 \\ a_0 = 1, a_1 = a_2 = 0. \end{cases}$$

De plus, on a

$$\begin{cases} u = a_0 + a_1 2 + a_2 2^2 + \cdots \\ a_0 = 1, a_1 = a_2 = 0 \end{cases}$$

$$\Rightarrow u = 1 + a_3 2^3 + a_4 2^4 + \cdots = 1 + 2^3.(a_3 + a_4 2 + \cdots).$$

On obtient

$$u \equiv 1 \mod 8.$$

□

Exemple 2.7.3.

1) *Ils existent des nombres dans $\mathbb{Q}_3$ qui n'admettent pas des racines carrées par exemple*

$$a = 5 = 2 + 1 \cdot 3.$$

En effet, soit

$$x = \alpha_0 + \alpha_1.3 + \cdots + \alpha_n.3^n + \cdots \in \mathbb{Q}_3, \alpha_n \in \{0, 1, 2\}.$$

Alors

$$x^2 = a \Longrightarrow (\alpha_0 + \alpha_1.3 + \cdots + \alpha_n.3^n + \cdots)^2 = 2 + 1 \cdot 3$$

Donc

$$\alpha_0^2 = 2 \mod 3.$$

Dans ce cas α_0 n'éxiste pas. Alors x est aussi n'existe pas.

2) *Le nombre 2-adique $y = -1$ n'a pas de racine carrée dans $\mathbb{Q}_2$ car*

$$-1 \not\equiv 1 \mod 8.$$

Le corollaire suivant est une conséquence immédiate de la proposition (2.7.1) :

Corollaire 2.7.1.

1) Supposons que $p \neq 2$ et u un entier p-adique unitaire $u \in \mathbb{Z}_p^\times$. S'il existe un $\alpha \in \mathbb{Z}_p$ tel que $\alpha^2 \equiv u \mod p$, alors u est un carré dans $\mathbb{Z}_p$.

2) Supposons que $p = 2$, alors un entier 2-adique unitaire $u \in \mathbb{Z}_2^\times$ est un carré dans $\mathbb{Z}_2^\times$ si et seulement si $u \equiv 1 \mod 8$.

CHAPITRE 3

MÉTHODE DE HOUSEHOLDER POUR RÉSOUDRE LES ÉQUATIONS POLYNOMIALES P-ADIQUES

Trouver une solution approchée d'une équation non linéaire donnée $f(x) = 0$ est l'un des sujets importants de l'analyse numérique. De nombreux modèles mathématiques de la physique, de l'économie, de l'ingénierie, des sciences et de toute autre discipline proposent des équations non linéaires de ce type. Ces derniers temps, plusieurs scientifiques et ingénieurs se sont concentrés sur la résolution des équations non linéaires à la fois numériquement et analytiquement. Dans la littérature, il existe plusieurs méthodes itératifs disponibles utilisant différentes techniques telles l'interpolation, la série de Taylor, les formules de quadrature, etc. avec des modifications et des améliorations, et différentes méthodes itératives hybrides (pour plus de détails voir [1, 6, 12].

Ce chapitre est une application intéressante des outils de l'analyse numérique à la théorie des nombres. On verra comment utiliser la méthode numérique de Householder pour calculer le zéro d'une fonction p-adique sur $\mathbb{Q}_p$. On note que le but est de calculer les premiers chiffres du développement p-adique des racines carrées d'un nombre p-adique $a \in \mathbb{Q}_p$ à l'aide de suites de nombres p-adiques construite par la méthode de Householder.

3.1 Construction de la méthode de Householder

L'itération de Householder ou méthode de Householder désigne un algorithme de recherche d'un zéro d'une fonction utilisé pour les fonctions d'une variable réelle deux fois dérivables et à dérivée seconde continue. Il doit son nom à son inventeur, le mathématicien Alston Scott Householder. Un mathématicien spécialiste de biomathématique et d'analyse numérique né le 5 mai 1904, à Rockford dans l'Illinois et mort le 4 juillet 1993. Les méthodes Householder sont des méthodes de type Newton avec un ordre de convergence plus élevé.

Étant donné une fonction $F : X \longrightarrow X$ et un point $x_0 \in X$, on peut itérer F pour générer la suite de points

$$x_0, x_1 = F(x_0), x_2 = F(x_1), \cdots$$

La suite ainsi obtenue,

$$\forall n \in \mathbb{N} : x_{n+1} = F(x_n). \tag{3.1}$$

Cette relation peut également s'écrire

$$\forall n \in \mathbb{N} : x_n = F^n(x_0).$$

Telles que

$$\forall n \in \mathbb{N} : \begin{cases} F^n = \underbrace{F \circ F \circ \cdots \circ F}_{n \text{ fois}}, \\ F^0 = Id_X. \end{cases}$$

Un point α est appelé un point fixe de F si $F(\alpha) = \alpha$ et F est une fonction auxiliaire "bien" choisie. Graphiquement, lorsque X est un sous-ensemble des nombres réels, les points fixes de F s'obtiennent en traçant la droite d'équation $y = x$, tous les points d'intersection de la courbe représentative de F avec cette droite sont alors les points fixes de F, (Lorsque X est un sous-ensemble des nombres réels, le graphe de F coupe la ligne $y = x$ à chaque point fixe).

Considérons maintenant le problème de trouver une racine α de l'équation

$$f(x) = 0. \tag{3.2}$$

Une façon d'approximer α est de trouver une autre fonction F, appelée fonction d'itération pour f (notée $F.I$) et pour laquelle α est un point fixe. Ensuite, pour une valeur initiale convenablement choisie x_0, l'itération (3.1) converge vers α. Notons que le choix de F n'est pas unique. L'une des méthodes numériques les plus connues pour résoudre ce problème est la méthode de Newton. La suite d'itérés de la méthode de Newton est donnée par

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{3.3}$$

EIle est connue aussi sous le nom de Newton – Raphson. Cette méthode est une méthode particulière de point fixe (3.1) avec

$$F(x) = x - \frac{f(x)}{f'(x)}. \tag{3.4}$$

Évidemment, α est un point fixe de F si α est une racine de (3.2).

La méthode de Newton est étroitement liée à la série de Taylor. Étant donné une fonction f, la série de Taylor de la fonction f autour d'un point x_0 est donnée par

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + f''(x_0)\frac{(x - x_0)^2}{2} + \cdots \tag{3.5}$$

Pour trouver x, nous limitons cette série de Taylor après le terme d'ordre 1 et nous exprimons

que le souhait est de trouver une valeur de x telle que $f(x) = 0$. Autrement dit dans la méthode de Newton, on ne conserve que les deux premiers termes de la série pour donner

$$f(x) = f(x_0) + f'(x_0)(x - x_0).$$

Ce qui donne

$$x = x_0 + \frac{f(x) - f(x_0)}{f'(x_0)}.$$

Mais comme on a tronqué la série de Taylor, ceci ne constitue qu'une approximation de la solution cherchée. Ainsi la valeur trouvée qui est proche de la valeur pour laquelle $f(x) = 0$ et donnée par

$$x = x_0 - \frac{f(x_0)}{f'(x_0)}. \tag{3.6}$$

La technique peut être répétée pour améliorer encore la valeur de la solution et l'algorithme d'itération est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}. \tag{3.7}$$

L'algorithme est répété jusqu'à ce que le degré de précision souhaité soit atteint.

Maintenant, on considère le développement de Taylor de second ordre de f au point x_0, c'est-à-dire

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + \frac{(x - x_0)^2}{2}f''(x_0) = 0.$$

Par suite

$$x = x_0 - \frac{f(x_0)}{f'(x_0)} - \frac{f''(x_0)(x - x_0)^2}{2f'(x_0)}. \tag{3.8}$$

La substitution à nouveau de (3.6) dans le côté droit de (3.8) donne la deuxième approximation

$$x = x_0 - \frac{f(x_0)}{f'(x_0)} - \frac{f''(x_0)\left(f(x_0)\right)^2}{2\left(f'(x_0)\right)^3}.$$

Cette formule nous permet de proposer la méthode itérative suivante pour résoudre l'équation non linéaire (3.2). Pour une valeur initiale convenablement choisie x_0, la solution approchée x_{n+1} est générée par le schéma itératif suivant

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} - \frac{\left(f(x_n)\right)^2 f''(x_n)}{2\left(f'(x_n)\right)^3}, n = 0, 1, 2, \cdots \tag{3.9}$$

Cette itération est appelée la méthode itérative de Householder pour résoudre les équations non linéaires.

3.2 Etude de la méthode

Notre travail consiste à utiliser la méthode de Householder pour résoudre un problème de recherche de racine de $f(x) = 0$ dans le cadre p-adique. On verra comment utiliser cette méthode pour calculer les premiers chiffres (les développements finis p-adiques) du développement p-adique des racines carrées d'un nombre p-adique $a \in \mathbb{Q}_p$ à l'aide de suites de nombres p-adiques construite par la méthode de Householder. Pour cela, on se propose d'étudier le problème suivant

$$\begin{cases} f(x) = x^2 - a = 0 \\ \\ a \in \mathbb{Q}_p^* \ , p\text{-premier.} \end{cases} \tag{3.10}$$

La solution de (3.10) est approchée par une suite des nombres p-adiques $(x_n)_n \in \mathbb{Q}_p$ construite par la méthode de Householder.

Principe générale de calcul : Le principe de calcul pour la fonction définie par

$$f(x) = x^2 - a = 0. \tag{3.11}$$

Supposons que $a \in \mathbb{Q}_p^*$ admet une racine carrée, alors la valuation p-adique de a est paire notée $2m, m \in \mathbb{Z}$ et

$$|a|_p = p^{-v_p(a)} = p^{-2m}.$$

D'après la proposition (2.6.1), si $(x_n)_n$ est une suite des nombres p-adiques qui converge vers un nombre p-adique $r \neq 0$ alors à partir d'un certain rang la suite des valeurs absolues p-adiques est stationnaire, on a donc

$$|x_n|_p = |r|_p \,. \tag{3.12}$$

Nous savons aussi que s'il existe un nombre p-adique r tel que

$$r^2 = a,$$

alors

$$|r|_p^2 = |a|_p = p^{-2m}.$$

Par conséquent

$$|r|_p = p^{-m}. \tag{3.13}$$

Alors la suite $(x_n)_n$ devrait tendre vers r , ainsi à partir d'un certain rang, on a

$$|x_n|_p = |r|_p = p^{-m}. \tag{3.14}$$

3.3 Analyse de convergence

L'efficacité d'une méthode est fondamentale pour résoudre effectivement des problèmes. Pour cela il faut étudier la performance de la méthode à travers :

• Déterminer la vitesse de convergence de la suite $(x_n)_n$. La vitesse de convergence est un facteur important de la qualité des algorithmes ; si la vitesse de convergence est élevée, l'algorithme converge rapidement et le temps de calcul est moindre. Pour mesurer la vitesse de convergence d'une méthode itérative, on étudie l'évolution de la suite $(e_{n+n_0})_n$ des écarts

$$e_{n+n_0} = x_{n+n_0+1} - x_{n+n_0},$$

entre les itérés de la suite $(x_n)_n$ obtenus à chaque étapes de l'itération avec n_0 représente un rang quelconque. Par exemple convergence linéaire, quadratique, cubique...

• Déterminer combien d'itérations nécessaires pour que $(x_n)_n$ soit proche de la solution de l'équation avec une précision donnée M qui représente le nombre de chiffres p-adiques dans le développement de $\sqrt{a}$. Donc, il est question de trouver n tel que

$$\left|e_{n+n_0} = x_{n+n_0+1} - x_{n+n_0}\right|_p \leq p^{-M}.$$

Définition 3.3.1. *Soit $a \in \mathbb{Q}_p^*$. On dit que $b \in \mathbb{Q}_p$ est une racine carrée de a d'ordre r si et seulement si $a^2 \equiv b \mod p^r$.*

Remarque 3.3.1.
(1) Si $a^2 \equiv b \mod p^r$, alors

$$a^2 - b \equiv 0 \mod p^r \Longrightarrow p^r \text{ divise } (a^2 - b)$$

$$\Longrightarrow v_p(a^2 - b) \geq v_p(p^r) = r$$

$$\Longrightarrow -v_p(a^2 - b) \leq -r$$

$$\Longrightarrow p^{-v_p(a^2-b)} \leq p^{-r}$$

$$\Longrightarrow \left|a^2 - b\right|_p \leq p^{-r}.$$

(2) De même si $\left|a^2 - b\right|_p \leq p^{-r}$, alors $a^2 - b \equiv 0 \mod p^r$.

On a la suite d'itérés de la méthode de Householder est

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} - \frac{\left(f(x_n)\right)^2 f''(x_n)}{2\left(f'(x_n)\right)^3}. \tag{3.15}$$

Donc l'itération de la méthode Householder associée à la fonction f donnée en (3.10) s'écrit sous la forme

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{1}{2x_n}\left(x_n^2 - a\right) - \frac{1}{8x_n^3}\left(x_n^2 - a\right)^2. \tag{3.16}$$

L'efficacité de la méthode de Householder est donnée par le théorème suivant :

Théorème 3.3.2. *Si x_{n_0} est la racine carrée de a d'ordre r, alors*
1) Si $p \neq 2$, alors x_{n+n_0} est la racine carrée de a d'ordre w_n, i.e,

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \mod p^{w_n}. \tag{3.17}$$

où la suite $(w_n)_n$ est définie par

$$\forall n \in \mathbb{N} : w_n = 3^n r + 2m(1 - 3^n).$$

De plus la suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{s_n}. \tag{3.18}$$

Telle que

$$\forall n \in \mathbb{N} : s_n = 3^n r + m(1 - 2 \cdot 3^n). \tag{3.19}$$

2) Si $p = 2$, alors x_{n+n_0} est la racine carrée de a d'ordre w'_n, i.e,

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \mod 2^{w'_n}. \tag{3.20}$$

où la suite $(w'_n)_n$ est définie par

$$\forall n \in \mathbb{N} : w'_n = 3^n r + (2m + 3)(1 - 3^n).$$

et la suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{s'_n}. \tag{3.21}$$

Telle que

$$\forall n \in \mathbb{N} : s'_n = 3^n r + m(1 - 2 \cdot 3^n) - 3^{n+1}. \tag{3.22}$$

Preuve.
Etape 1 : Soit $(x_n)_n$ la suite définie par (3.16). Nous avons

$$\forall n \in \mathbb{N} : x_{n+1}^2 - a = \frac{1}{64} \frac{1}{x_n^6} \left(a - x_n^2\right)^3 \left(a - 9x_n^2\right). \tag{3.23}$$

Supposons que x_{n_0} soit la racine carrée de a d'ordre r , tels que n_0 représente un rang quelconque et $r \in \mathbb{N}$, i.e,

$$x_{n_0}^2 - a \equiv 0 \mod p^r. \tag{3.24}$$

Alors

$$v_p\left(x_{n_0}^2 - a\right) \geq r.$$

On obtient donc

$$\left|x_{n_0}^2 - a\right|_p \leq p^{-r}.$$

D'autre part, on pose pour tout $n \in \mathbb{N}$,

$$g(x_n) = \frac{1}{64}\frac{1}{x_n^6}\left(a - 9x_n^2\right). \tag{3.25}$$

Par suite

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

En utilisant le fait que

$$|64|_p = \begin{cases} 1, \text{ if } p \neq 2, \\ \\ \frac{1}{64} = \frac{1}{2^6}, \text{ if } p = 2. \end{cases} \tag{3.26}$$

On a

$$\left|g(x_{n_0})\right|_p = \left|\frac{1}{64}\frac{1}{x_{n_0}^6}\left(a - 9x_{n_0}^2\right)\right|_p = \left|\frac{1}{64}\right|_p \cdot \left|\frac{1}{x_{n_0}^6}\right|_p \cdot \left|a - 9x_{n_0}^2\right|_p.$$

Cela donne

$$\left|g(x_{n_0})\right|_p \leq \left|\frac{1}{64}\right|_p \cdot \left|\frac{1}{x_{n_0}^6}\right|_p \cdot \max\left\{|a|_p, \left|9x_{n_0}^2\right|_p\right\}$$

$$\leq \begin{cases} p^{6m} \cdot p^{-2m}, \text{ si } p \neq 2 \\ \\ 2^6 \cdot 2^{6m} \cdot 2^{-2m}, \text{ si } p = 2 \end{cases}$$

$$\leq \begin{cases} p^{4m}, \text{ si } p \neq 2 \\ \\ 2^{4m+6}, \text{ si } p = 2. \end{cases}$$

Il s'ensuit que, pour tout $n \in \mathbb{N}$,

$$\left|g(x_{n+n_0})\right|_p \leq \begin{cases} p^{4m}, \text{ si } p \neq 2 \\ \\ 2^{4m+6}, \text{ si } p = 2. \end{cases}$$

Alors

$$\left|x_{n_0+1}^2 - a\right|_p = \left|g(x_{n_0})\right|_p \cdot \left|a - x_{n_0}^2\right|_p^3.$$

Par conséquent,

$$\begin{cases} \left|x_{n_0+1}^2 - a\right|_p \leq p^{4m} \cdot p^{-3r} = p^{-(3r-4m)}, \text{ si } p \neq 2 \\ \\ \left|x_{n_0+1}^2 - a\right|_2 \leq 2^{4m+6} \cdot 2^{-3r} = 2^{4m+6} \cdot 2^{-[3r-(4m+6)]}, \text{ si } p = 2. \end{cases}$$

On obtient

$$\begin{cases} x_{n_0+1}^2 - a \equiv 0 \mod p^{3r-4m}, \text{ si } p \neq 2 \\ \\ x_{n_0+1}^2 - a \equiv 0 \mod 2^{3r-(4m+6)}, \text{ si } p = 2. \end{cases}$$

De cette manière, on obtient
Si $p \neq 2$, alors

$$x_{n_0}^2 - a \equiv 0 \mod p^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \mod p^{3r-4m} \\ x_{n_0+2}^2 - a \equiv 0 \mod p^{9r-16m} \\ x_{n_0+3}^2 - a \equiv 0 \mod p^{27r-52m} \\ \quad . \\ \quad . \\ \quad . \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \mod p^{w_n}, \tag{3.27}$$

Où la suite $(w_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \begin{cases} w_{n+1} = 3w_n - 4m, \\ \\ w_0 = r. \end{cases} \tag{3.28}$$

Il est clair que la suite $(w_n)_n$ est une suite récurrente linéaire d'ordre 1, dont le terme général est donné par

$$\forall n \in \mathbb{N} : w_n = a^n.w_0 + b(\frac{1-a^n}{1-a}).$$

Telles que

$$a = 3, b = -4m.$$

Par suite

$$\forall n \in \mathbb{N} : w_n = 3^n r + 2m(1-3^n). \tag{3.29}$$

De plus

$$v_p(x_{n+n_0}^2 - a) \geq w_n. \tag{3.30}$$

Si $p = 2$**,** alors

$$x_{n_0}^2 - a \equiv 0 \mod 2^r \Longrightarrow \begin{cases} x_{n_0+1}^2 - a \equiv 0 \mod 2^{3r-(4m+6)} \\ x_{n_0+2}^2 - a \equiv 0 \mod 2^{9r-8(2m+3)} \\ x_{n_0+3}^2 - a \equiv 0 \mod 2^{27r-26(2m+3)} \\ \quad . \\ \quad . \\ \quad . \end{cases} \tag{3.31}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0}^2 - a \equiv 0 \mod 2^{w'_n}. \tag{3.32}$$

Où la suite $(w'_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \begin{cases} w'_{n+1} = 3w'_n - (4m+6) \\ \\ w'_0 = r. \end{cases} \tag{3.33}$$

Ce qui donne

$$\forall n \in \mathbb{N} : w'_n = 3^n r + (2m+3)(1-3^n). \tag{3.34}$$

Par suite

$$\forall n \in \mathbb{N} : w'_n = w_n + 3(1-3^n). \tag{3.35}$$

De plus

$$v_2(x_{n+n_0-1}^2 - a) \geq w'_n. \tag{3.36}$$

Etape 2 : On a

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = -\frac{1}{8}\frac{1}{x_n^3}\left(a - x_n^2\right)\left(a - 5x_n^2\right). \tag{3.37}$$

Cela donne

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} = -\frac{1}{8}\frac{1}{x_{n+n_0}^3}\left(a - x_{n+n_0}^2\right)\left(a - 5x_{n+n_0}^2\right). \tag{3.38}$$

Posons pour tout $n \in \mathbb{N}$,

$$h(x_n) = -\frac{1}{8}\frac{1}{x_n^3}\left(a - 5x_n^2\right).$$

Par ailleurs

$$|8|_p = \begin{cases} 1, \text{ si } p \neq 2 \\ \\ \frac{1}{8} = \frac{1}{2^3}, \text{ si } p = 2. \end{cases} \tag{3.39}$$

Ce qui donne

$$\left|h(x_{n+n_0})\right|_p = \left|-\frac{1}{8}\frac{1}{x_{n+n_0}^3}\left(a - 5x_{n+n_0}^2\right)\right|_p = \left|\frac{1}{8}\right|_p \cdot \left|\frac{1}{x_{n+n_0}^3}\right|_p \cdot \left|a - 5x_{n+n_0}^2\right|_p$$

$$\leq \left|\frac{1}{8}\right|_p \cdot \left|\frac{1}{x_{n+n_0}^3}\right|_p \cdot \max\left\{|a|_p, \left|5x_{n+n_0}^2\right|_p\right\}$$

$$\leq \begin{cases} p^{3m} \cdot p^{-2m}, \text{ si } p \neq 2 \\ \\ 2^3 \cdot 2^{3m} \cdot 2^{-2m}, \text{ si } p = 2. \end{cases}$$

Il s'ensuit que, pour tout $n \in \mathbb{N}$,

$$\left|h(x_{n+n_0})\right|_p \leq \begin{cases} p^m, \text{ si } p \neq 2, \\ \\ 2^{m+3}, \text{ si } p = 2. \end{cases}$$

On obtient ce qui suit

$$\left|x_{n+n_0+1} - x_{n+n_0}\right|_p = \left|h(x_{n+n_0})\left(a - x_{n+n_0}^2\right)\right|_p = \left|h(x_{n+n_0})\right|_p \cdot \left|a - x_{n+n_0}^2\right|_p$$

$$\leq \begin{cases} p^m \cdot p^{-w_n}, \text{ si } p \neq 2 \\ \\ 2^{m+3} \cdot 2^{-w'_n}, \text{ si } p = 2. \end{cases}$$

Par conséquent

$$\begin{cases} x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{w_n - m}, \text{ si } p \neq 2, \\ \\ x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{w'_n - (m+3)}, \text{ si } p = 2. \end{cases}$$

Il s'ensuit que, si $p \neq 2$, alors

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{s_n}. \tag{3.40}$$

Telle que

$$\forall n \in \mathbb{N} : s_n = w_n - m = 3^n r + m(1 - 2 \cdot 3^n). \tag{3.41}$$

De plus

$$v_p(x_{n+n_0+1} - x_{n+n_0}) \geq s_n. \tag{3.42}$$

Si $p = 2$, alors

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 2^{s'_n}. \tag{3.43}$$

Telle que

$$\forall n \in \mathbb{N} : s'_n = w'_n - (m+3) = 3^n r + m\left(1 - 2 \cdot 3^n\right) - 3^{n+1} = s_n - 3^{n+1}. \tag{3.44}$$

Par suite

$$\forall n \in \mathbb{N} : s'_n = s_n - 3^{n+1}. \tag{3.45}$$

De plus

$$v_2(x_{n+n_0+1} - x_{n+n_0}) \geq s'_n. \tag{3.46}$$

Ceci achève la preuve. □

CONCLUSION GÉNÉRALE

Nous pouvons résumer nos résultats principaux de la manière suivante.

Conclusion 3.3.1.
(1) ***Si*** $p \neq 2$*, alors*
a) La vitesse de convergence de la suite $(x_n)_n$ *obtenue par la méthode de Householder est de l'ordre* s_n*.*
b) Pour déterminer le nombre d'itérations nécessaires n pour M chiffres donnés (ou pour avoir une précision de p^{-M}*, ce qui correspond, à peu près, à M chiffres exacts), on pose*

$$v_p(x_{n+n_0+1} - x_{n+n_0}) = s_n = 3^n r + m(1 - 2 \cdot 3^n) \geq M.$$

On obtient

$$n = \left[\frac{\ln(\frac{M-m}{r-2m})}{\ln 3} \right], \tag{3.47}$$

avec $r - 2m > 0$ *où* $[\cdot]$ *désigne la partie entière.*
(2) ***Si*** $p = 2$*, alors*
a) La vitesse de convergence de la suite $(x_n)_n$ *obtenue par la méthode de Householder est de l'ordre* s'_n*.*
b) Pour déterminer le nombre d'itérations nécessaires n pour M chiffres donnés, on pose

$$v_2(x_{n+n_0+1} - x_{n+n_0}) = s'_n = 3^n r + m\,(1 - 2 \cdot 3^n) - 3^{n+1} \geq M,$$

on obtient

$$n = \left[\frac{\ln(\frac{M-m}{r-2m-3})}{\ln 3} \right], \tag{3.48}$$

avec $r - (2m + 3) > 0$.
(3) La convergence vers zéro pour tout nombre p-adique $a \in \mathbb{Q}_p$ *telle que* $p \neq 2$ *est beaucoup plus rapide que celle de* $\mathbb{Q}_2$*.*
(4) Dans le contexte p-adique, la vitesse de convergence de la méthode de Householder est cubique (d'ordre 3), c'est à dire le nombre de chiffres significatifs exacts triple à chaque itération.

BIBLIOGRAPHIE

[1] A. Quarteroni, R. Sacco and F. Saleri. *Numerical mathematics (Texts in applied mathematics ; 37)*. Springer Science & Business Media. 2010.

[2] A. M. Robert. *A course in p-adic analysis*. Vol. 198. Springer Science & Business Media, 2013.

[3] B. Fine and G. Rosenberger. *Number Theory : An Introduction via the Density of Primes*, Birkhauser, 2016.

[4] F. Q. Gouvea. *p-adic Numbers : An Introduction*, Springer Science & Business Media, 2012.

[5] G. Bachman. *Introduction to p-adic numbers and valuation theory*, Academic Press, New York, 1964.

[6] J. F. Epperson. *An Introduction to numerical methods and analysis*, John Wiley & Sons, 2013.

[7] J. F. T Rabago. *Halley's method for approximating roots of p-adic polynomial equations*. International Journal Mathematical Analysis,(Ruse), 10 (10), 493-502, 2016.

[8] M. Kecies. *Householder's method for solving the p-adic polynomial equations*. Malaya Journal of Matematik, 10(01), 36-46, 2022.

[9] M. Kecies. *The performance of the secant method in the field of p-dic numbers*, Malaya Journal of Matematik, 9(2), 28-38, 2021.

[10] M. P. Knapp and C. Xenophontos. *Numerical Analysis meets Number Theory : Using root finding methods to calculate inverses mod p^n*. Applicable Analysis and Discrete Mathematics, 4, 23-31, 2010.

[11] P. S. P. Ignacio, J. M. Addawe, W. V. Alangui and J. A Nable. *Computation of square and cube roots of p-adic numbers via Newton-Raphson method.* Journal of Mathematics Research, 5, 31-38, 2013.

[12] R. Picasso, J. Rappaz and M. Picasso. *Introduction à l'analyse numérique*. Ppur Presses Romandes, 2010.

[13] S. Albeverio, A.Y. Khrennikov and V. M. Shelkovich. *Theory of p-adic distributions : linear and nonlinear models*. Cambridge University Press, 2010.

[14] S. Katok. *p-adic analysis compared with real, Vol. 37*, American Mathematical Soc, 2007.

[15] T. Zerzaihi and M. Kecies. *General approach of the root of a p-adic number*. Filomat. 27, 431-436, 2013.

[16] T. Zerzaihi, M. Kecies and M.P. Knapp. *Hensel codes of square roots of p-adic numbers*. Applicable Analysis and Discrete Mathematics, 4, 32-44, 2010.

[17] W.A . Coppel. *Number Theory : An introduction to mathematics*. Springer Science & Business Media, 2009.

[18] W. H. Schikhof. *Ultrametric calculus, an introduction to p-adic analysis*. Combridge university press, 1984.

Résumé

Dans ce travail nous nous intéressons au calcul des racines carrées des nombres p-adiques, en utilisant la méthode de Householder et ceci à travers le calcul de la solution approchée de $f(x) = x^2 - a = 0$ *où* $a \in Q_p$. *Nous déterminons également la vitesse de convergence et le nombre d'itérations nécessaires pour une précision donné.*

Mots clés *:* valuation p-adique, norme p-adique, nombre p-adique, racine carrée, Méthode itérative de Housholder, lemme de Hensel. vitesse de convergence.

Abstract

In this work we are concerned with the calculation of the square roots of p-adic numbers, using the Householder method and this through the calculation of the approached solution of $f(x) = x^2 - a = 0$ *in* Q_p. *We also determine the speed of convergence and the number of iterations required for a given precision .*

Key words : p-adic valuation, p-adic norm, p-adic number, square root, Householder iterative method, Hensel's lemma, rate of convergence.

ملـخـص

في هذا العمل ،نحن مهتمون بحساب الجذور التربيعية لأعداد البيأديك باستخدام طريقة هاوسهولدارو و هدا من خلال حساب الحل التقريبي للمعادلة $f(x) = x^2 - a = 0$. نحدد أيضا سرعة التقارب و عدد التكرارات المطلوبة لدقة معينة .

الكلمات المفتاحية : تقييم بيأديك ، نظيم بيأديك ، عدد بيأديك ،جدر تربيعي ،طريقة التكرار لهاوسهولدار ، توطئة هانسال ،سرعة التقارب.