الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي

Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

---

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. /11

Mémoire de fin d'étude

Présenté pour l'obtention du diplôme de

Licence Académique

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

Thème

PROBLEME DE SKOLEM POUR LES SUITES RECURRENTES LINEAIRES

Dirigé par : Ismail Kaouache

Presenté par : 1.Ismahene Metaai
2.Aida Bara

Année universitaire
2010-2011

دعاء

اللهم لا تجعلنا نصاب بالغرور إذا نجحنا

و باليأس

إذا أخفقنا و ذكرنا أن

الإخفاق هو التجربة التي تسبق النجاح

اللهم إذا أعطيتنا نجاحا فلا تأخذ تواضعنا

و إذا أعطيتنا تواضعا فلا تأخذ

اعتزازنا بكرامتنا .

اللهم اختم بالسعادة أحلامنا و حقق بالزيادة آمالنا

ربنا تقبل دعائنا

إنك أنت السميع العليم

Remerciements

Nos remerciements vous tout premièrement a dieu tout puissant pour la volonté , la santé et la patience qu' il m'a donné pour terminer ce mémoire .

Nous remercions vivement monsieur S- kaouache d'avoir voulu proposes et assurer la direction de ce mémoire sa disponibilité son soutien ses encouragements et ses précieux conseils tout au long de ce travail.

Sans oublier tous les enseignants qui ont contribué a notre formation durant notre vie scolaire surtout les enseignant de l'institut (S- T) .

Nous remercions également mes collègues dans l'étude .

Table des matières

Introduction Générale

Les suites linéaires récurrentes constituent une partie fondamentale de la théorie des nombres pour plusieurs années. En outre, ces suites apparaissent partout en mathématiques et en informatique. Par exemple la théorie des séries entières représentant les fonctions rationnelles ; les nombres générateurs pseudo-aléatoires, les suites automatiques et les automates cellulaires. Les solutions de certaines classes d'équations diophantiennes et de quelques problèmes combinatoires forment des suites linéaires récurrentes. Une grande variétés de séries de puissances, par exemple les fonctions Zeta de variétés algébriques sur des corps finis, les fonctions Zeta dynamiques, les fonctions génératrices provenant de la théorie des groupes, les séries de Hilbert dans une algèbre commutative et les séries de Poincaré sont toutes connues d'être rationnelles dans de nombreux cas. Les coefficients de la série représentante ces fonctions sont des suites linéaires récurrentes, et donc tant de puissants résultats de la présente étude peuvent être appliqués. Les suites linéaires récurrentes participent également à la preuve du dixième problème de Hilbert sur $\mathbb{Z}$. Elles apparaissent encore dans plusieurs parties de la mathématique appliquée et d'informatique. Plusieurs systèmes de polynômes orthogonaux, y compris les polynômes de Tchebychev, les polynômes de Dickson satisfont des relations de récurrences sous forme de suites linéaires récurrentes. En théorie d'approximation, en cryptographie et en analyse des séries temporelles.

L'application de l'analyse p-adique dans les suites linéaires récurrentes qui nous intéresse dans ce travail est portée sur un célèbre problème dit "Problème de Skolem". Un problème qui consiste à déterminer le nombre d'itérations d'un élément d'une suite linéaire récurrente. La plupart des résultats concernant ce problème utilisent des arguments p-adique ; en particulier les propriétés des normes p-adiques (non-Archimédiennes). Le théorème de Strassman appelé souvent "théorème de préparation p-adique de Weierstrass" qui consiste à borner le nombre de solutions d'une équation à variables p-adiques.

Ce mémoire est composé de deux chapitres. Il est structuré de la manière suivante :

Dans le premier chapitre, on introduit les éléments nécessaires pour une bonne compréhension du problème de Skolem qui sera étudié. Nous rappelons quelques principes et résultats fondamentaux de la théorie des suites récurrentes linéaires, notamment le théorème d'existence concernant la solution des suites récurrentes linéaires.

Le deuxième chapitre vise à donner du théorème de Skolem-Mahler-Lech une preuve simple. Nous rappelons pour un point de départ quelques outils de l'analyse p-adique qui seront utiles pour l'étude mathématique de notre problème. Ces rappels porteront sur le corps ultra-métrique, le corps des nombres p-adiques, notamment la valuation p-adique, la norme p-adique et quelques propriétés analytiques du corps des nombres p-adiques. Nous présentons aussi le théorème de Strassman. Ensuite, nous démontrons le théorème de Skolem-Mahler-Lech.

Chapitre 1

Introduction à la théorie des suites récurrentes linéaires

Le but de ce chapitre est d'établir le modèle mathématique qui décrit le problème de Skolem.pour les suites récurrentes linéaires.

Dans ce chapitre, on introduit les éléments nécessaires pour une bonne compréhension du problème qui sera étudié. Nous rappelons quelques principes et résultats fondamentaux de la théorie des suites récurrentes linéaires. Pour plus de détails sure ces notions, nous indiquons par exemple les travaux [6] , [8] , [9] , [12] et [14] .

1.1 Formulation variationnelle de problème

1.1.1 Définition d'une suite récurrente linéaire

On appelle suite récurrente linéaire toute suite $(u_n)_{n\in\mathbb{N}}$ qui satisfait la relation suivante

$$u_n = c_{k-1}u_{n-1} + c_{k-2}u_{n-2} + ... + c_0u_{n-k} \tag{1.1}$$

pour tout $n \geq k$, avec les coefficients fixés $c_j \in \mathbb{Z}$ pour tout $j = 0, ..., k-1$.
On sait que la relation (1.1) est une relation récurrente de dégré k.
Ici on suppose que dans (1.1), $c_0 \neq 0$, car $c_0 = 0$ implique que la relation linéaire (1.1) est de degré $k-1$.
Les éléments $u_0, u_1, ..., u_{k-1}$ de la suite $(u_n)_{n\in\mathbb{N}}$ sont appelés des conditions initiales.

Exemple 1.1.1 *La suite de Fibonacci* $(u_n)_{n\in\mathbb{N}}$ *définie par*

$$u_n = u_{n-1} + u_{n-2}, n \geq 2, \text{ avec } u_0 = u_1 = 1$$

est l'une des suites récurrentes linéaires les plus connues.

Dans ce travail, nous nous intéresserons au problème de Skolem suivant :
Problème de Skolem [5] **:** Etant donnée une suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$ définie par la relation (1.1) avec ses conditions initiales, on cherche s'il existe un entier positif n tel que $u_n = 0$.

1.2 Solution d'une suite récurrente linéaire

Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire définie par la relation (1.1).
Le polynôme

$$P(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - ... - a_k \tag{1.2}$$

s'appel le polynôme caractéristique de la suite $(u_n)_{n\in\mathbb{N}}$.

Le résultat suivant est essentiel pour l'étude de notre problème.

Théorème 1.2.1 *Supposons que la relation de récurrence* (1.1) *a lieu et que* $P(x)$ *le polynôme caractéristique de cette relation.*
Si

$$P(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}$$

Alors, il existe des polynômes uniques $P_1(x), P_2(x), ..., P_n(x)$, *avec* $\deg(p_i) \leq n_i - 1$, *tels que*

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n \tag{1.4}$$

Réciproquement, toute suite $(u_n)_{n\in\mathbb{N}}$ *de la forme (1.4) satisfait la relation de récurrence (1.1).*

Pour démontrer ce théorème, on va utiliser les lemmes suivants

Lemme 1.2.2 *Soit* $P(x)$ *un polynôme défini par* (1.2) *qui admet* α *comme un zéros d'ordre* $m \geq 1$ *.*
On définit :

$$\begin{cases} P_0(x) = P(x) \\ P_{i+1}(x) = xP_i'(x), \forall i \geq 1 \end{cases} \tag{1.5}$$

Alors il existe des pôlynomes $Q_i(x)$ *tels que*

$$P_i(x) = (x - \alpha)^{m-i}\, Q_i(x) \;, \forall i \in \{0, 1, ..., m-1\} \tag{1.6}$$

Récéproquement

Si $\alpha \neq 0$ et $P_i(\alpha) = 0$; $\forall i = 0, \overline{m-1}$, alors

$$P_0(x) = (x-\alpha)^m Q_0(x) \tag{1.7}$$

où $Q_0(x)$ est un polynôme.

Preuve. Tout d'abord, on va montrer par récurrence que pour tout $i \geq 1$, $P_i(x)$ peut se représenter par

$$P_i(x) = \sum_{j=1}^{i} C_j^{(i)} x^j P^{(j)}(x) \tag{1.8}$$

Le cas $i = 1$ est evident (puisque $P_1(x) = xP'(x)$) .
Supposons maintenant que (1.8) est vraie jusqu'à l'ordre i . Alors

$$\begin{aligned} P_i'(x) &= \sum_{j=1}^{i} C_j^{(i)} \left(jx^{j-1} P^{(j)}(x) + x^j P^{(j+1)}(x) \right) \\ &= \sum_{j=1}^{i} C_j^{(i)} j x^{j-1} P^{(j)}(x) + \sum_{j=2}^{i+1} C_{j-1}^{(i)} x^{j-1} P^{(j)}(x) \end{aligned}$$

Par conséquent

$$\begin{aligned} P_{i+1}(x) &= xP_i'(x) \\ &= xP'(x) + \sum_{j=2}^{i} \left(jC_j^{(i)} + C_{j-1}^{(i)} \right) x^j P^{(j)}(x) + x^{i+1} P^{(i+1)}(x) \end{aligned}$$

Donc

$$P_{i+1}(x) = \sum_{j=1}^{i+1} C_j^{(i+1)} x^j P^{(j)}(x)$$

D'autre part, si α est une racine d'ordre m du $P(x)$, alors α est une racine d'ordre $m-j$ du $P^{(j)}(x)$.
Ceci implique que

$$P^{(j)}(x) = (x-\alpha)^{m-j} \; R_j(x)$$

où $R_j(x)$ est un polynôme.
Récéproquement : Supposons maintenant que $P_i(\alpha) = 0$; $\forall i = 0, \overline{m-1}$, et montrons par récurrence que

$$P_0(x) = (x-\alpha)^m Q_0(x), \text{où } Q_0(x) \text{ est un polynôme}$$

En effet . Si $m=1$, on aura

$$\begin{aligned} P_0(\alpha) &= P(\alpha) \\ &\Longrightarrow (x-\alpha)/P(x) \\ &\Longrightarrow P(x)=(x-\alpha).Q_0(x) \end{aligned}$$

Supposons maintenant, que la propriété est vraie pour tout nombre strictement inférieur à m , alors
Si $P_{m-1}(\alpha)=0$, on obtient

$$\begin{aligned} 0 &= \sum_{j=1}^{m-1} C_j^{(m-1)} \alpha^j P^{(j)}(\alpha) = 0+.....0+\alpha^{m-1}P^{(m-1)}(\alpha) \text{ pour tout } \alpha \neq 0 \\ &\Longrightarrow P^{(m-1)}(\alpha)=0 \Longrightarrow (x-\alpha)^m/P(x) \\ &\Longrightarrow P(x)=(x-\alpha)^m Q_0(x) \end{aligned}$$

■

Lemme 1.2.3 *Sous les conditions du lemme précédent, on a*

$$i)\sum_{p=0}^{k-1} p^i c_p \alpha^p = k^i.\alpha^k; \forall \overline{i=0,\ m-1} \tag{1.9}$$

$$ii)\sum_{p=1}^{k} c_{k-p} p^i \alpha^{k-p} = 0; \forall \overline{i=1,\ m-1} \tag{1.10}$$

.

$$iii)\sum_{p=1}^{k} c_{k-p}(n-p)^j \alpha^{k-p} = n^j \alpha^k; \forall j=\overline{0,m-1} \tag{1.11}$$

Preuve. $i)$ On va montrer par récurrence que

$$P_i(x)=k^i x^k - \sum_{p=0}^{k-1} p^i c_p x^p \ ;\ \forall \overline{i=0,\ m-1}$$

En effet . Pour $i=0$, on obtient

$$k^0 x^k - \sum_{p=0}^{k-1} p^0 c_p x^p = x^k - \sum_{p=0}^{k-1} c_p x^p = P_0(x)$$

Supposons maintenant que la relation est vraie jusqu'à l'ordre i . On a

$$\begin{aligned} P_{i+1}(x) &= xP_i'(x) = x\left[kk^{i-1}x^{k-1} - \sum_{p=0}^{k-1} pp^i c_p x^{p-1}\right] \\ &= k^{i+1}x^k - \sum_{p=0}^{k-1} p^{i+1} c_p x^p \end{aligned}$$

Mais d'après le lemme précédent, on a

$$P_i(\alpha) = 0; \forall \overline{i = 0,\ m-1}$$

Ce qui implique

$$\sum_{p=0}^{k-1} p^i c_p \alpha^p = k^i \alpha^k$$

ii) Un calcul direct donne

$$\begin{aligned} \sum_{p=1}^{k} c_{k-p} p^i \alpha^{k-p} &= \sum_{p'=0}^{k-1} c_{p'} \left(k - p'\right)^i \alpha^{p'} \text{ (en posant } p' = k - p) \\ &= \sum_{t=0}^{i} (-1)^t C_i^t k^{i-t} \sum_{p'=0}^{k-1} c_{p'} p'^t \alpha^{p'} \end{aligned}$$

En utilisant le résultat précédent, on trouve

$$\sum_{p'=0}^{k-1} c_{p'} p'^t \alpha^{p'} = k^t \alpha^k$$

Alors

$$\sum_{p=1}^{k} c_{k-p} p^i \alpha^{k-p} = \sum_{t=0}^{i} (-1)^t C_i^t k^{i-t} k^t \alpha^k = k^i \alpha^k \sum_{t=0}^{i} (-1)^t C_i^t = 0$$

iii) Nous avons

$$\begin{aligned}
\sum_{p=1}^{k} c_{k-p}\left(n-p\right)^{j}\alpha^{k-p} &= \sum_{p=1}^{k} c_{k-p}\sum_{t=0}^{j} C_j^t n^{j-t}\left(-p\right)^{t}\alpha^{k-p} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\left(-1\right)^{t}\sum_{p=1}^{k} c_{k-p}p^{t}\alpha^{k-p} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\left(-1\right)^{t}\sum_{p'=0}^{k-1} c_{p'}\left(k-p'\right)^{t}\alpha^{p'} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\left(-1\right)^{t}\sum_{i=0}^{t}\left(-1\right)^{i} C_t^i k^{t-i}\sum_{p'=0}^{k-1} c_{p'}p'^{i}\alpha^{p'} \\
&= \sum_{t=0}^{j} C_j^t n^{j-t}\left(-1\right)^{t}\sum_{i=0}^{t}\left(-1\right)^{i} C_t^i k^{t-i}k^{i}\alpha^{k} \\
&= n^{j}\alpha^{k}+\sum_{t=1}^{j} C_j^t n^{j-t}\left(-1\right)^{t}k^{t}\alpha^{k}\sum_{i=0}^{t}\left(-1\right)^{i} C_t^i
\end{aligned}$$

$$= n^{j}\alpha^{k}$$

■

Pr**euve du théorème** (1.2.1)

Supposons que $(u_n)_{n\in\mathbb{N}}$ est une suite définie par (1.1).

Et soit

$$P(x)=\prod_{i=1}^{r}\left(x-\alpha_i\right)^{n_i}$$

le polynôme caractéristique de la relation (1.1).

On considère la fonction génératrice suivante

$$F(x)=\sum_{n=0}^{+\infty} u_n x^n \tag{1.12}$$

Alors, pour tout $n\geq k$, on a

$$x^n u_n = c_{k-1}u_{n-1}x^n + c_{k-2}u_{n-2}x^n + ... + c_0 u_{n-k}\, x^n$$

Ce qui implique

$$\begin{aligned}
\sum_{n=k}^{+\infty} x^n u_n &= \sum_{n=k}^{+\infty} (c_{k-1}u_{n-1}x^n + c_{k-2}u_{n-2}x^n + ... + c_0 u_{n-k}\ x^n) \\
&= c_{k-1}x\sum_{n=k}^{+\infty} u_{n-1}x^{n-1} + c_{k-2}x^2\sum_{n=k}^{+\infty} u_{n-2}x^{n-2} + ... + c_0 x^k \sum_{n=k}^{+\infty} u_{n-k}\ x^{n-k} \\
&= c_{k-1}x\sum_{n=k}^{+\infty} u_{n-1}x^{n-1} + c_{k-2}x^2\sum_{n=k}^{+\infty} u_{n-2}x^{n-2} + ... + c_0 x^k \sum_{n=k}^{+\infty} u_{n-k}\ x^{n-k}
\end{aligned}$$

Donc

$$\begin{aligned}
F(x) - \sum_{m=1}^{k} u_{k-m}x^{k-m} = \ & c_{k-1}x\left(F(x) - \sum_{m=2}^{k} u_{n-m}x^{k-m}\right) + c_{k-2}x^2\left(F(x) - \sum_{m=3}^{k} u_{n-m}x^{k-m}\right) + \\
& + ... + c_1 x^{k-1}\left(F(x) - u_0\right) + c_0 x^k F(x)
\end{aligned}$$

Ce qui donne

$$\begin{aligned}
F(x) &= \frac{\sum_{m=1}^{k} u_{k-m}x^{k-m} - c_{k-1}x\left(\sum_{m=2}^{k} u_{k-m}x^{k-m}\right) - c_{k-2}x^2\left(\sum_{m=3}^{k} u_{k-m}x^{k-m}\right) - ... - c_1x^{k-1}u_0}{1 - \sum_{m=1}^{k} c_{k-m}x^m} \\
&= \frac{\sum_{m=1}^{k} u_{k-m}x^{k-m} - c_{k-1}\sum_{m=2}^{k} u_{k-m}x^{k-(m-1)} - c_{k-2}\sum_{m=3}^{k} u_{k-m}x^{k-(m-2)} - ... - c_1x^{k-1}u_0}{1 - \sum_{m=1}^{k} c_{k-m}x^m}
\end{aligned}$$

Posons

$$R(x) = \sum_{m=1}^{k} u_{k-m}x^{k-m} - c_{k-1}\sum_{m=2}^{k} u_{k-m}x^{k-(m-1)} - c_{k-2}\sum_{m=3}^{k} u_{k-m}x^{k-(m-2)} - ... - c_1x^{k-1}u_0$$

et

$$Q(x) = 1 - \sum_{m=1}^{k} c_{k-m}x^m$$

où $\deg R \leq k-1$, et $\deg Q = k$ (car $c_0 \neq 0$).
Alors

$$\begin{aligned}
Q(\frac{1}{x}) &= 1 - \sum_{m=1}^{k} c_{k-m} x^{-m} \\
&\Rightarrow \; x^k Q(\frac{1}{x}) = x^k - \sum_{m=1}^{k} c_{k-m} x^{k-m} \\
&= \; P(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}
\end{aligned}$$

Donc

$$\begin{aligned}
\frac{1}{x^k} Q(x) &= \prod_{i=1}^{r} \left(\frac{1}{x} - \alpha_i \right)^{n_i} \\
&= \prod_{i=1}^{r} \left(\frac{1}{x} \right)^{n_i} \prod_{i=1}^{r} (1 - \alpha_i x)^{n_i} \\
&= \frac{1}{x^k} \prod_{i=1}^{r} (1 - \alpha_i x)^{n_i} \;\; (\text{ car } \sum_{i=1}^{r} n_i = k \;)
\end{aligned}$$

Alors

$$Q(x) = \prod_{i=1}^{r} (1 - \alpha_i x)^{n_i}$$

En utilisant la division Euclidienne, on peut décomposer la fonction F comme suit

$$F(x) = \frac{R(x)}{\prod_{i=1}^{r} (1 - \alpha_i x)^{n_i}} = \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{r_{ij}}{(1 - \alpha_i x)^j}$$

Moyennant maintenant de l'expression

$$\left(\frac{1}{1-y} \right)^j = \left(\sum_{n=0}^{+\infty} y^n \right)^j = \sum_{h=0}^{+\infty} c_{j-1}^{h+j-1} y^h,$$

il s'ensuit

$$\begin{aligned}
F(x) &= \sum_{i=1}^{r} \sum_{j=1}^{n_i} r_{ij} \left(\sum_{h=0}^{+\infty} c_{j-1}^{h+j-1} \alpha_i^h x^h \right) \\
&= \sum_{h=0}^{+\infty} \left(\sum_{i=1}^{r} \left(\sum_{j=1}^{n_i} r_{ij} c_{j-1}^{h+j-1} \right) \alpha_i^h \right) x^h \qquad (1.13)
\end{aligned}$$

De (1.12) et (1.13), on déduit que

$$u_h = \sum_{i=1}^{r} P_i(h)\alpha_i^h,$$

où

$$P_i(h) = \sum_{j=1}^{n_i} r_{ij} c_{j-1}^{h+j-1}$$

D'autre part, les combinaisons c_{j-1}^{h+j-1} sont des polynômes de degré $j-1$.
Alors, pour tout $i = 1, ...r$, les $P_i(h)$ sont des polynômes de degré inférieur ou égale $n_i - 1$.

Unicité

Comme la suite $(u_n)_{n\in\mathbb{N}}$ est de degré k, alors on peut supposer que $c_0 \neq 0$, et dans ce cas, toutes les racines α_i, $\overline{i = 1, r}$ sont différentes de zéro.
Posons

$$P_i(x) = \sum_{j=0}^{n_i-1} p_{ij} x^j \text{ (car } \deg(P_i) \leq n_i - 1)$$

Or les p_{ij}, $1 \leq i \leq r$ et $0 \leq j \leq n_i - 1$ sont les inconnues d'un système de k équations linéaires obtenues à partir de :

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n$$

et les conditions initiales $u_0, \ldots\ldots\ldots, u_{k-1}$.
La formule précédente peut s'écrire sous la forme

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n = \sum_{i=1}^{r} \sum_{j=0}^{n_i-1} p_{ij} n^j \alpha_i^n, \tag{1.14}$$

où $n = 0, \ldots\ldots, k-1$.
Le déterminant du système (1.14) est de la forme

$$\begin{vmatrix} 1 & 0 & . & 1 & 0 & . & 0 \\ \alpha_1 & \alpha_1 & . & \alpha_r & \alpha_r & . & \alpha_r \\ \alpha_1^2 & 2\alpha_1^2 & . & \alpha_r^2 & 2\alpha_r^2 & . & 2^{n_r-1}\alpha_r^2 \\ \alpha_1^3 & 3\alpha_1^3 & . & \alpha_r^3 & 3\alpha_r^3 & . & 3^{n_r-1}\alpha_r^3 \\ . & . & . & . & . & . & . \\ \alpha_1^{k-1} & (k-1)\,\alpha_1^{k-1} & . & \alpha_r^{k-1} & (k-1)\,\alpha_r^{k-1} & . & (k-1)^{n_r-1}\,\alpha_1^{k-1} \end{vmatrix} \tag{1.15}$$

On va démontrer que le déterminant (1.15) n'est pas nul, ce qui signifie que les coéfficients p_{ij} sont uniques.

Pour cela, il suffit de démontrer que les vecteurs colonnes de (1.15) sont linéairements indépendants .
Supposons donc qu'il existe des constantes $a_0, \ldots ., a_{k-1}$ tels que

$$\sum_{l=0}^{k-1} a_l l^i \alpha_j^l = 0, \tag{1.16}$$

pour tout $j = \overline{1,\ r}$ et $i = \overline{0,\ n_j - 1}$.
On pose maintenat

$$C(x) = \sum_{l=0}^{k-1} a_l x^l \tag{1.17}$$

Et on définit

$$\begin{cases} C_0(x) = C(x) \\ C_{i+1}(x) = xC_i'(x)\,; \forall i \geq 0 \end{cases}$$

Moyennant de (1.6), il s'ensuit

$$C_i(\alpha_j) = 0, \text{ pour tout } j \overline{= 1, r} \text{ et } i \overline{= 0, n_j \ - 1}$$

Le lemme (1.2.2) implique que $C(x)$ est divisible par $(x - \alpha_1)^{n_1}, (x - \alpha_2)^{n_2}, \ldots, (x - \alpha_r)$.
Dans ce cas, il existe un polynôme $q(x)$ tel que

$$C(x) = (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \ \ldots (x - \alpha_r)^{n_r} q(x)$$

Ce qui implique que

$$\deg(C(x)) \geq n_1 + \ \ldots\ldots + n_r = k, oubienC(x) = 0$$

D'après (1.17), la première option n'est pas satisfaite, alors $C(x)$ est identiquement nul, et donc

$$a_0 = a_1 = \ldots = a_{k-1} = 0$$

Réciproquement :
Supposons que $(u_n)_{n \in \mathbb{N}}$ s'écrit sous la forme

$$u_n = \sum_{i=1}^{r} P_i(n)\, \alpha_i^n$$

On veut montrer que

$$u_n = c_{k-1}u_{n-1} + c_{k-2}u_{n-2} + \ \ . . . + c_0u_{n-k}$$

On étude la différence

$$D = u_n - c_{k-1}u_{n-1} - c_{k-2}u_{n-2} - \ \ . . . - c_0u_{n-k}$$

Alors

$$D = \sum_{i=1}^{r} P_i\left(n\right)\alpha_i^n - \sum_{s=1}^{k} c_{k-s} \sum_{i=1}^{r} P_i\left(n-s\right)\alpha_i^{n-s}$$

En posant $c_k = -1$ et $P_i\left(x\right) = \sum\limits_{j=0}^{n_i-1} p_{ij}\ x^j$ dans l'égalité précédente, on obtient

$$\begin{aligned} D &= -\sum_{s=0}^{k} c_{k-s} \sum_{i=1}^{r} P_i\left(n-s\right)\alpha_i^{n-s} \\ &= -\sum_{i=1}^{r}\sum_{s=0}^{k}\sum_{j=0}^{n_i-1} p_{ij}\left(n-s\right)^j c_{k-s}\alpha_i^{n-k}\alpha_i^{k-s} \\ &= -\sum_{i=1}^{r}\alpha_i^{n-k}\sum_{j=0}^{n_i-1} p_{ij}\sum_{s=0}^{k} c_{k-s}\left(n-s\right)^j\alpha_i^{k-s} \end{aligned}$$

Moyennant maintenant du lemme (1.2.3), il s'ensuit

$$\begin{aligned} \sum_{s=0}^{k} c_{k-s}\left(n-s\right)^j\alpha_i^{k-s} &= -n^j\alpha_i^k + \sum_{s=1}^{k} c_{k-s}\left(n-s\right)^j\alpha_i^{k-s} \\ &= -n^j\alpha_i^k + n^j\alpha_i^k = 0 \end{aligned}$$

Par suite

$$u_n = c_{k-1}u_{n-1} + c_{k-2}u_{n-2} + ... + c_0u_{n-k}\ ,\ \text{pour tout } n \geq k$$

Chapitre 2

Théorème de Skolem-Mahler-Lech

Cette partie vise à donner du théorème de Skolem-Mahler-Lech une preuve simple. Nous rappelons pour un point de départ quelques utils de l'analyse p-adique fréquemment utilisé dans notre travail. Ces rappels porteront sur le corps ultramétrique, le orps des nombres p-adiques, notamment la valuation p-adiquie, la norme p-adique et quelques proprietés analytiques du corps de nombres p-adiques. Nous présentons aussi le théorème de Strassman [21] .

Pour plus de détails sur ces notions et plus généralement pour tout ce qui concerne les séries de puissances p-adiques, nous indiquons les travaux [7] et plus récemment [13] .

Ensuite, nous dèmontrons le théorème de Skolem-Mahler-Lech.

2.1 Eléments d'nalyse p-adique

Le but de cette section est d'exposer les différents concepts et les notions indisponibles à l'étude de notre problème.

2.1.1 Corps ultramétrique

Définition 2.1.1 *Soit $\mathbb{k}$ un corps munit d'une norme $\|.\|$.*

On dit que la norme $\|.\|$ est ultramétrique (non-Archimédiènne), si et seulement si

$$\forall x,\, y \in \mathbb{k} : \|x + y\| \leq \max\{\|x\|, \|y\|\} \tag{2.1}$$

Tout corps munit d'une norme non-archimédiènne s'appelle un corps ultamétrique.

Remarque 2.1.2 *Si $d_{\|.\|}$ est la distance induite par la norme $\|.\|$, alors la relation pré-*

cédente peut s'écrire sous la forme

$$\forall x,\ y,\ z \in \mathbb{k} : d_{\|.\|}(x,z) \leq \max\left\{d_{\|.\|}(x,y), d_{\|.\|}(y,z)\right\} \tag{2.2}$$

Proposition 2.1.3 *Si* $\|.\|$ *est ultramétrique, alors*

$$\forall n \in \mathbb{N} : \|n\| \leq 1 \tag{2.3}$$

Preuve. Supposons que $\|.\|$ est ultramétrique et montrons par récurrence que

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

Pour $n = 1$; on a

$$\|1\| = 1 \leq 1.$$

Supposons maintenant que

$$\|n-1\| \leq 1$$

Alors

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

■

2.1.2 Corps des nombres p-adiques

Valuations p-adiquies

Définition 2.1.4 ***(valuation p-adique)*** *Soit* p *un nombre premier et soit* $x \in \mathbb{N}$*. On appelle valuation p-adique du* x *notée* $v_p(x)$ *le plus grand exposant de* p *tel que* $p^{v_p(x)}$ *divise* x*. C'est-à-dire*

$$\begin{array}{rccl} v_p: & \mathbb{N} & \longrightarrow & \mathbb{N} \cup \{+\infty\} \\ & x & \longmapsto & v_p(x) = \begin{cases} \max\{r \in \mathbb{Z}_+ : p^r/x\} & , \ si\ x \neq 0 \\ +\infty & , \ si\ x = 0 \end{cases} \end{array} \tag{2.1}$$

L'expression (2.4) peut s'écrire sous la forme

$$x = p^{v_p(x)}.x',\ où\ (p, x') = 1 \tag{2.5}$$

Il est claire que si $x = \frac{a}{b} \in \mathbb{Q}^*$, on trouve

$$v_p(x) = v_p(a) - v_p(b) \tag{2.6}$$

Norme p-adique

Définition 2.1.5 ***(norme p-adique)*** *Soit p un nombre premier. La norme p-adique d' un nombre rationnel x est une application $\|.\|_p : \mathbb{Q} \longrightarrow \mathbb{R}_+$ définie par*

$$x \longmapsto \|x\|_p = \begin{cases} p^{-v_p(x)}, \text{ si } x \neq 0 \\ 0, \text{ si } x = 0 \end{cases} \tag{2.7}$$

Exemple 2.1.6 *Pour la distance usuelle, on a*

$$d_{|.|}(10,3) = |10-3| = 7$$

Tandis que pour la norme $5-$adique on trouve

$$d_{|.|_5}(10,3) = \|10-3\|_5 = \|7\|_5 = 5^0 = 1$$

car

$$\begin{aligned} 7 &= 2 + 1.5 \\ &\Rightarrow V_5(7) = 0 \end{aligned}$$

Lemme 2.1.7 *Soit $p > 2$ un nombre premier, alors pour tout $n \in \mathbb{N}$, nous avons*

$$v_p\left(\frac{p^n}{n!}\right) \geq n\,\frac{p-2}{p-1} \tag{2.8}$$

Preuve. Pour tout $n \in \mathbb{N}$, on a

$$v_p\left(\frac{p^n}{n!}\right) = v_p(p^n) - v_p(n!) = n - v_p(n!)$$

D'autre part

$$\begin{aligned} v_p(n!) &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... \\ &\leq \frac{n}{p} + \frac{n}{p^2} + ... = \frac{n}{p-1} \end{aligned}$$

Donc

$$v_p\left(\frac{p^n}{n!}\right) \geq n - \frac{n}{p-1} = n\,\frac{p-2}{p-1}$$

■

Les nombres p-adiques

On sait que $\mathbb{R}$ est la complétion de $\mathbb{Q}$ par rapport à la valeur absolue usuelle, et dans ce cas les éléments de $\mathbb{R}$ sont les classes d'équivalences des suites de Cauchy de $\mathbb{Q}$. La même procédure se fait pour une valeur absolue ultramétrique $\|.\|_p$. La complétion de $\mathbb{Q}$ par rapport à la valeur absolue $\|.\|_p$ donne un corps ultramétrique appelé corps des nombres $p-$adiques et se note $\mathbb{Q}_p$. Ainsi les éléments de $\mathbb{Q}_p$ sont les classes d'équivalences des suites de Cauchy dans $\mathbb{Q}$, muni de la relation suivante :

$$(a_n)\ R\ (b_n) \iff \lim_{n\longrightarrow\infty} \|a_n - b_n\|_p = 0 \tag{2.9}$$

Remarque 2.1.8 *La valeur absolue $\|.\|_p$ peut être prolonger de $\mathbb{Q}$ sur tout $\mathbb{Q}_p$ de la façon suivante :*

Pour tout $x \in \mathbb{Q}_p$, il existe une suite $(x_n) \in \mathbb{Q}$ telle que

$$\lim_{n\longrightarrow\infty} \|x_n - x\|_p = 0 \tag{2.10}$$

Définition 2.1.9 ***Remarque 2.1.10*** *On note par $\mathbb{Z}_p$ l'ensemble des entiers p-adiques .*

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : a = \sum_{n=0}^{\infty} \alpha_n p^n,\ \text{pour tout } 0 \leq \alpha_n \leq p-1 \right\} \tag{2.11}$$

Puisque dans le cas d'un entier p-adique a, $v_p(x)$ est positive . On a la caractérisation suivante

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : \|a\|_p = p^{-V_p(x)} \leq 1 \right\} \tag{2.12}$$

C'est-à-dire que $\mathbb{Z}_p$ représente le disque d'unité de rayon 1 et de centre 0 .

Remarque 2.1.11 *Le corps $\mathbb{Q}_p$ est l'ensemble des fractions de $\mathbb{Z}_p$.*
ie :

$$\mathbb{Q}_p = \left\{ \frac{a}{b}\ ;\ (a,b) \in \mathbb{Z}_p.\mathbb{Z}_p^* \right\} \tag{2.13}$$

Propriétés analytiques des nombres p-adiques Généralement les propriétés analytiques de $\mathbb{Q}_p$ sont analogues à celles de $\mathbb{R}$, mais la différence est remarquable entre ses deux corps dans les critères de convergence des suites et des séries de puissances .

Voici quelques propriétés analytiques de $\mathbb{Q}_p$.

Théorème 2.1.12 *Soit $(a_n)_{n\in\mathbb{N}}$ une suite de $\mathbb{Q}_p$, alors $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy convergente si et seulement si*

$$\lim_{n\longrightarrow\infty} \|a_{n+1}-a_n\|_p = 0 \tag{2.14}$$

Preuve. Supposons à présent que

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

Alors

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

En tenant compte maintenant des inégalités

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

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

On déduit que (a_n) est une suite de Cauchy . ■

Remarque 2.1.13 *En générale, la dernière propriété n'est pas vérifiée dans $\mathbb{R}$.*
C'est-a-dire

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

n'implique pas que $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy.

Proposition 2.1.14 *Si la série $\sum\limits_{i=0}^{\infty}\|a_i\|_p$ converge dans $\mathbb{R}$, alors $\sum\limits_{i=0}^{\infty}a_i$ converge dans $\mathbb{Q}_p$.*

Preuve. Puisque $\sum\limits_{i=0}^{\infty}\|a_i\|_p$converge, alors la suite des sommes partielles

$$\left(S_n = \sum_{i=0}^{n}\|a_i\|_p\right)_{n\in\mathbb{N}}$$

est de Cauchy.
ie :

$$\forall\varepsilon\succ 0,\ \exists N\in\mathbb{N}\ ;\ \forall m\succ n\geq N : \sum_{i=n+1}^{m}\|a_i\|_p \prec \varepsilon$$

Soit $\left(\overline{S}_n = \sum\limits_{i=0}^{n} a_i\right)_{n\in\mathbb{N}}$ la suite des sommes partielles de la série $\sum\limits_{i=0}^{\infty} a_i$. Alors

$$\begin{aligned}\left\|\overline{S}_m - \overline{S}_n\right\|_p &= \left\|\sum_{i=n+1}^{m} a_i\right\|_p \\ &\leq \sum_{i=n+1}^{m} \|a_i\|_p \prec \varepsilon\end{aligned}$$

Ce qui implique que $\left(\overline{S_n} = \sum\limits_{i=0}^{n} a_i\right)_{n\in\mathbb{N}}$ est une suite de Cauchy.

Par suite $\sum\limits_{i=0}^{\infty} a_i$ converge dans $\mathbb{Q}_p$. ■

Proposition 2.1.15 *Soit* $(a_n)_{n\in\mathbb{N}}$ *une suite de* $\mathbb{Q}_p$ *.*
Si $\lim\limits_{n\longrightarrow\infty} a_n = a$ *dans* $\mathbb{Q}_p$*, alors*

$$\exists\ N \in \mathbb{N}\ ,\ \forall n \geq N\ :\ \|a_n\|_p = \|a\|_p \tag{2.15}$$

Preuve. Supposons que $(a_n)_{n\in\mathbb{N}}$ est une suite de $\mathbb{Q}_p$, telle que

$$\lim_{n\longrightarrow\infty} a_n = a$$

$(a_n)_{n\in\mathbb{N}}$ est convergente dans $\mathbb{Q}_p$; et donc elle est de Cauchy .
C'est-à-dire

$$\forall\varepsilon \succ 0\ ,\ \exists n_0 \in \mathbb{N}\ ;\ \forall m \succ n \geq n_0 \Rightarrow \|a_m - a_n\|_p \prec \varepsilon$$

D'autre part

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

Alors $\left(\|a_n\|_p\right)_n$ est une suite de Cauchy dans $\mathbb{R}$, donc elle est convergente.
Posons

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

Si $\|a\|_p \neq 0 \implies \|a\|_p \succ 0$.
Alors, pour $\varepsilon = \frac{l}{2} \succ 0$, il vient

$$\exists n_1 \in \mathbb{N},\ \forall n \geq n_1 :\ \left|\|a_n\|_p - l\right| \prec \frac{l}{2}$$

Ce qui implique

$$\|a_n\|_p \succ \frac{l}{2}$$

De même, puisque $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{Q}_p$, alors, pour $\varepsilon = \frac{l}{2}$

$$\exists n_2 \in \mathbb{N} \text{ tel que } \forall m \succ n \geq n_2 \implies \|a_m - a_n\|_p \prec \frac{l}{2}$$

Donc, si $n \succ n_3 = \max\{n_1, n_2\}$, on a

$$\begin{aligned} \|a_m\|_p &= \|a_m - a_n + a_n\|_p \\ &\leq \max\left\{\|a_m - a_n\|_p, \|a_n\|_p\right\} = \|a_n\|_p \end{aligned}$$

Faisons m tends vers $+\infty$, on aura

$$\|a_n\|_p = \|a\|_p \ , \forall n \succ n_3$$

■

Proposition 2.1.16 *Soit* $\sum\limits_{n=0}^{\infty} a_n$ *une série dans* $\mathbb{Q}_p$ *; alors*

$$\sum_{n=0}^{\infty} a_n \text{ converge dans } \mathbb{Q}_p \iff \lim_{n\longrightarrow\infty} a_n = 0 \tag{2.16}$$

De plus

$$\left\|\sum_{n=0}^{\infty} a_n\right\|_p \leq \max_{n\geq 0}\left\{\|a_n\|_p\right\} \tag{2.17}$$

Preuve.

1) *On sait que la série* $\sum\limits_{n=0}^{\infty} a_n$ *converge si la suite des sommes partielles* $\left(S_n = \sum\limits_{i=0}^{n} a_i\right)_{n\in\mathbb{N}}$ *est convergente .*

Et comme

$$S_n - S_{n-1} = a_n$$

Alors, d'après le théorème (2.1.12)*, la série* $\sum\limits_{n=0}^{\infty} a_n$ *converge si et seulement si* a_n *tend vers* 0*, quand* n *tend vers* $+\infty$

2) *Supposons que* $\sum\limits_{n=0}^{\infty} a_n$ *converge . Puisque* a_n *tend vers* 0*, alors*

$$\exists N \in \mathbb{N} : \left\|\sum_{n=0}^{\infty} a_n\right\|_p = \left\|\sum_{n=0}^{N} a_n\right\|_p$$

De plus

$$\max\left\{\|a_n\|_p, \ 0 \leq n \leq N\right\} = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

D'où

$$\left\|\sum_{n=0}^{N} a_n\right\|_p \leq \max\left\{\|a_n\|_p\,,\; 0 \leq n \leq N\right\} = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

■

Théorème 2.1.17 *(Théorème de permutation)*

Soit $b_{i,j} \in \mathbb{Q}_p$, $i, j = 1, 2, ...$vérifie le critère de convergence suivant

$$\forall \varepsilon \succ 0,\ \exists n_0 = n_0(\varepsilon),\ tel\ que\ \max(\ i,\ j\ ) \geq n_0 \Rightarrow ||b_{i,j}||_p \prec \varepsilon$$

Alors, les deux séries $\sum\limits_i \left(\sum\limits_j b_{i,j}\right)$ et $\sum\limits_j \left(\sum\limits_i b_{i,j}\right)$ sont convergentes.

De plus

$$\sum_i \left(\sum_j b_{i,j}\right) = \sum_j \left(\sum_i b_{i,j}\right) \tag{2.18}$$

Preuve. En effet. Nous avons

$$\sum_j b_{i,j} \leq \max_j ||b_{i,j}||_p \prec \varepsilon, \text{ pour tout } j\ \geq n_0$$

De même

$$\sum_i b_{i,j} \leq \max_i ||b_{i,j}||_p \prec \varepsilon, \text{ pour tout } i \geq n_0$$

D'aprés la proposition (2.1.15), les deux séries $\sum\limits_i \left(\sum\limits_j b_{i,j}\right)$ et $\sum\limits_j \left(\sum\limits_i b_{i,j}\right)$ sont convergentes.

D'autre part

$$\begin{aligned}\left|\sum_{i=1}^{+\infty}\left(\sum_{j=1}^{+\infty} b_{i,j}\right) - \sum_{i=1}^{N}\left(\sum_{j=1}^{N} b_{i,j}\right)\right| &= \left|\sum_{i=1}^{N}\left(\sum_{j=N+1}^{+\infty} b_{i,j}\right) + \sum_{i=N+1}^{+\infty}\left(\sum_{j=1}^{+\infty} b_{i,j}\right)\right| \\ &\leq \max_{\max(\ i,\ j\ )\geq N} ||b_{i,j}||_p \leq \max_{\max(\ i,\ j\ )\geq n_0} ||b_{i,j}||_p \prec \varepsilon\end{aligned}$$

Ce qui implique que

$$\sum_{i=1}^{N}\left(\sum_{j=1}^{N} b_{i,j}\right) \overset{N\to+\infty}{\longrightarrow} \sum_{i=1}^{+\infty}\left(\sum_{j=1}^{+\infty} b_{i,j}\right)$$

Et comme

$$\sum_{i=1}^{N}\left(\sum_{j=1}^{N} b_{i,j}\right) = \sum_{j=1}^{N}\left(\sum_{i=1}^{N} b_{i,j}\right)$$

On déduit que

$$\sum_{i}\left(\sum_{j} b_{i,j}\right) = \sum_{j}\left(\sum_{i} b_{i,j}\right)$$

■

Le résultat suivant est essentiel pour l'étude de notre problème.

Théorème 2.1.18 *(**théorème de Strassman** [21]). Soit*

$$F(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[x]$$

une série de puissances non nule.
Si $\lim\limits_{n\longrightarrow+\infty} a_n = 0$, *alors* $F(x)$ *converge pour tout* x *de* $\mathbb{Z}_p$.
De plus, s'il existe un entier positif N, *tel que*

$$\begin{cases} i\ )\ \|a_N\|_p = \max\limits_{n\geq 0}\left\{\|a_n\|_p\right\} \\ ii\ )\ \|a_n\|_p \prec \|a_N\|_p\,, \text{pour } n \succ N \end{cases}$$

Alors $F(x) : \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ *admet au maximum* N *zéros.*

Preuve. Par récurrence .
Si $N = 0$, notre hypothèse signifie que $\|a_0\|_p \succ \|a_n\|_p$, $\forall n \succ 0$.
On va montrer que dans ce cas $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$.
Supposons le contraire. C'est-à-dire

$$F(x) = a_0 + a_1 x + ... + ... = 0$$

On en déduit que

$$\begin{aligned} \|a_0\|_p &= \left\|a_1 x + a_2 x^2 + \ .\ .\ .+\ .\ .\ .\ .\right\|_p \\ &\leq \max_{n\geq 1}\left\{\|a_n\|_p\right\} \\ &\prec \|a_0\|_p \end{aligned}$$

Qui est une contradiction.
Donc $F(x)$ n'admet aucune racine dans $\mathbb{Z}_p$.
Supposons maintenant qu'il existe $N \succ 0$ et que les deux hypothèses du théorème sont satisfaites.
Cest-à-dire

$$\|a_N\|_p = \max_{n\geq 0}\left\{\|a_n\|_p\right\}$$

et que

$$\|a_n\|_p \prec \|a_N\|_p \text{, pour tout } n \succ N$$

Montrons que $F(x)$ admet au maximum N zéros dans $\mathbb{Z}_p$.
Soit $\alpha \in \mathbb{Z}_p$ tel que $F(\alpha) = 0$, alors

$$\forall x \in \mathbb{Z}_p : F(x) = F(x) - F(\alpha)$$

$$= \sum_{n=0}^{\infty} a_n (x^n - \alpha^n)$$

$$\begin{aligned} &= (x-\alpha)\sum_{n\geq 1}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j} \\ &= (x-\alpha)\sum_{j=0}^{\infty} b_j x^j,\ \text{ où } b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k \\ &= (x-\alpha)\, g(x) \text{ , où } g(x) = \sum_{j=0}^{\infty} b_j x^j, \end{aligned}$$

Nous avons

$$\begin{aligned} \|b_j\|_p &\leq \max\left\{\|a_{j+1+k}\|_p\right\} \\ &\leq \|a_N\|_p \text{ ; } \forall j = o, ... \end{aligned}$$

En particulier

$$\begin{aligned} \|b_{N-1}\|_p &= \left\|a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \ ...+\ ...\right\|_p \\ &= \|a_N\|_p = \max_j \|b_j\|_p \end{aligned}$$

Et Si $j \succ N-1$, on a

$$\begin{aligned} \|b_j\|_p &\leq \max_{k\geq 0}\left\{\|a_{j+1+k}\|_p\right\} \leq \max_{i\geq N+1}\left\{\|a_i\|_p\right\} \\ &\prec \|a_N\|_p = \|b_{N-1}\|_p \end{aligned}$$

Par l'hypothèse de récurrence, on déduit que $g(x)$ admet au maximum $N-1$ zéros. Par suite, g admet au maximum N zéros. ■

2.2 Théorème de Skolem-Mahler Lech

Théorème 2.2.1 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite définie par $u_n = \sum_{i=1}^{r} P_i(n)\,\alpha_i^n$ sur $\mathbb{Q}_p$, où $\alpha_i \equiv 1(\bmod p)$, pour tout $i = \overline{1.r}$.*
Et soit

$$\mathbb{Z}(u_n) = \{i \in \mathbb{N} : u_i = 0\}$$

Alors $\mathbb{Z}(u_n)$ est une réunion finie d'ensembles finis ou périodiques.

Remarque 2.2.2 *On va construire pour un point de départ $p-1$ série de puissances*

$$F_r(x) = \sum_{j=0}^{\infty} f_j^r x^j, \text{ pour tout } r = \overline{0.p-2}. \tag{2.19}$$

telles que

$$F_r(s) = \sum_{i=1}^{r} P_i\left(r + s(p-1)\right)\alpha_i^{r+s(p-1)}, \text{ pour tout } s \in \mathbb{N} \tag{2.20}$$

Comme

$$\alpha_i^{r+s(p-1)} = \alpha_i^r\left((\alpha_i)^{p-1}\right)^s$$

On va d'abord étudier le cas

$$\alpha^n = F(n),\ n \in \mathbb{N}$$

Nous avons le lemme suivant

Lemme 2.2.3 *Soit $p > 2$ un nombre premier. Si $\alpha \in \mathbb{Q}_p$ avec $\alpha \equiv 1(\bmod p)$, alors pour tout $x \in \mathbb{Z}_p$, il existe une serie de puissances*

$$F(x) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} k_{ij}\frac{\beta^i}{i!}x^j, \tag{2.21}$$

qui converge dans $\mathbb{Z}_p$ et que

$$F(n) = \alpha^n, \forall n \in \mathbb{N}. \tag{2.22}$$

Preuve. Soient n un entier positif et $\beta \in \mathbb{Q}_p$, tel que

$$\beta = \alpha - 1$$

Alors

$$\begin{aligned}
\alpha^n &= (\beta+1)^n = \sum_{i=0}^{n} c_n^i \beta^i \\
&= \sum_{i=0}^{+\infty} c_n^i \beta^i \text{ (car } \left|\left|c_n^i \beta^i\right|\right|_p \leq 1 \cdot ||\beta||_p^i \leq p^{-i} \to 0, \text{ quand } i \to +\infty) \\
&= \sum_{i=0}^{+\infty} n(n-1).......(n-i+1)\frac{\beta^i}{i!}
\end{aligned}$$

Posons

$$x(x-1).......(x-i+1) = \sum_{j=0}^{+\infty} k_{ij} x^j \text{ (avec } k_{ij} = 0, \text{si } j \succ i)$$

Donc

$$\alpha^n = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} k_{ij} n^j \frac{\beta^i}{i!}$$

On veut vérifier qu'il est possible de permuter les deux sommes.
Si $j \succ i$, alors

$$\left|\left|k_{ij} n^j \frac{\beta^i}{i!}\right|\right|_p = ||0||_p = 0$$

Si $j \leq i$, alors

$$\begin{aligned}
\left|\left|k_{ij} n^j \frac{\beta^i}{i!}\right|\right|_p &\leq 1 \cdot \left|\left|\frac{\beta^i}{i!}\right|\right|_p \leq ||\beta||_p^i \cdot \left|\left|\frac{1}{i!}\right|\right|_p \\
&\leq p^{-i} \cdot p^{\frac{i}{p-1}} = p^{-i\frac{p-2}{p-1}} \underset{i\to\infty}{\longrightarrow} 0, \text{ pour tout } p > 2
\end{aligned}$$

Donc, on peut permuter les deux sommes. Par suite

$$\begin{aligned}\alpha^n &= \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty}k_{ij}\frac{\beta^i}{i!}\right)n^j\\ &= \sum_{j=0}^{\infty}f_j n^j\end{aligned}$$

où

$$f_j = \sum_{i=0}^{\infty}k_{ij}\frac{\beta^i}{i!}.$$

Posons

$$F(x) = \sum_{j=0}^{\infty}f_j x^j$$

Il est claire que $F(x)$ converge dans $\mathbb{Z}_p$, et que $F(n) = \alpha^n$, pour tout $x \in \mathbb{Z}_p$. ■

Remarque 2.2.4 *En peut utiliser le résultat du lemme précédent si en remplace α par α^{p-1}, car*

$$\alpha \equiv 1(\operatorname{mod} p) \Rightarrow \alpha^{p-1} \equiv 1(\operatorname{mod} p)$$

Preuve du théorème de Skolem-Mahler-Lech

La preuve de ce théorème se déduite alors de manière presque immédiate.
En effet, soit

$$u_n = \sum_{i=1}^{r}P_i\left(n\right)\alpha_i^n,$$

où $\alpha_i \equiv 1(\operatorname{mod} p)$.
Pour tout $n \in \mathbb{N}$, on peut écrire $n = m + (p-1)N$, où $0 \leq m \leq p-2$ et $N \in \mathbb{N}$.
Alors

$$u_{m+(p-1)N} = \sum_{i=1}^{r}h_i(m+(p-1)N){\alpha_i}^m({\alpha_i}^{p-1})^N$$

Donc, d'aprés le lemme précédent, chacunne des suites ci-dessous

$$\begin{aligned}
u_{(p-1)N} &= \sum_{i=1}^{r} h_i((p-1)N)(\alpha_i{}^{p-1})^N \\
u_{1+(p-1)N} &= \sum_{i=1}^{r} h_i(1+(p-1)N)\alpha_i(\alpha_i{}^{p-1})^N \\
&\ . \\
&\ . \\
&\ . \\
u_{(p-2+(p-1)N)} &= \sum_{i=1}^{r} h_i(p-2)+(p-1)N)\alpha_i{}^{p-2}(\alpha_i{}^{p-1})^N
\end{aligned}$$

est égale à une série de puissances qui converge dans $\mathbb{Z}_p$.
D'aprés le théorème de Strassman,elle admet un nombre fini de zéros ou identiquement nulle.
Par suite, l'ensemble $\mathbb{Z}(u_n)$ est une réunion finie d'ensembles finis ou périodiques.

Conclusion 2.2.5 *Cette étude réalisée constitue une partie fondamentale dans les travaux de recherche dans le domaine de la théorie des suites récurrentes linéaires . L'un des passionnant sujets évoquant celles-ci est le problème de Skolem pour les suites récurrentes linéaires. Ce domaine n'est pas complètement investi, car les problèmes de Skolem pour des suites récurrentes ayant une loi de comportement non linéaire sont encore ouverts.*
Signalons aussi que des études récentes sont faites dans le domaine de la recherche des solutions des suites récurrentes non linéaires et que la voie dans cette direction est loin d'être terminée.

Bibliographie

[1] A. M. Robert, A Course in p-adic Analysis, Springer-Verlag Berlin Heidelbery New York, 2000.

[2] C. Lech. A note on recurring series. Ark. Mat. 2 (1953), 417–421.

Everest, G., van der Poorten, A., Shparlinski, I., Ward, T. : Recurrence Sequences, Mathematical Surveys and Monographs, vol. 104. Am. Math. Soc., Providence, RI (2003)

[3] G. Hansel. Une d´emonstration simple du théorème de Skolem-Mahler-Lech. Theoret. Comput. Sci. 43 (1986), no. 1, 91–98.

[4] K. Mahler : Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen. Proc. Akad. Wet. Amsterdam 38, 51–60 (1935)

[5] T. Skolem : Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen. In : Comptes rendus du congrés des mathèmaticiens scandinaves, Stockholm, 1934, pp. 163–188. (1935).

[6] V. Halava, T. Harju,M. Hirvensalo and J. Karhumaki. Skolem's Problem– On the Border Between Decidability and Undecidability. TUCS Technical Report No 683,pp.19, 21-22. (April 2005)

[7] Y . Amice, Les nombres p-adiques .Colledtion sup, no 14, Les presses universitaires de France, Paris
1975 .

[8] J . Berstel, sur le calcul des termes d'une suite récurrente linéaire, exposé fait à
l'I .R .R .I .A(Rocquencourt) en mars 1974 .

[9] Berstel and M . Mignotte ; deux propriétés décidables des suites récurrentes linéaires . Bull . Soc .
Math . France . 104, pp 175-184(1976) .

[10] F . Beukers, the multiplicity of binary recurrences, composito math .40(1980),pp 251-267 .

[11] P . Borwein and T . Erdelyi : polynomials and polynomial inequalities . Springer(1995) .

[12] L . Cerlienco, M . Mignotte et F . Piras, Suites récurrentes linéaires . Propriétés algébriques et
arithmétiques, L'enseignement Mathématiques 33(1987), pp67-108 . .

[13] S . Katok, real and p-adic analysis, course notes for Math 497C, Mass Program, Fall 2000(2001) .

[14] M . Mignotte . Suites récurrentes linéaires, Séminaire Delange-Pisot-Poitou . Théorie des nombres, tome 15, no 2 (1973-1974), exp .no G 14, pp 1-9 .

[15] P . Robba, Zéros de suites récurrentes linéaires, Groupe de travail ultramétrique, tome5 (1977-1978), exp .no 13, pp 1-5 .

[16] H .P . Schlickewei, Multiplicities of recurrence sequences, Acta .Math . 176 (1996), pp 171-243 .

[17] H .P . Schlickewei and A .J . Van der Poorten, Zeros of recurrence sequences, Bull . Austral . Math . Soc . 44(1991), pp 215-223 .

[18] W . M . Schmidt, The zero multiplicity of linear recurrence sequences, Acta . Math . 182(1999), pp 243-282 .

[19] W . M . Schmidt, zeros of linear recurrence sequences, publ . Math . Debrecen . 56(2000), pp 609-630 ..

[20] N .K . Vereshchagin, Occurrence of zero in a linear recursive sequence, Vestnik Moskov . Univ . Math . Vol .41(1986) .

[21] R. Strassman, Uber den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen, J. furbMath. 159 (1928), 13-28.