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 Technologie **Département de Mathématiques et Informatique**

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

En: Mathématiques
Spécialité : Mathématiques appliquées

Méthode de Halley pour trouver les racines d'équations polynomiales p-adiques

Préparé par: Benhemimed Leyla
Dekhmouche khouloud

Devant le jury:

Kaouache Smail	**M.C.B**	**C.U. Abd Elhafid Boussouf**	**Président**
Kecies Mohamed	**M.A.A**	**C.U. Abd Elhafid Boussouf**	**Rapporteur**
Labed Boudjema	**M.A.A**	**C.U. Abd Elhafid Boussouf**	**Examinateur**

Année Universitaire : 2019/2020

Résumé

Ce travail propose un analogue de la méthode de Halley pour résoudre un problème de recherche de racine $f(x) = 0$ dans le contexte p-adique. En particulier, une racine de l'équation polynomiale $f(x) = x^3 - a = 0$, où $a \in \mathbb{Q}_p$ et $\mathbb{Q}_p$ dénote l'ensemble des nombres p-adiques, est calculée par la méthode de Halley. Cette méthode a une convergence d'ordre 3 et converge plus rapide que la méthode de Newton.

2010 Mathematics subject classification : 26E30. 34K28. 11E95.

Mots clés : *valuation p-adique, norme p-adique, nombre p-adique, racine cubique, développement p-adique, Méthode de Newton, Méthode de Halley, vitesse de convergence.*

Abstract

This work proposes an analogue of Halley's method for solving a root-finding problem $f(x) = 0$ in the p-adic setting. In particular, a root of the polynomial equation $f(x) = x^3 - a = 0$, where $a \in \mathbb{Q}_p$ and $\mathbb{Q}_p$ denotes the set of p-adic numbers, is computed through Halley's method. This method has convergence of order 3 and converges faster than Newton's method.

2010 Mathematics subject classification : 26E30. 34K28. 11E95

Key words : *p-adic valuation, p-adic norm, p-adic number, cubic root, p-adic development, Newton's method, Halley's Method, speed of convergence.*

Life is good only for two things, discovering mathematics and teaching mathematics.

Siméon Denis Poisson

Remerciements

Au non du Dieu le miséricordieux par essence et par excellence
Nous adressons notre profond remerciement tout d' abord notre encadreur Mr.Mohammed Kecies *Pour sa patience,et surtout pour sa confiance, ses remarques et ses conseile,sa disponibilitè et sa bienveillance.*

Nous exprimons notre profonde reconnaissance à Monsieur Kaouache Smail*, Maître de conférence à l'université de Mila, pour avoir accepté de présider le jury de mémoire et pour son aide précieuse.*

Nous adressons, également, nos remerciements chaleureux à Monsieur Labed Boudjema*, Maître assistant à l'université de Mila, qui a bien voulu prendre la responsabilité d'évaluer ce travail, qu'il soit vivement remercié.*
Nous voudrions également remercier tout le personnel de linstitut de sciences et de la technologie

Enfin ,nous remercions toutes personnes qu'ont contribué de prés ou de lois à l'achèvement de ce travail.

MERCI POUR TOUT

Dédicace

ma chère mère,

“Tu m’as donnée la vie,la tendresse et courage pour réussir.
Tout ce que je preux t’ offris ne pourra exprimer l amour etla reconnaissance que je te porte.
En témoignage,je t’offre ce modeste travail pour te remercier pour tes sacrifices et pour l’affection dont tu m’ as toujours entourée.”

À mon cher père,que dieu ait pitié de lui

À mon cher mari

À mes frères :

Fouhed,Lazhar,Badis,Ridha et Idriss

À mes soeurs :

Fatima Zahra,warda que dieu ait pitié de lui,Hanane et Rania

À ma famille

À mon encadreur :

Mr.Mohammed Kecies

À mes amis(es) :

Dekhmouche khouloud,Zinab ,khadijda .....la liste est tréslong.

Et à tous les gens qui m’ ont aidédans ma vie

Je dédie ce mémoire

LEYLA

Dédicace

mes très chers parents

ma mère et mon père
Pour leur patience, leur amour, leur soutien, leur fatigue et leurs encouragements

A mes frères :

Mahrez et mon petit frère marée Nafaâ

A mes soeurs :

Racha, Hadjer et ma petite soeur Asma

A mes amis(es) :

Tout d'abord,je remercie ma collégue Leyla ,avec qui elle a partagé ce travail
Afaf, Souad, Ama, Kawther, Aida, Somia et toutes les copines de l'école

Et à mon Encadreur :

Mohamed Kecies

Je dédie ce mémoire

KHOULOUD

Table des matières

Table des figures

Abréviations et notations

Les notations suivantes seront utilisées dans toute la thèse :

$\min, \max$	Minimum,Maximum respectivement.
p	Un nombre premier.
v_p	Valuation p-adique.
$\|.\|_p$	Norme p-adique.
d_p	Distance p-adique.
.	Point p-adique.
$\mathbb{Q}$	Ensemble des nombres rationnels.
$\mathbb{R}$	Ensemble des nombres réels.
$\mathbb{Q}_p$	Ensemble des nombres p-adiques.
$\mathbb{Z}_p$	Ensemble des entiers p-adiques.
$\mathbb{Z}_p^\times$	Ensemble des nombres p-adiques unitaires.
$[.]$	Partie entière.
$\langle . \rangle$	Partie fractionnelle.

Introduction Générale

Le problème de recherche de racine est l'un des problèmes de calcul les plus importants. Elle se pose dans une grande variété d'applications pratiques en physique, chimie, biosciences, ingénierie, etc. En effet, la détermination de tout inconnu apparaissant implicitement dans les formules scientifiques ou d'ingénierie pose un problème de recherche de racines. Plus précisément, Le problème de recherche de racine est énoncé comme suit : étant donné une fonction f. Trouver un nombre $x = \alpha$ tel que $f(\alpha) = 0$.

À l'exception de certaines fonctions très spéciales, il n'est pas possible de trouver une expression analytique pour la racine, à partir de laquelle la solution peut être déterminée exactement. Autrement dit, en général les solutions explicites sont difficiles, voir impossible, à obtenir analytiquement. Ainsi, la plupart des méthodes de calcul du problème de recherche de racines doivent être de nature itérative. Lorsque des solutions analytiques ne sont pas possibles pour ces équations, les méthodes d'approximation numérique sont utiles pour obtenir des solutions approximatives. On remplace alors la résolution mathématique exacte du problème par sa résolution numérique qui est, en général, approchée. L'idée fondamentale d'une méthode est de construire une suite de vecteurs $(x_n)_n$ qui converge vers le vecteur α, solution du problème $f(x) = 0$. Ces méthodes sont devenues aujourd'hui un outil essentiel pour l'investigation dans les différents problèmes fondamentaux de notre assimilation des phénomènes scientifiques qui sont difficiles, à savoir impossible à résoudre dans le passé. Ainsi, notons qu'il existe actuellement de nombreuses méthodes numériques utilisées pour résoudre numériquement les équations non linéaires $f(x) = 0$ (méthode de Newton, sécante, point fixe...).

L'intérêt des méthodes itératives, comparées aux méthodes directes, est d'être simples à programmer et de nécessiter moins de place en mémoire. En revanche le temps de calcul est souvent plus long.

Dans ce travail, Nous allons présenter une dérivation simple de la méthode de Newton, nommée méthode de Halley. Cette méthode a été découverte par Edmond Halley (un mathématicien anglais 1656-1742), elle s'applique à une fonction de C^2 (i.e, f' et f'' sont continues) pour trouver une approximation numérique des racines à l'équation $f(x) = 0$. Pour une discussion approfondie de la propriété de convergence de la méthode de Halley, nous renvoyons les lecteurs à [9] et pour une discussion plus approfondie de la méthode, on peut consulter [11] et [22].

Ce travail propose un analogue de la méthode de Halley pour résoudre un problème de recherche de racine $f(x) = 0$ dans le cadre p-adique. En particulier, une racine de l'équation polynomiale $f(x) = x^3 - a$, où $a \in \mathbb{Q}_p$ dénote l'ensemble des nombres p-adiques, est calculée par la méthode de Halley. On verra comment utiliser cette méthode pour calculer les premiers chiffres (les développements finis p-adiques) du développement p-adique des racines cubiques d'un nombre p-adique $a \in \mathbb{Q}_p$ à l'aide de suites de nombres p-adiques construite par cette méthode.

Les nombres p-adiques ont été inventés dans les années 1900 par le mathématicien allemand K. Hensel. Le but initial est de répondre à des questions de théorie des nombres. Très vite, ils apparaissent comme un objet mathématique à part entière, ils donnent un cadre d'étude à la fois naturel et complètement différent des nombres réels. Pour tout p premier, le corps commutatif $\mathbb{Q}_p$ des nombres p-adiques peut être construit par complétion de $\mathbb{Q}$, d'une façon analogue à la construction des nombres réels $\mathbb{R}$ par les suites de Cauchy, mais pour une valeur absolue moins familière, nommée valeur absolue p-adique. De plus, la valeur absolue p-adique sur le corps $\mathbb{Q}_p$ est une valeur absolue non archimédienne : on obtient sur ce corps une analyse différente de l'analyse usuelle sur les réels, que l'on appelle analyse p-adique. 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 [5] ; [6], [7], [18], et [24].

Plusieurs études ont été faites en ce qui concerne la recherche des racines carrées et des racines cubiques des nombres p-adiques. En 2010, par exemple, Knapp et Xenophontos [14] ont montré comment les méthodes classiques de recherche de racines issues de l'analyse numérique peuvent

être utilisées pour calculer l'inverse d'un entier modulo p^n. La même année, Zerzaihi, Kecies et Knapp [21] ont appliqué des méthodes classiques de recherche de racines, comme la méthode des points fixes, pour trouver des racines carrées de nombres p-adiques à travers le lemme de Hensel. En 2011, Zerzaihi et Kecies [19] ont utilisé la méthode sécante pour trouver les racines cubiques des nombres p-adiques. Ces auteurs [20] ont ensuite appliqué la méthode de Newton pour trouver les racines cubiques des nombres p-adiques dans $\mathbb{Q}_p$. Un problème similaire est également apparu dans [15] où Ignacio et al. calculé les racines carrées des nombres p-adiques via la méthode de Newton Raphson. En 2016, l'auteur [12] a décrit un analogue de la méthode de Halley pour approximer les racines des équations polynomiales p-adiques générale $f(x) = 0$ dans $\mathbb{Z}_p$ où $\mathbb{Z}_p$ dénote l'ensemble des entiers p-adiques

Ce mémoire est composé de l'introduction 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 cubiques d'un nombre p-adique à l'aide de suite de nombres p-adiques construite par la méthode de Halley.
On termine ce mémoire par une conclusion générale.

Chapitre 1

Corps valués ultramétriques complets

Les espaces pour lesquels le critère de Cauchy est une condition nécessaire et suffisante de convergence (c'est-à-dire, dans lesquels toute suite de Cauchy est convergente) sont appelés espaces complets. En partant d'un espace métrique E non complet, on peut construire (par complétion) un espace complet $\hat{E}$ (qui sera appelé le complété de E). 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.

Dans ce chapitre, 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.

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 :*
   - *(a)* $\forall x \in K : \|x\| = 0 \Longleftrightarrow x = 0.$
   - *(b)* $\forall x, y \in K : \|x \cdot y\| = \|x\| \cdot \|y\|.$

(c) $\forall x, y \in K : \|x+y\| \leq \|x\| + \|y\|$ *(l'inégalité triangulaire).*

2. *On dit que la norme* $\|.\|$ *est ultramétrique ou non archimédienne si :*

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

c'est à dire une norme qui vérifie une condition plus forte que l'inégalité triangulaire.

3. *Une norme constante* $\|.\|$ *est dite triviale si et seulement si*

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

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* $(\mathbb{R}_+^*, .)$ *et donc que* $\|1\| = 1$.

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

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

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

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

Définition 1.1.3

1. *On appelle corps valué, tout couple de la forme* $(K, \|.\|)$ *ou* K *est un corps et* $\|.\|$ *est une norme sur* K.

2. *On appelle la distance induite sur* K *par* $\|.\|$, *la distance* $d_{\|.\|}$ *sur* K *définie par*

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

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

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

et la distance induite par cette norme appelée distance ultramétrique.

4. *Lorsque K muni de la distance ultramétrique, on dit que K est un corps valué ultramétrique. Dans le cas contraire, on dit que K est un corps valué archimédien.*

Proposition 1.1.1 *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. Voir [17]. □

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

Proposition 1.1.2 *Si K est un corps non-archimédien, alors pour $x, y \in K$*

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

Ainsi, tout triangle dans un espace ultra-métrique est isocèle et la longueur de sa base ne dépasse pas la longueur des côtés.

Preuve. En échangeant x et y si nécessaire, on peut supposer que $\|x\| > \|y\|$. Par l'inégalité triangulaire forte, on a

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

D'autre part, on a

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

Or $\|x\| > \|y\|$, alors nous devons avoir

$$\|x\| \leq \|x + y\|$$

Par conséquent,

$$\|x\| = \|x + y\|$$

□

Ainsi pour un corps non-archimédien $\|x \pm y\| \leq \max\{\|x\|, \|y\|\}$, et dans le cas où $\|x\| \neq \|y\|$, l'inégalité ci-dessus devient une égalité.

Définition 1.1.4 *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 E est dit complet si toute suite de Cauchy de E a une limite dans M. C'est-à-dire qu'elle converge dans E.*

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 définies dans $(K, \|.\|)$*.*
On définit sur $SC(K)$ *les lois suivantes :*

$$\textit{Addition} \ : \ \left\{ \begin{array}{ccc} + : SC(K) \times SC(K) & \longrightarrow & SC(K) \\ ((a_n)_n, (b_n)_n) & \longmapsto & (a_n + b_n)_n \end{array} \right.$$

$$\textit{Multiplication} \ : \ \left\{ \begin{array}{ccc} \cdot : SC(K) \times SC(K) & \longrightarrow & SC(K) \\ ((a_n)_n, (b_n)_n) & \longmapsto & (a_n \cdot b_n)_n \end{array} \right.$$

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).*

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* $\Re$ *par*

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

$\Re$ *est une relation équivalence.*

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* $\Re$ *définie précédente. 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. Voir [18]. □

4)Etape 5 : 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

1) *L'application* $\|.\|_{\hat{K}}$ *est une norme sur* $\hat{K}$ *, de plus elle est non archimédienne si* $\|.\|_K$ *est aussi.*

2) $(\hat{K}, \|.\|_{\hat{K}})$ *est un espace complet, de plus* K *est un sous ensemble dense dans* $\hat{K}$*.*

Preuve. Voir [18]. □

Chapitre 2

Corps des nombres $p-$adiques

Pour chaque p premier, on va construire de nouveaux nombres, appelés nombres p-adiques. D'une part un anneau topologique noté $\mathbb{Z}_p$ (entiers p-adiques) qui étend l'anneau $\mathbb{Z}$ des entiers, et d'autre part un corps topologique noté $\mathbb{Q}_p$ (nombres p-adiques) qui étend le corps $\mathbb{Q}$ des rationnels. Les nombres p-adiques $\mathbb{Q}_p$ forment le corps des fractions des entiers p-adiques $\mathbb{Z}_p$ (c'est- a-dire que tout élément de $\mathbb{Q}_p$ est un quotient de deux éléments de $\mathbb{Z}_p$), tout comme $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. Ainsi, les corps $\mathbb{Q}_p$ des nombres p-adiques sont construits par complétion du corps $\mathbb{Q}$ des nombres rationnels lorsque celui-ci est muni d'une norme particulière nommée norme p-adique et notée $||_p$. 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.*

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

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

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

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 $n = p_1^{m_1}.p_2^{m_2}...p_k^{m_k}$, 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

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

De même pour $v_5(2009!) = 500$. *En effet, on a* $n = 2009$, *alors*

$$n = 4 + 5 + 5^3 + 3.5^4$$

On obtient

$$v_5(2009!) = \frac{2009 - S_5(2009)}{5-1} = \frac{2009-9}{4} = 500$$

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 $|.|_p$ 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* $x = \dfrac{99}{140} = \dfrac{3^2 \cdot 11}{2^2 \cdot 5 \cdot 7} = 2^{-2} \cdot 5^{-1} \cdot 7^{-1} \cdot 3^2 \cdot 11 \in \mathbb{Q}$. *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* $|x|_p \neq |y|_p$ *alors*

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

Remarque 2.2.2 *On peut définir sur le corps des nombres rationnels* $\mathbb{Q}$ *trois types de valeurs absolues :*

1) Valeur absolue triviale

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

2) Valeur absolue ordinaire

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

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 2.2.3 *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 $|\ \ |_\infty$. 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 $|\ \ |_p$.

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 $|\ \ |_p$. Il donne aussi la relation entre les différentes normes $p-$adiques.

Théorème 2.2.1 (*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 $\mathbb{Q}_p$.

On définit $\mathbb{Q}_p$, corps des nombres $p-$adiques, comme le complété de $\mathbb{Q}$ pour la norme $p-$adique $|\ \ |_p$, c'est-à-dire que l'on prend, comme pour définir $\mathbb{R}$, l'anneau des suites de Cauchy (pour la norme $|\ \ |_p$) 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 $x_{n-1} = a_0 + a_1 5 + ... + a_{n-1}5^{n-1}$ 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*

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

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
$$\forall x, y \in \mathbb{Q}_p : |x + y|_p \leq \max\left\{|x|_p, |y|_p\right\}$$
$$\Longrightarrow |x + x|_p \leq |x|_p$$

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* $|a - \alpha|_p \leq |p|_p = p^{-1}$.

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
$$|a|_p = |p|_p^{v_p(a)} = 1 \Longleftrightarrow v_p(a) = 0$$
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
$$|a - sm|_p = \frac{|m|_p}{|n|_p}.|1 - sn|_p = |pt|_p \leq |p|_p = p^{-1}$$
Par division euclidienne, on a $sm = pk + \alpha$, avec $0 \leq \alpha \leq p - 1$ et
$$|sm - \alpha|_p = |p|_p.|k|_p \leq |p|_p = p^{-1}$$
D'où
$$|a - \alpha|_p = |a - sm + sm - \alpha|_p \leq \max\left\{|a - sm|_p, |sm - \alpha|_p\right\} \leq |p|_p = p^{-1}$$
De plus $|a|_p = |\alpha|_p = 1$. □

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

Théorème 2.3.1 *[17] 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 $a = \beta_n \beta_{n+1} ... \cdot \beta_0 \beta_1 \ldots$ 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 $n > 0$*
4. *On note par $[a]$ la partie entière (régulière) d'un nombre $p-$adique $a \in \mathbb{Q}_p$, telle que*

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

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

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

donc, on obtient la décomposition suivante

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

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

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

   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 $(2.2.2)$, $\left|\mathbb{Q}\right|_p = \{0\} \cup \{p^n : n \in \mathbb{Z}\}$, 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

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

□

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 2.3.2 *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

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

Alors le nombre

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

est un entier rationnel et x peut être exprimé comme suit

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

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 [18]. □

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 $x = \frac{1}{3} \in \mathbb{Q}$.

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

Lemme 2.3.2 *Soient $x, y \in \mathbb{Q}_p$, alors $x \equiv y \mod p^n$ si et seulement si $|x-y|_p \leq p^{-n}$.*

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

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

□

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

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

De plus, on sait que

$$\forall x \in \mathbb{Z} : v_p(x) \geq 0$$

$$\Longrightarrow |x|_p \leq 1$$

$$\Longrightarrow x \in \mathbb{Z}_p$$

□

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*

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

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

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

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

$$|u|_p = 1$$

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

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

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. □

Proposition 2.4.3 *Nous pouvons encore remarquer que tout nombre p-adique non nul peut s'écrire de manière unique comme $x = p^n.u$ avec $n \in \mathbb{Z}$ et u une unité de $\mathbb{Z}_p$.*

Preuve.

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

$$x = \frac{a}{b}, a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p^*$$

et par la proposition $(2.4.2)$, on a l'existence de m_1, m_2 et $u_1, u_2 \in \mathbb{Z}_p^{\times}$ tels que

$$\begin{cases} a = u_1.p^{m_1} \\ \\ b = u_2.p^{m_2} \end{cases}$$

Donc

$$\begin{cases} x = \frac{u_1}{u_2}.p^{m_1 - m_2} = u.p^m \\ m = m_1 - m_2 \in \mathbb{Z} \\ u = \frac{u_1}{u_2} \in \mathbb{Z}_p^{\times} \end{cases}$$

d'où l'existence.

2) **Unicité :** Pour montrer l'unicité de la représentation de x, il suffit de recopier la preuve de la proposition $(2.4.2)$. □

Remarque 2.4.4 *D'après la proposition précédente, nous pouvons étendre la définition de valuation p-adique à $\mathbb{Q}_p$ tout entier en posant pour $0 \neq x = p^m.u$,*

$$v_p(x) = v_p(p^m.u) = m \in \mathbb{Z}$$

Si $x = \frac{a}{b}$ *avec* $a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^*$, *alors* $v_p(x) = v_p(a) - v_p(b) \in \mathbb{Z}$ *et, comme nous l'avons déjà démontré, nous avons la relation*

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

pour tout $x, y \in \mathbb{Z}_p$. *Il s'ensuit que la valuation* p*-adique est un morphisme de* $(\mathbb{Q}_p^*, .)$ *dans* $(\mathbb{Z}, +)$

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*

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

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.

Lemme 2.4.1 *Tout nombre* p*-adique non nul* $x \in \mathbb{Q}_p^*$ *est inversible.*

Preuve. On a

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

On pose

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

Alors

$$u = a_0 + \sum_{k=1}^{\infty} a_k.p^k = a_0 + p.\sum_{k=1}^{\infty} a_k.p^{k-1} = a_0 + p.\sum_{k=0}^{\infty} a_{k+1}.p^k = a_0 - p.y$$

Où

$$y = -\sum_{k=0}^{\infty} a_{k+1}.p^k \in \mathbb{Z}_p$$

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

$$u = 1 - p.y$$

Donc

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

Ce qui donne

$$x^{-1} = p^{-k}.u^{-1} \in \mathbb{Q}_p$$

Alors x est inversible dans $\mathbb{Q}_p$. □

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 2.4.4 *(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

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

Nous allons présenter ici une proposition qui nous permet de déterminer les éléments de $\mathbb{Q}_p$ qui sont des cubes.

Proposition 2.4.5 *[20] (Existence des racines cubiques)*
Soit p un nombre premier, alors
(1) Supposons que $p \neq 3$, et soit $a = p^{v_p(a)}.u \in \mathbb{Q}_p^*$, $u \in \mathbb{Z}_p^\times$ un nombre p-adique unitaire. Alors a est un cube dans $\mathbb{Q}_p$, si et seulement si $v_p(a) = 3m, m \in \mathbb{Z}$ et que l'image de u dans $\mathbb{Z}_p^\times$ soit un cube, i.e, $u = v^3, v \in \mathbb{Z}_p^\times$.
(2) Supposons que $p = 3$, alors $a = 3^{v_3(a)}.u \in \mathbb{Q}_3^*$ est un cube dans $\mathbb{Q}_3$, si et seulement si $v_3(a) = 3m, m \in \mathbb{Z}$ et $u \equiv 1 \mod 9$ ou $u \equiv 2 \mod 3$.

2.5 Valeurs absolues équivalentes

Pour voir combien de topologies différentes on peut définir sur $\mathbb{Q}$, nous avons besoin de voir la notion de valeurs absolues équivalentes. Rappelons que deux distances d_1 et d_2 sur un espace métrique X définissent la même topologie si les ouverts pour la distance d_1 sont les ouverts pour la distance d_1.

Définition 2.5.1 *On dit que deux valeurs absolues sur K, $|\ |_1$ et $|\ |_2$, sont équivalentes ssi leurs distances associées respectives induisent la même topologie sur K.*

Nous donnons sans preuve les résultats suivants :

Théorème 2.5.1 *[3] Soit K un corps,$|\ \ |_1$ et $|\ \ |_2$ deux valeurs absolues sur K. Les propositions suivantes sont équivalentes :*

1) *Les valeurs absolues $|\ \ |_1$ et $|\ \ |_2$sont équivalentes.*

2) *Pour toute suite $(x_n)_n$ de K, $|x_n|_1 \underset{n\longrightarrow\infty}{\longrightarrow} 0 \Longleftrightarrow |x_n|_2 \underset{n\longrightarrow\infty}{\longrightarrow} 0$*

3) *il existe un réel positif α tel que, $\forall x \in K : |x|_1 = |x|_2^{\alpha}$*

Théorème 2.5.2 *(Ostrowski) [3] Une norme non triviale sur $\mathbb{Q}$ est équivalente à la norme usuelle $|\ \ |_\infty$ ou à la norme $p-$adique $|\ \ |_p$ pour un unique nombre premier p.*

Remarque 2.5.1

1) *Le théorème d'Ostrowski affirme que les valeurs absolues $p-$adiques sont les seules autres valeurs absolues non triviales sur $\mathbb{Q}$ que $|\ \ |_\infty$.*

2) *Par le théorème d'Ostrowski, on peut conclure qu'on ne peut que définir deux types de topologies sur $\mathbb{Q}$: celle de la valeur absolue ordinaire et celle de la valeur absolue $p-$adique.*

Corollaire 2.5.1 *Deux valeurs absolues $p-$adiques $|\ \ |_{p_1}$ et $|\ \ |_{p_2}$ sont équivalentes ssi $p_1 = p_2$.*

Preuve. La réciproque est triviale. Pour l'implication directe, il suffit de considérer la suite $(p_1^n)_{n\in\mathbb{N}}$. Elle converge vers 0 pour $|\ \ |_{p_1}$ car $|p_1^n|_{p_1} = p_1^{-n} \longrightarrow 0$ quand $n \longrightarrow \infty$ et si $p_1 \neq p_2$ elle ne converge pas vers 0 pour $|\ \ |_{p_2}$ car $|p_1^n|_{p_2} = 1 \nrightarrow 0$. □

Corollaire 2.5.2 *Soit $|\ |$ une norme non triviale sur $\mathbb{Q}$. Alors*

i) $|\ |$ est archimédienne ssi elle est équivalente à la valeur absolue ordinaire $|\ \ |_\infty$.

ii) $|\ |$ est non archimédienne ssi elle est équivalente à une certaine valeur absolue $p-$adique $|\ \ |_p$.

2.6 Fonctions $p-$adiques

Définition 2.6.1

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

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

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

Exemple 2.6.1 *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 2.6.2

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 2.6.2 *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* $f'(x) = \sum\limits_{i=1}^{n} i\alpha_i x^{i-1}$.

2.7 Propriétés topologiques et analytiques des nombres $p-$adiques

2.7.1 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 2.7.1 *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 *(Suites stationnaires)*

Soit $(a_n)_n$ est une suite des nombres $p-$adiques. Si $\lim\limits_{n\longrightarrow\infty} a_n = a$ avec $a \in \mathbb{Q}_p$ et $|a|_p \neq 0$. Alors la suite des normes $p-$adiques $\left\{|a_n|_p, n \in \mathbb{N}\right\}$ doit se stabiliser (ou stationnaire) pour n assez grand, c'est-à-dire qu'il existe N tel que

$$|a_n|_p = |a|_p, \forall n \geq N$$

Preuve. Soit $(a_n)_n \in \mathbb{Q}_p$, telle que $\lim\limits_{n\longrightarrow\infty} a_n = a$. Donc $(a_n)_n$ est une suite convergente dans $\mathbb{Q}_p$

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

D'autre part, on a

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

donc $(|a_n|_p)_n$ est une suite de Cauchy dans $\mathbb{R}$ complet, ce qui donne $(|a_n|_p)_n$ est convergente dans $\mathbb{R}$ et soit l sa limite

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

Or

$$|a|_p \neq 0 \Longrightarrow |a|_p > 0$$

alors

$$\forall \varepsilon = \frac{l}{2} > 0, \exists N_1 \in \mathbb{N} : \forall n \geq N_1 \Longrightarrow |a_n|_p > \frac{l}{2} \tag{2.2}$$

En effet, on a

$$\left||a_n|_p - l\right| < \frac{l}{2} \Longrightarrow \frac{l}{2} < |a_n|_p < \frac{l}{2} + l$$

de même, comme $(a_n)_n$ est de Cauchy dans $\mathbb{Q}_p$, alors

$$\forall \varepsilon = \frac{l}{2} > 0, \exists N_2 \in \mathbb{N} : \forall m, n \geq N_2 \Longrightarrow |a_m - a_n|_p < \frac{l}{2} \tag{2.3}$$

donc

$$\begin{aligned} \forall n \quad &\geq \quad N_3 = \max(N_1, N_2) \Longrightarrow |a_m|_p = |a_m - a_n + a_n|_p \\ &= \quad \max(|a_m - a_n|_p, |a_n|_p) \\ &= \quad |a_n|_p, \forall n \geq N_3 \end{aligned}$$

pour $m \longrightarrow \infty$, alors

$$|a|_p = |a_n|_p, \forall n \geq N_3$$

□

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$(2.7.1)$ devient un outil important pour déterminer si une série de nombres $p-$adiques converge dans $\mathbb{Q}_p$ ou non.

Définition 2.7.1 *(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 $\mathbb{R}$.*

Comme dans $\mathbb{R}$, il résulte de l'inégalité triangulaire que la convergence absolue d'une série implique sa convergence dans $\mathbb{Q}_p$.

Proposition 2.7.2 *Si la série $\sum_{n=0}^{+\infty} |a_n|_p$ converge (absolument) dans $\mathbb{R}$, alors $\sum_{n=0}^{+\infty} a_n$ converge dans $\mathbb{Q}_p$.*

Preuve. Supposons que $\sum_{n=0}^{+\infty} |a_n|_p$ converge. Alors, la suite de ses sommes partielles est de Cauchy, c'est-à-dire pour tout $\varepsilon > 0$ il existe $N \in \mathbb{N}$ tel que Pour tout $m > n > N$, nous avons $\sum_{i=n+1}^{m} |a_i|_p < \varepsilon$. Par l'inégalité triangulaire, nous obtenons

$$|S_m - S_n|_p = \left| \sum_{i=n+1}^{m} |a_i|_p \right| \leq \sum_{i=n+1}^{m} |a_i|_p \leq \varepsilon$$

Par conséquent $(S_n)_n$ est une suite de Cauchy et par définition $\sum_{n=0}^{+\infty} a_n$ converge dans $\mathbb{Q}_p$. □

Remarque 2.7.1 *Comme dans $\mathbb{R}$, la convergence n'implique pas la convergence absolue. Autrement dit, dans $\mathbb{Q}_p$ il existe des séries $p-$adiques qui convergent, mais ne convergent pas absolument.*

Cependant nous pouvons obtenir un résultat beaucoup mieux dans $\mathbb{Q}_p$ comme indiqué la proposition suivante.

Proposition 2.7.3 *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 Il résulte du théorème $(2.7.1)$ 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 $(2.7.1)$ 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 2.7.2 *Cette propriété est fausse dans* $(\mathbb{R}, |.|)$*, 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* $(\mathbb{R}, |.|)$ *dont le terme général tend vers* 0*, mais qui ne converge pas, est la série harmonique* $\sum_{n\geq 1} \frac{1}{n}$*.*

Exemple 2.7.1

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* $a_n = u_n.n!$ *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* $|u_n.n!|_p \leq |n!|_p$ *et* $n! \longrightarrow 0$ *quand* $n \longrightarrow \infty$*.*

2.7.2 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 2.7.2 *(Topologie $p-$adique). On définit la topologie $p-$adique par la famille des boules*

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

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

Proposition 2.7.4 *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 $(1.1.2)$. □

Proposition 2.7.5 *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 $(2.7.4)$, on a

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

Alors

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

□

Proposition 2.7.6 *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

$$r_1 = |y-a|_p = |y - x_0 + x_0 - a|_p$$

$$\leq |y-x_0|_p + |x_0 - a|_p$$

$$< r_1 - r + r = r_1$$

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

Proposition 2.7.7 *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 2.7.8 *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*

$$B(a,r) \cap B(b,s) \neq \varnothing \Longrightarrow B(a,r) \subset B(b,s) \text{ ou } B(b,s) \subset B(a,r) \tag{2.4}$$

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 $(2.7.7)$

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

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

Méthode de Halley pour trouver les racines d'équations polynomiales p-adiques

En mathématiques, il est souvent souhaitable de résoudre l'équation $f(x) = 0$ analytiquement, mais souvent cela ne peut pas être fait. Les équations de cette forme se produisent souvent en algèbre, calcul différentiel, physique, équations différentielles, chimie, etc... Lorsque des solutions analytiques ne sont pas possibles pour ces équations, les méthodes d'approximation numérique sont utiles pour obtenir des solutions approximatives. On remplace alors la résolution mathématique exacte du problème par sa résolution numérique qui est, en général, approchée. L'analyse numérique est la branche des mathématiques qui étudie les méthodes de résolution numérique des problèmes, méthodes que l'on appelle constructives. Par méthode constructive, on entend un ensemble de règles (on dit : algorithme) qui permet d'obtenir la solution numérique d'un problème avec une précision désirée après un nombre fini d'opérations arithmétiques. Ces méthodes sont devenues aujourd'hui un outil essentiel pour l'investigation dans les différents problèmes fondamentaux de notre assimilation des phénomènes scientifiques qui sont difficiles, à savoir impossible à résoudre dans le passé. Ainsi, notons qu'il existe actuellement de nombreuses méthodes numériques utilisées pour résoudre numériquement les équations non linéaires $f(x) = 0$ (méthode de Newton, sécante, point fixe...).

3.1 Construction de la méthode de Halley

La méthode itérative de Newton est très populaire à cause de la simplicité de sa formulation et de son ordre de convergence. Nous allons présenter ici une dérivation simple de cette méthode, nommée méthode de Halley. Cette méthode a été découverte par Edmond Halley (un mathématicien anglais 1656-1742), elle s'applique à une fonction de C^2 (i.e, f' et f'' sont continues) pour trouver une approximation numérique des racines à l'équation $f(x) = 0$.

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

$$x_0, x_1 = F(x_0), x_2 = F(x_1), ...$$

La suite ainsi obtenue,

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

est appelée l'orbite de x_0 sous itération de F. Cette relation peut également s'écrire

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

Telles que

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

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

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

Évidemment, α est un point fixe de F si α est une racine de (3.2). Cette méthode possède également une belle interprétation géométrique. Nous commençons cependant par donner une première façon d'en obtenir l'algorithme, basée sur l'utilisation du développement de Taylor.
Étant donné une fonction f et soit une équation à résoudre de la forme

$$f(x) = 0$$

La série de Taylor de la fonction f autour d'un point x_0 est donnée par

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + f''(x_0)\frac{(x - x_0)^2}{2} + ... \tag{3.4}$$

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, nous négligeons les termes d'ordre supérieur ou égal à 2 de la série pour obtenir

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

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. On appelle x_1 la valeur ainsi trouvée qui est proche de la valeur pour laquelle $f(x) = 0$ et donnée par

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

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

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \tag{3.5}$$

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

Interprétation géométrique de la méthode de Newton.

La figure 3.1 permet de donner une interprétation géométrique assez simple de la méthode de Newton. Sur cette figure, on a représenté la fonction f, la valeur initiale x_0 et le point $(x_0, f(x_0))$ qui est sur la courbe. La droite tangente à la courbe en ce point est de pente $f'(x_0)$ et a pour équation

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

qui correspond au développement de Taylor de degré 1 autour de x_0. Cette droite coupe l'axe des x en $y = 0$, c'est-à-dire en

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

qui devient la nouvelle valeur estimée de la solution. On reprend ensuite le même raisonnement à partir du point $(x_1, f(x_1))$ et ainsi de suite. On obtient, de cette manière, la solution approchée x_{n+1} n'est autre que le point d'intersection de l'axe des abscisses et la tangente, au point $(x_n, f(x_n))$, d'équation

$$D : y = f(x_n) + f'(x_n)(x - x_n)$$

On obtient ainsi une suite de points qui converge vers la solution de l'équation. Le lien entre deux termes consécutifs de la suite est donné par la formule (3.5).

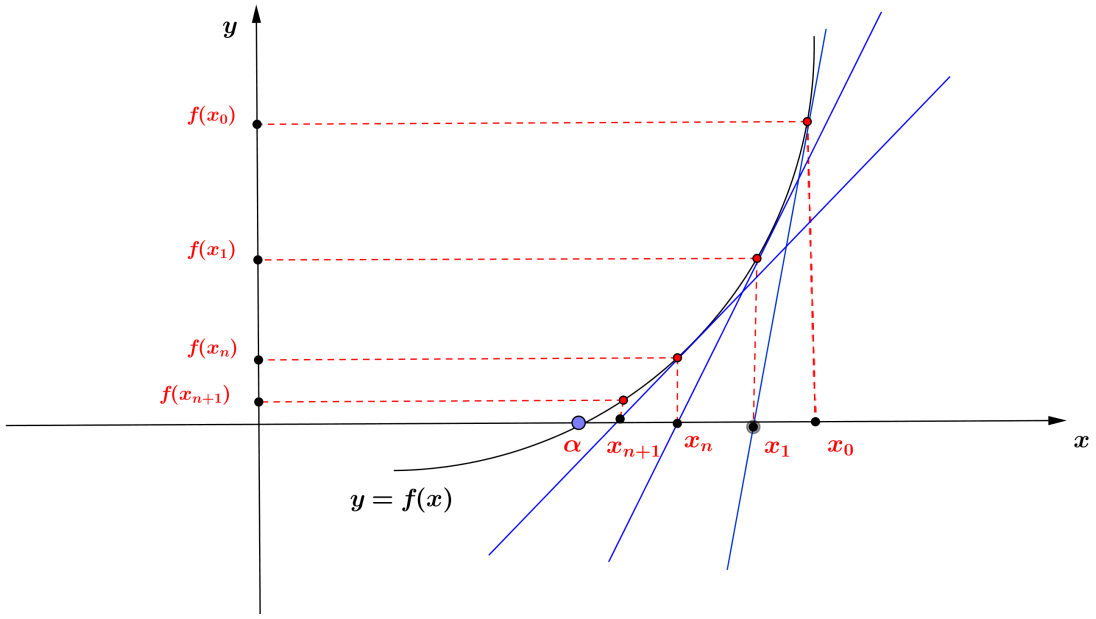

FIGURE 3.1 – Interprétation géométrique de la méthode de Newton.

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

$$y(x) = f(x) = f(x_n) + f'(x_n)(x - x_n) + f''(x_n)\frac{(x - x_n)^2}{2} \tag{3.6}$$

où x_n est à nouveau une racine approchée de $f(x) = 0$. Comme avec la méthode de Newton, le but est de déterminer un point x_{n+1}, dans lequel la courbe $y = f(x)$ coupe l'axe des abscisses x, c'est-à-dire de résoudre l'équation

$$f(x_n) + f'(x_n)(x_{n+1} - x_n) + f''(x_n)\frac{(x_{n+1} - x_n)^2}{2} = 0$$

Par suite

$$f(x_n) + (x_{n+1} - x_n)\left(f'(x_n) + \frac{f''(x_n)}{2}(x_{n+1} - x_n)\right) = 0$$

il résulte que

$$x_{n+1} - x_n = -\frac{f(x_n)}{f'(x_n) + \frac{f''(x_n)}{2}(x_{n+1} - x_n)} \tag{3.7}$$

En approximant la différence $(x_{n+1} - x_n)$ restant sur le côté droit de (3.7) par la valeur $\left(-\frac{f(x_n)}{f'(x_n)}\right)$ donnée en (3.5), on obtient

$$\forall n \in \mathbb{N} : x_{n+1} = x_n - \frac{2f'(x_n)f(x_n)}{2f'(x_n)^2 - f''(x_n)f(x_n)} \tag{3.8}$$

qui est l'algorithme récursif de la méthode de Halley.

Remarque 3.1.1 *La formule* (3.8) *montre également la similitude entre la méthode de Halley et celle de Newton. Lorsque la dérivée seconde est très proche de zéro, les itérations sont presque les mêmes que dans la méthode de Newton.*

3.2 Etude de la méthode

Notre travail consiste à utiliser la méthode de Halley 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 cubiques d'un nombre p-adique $a \in \mathbb{Q}_p$ à l'aide de suites de nombres p-adiques construite par la méthode de Halley. Pour cela, on se propose d'étudier le problème suivant

$$\begin{cases} f(x) = x^3 - a = 0 \\ a \in \mathbb{Q}_p^* \ , \ p\text{-premier} \end{cases} \tag{3.9}$$

La solution de (3.9) est approchée par une suite des nombres p-adiques $(x_n)_n \in \mathbb{Q}_p$ construite par la méthode de Halley.

Principe général de calcul :

Le principe de calcul pour la fonction définie par

$$f(x) = x^3 - a = 0 \tag{3.10}$$

Supposons que $a \in \mathbb{Q}_p^*$ admet une racine cubique, alors $v_p(a) = 3m, m \in \mathbb{Z}$ et

$$|a|_p = p^{-v_p(a)} = p^{-3m}$$

D'après la proposition $(2.7.1)$, si $(x_n)_n$ est une suite des nombres p-adiques qui converge vers un nombre p-adique $c \neq 0$ alors à partir d'un certain rang, on a

$$|x_n|_p = |c|_p \tag{3.11}$$

Autrement dit la suite des valeurs absolues est stationnaire.

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

$$c^3 = a$$

Alors

$$|c|_p^3 = |a|_p = p^{-3m}$$

Par conséquent

$$|c|_p = p^{-m} \tag{3.12}$$

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

$$|x_n|_p = |c|_p = p^{-m} \tag{3.13}$$

3.2.1 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 (ou ordre) de convergence de la suite $(x_n)_n$. L'ordre de convergence est une indication de la vitesse à laquelle une méthode itérative converge. Plus l'ordre de convergence est

grand, moins on a besoin de faire d'itération pour être proche de la bonne solution. Ceci justifie donc l'intérêt d'avoir un ordre de convergence aussi grand que possible. De plus, L'ordre de convergence est un bon estimateur du nombre d'itérations nécessaire pour atteindre une certaine précision.

Pour mesurer la vitesse de convergence d'une méthode itérative, on étudie l'évolution de la suite $(e_n)_n$ des écarts

$$e_n = x_{n+n_0+1} - x_{n+n_0}$$

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 $\sqrt[3]{a}$. Donc, il est question de trouver n tel que

$$|e_n = x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{-M} \tag{3.14}$$

Remarque 3.2.1

(1) Si le l'ordre de convergence d'une méthode est p (c'est-à-dire que la méthode converge avec l'ordre p), alors après chaque itération, le nombre de chiffres significatifs exacts de x_n (ceux identiques à ceux de α) augmente d'un facteur d'environ p. Par exemple, si notre approximation converge de façon quadratique (resp : cubique)(c'est-à-dire avec l'ordre 2 (resp, 3)), alors le nombre de chiffres significatifs exacts double (resp. triple) à chaque itération.

(2) On dit qu'une méthode d'itération est plus rapide qu'une autre, si la méthode obtient le même résultat avec moins d'itérations. Evidement avec les même conditions aux départ (même approche de x_0 vers α). On dit aussi que la vitesse d'itération est plus grande..

Définition 3.2.1 *Soit $a \in \mathbb{Q}_p^*$. On dit que $b \in \mathbb{Q}_p$ est une racine cubique de a d'ordre r si et seulement si $b^3 \equiv a \mod p^r$.*

Remarque 3.2.2

(1) Si $a^3 \equiv b \mod p^r$, *alors*

$$\begin{aligned} a^3 - b &\equiv 0 \mod p^r \Longrightarrow p^r \text{ divise } (a^3-b) \\ &\Longrightarrow v_p(a^3-b) \geq v_p(p^r) = r \\ &\Longrightarrow -v_p(a^3-b) \leq -r \\ &\Longrightarrow p^{-v_p(a^3-b)} \leq p^{-r} \\ &\Longrightarrow \left|a^3-b\right|_p \leq p^{-r} \end{aligned}$$

(2) De même si $\left|a^3-b\right|_p \leq p^{-r}$, *alors* $a^3 - b \equiv 0 \mod p^r$.

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

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

Telles que

$$\begin{cases} f(x) = x^3 - a \\ f'(x) = 3x^2 \\ f''(x) = 6x \end{cases}$$

Ce qui donne

$$x_{n+1} = x_n - \frac{2\left(x_n^3-a\right)3x_n^2}{2\left(3x_n^2\right)^2 - 6x_n\left(x_n^3-a\right)} = x_n - \Big(-\left(a+2x_n^3\right)^{-1}\left(a-x_n^3\right)x_n\Big) = x_n - \left(a+2x_n^3\right)^{-1}\left(x_n^3-a\right)x_n$$

On obtient

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

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+1}^3 - a = \frac{\left(a+x_n^3\right)\left(x_n^3-a\right)^3}{\left(a+2x_n^3\right)^3} \tag{3.17}$$

et

$$\forall n \in \mathbb{N} : x_{n+1} - x_n = -\frac{x_n\left(x_n^3-a\right)}{\left(a+2x_n^3\right)} \tag{3.18}$$

Par ailleurs, on a

$$|27|_p = \begin{cases} \frac{1}{27}, & \text{si } p = 3 \\ 1, & \text{si } p \neq 3 \end{cases} \tag{3.19}$$

et

$$|3|_p = \begin{cases} \frac{1}{3}, & \text{si } p = 3 \\ 1, & \text{si } p \neq 3 \end{cases} \tag{3.20}$$

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

Théorème 3.2.1 *Si x_{n_0} est la racine cubique de a d'ordre r, alors*

① *Si $p \neq 3$, alors x_{n+n_0} est la racine cubique de a d'ordre v_n, i.e,*

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod p^{v_n} \tag{3.21}$$

où la suite $(v_n)_n$ est définie par

$$\forall n \in \mathbb{N} : v_n = 3^n r - 3(3^n - 1)m \tag{3.22}$$

et la suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{w_n} \tag{3.23}$$

Telle que

$$\forall n \in \mathbb{N} : w_n = 3^n r - \left(3^{n+1} - 1\right) m \tag{3.24}$$

② *Si $p = 3$, alors x_{n+n_0} est la racine cubique de a d'ordre v'_n, i.e,*

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod 3^{v'_n} \tag{3.25}$$

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

$$\forall n \in \mathbb{N} : v'_n = 3^n r - \frac{(3^n - 1)}{2}(6m + 3) \tag{3.26}$$

et la suite des écarts est donnée par

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 3^{w'_n} \tag{3.27}$$

Telle que

$$\forall n \in \mathbb{N} : w'_n = 3^n r - \frac{(3^{n+1} - 1)}{2}(2m + 1) \tag{3.28}$$

Preuve.

Etape 1 : Supposons que x_{n_0} soit la racine cubique de a d'ordre r , tels que n_0 représente un rang quelconque et $r \in \mathbb{N}$. Donc

$$x_{n_0}^3 - a \equiv 0 \mod p^r \Longrightarrow \left|x_{n_0}^3 - a\right|_p \leq p^{-r} \tag{3.29}$$

alors

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

En appliquant l'inégalité triangulaire forte, et (3.29), on a

$$\left|x_{n_0+1}^3-a\right|_p\leq\left|\frac{1}{\left(a+2x_{n_0}^3\right)^3}\right|_p.\max\left\{|a|_p,\left|x_{n_0}^3\right|_p\right\}.p^{-3r} \tag{3.30}$$

D'autre part, on a

$$\left|\frac{1}{\left(a+2x_{n_0}^3\right)^3}\right|=\frac{1}{\left|\left(a+2x_{n_0}^3\right)^3\right|_p}=\frac{1}{\left|\left(a+2x_{n_0}^3\right)\right|_p^3}$$

D'après la proposition $(2.7.1)$, on déduit

$$\frac{1}{\left|\left(a+2x_{n_0}^3\right)\right|_p^3}=\frac{1}{|3a|_p^3}=\frac{1}{|27|_p}.\frac{1}{|a|_p^3}=\frac{1}{|27|_p}.\frac{1}{p^{-9m}} \tag{3.31}$$

Les relations (3.30), et (3.31) impliquent

$$\begin{aligned}\left|x_{n_0+1}^3-a\right|_p&\leq\left(\frac{1}{|27|_p}.p^{9m}\right).\left(p^{-3m}\right).\left(p^{-3r}\right)\\&\leq\frac{1}{|27|_p}.p^{6m}.p^{-3r}\end{aligned}$$

Par (3.19), on trouve

$$\begin{cases}\left|x_{n_0+1}^3-a\right|_p\leq p^{-3r}.p^{6m}=p^{-(3r-6m)},&\text{si } p\neq 3\\[2ex]\left|x_{n_0+1}^3-a\right|_3\leq 3^3.3^{6m}.3^{-3r}=3^{-(3r-(6m+3))},&\text{si } p=3\end{cases}$$

Ce qui donne

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

De manière similaire, on trouve

• si $p\neq 3$, alors

$$\begin{cases}x_{n_0}^3-a\equiv 0 \mod p^{v_0}\\ v_0=r\end{cases}\Longrightarrow\begin{cases}x_{n_0+1}^3-a\equiv 0 \mod p^{v_1}, v_1=3r-6m\\ x_{n_0+2}^3-a\equiv 0 \mod p^{v_2}; v_2=9r-24m\\ x_{n_0+3}^3-a\equiv 0 \mod p^{v_3}, v_3=27r-78m\\ .\\ .\\ .\end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod p^{v_n} \tag{3.32}$$

où la suite $(v_n)_n$ est définie par

$$\forall n \in \mathbb{N} : \begin{cases} v_{n+1} = 3v_n - 6m \\ v_0 = r \end{cases}$$

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

$$\forall n \in \mathbb{N} : v_n = 3^n r - 3(3^n - 1)m \tag{3.33}$$

Par conséquent

$$v_p(x_{n+n_0}^3 - a) \geq 3^n r - 3(3^n - 1)m \tag{3.34}$$

• Si $p = 3$, alors

$$\begin{cases} x_{n_0}^3 - a \equiv 0 \mod 3^{v_0} \\ v_0' = r \end{cases} \Longrightarrow \begin{cases} x_{n_0+1}^3 - a \equiv 0 \mod 3^{v_1'}, v_1' = 3r - 6m - 3 \\ x_{n_0+2}^3 - a \equiv 0 \mod 3^{v_2'}, v_2' = 9r - 24m - 12 \\ x_{n_0+3}^3 - a \equiv 0 \mod 3^{v_3'}, v_3' = 27r - 78m - 39 \\ . \\ . \\ . \end{cases}$$

Par conséquent

$$\forall n \in \mathbb{N} : x_{n+n_0}^3 - a \equiv 0 \mod 3^{v_n'} \tag{3.35}$$

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

$$\forall n \in \mathbb{N} : \begin{cases} v_{n+1}' = 3v_n' - (6m+3) \\ v_0' = r \end{cases}$$

Par suite

$$\forall n \in \mathbb{N} : v_n' = 3^n r - \frac{(3^n - 1)}{2}(6m + 3)$$

Par conséquent

$$v_3(x_{n+n_0}^3 - a) \geq 3^n r - \frac{(3^n - 1)}{2}(6m + 3) \tag{3.36}$$

Ce qui donne

$$\forall n \in \mathbb{N} : v_n' = v_n - 3\frac{(3^n - 1)}{2} \tag{3.37}$$

Etape 2 : on a

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

Ce qui donne

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

On obtient

$$|x_{n+n_0+1} - x_{n+n_0}|_p = \frac{1}{\left|a+2x_{n+n_0}^3\right|_p}.\,|x_{n+n_0}|_p\,.\left|x_{n+n_0}^3 - a\right|_p$$

D'après la proposition $(2.7.1)$, on déduit

$$\left|a+2x_{n+n_0}^3\right|_p = |3|_p\,.p^{-3m}$$

et par (3.13), on a

$$|x_{n+n_0}|_p = p^{-m}$$

On obtient

$$|x_{n+n_0+1} - x_{n+n_0}|_p = \frac{1}{\left|a+2x_{n+n_0}^3\right|_p}.\,|x_{n+n_0}|_p\,.\left|x_{n+n_0}^3 - a\right|_p = \frac{1}{|3|_p\,.p^{-3m}}.p^{-m}.\left|x_{n+n_0}^3 - a\right|_p$$

Les relations (3.20) , (3.32) et (3.35) impliquent

$$\begin{cases} |x_{n+n_0+1} - x_{n+n_0}|_p \leq p^{2m}.p^{-v_n} = p^{-(v_n-2m)}, \text{ si } p \neq 3 \\ |x_{n+n_0+1} - x_{n+n_0}|_3 \leq 3.3^{2m}.3^{-v'_n} = 3^{-(v'_n-2m-1)}, \text{ si } p = 3 \end{cases}$$

Ainsi, pour $p \neq 3$, on a

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod p^{w_n} \tag{3.38}$$

Telle que

$$\forall n \in \mathbb{N} : w_n = v_n - 2m$$

Par suite,

$$\forall n \in \mathbb{N} : w_n = 3^n r - \left(3^{n+1} - 1\right) m \tag{3.39}$$

Ce qui entraine

$$v_p(x_{n+n_0+1} - x_{n+n_0}) \geq 3^n r - \left(3^{n+1} - 1\right) m \tag{3.40}$$

Pour $p = 3$, on a

$$\forall n \in \mathbb{N} : x_{n+n_0+1} - x_{n+n_0} \equiv 0 \mod 3^{w'_n}$$

Telle que

$$\forall n \in \mathbb{N} : w'_n = v'_n - 2m - 1 \tag{3.41}$$

Par suite

$$\forall n \in \mathbb{N} : w'_n = 3^n r - \frac{(3^{n+1} - 1)}{2}(2m + 1) \tag{3.42}$$

Ce qui entraine

$$v_3(x_{n+n_0+1} - x_{n+n_0}) \geq 3^n r - \frac{(3^{n+1} - 1)}{2}(2m + 1) \tag{3.43}$$

De plus

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

□

Remarque 3.2.3 *Dans le cas réel, la méthode de Halley a une convergence cubique. Cela signifie que le nombre de chiffres significatifs exacts triple à chaque itération. Pour une discussion approfondie de la propriété de convergence de la méthode de Halley, nous renvoyons les lecteurs à [9] et pour une discussion plus approfondie de la méthode, on peut consulter [11] et [22].*

Conclusion Générale

Nous pouvons résumer nos résultats principaux de la manière suivante.

Conclusion 3.2.1

① ***Si*** $p \neq 3$, *alors*

ⓐ *La vitesse de convergence de la suite* $(x_n)_n$ *obtenue par la méthode de Halley est de l'ordre* w_n .

ⓑ *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*

$$w_n = (3^n r - \left(3^{n+1} - 1\right) m) \geq M$$

on obtient

$$n = \left[\frac{\ln(\frac{M-m}{r-3m})}{\ln 3} \right] \tag{3.44}$$

avec $r - 3m > 0$.

② ***Si*** $p = 3$, *alors*

ⓐ *La vitesse de convergence de la suite* $(x_n)_n$ *obtenue par la méthode de Halley est de l'ordre* w'_n.

ⓑ *Pour déterminer le nombre d'itérations nécessaires* n *pour* M *chiffres donnés, on pose*

$$w'_n = 3^n r - \frac{(3^{n+1} - 1)}{2} (2m + 1) \geq M$$

on obtient

$$n = \left[\frac{\ln(\frac{2M-2m-1}{2r-6m-3})}{\ln 3} \right] \tag{3.45}$$

avec $2r - 6m - 3 > 0$.

③ *La convergence vers zéro pour tout nombre p-adique* $a \in \mathbb{Q}_p$ *telle que* $p \neq 3$ *est beaucoup plus rapide que celle de* $\mathbb{Q}_3$.

④ *Dans le contexte p-adique, la vitesse de convergence de la méthode de Halley 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, F. Saleri. Méthodes Numériques : Algorithmes, analyse et applications, Springer Science & Business Media, 2008.

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

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

[4] C.k. Koç. A Tutorial on p-adic Arithmetic. Electrical and Computer Engineering, Oregon State University, Corvallis, Oregon 97331, 2002.

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

[6] F. V. Bajers. P-adic numbers, Aalborg University. Departement Of Mathematical Sciences. 7E 9222 Aalborgest. Groupe E3-104, 18-12-2000.

[7] F. Q. Gouvêa, P-adic numbers : An introduction, Springer-Verlag Berlin Heidelberg New York, Second Edition, Universitext, 2000.

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

[9] G. Alefeld. On the Convergence of Halley's Method, Amer. Math. Monthly, 88 (1981), no. 7, 530-536.

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

[11] J. M. Ortega, W. C. Rheinbolt. Iterative Solution of Nonlinear Equation in Several Variables. Vol. 30. Siam, 1970.

[12] J. F. T Rabago. Halley's method for approximating roots of p-adic polynomial equations, Int. J. Math. Anal. (Ruse), 10 (10), 493-502, 2016

[13] J.F. Epperson. An introduction to numerical methods and analysis, John Wiley & Sons, 2013.

[14] M. P. Knapp, C. Xenophontos. Numerical Analysis meets Number Theory : Using root finding methods to calculate inverses mod p^n, Appl. Anal. Discrete Math. 4, 23-31, 2010.

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

[16] S. Albeverio, A. Yu. Khrennikov and V. M. Shelkovich, Theory of p-adic distributions : Linear and nonlinear models, London Mathematical Society, Cambridge University Press, 2010.

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

[18] S. Katok. p-adic Analysis Compared with Real, Vol. 37, American Mathematical Soc, 2007.

[19] T. Zerzaihi, M. Kecies. Computation of the cubic root of a p-adic number. J.M.R. 3, 40-47, 2011.

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

[21] T. Zerzaihi, M. Kecies, M.P. Knapp. Hensel codes of square roots of p-adic numbers. Appl. Anal. Discrete Math. 4, 32-44, 2010.

[22] T. R. Scavo, J. B. Thoo. On the Geometry of Halley's Method, Amer. Math. Monthly, 102, no. 5, 417-426, 1995.

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

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

Résumé

Ce travail propose un analogue de la méthode de Halley pour résoudre un problème de recherche de racine $f(x)=0$ dans le contexte p-adique. En particulier, une racine de l'équation polynomiale $f(x)=x^3-a=0$, où $a\in Q_p$ et Q_p dénote l'ensemble des nombres p-adiques, est calculée par la méthode de Halley. Cette méthode a une convergence d'ordre 3 et converge plus rapide que la méthode de Newton.

2010 Mathematics subject classification : 26E30. 34K28. 11E95.

Mots clés : valuation p-adique, norme p-adique, nombre p-adique, racine cubique, développement p-adique, Méthode de Newton, Méthode de Halley, vitesse de convergence.

Abstract

This work proposes an analogue of Halley's method for solving a root-finding problem f(x)=0 in the p-adic setting. In particular, a root of the polynomial equation $f(x)=x^3-a=0$, where $a\in Q_p$ and Q_p denotes the set of p-adic numbers, is computed through Halley's method. This method has convergence of order 3 and converges faster than Newton's method.

2010 Mathematics subject classification : 26E30. 34K28. 11E95

Key words : p-adic valuation, p-adic norm, p-adic number, cubic root, p-adic development, Newton's method, Halley's Method, speed of convergence.

ملخص

يقترح هذا العمل نظيرًا لطريقة هالي لحل مشكلة إيجاد الجذر f (x) = 0 في سياق البيأديك .
على وجه الخصوص ، يتم حساب جذر المعادلة متعددة الحدود $f(x)=x^3-a=0;a\in Q_p$ حيث Q_p تشير إلى مجموعة أعداد البيأديك بواسطة طريقة هالي. هذه الطريقة لها تقارب تكعيبي وتتقارب أسرع من طريقة نيوتن.

الكلمات المفتاحية: تقييم البيأديك ، نظيم البيأديك ، عدد البيأديك ، جذر تكعيبي ، نشر البيأديك ، طريقة نيوتن ، طريقة هالي ، سرعة التقارب.