الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMMED SEDDIK BENYAHIA – JIJEL

FACULTE DES SCIENCES EXACTES ET INFORMATIQUE

DEPARTEMENT DE MATHEMATIQUES

N° d'ordre : ……..…

N° de série : …….

THESE

Présenté en vue de l'obtention du diplôme de :

DOCTORAT EN SCIENCES

Spécialité : Mathématiques

Option : Analyse

Thème

Caractérisation algébrique d'un nombre *p*-adique dont le développement de Hensel est engendré par une fraction continue

Par :

Rafik BELHADEF

Devant le jury :

Président :	**D. Laouir-Azzam**	**Professeur**	**Univ. Mohammed Seddik Benyahia, Jijel**
Rapporteur :	**T. Zerzaihi**	**Professeur**	**Univ. Mohammed Seddik Benyahia, Jijel**
Co-rapporteur :	**H.A. Esbelin**	**M.C**	**Univ. Blaise Pascale, France**
Examinateurs :	**M. Denche**	**Professeur**	**Univ. Constantine1**
	L. Noui	**Professeur**	**Univ. Hadj Lakhder Batna**
	M. Kerada	**M.C.A**	**Univ. Mohammed Seddik Benyahia, Jijel**

Soutenue le : …….

Dédicace إهداء

أهدي هذا العمل المتواضع إلى أعز إنسانين في الحياة: أمي وأبي حفظهما الله، وإلى زوجتي الغالية رعاها الله، وإلى إبنيَّ هيثم ومنصف، و إلى كل العائلة الكريمة.

Remerciements

Allah الله

أحمد الله الذي وفقني إلى إتمام هذا العمل،.. وأدعو الله أن يجعله في ميزان حسناتي ويهديني إلى ما فيه الخير والصلاح. الحمد لله حمدا طيبا مباركا فيه، كما يحب ربي ويرضى.

Le Jury

Mr. Zerzaihi Tahar, professeur à l'université de Jijel, mon directeur de thèse, et Mr. Esbelin Henri-Alex, maître de conférences à l'université de Blaise Pascal en France, mon co-directeur de thèse, ont accompagné mes premiers pas mathématiques dans monde des nombres p-adiques et les fractions continues et, depuis, leur soutien ne s'est jamais altéré. J'ai conscience de leur devoir beaucoup. Ils ont profondément influencé ce travail, qui est en partie le leur, même si toute critique doit bien sûr être adressée au seul auteur de cette thèse. Par leur intégrité, leur rigueur, leur curiosité et leur générosité.

Je remercie encore une fois, Monsieur Esbelin, d'avoir accepté de m'accueillir dans son ex-laboratoire (LAIC), et d'avoir mis à ma disposition tous les moyens nécessaires à mon travail de recherche, durant mon stage de longue durée à Clermont-Ferrand.

C'est avec beaucoup de plaisir que je remercie Mme. Laouir Dalila, professeur à l'université de Jijel, d'avoir accepté la tâche de président du jury et de s'être acquitté de celle-ci avec le plus grand soin.

Dés mes études DES et de magister, j'ai eu l'occasion de découvrir certains travaux de Mr. Denche Mohamed, professeur à l'université de Constantine1. Je suis honoré qu'il se soit penché sur mon travail pour rédiger un rapport et d'être membre du jury, après qu'il se soit déjà membre du jury de mon magister..

Je remercie également chaleureusement Mr. Naoui Lemnaouar, professeur à l'université de Batna, de prendre part à ce jury, et de me fait un rapport pour cette thèse.

Depuis plusieurs années, j'ai eu la chance de bénéficier des encouragements de Mr. Kerada Mohamed, maître de conférences à l'université de Jijel. Je le remercie beaucoup de l'intérêt porté à mon travail et je suis très heureux de le compter parmi mes examinateurs, après qu'il se soit déjà membre du jury de mon magister.

Les institutions

Je voudrais exprimer toute ma gratitude au Laboratoire de mathématiques pures et appliquées (LMPA), ainsi au son directeur Mr. Yarou Mustapha, pour la liberté qu'il m'offre. Il infléchit les notions d'espace et de temps, rendant le rêve possible.
Je suis très reconnaissant envers le département de mathématiques, et son chef Mr. Bensuileh Bechir, des excellentes conditions de travail qui m'ont été offertes.

Les collègues

A défaut d'avoir un mot pour chacun, je dois me contenter d'en adresser quatre à tous : je vous remercie sincèrement. Il en est quand même deux qu'il me faut nommer, Mustapha Fezani, Nabil Mahamdioua, pour m'avoir montré que derrière l'austérité d'un organisme peuvent se cacher les meilleurs des amis.

Mes remerciements vont aussi à Boutabaa Abdelbaki, de m'accueillir dans le laboratoire de mathématiques à l'université Blaise Pascal, durant mes stages. De nombreuses discussions avec lui, m'ont permis de mieux comprendre les nombres p-adiques. Je le remercie pour qui s'est toujours montré disponible pour répondre à mes questions.

D'autres personnes m'ont encouragé à finir ce travail par des gestes d'amitié dont je suis reconnaissant. A titre d'exemple, je citerai : Tahar Boumezbeur, Ammar Tibouche, Abdelfettah Belafrites, Nouressadat Touafek. En dehors de l'université : Abdelmalek Bouzenoun et Omer Alioua.

La famille

Il est un point où l'exercice des remerciements peut prendre un tour plus personnel; à chacun sa pudeur. A ma famille et mes amis, je voudrais simplement dire merci d'être là, car le reste n'est que fiction. A mes parents, je souhaite adresser un remerciement particulier pour la tendresse avec laquelle ils suivent mon excursion mathématique.

Lorsque vient le moment de fermer la porte du bureau, et de poser la craie, lorsqu'il faut s'extraire du monde des pensées pour retrouver les siens, c'est chaque fois avec le plus grand bonheur que je parcours le chemin. Pour cela, et tant de choses encore, je remercie ma femme « Meriem », qui répondait toujours présent pour m'aider chaque fois que j'avais un problème informatique, merci Meriem de m'avoir supporté et aidé.

Jijel, 13 septembre 2015

Table des matières

Introduction Générale **3**

Notation **6**

1 Préliminaires sur les nombres p-adiques **7**
1.1 Valuations et normes p-adiques 8
1.1.1 Valuations p-adiques 8
1.1.2 Normes p-adiques 9
1.2 Construction du corps des nombres p-adiques 13
1.3 Propriétés du corps $\mathbb{Q}_p$ 17
1.3.1 Développement de Hensel 17
1.3.2 Propriétés analytiques 21
1.3.3 Lemme de Hensel 24

2 Automates finis et fractions continues **32**
2.1 Automates finis 32
2.1.1 Définitions et propriétés 32
2.1.2 Nombres et suites automatiques 35
2.2 Fractions continues 41
2.2.1 Définitions et propriétés 41
2.2.2 Fractions continues p-adiques 48
2.3 Théorèmes dans le cas réel 56
2.3.1 Questions de transcendance 56
2.3.2 Théorème du sous-espace 59

3 Etudes de la complexité et de la transcendance **62**
3.1 Complexité des développements d'un nombre rationnel 62
3.1.1 Caractérisation d'un nombre rationnel 62
3.1.2 Complexité du développement de Hensel 67

3.1.3 Complexité du développement en FCB 72
3.1.4 Complexité du développement en FCS 76
3.2 Etude de la transcendance 80
3.2.1 Transcendance d'un développement en FCB 80
3.2.2 Transcandence des fractions continues p-adique de Thue-Morse . . . 84

A Corps normés **88**

B Théorème de complétion **92**

Bibliographie **99**

Introduction Générale

Un thème très important dans la théorie des nombres est de trouver les solutions rationnelles des équations diophantiennes telles que $y^2 = x^3 - 7$, $x^3 + y^3 + z^3 = 4$,... etc. Ce qui nous conduit à étudier la caractérisation des nombres rationnels et des nombres non-rationnels (irrationnels), telles que : l'algébricité, la transcendance et la complexité du développement.

Un nombre réel ou p-adique est dit **"algébrique"** s'il est racine d'un polynôme à coefficients rationnels (ou entiers relatifs). Ainsi $\sqrt{2}$ est algébrique de degré 2 car c'est une racine de $X^2 - 2$. Naturellement, les nombres rationnels sont algébriques ; car $\frac{a}{b}$ est racine du polynôme $bX - a$. Un nombre qui n'est pas algébrique est dit **"transcendant"**.

La façon dont les nombres algébriques irrationnels peuvent être approchés par des nombres rationnels est une question centrale en analyse diophantienne. Cette problématique est bien sûr intimement liée au développement en fraction continue des nombres algébriques irrationnels.

On sait, par exemple, que le développement en fraction continue d'un nombre réel irrationnel α est ultimement périodique si, et seulement si, α est quadratique, i.e. racine d'un polynôme de degré 2. En revanche, on ne dispose que de très peu d'informations sur la taille des quotients partiels des nombres algébriques de degré supérieur ou égal à 3. Formellement, on conjecture, par exemple que la suite formée par leurs quotients partiels n'est pas bornée. Il s'agit d'un problème important suggéré par Khintchine [38].

Plus modestement, on peut penser que si la suite des quotients partiels d'un nombre irrationnel est suffisamment "simple", alors ce dernier est soit quadratique, soit transcendant. Cette alternative séduisante se doit d'être formalisée, le terme "simple" pouvant conduire à des interprétations différentes. Il peut désigner aussi bien des nombres réels ou p-adiques dont le développement en fraction continue peut être produit par un algorithme simple (par exemple par une machine de Turing comme les automates finis), que provenant d'un système dynamique simple.

De nos jours, l'existence de nombres réels transcendants est facile à montrer. Pour chaque degré $n \geq 1$ il n'y a qu'un nombre dénombrable de polynômes de degré n à coefficients rationnels, donc un nombre dénombrable de nombres algébriques de degré fixé, et donc un nombre dénombrable de nombres algébriques. Puisque $\mathbb{R}$ n'est pas dénombrable cela prouve qu'il existe des nombres réels transcendants. Cette preuve, due à Cantor, n'a été donnée que très tardivement, à la charnière des deux siècles." Texte inspiré du papier

de Waldscmidt "Un Demi-siècle de Transcendance" [64], on trouve plus de détails sur l'histoire des nombres transcendants dans ce survol.

Ce thème a en fait une longue histoire. Le premier résultat de ce type remonte aux travaux de Liouville [42], puis son théorème d'approximation a connu des raffinements, améliorations et généralisations, qui culminent avec le théorème du sous-espace de Schmidt et sa version pour les nombres p-adiques.

Plusieurs auteurs avaient traité la caractérisation algébrique des nombres réels, en utilisant le développement en base entière (décimal, par exemple) engendré par un automate fini et/ou une fraction continue réel, voir par exemple les travaux : [1], [2], [3, [4], [5], [7], [8], [10], [28], [30], [35], [43], [51]. Cette étude conduit à l'analyse des propriétés diophantiennes : transcendance, mesures d'irrationalité, indépendance algébrique, périodicité et complexité du développement. Ces propriétés sont utiles dans des applications en théorie des nombres (approximation diophantienne), en systèmes dynamiques, en géométrie discrète, ou en informatique théorique et même en physique.

Par contre, la caractérisation des nombres p-adiques, n'a pas bien était étudié, il y avait peu d'articles qui traite les propriétés des fractions continues p-adiques, en citant : [17], [22], [25], [27], [31], [41], [49], [66].

L'analogue p-adiques des fractions continues réelles a été étudié pour la première fois par Mahler en 1934 [47] et en 1940 [46]. L'algorithme p-adique qui reproduit mieux l'algorithme classique réel en utilisant les parties entières a été mentionné dans les premiers articles sur le sujet, mais cet algorithme n'a pas été poursuivi parce qu'il ne donne pas de très bonnes approximations. Les fractions continues basées sur cet algorithme, ont été développés par Ruban [55, 1970], qui a montré que ces fractions continues fait avoir de belles propriétés ergodiques. Avant Ruban, il y avait Schneider [59, 1968] qui a laissé une trace dans ce domaine, c'est la définition qui porte son nom.

Les fractions continues p-adique de Ruban et celles de Schneider [59] sont basé sur la difficulté qu'il y a des nombres rationnels possédant des fractions continues infinies, ainsi, Schneider dans son article [59] a essayé de traiter le problème de la caractérisation des nombres rationnels en termes de leurs fractions continues p-adiques. Bundschuh [27] en 1977 avait aussi participé à la caractérisation des fractions continues p-adiques de Schneider d'un nombre rationnel, il avait démontré que suivant cette définition, le développement des rationnels est fini ou stationnaire à partir d'un certain rang. Nous avons également Laohakosol [41, 1985] qui s'est basé sur le travail de Bundschuh pour caractériser les fractions continues p-adiques de Ruban. Enfin, n'oublions pas de citer les fameux travaux de Browkin dans deux articles [25, 1978] et [26, 2000], dont il avait donné d'autres méthodes pour définir les fractions continues p-adiques, ainsi il a caractérisé le développement d'un nombre quadratique.

Trouver un analogue du théorème de Lagrange dans le cas p-adique est l'un des aspects les plus étudiés pour les fractions continues p-adiques. Généralement, il est facile de montrer qu'une fraction continue périodique représente un nombre rationnel ou un nombre irrationnel quadratique.

L'objectif de notre travail est de donner une caractérisation algébrique et arithmétique d'un nombre p-adique, en utilisant son développement de Hensel et/ou son développement en fraction continue p-adique. On va démontrer des théorèmes de transcendance et de complexité dans le cas p-adique, qui sont similaire à des théorèmes dans le cas réel.

On a réparti cette thèse sur une introduction générale, trois chapitres et deux annexes, ainsi que les notations et une liste des références.

Dans le premier chapitre, on va décrire les méthodes de construction du corps des nombres p-adiques, ainsi que l'anneau des entiers p-adiques, ensuite on définit le développement de Hensel, on donne quelques propriétés analytiques et arithmétiques du corps des nombres p-adiques telle que le fameux lemme dite de Hensel.

Dans le deuxième chapitre, on a présenté les définitions et les propriétés essentielles des automates finis et des fractions continues réelles et p-adiques, en expliquant les différents théorèmes concernant la transcendance du développement décimal et du développement de Hensel engendré par un automate fini. Les résultats de cette partie reposent la plupart sur un outil diophantien puissant : le théorème du sous-espace de Schmidt, qu'on va donner son énoncé, ainsi que sa version p-adique démontré par Schlickewei.

Dans le troisième chapitre, qui occupe une place centrale dans cette thèse, on a étudié dans la première section, la complexité du développement en fraction continue d'un nombre rationnel, autrement dit la version p-adique du théorème du Lamé connu dans le cas réel. Dans la deuxième section, on présente nos résultats principaux sur la complexité du développement de Hensel et en fraction continue d'un nombre rationnel, ainsi que la transcendance d'un nombre p-adique dont son développement en fraction continue est un mot du Thue-Morse, qui vérifie des propriétés de combinatoires.

Nous terminons cette thèse par deux annexes et quelques références sur le sujet étudier. La première annexe est sur les corps normés, la deuxième est sur le théorème de la complétion d'un corps ultramétrique non complet.

Notation

p un nombre premier, $p = 2, 3, 5, 7, ..., 2011, 2017, ...$.
$PGCD\,(a, p)$ le plus grand commun diviseur de a et p.
$\mathbb{N}$ l'ensemble des nombres naturels.
$\mathbb{Z}$ l'ensemble des nombres entiers réels.
$\mathbb{Q}$ l'ensemble des nombres rationnels.
$\mathbb{R}$ l'ensemble des nombres réels.
$\mathbb{Z}_p$ l'ensemble des entiers p-adiques.
$\mathbb{Q}_p$ l'ensemble des nombres p-adiques.
$\mathbb{Z}/n\mathbb{Z}$ l'ensemble de division de $\mathbb{Z}$ sur $n\mathbb{Z}$.
$K[X]$ l'ensemble des polynômes à coefficients dans K.
$|.|_\infty = |.|$ la valeur absolue usuel.
$|.|_p$ la valeur absolue p-adique.
$v_p(.)$ la valuation p-adique.
$[x]$ la partie entière réel de x.
$[x]_p$ la partie entière p-adique de x.
$\langle x \rangle_p$ la partie fractionnaire p-adique de x.
$\ln(.)$ le logarithme népérien (de base e).
$\mathrm{mod}\, p$ modulo un nombre p.
C_n^k coefficients binomiaux (combinaison de k parmi n).

Chapitre 1

Préliminaires sur les nombres p-adiques

Les définitions et les théorèmes de ce chapitre apparaissent dans plusieurs livres classiques sur les nombres p-adiques, comme : [12], [36],[37], [40], [53], [56].

Les corps des nombres p-adiques ont été introduits par le mathématicien allemand Kurt Hensel à la fin du $19^{ème}$ siècle (1897). Hensel a commencé avec la question suivante :

Est-il possible de définir un nombre rationnel $x \in \mathbb{Q}$ par une série de puissance de la forme

$$x = \sum_{n \geq k} \alpha_n p^n, \text{ avec } \alpha_n \in \{0, 1, ..., p-1\} \text{ et } k \in \mathbb{Z} \tag{1.1}$$

Hensel savait, par exemple, que

$$\frac{4}{3} = \sum_{n=-\infty}^{n=0} 2^{2n} \tag{1.2}$$

Il a étudié la possibilité d'élargir $x = \frac{4}{3}$ dans une série à l'égard de puissances positives de $p = 2$

$$\frac{4}{3} = \sum_{n=0}^{+\infty} \alpha_n 2^n, \text{ avec } \alpha_n = \overline{0,1} \tag{1.3}$$

Ces manipulations avec les nombres rationnels et les séries, généré l'idée qu'il existe une certaine structure algébrique similaire au système des nombres réels $\mathbb{R}$. En fait, les corps des nombres p-adiques étaient les premiers exemples de corps infinis différents de $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

La construction de nouveaux corps $\mathbb{Q}_p$ induit un intérêt vif dans la théorie des nombres et l'algèbre. Pratiquement cent années avant, les nombres p-adiques ont été intensivement

utilisé que dans les mathématiques pures, principalement dans la théorie des nombres, voir, par exemple, le livre classique de Borevich et Schafarevich [24]. En particulier, les nombres p-adiques sont utiles dans de certains problèmes théoriques dans le corps des nombres rationnels $\mathbb{Q}$.

1.1 Valuations et normes p-adiques

1.1.1 Valuations p-adiques

Définition 1.1.1 *On définit la valuation p-adique d'un entier naturel non nul a, on la note* $v_p(a)$*, par*

$$v_p(a) = \max\{r \in \mathbb{N}/\ p^r \ \textit{divise}\ a\} \tag{1.4}$$

Ainsi, on peut écrire

$$a = \xi.p^{v_p(a)}$$

avec $\xi \in \mathbb{Z}$ *et* $PGCD(\xi, p) = 1$*. Par convention on écrit* $v_p(0) = +\infty$*.*

Définition 1.1.2 *Soit un nombre rationnel* $x = \dfrac{a}{b}$*, où a et b sont des entiers réels non nul. On appelle valuation p-adique de x le nombre*

$$v_p(x) = v_p(a) - v_p(b) \tag{1.5}$$

On peut écrire dans ce cas $x = \lambda.p^{v_p(x)}$*, avec* $\lambda \in \mathbb{Q}$ *et* $PGCD(\lambda, p) = 1$*.*

Remarque 1.1.3 *L'application*

$$\begin{array}{rcl} v_p(.) & : & \mathbb{Q} \longrightarrow \mathbb{N} \\ x & \longrightarrow & v_p(x) \end{array} \tag{1.6}$$

est bien défini. En effet, si $x = \dfrac{a}{b} = \dfrac{a'}{b'}$*, on a* $v_p(x) = v_p(a) - v_p(b) = v_p(a') - v_p(b')$*.*

Proposition 1.1.4 *L'application* $v_p(.)$ *satisfait les trois conditions suivantes,* $\forall x, y \in \mathbb{Q}$ *:*
1) $v_p(x.y) = v_p(x) + v_p(y)$
2) $v_p(x + y) \geq \min(v_p(x), v_p(y))$
3) $v_p(x + y) = \min(v_p(x), v_p(y))$*, si* $v_p(x) \neq v_p(y)$

Preuve. 1) Soit $x = \frac{a}{b}.p^{v_p(x)}$, $y = \frac{c}{d}.p^{v_p(y)}$, avec a, b, c, d sont des entiers réels premiers

avec p, on a

$$\begin{aligned} v_p(x.y) &= v_p\left(p^{v_p(x)+v_p(y)}.\frac{ac}{bd}\right) \\ &= v_p(x)+v_p(y) \end{aligned}$$

puisque $PGCD(ac,p)=1$ et $PGCD(bd,p)=1$.
2) Supposons que $r=v_p(x)$ et $s=v_p(y)$, avec $s\geq r$, on a

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

vu que $PGCD(bd,p)=1$, donc

$$v_p\left(\frac{ad+p^{s-r}cb}{bd}\right)\geq 0 \tag{1.7}$$

alors $v_p(x+y)\geq r$.
3) Si $s\neq r$, on suppose que $s>r$, alors

$$v_p\left(\frac{ad+p^{s-r}cb}{bd}\right)=0 \tag{1.8}$$

d'où

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

■

1.1.2 Normes p-adiques

Définition 1.1.5 *Soit $x\in\mathbb{Q}$. On considère la fonction $|.|_p$ définie par*

$$\begin{aligned} |.|_p \quad &: \quad \mathbb{Q}\longrightarrow\mathbb{R}^+ \\ x \quad &\longmapsto \quad |x|_p=\begin{cases} p^{-v_p(x)} & , \quad x\neq 0 \\ 0 & , \quad x=0 \end{cases} \end{aligned} \tag{1.9}$$

Proposition 1.1.6 *L'application $|.|_p$ est une norme ultramétrique sur le corps $\mathbb{Q}$, appelée norme p-adique.*

Preuve. Pour la première et la deuxième propriété de la norme (**voir l'annexe1**), une petite vérification est facile.

On va démontrer l'inégalité ultramétrique, on suppose que x, y et $x+y$ ne sont pas nuls, et Supposons aussi que $|x|_p \geq |y|_p$, d'où $v_p(x) \leq v_p(y)$, donc d'après la deuxième propriété de la valuation p-adique, on a

$$|x+y|_p = p^{-v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}} = p^{-v_p(x)} = |x|_p \tag{1.10}$$

d'où

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

■

Remarque 1.1.7 *L'application $x \longmapsto |x|_p$ est une valeur absolue définie sur le corps $\mathbb{Q}$ **(voir l'annexe1)**.*

Remarque 1.1.8 *Une propriété importante de l'application $x \longmapsto |x|_p$ c'est que l'image de $\mathbb{Q}$ est un ensemble discret définie par*

$$|\mathbb{Q}|_p = \{0\} \cup \left\{\ p^k\ /\ k \in \mathbb{Z}\right\} = \left\{..., \frac{1}{p^2}, \frac{1}{p}, 0, 1, p, p^2, p^3, ...\right\} \tag{1.11}$$

Remarque 1.1.9 *On peut définir sur le corps des nombres rationnels $\mathbb{Q}$ trois types de valeurs absolues :*

1) Valeur absolue triviale :

$$|x|_t = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0 \end{cases} \tag{1.12}$$

2) Valeur absolue naturelle (ordinaire) :

$$|x| = |x|_{+\infty} = \max(x, -x) = \begin{cases} x\ , & si\ x \geq 0 \\ -x\ , & si\ x < 0 \end{cases} \tag{1.13}$$

3) Valeur absolue p-adique :

$$|x|_p = \begin{cases} p^{-v_p(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases} \tag{1.14}$$

Le théorème d'Ostrowski nous montre que ce sont les seules valeurs absolues sur $\mathbb{Q}$.

Remarque 1.1.10 *Il est connu que l'ensemble des entiers relatifs $\mathbb{Z}$ est un ensemble non borné pour la valeur absolue usuelle $|.|_{+\infty}$. Par contre, tout entier z s'écrit sous la forme $m.p^r$ où $r \in \mathbb{N}$ et $m \in \mathbb{Z}$ premier avec p, donc*

$$\forall z \in \mathbb{Z}, \ \ |z|_p = p^{-r} \leqslant 1 \tag{1.15}$$

ce qui veut dire que l'ensemble $\mathbb{Z}$ est borné pour la valeur absolue p-adique $|.|_p$.

Théorème 1.1.11 ***(Théorème d'Ostrowski)***
Toute valeur absolue non triviale $\|.\|$ sur $\mathbb{Q}$ est équivalente à la valeur absolue archimédienne (usuel) $|.|_{+\infty}$ ou à une valeur absolue p-adique $|.|_p$.

Preuve. On suppose que $\|.\|$ est une valeur absolue archimédienne, c'est-à-dire qu'il existe $k \in \mathbb{N}^*$ tel que $||k|| > 1$. Comme $||x.1|| = ||x||\,.\,||1||$ il vient que $||1|| = 1$, et d'après l'inégalité triangulaire on a

$$k = \underbrace{1+1+...+1}_{k \text{ fois}} \Longrightarrow ||k|| \leq \underbrace{\|1\|+...+\|1\|}_{k \text{ fois}} = \underbrace{1+1+...+1}_{k \text{ fois}} = k$$

et de plus, il existe $\alpha \in]0,1]$ tel que l'on ait $||k|| = k^\alpha$.

Soit $m \in \mathbb{N}$, on peut écrire m en base k sous la forme

$$m = \sum_{i=0}^{n} a_i k^i \ \ \text{avec } a_i \in \{0,1,...,k-1\} \ \text{ et } a_n \neq 0$$

de telle sorte que l'on a $m \geq k^n$. Comme $||a_i|| \leq a_i \leq k-1, \forall i = \overline{0,n}$ et $||k^i|| = ||k||^i = k^{i\alpha}$, on obtient la majoration

$$\begin{aligned} ||m|| &\leq (k-1)\sum_{i=0}^{n} k^{i\alpha} = \frac{k-1}{k^\alpha - 1}(k^{(n+1)\alpha} - 1) \\ &\leq \left(k^\alpha . \frac{k-1}{k^\alpha - 1}\right).k^{n\alpha} \leq Cm^\alpha, \end{aligned}$$

où la constante $C = k^\alpha \dfrac{(k-1)}{k^\alpha - 1}$ est indépendante de m. On peut appliquer cette inégalité à m^n, ce qui nous donne $\|m\|^n \leq Cm^{n\alpha}$, prenant la racine $n-ième$ de cette inégalité et passant à la limite, on trouve $\|m\| \leq m^\alpha$. On a donc

$$\frac{\log \|m\|}{m} \leq \frac{\log \|k\|}{k} \quad , \ \forall m \in \mathbb{N}. \tag{1.16}$$

Par symétrie, on en déduit le fait que si $\|m\| > 1$, alors cette inégalité est une égalité.

Dans le cas général, il existe $n \in \mathbb{N}$ tel que l'on ait $\|k^n m\| > 1$, ce qui montre que l'on a égalité $\forall m \in \mathbb{N}$, puis en utilisant la multiplicativité de la norme et le fait que $\|-1\| = 1$, que $\|x\| = \|x\|_{+\infty}^{\alpha}$ quel que soit $x \in \mathbb{Q}$. On a donc montré que s'il existe $k \in \mathbb{N}$ tel que $\|k\| > 1$, alors $\|.\|$ est équivalente à la norme usuelle.

Dans le cas contraire, on a $\|l\| \leq 1$ pour tout nombre premier l. Comme on a supposé $\|.\|$ non trivial, il existe au moins un nombre premier p tel que $\|p\| < 1$. S'il existe un autre q, alors d'après le théorème de Bezout, on peut trouver u_n, $v_n \in \mathbb{Z}$ telle que l'on ait $u_n p^n + v_n q^n = 1$. On obtient donc

$$\begin{aligned} 1 &= \|1\| = \|u_n p^n + v_n q^n\| \\ &\leq \|u_n\| \|p^n\| + \|v_n\| \|q^n\| \\ &\leq \|p^n\| + \|q^n\|, \end{aligned}$$

Ce qui est impossible pour n assez grand, Il existe donc un seul nombre premier p tel que $\|p\| < 1$ et $\|.\|$ est équivalente à la norme p-adique. Ce qui termine la démonstration. ■

Corollaire 1.1.12 *Deux normes $|.|_{p_1}$ et $|.|_{p_2}$ sont équivalentes si et seulement si $p_1 = p_2$.*

Preuve. Il suffit de considérer la suite $(p_1^n)_n$. Cette suite converge vers 0 pour $|.|_{p_1}$ car $|p_1^n|_{p_1} = p_1^{-n} \underset{n \to +\infty}{\longrightarrow} 0$, mais elle ne converge pas vers 0 pour $|.|_{p_2}$ si $p_1 \neq p_2$, car $|p_1^n|_{p_2} = 1 \neq 0$. ■

Le lemme suivant nous donne une façon d'approximer un nombre rationnel par un entier naturel, cette propriété sera utile dans la suite :

Lemme 1.1.13 *Soit $x \in \mathbb{Q}$ avec $|x|_p \leq 1$, alors*

$$\exists \alpha \in \{0, ..., p-1\} : |x - \alpha|_p \leq \frac{1}{p}$$

et de plus

$$\forall n \in \mathbb{N}, \exists \alpha_n \in \{0, ..., p-1\} : |x - \alpha_n|_p \leq \frac{1}{p^n}$$

Preuve. On va démontrer le résultat pour $|x|_p = 1$, puis pour $|x|_p < 1$.
i) Soit $x = \frac{a}{b} \in \mathbb{Q}$, tel que $a \in \mathbb{Z}, b \in \mathbb{Z}^*$. On suppose que $|x|_p = 1$, c-à-d que $v_p(x) = 0$, autrement dit $PGCD(a, p) = PGCD(b, p) = 1$. On a

$$PGCD(b, p) = 1 \Longrightarrow \exists \lambda_1, \lambda_2 \in \mathbb{Z} : \lambda_1 b + \lambda_2 . p = 1.$$

On en déduit que $x - a\lambda_1 = \frac{a(1-\lambda_1 b)}{b}$ et que

$$|x - a\lambda_1|_p = \left|\frac{a}{b}\right|_p . |1 - \lambda_1 b|_p \leq |1 - \lambda_1 b|_p = |\lambda_2 p|_p \leq \frac{1}{p}. \tag{1.17}$$

Par division euclidienne, on a $a\lambda_1 = kp + \alpha$, avec $\alpha \in \{0, ..., p-1\}$ et $PGCD(k, p) = 1$, alors

$$|a\lambda_1 - \alpha|_p = |kp|_p \leq \frac{1}{p}.$$

D'où

$$|x - \alpha|_p = |x - a\lambda_1 + a\lambda_1 - \alpha|_p \leq \max\left\{|x - a\lambda_1|_p, |a\lambda_1 - \alpha|_p\right\} \leq \frac{1}{p} \tag{1.18}$$

Pour démontrer la deuxième inégalité, nous avons

$$\begin{aligned} PGCD(p, b) &= 1 \Longrightarrow PGCD(p^n, b) = 1, \forall n \in \mathbb{N} \\ &\Longrightarrow \exists \mu_1, \mu_2 \in \mathbb{Z} : \mu_1 b + \mu_2 . p^n = 1. \end{aligned}$$

On fait les mêmes étapes, on trouve $\forall n \in \mathbb{N}, \exists \alpha_n = a\mu_1 - kp^n \in \{0, ..., p-1\}$ tel que $|x - \alpha_n|_p \leq \frac{1}{p^n}$.
ii) Maintenant, soit $|y|_p < 1$, c'est-à-dire que $|y|_p \leq \frac{1}{p}$. Si on met $x = p^{v_p(y)}.y$, on aura $|x|_p = 1$, et Compte tenu de ce qui précède

$$\exists \alpha \in \{0, ..., p-1\} : |x - \alpha|_p \leq \frac{1}{p} \tag{1.19}$$

donc

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

d'autre part, on a

$$|y - x|_p = \left|y - p^{v_p(y)}.y\right|_p = |y|_p . \left|1 - p^{v_p(y)}\right|_p \leq \frac{1}{p} \tag{1.20}$$

alors d'après (1.19) et (1.20) on trouve

$$|y - \alpha|_p \leq \frac{1}{p}$$

■

1.2 Construction du corps des nombres p-adiques

Dans cette section, Nous allons construire le corps des nombres p-adiques $\mathbb{Q}_p$ en utilisant la méthode topologique (analytique) basé sur le théorème de complétion. Tandis qu'il y a une autre méthode dite algébrique dont on passe par l'anneau des entiers p-adiques $\mathbb{Z}_p$ en considérant son corps des fractions. Cependant, la construction importe

peu, les deux méthodes sont équivalentes. On peut trouver les démonstrations dans les livres de : Bachman [12], Robert [53] et Schikhof [56].

On remarque que $\mathbb{Q}$ n'est pas complet pour la norme p-adique. En effet, soit pour $a \in \mathbb{Q}$ et $1 \leq a \leq p-1$ la suite de terme générale $u_n = a^{p^n}$, puisque d'après le théorème de Fermat-Euler on a $a^{p^n(p-1)} - 1 = 0 \bmod p^n$, d'où

$$|u_{n+1} - u_n|_p \leq \left|a^{p^n}\left(a^{p^n(p-1)} - 1\right)\right|_p \leq p^{-n} \tag{1.21}$$

donc

$$\begin{aligned} |u_m - u_n|_p &= |u_m - u_{m-1} + u_{m-1} - u_{m-2} + ... + u_{n+1} - u_n|_p \\ &\leq \max(|u_m - u_{m-1}|_p, ..., |u_{n+1} - u_n|_p) \leq p^{-n} \end{aligned}$$

ce qui donne

$$\lim_{n \to +\infty} |u_m - u_n|_p = 0$$

alors cette suite est de Cauchy dans $\mathbb{Q}$ muni de la norme $|.|_p$.
Supposons qu'elle converge vers $u \in \mathbb{Q}$, il vient que

$$\begin{aligned} u &= \lim_{n \to +\infty} u_n = \lim_{n \to +\infty} u_{n+1} \\ &= \lim_{n \to +\infty} (u_n)^p = u^p \end{aligned}$$

cela signifie que u est une $(p-1)$ ième racine de l'unité dans $\mathbb{Q}$, donc égale 1.
D'autre part, on a

$$\begin{aligned} |u - a|_p &= \left|u - a^{p^n} + a^{p^n} - a\right|_p \\ &\leq \max\left\{\left|u - a^{p^n}\right|_p, \left|a^{p^n} - a\right|_p\right\} = \left|a^{p^n} - a\right|_p \\ &\leq \left|a^{p^n - 1} - 1\right|_p < 1 \end{aligned}$$

donc $p^{-v_p(u-a)} < 1$, c'est-à dire $v_p(u-a) \geq 1$, alors p divise $u - a$, ce qui veut dire $u = a$. Alors, si $a \neq 1$ on aura une contradiction. Donc $u \notin \mathbb{Q}$.

Définition 1.2.1 *Le corps des nombres p-adiques $\mathbb{Q}_p$ est défini comme le complété de l'espace normé $(\mathbb{Q}, |.|_p)$ en appliquant le théorème de complétion. On prolonge la valeur absolue p-adique $|.|_p$ définie sur $\mathbb{Q}$ à tout le corps $\mathbb{Q}_p$ de la manière suivante : soit $x \in \mathbb{Q}_p$ et $(x_n)_n$ une suite de Cauchy de nombres rationnels représentant x. La suite $\left(|x_n|_p\right)_n$ est*

une suite de Cauchy dans $\mathbb{R}^+$ *car*

$$\Big||x_n|_p - |x_m|_p\Big| \leq |x_n - x_m|_p$$

donc elle converge vers une limite ℓ *dans* $\mathbb{R}^+$*. Cette limite est appelée la valeur absolue p-adique de* x*, c'est une norme non-archimédienne, et on a*

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

On peut également, étendre la valuation p-adique au $\mathbb{Q}_p$ *:* $v_p(x) = \lim_{n\to+\infty} v_p(x_n)$

Proposition 1.2.2 $\mathbb{Q}_p$ *muni de la norme* $|.|_p$ *est un corps complet ultramétrique.*

Preuve. Application du théorème de complétion (voir **l'annexe2**). ■

Définition 1.2.3 *On définit l'ensemble des entiers p-adiques, on le note* $\mathbb{Z}_p$*, comme étant le disque de l'unité de rayon* 1 *et de centre* 0*, en outre terme*

$$\mathbb{Z}_p = \Big\{x \in \mathbb{Q}_p : |x|_p \leq 1\Big\}$$

Remarque 1.2.4 *L'autre méthode algébrique pour construire les nombres p-adiques consiste a défini le corps* $\mathbb{Q}_p$ *comme l'ensemble des fractions de* $\mathbb{Z}_p$

$$\mathbb{Q}_p = \Big\{\frac{a}{b} : (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p - \{0\}\Big\} \tag{1.22}$$

Lemme 1.2.5 *Soient* $x \in \mathbb{Q}_p$*,* $k \in \mathbb{Z}$*, alors*

$$\Big\{y \in \mathbb{Q}_p : |y - x|_p \leq p^k\Big\} = x + p^{-k}.\mathbb{Z}_p$$

Preuve. Nous avons

$$\begin{aligned} x + p^{-k}.\mathbb{Z}_p &= \big\{x + p^{-k}z :\ z \in \mathbb{Z}_p\big\} \\ &= \Big\{x + u :\ |u|_p \leq p^k\Big\} \\ &= \Big\{y \in \mathbb{Q}_p : |y - x|_p \leq p^k\Big\} \end{aligned}$$

■

Définition 1.2.6 *On définit l'ensemble des nombres p-adiques inversibles, on le note par* $\mathbb{Z}_p^*$*, par*

$$\mathbb{Z}_p^* = \Big\{\alpha \in \mathbb{Z}_p : |\alpha|_p = 1\Big\}$$

La proposition suivante donne la relation entre les trois ensembles $\mathbb{Z}_p, \mathbb{Z}_p^*$ et $\mathbb{Q}_p$

Proposition 1.2.7 *On peut écrire tout nombre p-adique x d'une façon unique sous la forme*

$$x = p^n.\lambda \qquad avec \quad \lambda \in \mathbb{Z}_p^*, n \in \mathbb{Z}$$

Preuve. Si $x \in \mathbb{Z}_p$, alors $\exists\,(x_n)_n \subset \mathbb{Q}$ de Cauchy, tel que $x = \lim\limits_{n\to+\infty} x_n$. Tandis que chaque terme x_n s'écrit sous une forme unique (d'après la définition (1.1.2))

$$x_n = \xi_n.p^{v_p(x_n)}, \text{ avec } \xi_n \in \mathbb{Q} \quad \text{et} \quad v_p(\xi_n) = 0 \tag{1.23}$$

donc

$$x = \lim_{n\to+\infty} x_n = \lim_{n\to+\infty} \xi_n.p^{\lim\limits_{n\to+\infty} v_p(x_n)} = \xi.p^{v_p(x)}$$

avec

$$v_p(\xi) = \lim_{n\to+\infty} v_p(\xi_n) = 0$$

c'est-à-dire que $|\xi|_p = 1$, d'où $\xi \in \mathbb{Z}_p^*$.
Maintenant, si $x \in \mathbb{Q}_p$. Par la définition algébrique de $\mathbb{Q}_p$, x s'écrit sous la forme

$$x = \frac{a}{b} \quad , (a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p - \{0\}$$

d'autre part $a = \alpha.p^{v_p(a)}$ et $b = \beta.p^{v_p(b)}$ avec $(\alpha,\beta) \in (\mathbb{Z}_p^*)^2$. Donc

$$x = \frac{\alpha}{\beta}.p^{v_p(a)-v_p(b)} = \lambda.p^n \tag{1.24}$$

avec

$$n = v_p(a) - v_p(b) \in \mathbb{Z} \quad \text{et} \quad \lambda = \frac{\alpha}{\beta} \in \mathbb{Z}_p^*$$

Il reste à démontrer l'unicité de la représentation : Supposons que x admet deux représentations

$$\begin{cases} x = \lambda'.p^{m'} \ , \ \lambda' \in \mathbb{Z}_p^*, \ m' \in \mathbb{Z} \\ \qquad\qquad \text{et} \\ x = \lambda''.p^{m''}, \ \lambda'' \in \mathbb{Z}_p^* \ , m'' \in \mathbb{Z} \end{cases}$$

donc

$$\lambda'.\lambda''^{-1} = p^{m'-m''} \Longrightarrow v_p(\lambda'.\lambda''^{-1}) = m' - m'' \tag{1.25}$$

or que $v_p(\lambda'.\lambda''^{-1}) = 0$ (car $\lambda'.\lambda''^{-1} \in \mathbb{Z}_p^*$), ce qui implique $m' = m''$. ■

1.3 Propriétés du corps $\mathbb{Q}_p$

Nous présentons dans cette section les propriétés du corps $\mathbb{Q}_p$, à savoir, le développement de Hensel qui est une autre façon de représenter un nombre p-adique. Nous traitons aussi quelques propriétés analytiques de ce corps et nous discutons le lemme de Hensel, qui est un résultat fondamental et certainement l'un des plus importants.

1.3.1 Développement de Hensel

Définition 1.3.1 *Soit $x \in \mathbb{Z}_p$, il existe une suite de Cauchy $(x_n)_n \subset \mathbb{Z}$ qui s'appelle représentant canonique de x, et une suite $(\alpha_n)_n$ d'éléments de $\{0, 1, ..., p-1\}$, telle que : $x = \lim_{n \to +\infty} x_n$ selon la norme $|.|_p$, et*

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

Dans ce cas, on a

$$x = \lim_{n \to +\infty} \sum_{i=0}^{n} \alpha_i p^i = \sum_{n=0}^{+\infty} \alpha_n p^n \tag{1.26}$$

*La série $\sum_{n=0}^{+\infty} \alpha_n p^n$ s'appelle "**développement de Hensel**" de l'entier p-adique x, et les coefficients α_n s'appellent les chiffres p-adiques.*

Dans le théorème suivant on va démontrer l'existence de la suite $(x_n)_n$ et qu'elle vérifie certaines conditions :

Théorème 1.3.2 *Soit $x \in \mathbb{Q}_p$ avec $|x|_p \leq 1$, alors il existe une suite de Cauchy $(x_n)_n \subset \mathbb{Z}$ représente la classe d'équivalence x, telle que*

$$\begin{cases} x_n \in \{0, 1, ..., p^n - 1\} \\ \quad et \\ x_{n+1} = x_n \bmod p^{n+1} \end{cases}$$

Preuve. D'après le lemme (1.1.13)

$$\exists \alpha_0 \in \{0, 1, ..., p-1\} : |x - \alpha_0|_p \leq \frac{1}{p} < 1 \tag{1.27}$$

et comme la norme du nombre $(x-\alpha_0)$ est inférieure à $\frac{1}{p}$, alors $\left|\frac{\alpha_0-x}{p}\right|_p \leq 1$, en appliquant de nouveau le lemme (1.1.13)

$$\exists \alpha_1 \in \{0,1,...,p-1\} : \left|\frac{\alpha_0-x}{p}-\alpha_1\right|_p = \left|\frac{1}{p}\right|_p . |x-(\alpha_0+\alpha_1 p)|_p \leq \frac{1}{p}$$

donc

$$|x-(\alpha_0+\alpha_1 p)|_p \leq \frac{1}{p^2}$$

Ainsi, on obtient par récurrence une suite d'entiers relatifs $\alpha_n \in \{0,1,...,p-1\}$ telle que

$$|x-(\alpha_0+\alpha_1 p+ ..... +\alpha_n p^n)|_p \leq p^{-n} \tag{1.28}$$

on met $x_n = \alpha_0+\alpha_1 p+\alpha_2 p^2+ ..... +\alpha_n p^n$, on a donc $|x-x_n|_p \leq p^{-n}$.
Nous pouvons vérifier facilement que $(x_n)_n$ est une suite de Cauchy et qu'elle satisfait

$$\begin{cases} x_n \in \mathbb{Z}, \quad x_n \in \{0,1,...,p^n-1\} \\ \\ x_{n+1} = x_n \bmod p^{n+1} \\ \\ \lim\limits_{n\to+\infty} x_n = x \text{ (selon la norme } |.|_p) \end{cases}$$

d'où ce qu'on voulait démontrer. ■

Remarque 1.3.3 *Si $|y|_p > 1$, i.e. $\exists m \in \mathbb{Z}^+ : |y|_p = p^m$. Pour se ramener au cas $|x|_p \leq 1$, on pose $x = p^m.y$, donc $|x|_p = 1 \leq 1$. En appliquant le théorème (1.3.2) on a*

$$x = \sum_{n=0}^{+\infty} \alpha_n p^n \Longrightarrow y = p^{-m}x = \sum_{n=0}^{+\infty} \alpha_n p^{n-m} = \sum_{k=-m}^{+\infty} \alpha_{k+m} p^k$$

Cela signifie que tout nombre p-adique $a \in \mathbb{Q}_p$ admet un développement p-adique sous forme d'une série

$$a = \sum_{k=-m}^{+\infty} \beta_k p^k \quad , \quad avec \quad \beta_k \in \{0,1,2,...,p-1\}, \quad m \in \mathbb{Z}^+$$

et dans ce cas on a $m = v_p(a)$.

Remarque 1.3.4 *On peut écrir les nombres p-adiques en utilisant se qu'on appel la vir-*

gule (le point) p-adique :

$$\begin{aligned} x &\in \mathbb{Z}_p \Longrightarrow x = \sum_{n=0}^{+\infty} \alpha_n p^n = 0 \cdot \alpha_0 \alpha_1 ..... \alpha_n ..... \\ a &\in \mathbb{Q}_p \Longrightarrow a = \sum_{n=-m}^{+\infty} \beta_k p^k = \beta_{-m} \beta_{-m+1} ... \beta_{-1} \cdot \beta_0 \beta_1 ..... \beta_n ..... \end{aligned}$$

Exemple 1.3.5 *i)* $x = 0 \cdot 31104444444.... = 3.5^0 + 1.5^1 + 1.5^2 + 4.5^3 + 4.5^3 + 4.5^3 + ...$, $m = 0$, $p = 5$.
ii) $a = 1221 \cdot 21 = 1.3^{-2} + 2.3^{-1} + 2.3^{-2} + 1.3^{-1} + 2.3^0 + 1.3^1 + 0.3^2 + 0.3^3 + ...$, $m = -4$, $p = 3$.
iii) $y = \cdot 00634 = 0.7^0 + 0.7^1 + 6.7^2 + 3.7^3 + 4.7^4 + 0.7^5 + 0.7^6 + ...$, $m = 2$, $p = 7$.

Proposition 1.3.6 *Le développement de Hensel est unique.*

Preuve. Soit x un nombre p-adique développable en deux séries de Hensel

$$\begin{cases} x = \sum_{n=0}^{+\infty} \alpha_n p^n = \alpha_0 + \alpha_1 p + ... + \alpha_n p^n + ... \\ \text{et} \\ x = \sum_{n=0}^{+\infty} \alpha'_n p^n = \alpha'_0 + \alpha'_1 p + ... + \alpha'_n p^n + ... \end{cases}$$

et soit m le premier indice tel que $\alpha_m \neq \alpha'_m$, on suppose que $\alpha_m < \alpha'_m$. On a

$$1 \leq \alpha'_m - \alpha_m \leq p - 1 \tag{1.29}$$

soit

$$\begin{aligned} x_m &= \alpha_0 + \alpha_1 p + ... + \alpha_m p^m \\ x'_m &= \alpha'_0 + \alpha'_1 p + ... + \alpha'_m p^m \end{aligned}$$

alors

$$x'_m - x_m = (\alpha'_m - \alpha_m) p^m \Longrightarrow |x'_m - x_m|_p = p^{-m}$$

d'autre part on a

$$\begin{aligned} |x'_m - x_m|_p &= |x'_m - x + x - x_m|_p \\ &\leq \max \left\{ |x'_m - x|_p , |x - x_m|_p \right\} \\ &< p^{-m} \end{aligned}$$

Contradiction. ■

Remarque 1.3.7 *Le développement p-adique est analogue au développement décimal d'un nombre réel* $x = \sum_{k=-m}^{+\infty} \alpha_k 10^{-k}$, *avec* $\alpha_k \in \{0, 1, 2, ..., 10-1\} = \{0, 1, 2, ..., 9\}$.

Remarque 1.3.8 *On peut utiliser le développement de Hensel pour donner une autre définition de l'ensemble des entiers p-adiques* $\mathbb{Z}_p$ *: Ce sont les nombres p-adiques dont son développement de Hensel ne contient que les puissances positives de p, c'est-à-dire*

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p : x = \sum_{n=0}^{+\infty} \alpha_n p^n \right\} \tag{1.30}$$

Ainsi, l'autre définition de l'ensemble des nombres inversibles

$$\mathbb{Z}_p^* = \left\{ x \in \mathbb{Q}_p : x = \sum_{n=0}^{+\infty} \alpha_n p^n, \text{ tel que } \alpha_0 \neq 0 \right\}.$$

Exemple 1.3.9 *Le développement de Hensel de* $x = -1$ *est donné par*

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

on aboutit à

$$\frac{-1}{p-1} = \sum_{k=0}^{+\infty} p^k \tag{1.31}$$

donc $p-1$ *est inversible et son inverse est* $\frac{1}{p-1} = -1$.

Définition 1.3.10 *On définit la partie entière p-adique de* $x \in \mathbb{Q}_p$, *on la note par* $[x]_p$

$$[x]_p = \sum_{k=1}^{+\infty} \alpha_k p^k = \alpha_1 p + \alpha_2 p^2 + ...$$

et On définit la partie fractionnaire p-adique de $x \in \mathbb{Q}_p$, *on la note par* $\langle x \rangle_p$

$$\langle x \rangle_p = \sum_{-m \leq k \leq 0} \alpha_k p^k = \frac{\alpha_{-m}}{p^m} + \frac{\alpha_{-m+1}}{p^{m-1}} + ... + \frac{\alpha_{-1}}{p} + \alpha_0 \tag{1.32}$$

Dans ce cas nous avons $x = [x]_p + \langle x \rangle_p$.

Remarque 1.3.11 *Si* $x \in \mathbb{Z}_p$ *on a* $[x]_p = x - \alpha_0$ *et* $\langle x \rangle_p = \alpha_0$.

1.3.2 Propriétés analytiques

L'espace des nombres p-adiques est analogue a l'espace des nombres réels. Par ailleurs, le corps $\mathbb{Q}_p$ possède des propriétés plus larges que celles dans le cas réel et d'autres propriétés n'existent pas dans $\mathbb{R}$.

Le point le plus intéressant dans cette partie c'est la convergence des suites et des séries dans l'espace normé $(\mathbb{Q}_p, |.|_p)$, dont l'analogue des résultats donnés n'est pas vrai dans $\mathbb{R}$, ou bien il est vrai partiellement.

Théorème 1.3.12 *Soit* $(a_n)_n$ *une suite dans* $\mathbb{Q}_p$*, alors* $(a_n)_n$ *est de Cauchy si et seulement si*

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

Preuve. Voir **l'annexe1**. ■

Proposition 1.3.13 *Soit* $(a_n)_n$ *une suite dans* $\mathbb{Q}_p$*, si* $\lim_{n \to +\infty} a_n = a \neq 0$ *dans* $\mathbb{Q}_p$*, alors*

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

Preuve. Tant que $(a_n)_n$ est convergente, elle est donc une suite de Cauchy dans $\mathbb{Q}_p$, autrement dit

$$\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} : \forall m > n > n_0 \Longrightarrow |a_m - a_n|_p < \varepsilon \tag{1.33}$$

alors

$$\Big| |a_m|_p - |a_n|_p \Big| \leq |a_m - a_n|_p < \varepsilon$$

donc $(|a_n|_p)_n$ est de Cauchy dans $\mathbb{R}$ d'où elle est convergente dans $\mathbb{R}$, et soit ℓ sa limite. On a

$$\lim_{n \to +\infty} |a_n|_p = |a|_p = \ell$$

D'autre part $a \neq 0 \Longrightarrow |a|_p \neq 0$ i.e. $|a|_p > 0$, alors

$$\exists N_1 \in \mathbb{N}, \forall n \geq N_1 : \Big| \ |a_n|_p - \ell \Big| < \frac{\ell}{2} \Longrightarrow \frac{\ell}{2} < |a_n|_p < \frac{\ell}{2} + \ell \tag{1.34}$$

ce qui veut dire

$$\exists N_1 \in \mathbb{N}, \forall n \geq N_1 : |a_n|_p > \frac{\ell}{2}$$

Prenons $\varepsilon = \frac{\ell}{2}$, dans (1.33), on aura

$$\exists N_2 \in \mathbb{N} : \forall m, n \geq N_2 \Longrightarrow |a_m - a_n|_p < \frac{\ell}{2} < |a_n|_p \tag{1.35}$$

donc pour $N = \max(N_1, N_2)$ et $n, m \geq N_3$, on obtient

$$\begin{aligned} |a_m|_p &= |a_m - a_n + a_n|_p \\ &= \max(|a_m - a_n|_p, |a_n|_p) \\ &= |a_n|_p \end{aligned}$$

d'où ce qu'on cherche. ■

Proposition 1.3.14 *Soit* $\sum_{n\geq 0} a_n$ *une série dans* $\mathbb{Q}_p$*, alors cette série converge dans* $\mathbb{Q}_p$ *si est seulement si la suite* $(a_n)_n$ *converge vers* 0 *dans* $\mathbb{Q}_p$*, de plus on a*

$$\left|\sum_{n\geq 0} a_n\right|_p \leq \max\left\{|a_n|_p, n \in \mathbb{N}\right\} \tag{1.36}$$

Preuve. On sait que la série $\sum_{n\geq 0} a_n$ converge si et seulement si la suite de sommes partielles $S_n = a_0 + a_1 p + ... + a_n p^n$ converge. Donc, d'après les résultats précédents, il vient que

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

c'est-à-dire que $\lim_{n\to+\infty} |a_n|_p = 0$ (puisque $S_n - S_{n-1} = a_n$) d'où $(a_n)_n$ converge vers 0. Et vice versa, si $(a_n)_n$ converge vers 0 on démontre que la série $\sum_{n\geq 0} a_n$ converge.
Pour démontrer l'inégalité (1.36), nous avons d'après la propriété ultramétrique de la norme p-adique

$$\left|\sum_{k=0}^{n} a_k\right|_p \leq \max\left\{|a_k|_p, 0 \leq k \leq n\right\} \tag{1.37}$$

On obtient donc, le résultat par passage à la limite quand $n \to +\infty$. ■

Exemple 1.3.15 *La série*

$$\sum_{n\geq 0} p^n = 1 + p + p^2 + p^3 + ...$$

converge $\forall p \geq 2$ *dans* $\mathbb{Q}_p$ *vers le nombre* $\frac{1}{1-p}$*. En effet, on a*

$$\sum_{k=0}^{n} p^k = \frac{1 - p^{n+1}}{1 - p}$$

d'autre part $\lim_{n\to+\infty} p^{n+1} = 0$ *au sens de la norme p-adique, d'où*

$$\sum_{n\geq 0} p^n = \lim_{n\to+\infty} \sum_{k=0}^{n} p^k = \lim_{n\to+\infty} \frac{1-p^{n+1}}{1-p} = \frac{1}{1-p} \tag{1.38}$$

On s'inspire de cette série, pour obtenir les développements suivants

$$\begin{aligned}
\text{dans } \mathbb{Q}_3 \quad &: \quad -\frac{1}{2} = \sum_{n\geq 0} 3^n = 1 + 3 + 3^2 + 3^3 + ... \\
\text{dans } \mathbb{Q}_5 \quad &: \quad -\frac{1}{4} = \sum_{n\geq 0} 5^n = 1 + 5 + 5^2 + 5^3 + ... \\
\text{dans } \mathbb{Q}_7 \quad &: \quad -\frac{1}{6} = \sum_{n\geq 0} 7^n = 1 + 7 + 7^2 + 7^3 + ...
\end{aligned}$$

Exemple 1.3.16 *La série*

$$\sum_{n\geq 0} p^{2n} = 1 + p^2 + p^4 + p^6 + ...$$

converge dans $\mathbb{Q}_p, \forall p$ *vers le nombre* $\frac{1}{1-p^2}$. *En effet, on a*

$$\sum_{n\geq 0} p^{2n} = \sum_{n\geq 0} \left(p^2\right)^n = \frac{1}{1-p^2}$$

On peut donc calculer certains développements à l'aide de cette série, on a pour $p \geq 5$

$$\begin{aligned}
x &= 2 + 3p + p^2 + 3p^3 + p^4 + 3p^5 + p^6 + ... \\
&= 2 + 3p(1 + p^2 + p^4 + ...) + p^2(1 + p^2 + p^4 + ...) \\
&= 2 + \left(3p + p^2\right)(1 + p^2 + p^4 + ...) \\
&= 2 + \left(3p + p^2\right) \sum_{n\geq 0} p^{2n} \\
&= 2 + \frac{3p + p^2}{1 - p^2}
\end{aligned}$$

Par exemple

$$\begin{aligned}
\text{dans } \mathbb{Q}_5 \quad &: \quad \frac{1}{3} = 2 + 3.5 + 5^2 + 3.5^3 + 5^4 + 3.5^5 + ... \\
\text{dans } \mathbb{Q}_7 \quad &: \quad \frac{13}{24} = 2 + 3.7 + 7^2 + 3.7^3 + 7^4 + 3.7^5 + ...
\end{aligned} \tag{1.39}$$

Remarque 1.3.17 *Les définitions et les propriétés des fonctions sur* $\mathbb{R}$ *restent vrais sur* $\mathbb{Q}_p$*, ainsi les polynômes sont continues et dérivables sur* $\mathbb{Q}_p$*.*

1.3.3 Lemme de Hensel

Nous donnons ici un résultat important due à Hensel, permet de caractériser un type des nombres p-adiques algébriques, ce sont les racines des équations polynômiales dans $\mathbb{Q}_p$, comme ceux qui sont racines de l'unité.

La proposition suivante (Pour les polynômes à coefficients entiers) est utile pour la démonstration du lemme de Hensel, cette proposition est une dérivée de la méthode de Newton en analyse numérique :

Proposition 1.3.18 *Soit* $F(x) \in \mathbb{Z}[x]$ *,et* $a_0 \in \mathbb{Z}$ *une racine de* $F(x)$ *modulo* p*, i.e.* $F(a_0) = 0 \bmod p$ *et supposons que* $F'(a_0)$ *admet un inverse modulo* p*, i.e.*

$$\exists u \in \mathbb{Z} \ \left(u = F'^{-1}(a_0)\right) : uF(a_0) = 1 \bmod p$$

Donc la suite définie par

$$a_{n+1} = a_n - F'^{-1}(a_0)F(a_n)$$

est de Cauchy au sens de la norme $|.|_p$ *, et elle converge vers une racine de* $F(x)$ *dans* $\mathbb{Q}_p$*.*

Maintenant, voila l'énoncé du lemme de Hensel :

Théorème 1.3.19 (Lemme de Hensel) *Soient* $F \in \mathbb{Z}_p[x]$ *, i.e.*

$$F(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n, \quad \textit{tel que } \alpha_i \in \mathbb{Z}_p, \forall i \in \mathbb{N}$$

et $a \in \mathbb{Z}_p$ *tels que*

$$F(a) = 0 \bmod p \quad \textit{i.e.} \quad |F(a)|_p \leq p^{-1} \tag{1.40}$$

Si on a

$$F'(a) \neq 0 \bmod p \quad \textit{i.e.} \quad |F'(a)|_p = 1 \tag{1.41}$$

Alors il existe un entier p-adique unique $b = a - \frac{F(a)}{F'(a)}$ *tels que :*

$$b = a \bmod p \quad \textit{et} \quad F(b) = 0$$

Preuve. Nous avons d'après (1.40)

$$|F(a)|_p \leq p^{-1} \Longrightarrow |F(a)|_p < 1$$

On a aussi $a \in \mathbb{Z}_p$, donc d'après la définition du développement du Hensel, on peut trouver une suite de Cauchy $(a_m)_{m\in\mathbb{N}}$ dans $\mathbb{Z}$ converge vers a. Et de plus

$$|a_m - a|_p < \frac{1}{p^m} \quad ; \forall m \in \mathbb{N} \tag{1.42}$$

Soit par exemple $m = 0$ on a $|a_0 - a|_p < 1$. On va montrer que

$$F(a_0) = 0 \bmod p \quad \text{et} \quad F'(a_0) = 1 \bmod p$$

En effet

$$\begin{aligned} |F(a_0)|_p &= |F(a_0) - F(a) + F(a)|_p \\ &\leq \max\left\{|F(a_0) - F(a)|_p ; |F(a)|_p\right\} \end{aligned}$$

donc

$$\begin{aligned} F(a_0) - F(a) &= \alpha_1 (a_0 - a) + \alpha_2 \left(a_0^2 - a^2\right) + ... + \alpha_n \left(a_0^n - a^n\right) \\ &= (a_0 - a) \underbrace{[\alpha_1 + \alpha_2 (a_0 - a) + ...]}_{B\in\mathbb{Z}_p} = (a_0 - a) .B \end{aligned}$$

alors

$$|F(a_0) - F(a)|_p = |a_0 - a|_p |B|_p < |B|_p < 1 \tag{1.43}$$

c'est à dire que $|F(a_0)|_p < 1$.
D'autre part

$$\begin{aligned} |F'(a_0)|_p &= |F'(a_0) - F'(a) + F'(a)|_p \\ &\leq \max\left\{|F'(a_0) - F'(a)|_p ; |F'(a)|_p\right\} \end{aligned}$$

de la même façon, F' s'écrit

$$F'(x) = \alpha_1 + 2\alpha_2 x + ... + n\alpha_n x^{n-1} \tag{1.44}$$

donc

$$\begin{aligned} F'(a_0) - F'(a) &= 2\alpha_2 (a_0 - a) + 3\alpha_3 \left(a_0^2 - a^2\right) + ... + n\alpha_n \left(a_0^{n-1} - a^{n-1}\right) \\ &= (a_0 - a) \underbrace{\left[2\alpha_2 + 3\alpha_3 (a_0 - a) + ...\right]}_{C \in \mathbb{Z}_p} = (a_0 - a) .C \end{aligned}$$

il vient que

$$|F'(a_0) - F'(a)|_p = |a_0 - a|_p |C|_p < 1 = |F'(a)|_p$$

d'où

$$|F'(a_0)|_p = \max \left\{ |F'(a_0) - F'(a)|_p ; |F'(a)|_p \right\} = 1$$

Les conditions de la proposition précédente sont vérifiées. Alors la suite définie par

$$a_{(n+1)0} = a_{(n)0} - F'^{-1}(a_0) F(a_{(n)0}) \tag{1.45}$$

est de Cauchy, et sa limite est une racine du polynôme F dans $\mathbb{Q}_p$. On refait cette procédure pour a_1, on va trouver une suite

$$a_{(n+1)1} = a_{(n)1} - F'^{-1}(a_1) F(a_{(n)1})$$

On continue le processus jusqu'à l'ordre m, on trouvera encore une suite de Cauchy définit par

$$a_{(n+1)m} = a_{(n)m} - F'^{-1}(a_m) F(a_{(n)m}) \tag{1.46}$$

Donc pour $n = 0$

$$a_{(0)m} \underset{m \to +\infty}{\to} a$$

et pour $n = 1$

$$a_{(1)m} \underset{m \to +\infty}{\to} a_1$$

D'autre part, on a

$$a_{(1)m} = a_{(0)m} - F'^{-1}(a_m) F(a_{(0)m})$$

En passe a la limite quand $m \to +\infty$ on aboutit à

$$a_1 = a - F'^{-1}(a) F(a)$$

Pour $n = 2$, on a

$$a_{(2)m} \underset{m \to +\infty}{\to} a_2$$

et

$$a_2 = a_1 - F'^{-1}(a)F(a_1)$$

De cette manière on a défini une suite $(a_n)_n$ telle que

$$\begin{aligned} a_{(0)0}\ a_{(0)1}a_{(0)2}...a_{(0)m} \underset{m\to+\infty}{\to} a_0 &= a \\ a_{(1)0}\ a_{(1)1}a_{(1)2}...a_{(1)m} \underset{m\to+\infty}{\to} a_1 &= a - F'^{-1}(a)F(a) \\ a_{(2)0}\ a_{(2)1}a_{(2)2}...a_{(2)m} \underset{m\to+\infty}{\to} a_2 &= a_1 - F'^{-1}(a)F(a_1) \\ &..... \\ a_{(n)0}\ a_{(n)1}a_{(n)2}...a_{(n)m} \underset{m\to+\infty}{\to} a_{n+1} &= a_n - F'^{-1}(a)F(a_n) \end{aligned} \tag{1.47}$$

donc

$$a_{n+1} = a_n - F'^{-1}(a)F(a_n) \quad \forall n \in \mathbb{N}$$

de la même façon qu'on a fait pour $(a_{0m})_{m\in\mathbb{N}}$, on montre que la suite $(a_{nm})_{m\in\mathbb{N}}$ est de Cauchy $\forall n \in \mathbb{N}$, donc elle converge vers un nombre dans $\mathbb{Z}_p$ c'est à dire que $a_n \in \mathbb{Z}_p$,$\forall n \in \mathbb{N}$.
Maintenant ; en montre l'inégalité suivante

$$|F(a_n)|_p < \frac{1}{p^n} \quad , \forall n \in \mathbb{N}. \tag{1.48}$$

En effet, on remarque que

$$F(a_{nm}) = 0 \bmod p^n \quad , \forall n, m \in \mathbb{N}. \tag{1.49}$$

tel que $(a_{nm})_{m\in\mathbb{N}}$ est une suite de Cauchy définit dans (1.46), elle converge vers a_n quand $m \to +\infty$, d'où

$$|F(a_n)|_p = \lim_{m\to+\infty} |F(a_{nm})|_p < \frac{1}{p^n}.$$

Donc, d'après la proposition précédente la suite $(a_{nm})_{n\in\mathbb{N}}$ tend vers une racine b_m de F dans $\mathbb{Q}_p$; i.e.

$$F\left(\lim_{n\to+\infty} a_{nm}\right) = 0$$

Passons à la limite quand $m \to +\infty$ on obtient (F est un polynôme, donc continue sur

$\mathbb{Z}_p$)

$$\begin{aligned} F\left(\lim_{n\to+\infty} a_n\right) &= F\left(\lim_{n\to+\infty}\left(\lim_{m\to+\infty} a_{nm}\right)\right) \\ &= \lim_{m\to+\infty}\left[F\left(\lim_{n\to+\infty} a_{nm}\right)\right] = 0 \end{aligned}$$

c'est-à-dire

$$F(b) = 0$$

D'où ce qu'on voulait démontrer. ■

On donne maintenant deux applications du lemme de Hensel pour caractériser un type des nombres algébriques. Ce sont les racines $n^{ème}$ de l'unité, appelé souvent représentant de Taichmüller, et les racines carrés d'un nombre p-adique :

Représentant de Taichmüller

Considérons le polynôme $F(x) = X^{p-1} - 1$, on a

$$\forall s = \overline{1, p-1} : \ F(s) = 0 \bmod p$$

et

$$F'(s) = 1 \bmod p$$

En effet, nous avons

$$\begin{aligned} 1 &\leq s \leq p-1 \Rightarrow |s|_p = |1|_p = 1 \\ &\Rightarrow |s|_p^{p-1} = |1|_p = 1 \end{aligned}$$

donc

$$\begin{aligned} \left|s^{p-1} - 1\right|_p &< \max(\left|s^{p-1}\right|_p, |1|_p) \\ &= \max(|s|_p^{p-1}, |1|_p) = 1 \end{aligned}$$

ce qui implque

$$\left|s^{p-1} - 1\right|_p < 1 \Rightarrow \left|s^{p-1} - 1\right|_p \leq \frac{1}{p}$$

puisque

$$\forall \alpha \in \mathbb{Q}_p; |\alpha|_p \in \{p^m, m \in \mathbb{Z}\} \cup \{0\}.$$

D'autre part

$$F'(x) = (p-1)X^{p-2} - 1 \tag{1.50}$$

d'où

$$\begin{aligned} |F'(s)|_p &= \left|(p-1)s^{p-2} - 1\right|_p = \left|ps^{p-2} - s^{p-2} - 1\right|_p \\ &\leq \max(|p|_p \left|s^{p-2}\right|_p, \left|s^{p-2}\right|_p, |1|_p) \\ &= \max(\frac{1}{p}, 1) = 1 \end{aligned}$$

tandis que

$$\left|s^{p-2}\right|_p = |1|_p = 1 > \frac{1}{p} = |p|_p |s|_p$$

donc $F'(s) = 1 \bmod p$.

En appliquant le lemme de Hensel pour les nombres $s = 1, ..., p-1$, on trouve $p-1$ racines de F dans $\mathbb{Z}_p$, on les note $w_1, ..., w_{p-1}$, telles que : $F(w_s) = 0 \quad$ et $\quad w_s = s \bmod p$.

Nous avons, évidement, $w_1 = 1$, et on pose aussi $w_0 = 0$; donc on peut caractériser les représentant de Taichmüller ainsi :

Proposition 1.3.20 *Il existe une unique famille*

$$(w_i)_{i=\overline{0,p-1}} \in (\mathbb{Z}_p)^p$$

appelée ***" famille des représentants de Teichmüller"*** *tel que pour tout* $s \in \{1, ..., p-1\}$

$$w_s = s \bmod p \quad et \quad w_s^p = w_s. \tag{1.51}$$

Par ailleurs ; on a $w_0 = 0$ *et* $w_1 = 1$.

Les racines carrées dans $\mathbb{Q}_p$

Proposition 1.3.21 *Soit* $a = \lambda.p^{v_p(a)} \in \mathbb{Q}_p^*$ *, avec* $\lambda = a_0 + a_1 p + a_2 p^2 + ... \in \mathbb{Z}_p^*$. *Alors a admet une racine carrée si et seulement si les deux conditions suivantes soient vérifiées*

$$\begin{cases} i)\ v_p(a)\ \textit{est pair} \\ \quad\ \textit{et} \\ ii)\ \begin{cases} \textit{Si } p = 2 :\ v_2(\lambda) \geq 3\ \textit{(i.e. } \lambda = 1 \bmod 8\textit{)} \\ \textit{Si } p > 2 :\ a_0 \in \mathbb{Z}\ \textit{admet une racine carrée dans } \mathbb{Q}_p. \end{cases} \end{cases}$$

Preuve. Soit $a = \lambda.p^{v_p(a)} \in \mathbb{Q}_p^*$, $\lambda \in \mathbb{Z}_p^*$. Il s'écrit sous la forme

$$a = p^{v_p(a)}(a_0 + a_1 p + a_2 p^2 + ...) = p^{v_p(a)}.\lambda \quad , \text{ avec } a_0 \neq 0 \ , \ \lambda \in \mathbb{Z}_p^* \tag{1.52}$$

Supposons que a est un carré dans $\mathbb{Q}_p^*$, il existe donc

$$x = p^{v_p(x)}(x_0 + x_1 p + x_2 p^2 + ...) = p^{v_p(x)}.\mu \in \mathbb{Q}_p^* \quad , \text{avec } x_0 \neq 0 \ , \ \mu \in \mathbb{Z}_p^*$$

tel que $x^2 = a$, d'où

$$p^{2v_p(x)}\mu^2 = p^{v_p(a)}\lambda \Longleftrightarrow v_p(a) = 2v_p(x) \ \text{ et } \ \mu^2 = \lambda$$

donc $v_p(a)$ est un nombre pair.
Pour démontrer ii) on distingue les deux cas suivant :
1) Si $p = 2$, on a $x_0 \neq 0$ et $a_0 \neq 0$, donc $x_0 = a_0 = 1$. D'autre part $x_1^2 - a_1 = 0 \bmod p$, on obtient

$$\begin{aligned} \mu^2 &= (1 + x_1 2 + x_2 2^2 + ...)^2 \\ &= 1 + x_1 2^2 + x_1^2 2^2 + x_2 2^3 + ... \\ &= 1 + (\frac{x_1 + x_1^2}{2} + x_2)2^3 + ... \end{aligned}$$

Or que

$$\frac{x_1 + x_1^2}{2} + x_2 \in \{0, 1\}$$

pour $x_1, x_2 \in \{0, 1\}$, donc

$$\mu^2 = \lambda \Longleftrightarrow 1 + \left(\frac{x_1 + x_1^2}{2} + x_2\right) 2^3 + ... = 1 + a_1 2 + a_2 2^2 + ... \tag{1.53}$$

Ce qui donne $a_1 = a_2 = 0$, d'où

$$\begin{aligned} \lambda &= 1 + a_3 2^3 + a_4 2^4 + ... \\ &= 1 + 2^3.(a_3 + a_4 2^4 + ...) \end{aligned}$$

Alors $\lambda = 1 \bmod 8$.
2) Si $p > 2$, alors $x_0^2 - a_0 = 0 \bmod p$. On applique le lemme de Hensel sur le polynôme

$F(y) = y^2 - a_0$, tels que

$$\begin{cases} F(\mu) = \lambda - a_0 = 0 \bmod p \\ \\ \text{et} \\ \\ F'(\mu) = 2x_0 \quad , \quad |F'(x_0)|_p = |2x_0|_p = 1 \end{cases}$$

donc il existe un entier p-adique unique b tels que $F(b) = b^2 - a_0 = 0$, ce qui veut dire que a_0 admet une racine carrée dans $\mathbb{Q}_p$. ■

Remarque 1.3.22 *D'après cette proposition le nombre p-adique $x = \sqrt{a}$ est algébrique de degré 2, i.e. quadratique.*

Exemple 1.3.23 *Comme nous avons $-1 \neq 1 \bmod 8$ donc le nombre 2-adique $y = -1$ n'a pas de racine carrée dans $\mathbb{Q}_2$.*

Exemple 1.3.24 *Dans $\mathbb{Q}_5$ le nombre $a = 7$ n'admet pas une racine carrée. En effet, soit*

$$x = x_0 + x_1.5 + ... + x_n.5^n + ... \in \mathbb{Q}_5$$

on a

$$x^2 = a \Longrightarrow (x_0 + x_1.5 + ... + x_n.5^n + ...)^2 = 7 = 2 + 1.3$$

donc

$$x_0^2 = 2 \bmod 5 \quad \textit{avec } x_0 \in \{0, 1, 2, 3, 4\}$$

alors x_0 n'existe pas. C'est-à-dire que l'équation $x^2 = a$ n'a pas de solution x.

Chapitre 2

Automates finis et fractions continues

2.1 Automates finis

Les automates finis constituent l'un des modèles de calcul les plus basiques. Ils forment toutefois une classe remarquable de machines de Turing, qui est un modèle abstrait (algorithmique) du fonctionnement des appareils mécaniques de calcul, tel un ordinateur et sa mémoire. Un autre aspect important de l'utilisation des automates finis en théorie des nombres vient du fait qu'ils peuvent être utilisés comme des machines permettant de reconnaître des ensembles de nombres intéressants. Nous rappelons dans cette partie quelques définitions relatifs à cette notion.

Intuitivement, une suite $a = (a_n)_n \geq 0$ est dite k-automatique si a_n est une fonction assez simple de l'écriture de l'entier n en base k (fonction à états finis). Cela signifie qu'il existe un automate fini qui, lorsqu'on lui donne en entrée l'écriture en base k de l'entier n, produit en sortie le symbole a_n. Ces suites ont une structure très riche et jouissent de nombreuses propriétés. L'ouvrage d'Allouche et Shallit [11] est une excellente référence sur ce sujet, et les définitions et les théorèmes de cette section apparaissent, la plus part, dans ce livre.

2.1.1 Définitions et propriétés

Définition 2.1.1 • *On appelle* ***alphabet*** *tout ensemble fini, on le note* $\mathbf{A}$*. un élément* w *de l'alphabet est appelé* ***lettre****.*

• *Un* ***mot*** W *est la concaténation des lettres de* $\mathbf{A}$*, on écrit*

$$W = w_1 w_2 w_3 ... w_n \quad avec\ w_i \in \mathbf{A}, \forall i = \overline{1, n}$$

• *La* ***longueur*** *de* W *est le nombre des lettres que contient* W*, on le note* $|W|$*. D'où on aura*

$$|W| = |w_1 w_2 w_3 ... w_n| = n$$

• *Le* ***miroir*** *de* W *est le mot* $\overline{W}$ *défini par* $\overline{W} = x_n ... x_2 x_1$*. D'où on a* $|W| = \left|\overline{W}\right| = n$*.*
Par exemple : $W = 2015$ *donc* $\overline{W} = 5102$*. Notons que* $\overline{WX} = \overline{X}\,\overline{W}$*.*
• *On dit que le mot* W *est un* ***palindrome*** *si* $W = \overline{W}$*.*
Par exemple : $W =$ *sos ,* $W =$ *le sel on a* $\overline{W} = W$*.*
• *On dit que le mot* W *est un* ***quasi-palindrome*** *s'il est de la forme* $W = XYZ\overline{Y}\,\overline{X}$ *où* X, Y, Z *sont des mots, dans ce cas on a* $\overline{W} = XY\overline{Z}\,\overline{Y}\,\overline{X}$*.*
Par exemple : $W = 1034214301$*, on a* $\overline{W} = 1034124301$*.*
• *On note par* $|W|_w$ *le nombre d'occurrences de la lettre* w *dans le mot* W*.*
Par exemple

$$|W|_1 = |110010001|_1 = 4$$

• *Un* ***carré*** *est un mot du type* $\mathbf{X} = WW = W^2$*.*
Par exemple : $W =$ *aab et* $\mathbf{X} =$*aabaab.*
• *Le* ***mot vide*** ε *est le mot de longueur zéro.*
• *On définit les ensembles suivants :*

$$\begin{cases} \mathbf{A}^n = \{W \in A/ \quad |W| = n\}, \\ \mathbf{A}^0 = \{\varepsilon\}, \ \textit{par convention}, \\ \mathbf{A}^+ = \bigcup\limits_{n>0} \mathbf{A}^n, \\ \mathbf{A}^* = \bigcup\limits_{n\geq 0} \mathbf{A}^n = \mathbf{A}^+ \bigcup \mathbf{A}^0. \end{cases}$$

• *On appelle* ***langage*** *sur un alphabet* $\mathbf{A}$ *tout sous ensemble de* $\mathbf{A}^*$*, on le note* $\mathbf{L}$*.*

Exemple 2.1.2 *Soit l'alphabet* $\mathbf{A} = \{a, b, c\}$*, le mot* $W = ab$ *est de longueur* 2*, i.e* $|W| = 2$*. Pour le mot* $y = cbb$ *on a*

$$|y| = 3 \quad et \quad |y|_b = 2$$

On peut définir un langage sur cet alphabet par

$$L = \{\ W \in \mathbf{A}^*/ \quad |W| = 10 \ et \ |W|_a = 5\ \}.$$

c'est-à-dire l'ensemble des mots de longueur 10 *tel que la lettre* a *apparaît* 5 *fois.*

Exemple 2.1.3 *Soit l'alphabet* $\mathbf{A} = \{0, 1\}$*. Le mot* $W = 0101101110$ *est de longueur* 10*,*

i.e $|W| = 10$, *et de plus* $|W|_0 = 4$. *Voici un langage défini sur cet alphabet*

$$L = \{W \in \mathbf{A}^* / \ |W| \leq 25\}.$$

Donnons à présent une définition plus formelle de la notion d'automate fini :

Définition 2.1.4 *Un* ***automate fini*** *est un* 5*-uplet (quintuplet)* $\mathcal{F} = (\mathbf{A}, Q, E, G, \delta)$ *telle que :*
$\mathbf{A}$ *est un alphabet.*
Q *est un ensemble fini, appelé ensemble des états de l'automate.*
$E \subset Q$ *l'ensemble des états initiaux de l'automate.*
$G \subset Q$ *l'ensemble des états finaux (terminaux, acceptants) de l'automate.*
$\delta : Q \times \mathbf{A} \to Q$ *une application de transition.*
On dit aussi que $\mathcal{F}$ *est un* k*-automate fini.*

Définition 2.1.5 *On dit qu'un mot* W *est reconnu par un automate fini* $\mathcal{F}$ *s'il y a une suite de transitions* $(q_0, q_1, ..., q_n)$*, partant d'un état initial aboutissant à un état final, et dont la suite des étiquettes est* W*.*

Définition 2.1.6 *Le langage reconnu par l'automate* $\mathcal{F}$ *est l'ensemble de tous les mots reconnus par cet automate, on le note* $L(\mathcal{F})$*.*

Exemple 2.1.7 *Soit l'automate fini* $\mathcal{F}$= $(\mathbf{A}, Q, E, G, \delta)$*, où*

$$\mathbf{A} = \{a, b\}, \quad Q = \{q_0, q_1, q_2\}, \quad E = \{q_0\}, \quad G = \{q_2\}.$$

$\delta : Q \times \{a, b\} \to Q$ *l'application de transition définie par :*

$$\begin{aligned} \delta(q_0, a) &= q_1 \quad , \quad \delta(q_0, b) = q_0 \\ \delta(q_1, a) &= q_1 \quad , \quad \delta(q_1, b) = q_2 \\ \delta(q_2, a) &= q_1 \quad , \quad \delta(q_2, b) = q_0 \end{aligned}$$

Les mots suivants sont reconnaissables par cet automate : $x = aab$, $y = aaab$, $z = aabaaab$.
Il y a une autre représentation de cet automate, c'est la représentation graphique :

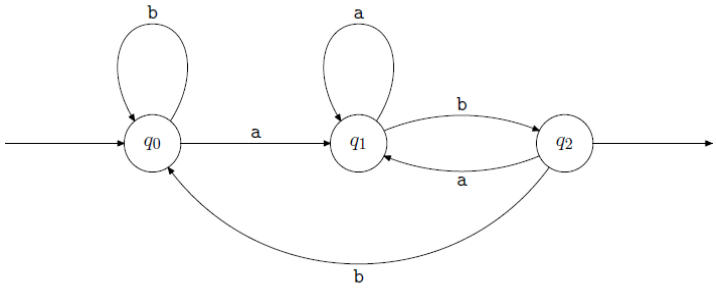

Fig.1. Automate fini à trois états.

Définition 2.1.8 *Un automate fini* $\mathcal{F}= (\mathbf{A}, Q, E, G, \delta)$ *est dit* ***déterministe (AFD),*** *s'il admet un seul état initial, et à partir de chaque état il y a au plus une transition ; autrement dit :*

- $cardE = 1$.
- $card\{q' \in Q/\ \delta(q, w) = q'\} \leq 1\ ,\ \forall q \in Q\ ,\ \forall w \in \mathbf{A}$.

Dans le cas contraire on dit automate ***non déterministe (AFND).***

Théorème 2.1.9 *Tout automate non déterministe peut être transformé en un automate déterministe (AFD).*

Remarque 2.1.10 *Dans les applications en théorie des nombres, on utilise que les automates finis déterministes pour assurer l'unicité des mots engendrés.*

2.1.2 Nombres et suites automatiques

Une suite $(a_n)_{n\geq 0}$ à valeurs dans un alphabet fini d'entiers naturels $\{0, 1, 2, ..., k-1\}$, peut être considérée comme le développement en base k d'un nombre réel ou d'un nombre p-adique si k est premier ; on peut également lui associer le nombre dont le développement en fraction continue est donné par la suite $(1 + a_n)_{n\geq 0}$, et dans tous les cas, étudier, par des méthodes d'approximation, la nature algébrique de ce nombre en relation avec la nature combinatoire de la suite initiale.

Si l'on se donne une suite de 0 et de 1, on peut lui associer aisément un nombre réel en mettant une virgule, disons après le premier terme, et en considérant le nombre réel dont cette expression est le développement en base 2. Par exemple, en partant de la suite de Thue-Morse

$$0110100110010110100101 10\ldots$$

on obtient le nombre (écrit en base 2)

$$0,11010011001011010010110\ldots$$

On peut démontrer que ce nombre est transcendant.

Plus généralement, il se produit le phénomène suivant : si on prend une suite engendrée par un automate comme ci-dessus, ou bien cette suite est ultimement périodique, c'est-à-dire périodique à partir d'un certain rang, et le nombre (réel ou p-adique) associé est rationnel, ou bien elle n'est pas ultimement périodique et ce nombre est transcendant. Ceci est un résultat dû à Loxton et van der Poorten [43], dont la preuve proposée repose sur une méthode introduite par Mahler, voir [15] et [64]. On peut aussi énoncer la contraposée du résultat de Loxton et van der Poorten : les chiffres d'un nombre algébrique irrationnel ne peuvent pas être engendrés par un automate fini. Comme le nombre $\sqrt{2}$:

Chiffres Décimales

$$\begin{aligned}\sqrt{2} \;=\; & 1.41421356237309504880168872420969807856967187537694807317667973\\ & 79907324784621070388503875343276415727350138462309122970249248 3\\ & 60558507372126441214970999358314132226659275055927557999505011 5\\ & 27820605714701095599716059702745345968620147285174186408891986 0\end{aligned}$$

Chiffres binaires

$$\begin{aligned}\sqrt{2} \;=\; & 1.01101010000010011110011001100111111100111011110011001001000 0\\ & 10001011001011111011000100110110011011101010100101010111110100\\ & 11111000111010110111101100000101110101000100100111011101010000\\ & 10011001110110100010111101011001000010110000011001100111001100\end{aligned}$$

Définition 2.1.11 *Soient $k \in \mathbb{N}^* - \{1\}$ et $(a_n)_{n\geq 0}$ une suite à valeurs dans $\mathbf{A} = \{0, 1, 2, ..., k-1\}$. On dit que la suite $(a_n)_{n\geq 0}$ est k-automatique ; s'il existe un automate fini $\mathcal{F} = (\mathbf{A}, Q, E, G, \delta)$ et une application*

$$\varphi : Q \to \{0, 1, 2, ..., k-1\}$$

telle que $\varphi(q) = a_n$ où q est l'état atteint par l'automate pour l'entrée n en base k. Autrement dit, une suite est k-automatique si son n-ième terme, $\forall n \in \mathbb{N}$, est engendré par une machine à états finis, lisant en entrée le développement de n en base k.

Définition 2.1.12 *On identifie la suite $(a_n)_{n\geq 0}$ d'éléments de $\mathbf{A}$ avec le mot infini $a_0a_1...a_n...$ dans $\mathbf{A}^*$.*

Exemple 2.1.13 *Soit la suite* $(a_n)_{n\geq 0}$ *définie par :*

$$a_n = \begin{cases} 1 & si\ n = 0\,[3]\,. \\ 0 & sinon. \end{cases}$$

Et soit l'automate fini $\mathcal{F}= (\mathbf{A}, Q, E, G, \delta)$*, donné par :*
l'alphabet $\mathbf{A} = \{0, 1, 2\}$*, les ensembles des états*

$$Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6\}\,, E = \{q_0\}\,, G = \{q_1, q_3, q_4, q_6\}\,,$$

l'application de transitions :

$$\begin{aligned} \delta(q_0, 0) &= q_1, \delta(q_0, 1) = q_4, \delta(q_0, 2) = q_4 \\ \delta(q_i, j) &= q_{i+1} \quad ,\ i = 1, 4 \quad ,\ j = 0, 1, 2 \\ \delta(q_i, 0) &= q_i, \delta(q_i, j) = q_{i+1} \quad ,\ i = 2, 5 \quad ,\ j = 1, 2 \\ \delta(q_i, 0) &= q_{i-1}, \delta(q_i, j) = q_i \quad ,\ i = 3, 6 \quad ,\ j = 1, 2 \end{aligned}$$

On donne aussi, une application $\varphi : Q \to \{0, 1, 2\}$ *définie par*

$$\begin{aligned} \varphi(q_i) &= 1,\ i = 1, 3 \\ \varphi(q_i) &= 0,\ i = 4, 6 \end{aligned}$$

Il est clair que, si $n = 0\,[3]$ *alors son écriture en base* 3 *commence par* 0*, donc l'automate atteint les états* q_1 *et* q_3 *pour l'entrée* n *en base* 3*, d'où*

$$a_n = \varphi(q_i) = 1 \quad ,\ i = 1, 3.$$

Dans l'autre cas, l'écriture en base 3 *de* n *commence par* 1 *ou* 2*, ainsi que l'automate atteint les états* q_4 *et* q_6 *; d'où*

$$a_n = \varphi(q_i) = 0 \quad ,\ i = 4, 6.$$

Nous avons démontré que la suite $(a_n)_{n\geq 0}$ *est* 3*-automatique.*

La suite de Thue–Morse, également appelée suite de Prouhet-Thue-Morse, est probablement l'exemple le plus célèbre de suite automatique. Cette suite a été utilisée pour la première fois de façon implicite par le mathématicien français Eugène Prouhet en 1851, pour donner une solution à un problème de théorie des nombres appelé depuis le problème de Prouhet-Tarry-Escott. Le mathématicien norvégien Axel Thue l'a découverte et

l'utilisée dans l'article [63] publié en 1912 qui, avec un autre article datant de 1906, est l'article fondateur de la combinatoire des mots. La suite a été redécouverte par Marston Morse en 1921. Morse l'a utilisée dans son article [48] pour donner un exemple d'une suite récurrente non périodique.

Il y a plusieurs manières équivalentes de définir la suite de Thue-Morse, on donne ici deux définitions :

Définition 2.1.14 *Soit la suite* $(t_n)_{n\geq 0}$ *définie par*

$$t_n = \begin{cases} 0 & \text{si le nombre des } 1 \text{ dans l'écriture binaire de } n \text{ est paire.} \\ 1 & \text{sinon.} \end{cases}$$

cette suite est 2*-automatique.*
En effet, il existe un automate fini définie par l'alphabet $\mathbf{A} = \{0, 1\}$*, l'ensembles des états* $Q = \{q_0, q_1\}$*,* $E = \{q_0\}$ *,* $G = \{q_1\}$*, l'application de transitions :* $\delta(q_0, 0) = q_0$ *,* $\delta(q_0, 1) = q_1$ *,* $\delta(q_1, 0) = q_1$ *,* $\delta(q_1, 1) = q_0$*, et une application* $\varphi : Q \to \{0, 1\}$ *définie par* $\varphi(q_0) = 0$ *,* $\varphi(q_1) = 1$*, tels que :*
Si le nombre des 1 *dans l'écriture binaire de* n *est paire on a* $t_n = \varphi(q_0) = 0$ *; et si le nombre des* 1 *dans l'écriture binaire de* n *est impaire on a* $t_n = \varphi(q_1) = 1$ *.*
La suite $(t_n)_{n\geq 0}$ *est appelé* ***suite de Thue-Morse****, de sorte qu'elle calcule le nombre de* 1 *modulo* 2 *dans la représentation de* n *en base* 2

n	0	1	2	3	4	5	6	7	8	...
$(n)_2$	0	1	10	11	100	101	110	111	1000	...
t_n	0	1	1	0	1	0	0	1	1	...

Le ***mot de Thue-Morse (infini)*** *qui correspond est donné par*

$$W = 01101001100101101001011001101001100101100110100101101001100101 10\ldots$$

La figure suivante nous donne un aperçu sur cette suite

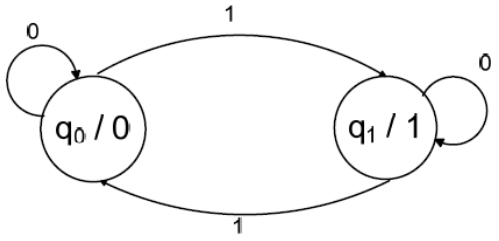

Fig.1. Automate fini engendrant la suite de Thue-Morse.

Dans le chapitre 3 on va utiliser la définition suivante :

Définition 2.1.15 *Soient α et β deux entiers naturels différents. La suite de Thue-Morse $(t_n)_{n\geq 0}$ à valeurs dans l'ensemble $\mathbf{A} = \{\alpha, \beta\}$ est définie par $t_n = \alpha$ (resp.β) si l'écriture binaire de n contient un nombre paire (resp. impair) du chiffre 1. Autrement dit*

$$t_n = \begin{cases} \alpha & \text{si l'écriture binaire de } n \text{ contient un nombre paire de } 1. \\ \beta & \text{sinon.} \end{cases} \tag{2.1}$$

La suite de Thue-Morse a de nombreuses propriétés. Dans ce qui suit, on a besoin des théorèmes suivants :

Théorème 2.1.16 *On peut définir la suite de Thue-Morse par les relations de récurrence suivantes :*

$$\begin{cases} t_0 = 0 \\ t_{2n} = t_n \quad , \quad t_{2n+1} = 1 - t_n \quad , \quad \forall n \geq 0 \end{cases}$$

Preuve. Voir [11]. ■

Théorème 2.1.17 *Le mot fini défini par les lettres de la suite de Thue-Morse*

$$W = t_0 t_1 ... t_{4^k-1}, \forall k \geq 1$$

est un palindrome , i.e. $W = \overline{W}$, et les deux lettres de l'alphabet $\mathbf{A}$ ont le même nombre d'occurrences.

Preuve. Voir [11]. ■

Définition 2.1.18 *Soit $\lambda = \sum_{n\geq 0} a_n p^n \in \mathbb{Z}_p$; on dit que λ est k-automatique, pour $2 \leq k \leq p-1$, si la suite des chiffres $(a_n)_{n\geq 0}$ est k-automatique.*

Définition 2.1.19 *Soit $\beta = \sum_{n\geq -N} a_n p^n \in \mathbb{Q}_p$; pour $n \geq -N$ on pose $b_{n+N} = a_n$, on trouve que*

$$\beta = \sum_{n\geq -N} b_{n+N} p^n = \sum_{m\geq 0} b_m p^{m-N}$$

On dit que β est k-automatique si la suite des chiffres $(b_m)_{m\geq 0}$ est k-automatique.

Exemple 2.1.20 *Soit l'entier 2-adique*

$$\begin{aligned} \lambda &= \sum_{n\geq 0} 2^{2n} = 1 + 2^2 + 2^4 + 2^6 + 2^8 + ... \\ &= 10101010101010101010101010101010... \end{aligned}$$

la suite des chiffres $(a_n)_{n\geq 0}$ *est définie par :*

$$a_n = \begin{cases} 1 & \text{si } n \text{ est pair.} \\ 0 & \text{si } n \text{ est impair.} \end{cases}$$

C'est une suite 2*-automatique. En effet, on a l'automate fini* $\mathcal{F}= (\mathbf{A}, Q, E, F, \delta)$ *, où :*

$$\mathbf{A} = \{0,1\}.Q = \{q_0, q_1, q_2\}.E = \{q_0\}.G = \{q_1, q_2\}.$$

$\delta : Q \times \mathbf{A} \to Q$ *l'application de transition définie par :*

$$\delta(q_0,0) = q_1, \delta(q_0,1) = q_2, \delta(q_1,0) = q_1, \delta(q_1,1) = q_1, \delta(q_2,0) = q_2, \delta(q_2,1) = q_2.$$

Et l'application

$$\varphi : Q \to \{0,1\}$$

définie par $\varphi(q_1) = 1$ *,* $\varphi(q_2) = 0$*.*
Si n *est pair, alors son écriture binaire commence par* 0*, donc l'état atteint par l'automate est* q_1 *, d'où on a*

$$a_n = \varphi(q_1) = 1.$$

Et si n *est impair, donc son écriture binaire commence par* 1*, et l'état atteint par l'automate est* q_2 *, d'où on a*

$$a_n = \varphi(q_2) = 0.$$

Alors le nombre λ *est* 2*-automatique.*

Exemple 2.1.21 *Soit l'entier p-adique*

$$\gamma = \sum_{n\geq 0} a_n p^n$$

avec $(a_n)_{n\geq 0}$ *est une suite de Thue-Morse ; Il est clair que ce nombre est* 2*-automatique, et nous avons :*

$$\begin{aligned} \gamma &= 2 + 2^2 + 2^4 + 2^7 + 2^8 + 2^{11} + \ldots && \textit{développement p-adique} \\ &= 011010011001011010010 11\ldots && \textit{mot de Thue-Morse correspond} \end{aligned}$$

2.2 Fractions continues

Pour les définitions et les théorèmes de cette section on pourra consulter : [24, 34, 38] pour le cas réel, et 25, 26, 27,59] pour le cas p-adique.

L'un des outils privilégiés pour étudier l'approximation d'un nombre réel ou p-adique par des nombres rationnels est d'utiliser le développement en fraction continue.

Dans le cas réel, la méthode pour construire les fractions continues est clair, puisque pour tout nombre réel x, il y a au plus deux valeurs d'un nombre entier α tel que $0 \leq |x-\alpha| < 1$. Dans le cas p-adique, il existe une infinité d'entiers $\alpha \in \mathbb{Z}$ tel que $0 \leq |x-\alpha|_p < 1$. Cependant, il est difficile de trouver une méthode analogue au cas réel pour définir les fractions continues p-adique. Dans la suite, on va décrire la défintion commune pour les deux cas, puis on distingue le cas p-adique dans la section suivante.

2.2.1 Définitions et propriétés

Définition 2.2.1 *Dans un corps $\Bbbk = \mathbb{R}$ ou $\mathbb{Q}_p$, nous définissons les fractions continues par une suite de fonctions homographique : (i.e. sous la forme d'un quotient de deux fonctions affines)*

$$\begin{cases} [a;x] = a + \dfrac{1}{x} \\ [a_0;a_1,x] = [a_0;[a_1,x]] = a_0 + \dfrac{1}{a_1 + \dfrac{1}{x}} \\ \qquad\qquad \ldots\ldots \\ [a_0;a_1,a_2,...,a_n,x] = [a_0;a_1,a_2,...,a_{n-1},[a_n,x]] \end{cases}$$

avec $a_i \in \mathbb{Q}$, $\forall i \geq 0$. On appelle $(a_i)_{i\in\mathbb{N}}$ la suite des quotients partiels, et on appelle $[a_0;a_1,a_2,...,a_i]$ la $i^{ème}$ réduite de ce développement, on la note $\dfrac{p_i}{q_i}$.

Remarque 2.2.2 *Si le développement est infini (on écrit $[a_0;a_1,a_2,...,a_n,...]$), et s'il est périodique à partir de a_k on écrit $[a_0;a_1,a_2,...,\overline{a_k}]$.*

Il y a des critères de convergence pour les fractions continues réelles infinies dans plusieurs références citées avant. On donne dans la section 2.2.2 des critères de convergence pour les fractions continues p-adiques.

On va utiliser les matrices pour décrire l'expression explicite de $\dfrac{p_i}{q_i}$:

Définition 2.2.3 *La matrice de la fonction homographique* $a_k + \dfrac{1}{z}$ *est donnée par*

$$\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}$$

donc la matrice de la fonction homographique $[a_0; a_1, a_2, ..., a_k, z]$ *est donnée par*

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} ... \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}$$

Il en résulte une matrice 2×2*, on la note*

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

d'où, on a

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} ... \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}$$

C'est-à-dire qu'on aura

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + ... \cfrac{1}{a_k + \cfrac{y}{x}}}} = \left[a_0; a_1, a_2, ..., a_k, \frac{x}{y}\right] = \frac{p_k x + p_{k-1} y}{q_k x + q_{k-1} y}$$

avec les relations de récurrences pour $i \in \mathbb{N}$ *:*

$$\begin{cases} p_{-1} = 1, p_0 = a_0, \\ p_{i+1} = a_{i+1} p_i + p_{i-1} \\ \quad et \\ q_{-1} = 0, q_0 = 1, \\ q_{i+1} = a_{i+1} q_i + q_{i-1}, \end{cases}$$

et pour $k \in \mathbb{N}$ *on a :*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + ... \cfrac{1}{a_k}}} = [a_0; a_1, a_2, ..., a_{k-1}, a_k] = \frac{p_k}{q_k} \tag{2.2}$$

Cette définition exige que q_k n'est pas nul, on remarque aussi que p_i et q_i ne sont pas

des entiers. Nous aurons donc besoin d'introduire ces nombres en fractions de nombres entiers :

Définition 2.2.4 *Soit $a_i = \frac{b_i}{c_i}$ avec $b_i \in \mathbf{Z}^*$ et $c_i \in \mathbf{N}^*$, on définit des nouveaux réduites par :*

$$p'_n = \left(\prod_{j=0}^{j=n} c_j\right) p_n \qquad et \quad q'_n = \left(\prod_{j=0}^{j=n} c_j\right) q_n \tag{2.3}$$

Il est facile de prouver par induction que p'_n, $q'_n \in \mathbf{Z}^*$; $\forall n \in \mathbb{N}$.

Proposition 2.2.5 *La suite des réduites vérifie l'équation :*

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}, \quad \forall k \in \mathbb{N}.$$

Preuve. On va démontrer la relation par récurrence :
Pour $k = 0$: $p_0 q_{-1} - q_0 p_{-1} = a_0.0 - 1.1 = (-1)^{0+1}$.

Supposons que le relation est vrai pour k, i.e. $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$.
nous avons pour $k+1$:

$$p_{k+1} = a_{k+1} p_k + p_{k-1} \quad \text{et} \quad q_{k+1} = a_{k+1} q_k + q_{k-1} \tag{2.4}$$

d'où

$$\begin{aligned} p_{k+1} q_k - q_{k+1} p_k &= (a_{k+1} p_k q_k + p_{k-1} q_k) - (a_{k+1} q_k p_k + q_{k-1} p_k) \\ &= -(p_k q_{k-1} - q_k p_{k-1}) = -(-1)^{k+1} = (-1)^{k+2} \end{aligned}$$

ce qu'il faut démontrer. ■

Les deux questions naturelles suivantes ont connu des réponses en considérant $\mathbb{Q}$ comme un sous ensemble de $\mathbb{R}$ ou de $\mathbb{Q}_p$:

Question 1 : Étant donné une suite $(a_i)_{i\in\mathbb{N}}$ à valeurs dans $\mathbb{Q}^*$, Est-ce que la suite des réduites $([a_0; a_1, a_2, ..., a_i])_{i\in\mathbb{N}}$ admet une limite dans $\mathbb{R}$? dans $\mathbb{Q}_p$?

Question 2 : Étant donné un nombre réel ou p-adique α, est-ce qu'on peut trouver une suite $(a_i)_{i\in N}$ à valeurs dans $\mathbb{Q}^*$ tel que la suite $([a_0; a_1, a_2, ..., a_i])_{i\in\mathbb{N}}$ converge vers α dans $\mathbb{R}$? dans $\mathbb{Q}_p$?

Afin d'étudier la convergence de la suite $([a_0; a_1, a_2, ..., a_i])_{i\in N}$, nous considérons la série $\sum_{i=1}^{i=k} \left(\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}\right)$; d'après la proposition (2.2.5), on trouve

$$\frac{p_k}{q_k} = \frac{p_0}{q_0} + \sum_{i=1}^{k} \frac{(-1)^{i+1}}{q_i q_{i-1}}. \tag{2.5}$$

On note $[a_0; a_1, ..., a_i, ...]$ la limite de $[a_0; a_1, a_2, ..., a_i]$ si elle existe. La propriété suivante est connue dans le cas réel :

Théorème 2.2.6 *Si la suite des quotients partiels $(a_n)_{n\in\mathbb{N}}$ satisfait*

$$Min\{a_n, n \in \mathbb{N}\} > 0,$$

alors la suite des réduites $([a_0; a_1, a_2, ..., a_k])_{k\in\mathbb{N}}$ admet une limite dans $\mathbb{R}$ et on a de plus

$$|q_n [a_0; a_1, a_2, ..., a_k, ...] - p_n| \leq \frac{1}{|q_{n+1}|}. \tag{2.6}$$

Preuve. Notons que $q_n q_{n+1}$ est croissant. En effet, on a $\forall n \in \mathbb{N}$:

$$\begin{aligned} a_{n+1} \quad &> \quad 0, q_n > 0 \Longrightarrow a_{n+1}q_n > 0 \\ &\Longrightarrow \quad a_{n+1}q_n + q_{n-1} > q_{n-1} \\ &\Longrightarrow \quad q_{n+1} > q_{n-1} \Longrightarrow q_n q_{n+1} > q_{n-1}q_n \end{aligned}$$

Soit maintenant $\xi = Min\{a_i; i \in \mathbb{N}\}$. On aura les deux cas suivants :
i) Si $\xi > 1$, on démontre par récurrence l'inégalité :

$$\forall n \in \mathbb{N} : q_n \geq \xi^n \tag{2.7}$$

Nous avons : $q_0 = 1 = \xi^0$, $q_1 = a_1 \geq \xi^1$, on suppose $q_n \geq \xi^n$, on a

$$q_{n+1} = a_{k+1}q_k + q_{k-1} \geq \xi^{n+1} + \xi^{n-1} \geq \xi^{n+1}$$

donc la relations est vraie $\forall n \in \mathbb{N}$.
A partir de l'inégalité (2.7), on aboutit à

$$\left|\frac{(-1)^{i+1}}{q_i q_{i-1}}\right| \leq \frac{1}{\xi^{2i-1}}$$

Cela signifie, d'après (2.5), que la série

$$\sum_{i=1}^{+\infty} \frac{(-1)^{i+1}}{q_i q_{i-1}}$$

converge (elle est bornée par la série géométrique convergente $\sum_{i=1}^{i=+\infty} \frac{1}{\xi^{2i-1}}$, avec $\frac{1}{\xi} < 1$). d'où la suite des réduites $\left(\frac{p_k}{q_k}\right)_k$ converge quand $k \to +\infty$.
ii) Si $1 \geq \xi > 0$, on démontre par récurrence :

$$\forall n \in \mathbb{N} : q_n \geq \xi \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n-1} \tag{2.8}$$

En effet, pour $n = 0$, on a $q_0 = 1 \geq \frac{2\xi}{\xi+\sqrt{\xi^2+4}}$.
Supposons que la relation est vraie $\forall k = \overline{0,n}$, nous avons :

$$\begin{aligned}
q_{n+1} &= a_{n+1}q_n + q_{n-1} \\
&\geq \xi^2 \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n-1} + \xi \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n-2} \\
&\geq \xi \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n} \left[\frac{2\xi}{\xi + \sqrt{\xi^2+4}} + \frac{4}{\left(\xi + \sqrt{\xi^2+4}\right)^2} \right] \\
&\geq \xi \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n} \left[\frac{2\xi^2 + 2\xi\sqrt{\xi^2+4} + 4}{\left(\xi + \sqrt{\xi^2+4}\right)^2} \right] \\
&= \xi \left(\frac{\xi + \sqrt{\xi^2+4}}{2} \right)^{n}
\end{aligned}$$

On revient au premier cas (2.7), en remarquant que $\xi' = \frac{\xi+\sqrt{\xi^2+4}}{2} > 1$.
Pour démontrer l'inégalité (2.6), il suffit de passer à la limite quand $k \to +\infty$ dans la relation suivante :

$$\begin{aligned}
\left| [a_0; a_1, a_2, ..., a_k] - \frac{p_n}{q_n} \right| &= \left| \sum_{i=n+1}^{i=k} \frac{(-1)^{i+1}}{q_i q_{i-1}} \right| \\
&\leq \frac{1}{|q_n q_{n+1}|}
\end{aligned}$$

D'où ce qu'on voulait démontrer. ■

Dans les démonstrations de la transcendance du troisième chapitre, nous avons besoin d'une majoration de p_i et q_i, comme suit :

Lemme 2.2.7 *On Suppose que $a_i \in \mathbb{Q}_+^*$ et que l'ensemble $\{a_i; i \in \mathbb{N}\}$ est bornée. Soit $\Xi = Max\{a_i; i \in \mathbb{N}\}$, alors*

$$q_n \leq \left(\frac{\Xi + \sqrt{\Xi^2+4}}{2} \right)^{n} \text{ et } p_n \leq \left(\frac{\Xi + \sqrt{\Xi^2+4}}{2} \right)^{n+1}.$$

Preuve. On démontre par récurrence l'inégalité de q_n :

Pour $n = 0$: C'est évident. Pour $n = 1$

$$q_1 = a_1 \leq \Xi \leq \frac{\Xi + \sqrt{\Xi^2 + 4}}{2}$$

Supposons que la relation est vrai pour n, i.e.

$$q_n \leq \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^n$$

nous avons pour $n + 1$

$$\begin{aligned} q_{n+1} &= a_{n+1} q_n + q_{n-1} \\ &\leq \Xi \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^n + \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n-1} \\ &\leq \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+1} \left[\frac{2\Xi}{\Xi + \sqrt{\Xi^2 + 4}} + \frac{4}{\left(\Xi + \sqrt{\Xi^2 + 4} \right)^2} \right] \\ &= \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+1} \end{aligned}$$

Par la même procédure on démontre par récurrence l'inégalité de p_n :
Pour $n = 0$

$$p_0 = a_0 \leq \Xi \leq \frac{\Xi + \sqrt{\Xi^2 + 4}}{2}$$

et pour $n = 1$

$$p_1 = a_1 a_0 \leq \Xi^2 \leq \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^2$$

Supposons que la relation est vraie pour n, i.e. $p_n \leq \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+1}$.
Nous avons pour $n + 1$

$$\begin{aligned} p_{n+1} &= a_{n+1} p_n + p_{n-1} \\ &\leq \Xi \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+1} + \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^n \\ &\leq \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+2} \left[\frac{2\Xi}{\Xi + \sqrt{\Xi^2 + 4}} + \frac{4}{\left(\Xi + \sqrt{\Xi^2 + 4} \right)^2} \right] \\ &= \left(\frac{\Xi + \sqrt{\Xi^2 + 4}}{2} \right)^{n+1} \end{aligned}$$

ce qu'il falait démontrer. ■

L'algorithme suivant est la méthode la plus simple pour calculer les fractions continues d'un nombre rationnel dans $\mathbb{R}$:

Algorithme 2.2.8 *Soit $r \in \mathbb{Q}$, On pose $a_0 = [r]$, $r_1 = \dfrac{1}{r - a_0}$, puis en met $a_1 = [r_1]$, $r_2 = \dfrac{1}{r_1 - a_1}$, et ainsi de suite, tant que r_i n'est pas un entier.*
On trouve deux suites récurrentes définies par

$$\begin{cases} r_{n+1} = \dfrac{1}{r_n - a_n} \\ \\ a_n = [r_n] \end{cases}$$

Donc les fractions continues de r sont les termes de la suite $\left(\frac{P_n}{Q_n}\right)_{n\in\mathbb{N}}$ définie par

$$\begin{cases} P_0 = a_0 \quad , \quad P_1 = a_0 a_1 + 1 \\ Q_0 = 1 \quad , \quad Q_1 = a_1 \\ P_n = a_n P_{n-1} + P_{n-2} \\ Q_n = a_n Q_{n-1} + Q_{n-2} \end{cases}$$

Exemple 2.2.9 *On va appliquer cet algorithme dans $\mathbb{Q}_p$. Soit $p = 7$, $r = \dfrac{5}{21}$, On a*

$$\begin{aligned} \frac{5}{21} &= \frac{3.4 - 7}{3.7} = \frac{4}{7} - \frac{1}{3} \\ &= \frac{4}{7} + 2 + 2.7 + 2.7^2 + 2.7^3 + ... \end{aligned}$$

la partie fractionnaire de r est donnée par $a_0 = \langle r \rangle_7 = \frac{4}{7} + 2 = \frac{18}{7}$, donc

$$\begin{aligned} r_1 &= \frac{1}{r - a_0} = \frac{-3}{7} = \frac{4}{7} - 1 \\ &= \frac{4}{7} + 6 + 6.7 + 6.7^2 + 6.7^3 + ... \end{aligned}$$

il vient que $a_1 = \langle r_1 \rangle_7 = \frac{4}{7} + 6 = \frac{46}{7}$, d'où

$$\begin{aligned} r_2 &= \frac{1}{r_1 - a_1} = \frac{-1}{7} \\ &= \frac{6}{7} + 6 + 6.7 + 6.7^2 + 6.7^3 + ... \end{aligned}$$

c'est à dire que $a_2 = \langle r_2 \rangle_7 = \frac{6}{7} + 6 = \frac{48}{7}$ *alors*

$$r_3 = \frac{1}{r_2 - a_2} = \frac{-1}{7} = r_2$$

on aboutit à

$$a_3 = \langle r_3 \rangle_7 = \langle r_2 \rangle_7 = a_2$$

Ainsi, les suites $(a_n)_{n\in\mathbb{N}}$ *et* $(r_n)_{n\in\mathbb{N}}$ *sont stationnaires, donc infinis. Cela signifie que l'algorithme classique pour calculer le développement en fraction continue d'un nombre rationnel n'est pas fini dans le cas p-adique.*

On donne ici, les énoncés des trois théorèmes les plus célèbres dans le cas réel, qui caractérisent le développement d'un nombre rationnel en fraction continue, et celui d'un nombre quadratique :

Théorème 2.2.10 *Le nombre réel* r *est un rationnel si et seulement si la suite des quotients partiels* $(a_n)_{n\in\mathbb{N}}$ *est finie.*

Théorème 2.2.11 (Lamé) *Le nombre de termes du développement en fraction continue d'un rationnel* $\frac{a}{b}$ *est inférieur à cinq fois le nombre de chiffres servant à écrire le plus petit des deux entiers* a *et* b*.*

Théorème 2.2.12 (Lagrange) *La suite* $(a_n)_{n\in\mathbb{N}}$ *est ultimement périodique si et seulement si* r *est algébrique de degré deux (i.e. quadratique).*

2.2.2 Fractions continues p-adiques

Afin d'obtenir une réponse positive, avec une solution unique, à la **Question 2** : Est-ce qu'on peut trouver une suite $(a_i)_{i\in N}$ à valeurs dans $\mathbb{Q}^*$ tel que la suite $([a_0; a_1, a_2, ..., a_i])_{i\in\mathbb{N}}$ converge vers un nombre α dans $\mathbb{Q}_p$?

Plusieurs algorithmes *à la Euclide* ont été pris en considération. Il existe deux définitions différentes du développement en fraction continue d'un nombre p-adique, la première est celle de Schneider [59, 1968], et la deuxième est due à Ruban [55, 1970], cette dernière a été modifiée par Browkin [25, 1978], et elle est redécouverte par Wang [66, 67, 68, 1985]. Schneider semble être le premier qui a défini un algorithme des fractions p-adiques d'une manière naturelle, pourtant avant lui, il y avait Mahler [46] qui a donné une représentation géométrique des fractions continues d'un entier p-adique, mais cette construction n'était pas d'une manière naturelle, dans le sens qu'elle n'a pas eu lieu en choisissant les quotients partiels et en construisant les restes itérativement.

Nous mentionnons que Ruban a considéré les quotients partiels a_k dans l'ensemble $\mathbb{Z}\left[\frac{1}{p}\right] \cap]0, p[$ avec

$$\mathbb{Z}\left[\frac{1}{p}\right] = \left\{a_0 + a_1\frac{1}{p} + ... + a_k\frac{1}{p^k}/a_0, a_1, ..., a_k, k \in \mathbb{N}\right\} = \left\{\frac{\alpha}{p^k}/\ \alpha, k \in \mathbb{Z}\right\} \tag{2.9}$$

Tandis que Browkin a considéré les a_n dans $\mathbb{Z}\left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[$ telles que $|a_0|_p = 1$ et $|a_n|_p > 1$ pour tout n dans $\mathbb{N}^*$. Dans qui suit, on va décrire les trois définitions, ainsi que leurs algorithmes de calcul :

Définition 2.2.13 (Schneider) *Soit $x \in \mathbb{Z}_p$ un entier p-adique, avec $p \geq 3$, le développement en fraction continue de Schneider (on l'abrége FCS) de x est donné par la formule*

$$x = b_0 + \cfrac{p^{n_0}}{b_1 + \cfrac{p^{n_1}}{b_2 + \cfrac{p^{n_2}}{b_3 + ...}}} \tag{2.10}$$

avec $n_0 \in \mathbb{N}$, $b_0 \in \{0, 1, 2, ..., p-1\}$ et $n_j \in \mathbb{N}^*$, $b_j \in \{1, 2, ..., p-1\}$ $\forall j \in \mathbb{N}^*$.
On écrit

$$x = \begin{bmatrix} & p^{n_0}, & p^{n_1}, & p^{n_2}, & p^{n_3}, & ..... \\ \\ b_0; & b_1, & b_2, & b_3, & & ..... \end{bmatrix} \tag{2.11}$$

Algorithme 2.2.14 (Schneider) *Nous présentons ici, l'algorithme permettant de développer un nombre p-adique quelconque x en FCS :*

***étape* 0** : *On met* $x_0 = x$.

***étape* 0′**: *On choisit* $b_0 = \overline{0, p-1}$ *tel que* $v_p(x_0 - b_0) \geq 0$,

a ce stade on aura $n_0 = v_p(x_0 - b_0)$.

***étape* 1** : *On met* $x_1 = \dfrac{p^{n_0}}{x_0 - b_0}$, *donc* $x = x_0 = b_0 + \dfrac{p^{n_0}}{x_1}$.

***étape* 1′** : *On choisit* $b_1 = \overline{1, p-1}$ *tel que* $v_p(x_1 - b_1) > 0$,

a ce stade on aura $n_1 = v_p(x_1 - b_1)$.

***étape* 2** : *On met* $x_2 = \dfrac{p^{n_1}}{x_1 - b_1}$, *donc* $x = b_0 + \dfrac{p^{n_0}}{b_1 + \dfrac{p^{n_1}}{x_2}}$.

***étape* 2′**: *On choisit* $b_2 = \overline{1, p-1}$ *tel que* $v_p(x_2 - b_2) > 0$,

a ce stade on aura $n_2 = v_p(x_2 - b_2)$.

...

...

...

***étape* m** : *On met* $x_m = \dfrac{p^{n_{m-1}}}{x_{m-1} - b_{m-1}}$, *donc* $x = b_0 + \cfrac{p^{n_0}}{b_1 + \cfrac{p^{n_1}}{\ddots \cfrac{}{b_{m-1} + \cfrac{p^{n_{m-1}}}{x_m}}}}$

***étape* m′**: *On choisit* $b_m = \overline{1, p-1}$ *tel que* $v_p(x_m - b_m) > 0$,

a ce stade on aura $n_m = v_p(x_m - b_m)$.

...

...etc

Remarque 2.2.15 *Si* $x_m = b_m$ *l'algorithme s'arrête, et* b_m *c'est le dernier terme du développement en fraction continue de Schneider.*

Remarque 2.2.16 *Avec la définition de Schneider, les nombres rationnels n'admettent pas tous un développement fini en fraction continue. Dans le chapitre 3 on donne un théorème de Bundschuh qui caractérise les nombres rationnels qui ont un développement fini en FCS. Bundschuh a également démontré que les fractions continues de Schneider du nombre quadratique* $\sqrt{m} \in \mathbb{Q}_p$, *avec* $m \in \mathbb{N}$, *ne sont pas toujours périodiques. Le théorème de Lagrange n'est pas valide au cas des fractions continues de Schneider.*

Exemple 2.2.17 *Soit* $p = 3$, $r = -\dfrac{1}{2}$ *: D'après l'algorithme de Schneider on a*

étape 0/ *On met* $x_0 = -\dfrac{1}{2}$.

étape 0'/ *On choisit* $b_0 \in \{0, 1, 2\}$ *tel que* $v_p(-\dfrac{1}{2} - b_0) \geq 0$, *d'où* $b_0 = 0$, *on aura* $n_0 = 0$.

étape 1/ *On met* $x_1 = \dfrac{3^0}{-\dfrac{1}{2} - 0} = -2 = 1 + 2.3 + 2.3^2 + 2.3^3 + ...$

étape 1'/ *On choisit* $b_1 \in \{1, 2\}$ *tel que* $v_p(-2 - b_1) > 0$, *d'où* $b_1 = 1$, *on aura* $n_1 = 1$.

étape 2/ *On met* $x_2 = \dfrac{3^1}{-2 - 1} = -1 = x_1$.

étape 2'/ *Donc* $b_2 = b_1 = 2$ *et* $n_2 = n_1 = 1$.

.....

.....

étape m/ *On met* $x_m = x_{m-1} = ... = x_1 = -1$.

étape m'/ *Donc* $b_m = b_{m-1} = 2$ *et* $n_m = n_{m-1} = 1$.

.....

On d'autre terme, nous avons le développement

$$-\frac{1}{2} = \cfrac{3^0}{1 + \cfrac{3^1}{2 + \cfrac{3^1}{2 + \cfrac{3^1}{2 + ...}}}}$$

qui s'écrit aussi

$$-\frac{1}{2} = \left[\begin{array}{cccccc} & 3^0, & 3^1, & 3^1, & 3^1, & ..... \\ \\ 1; & 2, & 2, & 2, & 2, & ..... \end{array} \right]$$

On voit bien que le développement en FCS de $x = -\dfrac{1}{2}$ *dans* $\mathbb{Q}_3$ *est stationnaire, donc il est infini.*

Définition 2.2.18 (Ruban) *Le développement en fraction continue de Ruban (on l'abrége FCR) de* $x \in \mathbb{Q}_p$ *avec* $p \geq 3$, *est défini par*

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + ...}}} \tag{2.12}$$

tels que $b_j \in \mathbb{Z} \cap \left[\dfrac{1}{p}\right] \cap]0, p[\quad \forall j \in \mathbb{N}$, $|b_0|_p \geq 1$ *et* $|b_j|_p > 1 \quad \forall j \in \mathbb{N}^*$.

On écrit

$$x = \left[\begin{array}{cccccc} b_0; & b_1, & b_2, & b_3, & ..... \end{array} \right] \tag{2.13}$$

Algorithme 2.2.19 (Ruban) *Nous présentons ici, l'algorithme permettant de développer un nombre p-adique quelconque* x *en FCR :*

***étape* 0** : *On met* $x_0 = x$, *avec son développement de Hensel* $\sum_{k=-m}^{+\infty} \alpha_k p^k$.

***étape* 0′**: *On choisit* $b_0 = \langle x_0 \rangle_p = \frac{\alpha_{-m}}{p^m} + \frac{\alpha_{-m+1}}{p^{m-1}} + ... + \frac{\alpha_{-1}}{p} + \alpha_0$.

***étape* 0″**: *Si* $\langle x_0 \rangle_p = x_0$, *d'où* $[x]_p = 0$, *alors l'algorithme s'arrête, ce qui veut dire que le développement est fini et* x *est un nombre rationnel.*

Sinon on passe à l'étape suivant .

***étape* 1** : *On met* $x_1 = \dfrac{1}{x_0 - b_0}$.

***étape* 1′** : *On choisit* $b_1 = \langle x_1 \rangle_p$.

***étape* 1″**: *Si* $\langle x_1 \rangle_p = x_1$, *d'où* $[x_1]_p = 0$, *alors l'algorithme s'arrête, ce qui veut dire que le développement est fini et* x *est un nombre rationnel.*

Sinon on passe à l'étape suivant .

...

...

...

***étape* m** : *On met* $x_m = \dfrac{1}{x_{m-1} - b_{m-1}}$, *donc* $x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\vdots \cfrac{}{b_{m-1} + \cfrac{1}{x_m}}}}$

***étape* m′**: *On choisit* $b_m = \langle x_m \rangle_p$.

***étape* m″**: *Si* $\langle x_m \rangle_p = x_m$, *d'où* $[x_m]_p = 0$, *alors l'algorithme s'arrête, ce qui veut dire que le développement est fini et* x *est un nombre rationnel.*

Sinon on passe à l'étape suivant .

...

...etc

Exemple 2.2.20 *On prend le même nombre* $x = -\dfrac{1}{2}$ *dans* $\mathbb{Q}_3$. *D'après l'algorithme de Ruban nous avons les étapes suivantes :*

étape 0/ *On met* $x_0 = -\dfrac{1}{2}$, *on a* $-1 = 2 + 2.3 + 2.3^2 + 2.3^3 + ...$,

d'où $\dfrac{-1}{2} = \sum_{k=0}^{+\infty} 1.3^k = 1 + 1.3 + 1.3^2 + 1.3^3 + ...$

étape 0'/ *On choisit* $b_0 = \langle x_0 \rangle_p = 1$.

étape 1/ *On met* $x_1 = \dfrac{1}{-\frac{1}{2} - 1} = -\dfrac{2}{3} = \dfrac{1}{3} + 2 + 2.3 + 2.3^2 + 2.3^3 + ...$

(puisque $-2 = 1 + 2.3 + 2.3^2 + 2.3^3 + ...$*).*

étape 1'/ *On choisit* $b_1 = \langle x_1 \rangle_p = \dfrac{1}{3} + 2 = \dfrac{7}{3}$.

étape 2/ *On met* $x_2 = \dfrac{1}{-\frac{2}{3}-\frac{7}{3}} = -\dfrac{1}{3} = \dfrac{2}{3} + 2 + 2.3 + 2.3^2 + 2.3^3 + ...$

étape 2'/ *On choisit* $b_2 = \langle x_2 \rangle_p = \dfrac{2}{3} + 2 = \dfrac{8}{3}$.

étape 2/ *On met* $x_3 = \dfrac{1}{-\frac{1}{3}-\frac{8}{3}} = -\dfrac{1}{3} = x_2$.

étape 2'/ *On choisit* $b_3 = \langle x_3 \rangle_p = \langle x_2 \rangle_p = b_2$.

.....

.....

étape m/ *On met* $x_m = x_{m-1}$. $\forall m \geq 3$

étape m'/ *On choisit* $b_m = b_{m-1}$. $\forall m \geq 3$

le développement en FCR de $x = -\dfrac{1}{2}$ *dans* $\mathbb{Q}_3$ *est stationnaire, donc il est infini. On voit que*

$$\begin{aligned} \frac{-1}{2} &= \left[1; \frac{7}{3}, \frac{8}{3}, \frac{8}{3}, \frac{8}{3}, \frac{8}{3}, \frac{8}{3} ...\right] \\ &= 1 + \cfrac{1}{\frac{7}{3} + \cfrac{1}{\frac{8}{3} + \cfrac{1}{\frac{8}{3} + \cfrac{1}{\frac{8}{3} + ...}}}} \end{aligned}$$

Avant de définir les fractions continues de Browkin, on donne une définition concernant une autre écriture des nombres p-adiques avec des coefficients dans $\left\{-\dfrac{p-1}{2}, ..., \dfrac{p-1}{2}\right\}$, pour plus de détail on peut consulter [60], [25], [37] :

Définition 2.2.21 *Soit* $p \geq 3$, *tout élément* $\zeta \in \mathbb{Q}_p$, *admet un développement unique sous la forme*

$$\zeta = \sum_{j=-m}^{+\infty} c_j p^j \quad où\ c_j \in \left\{-\frac{p-1}{2}, ... -1, 0, 1..., \frac{p-1}{2}\right\}, \forall j \geq -m \tag{2.14}$$

Dans ce cas, la partie fractionnaire est donnée par

$$\langle \zeta \rangle_p = \frac{c_{-m}}{p^m} + \frac{c_{-m+1}}{p^{m-1}} + ... + \frac{c_{-1}}{p} + c_0 \in \mathbb{Z}\left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[$$

Définition 2.2.22 (Browkin) *Pour le développement en fraction continue de Browkin (on l'abrége FCB), Browkin a pris la même définition et le même algorithme de Ruban*

en utilisant l'écriture (2.14), donc il a changé la condition sur les b_j, par celle-ci

$$b_j \in \mathbb{Z}\left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[\qquad \forall j \in \mathbb{N}.$$

Algorithme 2.2.23 *On utilise le même algorithme de Ruban. On donne ici un programme de calcul des FCB :*

[*Step* 1] $i = 0$. *Let* $x_0 = x$ *and* $b_0 = \langle x_0 \rangle_p = \frac{\alpha_{-m}}{p^m} + \frac{\alpha_{-m+1}}{p^{m-1}} + ... + \frac{\alpha_{-1}}{p} + \alpha_0$
[*Step* 2] *if* $x_i = b_i$. *then* x_{i+1} *and* b_{i+1} *are undefined.*
If this is the case, quit the algorithm
[*Step* 3] *if* $i = i + 1$. *Let* $x_i = (x_{i-1} - b_{i-1})^{-1}$ *and* $b_i = \langle x_i \rangle_p$. *Go to Step 2.*

Pour les fractions continues de Ruban et Browkin, nous avons le critère de convergence suivant, qui est donné par Browkin lui même [25] :

Théorème 2.2.24 (Critère de convergence) *Si la suite des quotients partiels* $(a_k)_{k\in\mathbb{N}}$ *satisfait* $v_p(a_k) \leq -1$, $\forall k \in \mathbb{N}^*$, *alors la suite des réduites* $([a_0; a_1, a_2, ..., a_k])_{k\in\mathbb{N}}$ *admet une limite dans* $\mathbb{Q}_p$.

Ce théorème est une conséquence des deux lemmes suivants :

Lemme 2.2.25 *Sous l'hypothèse du critère de convergence précédent, on a*

$$|q_n|_p = |a_1 a_2 ... a_n|_p \qquad et \qquad |p_n|_p = |a_0 a_1 ... a_n|_p \qquad , \forall n \in \mathbb{N}^*$$

Preuve. Une simple récurrence sur n. En effet, pour la norme de q_n, on a pour $n = 1$

$$q_1 = a_1 q_0 + q_{-1} = a_1 \Longrightarrow |q_1|_p = |a_1|_p$$

On suppose que $|q_n|_p = |a_1 a_2 ... a_n|_p$ et on démontre que $|q_{n+1}|_p = |a_1 a_2 ... a_{n+1}|_p$, on a

$$q_{i+1} = a_{i+1} q_i + q_{i-1} \Longrightarrow |q_{n+1}|_p \leq \max\left\{|a_{n+1}|_p . |q_n|_p , |q_{n-1}|_p\right\} \tag{2.15}$$

tandis que $v_p(a_k) \leq -1$ entrain que $|a_k|_p \geq p > 1$, d'où

$$|a_{n+1}|_p . |q_n|_p = |a_1 a_2 ... a_{n-1} a_n a_{n+1}|_p > |a_1 a_2 ... a_{n-1}|_p$$

alors

$$|q_{n+1}|_p = |a_1 a_2 ... a_{n+1}|_p$$

Maintenant pour la norme de p_n, on a
pour $n = 1$

$$p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1 \Longrightarrow |p_1|_p \leq \max\left\{|a_1 a_0|_p, 1\right\}$$

tandis que $|a_1|_p . |a_0|_p > 1$, d'où

$$|p_1|_p = |a_0 a_1|_p$$

On suppose que $|p_n|_p = |a_0 a_1 ... a_n|_p$ et on démontre que $|p_{n+1}|_p = |a_0 a_1 ... a_{n+1}|_p$, on a

$$p_{i+1} = a_{i+1} p_i + p_{i-1} \Longrightarrow |p_{n+1}|_p \leq \max\left\{|a_{n+1}|_p . |p_n|_p, |p_{n-1}|_p\right\}$$

tandis que $|a_k|_p > 1$, d'où

$$|a_{n+1}|_p . |p_n|_p = |a_0 a_1 ... a_{n-1} a_n a_{n+1}|_p > |a_1 a_2 ... a_{n-1}|_p \tag{2.16}$$

alors

$$|p_{n+1}|_p = |a_0 a_1 ... a_{n+1}|_p$$

donc la propriété est vraie $\forall n \in \mathbb{N}^*$. ■

Il en résulte que d'après la formule (2.5) et sous l'hypothèse du critère de convergence (2.2.24), la série de somme partielle $\sum_{i=k+1}^{i=n} \frac{(-1)^{i+1}}{q_i q_{i-1}}$ converge vers $\frac{(-1)^{k+1}}{q_{k+1} q_k}$ dans $\mathbb{Q}_p$.

Lemme 2.2.26 *Sous l'hypothèse du critère de convergence, on a,* $\forall k \in \mathbb{N}$

$$|q_k [a_0; a_1, a_2, ..., a_n, ...] - p_k|_p = \frac{1}{|q_k|_p |a_{k+1}|_p} = \frac{1}{|a_1 a_2 ... a_k a_{k+1}|_p}$$

Preuve. Soit $k < n$, on a

$$\left|\frac{p_n}{q_n} - \frac{p_k}{q_k}\right|_p = \frac{1}{|a_1^2 a_2^2 ... a_k^2 a_{k+1}|_p}$$

Par passage à la limite quand n tend vers l'infini, on obtient

$$\left|[a_0; a_1, ..., a_n, ...] - \frac{p_k}{q_k}\right|_p = \frac{1}{|a_1^2 a_2^2 ... a_k^2 a_{k+1}|_p}$$

d'où le résultat. ■

Nous avons le lemme suivant, qui est un autre critère de convergence de Browkin donné dans [26] :

Lemme 2.2.27 *Soit $(b_j)_j$ une suite telles que*

$$\begin{cases} b_j \in \mathbb{Z}\left[\frac{1}{p}\right] & \forall j \in \mathbb{N} \\ v_p(b_{2j}) = 0 & \forall j \in \mathbb{N}^* \\ v_p(b_{2j+1}) < 0 & \forall j \in \mathbb{N} \end{cases}$$

Alors, la suite des réduites $\left(\frac{P_j}{Q_j}\right)_{j\in\mathbb{N}}$ du développement en fraction continue définie par les $(b_j)_{j\in\mathbb{N}}$ converge vers un nombre p-adique θ.

2.3 Théorèmes dans le cas réel

2.3.1 Questions de transcendance

Dans le cas réel, on trouve plusieurs travaux qui s'intéressent à la transcendance des nombres irrationnels définis par leur développement en base entière (écriture décimal, par exemple) ou en fraction continue. une liste non exhaustive de ces résultats apparaît dans les références : [1], [2], [3], [4], [10], [28], [35], [51], [43].

Historiquement, en deux notes de 1844 aux comptes rendus à l'Académie des Sciences, Joseph Liouville établit l'existence des nombres transcendants, qui portent son nom.

Liouville donne deux preuves de l'existence de tels nombres ; toutes deux s'appuient sur la théorie des fractions continues pour établir le résultat fondamental suivant :

• **Liouville (1844) :** si α est un nombre algébrique de degré d, alors pour tout nombre rationnel $\frac{a}{b} \neq \alpha$, il existe $C(\alpha)$ une constante dépends de α :

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{C(\alpha)}{b^d} \tag{2.17}$$

Après Liouville, des gens travaillent sur le raffinement du théorème de Liouville, comme :

• **Thue (1909) :** remplace $\frac{C(\alpha)}{b^d}$ par $\frac{C(\alpha,\varepsilon)}{b^k}$ où $k = \frac{d}{2} + 1 + \varepsilon$.

• **Siegel (1921) :** $k = 2\sqrt{d} + \varepsilon$.

• **Gelfond (1947) :** $k = \sqrt{2d} + \varepsilon$.

• **Roth (1954) :** $k = 2 + \varepsilon$.

D'après Waldscmidt dans son survol [64] : "*Il est surprenant qu'il soit difficile de démontrer qu'un nombre réel est irrationnel. On dispose pourtant de plusieurs arguments. Ainsi, un nombre réel est rationnel si et seulement si, dans une base donnée, son développement est ultimement périodique, cette propriété ne dépend pas de la base. Un autre*

critère porte sur le développement en fraction continue : un nombre réel est rationnel si et seulement si son développement en fraction continue est fini.

Le problème c'est que, pour les nombres réels « intéressants », ceux qui apparaissent comme des constantes de l'analyse faisant intervenir des limites (suites, séries, intégrales, produits infinis), nous ne connaissons, la plupart du temps, rien sur ces développements. Il y a cependant un petit nombre d'exceptions : ainsi, L. Euler a donné quelques développements en fraction continue, le plus célèbre étant celui du nombre $e = 2,718281...$

$$e = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + ... \cfrac{1}{a_n + \cfrac{1}{\ddots}}}}$$

avec la suite des quotients partiels

$$[a_0, a_1, a_2, ..., a_n...] = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, ..., 1, 2^m, 1, ...] \tag{2.18}$$

ce qui donne l'irrationalité du nombre e*. Mais ces exemples restent trés limités, et, de façon générale, il semble préférable de trouver une autre voie pour démontrer des énoncés d'irrationalité.*

On dispose d'un puissant critère d'irrationalité en terme d'approximation rationnelle : **un nombre réel est irrationnel si et seulement s'il possède une suite de bonnes approximations rationnelles**. *Un nombre rationnel est très mal approché par les nombres rationnels autres que lui-même : si* $\frac{a}{b}$ *et* $\frac{c}{d}$ *sont deux nombres rationnels distincts, on a*

$$\left|\frac{a}{b} - \frac{c}{d}\right| \geq \frac{1}{bd} \tag{2.19}$$

à l'opposé, si un nombre est irrationnel, il possède de très bonnes approximations rationnelles. De façon plus précise :

Critère d'irrationalité. *Soit* ϑ *un nombre réel. Alors :*

θ *est irrationnel* $\Longleftrightarrow \forall \epsilon > 0$, $\exists (p, q) \in \mathbb{Z}^2$ *avec* $q > 0$ *tel que :*

$$0 < |q\vartheta - p| < \epsilon.$$

Maintenant, nous introduisons deux conditions de combinatoires, souvent appelé "exposant diophantien". Elles sont particulièrement intéressantes, car elles jouent un rôle essentiel dans les théorèmes décrits dans le cas réel, pour l'étude des propriétés diophantiennes de nombres réels définis via leur développement dans une base entière. Ces conditions sont formellement introduites dans les articles [3], [4], [7].

Condition 2.3.1 ($(*)_w$) *Soit $w > 1$ un nombre rationnel. Soit le mot $a = (a_i)_i$, on dit que a vérifie la condition $(*)_w$ s'il n'est pas ultimement périodique, et s'il existe deux suites de mots finis $(U_n)_{n\geq 1}$ et $(V_n)_{n\geq 1}$ telles que $\forall n \geq 1$:*
1- $U_n V_n \overline{U_n}$ est le début de a.
2- $|V_n| \leq w\,|U_n|$.
3- $|U_n| \leq |U_{n+1}|$.

Condition 2.3.2 ($(*)_{w,w'}$) *Soit $w, w' > 1$ deux nombres rationnels. Soit le mot $a = (a_i)_i$, on dit que a vérifie la condition $(*)_{w,w'}$ s'il n'est pas ultimement périodique, et s'il existe trois suites de mots finis $(U_n)_{n\geq 1}$, $(V_n)_{n\geq 1}$ et $(D_n)_{n\geq 1}$ telles que $\forall n \geq 1$:*
1- $D_n U_n V_n \overline{U_n}$ est le début de a.
2- $|V_n| \leq w\,|U_n|$.
3- $|U_n| \geq w'\,|D_n|$.
4- $|U_n| \leq |U_{n+1}|$.

Ferenczi et Mauduit ont démontré dans [35] la transcendance d'un nombre réel dont le début de son développement décimal satisfait la condition $(*)_w$ pour $w > 2$, puis Adamczewski et Bugeaud dans [3] ont fait la généralisation pour $w > 1$, et pour les nombres p-adiques. Ils ont démontré également dans [4] la transcendance d'un nombre réel dont le début de son développement en fraction continue réel est un palindrome arbitrairement long, et de manière plus générale si le début de la suite des quotients partiels satisfait les condition de combinatoire $(*)_w$ et $(*)_{w,w'}$:

Théorème 2.3.3 (A&B1) *S'il existe un nombre réel $w > 1$ tel que la suite $\mathbf{a} = (a_k)_{k\geq 1}$ satisfait à la condition $(*)_w$, alors le nombre réel $\alpha = \sum_{k\geq 1} \frac{a_k}{b^k}$ est transcendant.*

Théorème 2.3.4 (A&B2) *Soit $a = (a_m)_{m\geq 1}$ une suite d'entiers naturels. S'il existe $w \in \mathbb{Q}^+$ tel que a satisfait la condition $(*)_w$, alors le nombre réel $\alpha = [0; a_1, a_2, ..., a_m, ...]$ est transcendant.*

Théorème 2.3.5 (A&B3) *Soit $a = (a_m)_{m\geq 1}$ une suite d'entiers naturels, Soit un nombre réel α définie par son développement en fraction continue $[0; a_1, a_2, ..., a_m, ...]$, supposons que la suite $\left(Q_k^{\frac{1}{k}}\right)_{k\geq 1}$ est bornée, et $M = \limsup_{k\to+\infty} Q_k^{\frac{1}{k}}$ et $m = \liminf_{k\to+\infty} Q_k^{\frac{1}{k}}$. Soit w et w' deux nombres rationnels positifs tels que*

$$w' > \frac{2\log M}{\log m} - 1$$

Si la suite des quotients partiels $(a_i)_i$ satisfait la condition $(*)_{w,w'}$, alors α est transcendant.

Dans le théorème suivant soient : $A = \{0, 2, ..., p-1\}$ un alphabet, $\mathbf{a} = (a_k)_{k \geq -m}$ une suite de l'alphabet A n'est pas ultimement périodique, $\alpha = \sum_{k=-m}^{+\infty} a_k p^k$ un nombre p-adique.

Théorème 2.3.6 (A&B4) *S'il existe un réel $w > 1$ tel que la suite $\mathbf{a} = (a_k)_{k \geq 1}$ satisfait à la condition $(*)_w$, alors le nombre p-adique α est transcendant.*

Avant de terminer, on donne le théorème d'Adamczewski et Bugeaud [3] concernant les automates finis, il s'applique également pour les nombres p-adique :

Théorème 2.3.7 (A&B5) *Le développement dans une base entière $b \geq 2$ d'un nombre algébrique irrationnel ne peut pas être engendré par un automate fini.*

Avant de terminer cette section on présente le théorème intéressant de Martine Queffélec [51], qui a démontré en 1998 la transcendance d'un nombre réel donné par son développement en fraction continues de Thue-Morse, dans l'un de nos résultats nous avons démontré un résultat similaire :

Théorème 2.3.8 (Queffélec) *Soient α et β deux entiers naturels déstingue et $(t_k)_{k \geq 0}$ une suite de Thue-Morse sur l'alphabet $\{\alpha, \beta\}$. Alors le nombre réel $[t_0; t_1, t_2, ..., t_k, ...]$ est transcendant.*

2.3.2 Théorème du sous-espace

On rappelle ici l'énoncé du théorème du sous-espace. Ce résultat obtenu par W.M. Schmidt [58] en 1970 est réellement un outil très puissant. Il intervient (ainsi que sa version p-adique) dans les démonstrations de transcendance dont il est question dans cette section (Théorèmes d'Adamczewski et Bugeaud) et dans le troisième chapitre (Théorèmes de Belhadef, Esbelin et Zerzaihi). On montrera comment un outil diophantien puissant, qui est le théorème du sous-espace de Schmidt, a été utilisé afin d'obtenir de nouveaux résultats sur la transcendance des nombres réels et des nombres p-adiques.

Théorème 2.3.9 (Schmidt) *Soient $m \geq 2$ un entier relatif, et $\delta > 0$ un nombre réel. Considérons $L_1, ..., L_m$ des formes linéaires en les variables $\mathbf{x}_1, ..., \mathbf{x}_m$, à coefficients algébriques réels et linéairement indépendantes sur $\overline{\mathbb{Q}}$. On pose*

$$\begin{aligned} \mathbf{x} &= (\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_m) \in \mathbb{Z}^m \diagdown \{0\} \\ \|\mathbf{x}\|_\infty &= \max\left(|\mathbf{x}_i|\,,\ i = \overline{1, m}\right) \end{aligned}$$

Alors, l'ensemble des solutions $\mathbf{x}$ *de l'inégalité*

$$\prod_{i=1}^{m} \|L_i(\mathbf{x})\|_\infty \leq \|\mathbf{x}\|_\infty^{-\delta} \tag{2.20}$$

est contenu dans une union finie de sous-espaces vectoriels propres de $\mathbb{Q}^m$.

Pour mieux comprendre le théorème du sous-espace, on va expliquer comment le théorème de Roth [54] (connu aussi sous le nom Thue-Siegel-Roth) et le théorème de Ridout [52] se déduisent facilement du théorème du sous-espace, cela donne une petite idée de la puissance de ce résultat :

Théorème 2.3.10 (Roth) *Soit* α *un nombre algébrique et* $\delta > 0$. *Alors l'inégalité*

$$|\alpha - \frac{r}{s}| \leq s^{-2-\delta}$$

ne possède qu'un nombre fini de solutions rationnelles $\frac{r}{s} \in \mathbb{Q}$.

Preuve. Prenons dans le théorème du sous-espace de Schmidt : $m = 2$, et

$$L_1(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{x}_1, L_2(\mathbf{x}_1, \mathbf{x}_2) = \alpha\mathbf{x}_1 - \mathbf{x}_2$$

Ces deux formes linéaires de deux variables sont linéairement indépendantes sur $\mathbb{R}$ et leurs coefficients sont des nombres algébriques.
L'inégalité de Schmidt

$$|L_1(\mathbf{x})L_2(\mathbf{x})| \leq |\mathbf{x}|^{-\delta} \tag{2.21}$$

correspond à $s\,|s\alpha - r| \leq s^{-\delta}$, pour $\mathbf{x} = (s, r)$ ■

Le théorème de Schmidt a été généralisé par H.P. Schlickewei, il considère plusieurs valeurs absolues (alors que Schmidt ne considère qu'une seule valeur absolue archimédienne). Schlickewei a obtenu une version p-adique très utile du théorème du sous-espace. Nous donnons ici une version simple de ce résultat, extraite de [57] :

Théorème 2.3.11 (Schlickewei) *Soient* $\nu \geq 2$ *un entier,* S *un ensemble fini de nombres premiers,* $\delta > 0$ *un nombre réel. Soient,* $L_{1,\infty}, ..., L_{\nu,\infty}$ *des formes linéaires en les variables* $\mathbf{x}_1, ..., \mathbf{x}_\nu$, *à coefficients algébriques réels et linéairement indépendantes sur* $\overline{\mathbb{Q}}$. *Pour tout* $p \in S$, *soient* $L_{1,p}, ..., L_{\nu,p}$ *des formes linéaires en les variables* $\mathbf{x}_1, ..., \mathbf{x}_\nu$, *à coefficients p-adiques algébriques et linéairement indépendantes sur* $\overline{\mathbb{Q}}$. *Alors, l'ensemble des solutions* $\mathbf{x}$ *de l'inégalité*

$$\prod_{i=1}^{\nu} \left(\|L_{i,\infty}(\mathbf{x})\|_\infty \prod_{p \in S} \|L_{i,p}(\mathbf{x})\|_p \right) \leq \|\mathbf{x}\|_\infty^{-\delta} \tag{2.22}$$

avec

$$\begin{aligned} \mathbf{x} &= (\mathbf{x}_1, ..., \mathbf{x}_\nu) \in \mathbb{Z}^\nu \diagdown \{0\} \\ \|\mathbf{x}\|_\infty &= \max\left(|\mathbf{x}_i|\,,\ i = \overline{1,\nu}\right) \\ \|\mathbf{x}\|_p &= \max\left(|\mathbf{x}_i|_p\,,\ i = \overline{1,\nu}\right) \end{aligned}$$

est contenu dans une union finie de sous-espaces vectoriels propres de $\mathbb{Q}^\nu$.

Notons que, de même que le théorème du sous-espace implique facilement le théorème de Roth, le théorème de Ridout découle du résultat de Schlickewei.

Théorème 2.3.12 (Ridout) *Pour tout nombre algébrique* α*, pour tout* $\delta > 0$*, l'ensemble des* $\frac{r}{s} \in \mathbb{Q}$ *avec* $s = 2^k$ *qui satisfaisant* $|\alpha - \frac{r}{s}| \leq s^{-1-\delta}$ *est fini.*

Preuve. Dans la version p-adique du théorème du sous-espace de Schmidt, on prend $\nu = 2$, $p = 2$,

$$\begin{aligned} L_{1,\infty}(\mathbf{x}_1, \mathbf{x}_2) &= \mathbf{x}_1 \quad , \quad L_{2,\infty}(\mathbf{x}_1, \mathbf{x}_2) = \alpha\mathbf{x}_1 - \mathbf{x}_2 \\ L_{1,2}(\mathbf{x}_1, \mathbf{x}_2) &= \mathbf{x}_1 \quad , \quad L_{2,2}(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{x}_2 \end{aligned}$$

donc, pour $\mathbf{x} = (s, r)$

$$\begin{aligned} |L_{1,\infty}(\mathbf{x})| &= s \quad , \quad |L_{2,\infty}(\mathbf{x})| = |s\alpha - r| \\ |L_{1,2}(\mathbf{x})|_2 &= s^{-1} \quad , \quad |L_{2,2}(\mathbf{x})|_2 = |r|_2 \leq 1 \end{aligned}$$

Le théorème du sous-espace nous donne

$$\prod_{i=1}^{2} \left(|L_{i,\infty}(\mathbf{x})| \,.\, |L_{i,p}(\mathbf{x})|_2\right) = |s\alpha - r| \,.\, |r|_2 \leq s^{-\delta} \tag{2.23}$$

d'où

$$|\alpha - \frac{r}{s}| \leq s^{-1-\delta}$$

■

Chapitre 3

Etudes de la complexité et de la transcendance

Dans la première section de ce chapitre, on s'intéresse à l'étude de la version p-adique du théorème du Lamé connu dans le cas réel, ce théorème porte sur la complexité du développement en fraction continue d'un nombre rationnel.

Dans la deuxième section, on présente notre résultat principal sur la transcendance du développement en fraction continue p-adique de Thue-Morse d'un nombre p-adique, avec des conditions de combinatoire sur les coefficients du développement, pour cela on va utiliser la méthode de Ruban pour définir les fractions continues p-adiques.

3.1 Complexité des développements d'un nombre rationnel

Trois propriétés importantes caractérisant un nombre rationnel, c'est que son développement décimal et p-adique est ultimement périodique, et son développement en fraction continue réel est fini. Un thème très important dans la théorie des nombres est de trouver la longueur de la partie périodique et de la partie finie. C'est ce qu'on désigne par le mot "complexité".

3.1.1 Caractérisation d'un nombre rationnel

Un théorème important concernant la caractérisation d'un nombre rationnel par son développement de Hensel, est connu par l'énoncé suivant :

Théorème 3.1.1 *[12] Soit $x \in \mathbb{Q}_p$ donné par son développement de Hensel $\sum_{n=-j}^{+\infty} \alpha_n p^n$. Alors, $x \in \mathbb{Q}$ si et seulement si la suite de coefficients $(\alpha_n)_n$ est ultimement périodique.*

Preuve. Supposons que $(\alpha_n)_n$ est périodique de longueur de période égale m, d'où

$$x = \sum_{n=0}^{+\infty} \alpha_n p^n = \alpha_0 + \alpha_1 p + ... + \alpha_{m-1} p^{m-1} + \alpha_0 p^m + \alpha_1 p^{m+1} + ... + \alpha_{m-1} p^{2m} + ...$$

Le nombre $y = \alpha_0 + \alpha_1 p + ... + \alpha_{m-1} p^{m-1}$ est un entier naturel, et on peut écrire :

$$x = y.(1 + p^m + p^{2m} + ...) = y.\frac{1}{1 - p^m} \tag{3.1}$$

Donc x est nombre rationnel (le cas ultimement périodique peut en être déduit facilement).

Maintenant, supposons que $x = \dfrac{a}{b} = \sum_{n=0}^{+\infty} \alpha_n p^n$ est un nombre rationnel, et démontrons que la suite de coefficients $(\alpha_n)_n$ est ultimement périodique.
On peut considérer, sans perte de généralité, que $PGCD\,(a, b) = PGCD\,(p, b) = 1$. Soit l'entier naturel $y_k = \alpha_0 + \alpha_1 p + ... + \alpha_{k-1} p^{k-1}$, il est clair que

$$0 \leq y_k \leq p^k - 1$$

à l'aide de la division Euclidienne, on peut écrire

$$\frac{a}{b} = y_k + p^k \frac{r_k}{b}$$

avec r_k est un entier relatif. Alors

$$\frac{a - \left(p^k - 1\right) b}{p^k} \leq r_k = \frac{a - y_k b}{p^k} \leq \frac{a}{p^k} \tag{3.2}$$

donc, pour k assez grand, on a $-b \leq r_k \leq 0$, i.e.

$$r_k \in \mathbb{Z} \cap [-b, 0]$$

cela signifie que l'ensemble de valeurs de r_k est fini pour k assez grand.

D'autre part, on peut réécrire x sous la forme suivante

$$x = y_{k+1} + p^{k+1} \frac{r_{k+1}}{b} = y_k + \alpha_k p^k + p^{k+1} \frac{r_{k+1}}{b}$$

d'où

$$y_k + p^k \frac{r_k}{b} = y_k + \alpha_k p^k + p^{k+1} \frac{r_{k+1}}{b}$$

on aboutit à

$$r_k = \alpha_k b + p r_{k+1} \quad , \ \forall k \geq 0$$

On a $\exists! \nu \in \mathbb{N} : p^\nu = 1 \bmod b$, donc $\frac{1-p^\nu}{b} \in \mathbb{Z}$, ce qui veut dire que $\alpha = \frac{r_k(1-p^\nu)}{b} \in \mathbb{Z}$.

D'autre part :

$$\begin{aligned} -b \quad &\leq \quad r_k \leq 0 \Longrightarrow 0 \leq -\frac{r_k}{b} \leq 1 \Longrightarrow 0 \leq -\frac{r_k\,(p^\nu - 1)}{b\,(p^\nu - 1)} \leq 1 \\ &\Longrightarrow \quad 0 \leq \frac{y}{p^\nu - 1} \leq 1 \;\Longrightarrow 0 \leq y \leq p^\nu - 1 \quad , \quad \text{avec } y = \frac{r_k\,(1-p^\nu)}{b} \end{aligned}$$

alors $y = y_0 + y_1 p + ... + y_{\nu-1} p^{\nu-1}$. Ce qui donne :

$$\begin{aligned} \frac{r_k}{b} &= \frac{y}{1-p^\nu} = \left(y_0 + y_1 p + ... + y_{\nu-1} p^{\nu-1}\right)\left(1 + p^\nu + ... + p^{2\nu} + ...\right) \\ &= y_0 + y_1 p + ... + y_{\nu-1} p^{\nu-1} + y_0 p^\nu + ... + y_{\nu-1} p^{2\nu} + ... \end{aligned}$$

Donc $\frac{r_k}{b}$ est périodique, ainsi que $x = \frac{a}{b}$ est ultimement périodique.

et tant que r_k prend un nombre fini de valeurs, c'est-à-dire qu'a partir d'un certain rang m, il existe un entier ν tel que

$$\forall n \geq m : r_{n+\nu} = r_n$$

Alors

$$\forall n \geq m : \alpha_n b + p r_{n+1} = \alpha_{n+\nu} b + p r_{n+\nu+1} \tag{3.3}$$

donc

$$(\alpha_n - \alpha_{n+\nu})\, b = p\,(r_{n+\nu+1} - r_{n+1})$$

nous avons $PGCD\,(b,p) = 1$, alors p divise $(\alpha_n - \alpha_{n+\nu})$. Or que $\alpha_i \in \{0, 1, ..., p-1\}$, donc

$$\alpha_n - \alpha_{n+\nu} = 0, \forall n \geq m$$

ce qui veut dire que la suite de coefficients $(\alpha_n)_n$ est périodique à partir du rang m. ■

Remarque 3.1.2 *Cette propriété est vraie même pour le développement décimal, donc elle est indépendante du choix de la base dans laquelle on fait le développement.*

Exemple 3.1.3 *Soit $x \in \mathbb{Q}_5$, donné par le développement*

$$x = 2 + 3.5 + 1.5^2 + 3.5^3 + 1.5^4 + 3.5^5 + ...$$

ce développement 5-adique de x est périodique à partir du deuxième terme, donc $x \in \mathbb{Q}$. On sait d'après la formule (1.39) que $x = \frac{1}{3}$.

Exemple 3.1.4 *Dans $\mathbb{Q}_p$, on sait que*

$$-1 = (p-1) + (p-1)\,p + (p-1)\,p^2 + ... \tag{3.4}$$

Par exemple, dans $\mathbb{Q}_3$ nous avons

$$\begin{aligned} -1 &= 2 + 2.3 + 2.3^2 + ... \\ &= 0 \cdot 22222222222222222222 \end{aligned}$$

d'où

$$\begin{aligned} -\frac{1}{2} &= 1 + 3 + 3^2 + 3^3 + ... \\ &= 0 \cdot 111111111111111111111 \end{aligned}$$

c'est un nombre rationnel et son développement est purement périodique.

En utilisant la méthode de Browkin, le développement en fraction continues p-adiques d'un nombre rationnel est fini, comme dans le cas réel. Nous donnons ici la version p-adique du théorème de Lamé (2.2.11), c'est-à-dire une borne de la longueur de ce développement, ainsi on va donner aussi la longueur de la partie non stationnaire du développement en fraction continue de Schneider .

Browkin dans son article [25] a posé deux questions liés au développement en fraction continue d'un nombre p-adique :

Question1. Est-ce que le développement en fraction continue d'un nombre rationnel est fini ? Si la réponse est non, peut-on déterminer les fractions continues infinies qui correspondent à des nombres rationnels ?

Question2. Est-ce que le développement en fraction continue d'un nombre p-adique quadratique est ultimement périodique (Théorème de Lagrange) ?

La réponse de la deuxième question est "**Non**" dans le cas général, "**Oui**" pour des cas particuliers, voir par exemple : [17, 18, 19, 20], [25], [27], [29], [31], [32], [41], [46], [61], [66].

La réponse de la première question est "**Oui**" pour la définition de Browkin, "**Non**" pour les autres définitions. On donne dans la suite l'énoncé de trois théorèmes qui caractérise les développements en fractions continues d'un nombre rationnel :
Le premier théorème dû à Bundschuh, qui a démontré dans [27] le résultat suivant, en utilisant les FCS :

Théorème 3.1.5 (Bundschuh) *Soit $r \in \mathbb{Q}$, alors le développement de r en FCS est*

stationnaire, d'où il est ultimement périodique. Plus précisément

$$\exists j_0 \geq 0, \forall j > j_0 : \ n_j = 1 \quad et \quad b_j = p-1.$$

i.e.

$$\begin{aligned} r &= \begin{bmatrix} p^{n_0}, & p^{n_1}, & ... & p^{n_{j_0}}, & \overline{p} \\ b_0; & b_1, & ... & b_{j_0}, & \overline{p-1} \end{bmatrix} \\ &= b_0 + \cfrac{p^{n_0}}{b_1 + \cfrac{p^{n_1}}{...b_{j_0} + \cfrac{p^{n_{j_0}}}{p-1+\cfrac{p}{p-1+\cfrac{p}{p-1+...}}}}} \end{aligned}$$

Le deuxième théorème dû à Laohakosol [41], c'était bien le premier qui a caractérisé les nombres rationnels avec leurs FCR :

Théorème 3.1.6 (Laohakosol) *Soit $r \in \mathbb{Q}$, alors le développement de r en FCR est fini ou périodique de la forme*

$$\begin{aligned} r &= \left[b_0; b_1, b_2, ..., b_{j_0}, \overline{(p-1)(1+p^{-1})}\right] \\ &= b_0 + \cfrac{1}{b_1 + \cfrac{1}{...b_{j_0} + \cfrac{1}{(p-1)(1+p^{-1}) + \cfrac{1}{(p-1)(1+p^{-1}) + \cfrac{1}{(p-1)(1+p^{-1})+...}}}}} \end{aligned}$$

Le troixième dû à Browkin [25], dont il a prouvé le résultat suivant, en utilisant les FCB :

Théorème 3.1.7 (Browkin) *Soit $r \in \mathbb{Q}$, alors le développement de r en FCB est fini.*

$$r = [a_0; a_1, a_2, ..., a_{j_0}]$$

D'après les énoncés et les théorèmes précédents, on aura trois problèmes ouverts suivants :

Problème1 Comment définir des développements en fractions continues p-adiques tels que la suite des quotients partiels $(a_n)_{n\in\mathbb{N}}$ soit finie pour tout rationnel ?

Problème2 Pour calculer les fractions continues p-adiques, on utilise le développement de Hensel qui est infini, donc on ne peut pas faire un algorithme fini. Comment définir un algorithme "fini" du développement en fraction continue p-adique d'un nombre rationnel ?

Problème3 (Sur la complexité du développement, ou version p-adique du théorème de **Lamé**)
Quel est le cardinal de l'ensemble

$$\left\{ n \in \mathbb{N} \diagup a_n = \langle r_n \rangle_p , a_0 = \langle r \rangle_p \right\}$$

pour $r \in \mathbb{Q}$; i.e. quelle est la longueur de la suite des quotients partiels $(a_n)_{n\in\mathbb{N}}$?

Afin d'obtenir des réponses à ces problèmes, on va définir des algorithmes pour un nombre rationnel donné $r \in \mathbb{Q}$, ces algorithmes vont nous aider à calculer les coefficients du développement de Hensel de ce nombre, et les quotients partiels du développement en fraction continue.

3.1.2 Complexité du développement de Hensel

Définition 3.1.8 *Soit $r = \frac{c}{d} \in \mathbb{Q}^+$, avec $c \in \mathbb{N}$, $d \in \mathbb{N}^*$, et c, d, p sont premiers entre eux. On définit une suite $(\beta_i)_{i\in\mathbb{N}}$ par*

$$\begin{cases} \beta_0 = c \\ \\ \beta_{i+1} = \dfrac{\beta_i - \alpha_i d}{p} \in \mathbb{Z} \\ \\ \alpha_i = \beta_i d^{-1} \bmod p \end{cases} \tag{3.5}$$

Proposition 3.1.9 *[21] La suite $(\alpha_i)_{i\in\mathbb{N}}$ donnée par la formule (3.5) détermine bien les coefficients du développement de Hensel de $\frac{c}{d}$.*

Preuve. On démontre par récurrence. On suppose que le développement de Hensel de $\frac{c}{d}$ est connu, et est donné par

$$\begin{aligned} \frac{c}{d} &= \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_i p^i + ... \\ \text{avec } \alpha_i &\in \{0, 1, .., p-1\} \quad \forall i \in \mathbb{N} \end{aligned}$$

Commençons par le premier terme, on a

$$\begin{aligned}\frac{c}{d} &= \alpha_0 + p\left(\alpha_1 + \alpha_2 p + ... + \alpha_i p^{i-1} + ...\right) \\ &= \alpha_0 \bmod p\end{aligned}$$

donc

$$\alpha_0 = cd^{-1} \bmod p = \beta_0 d^{-1} \bmod p \tag{3.6}$$

Pour le deuxième terme, on a

$$\begin{aligned}\frac{c}{d} &= \alpha_0 + \alpha_1 p + p^2\left(\alpha_2 + \alpha_3 p + ... + \alpha_i p^{i-2} + ...\right) \\ &= (\alpha_0 + \alpha_1 p) \bmod p^2\end{aligned}$$

d'où

$$\beta_1 = \frac{c - \alpha_0 d}{p} = \alpha_1 d \bmod p$$

Enfin

$$\alpha_1 = \beta_1 d^{-1} \bmod p \tag{3.7}$$

On fait la même chose pour les autres termes, on suppose que $\alpha_i = \beta_i d^{-1} \bmod p$ et $\beta_{i+1} = \dfrac{\beta_i - \alpha_i d}{p}$. On a

$$\begin{aligned}\alpha_i &= \beta_i d^{-1} \bmod p \Longrightarrow \alpha_{i+1} p + \alpha_i = \beta_i d^{-1} \bmod p \\ &\Longrightarrow \alpha_{i+1} p = \left(\beta_i d^{-1} - \alpha_i\right) \bmod p \\ &\Longrightarrow \alpha_{i+1} = \left(\frac{\beta_i - \alpha_i d}{p}\right) d^{-1} \bmod p = \beta_{i+1} d^{-1} \bmod p\end{aligned}$$

donc $\forall i \geq 0 : \alpha_i = \beta_i d^{-1} \bmod p$.
Supposons maintenant qu'on ne connaît pas les coefficients du développement de Hensel de $\frac{c}{d}$. Pour calculer ces coefficients, on commence par la division Euclidienne de $\frac{c}{d}$ sur p, on aura

$$\exists \alpha_0 \in \{0, 1, .., p-1\}, \exists \lambda_0 \in \mathbb{Z} \text{ tel que } \frac{c}{d} = \frac{\lambda_0}{d} p + \alpha_0 \tag{3.8}$$

il vient que

$$c = \lambda_0 p + \alpha_0 d$$

On met

$$\beta_1 = \lambda_0 = \frac{c - \alpha_0 d}{p} \in \mathbb{Z}$$

On refait la division Euclidienne pour $\frac{\beta_1}{d}$ sur p, on aura

$$\exists \alpha_1 \in \{0,1,..,p-1\}, \exists \lambda_1 \in \mathbb{Z} \text{ tel que } \frac{\beta_1}{d} = \frac{\lambda_1}{d}p + \alpha_1$$

il vient que

$$\beta_1 = \lambda_1 p + \alpha_1 d$$

On met

$$\beta_2 = \lambda_1 = \frac{\beta_1 - \alpha_1 d}{p} \in \mathbb{Z} \tag{3.9}$$

il est clair que

$$\alpha_1 = \beta_1 d^{-1} \bmod p$$

Ainsi, nous avons construit deux suites $(\alpha_i)_{i\in\mathbb{N}}, (\beta_i)_{i\in\mathbb{N}}$ définies par

$$\begin{cases} \beta_0 = c \\ \\ \beta_{i+1} = \dfrac{\beta_i - \alpha_i d}{p}, \forall i \in \mathbb{N} \\ \\ \alpha_i = \beta_i d^{-1} \bmod p, \forall i \in \mathbb{N} \end{cases}$$

et de plus on a défini le développement de Hensel de $\frac{c}{d}$

$$\frac{c}{d} = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + ... + \alpha_i p^i + ...$$

avec $\alpha_i \in \{0,1,..,p-1\} \quad \forall i \in \mathbb{N}$ ■

Lemme 3.1.10 *[21] Avec les donnés de la définition (3.1.8), on a*

$$c = d\left(\sum_{n=0}^{i-1} \alpha_n p^n\right) + \beta_i p^i \qquad , \quad \forall i \in \mathbb{N}^* \tag{3.10}$$

Preuve. On démontre ce lemme aussi par récurrence.
Pour $i = 1$ c'est évident

$$d\left(\sum_{n=0}^{0} \alpha_n p^n\right) + \beta_1 p = d\alpha_0 + \left(\frac{c - \alpha_0 d}{p}\right) p = c$$

Supposons que la relation est vraie pour i. D'aprés (3.5), on a $\beta_i = \alpha_i d + \beta_{i+1} p$.

Alors

$$\begin{aligned} c &= d\left(\sum_{n=0}^{i-1}\alpha_n p^n\right)+\beta_i p^i \\ &= d\left(\sum_{n=0}^{i-1}\alpha_n p^n\right)+\left(\beta_{i+1}p+\alpha_i d\right)p^i \\ &= d\left(\sum_{n=0}^{i}\alpha_n p^n\right)+\beta_{i+1}p^{i+1} \end{aligned}$$

Donc la relation est vrai $\forall\ n \geq 0$. ■

Pour démontrer que l'algorithme de calcul des coefficients s'arrête au bout d'un certain rang, il suffit de montrer que la suite $(|\beta_n|)_n$ est bornée ou décroissante.

Proposition 3.1.11 (Belhadef et Esbelin [21]) *La suite $(\beta_i)_{i\in\mathbb{N}}$ donné dans (3.5) vérifie les deux cas suivants :*
Cas1 : *Si $c < d$ (i.e. $0 \leq \frac{c}{d} < 1$), alors*

$$0 \leq |\beta_i| < d \quad , \quad \forall i \in \mathbb{N}$$

Cas2 : *Si $c > d$ (i.e. $\frac{c}{d} > 1$), alors pour*

$$m = \left\lceil \frac{\log\left(\dfrac{c(p-1)}{2dp}\right)}{\log p} \right\rceil$$

on a

$$\begin{cases} d \leq |\beta_i| \leq c & \text{pour} \quad 0 \leq i < m+1 \\ 0 \leq |\beta_i| < d & \text{pour} \quad m+1 \leq i \end{cases}$$

Preuve. Cas1 : On utilise la démonstration par récurrence. Pour $i = 0$ c'est trivial. Supposons qu'on a $|\beta_i| < d$, on va montrer que $\left|\beta_{i+1}\right| < d$. En effet, on a

$$\begin{aligned} \left|\beta_{i+1}\right| &= \left|\frac{\beta_i - \alpha_i d}{p}\right| \leq \frac{1}{p}\left|\beta_i\right| + \frac{1}{p}\left|\alpha_i d\right| \\ &< \frac{1}{p}d + \frac{p-1}{p}d = d \end{aligned}$$

Cas2 : On peut facilement démontrer par récurrence que $|\beta_i| \leq c$, $\forall i \in \mathbb{N}$. On va démontrer par l'absurde que

$$d \leq |\beta_i| \quad \text{pour tous } 0 \leq i \leq m+1$$

En effet, supposons qu'il existe $0 < k \leq m+1$ tel que $|\beta_k| < d$, c'est-à-dire que $-d < \beta_k < d$. D'après le lemme (3.1.10) on aboutit à

$$d\left(\sum_{n=0}^{k-1}\alpha_n p^n\right) - dp^k < c < d\left(\sum_{n=0}^{k-1}\alpha_n p^n\right) + dp^k$$

d'où

$$\begin{aligned} c &< d(p + p.p + ... + p.p^{k-1} + p^k) \Longleftrightarrow c < dp(1 + p + ... + p^{k-1} + p^{k-1}) \\ &\Longleftrightarrow c < dp\left(\frac{p^k - 1}{p-1} + p^{k-1}\right) \Longleftrightarrow c < \frac{dp}{p-1}\left(2p^k - p^{k-1} - 1\right) \\ &\Longleftrightarrow c < \frac{2p^{k+1}d}{p-1} \end{aligned}$$

donc

$$\frac{\log\left(\dfrac{c(p-1)}{2dp}\right)}{\log p} < k$$

alors

$$m+1 = \left[\frac{\log\left(\dfrac{c(p-1)}{2dp}\right)}{\log p}\right] + 1 \leq k \tag{3.11}$$

supposons que $m+1 = k$, on trouve que $c(p-1) = 2dp^k$. Cela signifie que p divise c, contradiction. Donc $k \geq m+2$, qui est lui même contradiction. Donc

$$\forall i = \overline{0, m+1} : d \leq |\beta_i| \leq c$$

Pour la deuxième partie, supposons qu'il existe $k \geq m+2$ tel que $|\beta_k| \geq d$, i.e.

$$\beta_k \geq d \quad \text{ou} \quad \beta_k \leq -d$$

d'après le lemme (3.1.10), on a

$$c \geq d\left(\sum_{n=0}^{k-1}\alpha_n p^n\right) + dp^k \geq dp^k \tag{3.12}$$

d'où

$$\frac{c(p-1)}{2dp} \geq \frac{(p-1)}{2}p^{k-1} \geq p^{k-2}$$

donc

$$\frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p} \geq k-2$$

alors

$$m+2 = \left[\frac{\log\left(\frac{c(p-1)}{2dp}\right)}{\log p}\right] + 2 \geq k$$

supposons que $m+2=k$, on trouve que $c(p-1) = 2dp^{k-1}$. C'est-à-dire que p divise c, et c'est une contradiction. D'où $m+2>k$, qui est aussi une contradiction. Ce qui veut dire que $d \leq |\beta_i| \leq c$, pour tous $0 \leq i \leq m+1$. ■

3.1.3 Complexité du développement en FCB

Maintenant, on donne un algorithme de calcul des quotients partiels du développement en fraction continue p-adique de Browkin (FCB) d'un nombre rationnel, puis on détermine la complexité du développement :

Définition 3.1.12 *Soit $r = \frac{a}{b} \in \mathbb{Q}$, on peut l'écrire sous la forme $r = \frac{\alpha}{\beta p^{k_0}}$, avec $k \in \mathbb{N}$ et $\alpha \in \mathbb{N}$, $\beta \in \mathbb{N}^*$, et α, β, p sont premiers entre eux. Soit le développement de $\frac{\alpha}{\beta}$ donné par (2.14)*

$$\frac{\alpha}{\beta} = u_0 + u_1 p + u_2 p^2 + ... + u_{k_0}p^{k_0} + u_{k_0+1}p^{k_0+1} + ...$$

on met

$$x_0 = u_0 + u_1 p + u_2 p^2 + ... + u_{k_0}p^{k_0} \in \mathbb{Z} \cap \left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[\tag{3.13}$$

d'où

$$r = \frac{u_0}{p^{k_0}} + \frac{u_1}{p^{k_0-1}} + ... + u_{k_0} + u_{k_0+1}p + u_{k_0+2}p^2 + ...$$

alors

$$\langle r \rangle_p = \frac{u_0}{p^{k_0}} + \frac{u_1}{p^{k_0-1}} + ... + u_{k_0} = \frac{x_0}{p^{k_0}} \qquad et \qquad a_0 = \langle r \rangle_p = \frac{x_0}{p^{k_0}} \tag{3.14}$$

d'autre part on a

$$\begin{aligned} \alpha - x_0\beta &= 0 \bmod p^{k_0+1} \Longleftrightarrow \frac{\alpha - x_0\beta}{p^{k_0}} = 0 \bmod p \\ &\Longleftrightarrow \frac{\alpha - x_0\beta}{p^{k_0}} \in \mathbb{Z} \ , \ et \ \frac{\alpha - x_0\beta}{p^{k_0}} = \beta_1 p^{k_1} \end{aligned}$$

avec $p \wedge \beta_1 = 1$, $k_1 = v_p\left(\dfrac{\alpha - x_0\beta}{p^{k_0}}\right) \in \mathbb{N}^*$.
On calcul r_1

$$\begin{cases} r_1 = \dfrac{1}{r - a_0} = \dfrac{1}{\frac{\alpha}{\beta p^{k_0}} - \frac{x_0}{p^{k_0}}} = \dfrac{\beta}{\beta_1 p^{k_1}} \\ a_1 = \langle r_1 \rangle_p = \dfrac{x_1}{p^{k_1}} \\ x_1 = \beta_0\beta_1^{-1} \bmod p^{1+k_1} \quad , \quad avec \quad x_1 \in \mathbb{Z} \cap \left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[\end{cases}$$

Puis on cherche $k_2 = v_p\left(\dfrac{\beta_0 - x_1\beta_1}{p^{k_1}}\right)$.
on calcul r_2

$$r_2 = \frac{1}{r_1 - a_1} = \frac{\beta_1}{\beta_2 p^{k_2}} \quad , \quad avec \quad \beta_2 = \frac{\beta_0 - x_1\beta_1}{p^{k_1}p^{k_2}} \tag{3.15}$$

Alors, les formes générales sont les suivantes

$$\begin{cases} \beta_0 = \beta, \beta_{-1} = \alpha \qquad et \qquad \beta_{n+1} = \dfrac{\beta_{n-1} - x_n\beta_n}{p^{k_n}p^{k_{n+1}}} \\ x_n \equiv \beta_{n-1}\beta_n^{-1} \bmod p^{1+k_n} \quad , \quad avec \quad x_n \in \mathbb{Z} \cap \left[\frac{1}{p}\right] \cap \left]-\frac{p}{2}, \frac{p}{2}\right[\\ r_n = \dfrac{\beta_{n-1}}{\beta_n p^{k_n}} \qquad et \qquad a_n = \langle r_n \rangle_p = \dfrac{x_n}{p^{k_n}} \\ k_{n+1} = v_p\left(\dfrac{\beta_{n-1} - x_n\beta_n}{p^{k_n}}\right) \end{cases}$$

Pour démontrer le théorème (3.1.14), on a besoin du lemme suivant :

Lemme 3.1.13 *Soit* $(\theta_i)_{i\in\mathbb{N}}$ *une suite récurrente linéaire définie par*

$$\theta_{i+1} = \frac{1}{2}\theta_i + \frac{1}{p^2}\theta_{i-1},\ \theta_0 = |\beta_0|\,,\ \theta_1 = |\beta_1|\,.$$

Si $|x_n| \leq \dfrac{p^{1+k_n} - 1}{2}$ *, alors la suite* $(\theta_i)_{i\in\mathbb{N}}$ *vérifie les deux assertions suivantes :*
1) $\forall i \geq 2 : \ |\beta_i| \leq \theta_i$.
2) $\lim\limits_{i\to+\infty} \theta_i = 0$.

Preuve. 1) On démontre par récurrence. Nous avons

$$|x_n| \leq \frac{p^{1+k_n}-1}{2} < \frac{p^{1+k_n}}{2}$$

donc

$$\left|\beta_{n+1}\right| \leq \frac{1}{p^{k_n}p^{k_{n+1}}}\left(\left|\beta_{n-1}\right| + |x_n|\,|\beta_n|\right) < \frac{1}{p^2}\left|\beta_{n-1}\right| + \frac{1}{2}|\beta_n| \tag{3.16}$$

pour $i = 2$ on a

$$|\beta_2| \leq \frac{1}{p^2}|\beta_0| + \frac{1}{2}|\beta_1| \ < \theta_2$$

Supposons que $|\beta_i| \leq \theta_i$, et on démontre que $\left|\beta_{i+1}\right| \leq \theta_{i+1}$, on a

$$\left|\beta_{n+1}\right| < \frac{1}{p^2}\left|\beta_{n-1}\right| + \frac{1}{2}|\beta_n| < \frac{1}{p^2}\theta_{i-1} + \frac{1}{2}\theta_i = \theta_{i+1}$$

donc la propriété $|\beta_i| \leq \theta_i$ est vrai $\forall i \geq 2$.
2) Le polynôme caractéristique de la suite $(\theta_i)_{i\in\mathbb{N}}$ est donné par

$$2p^2X^2 - p^2X - 2 = 0 \tag{3.17}$$

ce polynôme admet deux racines réelles

$$\lambda_1 = \frac{p+\sqrt{p^2+16}}{4p} \qquad \text{et} \qquad \lambda_2 = \frac{p-\sqrt{p^2+16}}{4p},$$

le terme général de la suite s'écrit

$$\theta_i = \left(\frac{|\beta_1| - \lambda_2|\beta_0|}{\lambda_1-\lambda_2}\right)\lambda_1^i + \left(\frac{|\beta_1| + \lambda_1|\beta_0|}{\lambda_1-\lambda_2}\right)\lambda_2^i \tag{3.18}$$

donc $\lim\limits_{i\longrightarrow+\infty}\theta_i = 0$ puisque $0 < \lambda_1 < 1$, $\dfrac{-1}{2} < \lambda_2 < 0$. ■

Proposition 3.1.14 (Belhadef et Esbelin [21]) *Si* $|x_n| \leq \dfrac{p^{1+k_n}-1}{2}$ *, alors l'ensemble*

$$\left\{n \in \mathbb{N} \diagup a_n = \langle r_n\rangle_p = \frac{x_n}{p^{k_n}}\right\}$$

est fini, et son cardinal est majoré par la partie entière réel du nombre

$$\frac{1}{\log\lambda_1}\left(\log\frac{1}{2} - \log\left(\frac{2|\beta_1|}{\lambda_1-\lambda_2} + |\beta_0|\right)\right) \tag{3.19}$$

avec λ_1 *et* λ_2 *sont les racines du polynôme* $2p^2X^2 - p^2X - 2 = 0$.

Preuve. Nous avons d'après le lemme précédent $\lim_{i \longrightarrow +\infty} \theta_i = 0$, donc

$$\exists N \in \mathbb{N} : i > N \Longrightarrow |\beta_i| < \theta_i < \frac{1}{2} \tag{3.20}$$

Mais on sait que $(|\beta_i|)_i$ est une suite de nombres naturels, donc $|\beta_i| = 0$, $\forall i > N$.
Ce qui démontre, que l'algorithme de calcul des $(a_n)_{n\in\mathbb{N}}$ s'arrête au bout d'un certain rang N ; donc l'ensemble $\left\{ n \in \mathbb{N} \diagup a_n = \langle r_1 \rangle_p = \frac{x_n}{p^{k_n}} \right\}$ est fini.
On va démontrer que

$$card \left\{ n \in \mathbb{N} \diagup a_n = \langle r_1 \rangle_p = \frac{x_n}{p^{k_n}} \right\} \leq \left[\frac{\log \frac{1}{2} - \log \left(\frac{2\,|\beta_1|}{\lambda_1 - \lambda_2} + |\beta_0| \right)}{\log \lambda_1} \right]$$

D'après toujours le lemme précédent, nous avons

$$\exists N \in \mathbb{N} : i > N \Longrightarrow \theta_i < \frac{1}{2}$$

D'autre part on a

$$|\lambda_2| < \lambda_1 \Longleftrightarrow \left|\lambda_2^i\right| \left(\frac{|\beta_1| + \lambda_1\,|\beta_0|}{\lambda_1 - \lambda_2} \right) < \lambda_1^i \left(\frac{|\beta_1| + \lambda_1\,|\beta_0|}{\lambda_1 - \lambda_2} \right) \tag{3.21}$$

donc

$$\begin{aligned} |\theta_i| &= \left| \left(\frac{|\beta_1| - \lambda_2\,|\beta_0|}{\lambda_1 - \lambda_2} \right) \lambda_1^i + \left(\frac{\lambda_1\,|\beta_0| + |\beta_1|}{\lambda_1 - \lambda_2} \right) \lambda_2^i \right| \\ &< \left(\frac{|\beta_1| - \lambda_2\,|\beta_0|}{\lambda_1 - \lambda_2} \right) \lambda_1^i + \left(\frac{|\beta_1| + \lambda_1\,|\beta_0|}{\lambda_1 - \lambda_2} \right) \lambda_1^i \\ &< \lambda_1^i \left(\frac{2\,|\beta_1|}{\lambda_1 - \lambda_2} + |\beta_0| \right) \end{aligned}$$

C'est-à-dire, pour que $\theta_i < \frac{1}{2}$, il suffit que

$$\log \left(\lambda_1^i \left(\frac{2\,|\beta_1|}{\lambda_1 - \lambda_2} + |\beta_0| \right) \right) \leq \log \frac{1}{2}$$

encore que

$$i \geq \frac{\log \frac{1}{2} - \log\left(\frac{2\,|\beta_1|}{\lambda_1 - \lambda_2} + |\beta_0|\right)}{\log \lambda_1} \tag{3.22}$$

On prend donc

$$N = \left[\frac{\log \frac{1}{2} - \log\left(\frac{2\,|\beta_1|}{\lambda_1 - \lambda_2} + |\beta_0|\right)}{\log \lambda_1} \right]$$

■

3.1.4 Complexité du développement en FCS

Pour le développement en fraction continue p-adique de Schneider (FCS) d'un nombre rationnel, on donne ici un algorithme de calcul des quotients partiels de ce développement, puis on détermine la complexité de la partie non stationnaire :

Définition 3.1.15 *Soit $r = \frac{a}{b} \in \mathbb{Q}$, avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et a , b, p sont premiers entre eux. On définit une suite $(y_m)_m$ par la relation de récurrence suivante :*

$$\begin{cases} y_{-1} = a \quad , \quad y_0 = b \\ \\ y_m = \dfrac{y_{m-1}}{x_m} \in \mathbb{Z} \end{cases} \tag{3.23}$$

C'est-à-dire qu'on a

$$\frac{y_m}{y_{m-1}} = \frac{1}{x_m} = \frac{x_{m-1} - b_{m-1}}{p^{n_{m-1}}}$$

On peut aussi calculer les termes de la suite $(y_m)_m$ par la méthode suivante :

Algorithme 3.1.16 *On cherche $b_0 \in \{0, 1, 2, ..., p-1\}$ et $\alpha_0 \in \mathbb{N}$ tel que*

$$y_1 = \frac{a - b_0 b}{p^{\alpha_0}}$$

est un entier premier avec b et p. Puis, on cherche $b_1 \in \{1, 2, ..., p-1\}$ et $\alpha_1 \in \mathbb{N}^*$ tel que

$$y_2 = \frac{y_0 - b_1 y_1}{p^{\alpha_1}}$$

est un entier premier avec b et p.

Ainsi, on définit la suite récurrente $(y_m)_m$ *par*

$$y_{m+1} = \frac{y_{m-1} - b_m y_m}{p^{\alpha_m}} \tag{3.24}$$

avec p *,*y_{m-1}*,* y_m*,* y_{m+1} *sont premiers entre eux, et* $b_m \in \{1, 2, ..., p-1\}$ *et* $\alpha_m \in \mathbb{N}^*$*.*
On peut retirer la formule suivante à partir de la précédente

$$\frac{y_{m-1}}{y_m} = b_m + p^{\alpha_m}\frac{y_{m+1}}{y_m} = b_m + \cfrac{p^{\alpha_m}}{\cfrac{y_m}{y_{m+1}}}$$

D'où, on aura

$$\frac{a}{b} = b_0 + \cfrac{p^{\alpha_0}}{b_1 + \cfrac{p^{\alpha_1}}{...b_m + \cfrac{p^{\alpha_m}}{\cfrac{y_m}{y_{m+1}}}}} \tag{3.25}$$

En utilisant l'écriture matricielle des fractions continues, donné dans la section 2 du deuxième chapitre, on obtient la formule

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b_0 & p^{\alpha_0} \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b_1 & p^{\alpha_2} \\ 1 & 0 \end{pmatrix}..\begin{pmatrix} b_m & p^{\alpha_m} \\ 1 & 0 \end{pmatrix}\begin{pmatrix} y_m \\ y_{m+1} \end{pmatrix}$$

Notons par M_n *la matrice*

$$M_m = \begin{pmatrix} b_0 & p^{\alpha_0} \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b_1 & p^{\alpha_2} \\ 1 & 0 \end{pmatrix}..\begin{pmatrix} b_m & p^{\alpha_m} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} U_m & V_m \\ W_m & Z_m \end{pmatrix}$$

Ce qui implique la relation de récurrence suivante

$$M_m = M_{m-1}\begin{pmatrix} b_m & p^{\alpha_m} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} U_{m-1} & V_{m-1} \\ W_{m-1} & Z_{m-1} \end{pmatrix}\begin{pmatrix} b_m & p^{\alpha_m} \\ 1 & 0 \end{pmatrix} \tag{3.26}$$

avec les condition initiales

$$M_{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad M_0 = \begin{pmatrix} b_0 & p^{\alpha_0} \\ 1 & 0 \end{pmatrix}$$

donc, on aboutit au système suivant

$$\begin{cases} U_m = b_m U_{m-1} + V_{m-1} \quad , \quad V_m = p^{\alpha_m} U_{m-1} \\ W_m = b_m W_{m-1} + Z_{m-1} \quad , \quad Z_m = p^{\alpha_m} W_{m-1} \end{cases}$$

i.e

$$\begin{cases} U_m = b_m U_{m-1} + p^{\alpha_{m-1}} U_{m-2} \\ W_m = b_m W_{m-1} + p^{\alpha_{m-1}} W_{m-2} \end{cases} \tag{3.27}$$

Bundschuh a démontré que le développement d'un nombre rationnel en FCS est stationnaire, i.e.

$$\exists k \geq 0, \forall j > k : \ n_j = 1 \quad \text{et} \quad b_j = p - 1.$$

Dans la proposition suivante, on va calculer la valeur de k. Autrement dit, la longueur de la partie non stationnaire :

Proposition 3.1.17 (Belhadef et Esbelin [21]) *Soient $p \geq 3$, et $r = \dfrac{a}{b} \in \mathbb{Q}$, donné par son développement en FCS qui est stationnaire (d'après Bundschuh). Donc la longueur de la partie non stationnaire est égale à*

$$k = \left\lfloor \frac{\ln |\theta|}{\ln \left| \dfrac{T_2}{T_1} \right|} \right\rfloor + 1$$

avec

$$\theta = \frac{(T_1 - p)\left(a + \frac{1}{2} b \left(\sqrt{4p+1} - 1\right)\right)}{(T_2 - p)\left(a - \frac{1}{2} b \left(\sqrt{4p+1} + 1\right)\right)}$$

et T_1, T_2 sont les racines de l'équation $T^2 - T - p = 0$. Avec $b_j = 1$, $\alpha_j = 1$ $\forall j \leq k$

Preuve. Dans le cas stationnaire des FCS d'un rationnel, il existe $k \in \mathbb{N}^*$ tels que $\forall m \geq k : |y_m| = 1$, $b_m = p - 1$, $\alpha_{m+1} = 1$. D'où

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} b_0 & p^{\alpha_0} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b_1 & p^{\alpha 1} \\ 1 & 0 \end{pmatrix} .. \begin{pmatrix} b_k & p^{\alpha_k} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \pm 1 \\ \mp 1 \end{pmatrix} \\ &= M_k \begin{pmatrix} \pm 1 \\ \pm 1 \end{pmatrix} = \begin{pmatrix} U_k & V_k \\ W_k & Z_k \end{pmatrix} \begin{pmatrix} \pm 1 \\ \mp 1 \end{pmatrix} \end{aligned}$$

Donc pour $b_j = 1$, $\alpha_j = 1$ $\forall j \leq k$, ce qui donne

$$\begin{pmatrix} a \\ b \end{pmatrix} = M_k \begin{pmatrix} +1 \\ -1 \end{pmatrix} = \begin{pmatrix} U_k & V_k \\ W_k & Z_k \end{pmatrix} \begin{pmatrix} +1 \\ -1 \end{pmatrix} \tag{3.28}$$

Alors, on trouve

$$\begin{cases} a = U_k - V_k = U_k - pU_{k-1} \\ b = W_k - Z_k = W_k - pW_{k-1} \end{cases} \tag{3.29}$$

Et le système (3.27) devient

$$\begin{cases} U_n = U_{n-1} + pU_{n-2} \\ W_n = W_{n-1} + pW_{n-2} \end{cases}$$

donc $(U_n)_n$ et $(W_n)_n$ sont deux suites récurrentes linéaires, dont les formes générales sont les suivantes

$$\begin{cases} U_n = \left(\frac{1}{2} + \frac{1}{2\sqrt{4p+1}}\right) T_2^k + \left(\frac{1}{2} - \frac{1}{2\sqrt{4p+1}}\right) T_1^k \\ W_n = \left(\frac{1}{\sqrt{4p+1}}\right) \left[T_2^k - T_1^k\right] \end{cases}$$

avec les premiers termes : $U_0 = 1$, $U_1 = 1$, $W_0 = 0$, $W_1 = 1$. Et T_2, T_1 sont les racines de l'équation caractéristique : $T^2 - T - p = 0$, ils sont données par

$$\begin{cases} T_1 = \dfrac{1 - \sqrt{4p+1}}{2} \\ T_2 = \dfrac{1 + \sqrt{4p+1}}{2} \end{cases} \tag{3.30}$$

Revenons à la formule (3.29), on obtient

$$\begin{cases} a = U_k - pU_{k-1} = \left(\dfrac{\sqrt{4p+1}+1}{2\sqrt{4p+1}}\right) T_2^{k-1}(T_2 - p) + \left(\dfrac{\sqrt{4p+1}-1}{2\sqrt{4p+1}}\right) T_1^{k-1}(T_1 - p) \\ b = W_k - pW_{k-1} = \left(\dfrac{1}{\sqrt{4p+1}}\right) \left(T_2^{k-1}(T_2 - p) - T_1^{k-1}(T_1 - p)\right) \end{cases}$$

On fait la division des deux nombres

$$\frac{a}{b} = \frac{\left(\sqrt{4p+1}+1\right) T_2^{k-1}(T_2 - p) + \left(\sqrt{4p+1}-1\right) T_1^{k-1}(T_1 - p)}{2\left(T_2^{k-1}(T_2 - p) - T_1^{k-1}(T_1 - p)\right)}$$

alors

$$T_2^{k-1}(T_2 - p)\left(a - \frac{1}{2}b\left(\sqrt{4p+1}+1\right)\right) = T_1^{k-1}(T_1 - p)\left(a + \frac{1}{2}b\left(\sqrt{4p+1}-1\right)\right)$$

donc

$$\frac{T_2^{k-1}}{T_1^{k-1}} = \frac{(T_1 - p)\left(a + \frac{1}{2}b\left(\sqrt{4p+1}-1\right)\right)}{(T_2 - p)\left(a - \frac{1}{2}b\left(\sqrt{4p+1}+1\right)\right)} \tag{3.31}$$

d'où

$$\left(\left|\frac{T_2}{T_1}\right|\right)^{k-1} = \left|\frac{(T_1 - p)\left(a + \frac{1}{2}b\left(\sqrt{4p+1}-1\right)\right)}{(T_2 - p)\left(a - \frac{1}{2}b\left(\sqrt{4p+1}+1\right)\right)}\right|$$

Enfin

$$k = \left[\frac{\ln |\theta|}{\ln \left| \frac{T_2}{T_1} \right|} \right] + 1 \tag{3.32}$$

avec

$$\theta = \frac{(T_1 - p)\left(a + \frac{1}{2}b\left(\sqrt{4p+1} - 1\right)\right)}{(T_2 - p)\left(a - \frac{1}{2}b\left(\sqrt{4p+1} + 1\right)\right)}$$

il est clair que $|T_2| > |T_1|$, donc il faut que $|\theta| > 1$, pour que k soit bien définir. Or que nous avons les deux cas suivants :
*) Si $b \geq 1$ et $a > \frac{1}{2}b\left(\sqrt{4p+1} + 1\right)$, alors $\theta > 1$.
**) Si $b \leq -1$ et $a > b\,(1-p)$, alors $\theta > 1$. ■

3.2 Etude de la transcendance

Dans cette section, on va donner des conditions suffisantes pour qu'un nombre p-adique défini par son développement en fraction continue soit rationnel, irrationnel quadratique ou transcendant, en utilisant la version p-adique du théorème de sous-espace de Schmidt due à Schlickewei.

3.2.1 Transcendance d'un développement en FCB

Dans son deuxième article [26], Browkin a donné un autre algorithme pour que le développement en FCB d'un nombre p-adique quadratique soit périodique. Nous nous sommes appuyé sur cette propriété pour donner une démonstration qui semble incomplète de la rationalité ou la transcendance d'un nombre p-adique dont le début de son développement en FCB vérifie les conditions de la proposition de Browkin :

Proposition 3.2.1 ([26]) *Soit $a, b, c \in \mathbb{Z}$, $p \geq 3$, $b' = PGCD(b, 2)$ tels que : p ne divise pas abc et $b.b'$ divise $c + 2a$ et $bc + 2p$ divise $c - 2a$.*
Alors :
1) *Le nombre*

$$m = a^2 + p\frac{2a\,(bc + p) + pc}{b\,(bc + 2p)}$$

est un entier, i.e., $m \in \mathbb{Z}$.
2) *Le développement de $\alpha = \sqrt{m}$ en fraction continue p-adique de Brwokin (lemme (2.2.27)), est périodique et est donné par*

$$\alpha = \left[a; \left\{\frac{b}{p}, c, \frac{b}{p}, 2a\right\}\right] = \left[a; \frac{b}{p}, c, \frac{b}{p}, 2a, \frac{b}{p}, c, \frac{b}{p}, 2a, ...\right] \tag{3.33}$$

Exemple 3.2.2 *Soit $p \geq 3$, on prend $a = p+1, b = c = 1$, donc*

$$\alpha = \left[p+1; \left\{\frac{1}{p}, 1, \frac{1}{p}, 2p+2\right\}\right] = \left[p+1; \frac{1}{p}, 1, \frac{1}{p}, 2p+2, \frac{1}{p}, 1, \frac{1}{p}, 2p+2, ...\right]$$

dans ce cas, on a

$$m = 2p^2 + 4p + 1 \Longrightarrow \alpha = \sqrt{2p^2 + 4p + 1}$$

Par exemple $p = 11$, on aura

$$\alpha = \left[12; \frac{1}{11}, 1, \frac{1}{11}, 24, \frac{1}{11}, 1, \frac{1}{11}, 24, ...\right]$$

d'où $m = 287 \Longrightarrow \alpha = \sqrt{287}$

Théorème 3.2.3 (Belhadef, Esbelin et Zerzaihi [23]) *Soit θ un nombre p-adique défini par son développement en FCB qui commence par*

$$\sigma = \left(a; \frac{b}{p}, c, \frac{b}{p}, 2a\right)$$

avec a, b, c, p définis comme dans la proposition précédente et de plus $a, b, c \in \mathbb{N}$.
Alors θ est transcendant ou rationnel.

Preuve. On va utiliser la démonstration par l'absurde. Supposons que θ est algébrique irrationnel.
Soit le nombre α défini par le développement en FCB donné dans (3.33)

$$\alpha = \left[a; \left\{\frac{b}{p}, c, \frac{b}{p}, 2a\right\}\right]$$

on a

$$\theta = \left[a; \frac{b}{p}, c, \frac{b}{p}, 2a, \theta_5, \theta_6, \theta_7, ...\right] \tag{3.34}$$

alors, d'après les propriétés des fractions continues p-adiques, et le lemme (2.2.27)

$$\begin{aligned} \left|\theta - \frac{P_n}{Q_n}\right|_p &= \frac{1}{|Q_n|_p^2 \, |\theta_{n+1}|_p} < \frac{1}{|Q_n|_p^2} \\ &\quad et \\ \left|\alpha - \frac{P_n}{Q_n}\right|_p &= \frac{1}{|Q_n|_p^2 \, |\alpha_{n+1}|_p} = \frac{1}{|Q_n|_p^2 \left|\frac{b}{p}\right|_p} = \frac{1}{|Q_n|_p^2} \end{aligned}$$

avec $n = 5k - 1$, $\dfrac{P_n}{Q_n}$ c'est la $n^{ème}$ réduite de θ et α (la dernière réduite commune, $n = 4$ dans (3.34).
d'où,

$$\begin{aligned} |\theta - \alpha|_p &\leq \left|\theta - \frac{P_n}{Q_n} - \alpha + \frac{P_n}{Q_n}\right|_p \\ &\leq \max\left(\left|\theta - \frac{P_n}{Q_n}\right|_p, \left|\alpha - \frac{P_n}{Q_n}\right|_p\right) = \frac{1}{|Q_n|_p^2} \end{aligned}$$

Pour $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) \in \mathbb{Q}^4$, soit les formes linéaires à coefficients algébriques p-adiques

$$L_{i,p}(\mathbf{x}) = \mathbf{x}_i \quad , i = \overline{1,4}$$

Nous avons la majoration suivante, pour $\mathbf{x}' = (Q_4, P_4, Q_n, P_n)$

$$\begin{aligned} |L_{1,p}(\mathbf{x}')|_p &= |Q_4|_p \leq 1 \\ |L_{2,p}(\mathbf{x}')|_p &= |P_4|_p \leq 1 \\ |L_{3,p}(\mathbf{x}')|_p &= |Q_n|_p \leq 1 \\ |L_{4,p}(\mathbf{x}')|_p &= |P_n|_p \leq 1 \end{aligned} \tag{3.35}$$

Maintenant, voyons α comme un nombre réel définie par son développement en fraction continue réel

$$\alpha = a + \cfrac{p}{b + \cfrac{p}{c + \cfrac{p}{b + \cfrac{p}{2a + \cfrac{p}{b + \cfrac{p}{c + \cfrac{p}{b + \cfrac{p}{2a + \ldots}}}}}}}}$$

Un petit calcul donne

$$\alpha^2 = m \qquad \text{et} \qquad \frac{P_4}{Q_4} = m.\frac{b\,(bc + 2p)\,(2m' - ap\,(bc + p))}{m'.\,(2ab\,(bc + 2p) + p\,(bc + p))} \tag{3.36}$$

avec $m' = a^2 b\,(bc + 2p) + 2ap\,(bc + p) + cp^2$.

Pour $\mathbf{x}=(\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3,\mathbf{x}_4)\in\mathbb{Q}^4$, soit les formes linéaires à coefficients algébriques réel

$$\begin{aligned}
L_1(\mathbf{x}) &= \alpha^2\mathbf{x}_1-\frac{m'.\left(a\left(b^2c+2bp\right)+p\left(bc+p\right)\right)}{b\left(bc+2p\right)\left(2m'-ap\left(bc+p\right)\right)}\mathbf{x}_2+\mathbf{x}_1\\
L_2(\mathbf{x}) &= \alpha\mathbf{x}_1-\mathbf{x}_2\\
L_3(\mathbf{x}) &= \alpha\mathbf{x}_3-\mathbf{x}_4\\
L_4(\mathbf{x}) &= \mathbf{x}_1
\end{aligned}$$

Nous avons les inégalités suivantes pour $\mathbf{x}'=(Q_4,P_4,Q_n,P_n)$:

$$\begin{aligned}
&|L_1(\mathbf{x}')|=\left|Q_4\alpha^2-Q_4m+Q_4\right|=|Q_4| \\
&|L_2(\mathbf{x}')|=|Q_4\alpha-P_4|\leq|Q_4|^{-1}\\
&|L_3(\mathbf{x}')|=|Q_n\alpha-P_n|\leq|Q_n|^{-1}\\
&|L_4(\mathbf{x}')|=|Q_4|
\end{aligned}\tag{3.37}$$

Donc, on combine les deux systèmes (3.35), (3.37), on peut trouver $\varepsilon>0$ tel que

$$\prod_{i=1}^{4}\left(|L_i(\mathbf{x})|\,.\,|L_{i,p}(\mathbf{x})|_p\right)\leq|Q_4|\,|Q_n|^{-1}\leq|Q_n|^{-1-\varepsilon}\tag{3.38}$$

A ce stade, on applique la version p-adique du théorème du sous-espace de Schmidt (due à Schlickewei), l'ensemble des solutions de l'inégalité (3.38) est inclus dans une union finie de sous-espaces propres de $\mathbb{Q}^4$. C'est-à-dire qu'il existe quatre entiers non nuls x_1,x_2,x_3,x_4, tel que pour $n\geq 4$ on a

$$x_1Q_4+x_2P_4+x_3Q_n+x_4P_n=0\tag{3.39}$$

1) Si $x_4\neq 0$:
On divise l'égalité (3.39) par Q_n, il vient que

$$\frac{1}{Q_n}\left(x_1Q_4+x_2P_4\right)+x_3+x_4\frac{P_n}{Q_n}=0$$

Passons à la limite quand n tends vers $+\infty$, nous trouvons

$$\beta\left(x_1Q_4+x_2P_4\right)+x_3+x_4\theta=0\tag{3.40}$$

avec $\beta=\lim\limits_{n\to+\infty}\dfrac{1}{Q_n}\in\mathbb{Q}$, donc θ est rationnel. Contradiction.
2) Si $x_4=0$:

On divise l'égalité (3.39) par P_n, il vient

$$\frac{1}{P_n}\left(x_1Q_4 + x_2P_4\right) + x_3\frac{Q_n}{P_n} = 0$$

Passons à la limite quand n tends vers $+\infty$, nous trouvons

$$\beta'\left(x_1Q_4 + x_2P_4\right) + \frac{x_3}{\theta} = 0 \tag{3.41}$$

avec $\beta' = \lim_{n\to+\infty}\frac{1}{P_n} \in \mathbb{Q}$, donc θ est rationnel. Contradiction.
Dans les deux cas, on a trouvé une contradiction, donc θ est un nombre rationnel ou transcendant. ■

Remarque 3.2.4 *Un travail de futur est d'ajouter des conditions sur le nombre θ pour compléter la démonstration.*

3.2.2 Transcandence des fractions continues p-adique de Thue-Morse

Adamczewski et Bugeaud ont démontré dans [3] la transcendance d'un nombre p-adique dont le début de son développement de Hensel satisfait la condition $(*)_w$ pour $w > 1$. Mais ils n'ont pas fait le même résultat pour les fractions continues p-adiques, comme pour les fractions continues réelles. Cela est dû au manque des définitions et propriétés du développement en fraction continue p-adique par rapport à celle dans $\mathbb{R}$ (d'après une conversation avec le deuxième auteur Alain Bugeaud). Cependant, nous avons démontré dans notre article [22], la transcendance d'un nombre p-adique donné par son développement en fraction continue p-adique dont il est un mot du Thue-Morse, et vérifie des conditions sur l'alphabet.

Théorème 3.2.5 (Belhadef, Esbelin et Zerzaihi [22]) *Soient $p \geq 3$, $\alpha = \frac{\alpha_1}{\alpha_2}$ et $\beta = \frac{\beta_1}{\beta_2}$ deux nombres rationnel appartient à $\mathbb{Z}\left[\frac{1}{p}\right] \cap (0;p)$ tels que*

$$\begin{aligned} v_p(\alpha_1) &= v_p(\beta_1) = 0 \\ &\quad et \\ v_p(\alpha_2) &\geq v_p(\beta_2) \geq 1 \end{aligned}$$

On note $\Xi = Max\{\alpha,\beta\}$. Soit $\theta \in \mathbb{Q}_p$ défini comme limite de la fraction continue $[0; a_1, a_2, ..., a_k, ...]$ où $a_i \in \{\alpha,\beta\}, \forall i \geq 1$. On suppose que la suite des quotients partiels

$(a_i)_{i\geq 1}$ *est de Thue-Morse. Si on a*

$$p^{\frac{5v_p(\beta_2)-v_p(\alpha_2)}{6}} > Max\{\alpha_2;\beta_2\} \times \frac{\Xi+\sqrt{\Xi^2+4}}{2} \tag{3.42}$$

alors θ *est transcendant ou quadratique.*

Preuve. Supposons que θ est algébrique de degré supérieur strictement à 2. On note $v_0 = -\dfrac{v_p(\alpha)+v_p(\beta)}{2}$.
Nous Considérons les formes linéaires en la variable $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$

$$\begin{aligned} L_{i,\infty}(\mathbf{x}) &= \mathbf{x}_i \quad , \ 1 \leq i \leq 3 \\ L_{1,p}(\mathbf{x}) &= \theta^2\mathbf{x}_3 - \mathbf{x}_1 \\ L_{2,p}(\mathbf{x}) &= \theta\mathbf{x}_3 - \mathbf{x}_2 \\ L_{3,p}(\mathbf{x}) &= \mathbf{x}_3 \end{aligned}$$

On va les évaluer pour le triple $\mathbf{x}' = \left(c_{4^k}p'_{4^k-1}, p'_{4^k}, q'_{4^k}\right)$ avec $k \in \mathbb{N}^*$, on a

$$\begin{cases} |L_{i,\infty}(\mathbf{x}')| = |\mathbf{x}'_i| \quad , \ 1 \leq i \leq 3 \\ |L_{1,p}(\mathbf{x}')|_p = \left|\theta^2 q'_{4^k} - c_{4^k}p'_{4^k-1}\right|_p \\ |L_{2,p}(\mathbf{x}')|_p = \left|\theta q'_{4^k} - p'_{4^k}\right|_p \\ |L_{3,p}(\mathbf{x}')|_p = \left|q'_{4^k}\right|_p \end{cases}$$

En appliquant les lemmes (2.2.25) et le théorème (2.1.17), on trouve

$$\begin{aligned} |L_{2,p}(\mathbf{x}')|_p &= |\Pi|_p \left|\theta q_{4^k} - p_{4^k}\right|_p = \frac{1}{|q_{4^k}|_p \left|a_{4^k+1}\right|_p} < \frac{1}{p^{4^k v_0}} |\Pi|_p \\ &\text{et} \\ |L_{3,p}(\mathbf{x}')|_p &= |\Pi|_p |q_{4^k}|_p = p^{4^k v_0} |\Pi|_p \end{aligned} \tag{3.43}$$

avec $\Pi = \prod_{j=1}^{4^k} c_j$.
Pour évaluer $L_{1,p}(\mathbf{x}')$ nous avons pour $n = 4^k$

$$\theta^2 - \frac{p_n}{q_n}\frac{p_{n-1}}{q_{n-1}} = \left(\theta + \frac{p_{n-1}}{q_{n-1}}\right)\left(\theta - \frac{p_n}{q_n}\right) + \frac{(-1)^{n+1}}{q_n q_{n-1}}\theta \tag{3.44}$$

d'où

$$\begin{aligned}\left|\theta^2-\frac{p_n}{q_n}\frac{p_{n-1}}{q_{n-1}}\right|_p &= \left|\left(\theta+\frac{p_{n-1}}{q_{n-1}}\right)\left(\theta-\frac{p_n}{q_n}\right)+\frac{(-1)^{n+1}}{q_nq_{n-1}}\theta\right|_p\\ &\leq \max\left\{\left|\theta+\frac{p_{n-1}}{q_{n-1}}\right|_p\left|\theta-\frac{p_n}{q_n}\right|_p;|\theta|_p\left|\frac{1}{q_nq_{n-1}}\right|_p\right\}\\ &< \frac{1}{|q_n|_p^2}\max\left\{\left|\theta+\frac{p_{n-1}}{q_{n-1}}\right|_p\left|\theta-\frac{p_n}{q_n}\right|_p;|\theta|_p\left|\frac{q_n}{q_{n-1}}\right|_p\right\}\end{aligned}$$

d'autre part, on a d'après le théorème (2.1.17) : $a_i=a_{n-i+1}$ et $a_0=0$, alors $p_n=q_{n-1}$.

Alors, on obtient l'estimation suivante

$$\begin{aligned}\left|\theta^2q_n-p_{n-1}\right|_p &= |q_n|_p\left|\theta^2-\frac{p_{n-1}}{q_n}\right|_p\\ &= |q_n|_p\left|\theta^2-\frac{p_n}{q_{n-1}}\frac{p_{n-1}}{q_n}\right|_p\\ &< \frac{1}{|q_n|_p}\max\left\{\left|\theta+\frac{p_{n-1}}{q_{n-1}}\right|_p;|\theta|_p\left|\frac{q_n}{q_{n-1}}\right|_p\right\}\end{aligned}$$

donc il existe une constante C_1 tel que

$$|L_{1,p}(\mathbf{x}')|_p=\left|\theta^2q'_{4^k}-c_{4^k}p'_{4^k-1}\right|_p=|\Pi|_p\left|\theta^2q_{4^k}-p_{4^k-1}\right|_p<\frac{C_1}{p^{4^kv_0}}|\Pi|_p \tag{3.45}$$

On fait maintenant le produit des trois formes

$$\prod_{i=1}^{3}\left(\left|L_{i,p}(\mathbf{x}')\right|_p\right)<\frac{C_1}{p^{4^kv_0}}|\Pi|_p^3 \tag{3.46}$$

Pour les formes linéaires réelles, nous avons l'inégalité suivante, en appliquant le lemme (2.2.7)

$$\prod_{i=1}^{3}\left(|L_{i,\infty}(\mathbf{x}')|\right)=\prod_{i=1}^{3}|\mathbf{x}'_i|=\left|c_{4^k}p'_{4^k-1}\right||p'_{4^k}||q'_{4^k}|<\Lambda^{3(1+4^k)}|\Pi|^3$$

avec $\Lambda=\dfrac{\Xi+\sqrt{\Xi^2+4}}{2}$. On aura donc pour $\delta\in\mathbb{R}_+^*$

$$\frac{1}{|\mathbf{x}'|^{\delta}}\prod_{i=1}^{3}\left(\frac{1}{|L_{i,\infty}(\mathbf{x}')|}\right)>\frac{1}{\Lambda^{(3+\delta)(1+4^k)}|\Pi|^{3+\delta}} \tag{3.47}$$

D'après l'inégalité (3.42) du théorème, on peut choisir δ tel que pour k assez grand, on combine les inégalités (3.46) et (3.47), pour aboutir à

$$\prod_{i=1}^{3}\left(\left|L_{i,\infty}\left(\mathbf{x}'\right)\right|.\left|L_{i,p}\left(\mathbf{x}'\right)\right|_{p}\right)<\frac{1}{\left|\mathbf{x}'\right|^{\delta}} \tag{3.48}$$

A ce stade, la version p-adique du théorème du sous-espace de Schmidt (due à Schlickewei), nous confirme l'existence des entiers non nuls y_1, y_2, y_3, tel que

$$y_1 c_{4^k} p'_{4^k-1} + y_2 p'_{4^k} + y_3 q'_{4^k} = 0$$

i.e

$$y_1\frac{p_{4^k-1}}{q_{4^k}} + y_2\frac{p_{4^k}}{q_{4^k}} + y_3 = 0 \tag{3.49}$$

donc

$$y_1.\frac{p_{4^k-1}}{q_{4^k-1}}.\frac{q_{4^k-1}}{q_{4^k}} + y_2.\frac{p_{4^k}}{q_{4^k}} + y_3 = 0$$

d'où

$$y_1.\frac{p_{4^k-1}}{q_{4^k-1}}.\frac{p_{4^k}}{q_{4^k}} + y_2.\frac{p_{4^k}}{q_{4^k}} + y_3 = 0 \tag{3.50}$$

d'autre part on sait que la suite de réduites $\left(\frac{p_n}{q_n}\right)_n$ tend vers θ dans $\mathbb{Q}_p$. Donc par passage à la limite dans l'équation (3.50) quand $k \longrightarrow +\infty$, on trouve

$$y_1\theta^2 + y_2\theta + y_3 = 0$$

Contradiction avec la supposition que θ est algébrique de degré supérieur strictement à 2. Alors θ est quadratique ou transcendant. ■

Annexe A

Corps normés

Pour plus de détails sur les corps normés voir les livres d'Alain Robert [53], de Fernando Gouvêa [36] et de Wim Schikhof [56].

Définition A.0.6 *Soit K un corps. Une norme sur K (qui dite valeur absolue) est une application $|.|$ définie sur K à valeurs dans $\mathbb{R}^+$ et vérifiant pour x, y dans K les trois conditions suivantes :*

1- $|x| = 0 \Longleftrightarrow x = 0$,
2- $|x.y| = |x| \,.\, |y|$,
3- $|x + y| \leq |x| + |y|$ *(inégalité triangulaire).*
On dit dans ce cas que K est un corps valué ou normé.

Définition A.0.7 *On appelle distance induite sur K par $|.|$, la distance $d_{|.|}$ sur K définie par*

$$\forall x, y \in K, d_{|.|}(x, y) = |x - y| \,. \tag{A1.1}$$

les propriétés de la norme $|.|$ assurent que $d_{|.|}$ est une distance sur K et donc elle définit une topologie sur K.

Proposition A.0.8 *Pour tous $(x, y) \in K^2$ muni de la norme $|.|$, on a :*
1) $|1| = |-1| = 1$.
2) $|x| = |-x| \,.$
3) $|x - y| \leq |x| + |y| \,.$
4) $|n| \leq n \quad \forall n \in \mathbb{N}$.

Preuve. 1) On a

$$|1| = |(\pm 1) \,.\, (\pm 1)| = |\pm 1|^2$$

donc $|\pm 1| = 1$.
2) Nous avons

$$|x| = |(-1)\,.\,(-x)| = |-1|\,.\,|-x| = |-x| \tag{A.1}$$

3) D'après l'inégalité triangulaire et 2)

$$|x - y| \leq |x + (-y)| \leq |x| + |-y| = |x| + |y|\,.$$

4) D'après l'inégalité triangulaire et 1)

$$|n| = \left|\underbrace{1 + 1 + ... + 1}_{n \text{ fois}}\right| \leq |1| + |1| + ... + |1| = \underbrace{1 + 1 + ... + 1}_{n \text{ fois}} = n.$$

■

Définition A.0.9 *Une valeur absolue est dite non-archimédienne si la distance associée est ultramétrique, c'est-à-dire si on avons, pour tout $(x, y) \in K^2$, l'inégalité triangulaire forte suivante*

$$|x + y| \leq \max(|x|, |y|) \tag{A1.2}$$

qui est plus forte que la condition (3).

Lemme A.0.10 *Si la norme $|.|$ est ultramétrique et $|x| \neq |y|$, alors $|x+y| = \max(|x|, |y|)$.*

Preuve. Supposons que $|x| < |y|$, i.e. $\max(|x|, |y|) = |y|$. Nous avons

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

d'où $|x| < |y| \leq \max(|x + y|, |x|)$, donc

$$\max(|x + y|, |x|) = |x + y| \tag{A.2}$$

alors

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

qui nous donne

$$|x + y| = |y| = \max(|x|, |y|)$$

■

Proposition A.0.11 *Pour que le corps valué $(K, |.|)$ soit ultramétrique il faut et il suffit que l'ensemble $\mathbb{N}$ soit borné par rapport à $|.|$, i.e.*

$$\forall n \in \mathbb{N} : |n| \leq 1 \tag{A.3}$$

Preuve. Supposons que $(K, |.|)$ est ultramétrique. On va démontrer l'inégalité (A.3) par récurrence :
Pour $n = 0$ on a $|0| = 0 \leq 1$; pour $n = 1$, on a d'après la proposition (A.0.8) $|1| = 1 \leq 1$. On suppose que $\forall k \in \{0, ..., n-1\} : |k| \leq 1$; on montre que $|n| \leq 1$. En effet, on a

$$|n| = |n - 1 + 1| \leq \max(|n-1|, |1|) = 1$$

Maintenant, supposons que $\forall n \in \mathbb{N} : |n| \leq 1$. On démontre que la norme de K est non-archimédienne

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

D'autre part, la condition $|n| \leq 1$, implique $\left|C_n^k\right| \leq 1$ (car C_n^k est un entier), alors

$$|x+y|^n \leq \sum_{k=0}^{n} |x|^k . |y|^{n-k} \leq (n+1) \left[\max(|x|, |y|)\right]^n$$

Donc $\forall n \in \mathbb{N}$

$$|x+y| \leq (n+1)^{\frac{1}{n}} \max(|x|, |y|) \tag{A.4}$$

Par passage à la limite quand $n \longrightarrow +\infty$, dans l'inégalité (A.4), on aura

$$|x+y| \leq \max(|x|, |y|)$$

■

Proposition A.0.12 *Voici des belles propriétés d'un espace muni d'une norme ultramétrique :*
(i) Tout triangle est isocèle.
(ii) Tout point d'une boule en est "le" centre.
(iii) Deux boules sont soit disjointes soit l'une est contenue dans l'autre.
(iv) Les boules sont à la fois ouvertes et fermées.
(v) La topologie est totalement discontinue.

Remarque A.0.13 *Lorsque L est un sous-corps de K, alors une norme sur K induite une norme sur L.*

Définition A.0.14 *Soit K un corps, une valuation v sur K est une application de K dans $\mathbb{R} \cup \{+\infty\}$ vérifiant les trois conditions suivantes :*
1) $v(x) = +\infty \Longleftrightarrow x = 0$,
2) $v(x.y) = v(x) + v(y)$,
3) $v(x + y) \geq \min(v(x), v(y))$.

Définition A.0.15 *Deux normes sur un corps K sont équivalentes si elles définissent la même topologie.*

Proposition A.0.16 *Deux normes $|.|_1$ et $|.|_2$ sont équivalentes si et seulement s'il existe $\alpha \in \mathbb{R}_+^*$ tel que l'on ait $|x|_1 = |x|_2^\alpha$ quel que soit $x \in K^*$.*

On termine cette section par un résultat concernant les suites de Cauchy dans un espace normé ultramétrique

Théorème A.0.17 *Soit $(a_n)_n$ une suite dans le corps ultramétrique $(K, |.|_K)$, alors $(a_n)_n$ est une suite de Cauchy si et seulement si*

$$\lim_{n \to +\infty} |a_{n+1} - a_n|_K = 0 \tag{A.5}$$

Preuve. Supposons que $(a_n)_n$ est de Cauchy, en d'autre terme

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

En particulier, si $m = n + 1$,on obtient $\lim_{n \to +\infty} |a_{n+1} - a_n|_K = 0$.

Réciproquement ; on suppose que $\lim_{n \to +\infty} |a_{n+1} - a_n|_K = 0$, i.e.

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} : n > N \Longrightarrow |a_{n+1} - a_n|_K < \varepsilon \tag{A.6}$$

Soit $m > n > N$, on a

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

d'où

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} : m, n > N \Longrightarrow |a_m - a_n|_K < \varepsilon \tag{A.7}$$

donc la suite $(a_n)_n$ est de Cauchy. ■

Annexe B

Théorème de complétion

Les définitions et les théorèmes de cette annexe apparaissent dans les livres : **(Voir [12], [37], [56].**

Soit $(F, \|.\|_F)$ un corps normé n'est pas complet par rapport à $\|.\|_F$. On va construire un autre corps $\overline{F}$ contenant F, et l'associe par une norme induite de la norme de F, de façon que $\overline{F}$ soit un corps complet. Le rôle principal dans cette opération sera joué par les suites de Cauchy : Ce sont les classes d'équivalence des suites de Cauchy de F qu'est sera déclaré comme éléments du corps $\overline{F}$. Ainsi, on va commencer par une discussion sur les suites de Cauchy dans un corps normé arbitraire.

On note par $SC(F)$ l'ensemble des suites de Cauchy définies dans l'espace $(F, \|.\|_F)$, i.e. l'ensemble des suites $\{a_n\}_{n\in\mathbb{N}} \subset F$ telle que

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} / \forall n > m \geq N \ : \|a_n - a_m\|_F < \varepsilon \tag{B.1}$$

L'ensemble $SC(F)$ est un anneau commutative, les opérations $+, -, \times$ sont interne, on les définit comme suit

$$\begin{aligned} \{a_n\}_{n\in\mathbb{N}} + \{b_n\}_{n\in\mathbb{N}} &= \{a_n + b_n\}_{n\in\mathbb{N}} \\ \{a_n\}_{n\in\mathbb{N}} \times \{b_n\}_{n\in\mathbb{N}} &= \{a_n \times b_n\}_{n\in\mathbb{N}} \end{aligned}$$

Ainsi, l'élément neutre par rapport à l'addition c'est la suite nulle $\{0\}_{n\in\mathbb{N}} = \{0, 0, ...\}$ et l'élément neutre par rapport à la multiplication c'est la suite $\{1\}_{n\in\mathbb{N}} = \{1, 1, ...\}$. L'ensemble $SC(F)$ n'est pas un corps, puisqu'il contient un zéro diviseur : $\{1, 0, ...\} \times \{0, 1, ...\} = \{0\}_{n\in\mathbb{N}}$.

Soit pour tout $a \in F$ la suite constante $\{a\}_{n\in\mathbb{N}} = \{a, a, ...\}$ elle est de Cauchy, d'où $SC(F)$ contient un ensemble isomorphe à F, ce qui revient à regarder tout élément de F comme un élément de $SC(F)$ en convenant que $a = \{a\}_{n\in\mathbb{N}} = \{a, a, ...\}$.

Maintenant, on note par $NUL(F)$ l'ensemble des suites d'éléments de F tendant vers 0, c'est-à-dire $\lim\limits_{n\to+\infty}\|a_n\|_F = 0$ on les appelle suites négligeables, il est facile de voir que $NUL(F) \subseteq SC(F)$ de faite que $NUL(F)$ est un idéal de $SC(F)$, i.e. le sous-anneau pour lequel, si $\overline{x} \in NUL(F)$ et $\overline{y} \in SC(F)$ nous avons $\overline{x} \times \overline{y} \in NUL(F)$. En effet, si $\{a_n\}_{n\in\mathbb{N}}$ et $\{b_n\}_{n\in\mathbb{N}}$ sont deux suites négligeables ; donc $\{a_n \pm b_n\}_{n\in\mathbb{N}}$ est une suite négligeable ; et si $\{a_n\}_{n\in\mathbb{N}} \in NUL(F)$ et $\{b_n\}_{n\in\mathbb{N}}$ est bornée (en particulier si elle est de Cauchy) alors $\{a_n b_n\}_{n\in\mathbb{N}}$ est dans $NUL(F)$.

On note la classe d'équivalence de $SC(F)$ sur $NUL(F)$ par

$$\overline{F} = SC(F)/NUL(F) \tag{B.2}$$

Ainsi, deux suites de Cauchy sont équivalentes si la soustraction des deux suites tends vers 0. Notons par $\overline{(a_n)}$ la classe d'équivalence qui représente la suite $\{a_n\}_{n\in\mathbb{N}}$, et par $\overline{(a)}$ la classe d'équivalence qui représente la suite constante $\{a\}_{n\in\mathbb{N}}$, et nous identifions $a \in F$ avec $\overline{(a)} \in \overline{F}$, de sorte que nous considérons F comme un sous-ensemble de $\overline{F}$ par l'injection suivante

$$\begin{array}{rccc} \psi: & F & \longrightarrow & \overline{F} \\ & a & \longrightarrow & \overline{(a)} \end{array}$$

Théorème B.0.18 *L'ensemble $\overline{F}$ est un corps.*

Preuve. On définit sur $\overline{F}$ les deux opérations internes suivantes, pour $\overline{(a_n)}, \overline{(b_n)} \in \overline{F}$

$$\begin{array}{rcl} \overline{(a_n)} + \overline{(b_n)} & = & \overline{(a_n + b_n)} \\ \overline{(a_n)}.\overline{(b_n)} & = & \overline{(a_n.b_n)} \end{array} \tag{B.3}$$

Il est facile de vérifier que $\left(\overline{F}, +, .\right)$ est un anneau commutative, son élément neutre par rapport à l'addition (resp. à la multiplication) c'est la classe d'équivalence de la suite nulle $\{0\}_{n\in\mathbb{N}}$ noté $\overline{(0)}$ (resp. la classe d'équivalence de la suite $\{1\}_{n\in\mathbb{N}}$ noté $\overline{(1)}$). Les deux opérations sont indépendantes du choix des représentants des classes d'équivalences.

Il reste à démontrer que chaque élément non nul de $\overline{F}$ est inversible, c'est-à-dire

$$\forall A \in \overline{F},\ \exists A' \in \overline{F} : A.A' = \overline{1} \tag{B.4}$$

En effet, soit $A \in \overline{F}$ tel que $A \neq \overline{0} \in NUL(F)$, et soit $\{a_n\}_{n\in\mathbb{N}}$ une suite de Cauchy de A, tant qu'elle n'est pas négligeable, alors

$$\exists \varepsilon > 0, \exists N \in \mathbb{N} : \|a_n\|_F > \varepsilon,\ \forall n \geq N.$$

En effet, on suppose le contraire, c'est-à-dire

$$\forall \varepsilon > 0, \forall N \in \mathbb{N},\ \exists n \geq N : \|a_n\|_F < \varepsilon$$

tandis que $\{a_n\}_{n\in\mathbb{N}}$ est une suite de Cauchy, i.e.

$$\forall \varepsilon > 0, \exists N' \in \mathbb{N},\ \forall n, m \geq N : \|a_m - a_n\|_F < \varepsilon$$

d'où

$$\forall \varepsilon > 0, \exists N' \in \mathbb{N},\ \forall n, m \geq N : \|a_m\|_F < \|a_n\|_F + \|a_m - a_n\|_F < 2\varepsilon \tag{B.5}$$

ce qui veut dire que $\{a_n\}_{n\in\mathbb{N}}$ est négligeable, contradiction.

Définissons une autre suite $\{r_n\}_{n\in\mathbb{N}}$ par

$$r_n = \begin{cases} 0 & , \quad \text{si} \quad n < N \\ \frac{1}{a_n} & , \quad \text{si} \quad n \geq N \end{cases}$$

cette suite $\{r_n\}_{n\in\mathbb{N}}$ est de Cauchy, en effet si $n, m \geq N$ on a

$$\|r_m - r_n\|_F = \|\frac{1}{a_m} - \frac{1}{a_n}\|_F = \frac{\|a_m - a_n\|_F}{\|a_m\|\|a_n\|_F} < \varepsilon^{-2}\|a_m - a_n\|_F \tag{B.6}$$

Notons la classe d'équivalence de $(r_n)_{n\in\mathbb{N}}$ par A', on a le produit

$$(b_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} \ \times (r_n)_{n\in\mathbb{N}} = \left\{ \underbrace{0, 0, ..., 0}_{(N-1)terme}, 1, 1, ... \right\}$$

donc

$$(b_n)_{n\in\mathbb{N}} - (1)_{n\in\mathbb{N}} = \left\{ \underbrace{-1, -1, ..., -1}_{(N-1)terme}, 0, 0, ... \right\} \in NUL(F)$$

alors $(b_n)_{n\in\mathbb{N}} \in \overline{(1)}$ d'où $\overline{(b_n)} = \overline{(1)}$. Alors $A.A' = \overline{(1)}$; ce qui preuve que les éléments non nuls de $\overline{F}$ admettent des inverses, ainsi $\overline{F}$ est un corps. ■

Définition B.0.19 *Pour tout $A = \overline{(a_n)} \in \overline{F}$ on définit l'application suivante*

$$\begin{aligned} \|.\|_{\overline{F}} \quad &: \quad \overline{F} \to \mathbb{R}^+ \\ A \quad &\to \quad \|A\|_{\overline{F}} = \lim_{n\to+\infty} \|a_n\|_F \end{aligned} \tag{B.7}$$

On va démontrer que cette application est une norme sur $\overline{F}$ et elle est non-archimédienne

si la norme de F est aussi ; on utilise le lemme suivant :

Lemme B.0.20 *Soit $(K, \|.\|_K)$ un corps ultramétrique, et soient $b \in K$ et une suite de Cauchy $(a_n)_{n\in\mathbb{N}} \subset K$ tels que $b \neq \lim_{n\to+\infty} a_n$. Alors la suite de nombres réels $(\|a_n - b\|_K)_{n\in\mathbb{N}}$ est stationnaire. En particulier ; si $(a_n)_{n\in\mathbb{N}}$ n'est pas une suite négligeable, alors la suite $(\|a_n\|_K)_{n\in\mathbb{N}}$ est stationnaire.*

Preuve. Soit $(a_n)_{n\in\mathbb{N}}$ une suite de Cauchy d'éléments de K, en d'autre terme

$$\forall \varepsilon > 0, \exists n_0 \geq 0 \ / \ m, n > n_0 \Rightarrow \|a_m - a_n\|_K < \varepsilon$$

d'autre part, on a pour $m, n > n_0$

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

alors la suite de nombres réels $(\|a_n - b\|_K)_{n\in\mathbb{N}}$ est de Cauchy, donc elle converge dans $\mathbb{R}$; soit ℓ sa limite. D'après les données du lemme, on a

$$\left[\|a_n - b\|_K \geq 0 \ , \forall n \in \mathbb{N} \ \text{ et } b \neq \lim_{n\to+\infty} a_n\right] \Rightarrow \ell > 0. \tag{B.8}$$

D'où on peut mettre $\varepsilon = \frac{\ell}{2}$ dans la définition des limites, on trouve

$$\exists n_1 \in \mathbb{N} \ / \ n, m > n_1 \Rightarrow \|a_m - a_n\|_K < \frac{\ell}{2}$$

et

$$\exists n_2 \in \mathbb{N} \ / \ n > n_2 \Rightarrow \|a_n - b\|_K > \frac{\ell}{2}.$$

Cela signifie que

$$\|a_n - b\|_K \neq \|a_m - a_n\|_K$$

Prenons $N = \max(n_1, n_2)$, donc pour $n, m > N$

$$\begin{aligned} \|a_m - b\|_K &= \|a_n - b + a_m - a_n\|_K \\ &= \max\{\|a_n - b\|_K, \|a_m - a_n\|_K\} \\ &= \|a_n - b\|_K \end{aligned}$$

d'où la suite $(\|a_n - b\|_K)_{n\in\mathbb{N}}$ est stationnaire à partir du rang N. Pour le cas particulier, il suffit de prendre $b = 0$. ■

Proposition B.0.21 *L'application $\|.\|_{\overline{F}}$ est une norme sur $\overline{F}$; elle est non-archimédienne si la norme de F est aussi.*

Preuve. Montrons d'abord que cette application est bien définie. On a

$$|\|a_m\|_F - \|a_n\|_F| \leq \|a_m - a_n\|_F \tag{B.9}$$

donc la suite de nombres réels $\{\|a_n\|_F\}_{n\in\mathbb{N}}$ est de Cauchy, alors elle converge vert une limite ℓ (puisque $\mathbb{R}$ est complet).

Soit une autre suite $\{a'_n\}_{n\in\mathbb{N}} \in A$, on a

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

alors

$$\lim_{n\to+\infty} \|a_n\|_F = \lim_{n\to+\infty} \|a'_n\|_F$$

d'où $\|.\|_{\overline{F}}$ est bien définie.
Maintenant, on va vérifier les trois propriétés de la norme :
1/ La première propriété : Soit $A = \overline{(a_n)} \in \overline{F}$, on a

$$\begin{aligned} A \quad &= \quad \overline{(a_n)} = \overline{0} \Leftrightarrow \{a_n\}_{n\in\mathbb{N}} \text{ est une suite négligeable} \\ &\Longleftrightarrow \quad \lim_{n\to+\infty} \|a_n\|_F = 0 \Longleftrightarrow \|A\|_{\overline{F}} = 0 \end{aligned}$$

2/ La deuxième propriété : Soit $A = \overline{(a_n)} \in \overline{F}$, $B = \overline{(b_n)} \in \overline{F}$, on a

$$\begin{aligned} \|A.B\|_{\overline{F}} &= \lim_{n\to+\infty} \|a_n.b_n\|_F \\ &= \lim_{n\to+\infty} \|a_n\|_F \,.\, \|b_n\|_F = \|A\|_{\overline{F}} \,.\, \|B\|_{\overline{F}} \end{aligned} \tag{B.10}$$

3/ La troixième propriété (l'inégalité triangulaire) : Soit $A = \overline{(a_n)} \in \overline{F}$, $B = \overline{(b_n)} \in \overline{F}$, on a

$$\begin{aligned} \|A + B\|_{\overline{F}} &= \lim_{n\to+\infty} \|a_n + b_n\|_F \\ &\leq \lim_{n\to+\infty} (\|a_n\|_F + \|b_n\|_F) \\ &\leq \lim_{n\to+\infty} \|a_n\|_F + \lim_{n\to+\infty} \|b_n\|_F \\ &= \|A\|_{\overline{F}} + \|B\|_{\overline{F}} \end{aligned}$$

donc l'application $\|.\|_{\overline{F}}$ est une norme sur $\overline{F}$.
Il reste à montrer que si la norme $\|.\|_F$ est non-archimédienne alors $\|.\|_{\overline{F}}$ est aussi. Pour cela, soit $\overline{(a_n)}$, $\overline{(b_n)} \in \overline{F}$ tel que : $\left\|\overline{(a_n)}\right\|_{\overline{F}} = \left\|\overline{(b_n)}\right\|_{\overline{F}}$.

Si l'une des deux normes est nulle, l'une des deux suites est négligeable, alors le résultat serait effectivement trivial. Supposons alors que les deux suites ne sont pas négligeables.

D'après le lemme précédent (B.0.20) on a

$$\begin{aligned} \exists M' &\in \mathbb{N} \ / \ \forall n > M' \Rightarrow \|a_n\|_F = \|a_{M'}\|_F \\ \exists M'' &\in \mathbb{N} \ / \forall \ n > M'' \Rightarrow \|b_n\|_F = \|b_{M'}\|_F \end{aligned} \tag{B.11}$$

donc

$$\begin{aligned} \exists M' &\in \mathbb{N} \ / \ \forall n > M' \Rightarrow \left\|\overline{(a_n)}\right\|_{\overline{F}} = \lim_{n\to+\infty} \|a_n\|_F = \|a_n\|_F \\ \exists M'' &\in \mathbb{N} \ / \forall \ n > M'' \Rightarrow \left\|\overline{(b_n)}\right\|_{\overline{F}} = \lim_{n\to+\infty} \|b_n\|_F = \|b_n\|_F \end{aligned}$$

Prenons

$$M = \max(M_1, M_2)$$

alors on a, $\forall n > M$

$$\begin{aligned} \|a_n + b_n\|_F &= \max(\|a_n\|_F, \|b_n\|_F) \\ &= \max\left(\left\|\overline{(a_n)}\right\|_{\overline{F}}, \left\|\overline{(b_n)}\right\|_{\overline{F}}\right) \end{aligned}$$

d'où

$$\left\|\overline{(a_n)} + \overline{(b_n)}\right\|_{\overline{F}} = \max\left(\left\|\overline{(a_n)}\right\|_{\overline{F}}, \left\|\overline{(b_n)}\right\|_{\overline{F}}\right)$$

d'où ce qu'on voulait montrer. ■

Théorème B.0.22 *$\overline{F}$ muni de la norme $\| \ .\|_{\overline{F}}$ est complet, et F est un sous-ensemble dense de $\overline{F}$.*

Preuve. Montrons d'abords la densité de F . Soit $A = \overline{(a_n)} \in \overline{F}$, pour tout entier positif fixé m nous considérons la suite constante $\lambda = \{a_m, a_m, ...\}$, d'où la suite $\{a_n - a_m\}_{m\in\mathbb{N}}$ représente la classe $A - \overline{\lambda}$, et tant que $\{a_n\}_{n\in\mathbb{N}}$ est de Cauchy, on peut écrire

$$\lim_{n\to+\infty} \|A - \lambda\|_{\overline{F}} = \lim_{n\to+\infty} \|a_n - a_m\|_F = 0 \tag{B.12}$$

donc F est dense de $\overline{F}$.

Soit, maintenant ; $\{A_n\}_{n\in\mathbb{N}}$ une suite de Cauchy dans $\overline{F}$, on va démontrer que $\overline{F}$ est complet, i.e.

$$\exists A \in \overline{F} : \ \lim_{n\to+\infty} \|A - A_n\|_{\overline{F}} = 0$$

En effet, d'après la densité de F dans $\overline{F}$, pour tout A_n il existe une suite $(a_{i,n})_{i\in\mathbb{N}} \in F$ tel que

$$\|A_n - a_{i,n}\|_{\overline{F}} \leq \frac{1}{n} \tag{B.13}$$

donc $\{A_n - (a_{i,n})\}_{n\in\mathbb{N}}$ est une suite négligeable, d'où elle est de Cauchy dans $\overline{F}$ ($a_{i,n}$ coïncide avec son représentant $\overline{a_{i,n}}$, donc on le considère comme un élément de $\overline{F}$). Nous avons

$$\{\overline{a_{i,n}}\}_{n\in\mathbb{N}} = \{A_n\}_{n\in\mathbb{N}} - \{A_n - (\overline{a_{i,n}})\}_{n\in\mathbb{N}}.$$

Alors $\{(\overline{a_{i,n}})\}_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\overline{F}$, or que les éléments de cette suite appartiennent a F, alors $\{a_{i,n}\}_{n\in\mathbb{N}}$ est lui même de Cauchy dans F, on note sa classe d'équivalence par A. De (B.12) et (B.13) il vient que $\{A - (\overline{a_{i,n}})\}_{n\in\mathbb{N}}$ et $\{A_n - (\overline{a_{i,n}})\}_{n\in\mathbb{N}}$ sont des suites négligeables dans $\overline{F}$. Donc sa différence

$$\{A - A_n\}_{n\in\mathbb{N}} = \{A - (\overline{a_{i,n}})\}_{n\in\mathbb{N}} - \{A_n - (\overline{a_{i,n}})\}_{n\in\mathbb{N}}$$

est une suite négligeable dans $\overline{F}$, ce qui implique que

$$\lim_{n\to+\infty} \|A - A_n\|_{\overline{F}} = 0 \tag{B.14}$$

ça veut dire

$$A = \lim_{n\to+\infty} A_n$$

alors toute suite de Cauchy dans $\overline{F}$ est converge, d'où $\overline{F}$ muni de la norme $\|\ .\|_{\overline{F}}$ est complet. ■

Remarque B.0.23 *Les opérations dans $\overline{F}$ sont prolongées de ceux de F par continuité ; i.e.*

si $A = \lim_{n\to+\infty} (\overline{a}_n)$, $B = \lim_{n\to+\infty} (\overline{b}_n)$; *alors* $A+B = \lim_{n\to+\infty} (\overline{a}_n + \overline{b}_n)$; $A.B = \lim_{n\to+\infty} (\overline{a}_n.\overline{b}_n)$.

Exemple B.0.24 *Le corps des nombres réels $\mathbb{R}$ (muni de la valeur absolue usuelle) est le complété du corps des nombres rationnels $\mathbb{Q}$. On peut donc définir un nombre réel comme étant une classe d'équivalence d'une suite de Cauchy des nombres rationnels.*

Bibliographie

[1] B. Adamczewski, Y. Bugeaud, A Short Proof of the Transcendence of Thue-Morse Continued Fractions, Amer. Math. Monthly 114 (2007), 536-540.

[2] B. Adamczewski, Y. Bugeaud & L. Davison, Continued fractions and transcendental numbers, Ann. Inst. Fourier 56 (2006), 2093-2113.

[3] B. Adamczewski, Y. Bugeaud, On the complexity of algebraic numbers, I. Expansions in integer bases, Annals of Math. 165 (2007), 547–565.

[4] B. Adamczewski, Y. Bugeaud, On the complexity of algebraic numbers, II. Continued fractions, Acta Math. 195 (2005) 1–20.

[5] B. Adamczewski, Y. Bugeaud, Palindromic Continued Fractions. Ann ; Ins. Fourier (Grenoble) 57 (2007), 1557-1574.

[6] B. Adamczewski, Y. Bugeaud, Real and p-adic expansions involving symmetric patterns, Int. Math. Res. Not., Volume 2006 (2006), Article ID 75968, 17 pages.

[7] B. Adamczewski, J. Cassaigne, Diophantine properties of real numbers generated by finite automata, Compositio Math. 142 (2006), 1351-1372.

[8] B. Adamczewski, J. Cassaigne, On the transcendence of real numbers with a regular expansion, J. Number Theory 301 (2003), 27–37.

[9] J.-P. Allouche, Automates et algébricités , J. Théor. Nombres Bordeaux 17 (2005), 1–11.

[10] J.-P. Allouche, J. L. Davison, M. Queffélec, and L. Q. Zamboni, Transcendence of Sturmian or morphic continued fractions, J. Number Theory 91 (2001), 39–66.

[11] J.-P. Allouche, J. Shallit, Automatic sequences : Theory, Applications, Generalizations, Cambridge University Press (2003).

[12] G. Bachman, Introduction to p-Adic Numbers and Valuation Theory, Academic press, new York and london, (1964).

[13] A. Baker, Continued fractions of transcendental numbers, Mathematika 9 (1962), 1–8.

[14] A. Baker, New advances in transcendence theory, Cambridge University Press (1988).

[15] A. Baker, On Mahler's classification of transcendental numbers, Acta Math. 111 (1964), 97–120.

[16] A. Baker, Transcendental number theory, Cambridge University Press (1975).

[17] E. Bedocchi, Fractions continues p-adiques : périodes de longueur paire, Boll. Un. Mat.Ital. (7) 7-A (1993), 259-265.

[18] E. Bedocchi, Nota sulle frazioni continue p-adiche, Ann. Mat. Pura Appl. 152 (1988), 197-207.

[19] E. Bedocchi, Remarks on periods of p-adic continued fractions, Boll. Un. Mat. Ital. (7) 3-A (1989), 209-214.

[20] E. Beddocchi, Sur le dévelopement de $\sqrt{m}$ en fraction continue p-adique, Manuscripta Math. 67 (1990), 187-195.

[21] R. Belhadef, H-A. Esbelin, Sur la version p-adique du théorème de Lamé, Soumis au Comptes rendus Mathematique, Paris.

[22] R. Belhadef, H-A. Esbelin and T. Zerzaihi, Transcendence of Thue–Morse p-Adic Continued Fractions, Mediterr. J. Math., Published online 03 june 2015, Springer Basel.

[23] R. Belhadef, H-A. Esbelin and T. Zerzaihi, On the periodicity of p-Adic Continued Fractions, Submitted in Mediterr. J. Math, Springer Basel.

[24] A. I. Borevich and I. R. Shafarevich, Number theory, Pure and Applied Mathematics, Vol. 20, Academic Press, New York, 1966.

[25] J. Browkin, Continued fractions in local fields, I. Demonstratio Math. 11 (1978), 67-82.

[26] J. Browkin, Continued fractions in local fields, II. Mathematics of Computation. vol 70. N 235 (2000), 1281-1292.

[27] P. Bundschuh, p-adische Kettenbrüche und Irrationalität p-adischer Zahlen. El. Math. 32. 36-40 (1977).

[28] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, Suites algébriques, automates et substitutions, Bull. Soc. Math. France 108 (1980), 401–419.

[29] A.A. Deanin, Periodicity of p-adic continued fraction expansions, J. Number Theory 23 (1986), 367-387.

[30] F. M. Dekking, Transcendance du nombre de Thue-Morse, C. R. Acad. Sci. Paris 285 (1977) 157–160.

[31] B. M. M. de Weger, Approximation lattices of p-adic numbers, J. Number Theory 24 (1986), 70-88.

[32] B.M.M. de Weger, Periodicity of p-adic continued fractions, Elem. Math. 43 (1988), 112-116.

[33] J. D. Dixon, Exact solution of linear equations using p-adic expansions, Numer. Math. 40, (1982) 137-141.

[34] D. Duverney, Théorie des nombres : Cours et exercices corrigés. Dunond (1998).

[35] S. Ferenczi & C. Mauduit, Transcendence of numbers with a low complexity expansion, J. Number Theory 67 (1997), 146–161.

[36] F. Q. Gouvêa, p-adic Numbers : An Introduction, Springer-Verlag Berlin Heidelberg, New York, Second Edition, Universitext, 2000

[37] S. Katok, p-adic Analysis Compared with Real. American Mathematical Society, (2007).

[38] A. YA. Khinchin, Continued Fractions. Phoenix Science Series. The University Of Chicago Press. 1964.

[39] A. Khrennikov, p-adic discrete dynamical systems and their applications in physics and cognitive sciences, Russian Journal of Mathematical Physics, v.11, N. 1, 2004, p.45-70.

[40] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer-Verlag (1984).

[41] V. Laohakosol, A characterization of rational numbers by p-adic Ruban continued fractions, J. Austral. Math. Soc. Ser. A 39 (1985), 300-305.

[42] J. Liouville, À propos de l'existence des nombres transcendants, Comptes-rendus de l'Académie des sciences, 1844.

[43] J.H. Loxton, A.J. van der Poorten, Arithmetic properties of automata : regular sequences, J. Reine Angew. Math., 392 (1988), pp. 57–69

[44] K. Mahler, Lectures On Diophantine Approximations, Part 1 : g-adic numbers and Roths theorem. University of Notre Dame. 1961.

[45] K. Mahler, Lectures on Transcendental Numbers, Springer-Verlag (1976).

[46] K. Mahler, On a geometrical representation of p-adic numbers, Ann. of Math. (2) 41, (1940). 8-56.

[47] K. Mahler, Zur approximation p-adischer irrationalzahlen, Nieuw Arch. Wisk. 18, 22-34, (1934).

[48] M. Morse, Recurrent geodesics on a surface of negative curvature, Trans. Amer. Math. Soc. 22 (1921) 84–100.

[49] T. Ooto, Transcendental p-adic continued fractions, arXiv :1407.0832, math.NT, (2014).

[50] A.N. Parsh, I.R. Shafarevich, Number theory IV : transcendental numbers, Springer-Verlag (1997).

[51] M. Queffélec, Transcendance des fractions continues de Thue-Morse, J. Number Theory 73 (1998) 201–211.

[52] D. Ridout, Rational approximations to algebraic numbers, Mathematika 4 (1957), 125–131.

[53] A.M. Robert, A Course in p-adic Analysis, Springer-Verlag, Graduate Texts in Mathematics,198 (2000).

[54] K. F. Roth, Rational approximations to algebraic numbers, Mathematika 2 (1955), 1–20 ; corrigendum, 169.

[55] A.A. Ruban, Certain metric properties of p-adic numbers, (Russian), Sibirsk. Mat. Zh. 11 (1970), 222-227.

[56] W.H. Schikhof, Ultrametric Calculus : An introduction to p-adic Analysis, Cambridge University Press (1984).

[57] H.P. Schlickewei, On prudects of special linear forms with algebric coefficients, Acta Arith. 31, (1976), 389-398.

[58] W.M. Schmidt, Diophantine approximation, Lecture Notes in Mathematics 785, Springer 1980.

[59] T. Schneider, Über p-adische Kettenbrüche, Symp. Math. 4, (1968/69), 181-189.

[60] Serre, J-P. A Course in Arithmetic, Springer, 1973.

[61] F. Tilborgs, Periodic p-adic continued fractions, Simon Stevin 64 (1990), 383-390.

[62] A. J. van der Poorten, Schneider's continued fraction, Number theory with an emphasis on the Markoff spectrum (Provo, UT, 1991), 271-281, Lecture Notes in Pure and Appl. Math., 147, Dekker, New York, 1993.

[63] A. Thue, Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, Norske vid. Selsk. Skr. Mat. Nat. Kl. 1 (1912) 1–67 ; reprinted in Selected Mathematical Papers of Axel Thue, T. Nagell, ed., Universitetsforlaget, Oslo, 1977, pp. 413–478.

[64] M. Waldschmidt, Un Demi-Siècle de Transcendance, Development of Mathematics, 1950–2000, Birkhäuser, Basel, (2000), pp. 1121–1186.

[65] M. Waldschmidt, Words and Transcendence, Analytic number theory, Cambridge University Press, Cambridge, (2009), pp. 449–470.

[66] L.X. Wang, p-adic continued fractions (I), Scientia Sinica, Ser. A 28 (1985), 1009-1017.

[67] L.X. Wang, p-adic continued fractions (II), Scientia Sinica, Ser. A 28 (1985), 1018-1023.

[68] L.X. Wang, M. Deze, p-adic continued fractions (III), Acta Math. Sinica (N.S.) 2 (1986), no. 4, 299-308.

ملخص

الهدف من هذه الأطروحة هو دراسة الخصائص الجبرية والحسابية لعدد p-adique، وذلك باستخدام النشر إلى كسور مستمرة، و باستخدام الآلات ذات الحالات المنتهية:

- ✓ حيث قمنا بإنشاء خوارزمية لحساب الكسور المستمرة، والبرهان أن هذه الخوارزمية تتوقف بعد رتبة معينة.
- ✓ قمنا باستخدام النسخة p-adique من نظرية الفضاء الجزئي لشميدت المبرهنة من طرف شليكفاي، من أجل إعطاء شروط كافية لكي يكون عدد p-adique معرف بنشره إلى كسور مستمرة (والتي هي عبارة عن متتالية Thue-Morse) هو عدد جبري من الدرجة الثانية أو عدد متسام.

كلمات مفتاحية: عدد p-adique، كسور مستمرة، آلات ذات حالات منتهية، الفضاء الجزئي لـ Schmidt، متتالية Thue-Morse، عدد متسام.

RESUME

L'objectif de cette thèse est d'étudie des caractéristiques algébriques et arithmétiques d'un nombre p-adique, en utilisant son développement en fractions continues et les automates finis:

- On a définit un algorithme de calcul des fractions continues, et on a démontré que cet algorithme s'arrête au bout d'un certain rang.
- On a utilisé la version *p*-adique du théorème du sous-espace de Schmidt due à Schlickewei, pour donner des conditions suffisantes pour qu'un nombre *p*-adique dont son développement en fractions continues est une suite de Thue-Morse, soit quadratique ou transcendant.

Mots cles : nombre p-adique, fractions continues, automates finis, sous-espace de Schmidt, suite de Thue-Morse, transcendence.

ABSTRACT

The objective of this thesis is to study algebraic and arithmetic characteristics of a *p*-adic number, using its development of continued fractions, and finite automata:

- We defines a calculation algorithm of continued fractions, and it was shown that this algorithm stops after a certain rank.
- We used the *p*-adic version of Schmidt subspace theorem due to Schlickewei, to give sufficient conditions for a *p*-adic number which its continued fraction is a sequence of Thue-Morse, is quadratic or transcendent.

Keywords : *p*-adic number, continued fractions, finite automata, Schmidt subspace, sequence of Thue-Morse, transcendent.