Zéros d'une suite récurrente linéaire, théorème de Skolem-Mahler-Lech

Camille Mondon

2019

Table des matières

1 Présentation du problème **1**

2 Éléments d'analyse p-adique, théorème de Strassmann **2**
2.1 Définitions, critères de convergence dans $\mathbb{Q}_p$ 2
2.2 Théorème de Strassmann pour les fonctions analytiques 2

3 Démonstration du théorème de Skolem-Mahler-Lech **3**
3.1 Notation matricielle 3
3.2 Restriction au corps engendré par les coefficients de la suite 3
3.3 Plongement de $\mathbb{Q}(\Lambda)$ dans $\mathbb{Q}_p$ 3
3.4 Démonstration dans le cas d'une suite de $\mathcal{R}(\mathbb{Z}_p)$ 4
3.4.1 Réduction modulo p 4
3.4.2 Finitude du nombre de zéros 4
3.5 Contre-exemple en caractéristique positive 4

4 Problème de Skolem : questions de décidabilité **5**
4.1 Finitude de l'ensemble des zéros 5
4.2 Vacuité de l'ensemble des zéros 5

A Preuves **1**
A.1 Quelques résultats d'analyse p-adique 1
A.2 Théorème de plongement de Cassels 2
A.3 Théorème de Blondel-Portier 4

B Bibliographie **4**

1 Présentation du problème

Énoncé : Comment le théorème de Skolem-Mahler-Lech illustre-t-il l'efficacité des méthodes d'analyse p-adique ? Qu'en est-il de la complexité du problème de Skolem ?

Positionnement thématique : Mathématiques (Algèbre, Analyse), Informatique théorique

Mots-clés : Analyse p-adique, Suites récurrentes linéaires, Théorème de Skolem-Mahler-Lech, Problème de Skolem

Si $\mathbb{K}$ est un corps et si $m \in \mathbb{N}^*$, on note $\Omega_m(\mathbb{K}) = \{(a_0, a_1, \dots, a_{m-1}) \in \mathbb{K}^m, a_0 \neq 0\}$. Pour $a = (a_0, \dots, a_{m-1})$ dans $\Omega_m(\mathbb{K})$, soit P_a le polynôme :

$$X^m - \sum_{i=0}^{m-1} a_i X^i$$

et $\mathcal{E}_a(\mathbb{K})$ l'espace des suites $(x_n)_{n\geq 0}$ de $\mathbb{K}^{\mathbb{N}}$ telles que :

$$\forall\, n \in \mathbb{N}, x_{n+m} = \sum_{i=0}^{m-1} a_i x_{m+i}$$

Soit enfin

$$\mathcal{R}(\mathbb{K}) = \bigcup_{m\in\mathbb{N}^*} \left(\bigcup_{a\in\Omega_m(\mathbb{K})} \mathcal{E}_a(\mathbb{K}) \right)$$

l'espace des suites de $\mathbb{K}^{\mathbb{N}}$ vérifiant une relation de récurrence linéaire homogène à coefficients constants non dégénérée. On généralisera ces notations en remplaçant $\mathbb{K}$ par un anneau commutatif $\mathbb{A}$, en supposant de plus l'inversibilité de a_0.
L'objectif de ce TIPE est de démontrer le théorème suivant :

Théorème (Skolem-Mahler-Lech)**.** *Soit $\mathbb{K}$ un corps de caractéristique nulle, et $(x_n)_{n\geq 0}$ dans $\mathcal{R}(\mathbb{K})$. Alors :*

$$\{n \in \mathbb{N}, x_n = 0\}$$

est l'union disjointe d'un ensemble fini et de progressions arithmétiques de même raison.

Les preuves les plus éclairantes de ce théorème dans le cas des nombres rationnels reposent sur un argument d'analyse p-adique, donnant du sens à une somme qui ne convergerait pas dans $\mathbb{Q}$. Dans le cas général, un théorème de plongement dans $\mathbb{Q}_p$, déjà présent chez Lech, a été explicité par Cassels dans [1].
En 1985, George Hansel a proposé une démonstration dans le cas $\mathbb{K} = \mathbb{Q}$ ne faisant pas appel à l'analyse p-adique (reprouvant en fait un théorème dans un cas particulier).

Nous prenons ici le parti de présenter une preuve p-adique suivant celle de Cassels, mais adoptant le point de vue matriciel de Hansel pour étudier les suites récurrentes linéaires (et ainsi éviter l'utilisation du corps de rupture du polynôme caractéristique).

2 Éléments d'analyse p-adique, théorème de Strassmann

2.1 Définitions, critères de convergence dans $\mathbb{Q}_p$

Nous noterons, si p est premier, $\mathbb{Q}_p$ le corps des nombres p-adiques (i.e. le complété de $\mathbb{Q}$ pour la norme p-adique $|\cdot|_p$) et

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |x|_p \leq 1\} = \{x \in \mathbb{Q}_p, v_p(x) \geq 0\}$$

l'anneau des entiers p-adiques.

Le principal avantage qu'a $\mathbb{Q}_p$ sur $\mathbb{Q}$ est sa complétude, qui fournit des résultats d'existence, proches de l'analyse réelle. En voici la différence notoire :

Propriété (fondamentale)**.** *La norme p-adique vérifie l'inégalité ultramétrique :*

$$\forall\,(x,y) \in \mathbb{Q}_p, |x+y|_p \leq \max(|x|_p, |y|_p)$$

Cette forme forte de l'inégalité triangulaire simplifie l'analyse dans $\mathbb{Q}_p$, en fournissant notamment un critère explicite de convergence des suites (et séries), et un théorème des séries doubles valable sous une hypothèse plus faible que la sommabilité.

Propriété. *Soit $(u_n)_{n\geq 0} \in \mathbb{Q}_p^{\mathbb{N}}$. Alors s'équivalent :*

- *(u_n) converge dans $\mathbb{Q}_p$;*
- *$|u_{n+1} - u_n|_p \to 0$ (i.e. $v_p(u_{n+1} - u_n) \to +\infty$).*

Théorème 1 (Séries doubles)**.** *Soit $(u_{i,j})_{(i,j)\in\mathbb{N}^2}$ une famille d'éléments de $\mathbb{Q}_p$ telle que si $\varepsilon > 0$, il existe $N(\varepsilon) \in \mathbb{N}$ pour lequel :*

$$\forall\,(i,j) \in \mathbb{N}^2, \max(i,j) \geq N(\varepsilon) \Rightarrow |u_{i,j}|_p \leq \varepsilon$$

Alors les séries $\sum_{i\geq 0}\left(\sum_{j=0}^{j=+\infty} u_{i,j}\right)$ et $\sum_{j\geq 0}\left(\sum_{i=0}^{i=+\infty} u_{i,j}\right)$ convergent et sont égales.

2.2 Théorème de Strassmann pour les fonctions analytiques

L'argument p-adique essentiel dans la preuve du théorème de Skolem-Mahler-Lech est le théorème de Strassmann, qui majore le nombre de zéros d'une fonction somme d'une série entière non nulle sur $\mathbb{Z}_p$ (boule unité de $\mathbb{Q}_p$) :

Théorème 2 (Strassmann)**.** *Soit $\sum_{n\geq 0} a_n x^n$ une série entière sur $\mathbb{Q}_p$, non identiquement nulle et de rayon supérieur à 1 (ce qui équivaut à la convergence vers 0 de $(a_n)_{n\geq 0}$). Notons $f : \mathbb{Z}_p \to \mathbb{Q}_p$ sa fonction somme. Soit $N = N(a) \in \mathbb{N}$ l'entier tel que :*

- *si $n \leq N$, $|a_n|_p \leq |a_N|_p$;*
- *si $n > N$, $|a_n|_p < |a_N|_p$.*

Alors f s'annule au plus en N points de $\mathbb{Z}_p$.

3 Démonstration du théorème de Skolem-Mahler-Lech

Dans cette partie, nous fixons $m \in \mathbb{N}^*$ et $a \in \Omega_m(\mathbb{K})$.

3.1 Notation matricielle

Afin d'éviter le passage par le corps de rupture de P_a, on peut adopter un point de vue matriciel. Soit $M_a \in \mathcal{M}_m(\mathbb{K})$ la matrice compagnon de P_a :

$$M_a = \begin{pmatrix} 0 & \dots & \dots & 0 & a_0 \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & a_{m-1} \end{pmatrix}$$

Alors si $(x_n)_{x\geq 0} \in \mathcal{E}_a(\mathbb{K})$, on a en notant $X_n = \begin{pmatrix} x_n \\ \vdots \\ x_{n+m-1} \end{pmatrix}$ si $n \in \mathbb{N}$:

$$X_n = {M_a}^n X_0$$

En notant μ la première forme coordonnée sur $\mathbb{K}^m$, on a :

$$\{n \in \mathbb{N}, x_n = 0\} = \{n \in \mathbb{N}, {M_a}^n X_0 \in \operatorname{Ker} \mu\}$$

De plus, $\det M_a = P_a(0) = -a_0 \neq 0$ donc M_a est dans $\mathrm{GL}_m(\mathbb{K})$.

3.2 Restriction au corps engendré par les coefficients de la suite

Il suffit d'observer que si $(x_n)_{n\geq 0}$ est un élément de $\mathcal{E}_a(\mathbb{K})$, alors il est en fait dans $\mathcal{E}_a(\mathbb{Q}(\Lambda))$ où $\Lambda = \{x_0, \dots, x_{m-1}, a_0, \dots, a_{m-1}\}$ est finie.

3.3 Plongement de $\mathbb{Q}(\Lambda)$ dans $\mathbb{Q}_p$

On peut donc supposer que $\mathbb{K}$ est de la forme $\mathbb{Q}(\Lambda)$ où Λ est un ensemble fini.
Il s'agit alors de trouver un plongement de $\mathbb{K}$ dans un corps p-adique (i.e la donnée d'un nombre premier p et d'un morphisme de corps de $\mathbb{K}$ dans $\mathbb{Q}_p$) envoyant les coefficients de la suite dans $\mathbb{Z}_p$ et préservant l'inversibilité de M_a dans l'anneau $\mathbb{Z}_p$.
Le résultat-clé est le suivant (prouvé par Cassels dans [1]) :

Théorème 3 (Cassels)**.** *Si A est une partie finie de $\mathbb{K}^*$, l'ensemble des nombres premiers $p > 2$ pour lesquels il existe un morphisme de corps Φ de $\mathbb{K}$ dans $\mathbb{Q}_p$ envoyant A dans ${\mathbb{Z}_p}^*$ est infini.*

N.B. : Dans le cas $\mathbb{K} = \mathbb{Q}$, le théorème n'est pas utile (cf. [2]). En effet, quitte à multiplier M_a et X_0 par une constante (qui ne change pas l'ensemble des zéros), on peut supposer que $M_a \in \mathcal{M}_m(\mathbb{Z})$ et $X_0 \in \mathbb{Z}^m$. Il suffit alors de choisir un nombre premier p ne divisant pas $\det M_a$.

3.4 Démonstration dans le cas d'une suite de $\mathcal{R}(\mathbb{Z}_p)$

3.4.1 Réduction modulo p

Nous pouvons donc considérer que $\mathbb{K}$ est un sous-corps de $\mathbb{Q}_p$, que X_0 est dans ${\mathbb{Z}_p}^m$ et M_a dans $\mathrm{GL}_m(\mathbb{Z}_p)$. Notons $\overline{M_a} \in \mathrm{GL}_m(\mathbb{F}_p)$ la réduction modulo p de M_a, et ρ l'ordre de $\overline{M_a}$ dans $\mathrm{GL}_m(\mathbb{F}_p)$.
Nous allons alors établir que :

$$\{n \in \mathbb{N}, {M_a}^n X_0 \in \operatorname{Ker} \mu\}$$

est union d'un ensemble fini et de progressions arithmétiques de raison ρ.

3.4.2 Finitude du nombre de zéros

Soit $N \in \mathcal{M}_m(\mathbb{Z}_p)$ telle que ${M_a}^\rho = I_n + pN$. Fixons de plus $r \in \{0, \dots, \rho - 1\}$. Si $n \in \mathbb{N}$:

$$\mu({M_a}^{\rho n + r} X_0) = \sum_{k=0}^{n} \binom{n}{k} p^k \mu(N^k {M_a}^r X_0)$$

Posons, si $k \in \mathbb{N}$:

$$u_{r,k} = \mu(N^k {M_a}^r X_0) \in \mathbb{Z}_p$$

et

$$H_k = \frac{1}{k!} \prod_{i=0}^{k-1} (X - i)$$

le k-ème polynôme de Hilbert. Alors, il suffit pour prouver le théorème, de montrer que la fonction f_r définie par :

$$f_r(n) = \sum_{k=0}^{n} p^k u_{r,k} H_k(n) \text{ si } n \in \mathbb{Z}_p$$

est soit identiquement nulle sur $\mathbb{Z}_p$, soit s'annule en un nombre fini de points.
Or f_r est somme d'une série entière sur $\mathbb{Z}_p$. Si elle n'est pas nulle, le théorème de Strassmann achève la preuve du théorème de Skolem-Mahler-Lech.

3.5 Contre-exemple en caractéristique positive

Si p est un nombre premier, plaçons-nous dans $\mathbb{K} = \mathbb{F}_p(X)$. Si $(x_n)_{n \geq 0}$ est définie par

$$\forall\, n \in \mathbb{N}, x_n = (X+1)^n - X^n - 1$$

alors $(x_n)_{n \geq 0}$ est dans $\mathcal{R}(\mathbb{K})$ et l'ensemble de ses zéros est :

$$\{p^j, j \in \mathbb{N}\}$$

4 Problème de Skolem : questions de décidabilité

4.1 Finitude de l'ensemble des zéros

Le théorème de Skolem-Mahler-Lech a pour conséquence directe le résultat suivant :

Propriété. *Il existe un algorithme décidant la finitude de l'ensemble des zéros d'un élément de* $\mathcal{R}(\mathbb{Q})$.

En effet, ρ divise $|\mathrm{GL}_m(\mathbb{F}_p)|$ et le théorème de Cayley-Hamilton permet de se ramener au calcul des m premières valeurs de chaque progression arithmétique.

4.2 Vacuité de l'ensemble des zéros

La preuve du théorème de Skolem-Mahler-Lech ne fournit pas de borne supérieure à l'ensemble des zéros dans le cas où il est fini. En fait, le problème de Skolem, sur l'existence d'un algorithme décidant la vacuité de l'ensemble des zéros d'une suite linéaire récurrence à coefficients rationnels, est un problème ouvert.
Il existe des résultats allant dans le sens de la difficulté du problème, comme celui qui suit (prouvé par Blondel et Portier dans [3]) :

Théorème 4 (Blondel-Portier)**.** *Le problème de l'existence d'un zéro dans une suite récurrente linéaire à coefficients entiers est NP-difficile.*

On ne sait pas à l'heure actuelle si le problème de Skolem est NP, ni même s'il est décidable. Pour plus d'informations, on peut consulter :

Vesa Halava, Tero Harju, Mika Hirvensalo, Juhani Karhumäki : *Skolem's Problem – On the Border Between Decidability and Undecidability*. Numéro 683 dans *TUCS Technical Report*, avril 2005.

A Preuves

A.1 Quelques résultats d'analyse p-adique

Preuve 1 (Séries doubles)**.** Tout d'abord on montre la définition des deux sommes. Comme, à $i \in \mathbb{N}$ fixé, $|u_{i,j}|_p \xrightarrow[j\to+\infty]{} 0$, la série $\sum_{j=0} u_{i,j}$ converge et :

$$\left|\sum_{j=0}^{+\infty} u_{i,j}\right|_p \leq \max\{|u_{i,j}|_p, j \in \mathbb{N}\}$$

Soit $\varepsilon > 0$. Alors si $i \geq N(\varepsilon)$, $\left|\sum_{j=0}^{+\infty} u_{i,j}\right|_p \leq \varepsilon$, ce qui montre la convergence de la série $\sum_{i\geq 0}\left(\sum_{j=0}^{+\infty} u_{i,j}\right)$. Le cas de la deuxième série se traite symétriquement.

Montrons maintenant que les deux sommes sont égales. Si $\varepsilon > 0$, on montre facilement :

$$\left|\sum_{i=0}^{N(\varepsilon)}\left(\sum_{j=0}^{N(\varepsilon)} u_{i,j}\right) - \sum_{i=0}^{+\infty}\left(\sum_{j=0}^{+\infty} u_{i,j}\right)\right|_p \leq \varepsilon \text{ et } \left|\sum_{i=0}^{N(\varepsilon)}\left(\sum_{j=0}^{N(\varepsilon)} u_{i,j}\right) - \sum_{j=0}^{+\infty}\left(\sum_{i=0}^{+\infty} u_{i,j}\right)\right|_p \leq \varepsilon$$

Par inégalité triangulaire puis en faisant tendre ε vers 0, on a l'égalité voulue.

Preuve 2 (Strassmann)**.** On procède par récurrence sur $N \in \mathbb{N}$. Notons, si N est dans $\mathbb{N}$:

$$\mathcal{P}_N : \text{« le théorème est vrai pour toute suite } (a_n)_{n\geq 0} \text{ telle que } N(a) = N \text{ »}$$

Initialisation : Par l'absurde, supposons $(a_n)_{n\geq 0} \in {\mathbb{Q}_p}^{\mathbb{N}}$ telle que $N(a) = 0$ et $x \in \mathbb{Z}_p$ tel que $f(x) = 0$. Alors on a :

$$|a_0|_p = \left|\sum_{n=1}^{+\infty} a_n\right|_p \leq \max\{|a_n|_p, n \in \mathbb{N}^*\} < |a_0|_p$$

On obtient donc une contradiction. D'où l'on a $\mathcal{P}_0$.

Hérédité : Soit un N dans $\mathbb{N}^*$ tel que $\mathcal{P}_{N-1}$ soit vérifiée, soit $(a_n)_{n\geq 0} \in {\mathbb{Q}_p}^{\mathbb{N}}$ telle que $N(a) = N$. Si f ne s'annule pas sur $\mathbb{Z}_p$, le théorème est vrai pour f. Sinon, soit $\alpha \in \mathbb{Z}_p$ tel que $f(\alpha) = 0$. Alors si $x \in \mathbb{Z}_p$:

$$f(x) = f(x) - f(\alpha) = \sum_{n=1}^{+\infty} a_n(x^n - \alpha^n) = (x-\alpha)\sum_{n=1}^{+\infty}\sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}$$

L'hypothèse du théorème des séries doubles est vérifiée, d'où :

$$f(x) = (x - \alpha)\, g(x) \qquad (*)$$

où : $g(x) = \sum_{n=0}^{+\infty} b_n x^n$ avec $b_n = \sum_{j=n+1}^{+\infty} a_j\, \alpha^{j-1-n}$ si $n \in \mathbb{N}$.
On vérifie alors que $N(b) = N - 1$, et par $\mathcal{P}_{N-1}$, g s'annule au plus $N - 1$ fois sur $\mathbb{Z}_p$. Alors $(*)$ achève la preuve de $\mathcal{P}_N$.

A.2 Théorème de plongement de Cassels

Preuve 3 (Cassels)**.** Nous démontrerons trois lemmes utiles dans un premier temps.

Lemme 1. *Si $n \in \mathbb{N}^*$ et $(P_j)_{1 \leq j \leq N}$ est une famille d'éléments non nuls de $\mathbb{Z}[X_1, \ldots, X_n]$, alors il existe $(a_1, \ldots, a_n)$ dans $\mathbb{Z}^n$ tel que :*

$$\forall\, j \in \{1, \ldots, N\}, P_j(a_1, \ldots, a_n) \neq 0$$

Preuve. Par récurrence sur $n \in \mathbb{N}^*$:

Initialisation : On prend a_1 dans $\mathbb{Z}$ non racine des $P_j, 1 \leq j \leq N$.

Hérédité : Si $n \in \mathbb{N}^*$ vérifie la propriété, soit $(a_1, \ldots, a_n)$ dans $\mathbb{Z}^n$ tel que les

$$P_j(a_1, \ldots, a_n, X_{n+1}), 1 \leq j \leq N$$

soient tous non nuls (par hypothèse de récurrence aux coefficients non nuls de X_{n+1}). On est ramené au cas $n = 1$.

Lemme 2. *Si $P \in \mathbb{Z}[X]$ est non constant, alors l'équation $P(x) \equiv 0\ [p]$ a une solution dans $\mathbb{Z}$ pour une infinité de nombres premiers p.*

Preuve. Notons $P = \sum_{k=0}^{n} a_k X^k$. Si $a_0 = 0$, on prend $x = 0$ pour tout nombre premier. Si $a_0 \neq 0$, supposons par l'absurde qu'il n'y ait qu'un ensemble fini $\mathcal{P}$ de tels nombres premiers. Soit $c \in \mathbb{Z}$ divisible par tous les $p \in \mathcal{P}$ tel que $P(a_0 c) \notin \{-a_0, +a_0\}$ (P est non constant). Alors $P(a_0 c) = a_0 r$ avec :

$$r = 1 + \sum_{k=1}^{n} a_k {a_0}^{k-1} c^k \equiv 1\ [p] \text{ si } p \in \mathcal{P}$$

Si q est un nombre premier divisant r, alors $q \notin \mathcal{P}$ mais $P(a_0 c) \equiv 0\ [q]$: contradiction.

Lemme 3. *Si p est un nombre premier, l'extension $\mathbb{Q}_p/\mathbb{Q}$ a un degré de transcendance infini.*

Preuve. $\mathbb{Q}_p$ est indénombrable, alors que la clôture algébrique de $\mathbb{Q}(a_1, \ldots, a_n)$ est dénombrable si $(a_1, \ldots, a_n) \in {\mathbb{Q}_p}^n$.

Pour montrer le théorème, on peut supposer, quitte à l'agrandir, que l'ensemble fini A est stable par passage à l'inverse. Il suffit alors de construire Φ tel que $\Phi(A) \subset \mathbb{Z}_p$.

Soit $(x_1, \ldots, x_m) \in \mathbb{K}^m$ une base de transcendance de $\mathbb{K}/\mathbb{Q}$. Alors $\mathbb{K}/\mathbb{Q}(x_1, \ldots, x_m)$ est une extension finie en caractéristique 0 donc on peut appliquer le théorème de l'élément primitif : il existe $y \in \mathbb{K}$ algébrique sur $\mathbb{Q}(x_1, \ldots, x_m)$ tel que $\mathbb{K} = \mathbb{Q}(y, x_1, \ldots, x_m)$. Un morphisme de corps $\Phi : \mathbb{K} \to \mathbb{Q}_p$ est alors déterminé par $(\Phi(y), \Phi(x_1), \ldots, \Phi(x_m))$. Écrivons alors, si $x \in A$:

$$x = \frac{P_x(y, x_1, \ldots, x_m)}{Q_x(x_1, \ldots, x_m)}$$

avec $P_x \in \mathbb{Z}[Y, X_1, \ldots, X_m]$ et $Q_x \in \mathbb{Z}[X_1, \ldots, X_m] \setminus \{0\}$.

Quitte à multiplier $\Pi_y \in \mathbb{Q}(x_1, \ldots, x_m)[Y]$ le polynôme minimal de y par une constante, on dispose de $H \in \mathbb{Z}[Y, X_1, \ldots, X_m]$ tel que $H(Y, x_1, \ldots, x_m)$ soit un annulateur irréductible de y. Notons $H_0 \in \mathbb{Z}[X_1, \ldots, X_m] \setminus \{0\}$ le coefficient dominant de H en Y. Le discriminant de Π_y est de la forme $\Delta(x_1, \ldots, x_m)$ où $\Delta \in \mathbb{Z}[X_1, \ldots, X_m] \setminus \{0\}$.

Par le lemme 1, on dispose de $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ tel que :

$$\Delta(a_1, \ldots, a_m) \neq 0, H_0(a_1, \ldots, a_m) \neq 0, Q_x(a_1, \ldots, a_m) \neq 0 \text{ si } x \in A$$

Par le lemme 2, l'ensemble $\mathcal{P}$ des nombres premiers p tels qu'il existe $b \in \mathbb{Z}$ vérifiant : $H(b, a_1, \ldots, a_m) \equiv 0\,[p]$ est infini. Quitte à exclure un nombre fini d'entre eux, on peut supposer en outre que si $p \in \mathcal{P}$: $\Delta(a_1, \ldots, a_m) \not\equiv 0\,[p]$ et $Q_x(a_1, \ldots, a_m) \not\equiv 0\,[p]$ si $x \in A$.

Soit $p \in \mathcal{P}$. Par le lemme 3, on dispose d'un m-uplet $(\theta_1, \ldots, \theta_m) \in {\mathbb{Q}_p}^m$ d'éléments algébriquement indépendants sur $\mathbb{Q}$. Quitte à les multiplier par des puissances de p, on peut supposer que si si $1 \leq j \leq m, |\theta_j|_p < 1$. Alors si $1 \leq j \leq m$, posons :

$$\xi_j = a_j + \theta_j$$

Alors $(\xi_1, \ldots, \xi_m)$ est un m-uplet d'éléments algébriquement indépendants sur $\mathbb{Q}$ et :

$$|\xi_j - a_j|_p < 1 \text{ si } 1 \leq j \leq m$$

de sorte que l'on ait : $|H(b, \xi_1, \ldots, \xi_m)|_p < 1$.

Alors par le lemme d'Hensel, on dispose de $\eta \in \mathbb{Z}_p$ tel que $H(\eta, \xi_1, \ldots, \xi_m) = 0$. D'où $P_x(\eta, \xi_1, \ldots, \xi_m) \in \mathbb{Z}_p$ et $Q_x(\xi_1, \ldots, \xi_m) \in \mathbb{Z}_p$ si $x \in A$.
On a même : $|Q_x(\xi_1, \ldots, \xi_m)|_p < 1$ si $x \in A$.

Il reste alors à définir Φ par :

$$\Phi(x_j) = \xi_j \text{ si } x \in A \text{ et } \Phi(y) = \eta$$

A.3 Théorème de Blondel-Portier

Preuve 4 (Blondel-Portier)**.** On suggère seulement les étapes de la preuve :

- Le problème de déterminer si un langage défini par une expression rationnelle sur l'alphabet $\{a\}$ est différent de a^* est NP-difficile (par réduction depuis 3-SAT).
- Le problème de déterminer si un automate fini déterministe sur l'alphabet $\{a\}$ reconnaît un langage différent de a^* est NP-difficile (par le théorème de Kleene).
- Le problème de déterminer si, pour un graphe orienté G et un couple de sommets (V_1, V_2) de G donnés, il existe un chemin de longueur k reliant V_1 à V_2 pour tout $k \geq 1$ est co-NP-difficile.
- Le problème de déterminer si, pour une matrice $A \in \{0,1\}^{n^2}$ et deux vecteurs $X, Y \in \{0,1\}^n$ donnés, il existe $k \geq 1$ tel que ${}^tXA^kY = 0$ est NP-difficile.
- Conclusion (en utilisant le point de vue matriciel).

B Bibliographie

[1] Cassels, J.W.S.: *Local Fields*. Numéro 3 dans *London Mathematical Society student texts*. 1986. Chapitre 5.

[2] Hansel, G.: *A Simple Proof of the Skolem-Mahler-Lech Theorem*. Dans *12th International Colloquium on Automata, Languages and Programming*, numéro 194 dans *Lecture Notes in Computer Science*, pages 244–249, 1985.

[3] Vincent D. Blondel, Natacha Portier: *The presence of a zero in an integer linear recurrent sequence is NP-hard to decide*. Dans *Linear Algebra and its Applications*, numéro 351-352, pages 91–98. Elsevier.