N° d'ordre : 31/2008-M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE

FACULTÉ DES MATHÉMATIQUES

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En MATHEMATIQHES

Spécialité : Algèbre et Théorie des Nombres

Par

SENOUCI aichouche

Sujet

UNE GÉNÉRALISTION DU THEOREME DE SKOLEM-MAHLER-LECH

Soutenu publiquement, le 17/06/2008 devant le jury composé de :

Mr.	**B.BITINA**	Professeur	U.S.T.H.B.	Président.
Mr.	**B.BENZAGHOUI**	Professeur	U.S.T.H.B.	Directeur de thése .
Mr.	**M.ZITOUNI**	Professeur	U.S.T.H.B.	Examinateur.
Mr.	**M.S.HACHAICHI**	Maître de Conférences	U.S.T.H.B.	Examinateur.
Mr.	**A.TADJINEI**	Chargé de cours	U.S.T.H.B.	invité.
Mr.	**A.BELLAGH**	Chargé de cours	U.S.T.H.B.	invité.

Remerciements

Je remercie tout d'abord ALLAH le tout puissant qui nous a donné le courage et l'espoir pour préparer ce modeste travail.

Je tiens à exprimer mes plus vifs remerciements à Monsieur ***B. Benzaghou*** *, mon Directeur de thèse pour l'intéressant sujet qu'il m'a proposé. Je lui suis également reconnaissante pour la confiance qu'il ma accordée. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes. J'exprime ma gratitude la plus sincere a* ***K. Bitina*** *qui m'honore en acceptant de présider le jury de ce mémoire.*

Je remercie aussi messieurs le professeur ***M.Zitouni*** *,* ***M.S Hachaichi*** *, Mohamed Mahfoud et M. Mohamed Saighi d'avoir fait partie de mon jury et l'intérêt qu'ils ont bien voulu porté à mon trava. messieurs A BELAGHE et A TADJINE d'avoir accepté de prendre part à ce jury.*

Je ne peux terminer sans évoquer aussi ce que je dois à tous ceux qui de prés ou de loin mont soutenu pour préparer ce mémoire et sans exprimer ma reconnaissance.

d'accepter la tâche d'être rapporteurs. Je les remercie également pour leur soutien et l'amitié qu'ils m'ont prodigués depuis longtemps..

Dédicaces

Je tiens à dédier ce travail à :

Mes Merveilleux parent qui m'ont donné Aucun mot, aucune phrase ne pouvaient décrire et exprimer tout l'amour que j'ai pour eux

A mes sœurs : Noura ,Dallel, Hanna etKhadidja

et mes frères :Mustapha et Billel

A la ptite « katkouta » « Ines »

A mes très chère :

Grand pères :Madani et Taibe

Grand mères :Khira et Aicha

A mes Tantes et mes oncles, pour leurs encouragements constants à continuer ;

A tous les autres membres de la famille "Senouci" et" Lassmi ", qui ont approuvé ma démarche ;

Enfin, à tous les martyrs de la Révolution Algérienne qui, par leur Sacrifice, ont permit que l'Algérie par conséquent l'université Algérienne recouvre sa liberté.

Table des matières

Introduction

Leur age, leur richesse ainsi que la diversité de leurs champs d'application font des suites récurrentes linéaires un sujet tellement vaste et si riche en résultats qu'il faudrait plusieurs ouvrages, en plus de ceux qui existent déjà , pour faire le tour de toutes leurs propriétés. On trouve dans [12] une très bonne introduction aux suites récurrentes linéaires ainsi qu'une bibliographie qui, jointe à celle qu'on trouve dans[15]

Nous donnons une généralisation du théorème de Skolem - Mahler - Lech qui est une caractérisation de l'ensemble des indices qui annule une suite récurrente linéaire.

Chapitre 1

Suites récurrentes linéaires et théorème de Skolem-Mahler -Lech

La premiere partie de ce travail est consacrée à l'étude de certaines propriétés algébriques des suites récurrentes linéaires à coeffcients constants .

1.1 Propriétés générales des suites récurrentes linéaires

Les suites récurrentes linéaires ont été étudiées depuis longtemps, d'abord pour le corps $\mathbb{Q}$, puis pour un corps de caractéristique quelconque ou sur un anneau commutatif .

1.1.1 Définitions et notations

Définition 1.1.1 *Soit K un corps commutatif et $u = (u(n))$ une suite d'éléments de K. u est une suite récurrente linéaire s'il existe un entier naturel s non nul et des éléments a_j $(j = 1, 2, ..., s)$ de K tel que l'on ait pour tout $n\ \epsilon\mathbb{N}$ la relation :*

$$u(n+s) = a_1u(n+s-1) + ... + a_su(n) \tag{1.1.1}$$

si (1.1.1) est la plus courte relation de récurrence vérifieé par u, s est dit ordre (ou longueur) de la suite U et on définit son polynôme caractéristique par

$$Q(X) = 1 - a_1X - a_2X^2 - ... - a_sX^s \tag{1.1.2}$$

Définition 1.1.2 *: Une série formelle* $f(X) = \sum_{n\geq 0} u(n)X^n \in K[[X]]$ *est une série rationnelle s'il existe deux polynômes* $P, Q \in K[X]$ *tels que*

$$f(X) = P(X)/Q(X) \qquad avec \;\; Q(0) \neq 0 \tag{1.1.3}$$

Notation 1.1.1 *On notera l'ensemble des suites récurrentes linéaires (en abrégé s.r.l) à valeurs dans* K *par* $r(K)$ *et l'ensemble des séries rationelles par* $R(K)$*.*

Définition 1.1.3 *Un polynôme expononentiel est une expression de type*

$$u(n) = \sum_{i=1}^{n} P_i(n)\alpha_i^n \qquad n \in \mathbb{N}^* \tag{1.1.4}$$

avec les α_i *étant des éléments non nuls de* $\bar{K}$ *et.* P_i *des polynômes de* $\bar{K}[x]$ $\quad i = \overline{1, n}$*.*

Théorème 1.1.1 *Soit* K *un corps commutatif de caractéristique nulle et* $u := (u(n))$ *une suite d'éléments de* K *alors les assertions suivantes sont équivalentes:*
i) u *est une suite récurrente linéaire.*
ii) $f(X) = \sum_{n\geq 0} u(n)X^n$ *est une série rationnelle.*
iii) pour tout $n \in \mathbb{N}$ *,* $u(n)$ *est un polynôme exponentiel.*

Preuve. La preuve se fera selon le chéma suivant $i) \Rightarrow ii) \Rightarrow iii) \Rightarrow i)$
$i) \Rightarrow ii)$
Soit u une suite récurrente linéaire d'éléments de K

$$u(n+h) = a_1 u(n+h-1) + ... + a_h u(n) \qquad n \in \mathbb{N}$$

son polynôme caractéristique est

$$Q(X) = 1 - a_1 X - a_2 X^2 - ... - a_h X^h$$

On considére la série $f(X) = \sum_{n\geq 0} u(n)X^n$ et vu que tous les termes de la suite u s'expriment en fonction des h premiers termes $u(0)$, ..., $u(h-1)$ on vérifie que

$$\begin{aligned} P(X) &= f(X)Q(X) \\ &= (\sum_{n\geq 0} u(n)X^n)(1 - a_1 X - a_2 X^2 - ... - a_h X^h) \end{aligned}$$

est un polynôme .

D'où $f(X) = P(X)/Q(X)$ *avec* $Q(0) = 1 \neq 0$ est une série rationnelle.

ii) $\Rightarrow$ *iii)*

Soit $f(X) \in R(K)$ c'est -à-dire qu'il existe deux polynômes A et B à coéfficients dans K tels que

$$f(X) \ = \ A(X)/B(X) \quad avec \ B(0) \neq 0 \tag{1.1.5}$$

Soient alors $\omega_1^{'}, ..., \omega_k^{'}$ les racines du polynôme B dans une extension algebrique L de K et soit τ_i la multiplicité de $\omega_i^{'}$ $(i = 1, ..., k)$

la décomposition en éléments simples de la fraction A/B est de la forme

$$\begin{aligned} f(X) \quad &= \quad A(X)/B(X) \qquad (1.1.6) \\ &= \quad E(X) + \sum_{i=1}^{k} \sum_{j=1}^{\tau_i} \frac{\alpha_{ij}}{(X - \grave{\omega}_i)^j} \end{aligned}$$

Où $E(X)$ est un polynôme à coefficients dans K (c'est le quotient de la division euclidienne de A par B) et où les α_{ij} appartient ou corps L.on a

$$(X - \omega_t)^{-j} = (-1)^j \omega_i^{-j} \sum_{n \geq 0} \binom{n+j-1}{j-1} \left(X\omega_i^{-1}\right)^n \tag{1.1.7}$$

jointe à (1.1.6) et (1.1.7) conduisent la relation

$$f(X) = E(X) + \sum_{n \geq 0} \sum_{i=1}^{k} \sum_{j=1}^{\tau_i} (-1)^j \omega_i^{n+j} \binom{n+j-1}{j-1} \alpha_{ij} X^n$$

Où on a posé

$$\omega_i = 1/\acute{\omega}_i \quad (i = 1, ..., k)$$

Si $E(X)$ a pour degré n_0 on a donc

$$u(n) = P_1(n)\omega_i^n + ... + P(n)\omega_k^n \quad pour \ n \geq n_0 \tag{1.1.8}$$

avec

$$P_i(n) = \sum_{j=1}^{\tau_i} (-1)^j \alpha_{ij} \omega_i^j \binom{n+j-1}{j-1} \tag{1.1.9}$$

iii) $\Rightarrow$ *i)*

Supposons maintenant que la relation (1.1.8) et 1.1.9 aient lieu pour $n \geq n_0$

Soit T l'opérateur de décalage qui à une suite $u = (u(n))_n$ associe la suite $Tu(n) = u(n+1)$ $n \geq 0$

On vérifie que la suite

$$(T - \omega_1 I)^{\tau_1} ... (T - \omega_k)^{\tau_k}(u(n))$$

est ultiment nulle et plus précisément que $(u(n))_{n\geq 0}$ satisfait a l'équation aux défférences finies à coéfficients constants

$$T^{n_0} G(T) u(n) = 0 \tag{1.1.10}$$

Ou

$$G(X) = \frac{X^m}{B(0)} B(X^{-1}) = \prod_{i=1}^{k} (X - \omega_i)^{\tau_i}$$

Si on pose dans (1.1.10)

$$G(X) = X^m - a_{m-1}X^{m-1} - ... - a_0 \ \ , m = \sum_{i=1}^{k} \tau_i$$

on a donc démontré que la suite $u(n)$ vérifie la condition

$$u(n+m) = a_{m-1}u(n+m-1) + ... + a_0 u(n) \ \ pour \ n \geq n_0$$

. ■

Remarque 1.1.1 *:*

-La relation de récurrence (1.1.1) est la plus courte si la représentation $P(X)/Q(X)$ est irreductible

-Lorsque la caractéristique du corps K est nulle chaque P_i est un polynôme (à coéfficients dans le corps L qui est le corps engendre par $\mathbb{Q}$ et les α_i les racines distinctes du polynôme caracteristique de la suite $(u(n))$ en n de degré petit que τ_i et même égal à $\tau_i - 1$ lorsque la représentation (1.1.3) est irreductible.

Exemple 1.1.1 *l'exemple le plus populaire de **s.r.l** et aussi le plus ancien il date de 1202 est la suite de **Fibonacci** (F_n) définie comme suit:*

$$\begin{aligned} F_0 &= 0 \qquad F_1 = 1 \\ F_{n+2} &= F_{n+1} + F_n \ \ pour \ n \geq 0 \end{aligned}$$

avec $F_n = \dfrac{\omega_1^n - \omega_2^n}{\omega_1 - \omega_2}$

1.1.2 Caractérisation des suites récurrentes linéaires (déterminant de Kronecker-Henkel)

Définition 1.1.4 *Soit u une suite d'élément de K on appelle déterminants de* ***Henkel*** *associés à u les déterminants :*

$$D_n^{(h)} := D_n^{(h)}(u) := |u(n+i+j)|_{0\leq i,j\leq h}$$

on appelle déterminants de ***Kronecker*** *associes à u les déterminants;*

$$\Delta_h := \Delta_h(u) := D_0^{(h)}(u) = |u(i+j)|_{0\leq i,j\leq h}$$

ce sont les déterminants de Henkel pour $n = 0$.

Théorème 1.1.2 *[2]Soit u une suite d'éléments de K*
u est une suite récurrente lineaire si et seulements si l'une des deux conditions suivantes est vérifiée:
i) *il existe deux entiers naturels h et n_0 tels que $D_n^{(h)}(u) = 0 \qquad \forall n \geq n_0$*
ii) *il existe un entier t_0 tel que $\Delta_t(u) = 0 \quad \forall t \geq t_0$*

propriétés:

a) Soit $u : \mathbb{N} \longrightarrow K$ une une suite récurrente linéaire d'ordre inférieur ou égal à h $(h \in \mathbb{N}^*)$ si les h termes consécutifs de la suite u sont nuls alors la suite u est identiquement nulle.
b) L'unicité de la décomposition d'une fraction rationnelle en éléments simples montre que le polynôme exponentiel est unique .

1.2 Démonstration du théorème de skolem-Mahler-lech

Dans ce paragraphe nous nous proposons d'étudier l'ensemble $I(u(n)) = \{n, u(n) = 0\}$ pour $(u(n))$ s.r.l .

Rappelons quelques résultats d'analyse p-adique

Théorème 1.2.1 *[1] Soit x un élément de $\in \mathbb{C}_p$ la série $\displaystyle\sum_{n=0}^{\infty} \frac{x^n}{n!}$ converge pour $v_p(x) > \dfrac{1}{p-1}$ et diverge pour $v_p(x) \leq \dfrac{1}{p-1}$*

La série $\sum_{n\geq 0}(-1)^{n-1}\frac{x^n}{n}$ *converge pour* $v_p(x)>0$ *et diverge pour* $v_p(x)\leq 0.$

Dans les domaines de convergence , on note $\exp(x)=\sum_{n=0}^{\infty}\frac{x^n}{n!}$ *et* $\log(1+x)=\sum_{n\geq 0}(-1)^{n-1}\frac{x^n}{n}.$

Définition 1.2.1 *Une fonction exposant* a^x $(a,x\in\mathbb{Q}_p)$ *est définie comme suit* $a^x=\exp(x\log a)$ *elle est définie lorsque* $|a-1|_p<1$ *et* $|x\log a|_p<p^{-1/p-1}$

Définition 1.2.2 *Soit* x *un élément de* $\mathbb{Q}_p$ *et* n *un entier naturel* $\binom{x}{n}$ *est définit par*

$$\binom{x}{n}=\frac{x(x-1)(x-2)...(x-n+1)}{n!}\ \textit{avec}\ \binom{x}{0}=1$$

est un polynôme en x *de degré* n *.*

Lemme 1.2.1 *[3]Soit* a *un élément algébrique sur* $\mathbb{Q}$ *avec* $|a|_p=1$ *et* $s\in\mathbb{N}$ *donné alors il éxiste* $m\in\mathbb{N}$ *tel que* $v_p(a^m-1)\succ s$
on peut choisir s *tel que* $x\rightsquigarrow(a^m)^x$*soit défini pour* $v_p(x)\geq\lambda$ *avec* $\lambda\prec 0$
le disque de convergence contient alors $A=\{\ x\ ,\ v_p(x)\geq 0\ \}$ *.*

Lemme 1.2.2 *Si* $x\in\mathbb{Z}_p$ *et* $n\in\mathbb{N}$ *alors* $\left|\binom{x}{n}\right|\leq 1.$

Preuve. pour $x\in\mathbb{N}$ et $n\geq 0$ donc $\binom{x}{n}\in\mathbb{N}$ d'où $\left|\binom{x}{n}\right|\leq 1$ or $\mathbb{N}$ est dense dans $\mathbb{Z}_p$ alors $\left|\binom{x}{n}\right|\leq 1$ pour $x\in\mathbb{Z}_p$. ■

Lemme 1.2.3 *Soit* $f(x)$ *une fonction p-adique analytique définie pour tout* $x\in\mathbb{Z}_p$*. si* $f(x)$ *a une infinité de zéros dans* $\mathbb{Z}$ *alors* $f(x)\equiv 0.$

Preuve. *Comme* $\mathbb{Z}$ *est dense dans* $\mathbb{Z}_p$ *et* $\mathbb{Z}_p$ *est un compact alors* $f(x)\equiv 0$ *car chaque zéro de* f *est un point limite d'une suite de* $\mathbb{Z}$*.* ■

Lemme 1.2.4 *Soit* p *un nombre premier .Alors pour tous entiers* a *et* b

$$(a+b)^p\equiv a^p+b^p(\text{mod}\ \ p).$$

Preuve. *On écrit la formule du binôme pour p premier :*

$$(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b^2 + ... + \frac{p(p-1)}{2}a^2b^{p-2} + pab^{p-1} + b^p$$

tous les termes du devlopment autres les termes extrêmes sont divisibles par p donc

$$(a+b)^p \equiv a^p + b^p (\text{mod } p)$$

■

Théorème 1.2.2 (petit théorème de Fermat)
Soit p un nombre premier alors pour tout entier x non divisible par p on a

$$x^{p-1} \equiv 1 (\text{mod } p)$$

Preuve.
On montre par récurrence que $x^{p-1} \equiv 1(\text{mod } p)$
pour $x = 1$
$2^p = (1+1)^p \equiv 1^p + 1^p (\text{mod } p) \equiv 2(\text{mod } p) \Rightarrow 2^{p-1} \equiv 1(\text{mod} p)$. *vérifie.*
Supposons $x^p \equiv x(\text{mod } p)$ *et montrons que* $(x+1)^p \equiv (x+1)\,(\text{mod } p)$.
$(x+1)^p \equiv (x^p + 1^p)\,(\text{mod } p) \equiv (x+1)(\text{mod } p)$ *(d'apres l'hypothése de récurrence)*
D'ou $(x+1)^{p-1} \equiv 1(\text{mod } p)$. ■

Théorème 1.2.3 généralisation de petit théorème de Fermat
Soient a et n deux entiers naturels tels que a est premier avec n alors on a

$$a^{\varphi(n)} \equiv 1\,(\text{mod } n)$$

avec φ la fonction de d'Euler qui vérifie :

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(n) &= (p_1-1)\,p_1^{k_1-1}...(p_r-1)\,p_r^{k_r-1} \qquad \textit{pour } n = p_1^{k_1}...p_r^{k_r} \textit{ avec } p_1,...,p_r \textit{ des nombre premiers} \\ \varphi(nm) &= \varphi(n)\,\varphi(m) \qquad \textit{pour } (n,m) = 1 \end{aligned}$$

Preuve.
Le groupe des élements inversibles $(\mathbb{Z}/n\mathbb{Z}, \times)^*$ est dordre $\varphi(n)$

Soit a et n deux entiers tels que $(a,n) = 1$, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z}, \times)^*$,soit m l'ordre de $\bar{a}$ donc m divise $\varphi(n)$ d'aprés le thèorème de lagrange d'où il existe $k \in \mathbb{N}$ tel que

$$\varphi(n) = k \times m$$

Comme $\bar{a}^m = 1$

$$\bar{a}^{\varphi(n)} = \bar{a}^{k\times m} = \bar{1}^k = \bar{1}$$

ce qui s'écrit également

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

■

Lemme 1.2.5 *Soient $\alpha_1, ..., \alpha_m$ des unités p-adiques de $\mathbb{Z}_p$ $\left(i.e \ \ |\alpha_j|_p = 1 \text{ avec } \quad j = 1, ..., m\right)$ et $\varepsilon > 0$. alors il existeun entier naturel D tels que $\left|\alpha_j^D - 1\right|_p < \varepsilon$.*

Preuve. *Soit $\varepsilon > 0$.soit $M := M(\varepsilon) \in \mathbb{N}$ tels que $p^{-M} < \varepsilon$.*
fixons un entier j , on a α_j est une unité p-adique α_j on peut l'écrire comme

$$\begin{aligned} \alpha_j &= a_0 + a_1 p + ... + a_{M-1} p^{M-1} + a_M p^M + ... \\ &= A + B \end{aligned}$$

avec $a_k = a_k(\alpha_j\ ) \in \{0, 1, ..., p-1\}$, $a_0 \neq 0$

$$\begin{aligned} A &= a_0 + a_1 p + ... + a_{M-1} p^{M-1} \\ B &= a_M p^M + ... \end{aligned}$$

Si on pose $n = p^M$ et comme $(A, p^M) = 1$ d'aprés la généralisation de petit théorème de Fermat 1.2.3 il éxiste un entier $d_j = \varphi(p^M) = (p-1)p^{M-1}$tels que $A^{d_j} \equiv 1 (\text{mod } p^M)$ donc

$$\begin{aligned} \alpha_j^{d_j} &= (A + B)^{d_j} \qquad (1.2.1) \\ &= A^{d_j} + \sum_{k=1}^{d_j} \binom{d_j}{k} A^{d_j - k} B^k \end{aligned}$$

donc d'aprés lemme1.2.2 et (1.2.1) ona

$$\left|\alpha_j^{d_j} - 1\right|_p \leq p^{-M} \prec \varepsilon$$

Donc pour chaque j *il existe* d_j *alors pour* $D = ppcm(d_1, ..., d_m)$ *on a*

$$\left|\alpha_j^D - 1\right|_p < \varepsilon$$

Ce qui termine la démonstration du lemme . ■

Lemme 1.2.6 *Soient* $g_j(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$ *;avec* $j = 1, ..., J$
Alors il existe $(a_1, ..., a_n) \in \mathbb{Z}^n$ *tel que*

$$g_j(a_1, ..., a_n) \neq 0 \quad j = 1, ..., J$$

Lemme 1.2.7 *Soit* $g(x) \in \mathbb{Z}[x]$ *alors il existe une infinité de nombres premiers p pour les quels la congruence*

$$g(x) \equiv 0 (\text{mod } p) \tag{1.2.2}$$

a une solution dans $\mathbb{Z}$ *; c'est -à-dire*

$$\exists b \in \mathbb{Z} \qquad tq \;\; g(b) \equiv 0 (\text{mod}\, p) \qquad\qquad *$$

Preuve. *Soit* $g(x) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0$
si a_0= $\mathbf{0}$ *on prend* $b = 0$.
si $a_0 \neq 0$ *supposons que (1.2.2) a une solution seulement pour un nombre fini de premiers* $p \in \wp$ *(peut être vide) soit c un entier qui est divisible par tout* $p \in \wp$ *alors*

$$g(a_0 c) = a_0 r \tag{1.2.3}$$

avec

$$r = a_n a_0^{n-1} c^n + a_{n-1} a^{n-2} c^{n-1} + ... + 1$$

r *est premier avec c et* r *est non divisible par tout* $p \in \wp$ *comme* $g(x)$ *est non constante par hypothése on peut choisit* $r \neq \pm 1$
Soit p'*un nombre premier qui divise* r *donc* $p' \notin \wp$ *par (1.2.3) on a* $g(a_0 c) \equiv 0 (\text{mod } p')$ *on pose* $b' = a_0 c$ *donc* $g(b') \equiv 0 (\text{mod } p')$ *contradiction avec* $\wp$ *contient tous les nombres premiers p qui vérifient (1.2.2) .* ■

Lemme 1.2.8 ***(lemme de Hensel)***
Soient K un corps valué complet et F un polynome non nul de $A[X]$, d est le degre de F,Supposons qu'il existe deux polynômes unitaires g et h dans $A[X]$ tels que

$$\bar{F} = \bar{g}\ \bar{h}\ , dg\ \ (g) + deg(\ h) \leq d\ \ et\ \ \left(\bar{g}\ ,\bar{h}\right) = 1$$

Alors il existe G et H dans $A[X]$ tels que

$$\begin{aligned} \bar{G} &= \bar{g}\ ,\bar{H} =\ \bar{h},\ \ deg\ G{=}deg\ g\ et \\ F &= GH. \end{aligned} \tag{1.2.4}$$

Théorème 1.2.4 (de Cassels)
Soit K une extension de type finie de $\mathbb{Q}$ et soit Ω une partie finie d'éléments non nuls de K alors il existe une infinité de nombres p pour les quels il existe un plongement ϕ_p de K dans $\mathbb{Q}_p$ tel que $\left|\phi_p(c)\right|_p = 1 \quad \forall\ c \in \Omega$.

Preuve. *Soit K une extension de type fini de $\mathbb{Q}$.*
Soit $(X_1, ..., X_m)$ une base de transcendance de K ,K alors une extension algebrique de $\mathbb{Q}(X_1, ...; X_m)$ soit encore y un élément primitif de K;$K = \mathbb{Q}(y, X_1, ...; X_m)$ on peut supposer que c et $1/c$ sont dans Ω pour tout $c \in \Omega$.il nous suffit demontrer alors que
$\left|\phi_p(c)\right|_p \leq 1 \quad \forall c \in \Omega$.*soit* $C_c = U_c(y, X_1, ..., X_m)/V_c(X_1, ..., X_m)$
avec

$$\begin{aligned} U_c(y, X_1, ..., X_m) &\in \mathbb{Z}[y, X_1, ..., X_m] \\ V_c(X_1, ..., X_m) &\in \mathbb{Z}[y, X_1, ..., X_m] \neq 0 \end{aligned}$$

Soit $H(y)$ le polynôme minimale de y sur $\mathbb{Q}(X_1, ...; X_m)$

$$H(y) = H(y, X_1, ..., X_m)$$

avec

$$H(y, X_1, ..., X_m) \in \mathbb{Z}[y, X_1, ..., X_m]$$

Si H est de degré s en y on note le coefficient constant par: $H_0(X_1, ..., X_m)$ donc

$$H(y) = H_0(X_1, ..., X_m) + ... + H_s(X_1, ..., X_m)y^s$$

le discriminant de $H(y)$ est

$$\Delta(X_1,...,X_m) \in \mathbb{Z}[X_1,...,Xm] \neq 0$$

par le lemme 1.2.6 $\exists(a_1,...,a_m) \in \mathbb{Z}^m$ *tel que*

$$\begin{aligned} \Delta(a_1,...,a_m) &\neq 0 \\ H_0(a_1,...,a_m) &\neq 0 \\ V_c(a_1,...,a_m) &\neq 0 \ \forall c \in \Omega \end{aligned}$$

Comme $H(y) \in \mathbb{Z}[X_1,...,Xm]$ *et* $H_0(y,a_1,...,a_m) \in \mathbb{Z}[y]$ *d'aprés le lemme 1.2.7 il existe une infinité de nombres premiers* p *tels que*

$$H(y,a_1,...,a_m) \equiv 0 (\operatorname{mod} p)$$

admet une solution dans $\mathbb{Z}$ *il existe une infinité de* p *pour les quels on a*

$$\begin{aligned} \Delta(a_1,...,a_m) &\not\cong 0(\text{mod } p) \\ H_0(a_1,...,a_m) &\not\cong 0(\text{mod } p) \\ V_c(a_1,...,a_m) &\not\cong 0(\text{mod } p) \\ \exists b &\in \mathbb{Z} \ tq \ H(b,a_1,...,a_m) \not\cong 0(\text{mod } p) \end{aligned}$$

Soient maintenant $\theta_1,...,\theta_m$ *,m éléments de* $\mathbb{Q}_p$ $\mathbb{Q}$*-algébriquement indépendants*
On peut supposer que $|\theta_j|_p < 1 \quad \forall j = 1,...,m$ *comme* θ_j *sont algébriquement indépendants alors posons*

$$\begin{aligned} \varepsilon_j &= a_j + \theta_j \\ \theta_j &= \varepsilon_j - a_j \text{ pour } j = 1...,m \\ |\varepsilon_j - a_j| &\prec 1 \end{aligned}$$

le lemme de hensel 1.2.7 appliqué à $H(y,\varepsilon_1,...,\varepsilon_m) \in \mathbb{Z}[y]$ *il existe* $\eta \in \mathbb{Q}_p$ *,* $|\eta - b|_p \prec 1$ *et* $H(\eta,\varepsilon_1,...,\varepsilon_m) = 0.$
l'application $\phi_p : K = \mathbb{Q}(y,X_1,...,X_m) \longrightarrow \mathbb{Q}(\eta,\varepsilon_1,...,\varepsilon_m) \subseteq \mathbb{Q}_p$
telle que $\phi_p(y) = \eta$ *et* $\phi_p(X_j) = \varepsilon_j$ *avec* $j = 1,...m$
est alors un plongement de K *dans* $\mathbb{Q}_p$ *et l'on a*

$$U_c(y,X_1,...,X_m) \in \mathbb{Z}[y,X_1,...,Xm]$$

$\left|\varepsilon_j\right|_p = \left|a_j + \theta_j\right|_p \leq \max(\left|a_j\right|_p, \left|\theta_j\right|_p) \leq 1$
car $a_j \in \mathbb{Z}, \left|\theta_j\right|_p \leq 1 \quad \forall j = 1, ..., m$ *et donc*

$$\begin{aligned} \left|U_c(\eta, \varepsilon_1, ..., \varepsilon_m)\right|_p &\leq 1 \\ V_c(\varepsilon_1, ..., \varepsilon_m) &= 1 \end{aligned}$$

Ainsi

$$\left|\phi_p(y)\right|_p = \left|\frac{U_c(\eta, \varepsilon_1, ..., \varepsilon_m)}{V_c(\varepsilon_1, ..., \varepsilon_m)}\right| \leq 1$$

D'où le théorème. ■

Théorème 1.2.5 ***(de Mahler)***
Soit K *un corps commutatif ,de caractéristique zéro.Soit* $S(x) = \sum_{n=0}^{\infty} a(n) X^n \in R(K)$ *et posons* $I(a(n)) = \{n, a(n) = 0\}$ *.Si* $I(a(n))$ *est infini ,alors il existe un entier* $m \geq 1$*,des entiers distincts* $\mu_1, ...\mu_s \in \{0, 1, ...m\}$ *tels que* $I(a(n))$ *soit la réunion d'une partie finie* I_0 *et des ensembles* I_{m,μ_i}

$$I_{m,\mu_i} = \{ \quad n, n \equiv \mu_i (\text{mod} \;\; m \;\;)\}$$

Preuve.
Cas K est un corps algebrique:
Comme $\sum_{n=0}^{\infty} a(n) X^n \in R(K)$ *alors* $a(n) = \sum_{i=1}^{k} P_i \alpha_i^n$ *avec* $\alpha_i \in \overline{K}^*$ *et* $P_i(X) \in \overline{K}[X]$ *. on se place dans* L *le corps engendrè par* $\mathbb{Q}_P$ *, les* α_i *et les coefficients du* P_i*,* $L = \mathbb{Q}_p(\alpha_1, ..., \alpha_k, coef P_i)$
L est une extension de $\mathbb{Q}_p$ *de degré fini , il existe un nombre premier* p *pour le quel* $\left|\alpha_i\right|_p = 1 \forall i$
d'apré le lemme 1.2.5 il existe un entier D *tel que*

$$\left|\alpha_i^D - 1\right|_p < p^{-1/p-1} \quad \forall j = 1, ..., k$$

nous savons que l'application $x \longrightarrow (\alpha_i^D)^x$ *est analytique et définie sur* $\mathbb{Z}_p$ *, considerons pour tout* $t \in \{0, 1, ..., D-1\}$

$$a_t(x) = \sum_{i=1}^{k} P_i(t + Dx) \alpha_i^t \left(\alpha_i^D\right)^x$$

La fonction $a_t(x)$ *est alors analytique sur* $\mathbb{Z}_p$*.*
supposons que $a_n(x)$ *a une infinite de zéros dans* $\mathbb{Z}$*,d'aprés le lemme 1.2.3 la fonction* $a_t(x)$

est identiquement nulle et on a $a_t(n) = 0 \ \forall n \in \mathbb{N}$*.donc* $n \in \{n, n \equiv t \,(\mathrm{mod}\, D)\}$.

Cas d'un corps de caracteristique zero :

Comme K *est de caracteruistique zéro on peut supposer qu'il contient* $\mathbb{Q}$

$a(n) = \sum_{i=1}^{k} P_i \alpha_i^n$ *ou* $P_i(x) \in L[x]$ *et* $\alpha_i \in L$ *avec* L *le corps engendré par* $\mathbb{Q}$ *et les* α_i *les racines distinctes du polynôme caracteristique de la suite* $a(n)$

$$G(x) = x^h - c_{h-1}x^{h-1} - \ldots - c_1 x - c_0$$

Si on pose $\Gamma = \{c_0, \ldots, c_{h-1}, \alpha_1, \ldots, \alpha_k\}$, L *une extension de type fini de* $\mathbb{Q}$ *D'aprés le théorème de **Cassels** 1.2.4 il existe une infinité de nombres premiers* p *et un homomorphisme* $\varphi_p :$ $L \longrightarrow \mathbb{Q}_p$ *tel que* $\left|\varphi_p(c)\right| = 1 \ \forall c \in \Gamma$ *donc si* $a(n) = 0$ *dans* L *alors* $\varphi_p(a(n)) = 0$ *dans* $\mathbb{Q}_p$*,c'est-à-dire* n *est solution dans* $\mathbb{Q}_p$ *de* $\sum_{i=1}^{k} A_i \beta_i^n = 0$

$$\varphi_p\left(\sum_{i=1}^{k} P_i \alpha_i^n\right) = \sum_{i=1}^{k} A_i \beta_i^n$$

avec $\beta_i = \varphi_p(\alpha_i) \in \mathbb{Q}_p$, $|\beta_i|_p = 1$ *et* $A_i[x] \in \mathbb{Q}_p[x]$

Par consequent ceci nous ramène aux calculs faits dans la 1^{ere} *partie.* ■

Ce théorème a été prouvé la première fois par Skolem [28] pour des suites récurrentes linéaires sur le corps $\mathbb{Q}$ plus tards par Mahler [17] pour des suites récurrentes linéaires sur un corps algébrique et sur un corps de caractéristique zéro par Lech [16],et plus tard par Mahler [18],[19] le livre de Everest [13] et autres Donne un historique du théorème de Skolem-Mahler- Lech .

Exemple 1.2.1 *Soit la suite récurrente* $a(n)$ *définit par:*

$$a(n+6) = 6a(n+4) - 12a(n+2) + 8a(n)$$

avec les conditions initiales

$$(a_0, a_1, \ldots, a_6) = (8, 0, 9, 0, 8, 0)$$

L'ensemble $A_k = \{k \in \mathbb{N} \ / \ a(k) = 0\}$ *est la reunion d'un ensemble fini et la progression arithmétique* $\{1, 3, 5, \ldots.\}$ *car*

$$a(n) = \begin{cases} 0 & \text{si } n \text{ impair} \\ (n-8)^2\, 2^{(n-6)/2} & \text{si } n \text{ est pair} \end{cases}$$

Mahler établit le lemme suivant dans sa démonstration 1.2.5

Lemme 1.2.9 *[18]Soit K un corps commutatif de caractéristique zéro, algebriquement clôs , et soit*

$$F(x) = \sum_{n=0}^{\infty} a(n)\, x^n \in R(K) \quad et\ a(n) = \sum_{i=1}^{s} P_i(n)\, \alpha_i^n$$

Soit $\Omega = \{\ \alpha_i/\alpha_j$, racine de l'unité autre que $1\ \}$.
Si $I(F) = \{\ n \in \mathbb{N}\ /\ a(n) = 0\}$ est infini , Alors $\Omega \neq \emptyset$.
Soit M le plus petit entier tel que $\zeta^M = 1$ pour tout $\zeta \in \Omega$ .Si $I_{m,\mu} = \{\ n\ ,\ n = \mu \bmod m\} \subset I(F)$ .Alors $I_{m',\mu} \subset I(F)$ avec $m' = ppcm(m, M)$.

1.3 Sur le théorème de Skolem-Mahler -Lech

Dans cette section nous présentons la démonstration d'un théorème analogue au théorème de Skolem-Mahler-Lech .

Définition 1.3.1 *Soient s, t, m des entiers positifs et $\{\Psi_1(x), ..., \Psi_s(x)\}$ un ensemble de s séries entieres de $\overline{\mathbb{Q}}[[x]]$ on dit que cet ensemble est $(m, t) -$ propre s'il existe un ensemble infini A de nombres premiers rationels p tel que pour tout plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$ le rayon de convergence de $\Psi_i(x)$ $i = 1, ..., s$ dans $\mathbb{C}_p$ est plus grand que $p^{-m/t(p-1)}$.*

Notation 1.3.1 *pour tout entier positif m on note par $J_m(x)$ la série*

$$J_m(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!^m}$$

Remarque 1.3.1 *pour $m = 1$:$J_1(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ est la série exponentielle .*

Théorème 1.3.1 *Soient s, t, m des entiers positifs si*

$$F(x) = \sum_{j=1}^{s} \Psi_i(x) J_m(\beta_j x^t) + P(x) \tag{1.3.1}$$

Avec $\{\Psi_1(x), ..., \Psi_s(x)\}$ est un ensemble (m, t) propre d'éléments dans $\bar{\mathbb{Q}}[[x]]$, $\beta_j \in \bar{\mathbb{Q}} \setminus \{0\}$ (un élément algébrique non nul) et $P \in \bar{\mathbb{Q}}[[x]]$

Alors il existe un entier positif d tel que pour $r \in \{0, 1, ..., d-1\}$ ona:

a) $a(kd+r) = 0$ *pour k suffisament grand ou*

b) $a(kd+r) \neq 0$ *pour k suffisament grand .*

avant d'entamer la démonstration du théorème, considérons les résultats suivants:

1.3.1 Fonction continue sur $\mathbb{Z}_p$

Soit $f(x)$ une fonction continue sur $\mathbb{Z}_p$ et a valeurs dans $\mathbb{Q}_p$,et soit $f_n(x)$ son $n^{\text{ième}}$ polynôme d'interpolation sur la suite des entiers naturels défini par

$$deg(\ f_n) \leq n \text{ et } f_n(j) = f(j) \quad \text{pour} \ \ (j = 1, ..., n)$$

On obtient .

$$f_n(x) = \sum_{k=0}^{n} a_k \binom{x}{k} \quad \text{ou} \quad a_k = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} f(j) \,.$$

Définition 1.3.2 *Soit E un espace de banach sur un corps valué K ,la famille $(e_i)_{i\in I}$ d'éléments de E est une base normale de E si tout $x \in E$ admet une unique représentation $x = \sum_{i\in I} x_i e_i$ où $x_i \in K$ et $x_i \longrightarrow 0$, $|x| = \sup_{i\in I} |x_i|$*

K.MAHLER a obtenu le resultat suivant en 1958.

Théorème 1.3.2 *[19]**de K.Mahler***

Soit f une fonction continue sur $\mathbb{Z}_p$, et a valeurs dans $\mathbb{Q}_p$,la suite f_n converge uniformement vers f sur $\mathbb{Z}_p$, alors f est somme de la série (uniformement convergente)

$$f(x) = \sum_{n\geq 0} a_n \binom{x}{n}$$

de plus

$$\|f\| = \max_{x\in\mathbb{Z}_p} |a_n|$$

et donc les polynôme $\binom{x}{n}$ constituent une base normale de l'éspace des fonctions continues sur $\mathbb{Z}_p$ muni de la norme de la convergence uniforme..

Remarque 1.3.2 *Par la compacité de $\mathbb{Z}_p$nous savons qu'il y a seulement un nombre fini de disques qui interviennent.*

Notation 1.3.2 *Soient E un espace de banach sur K , A l'anneau de valuation et et k le corps residuel de K.*
Nous noterons :

$$\begin{aligned} E_0 &= \{x \in E / |x| \leq 1\} \text{ est un A-module} \\ \grave{E}_0 &= \{x \in E / |x| \prec 1\} \\ \bar{E} &= E_0 / \grave{E}_0 \text{ c'est un } k\text{-espace vectoriel} \\ & \quad P \text{ la projection canonique de } E_0 \text{ sur } \bar{E} \end{aligned}$$

(*pour tout* $x \in E$, $x \neq 0$ *il existe* $a \in K$ *tel que* $|x| = |a|$)

ou ce qui est equivalent
(pour tout $x \in E, x \neq 0$ il existe $b \in K$ tel que $|bx| = 1) *$
Cette condition est nécessaire pour que E posséde une base normale.

Théorème 1.3.3 *[1]Soit E un espace de Banach sur K ;si Kest a valuation discrete et si E satisfait la condition * alors pour une famille $(e_i)_{i \in I}$ d'élements de E_0 les conditions suivantes sont equivalentes.*
i/ $(e_i)_{i \in I}$ est une base normale de E .
ii/ $(P(e_i))_{i \in I}$est une base du k espace vectoriel $\bar{E}$.

Proposition 1.3.1 *[1][2]Soit l'entier n ,tel que $n < p^h$, alors .*

$$v(x-y) \geq h \Rightarrow v\left(\binom{x}{n} - \binom{y}{n}\right) \geq 1$$

Théorème 1.3.4 *Pour tout entiers s non nul ,on a l'ensemble $\left\{q_n^s(x) = \binom{x}{n}^s ; n \in \mathbb{N}\right\}$ forme une base normale de l'espace $E = \varphi(\mathbb{Z}_P, \mathbb{Q}_P)$ qui est l'espace des fonctions continues de $\mathbb{Z}_p$ sur $\mathbb{Q}_P$.*

Preuve. D'aprés le théorème 1.3.3 Il suffit de preuver que pour tout $s \in \mathbb{N}^*$on a $\{\bar{q}_n^s; n \in \mathbb{N}\}$forme une base vectoriel de l'espace $\bar{E} = \varphi(\mathbb{Z}_P, \mathbb{Q}_P)$.
Soit $\bar{E}_h$ un espace valué de $IF_p = \mathbb{Z}/p\mathbb{Z}$ des fonctions constantes dans les boules

$$B_{p^{-h}}(a) = \left\{x \in \mathbb{Z}_P; |x-a| \leq p^{-h}\right\}$$

On a $\bar{E} = \bigcup \bar{E}_h$
donc il suffit de montrer que l'ensemble $\left\{\bar{q}_n^s(x); n < p^h\right\}$forme une base de $\bar{E}_h$.
pour $n < p^h$et $|x-y| < p^{-h}$on a d'aprés la proposition 1.3.1 $\left|\binom{x}{n} - \binom{y}{n}\right| < 1$ et par conséquent on a

$$\left|\binom{x}{n}^s - \binom{y}{n}^s\right| = \left|\binom{x}{n} - \binom{y}{n}\right| \left|\sum_{m=0}^{s-1} \binom{x}{n}^m \binom{y}{n}^{s-m-1}\right| < 1$$

donc $\bar{q}_n^s(x) = \bar{q}_n^s(y)$ ce qui montre $\bar{q}_n^s \in \bar{E}_h$ et $\bar{q}_n^s = \sum_{j=1}^{p^p-1} \bar{q}_n^s(j)\chi_j$ donc le matrice représentant les $\bar{q}_n^s$ sur les $\left\{\chi_j; n < p^h\right\}$ est triangulaire,ses éléments diagonaux sont égaux à 1.elle est donc inversible. ■

Lemme 1.3.1 *[30] Soit la série* $f(x) = \sum_{k=0}^{\infty} c(k) \binom{x}{k}^m$ *avec* m *un entier positif fixé , si* $\limsup |c(k)|^{1/k} < 1$ *alors* $f(x)$ *représente une fonction localement analytique sur* $\mathbb{Z}_p$.

Preuve. Du théorème (1.3.1)

Le cas t = 1

Soit p un nombre premier assez grand donc les rayons de convergence des $\Psi_j(x)$ dans $\mathbb{C}_p$ sont tous plus grand que $p^{-m/(p-1)}$ pour tout j et soient β_j des élements de $\mathbb{C}_p$de valuation p-adique vaut 1 et posons

$$\Psi_j(x) = \sum b_{j,k} x^k \tag{1.3.2}$$

On a

$$J_m(\beta_j x) = \sum \beta_j^n x^n / n!^m \tag{1.3.3}$$

D'aprés (1.3.2) et (1.3.3) on trouve la relation

$$\Psi_i(x) J_m(\beta_j x^t) = \sum g_j(n) \beta_j^n \frac{x^n}{n!^m}$$

avec

$$g_j(n) = \sum k!^m b_{j,k} \beta_j^{-k} \binom{n}{k}^m$$

On apar hypothése les $\Psi_j(x)$ est sont $(m,1)-propre$ alors par le lemmen 1.3.1 on a tout $g_j(x)$ peut être prolongé en une fonction localement analytique sur $\mathbb{Z}_p$.

comme β_j sont des unités p-adiques d'aprés le lemme 1.2.5 il existe un entier d tel que pour tout j on a

$$\left|\beta_j^d - 1\right| < p^{-1/p-1}$$

donc les fonctions β_j^{dk+r} sont des fonctions en k analytiques sur le disque $D(0,1^+)$ sur $\mathbb{C}_p$ et comme on a

$$F(x) = \sum a(n)\, x^n = \sum_{j=1}^{s} \Psi_j(x) J_m(\beta_j x^t) = \sum g_j(n)\, \beta_j^n x^n / n!^m$$

donc la fonction $a(kd+r)$ en k est une fonction localement analytique sur $\mathbb{Z}_p$, par consequence $a(kd+r)$ admet une infinité de zéro pour k assez grand ou bien $a(kd+r) \neq 0$ pour k suffisament grand.

Le cas général:

On montre le resultat pour les séries $F_r(x) = \sum a(kt+r)\, x^r$ pour $r \in \{0, 1, ..., t-1\}$ et on a:

$$x^r F_r\left(x^t\right) = \sum F(\zeta x)$$

La sommation étant faite sur les racines $t^{\text{éme}}$ de l'unité.

d'aprés la définition de F on a la relation suivante

$$x^r F_r\left(x^t\right) = \sum \tau_j\left(x^t\right) x^r J_m\left(\beta_j x^t\right)$$

avec $\tau_j\left(x^t\right) x^r := \sum \Psi_j(\zeta x) \zeta^{-r}$ la sommation étant faite sur les racines $t^{\text{éme}}$ de l'unité.

Posons R le rayon de convergence de τ_j dans $\mathbb{C}_p$ donc le rayon de convergence de $\tau_j\left(x^t\right)$ est $R^{1/t}$ et par conséquent l'ensemble de tout les $\tau_j(x)$ est $(m,1) - propre$ et comme on a la relation

$$F_r(x) = \sum \tau_j(x)\, J_m\left(\beta_j x\right)$$

donc on applique les résultats du cas $t = 1$.

ce qui achéve la démonstration. ■

Remarque 1.3.3 *La même preuve convient en remplaçant le terme $J_m(\beta_j x^t)$ dans le théorème 1.3.1 avec un terme de la forme $\sum Q_j(n)\beta_j^n x^{tn}/n!^m$ où $Q_j \in \overline{\mathbb{Q}}[x] \smallsetminus \{0\}$.*

Proposition 1.3.2 *Soient $\Psi(x)$ un élément non nul de $\overline{\mathbb{Q}}[[x]]$,m un entier positif et $\beta \in \overline{\mathbb{Q}} \smallsetminus \{0\}$*
supposons que $\Psi(x)$ est $(m,1)$ propre alors la série

$$F(x) = \Psi(x)J_m(\beta x)$$

à seulement un nombre fini de coefficients nuls.

Preuve. Soit

$$F(x) = \Psi(x)J_m(\beta x) = \sum a(n)\, x^n$$

non identiquement nul ,supposons le contraire c'est-à-dire qu'il existe un ensemble infini des entiers naturels n tels que la suite $a(n) = 0$.
Soit p_1 le premier nombre premier tels que Ψ est $(m,1) - propre$ par rapport à p_1 . Alors il existe un nombre naturel h_1 tels que , pour tout t dans l'ensemble $\{0,1,\ldots,p_1-1\}$ la fonction $a(kp_1+t)$ est une fonction de k, on peut la prolonger à une fonction analytique sur le disque $D(0,1)$ dans le corps $\mathbb{C}_{p_1}$, d'aprés la $1^{\text{ére}}$ partie de la démonstration du théorème 1.3.1 pour une valeur de t que l'on note t_1 on a un nombre infini d'entiers non négatifs k, tels que $a(kp_1+t_1) = 0$ et donc $a(kp_1+t_1) = 0$ pour tout k .
Soit maintenant p_2 un deuxième nombre premier ($p_2 \neq p_1$) tels que Ψ soit $(m,1) - propre$ respectivement à p_2. Il existe un nombre naturel h_2 tels que pour tout t dans $\left\{0,1,\ldots,p_2^{h_2}-1\right\}$ la fonction $a(kp_2+t)$ est une fonction en k qu'on peut prolonger en une fonction analytique sur le disque $D(0,1)$ de $\mathbb{C}_{p_2}$.Soit t_2 un élément arbitraire de l'ensemble $\left\{0,1,\ldots,p_2^{h_2}-1\right\}$ comme on a $(p_1,p_2) = 1$ alors $(p_1^{h_1},p_2^{h_2}) = 1$ d'où il existe un nombre infini de couple $(k,k\prime)$ tels que

$$kp_1^{h_1} + t_1 = k'p_2 + t_2$$

par conséquent pour tout t_2 dans$\left\{(0,1,\ldots,,p_2^{h_2}-1)\right\}$ on a

$$a(k'p_2+t_2) = 0 \quad \text{pour} \quad \text{tout} \quad k' \text{et } t_2$$

qui implique que $a(n) = 0$ pour tout n qui est une contradiction cela termine la démonstration . ∎

Corollaire 1.3.1 *Soit s un entier positif et $\Psi_j(x)$ et ϕ_j des sériers entieres algébriques non nulles de $\bar{\mathbb{Q}}[[x]]$, $\phi_j(0) = 0, \phi_j'(0) = \beta_j \neq 0$ pour $j = 1, ..., s$ posons*

$$F(x) = \sum_{j=1}^{s} \Psi_j(x) \exp(\phi_j(x))$$

alors $F(x)$ satisfait la conclusion du théorème 1.3.1

Preuve. Comme les séries $\Psi_j(x)$ sont algèbriques leurs rayons de convergence dans $\mathbb{C}_p$ sont inférieur à 1 pour p premier suffisamment grand et d'autre part on a $\phi_j(0) = 0, \phi_j'(0) = \beta_j \neq 0$ par conséquent on peut écrire ϕ_j sous la forme

$$\phi_j(x) = \beta_j x + x^2 H_j(x)$$

avec $H_j(x)$ est encore une série algèbrique et β_j un élément algébrique non nul ,les séries algebriques à des coefficients de Taylor avec des valeurs p-adiques inférieures ou égales à 1.donc le rayon de convergence pour chaque série $exp(x^2 H_j(x))$ dans $\mathbb{C}_p$ est au moins plus grand que le rayon de convergence de la série $exp(x^2)$ (i.e plus grand que $p^{-1/2(p-1)}$) .
On pose

$$\eta_j(x) = \Psi_j(x) exp(x^2 H_j(x)) \tag{1.3.4}$$

D'après ce qui précède l'ensemble $\{\eta_1(x), \ldots, \eta_s(x))\}$ est un $(1,1)-propre$ ceci nous permet d'appliquer le théorème 1.3.1 et de conclure la preuve . ■

Corollaire 1.3.2 *Soit E l'algébre des séries de la forme $(1 + ax)^b$ et les séries de la forme $\log(1 + cx)$, avec a, b, c sont des entiers algebriques alors toutes les séries de type (1.3.1) avec $\Psi j(x) \in E$ satisfont la conclusion du théorème 1.3.1 .*

Preuve. Il suffit de montrer que pour tout ensemble de s éléments de E est $(m,t)-$ *propre* pour tout couple d'entiers positifsn (m,t).
Soient $\Psi_1, \ldots, \Psi_s$ s éléments de E, et soit K le corps de nombres qui contient tous les éléments a, b, c les coefficients des séries algebriques qui apparaissent dans la définition de Ψ_j d'après le théorème de Cassels 1.2.4 il existe une infinité de nombres premiers p tel que il ya un plongement de K dans $\mathbb{Q}_p$,Comme les constantes sont dans $\mathbb{Q}_p$, pour p suffisament grand on peut assurer que ces constantes sont des éléments de $\mathbb{Z}_p$ donc a, b, c sont dans $\mathbb{Z}_p$

et d'où les fonctions $(1+ax)^b$ et $\log(1+cx)$ ont des rayons de convergence supérieurs ou égaux à 1 donc c'est le même cas pour tout les Ψ_j,par conséquence l'ensemble des fonctions est $(m,t)-propre$ pour tout entier m et t,ce qui permet d'appliquer le théorème 1.3.1 et de conclure la preuve. $\blacksquare$

Chapitre 2

Suites recurrentes lineaires en caracteristique non nulle

Le but de ce chapitre est d'étudier quelques problèmes sur les suites récurrentes lineaires en caracteristique p, comme l'analogue du théorème de Skolem-Mahler-Lech sur les zeros des suites récurrentes linéaires, et aussi certains théorèmes de G.Polya.

2.1 Algèbre de Hadamard:

Définition 2.1.1 *Le produit de Hadamard de deux séries est défini par :*

$$\sum_{n=0}^{\infty} a(n)\, x^n \odot \sum_{n=0}^{\infty} b(n)\, x^n = \sum_{n=0}^{\infty} a(n)\, b(n)\, x^n \qquad x \in K$$

L'ensemble des séries rationnelles muni de ce produit est une algébre de hadamard des séries rationnelles dont l'élément neutre est la série $\sum_{n\geq 0} \mathrm{x}^n = \dfrac{1}{1-x}$

Définition 2.1.2 ***a)****Une série géométrique est une série de la forme*

$$a\sum \lambda^n x^n \qquad \textit{avec}\ \ a, \lambda \in K \quad \textit{et}\ \lambda \neq 0$$

et si elle n'est pas nulle l'inverse de Hadamard est $a^{-1}\sum \lambda^{-n}x^n$
Etant données p séries :

$$S_i(x) = \sum_{n\geq 0} a(i+nt)\,x^n \qquad\qquad 0 \leq t \leq p$$

appelons emboîtement de ces séries la série :

$$\sum a(n)\,x^n = \sum_{0\leq t\leq p-1} x^i S_i\left(x^t\right)$$

b) *Une série semi-simple est une série qui est somme de séries géométriques.*

Notation 2.1.1 *Soit* K *un corps algébriquement clôs .*
Considérons le groupe multiplicatif $G = K^* = K \setminus \{0\}$ *et l'anneau* $K[t]$ *nous construisons la* $K[t]-$*algébre de* G *notée* $K[t][G]$.

Lemme 2.1.1 *[24]*
l'application $\varphi : \sum\limits_{\lambda\in G} P_\lambda(n)\,\lambda \longrightarrow \sum\limits_{n\geq 0} a(n)\,x^n$ *définie par*

$$\forall n \geq 0 \quad a(n) = \sum_{\lambda\in G} P_\lambda(n)\,\lambda^n$$

réalise un isomorphisme de $K-$*algébres de* $K[t][G]$ *dans l'algébre des séries rationnelles .*

Définition 2.1.3 *Si* $u(n) = \sum\limits_{i=1}^{s} P_i(n)\;\alpha_i^n$ *est un polynôme expononentiel ,la suite* $(u(n))$ *est dite non dégénerée si pour tout* $i \neq j$ *on a le quotient* α_i/α_j *n'est pas une racine de l'unité.*

Définition 2.1.4 *Soit* A *une partie de* $\mathbb{N}$ *on appelle densité banachique supérieure de* A *la quantité* $d^*(A)$ *suivante :*
$d^*(A)$ *est la limite supérieure des nombres* $card(I\cap A)\,/\,card(I)$ *.ou* I *décrit les intervalles de* $\mathbb{N}$ *et* $card(I)$ *tend vers* $+\infty$.

$$d^*(A) = \lim\ sup\ \frac{card(I\cap A)}{card(I)}$$

On dira que A *est de densité banachique nulle si* $d^*(A) = 0$.

Nous aurons besoin des résultats suivants:

Théorème 2.1.1 *[22]de Szemeredi*
Soit A une partie de $\mathbb{N}$ de densité banachique supérieure strictement positive Alors A contient des progressins arithmétique arbitrairement longues.

Théorème 2.1.2 *[29]Van Der Poorten*
Soit K un corps de caractéristique nulle ,et H un sous groupe de type fini du groupe multiplicatif de K soit m un entier naturel non nul ,il existe seulement un nombre fini d'éléments $\underline{x} = (x_0, ..., x_m)$ dans $IP^m(K)$ tel que :
a) $x_0 + x_1 + ... + x_m = 0$
b) x_i appartient à H pour toute i
c) $x_{i_0}, ..., x_{i_t} \neq 0$ pour toute partie non vide et propre $\{i_0, ..., i_t\}$ de $\{0, ..., m\}$.

Théorème 2.1.3 *[24]Reutenauer*
Soit K un corps de caractéristique non nulle p que l'on suppose algébriquement clôs .
Soit $u = (u(n))$ une suite récurrente linéaire d'éléments de K Alors il existe un entier d supérieur ou égal à 1, tel que pour tout r appartenant à $\{0, ..., d-1\}$ la suite $u(kd+r)$ soit nulle ou une somme de suites géométriques

Preuve. :
Soit $S(x) = P(x) \,/\, Q(x)$ une série rationnelle où P et Q sont des polynômes dans $K[x]$ tels que $\deg(P) < \deg(Q)$.

Décomposons cette fraction rationnelle en éléments simples,S est donc combinaison linéaire de séries de la forme:

$$T = \frac{1}{(1-\alpha x)^t} \qquad \text{avec } t \geq 1$$

Soit l et k deux entiers naturels tels que $t + l = p^k$ donc;

$$\begin{aligned} T &= \frac{(1-\alpha x)^l}{(1-\alpha x)^t (1-\alpha x)^l} = \frac{(1-\alpha x)^l}{(1-\alpha x)^{p^k}} = \frac{(1-\alpha x)^l}{1-\alpha^{p^k} x^{p^k}} \\ &= (1-\alpha x)^l \sum_{n \geq 0} \alpha^{np^k} x^{np^k} \end{aligned}$$

Ce qui montre que T est égal à un emboîtement de séries géométriques donc semi simples.
■

Définition 2.1.5 *Soit $x_1, ..., x_n$ avec $n \geq 2$, le déterminant de **Vandermonde** relatif aux x_i est le déterminant $V = V(x_1, ..., x_n)$ donné par :*

$$V = \begin{vmatrix} 1 & x_1 & x_1^2 & ... & x_1^{n-1} \\ 1 & x_2 & x_2^2 & ... & x_2^{n-1} \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ 1 & x_n & x_n^2 & ... & x_n^{n-1} \end{vmatrix}$$

Notons $C_0, ..., C_{n-1}$ les colonnes de V alors

$$V = \det(C_0, C_1 - x_1 C_0, C_2 - x_1 C_1, ..., C_{n-1} - x_1 C_{n-2})$$

c'est -à-dire:

$$V = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & x_2 - x_1 & (x_2 - x_1)\, x_2 & ... & (x_2 - x_1)\, x_2^{n-2} \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ 1 & x_n - x_1 & (x_n - x_1)\, x_n & ... & (x_n - x_1)\, x_n^{n-2} \end{vmatrix}$$

on obtient :

$$V(x_1, ..., x_n) = \prod_{1 \leq i, j, \leq n} (x_j - x_i) \text{ pour } i < j$$

Théorème 2.1.4 *Soit K un corps commutatif de caractéristique p non nulle et $(u(n))$ une suite récurrente lineaire d'éléments de K .il existe un entier d supérieur ou égale à 1 , tel que , en notant*

$$A_r = \{ \ k \quad / \quad u(kd + r) = 0\} \qquad \overline{r = 0, d - 1}$$

Alors on ait

a) Soit A_r est de densité banachique nulle.

b) Soit A_r est égal à $\mathbb{N}$.

Preuve.

D'aprés le théorème de **Reutenaur** 2.1.3 la suite $(u(n))$ s'écrit comme somme de séries géométriques avec a_i et b_i des éléments de K

$$u(n) = \sum_{i=1}^{t} a_i b_i^n$$

et comme on a $i \neq j$ alors b_i/b_j n'est pas une racine de l'unité et a_i non nul pour tout i.

Soit l'ensemble $A = \{n \in \mathbb{N} \ / \ u(n) = 0\}$,Nous allons raisonner par l'absurde en supposant donc que la densité banachique de l'ensemble A est strictement positive ,d'aprés le théorème de **Szemeredi** 2.1.1 il existe t éléments de A en progressions arithmétiques qu'on les note $kd + r$ avec $0 \leq k \leq t-1$ le systéme d'équations linéaires en les inconues X_i.

$$\sum_{i=1}^{t} \left(b_i^d\right)^k X_i = 0 \qquad\qquad \overline{k = 0, t-1}$$

Ce systéme admet une solution non triviale $X_i = a_i b_i^r$
remarquons que le déterminant de ce systéme est un déterminant de **Vandermonde** construit sur les $\left(b_i^d\right)$ est nul donc $b_i^d = b_j^d$ pour $i \neq j$ donc b_i/b_j est une racine de l'unité ,et cette contradiction démontre le théorème . ■

Remarque 2.1.1 *Le théorème 2.1.4 est vrai en toute caractéristique [8].*

Théorème 2.1.5 *Soit $(u(n))$ et $(v(n))$ deux suites récurrentes linéaires à valeurs dans un corps commutatif K de caractéristique quelconque on suppose que l'on a $u(n)v(n) = 0$ $\forall n$ alors il existe un entier q supérieur ou égal à 1 et une partition de $\{0, 1, ..., q-1\} = I \cup J$ telle que :*

$$\{n \in \mathbb{N} \ / \ u(n) \neq 0\} \subset I + q\mathbb{N} \quad \text{et} \quad \{n \in \mathbb{N} \ / \ v(n) \neq 0\} \subset J + q\mathbb{N}$$

Preuve.
D'aprés le théorème 2.1.4 il existe donc un entier naturel non nul d tel que chacune des suites $u(kd + r)$ et $v(kd + r)$ vérifie l'une des deux propriétés **a)**ou **b)** de l'énoncé de ce théorème2.1.4 .

Soit

$$I_r = \{ \ k \in \mathbb{N} \ / \ \ u(kd + r) = 0\} \text{ et } I'_r = \{ \ k \in \mathbb{N} \ / \ v(kd + r) = 0\}$$

on note $I = \{ \ r \ \ / \ \ d^*(A_r) = 0\}$

Si I est vide: on a $u(kd+r) = 0 \quad \forall k$ donc la suite u est une suite identiquement nulle et il n' y a rien à montrer .

Si I est non vide: soit γ un élément de I donc on a pour tout k

$$u(kd+\gamma)\, v(kd+\gamma) = 0$$

alors $v(kd+\gamma)$+0 sauf peut être pour un ensemble de densité nulle,

en résulte que

$$v(kd+\gamma) \ \ = 0 \quad \text{pour tout } k$$

Ceci démontre que

$$\{n \ / \ v(n) \neq 0\} \subset I + d\,\mathbb{N}$$

et on a la même chose pour la suite $(u(n))$

$$\{n \ / \ u(n) \neq 0\} \subset I + d\,\mathbb{N}$$

■

Corollaire 2.1.1 *[24]Soit $\mathbb{N} = A \cup B$ une partition telle que $A = \{n \ / \ a(n) \neq 0\}, B = \{n \ / \ b(n) \neq 0\}$ pour des séries rationnelles $\sum a(n) x^n$ et $\sum b(n) x^n$ Alors A et B sont réunion finie de progressions arithmétiques de même raison.*

Exemple 2.1.1 *l'exemple de Lech donné dans l'article [16]*

$$u(n) = (1+z)^n - 1 - z$$

en caractéristique $p > 0$ cette suite ne s'annule que lorsque n est une puissance de p.

2.2 Théorème de Polya:

Dans ce paragraphe nous caracterisons les suites récurrentes linéaires à valeurs dans $\mathbb{Q}$,ayant un nombre fini de facteurs premiers.

Définition 2.2.1 *Soit $(u(n))$ une suite récurrente linéaire a terme dans $\mathbb{Q}$, p un nombre premier .*

p est dit facteur premier de la suite$(u(n))$ s'il existe un entier $n \in \mathbb{N}$ tel que $v_p(u(n)) \neq 0, \infty$.
Une suite $(u(n))$ de $\mathbb{Q}$ est de Polya si pour presque tout nombre premier p la valuation p-adique v_p est trivial sur la suitee $(u(n))$.
Une série $\sum\limits_{n\geq 0} \alpha(n) x^n$ est dite une fonction de Polya s'il existe un entier $m \geq 1$ et des éléments $\alpha_0, ..., \alpha_{m-1}$ de K tels que pour $\mu = 0, ..., m-1$ on a $\alpha_{\mu+tm} = \alpha_\mu.\alpha_\mu^t$ pour tout $t \geq 0$.

Lemme 2.2.1 *Soit $S(x) = \sum\limits_{n\geq 0} u(n) x^n$ une série rationnelle pour tout $\sigma \in G =$ Galois de K , $\sigma S = \sum\limits_{n\geq 0} \sigma u(n) x^n$ et $N(S) = \prod\limits_{\sigma \in G} \sigma S$*
une suite de nombres algébriques $(u(n))$ est de Polya si la suite $(N(u(n)))$ est de polya

Remarque 2.2.1 *:*

- ▶ *L'ensemble des suites de Polya est multiplicativement stable .*
- ▶ *Les fonctions de Polya forment une partie multiplicativememt stable de $R(K)$.*

Théorème 2.2.1 ***de Polya:***
Soit $(u(n))$ une suite récurrente linèaire dans $\mathbb{Q}$.
$S = \{$ p, premier / il existe $n \in \mathbb{N}$; $v_p(u(n)) \neq 0, \infty$ $\}$.
Si S est un ensemble fini alors il existe un entier d non nul,et des éléments a_μ, b_μ dans $\mathbb{Z}$, $0 \leq \mu \leq d-1$ tels que :

$$F(x) = \sum u(n) x^n = \sum_{\mu=0}^{d-1} \frac{a_\mu x^\mu}{1 - b_\mu x^d} \tag{2.2.1}$$

Pour la demonstration du théorème de Polya 2.2.1 nous ferons usage des lemmes suivants:

Lemme 2.2.2 *[5] Soit $G(x) = \sum\limits_{n=0}^{\infty} u(n) x^n$ une série rationnelle non reduite a un polynôme et p un nombre premier alors il existe $n_0 \geq 0$ et $q \geq 1$ tel que l'application $n \longrightarrow v_p(u(n_0 + qn))$ est affine.*

Lemme 2.2.3 *[5]Soit $G(x) = \sum\limits_{n=0}^{\infty} u(n) x^n$une série rationelle à coefficients dans $\mathbb{C}$ alors il existe un entier d non nul tel que pour tout $\mu \in \{0, 1, ...d-1\}$ la série $G_r(x) =$*

$\sum\limits_{k=0}^{\infty} u(kd+r)x^k$ *satisfait a la proprieté* $(*)$
$(*)$ *soient* μ_i *les pôles de* G_r *alors aucun des quotients* μ_i/μ_j *n'est une racine de l'unité pour* $i \neq j$.

Preuve. Du théorème de Polya:
Soient $u(n)$ une une suite récurrente linéaire et $G(x) = \sum\limits_{n=0}^{\infty} u(n)x^n$ la série rationnelle associée ,tel que l'ensemble des facteurs premiers est fini.d'aprés le lemme 2.2.3 aucun des quotients μ_i/μ_j n'est une racine de l'unité pour $i \neq j$,avec les μ_i sont des pôles de G_r donc il sufit de montrer que $G(x)$ est une serie géométrique (ou encore que la s.r.l $(u(n))$est d'ordre un).si on applique succéssivement le lemme 2.2.2 ,on trouve des entiers n_0, q tels que pour tout j l'application $n \longrightarrow v_{p_j}(u(n_0+qn))$ est affine avec p_j sont les facteurs premiers de la suite $(u(n))$ $j = 1, ..., l$
posons

$$u(n) = \varepsilon_n p_1^{\Phi_1(n)} ... p_l^{\Phi_l(n)}$$

avec $\varepsilon_n \in \{0, 1, -1\}$ et $\Phi_j(n) \in \mathbb{Z}$.donc on a

$$u(n_0+qn) = \theta_n v w$$

où $\theta_n = \varepsilon_{n_0+qn}$,$v = p_1^{t_1}...p_l^{t_l}$, $w = p_1^{r_1}...p_l^{r_l}$.

on a

$$u(n) = \sum_{j=1}^{l} p_j(n)\mu_j^n$$

par suite

$$\begin{aligned} v(n) &= u(n_0+qn) = \sum_{j=1}^{l} p_j(n_0+qn)\mu_j^{n_0+qn} \\ &= \sum_{j=1}^{l} p_j(n_0+qn)\mu_j^{n_0}\left(\mu_j^q\right)^n \\ &= \sum_{j=1}^{l} A_j(n)\beta_j^n \end{aligned}$$

ou $A_j(x) = p_j(n_0+qx)\mu_j^{n_0}$ et $\beta_j = \mu_j^q$.
comme les μ_j^qsont tous distincts (les μ_j distincts d'aprés le lemme 2.2.3) ,et les $A_j(x)$ ne

sont pas identiquement nuls et donc la serie $\sum v(n) x^n$ n'est pas reduite a un polynôme donc $\theta_n \neq 0$ pour une infinité de n.
supposons $\theta_n = 1$ alors $v(n) - vw = 0$ pour une infinité de n, ($v(n)$ verifie une relation de récurrence) d'aprés le théorème de **Mahler** 1.2.5 on peut trouver deux entiers a et b tels que pour tout **l** on a

$$v(a+bl) = vw^{a+bl}$$

donc

$$vw^{a+bl} = \sum_{j=1}^{l} A_j (a+bl) \beta_j^a \left(\beta^b\right)^l$$

comme le polynôme exponentiel est unique alors on a $l = 1$ et $A_j(a+bl)$ est constant donc $A_1(x)$ et par suite $p_1(x)$ est constant..
d'ou $(u(n))$ est de la forrme

$$u(n) = p_1 \mu_j^n$$

avec p_1 constante . ■

2.2.1 Généralisation du théorème de Polya a un corps de nombres algébriques :

Le théorème de Polya se géneralise a un corps de nombres sous la forme suivante:

Théorème 2.2.2 *[5] Soient K un corps de nombres algebriques ,l'application norme $N : K \longrightarrow \mathbb{Q}$ et $(u(n))$ une suite de K telle que la suite $(N(u(n)))$ ait un nombre fini de facteurs premiers alors on a l'equivalence:*
($(u(n))$ est une une suite récurrente linéaire) $\Leftrightarrow$ (il existe un entier m non nul et des éléments $b_0, ..., b_{m-1}$ tels que pour $r \in \{0, ..., m-1\}$ on a $u(km+r) = u_r (b_r)^k$.

La demonstration de ce théorème repose sur la proposition suivante:

Proposition 2.2.1 *[5]Soit K un corps de caractéristique quelquconque $(u(n))$ une suite d'éléments de $K \setminus \{0\}$ pour que les suites $(u(n))$ et $(1/(u(n)))$ vérifient chacune une relation de récurrence linéaire à coefficients constants il faut et il suffit qu'il existe un entier m non nul , des éléments $b_0, ..., b_{m-1}$ de $K \setminus \{0\}$ tels que pour tout $r \in \{0, ..., m-1\}$ on a*

$$u(km+r) = u(r)(b_r)^k \qquad \textit{pour} \quad \textit{tout} \quad k \in \mathbb{N}.$$

Preuve. du théorème2.2.2 :
Supposons $u(n) \neq 0$ por tout n ,soit N l'application norme de K dans $\mathbb{Q}$ .si $u(n)$ est une s.r.l dans K alors $N(u(n))$ est une suite recurente linéaire sur $\mathbb{Q}$.or $N(u(n))$ a un nombre fini de facteurs premiers d'aprés le théorème et la proposition2.2.1 la suite $(1/N(u(n)))$ est une $s.r.l$ ce qui implique que la suite $(1/(u(n)))$ est aussi une suite récurrente linéaire . ∎

2.2.2 Généralisation du théorème de Polya a un corps de caractéristique quelconque:

Dans cette section nous présentons l'analogue du théorème de Polya pour un corps de caractéristique quelconque .

Théorème 2.2.3 *Soit K un corps de caractéristique quelconque et G un sous-groupe de type fini du groupe multiplicatif de K. Soit $u = u(n)$ une suite récurrente linéaire d'éléments de K .On suppose que pour tout n dans $\mathbb{N}$,on a la propriété suivante*

$$u(n) \qquad \textit{appartient à} \quad G \cup \{0\}$$

alors il existe un entier m non nul et des éléments $a_0, ...a_{m-1}$ dans K, $b_0, ..., b_{m-1}$ de $K \setminus \{0\}$ tels que pour tout $r \in \{0, ..., m-1\}$ on a

$$u(km + r) = a_r (b_r)^k \qquad\qquad \textit{pour tout } k \in \mathbb{N}$$

Remarque 2.2.2 *Si on prend le corps $K = \mathbb{Q}$ et le groupe G par le groupe des s-unités de $\mathbb{Q}$ on retrouve le théorème de Polya .*

Théorème 2.2.4 *[8]Soit K un corps commutatif de caractéristique p non nulle et $(u(n))$ suite récurrente linèaire d'éléments de K . il existe un entier d supérieur ou égal à 1 ,tel que en notant*

$$A_r = \{k \setminus u(kd + r) = 0\} \textit{ pour } r = \overline{0, d-1}$$

on ait l'alternative suivante:
a) A_r est de densité banachique nulle.
b) A_r est egal à $\mathbb{N}$.

Preuve. du théorème2.2.3 :

i)Cas d'un corps de caractéristique nulle:

Soit $(u(n))$ une s.r.l verifiant les hypothése du théoreme .sans restreindre la généralité on peut supposer que $(u(n))$ est non dégénérée et que pour tout n assez grand $u(n) \neq 0$.sous ces hypothéses nous allons démontrer que $(u(n))$ est d'ordre un .

On écrit la relation de récurrence vérifiée par la suite u sous la forme

$$a_s u(n+s) + a_{s-1} u(n+s-1) + ... + a_0 u(n) = 0$$

avec les a_i sont des éléments non tous nuls de K .on pose $F(x) = \sum u(n) x^n$

Il existe une partie D de $\{0, ..., s\}$ de cardinal superieur ou égal à deux ,telle que l'on ait pour une infinité de n les deux propriétés:

a) $\sum\limits_{j \in D} a_j u(n+j) = 0$.

b) Pour toute partie D' de D, non vide et propre ,on a

$$\sum_{j \in D'} a_j u(n+j) \neq 0$$

on a d'aprés la propriété **b)** si $j \in D$ alors a_j est non nul.

Soit H le sous-groupe de type fini de $K \setminus \{0\}$ engendré par G et tous les a_i

Notons $l+1$ le cardinal de D d'aprés le tnéorème2.1.4 on peut trouver un élément $\chi = (\chi)_{j \in D}$ de $IP^l(K)$ tel que l'on ait

$$(a_j u(n+j))_{j \in D} = \chi$$

Soient i_0, j_0 deux éléments distincts de D on peut trouver un élément λ non nul de K et une infinité de n tels que

$$u(n+j_0) = \lambda u(n+i_0)$$

En supposant $j_0 \geq i_0 + 1$,et en posant $t = j_0 - i_0$ donc il existe une infinité de n telles que on a la relation

$$v(n) = u(n+m) - \lambda u(n) = 0 \tag{2.2.2}$$

La suite v est récurrente linéaire et possède une infinité de termes nuls d'aprés le théoréme de Mahler 1.2.9 si $u(n)$ n'est pas identiquement nul alors il existe deux pôles distincts de fraction rationnelle $R(x) = \sum v(n) x^n$ dont le quotient est une racine de l'unité .

D'aprés la relation (2.2.2) on a les pôles de la série $R(x)$ sont les pôles de la série $F(x)$ et d'aprés ce qui précède sur la suite u on a alors

$$v(n) = 0 \text{ pour tout } n$$

On a la relation $S(x) = 1 - \lambda x^n / F(x)$ où S est un polynôme.
Si $F(x) = P(x)/Q(x)$ on voit que,en faisant l'hypothèse que P et Q sont premiers entre eux,que Q divise le polynôme $1 - \lambda x^n$ .Donc les racines de $Q(x)$ sont simples puisque les racines $1 - \lambda x^n$ le sont, de plus si le degré de Q est plus grand que un alors le rapport de deux racines est une racine de l'unité .Donc $d°Q = 1$ et P_i est un polynôme constant et ceci démontre le théorème dans le cas de caractéristique nulle.

ii) Le cas de la caractéristique non nulle.

1)Si K est un corps fini : la suite (u) prend alors un nombre fini de valeurs et par suite elle est périodique .Soit m sa période donc on a

$$u(m+n) = u(n) \qquad \text{pour} \quad \text{tout} \quad n \in \mathbb{N}$$

$$u(km+r) = u(r)(1)^k \quad \text{pour tout } k \text{ et } r \in \{0, \ldots, m-1\}$$

2)Si K est un corps infini :grâce au théorème 2.1.3 , on peut supposer que $u(n)$ s'écrit sous la forme $u(n) = \sum a_i b_i^n$,d'autre part on peut supposer que le corps K contient tous les a_i et b_i et est de type fini sur IF_P.

Nous appelons alors s le degré de transcendance de K sur IF_P et nous démontrons le théorème par récurrence sur s.

Pour $s = 0$ c'est le cas d'un corps fini, le théorème est vrai.

On suppose le théorème vrai pour un corps de degré transcendence inferieur où égal à $s - 1$ et on se place dans le cas ou' le degré de transcendance du corps est s.

i) Il suffit de démontrer le théorème pour le cas ou le corps K est une extension galoisienne de $IF_P(T_1, \ldots, Tm)$ où $T_1, \ldots, T_m$ sont des éléments de K algébriquement indépendants sur

IF_P.
En effet on choisit une base de transcendance $T_1, \ldots, T_m$ de K sur IF_P de sorte que K soit une extension algebrique finie de $IF_P(T_1, \ldots, T_m)$. On peut toujours supposer K est une extension galoisienne L de $IF_P(T_1, \ldots, T_m)$ telle que K soit purement inséparable de L. Il existe donc un entier naturel e tel que pour tout x de K, x^p appartient à L .on peut supposer en considérant des progressions arithmétiques, que la suite $u(n)$ s'écrit sous la forme $\sum a_i b_i^n$ avec b_i/b_j n'est pas une racine de l'unité pour $i \neq j$ .on applique alors l'homomorphisme injectif $q : x \longrightarrow x^p$ on a alors

$$v(n) = Q(u(n)) = u^p(n) = \sum a_i^p \, (b_i^p)^n$$

qui est une suite récurrente linéaire vérifiant les propriétés énoncées par le théorème et $a_i^p, b_i^p \in L$ comme le quotient b_i^p par b_i^p pour $i \neq j$ n'est pas une racine de l'unité en appliquant le théorème supposé vrai pour L , on en déduit que $t = 1$.

ii) On peut supposer que

a) K est galoisien sur$IF_P(T_1, \ldots, T_m)$

b) La suite $u(n)$ est à valeurs dans $IF_P(T_1, \ldots, T_m)$.

K galoisien sur $IF_P(T_1, \ldots, T_m)$ a été démontré dans **i)** on se place dans ce cas il existe H non nul dans $IF_P(T_1, \ldots, T_m)$ tel que pour tout $nH^{n+1}u\,(n)$ soit entier sur $IF_P(T_1, \ldots, T_m)$.

Comme la suite $H^{n+1}u(n)$ vérifie encore les hypothèses du théorème on peut donc supposer dés le départ que $u(n)$ est entier sur $IF_P(T_1, \ldots, T_m)$ pour tout n .

Soit alors N la norme de K sur $IF_P(T_1, \ldots, T_m)$ et V' la suite définie par $V' = N(u(n))$.

Pour tout n on a $V'\,(n) \in IF_P(T_1, \ldots, T_m)$ et V' appartient à un sous-groupe de type fini du groupe multiplicatif du corps $IF_P(T_1, \ldots, T_m)$ par conséquent ; si le théorème est vrai dans ce cas il existe un entier d $(d \geq 1)$ tel que pour tout $r \in \{0, 1, \ldots, d-1\}$ on a la situation suivante :

$V'(kd + r) = 0$ pour tout k Ou

$(1/V\prime(kd + r)$ est une s.r.l

Mais alors la suite $u(kd + r)$ est dans la même situation, dans le dernier cas elle est de la forme donnée par le théorème , grâce à la proposition 2.2.1 .

iii) Nous nous plaçons dans les hypothèses de **ii)** et nous terminons la démonstration du théorème .

puisque $u(n) \in IF_P(T_1, \ldots, T_m)$, on peut écrire pour tout n

$$u(n) = C_n H_1^{l^1} \ldots . H_m^{l_m}$$

Où les H_i sont des polynômes irréductibles distincts et fixés de $IF_P(T_1, \ldots, T_m)$ et C_n une suite d'éléments de IF_p.

On suppose de plus que la suite $(u(n))$ n'est pas identiquement nulle et s'écrit $u(n) = \sum_{i=1}^{t} a_i b_i^n$, le rapport de deux b_i d'indices distincts n'étant pas une racine de l'unité et aussi que les a_i et b_i sont des entiers sur $IF_P(T_1, \ldots, T_m)$.

Nous allons démontrer qu'il existe une progression arithmétique $kd_0 + r_0$, où d_0 est un entier supérieur où égal à un et $r_0 \in \mathbb{N}$,telle que toutes les fonctions $k \longrightarrow l, (kd_0 + r_0)$ soient des fonctions affines pour $j = 1, \ldots, m$.

Notons pour cela H l'un quelconque des polynomes H_i, et nous le démontrons pour H.Nous introduisons la valuation $H - adique$ sur le corps $IF_P(T_1, \ldots, T_m)$,en posons

$$F = (P(x)/Q(x)) = H^q(P_1/Q1)$$

où $q \in \mathbb{Z}$ et H ne divise ni Q_1 ni P_1 ,$V_H(F) = q$.

Soit W_H une extension de V_H du corps K , et π une uniformisante pour le corps valué (K, W_H) .

On écrit $b_i = \pi^{e_i} \beta_i$ avec $e_i \in \mathbb{N}$,β_i unité $W_H - adique$ et on note

$$I = \{i \; / e_i \text{ est minimal } \}$$

et e la valeur commune des e_i pour $i \in I$.

Soit $u(n) = \sum_{i \in I} a_i \beta_i^n$ la suite $u(n)$ est une s.r.l et vérifie une relation de récurrence linéaire de type :

$$u(n+h) = e_{n-1} u(n+h-1) + ... + e_0 u(n)$$

les e_i étant dans l'anneau de valuation de W_H pour tout j et e_0 étant une unité W_H- adique puisque tous les β_i sont des unités W_H-adique.Soit l un entier naturel tel que ,pour k variant entre 0 et $h-1$, $\pi^{-1} u(k)$ soit dans l'anneau de valuation, et qu'il existe k_o,$0 \leq k_0 \leq h-1$, tel que $\pi^{-1} u(k_0)$ soit une unité W_H -adique.

Soit $b\left(n\right)=\pi^{-1}a\left(n\right)$, la suite $b(n)$ est à valeurs dans l'anneau de valuation pour tout n ; et son image dans le corps résiduel de (K, W_H) n'est pas identiquement nulle puisque l'un au moins des $b(k)$ est une unité W_H- adique,la suite $b(n)$ verifie la même relation de récurrence que $a(n)$,donc l'image $\overline{b(n)}$ de $b(n)$ dans le corps résiduel de (K, W_H) vérifie :

$$\bar{b}\left(n+h\right)=\bar{e}_{n-1}\bar{b}\left(n+h-1\right)+...+\bar{e}_0\bar{b}\left(n\right)$$

Il en résulte qu'il existe une infinité de valeurs de n telles que $\bar{b}\left(n\right)$ soit non nulle ,puisque $\bar{e}_0$ n'est pas nul et que la suite $\bar{b}\left(n\right)$ est non identiquement nulle

Soit maintenant $r(n)$ la suite $\pi^{-1e_n}u\left(n\right)=b\left(n\right)+d\left(n\right)$ cette suite est pour n assez grand ,dans l'anneau de valuation de (K, W_H) et son image dans le corps résiduel $\bar{r}\left(n\right)$ est égal à $\bar{b}\left(n\right)$ .Elle est donc non nulle pour une infinité de valeurs de n.D'autre par puisque $u(n)$ est soit nule, soit appartient au sous-groupe de type fini de K^* il en est de même de $r(n)$,et donc aussi de son image $\bar{r}(n)$ dans le corps residuel.

Or d'aprés [11] le corps résiduel de (K, W_H) a un degré de transcendance strictement plus petit que celui de K qui est s.

On peut donc appliquer l'hypothése de récurrence à la suite $\bar{r}(n)$ il existe un entier d_0 non nul et des éléments a_r^*, b_r^* avec $r\in\{0,\ldots,d_0-1\}$ du corps residuel de (K, W_H) tels que pour tout k assez grand on ait :

$$\bar{r}(kd_0+r)=a_r^*\left(b_r^*\right)^k \qquad \text{pour} \quad r\in\{0,\ldots,d_0-1\}$$

Comme la suite $\bar{r}(n)$ a une infinité de termes non nuls, il existe au moins un indice r_0 tel que l'on ait $a_{r_0}^*$ et $b_{r_0}^*$ non nuls il en résulte que la valuation W_H- adique de $u(kd_0+r_0)$ est une fonction affine de k.

La suite $C(kd_0+r_0)$ est alors une suite récurrente toujours non nulle, et à valeurs dans IFp elle est périodique et on peut la supposer constante égale à C.

On a donc pour tout k assez grand :

$$\sum_{i=1}^{t}a_i\left(b_i\right)^{r_0}\left(b_i^{d_0}\right)^k-CH_1^{\lambda_1}...H_l^{\lambda_l}...H_m^{\lambda_m}\left(H_1^{\beta_1}...H_m^{\beta_m}\right)^k=0$$

Cette relation implique qu'il existe i_0 tel que l'on ait :

$$b_{i_0}^{d_0}=H_1^{\beta_1}...H_m^{\beta_m}$$

d'où la relation :

$$\sum_{i\neq i_0} a_i\,(b_i)^{r_0}\left(b_i^{d_0}\right)^k + \left(a_{i_0}\,(b_{i_0})^{r_0} - CH_1^{\lambda_1}...H_m^{\lambda_m}\right)\left(b_{i_0}^{d_0}\right)^k = 0$$

Comme tous les $b_i^{d_0}$sont distincts ,une telle relation n'est possible que s'il n'y a pas d'indice different de i_0 donc $t = 1$.

Ce qui achéve la démonstration du théorème. ■

Chapitre 3

Théorème de Skolem-Mahler -Lech pour les suites D-finie

3.1 Suite différentellement finie (D-finie):

Dans ce chapitre nous proposons d'étudier l'ensemble $I(u) = \{\ n \in \mathbb{N}\ /\ u(n) = 0\}$ pour u une suite différentellement finie donc c'est une généralisation du Théorème de Skolem-Mahler -Lech

Dans tout ce qui suit K est un corps commutatif de caractéristique nulle.

Définition 3.1.1 *Soit $F(x) = \sum\limits_{n \geq 0} a(n)\, x^n$ une série formelle à coefficients dans K ;on dit que la série F ,ou la suite $a(n)$ est différentiellement finie (en abrégé(D-finie)),si l'une des deux propriétés équivalentes suivantes est vérifiée:*

a) *F est solution d'une équation différentielle linéaire homogéne non triviale à coefficients dans $K[x]$.*

b)*La suite $a(n)$ vérifie une relation de récurrence linéaire homogéne non triviale à coefficients fonctions polynômes en la variable n .*

Définition 3.1.2 *Soit I un ensemble d'indices non vide et fini de cardinal $k+1$ et $u(n) = (u_i(n))_{i \in I}$ une suite d'éléments de $IP^k(K)$ avec $u_i(n)$ non nul pour tout i appartenant à I et tout n appartenant à $\mathbb{N}$.Soit J une partie non vide de I on dit que la partie J*

est irréductible pour l'entier n si les deux propriétés suivantes sont vérifiées:

i) $\sum\limits_{j \in J} u_j(n) = 0.$

ii) *Pour toute partie non vide A et propre de J on a $\sum\limits_{i \in A} u_i(n)$ non nul.*

Lemme 3.1.1 *[9]*

Soit I un ensemble d'indices non vide et fini de cardinal $k+1$ et $u(n) = (u_i(n))_{i \in I}$ une suite d'éléments de $IP^k(K)$ on suppose que $u_i(n)$ est non nul pour tout i et tout n et que $\sum\limits_{i \in I} u_i(n) = 0$ pour tout n dans $\mathbb{N}$.

Alors il existe une partition $I_1, ..., I_t$ de I et une partie infinie E de $\mathbb{N}$ telle que pour tout n dans E et tout j avec $1 \leq j \leq t$ et le I_j soit irréductible pour tout n.

Lemme 3.1.2 *[26]*

i) *Toute combinaison linéaire à coefficients dans K de suite D-finies à valeurs dans K est une suite D-finie .*

ii) *Soit $u(n)$ une suite D-finie dans K alors la suite $n \longrightarrow u(n+1)$ est aussi D-finie.*

Lemme 3.1.3 *[9]*

Soit $\sum\limits_{n \geq 0} a(n) x^n$ une série formelle algébrique à coefficients dans K alors la suite $a(n)$ est D-finie.

Lemme 3.1.4 *[6]*

Soit K une extension de type fini de $\mathbb{Q}$, soit Γ un sous groupe de type fini du groupe multiplicatif de K ,le sous-groupe Γ_0 défini par:

$$\Gamma_0 = \{ z \in K \ ; \ \exists \ n \ \in \mathbb{N}^*, z^n \in \Gamma \}$$

et aussi de type fini.

Théorème 3.1.1 *Soit G un sous-groupe de type fini du groupe multiplicatif de K et $S(x) = \sum\limits_{n \geq 0} u(n) x^n$ une série formelle à coefficients dans K on suppose que:*

i) S est D-finie.

ii) Il existe un entier m supérieur ou égal à un et des suites $c_j(n)$,$j = 1, 2, ..., m$ d'éléments de $G \cup \{0\}$ telles que l'on ait:

$$u(n) = \sum_{j=1}^{m} c_j(n) \qquad \textit{pour tout } n \in \mathbb{N}$$

Alors la série S représente la série de Taylor à lorigine d'une fraction rationnelle,qui si elle n'est pas un polynôme, n'a que des pôles simples.

Preuve.

Soit la suite $u(n)$ D-finie alors il existe un entier non nul k et des polynômes non tous nuls A_i dans $K[x]$ tels que l'on ait :

$$\sum_{i=0}^{k} A_i(n)\ \ u(n+i) = 0 \qquad\qquad \forall n \in \mathbb{N} \tag{3.1.1}$$

On peut supposer que les polynômes A_i sont premiers entre eux et que A_k est un polynôme non nul .comme on peut supposer sans restreindre la généralité que K est de type fini sur $\mathbb{Q}$.

On définit la suite $v(n)$ par la relation :

$$v(n) = \sum_{i=0}^{k} A_i(0)\ \ u(n+i) \tag{3.1.2}$$

Comme les polynômes A_i sont premiers entre eux l'un au moins des A_i est non nul donc si $v(n) = 0$ pour n assez grand on obtient une relation de récurrence linéaire non triviale pour la suite $u(n)$ à coefficients constants d'aprés les propriétés algébriques des suites récurrentes linéaires la série $\sum\limits_{n\geq 0} u(n)\, x^n$ est le développement de Taylor à lorigine d'une fraction rationnelle.

Donc pour démontrer le théorème nous prouvons que la suite $v(n)$ est nul pour n assez grand .

D'aprés i) du lemme *3.1.2* la suite $v(n)$ est une suite D-finie il existe alors un entier q non nul et des polynômes non tous nuls $B_j(x) \in K[x]$, $0 \leq j \leq q$.

tels que l'on ait

$$\sum_{j=0}^{q} B_j(n)\ \ v(n+j) = 0 \qquad\qquad \forall n \in \mathbb{N}$$

On peut supposer que $B_q(x)$ non identiquement nul .

Soit G le groupe multiplicatif de K donné dans les hypothéses du théorème .

On note H le sous-groupe du groupe multiplicatif de K défini par :

$$H = \{t \in K \ / \ \exists \ n \geq 1, t^n \in G\}$$

comme K est de type fini sur $\mathbb{Q}$, H est de type fini d'aprés le lemme 3.1.4 .

Soit b un entier non nul ,qui n'appartient pas à H.

Soit la partie Ω de $\mathbb{N}$ définit par

$$\Omega = \left\{ b^k + c \quad \text{avec} \quad k \in \mathbb{N} \text{ et } c \in \{0, ..., q-1\} \right\}$$

Nous allons démontrer que $v(n)$ est nulle pour tout élément n de Ω assez grand ce qui nous suffira pour démontrer que $v(n)$ est nulle pour n assez grand , n appartenant à $\mathbb{N}$.

Soit N un entier tel que pour tout x plus grand que N on ait $B_q(x)$ non nul .

Soit k_0 un entier tel que b^{k_0} soit strictement plus grand que N.et que $v(n)$ soit nulle pour tout n de Ω plus grand que b^{k_0}on a alors

$$v\left(b^{k_0} + c\right) = 0 \qquad \text{pour } c \in \{0, ..., q-1\} \quad \text{et } B_q\left(b^{k_0} + c\right) \neq 0$$

par récurrence on peut montrer qu'on a :

$$v\left(b^{k_0} + m\right) = 0 \qquad \forall m \in \mathbb{N}$$

Il nous reste à démonter que $v(n)$ est nulle pour tout élémentt n de Ω assez grand

Nous allons raisonner par l'absurde .

Soit $\Gamma = \{ \, n \in \Omega \, / \, v(n) \neq 0 \, \}$

Supposons que Γ est infini nons montrons qu'il existe une partie infinie Σ de Γ telle que $v(n) = 0$ pour tout n dans Σ.

D'aprés l'hypothèse ii) du théorème et la relation (3.1.1) on a pour tout n entier naturel assez grand dans Γ on a la relation :

$$\sum_{i=0}^{k} A_i(n) \sum_{j=1}^{m} c_j(n+i) = 0 \tag{3.1.3}$$

quitte à extraire une sous-suite de Γ , on peut écrire les éléments de Ω sous la forme $b^k + c$ où k appatient à une partie E infinie de $\mathbb{N}$ et c un élément fixe $c \in \{0, 1, ..., q-1\}$

Posons

$$A_i(x+c) = \sum m_{i,t} x^t \qquad \text{pour } i \in \{0, ..., k\} \quad \text{et} \quad m_{i,t} \in K$$

Nous voulons démontrer que l'on a

$$\sum_{i=0}^{n} A_i(x+c)\, u\left(b^k + c + i\right) = 0 \quad \text{pour} \quad k \in E_2.$$

avec E_2 est une partie infinie de E .

La suite $u(n)$ est D-finie pour tout n dans $\mathbb{N}$, en particulier pour n dans l'ensemble Γ . On a alors

$$\begin{aligned}\sum_{i=0}^{k} A_i\left(b^k+c\right)u\left(b^k+c+i\right) &= 0 \Longrightarrow \sum_{i=0}^{k} A_i(x+c)\sum_{j=1}^{m} c_j\left(b^k+c+i\right)=0\\ &\Longrightarrow \quad \sum_{i=0}^{k}\left(\sum_t m_{i,t}b^{kt}\right)\sum_{j=1}^{m} c_j\left(b^k+c+i\right)=0\\ &\Longrightarrow \quad \sum_{(i,j,t)} m_{i,t}b^{kt}c_j\left(b^k+c+i\right)=0\end{aligned}$$

on note

$$g_{i,j,t}=m_{i,t}b^{kt}c_j\left(b^k+c+i\right)$$

la relation (3.1.3) devient:

$$\sum g_{i,j,t}=0$$

pour k dans E,et la sommation se fait sur les indices (i,j,t) tels que $m_{i,t}$ soit non nul .Soit U l'ensemble de ces indices .

les $c_j(n)$ sont soit dans le groupe G , soit nuls .on peut définir deux parties de U dépendantes de k la partie formée des indices (i,j,t) dans U tels que le terme $g_{i,j,t}$ soit nul et son complémentaire.

Prenons une partie infinie E_1 de E telle que l'ensemble des ces indices (i,j,t) vérifiant $g_{i,j,t}$ non nul .

soit une partie fixe de U que le notons L.

Si L est vide

$\forall(i,j,t)\in U$ le terme $g_{i,j,t}=0$ par conséquent on aura trivialement

$$\sum_{i=0}^{k} A_i(x+c)\,u\left(b^k+c+i\right)=0$$

Supposons alors dans se qui suit que L est non vide .

Soit R le sous groupe de K^*engendré par G , b et tous les $m_{i,t}$ non nuls .

R est un sous groupe de type fini de K^*, d'aprés le lemme 3.1.1 on peut trouver une partition $L_1,...,L_l$ de l'ensemble L, et une partie E_2de E_1 telle que pour tout $d\in\{1,...,l\}$ et tout k dans E_2 ;L_l soit irréductible pour k , fixons un entier d.

pour un indice (i,j,t) dans L on désigne le couple (i,j) par la premiere composante et t la deuxième composante.

Soient $s = (i,j,t)$ et $s' = (i',j',t')$ deux éléments distincts de L_l,Nous utilisons le théorème 2.1.2 du chapitre 2 donc il existe un élément $\lambda \in K^*$ et une infinité de valeurs k dans E_2 tels que l'on a:

$$\begin{aligned} g_{i,j,t} &= \lambda g_{i',j',t'} \Longrightarrow m_{i,t} b^{kt} c_j \left(b^k + c + i\right) = m_{i',t'} b^{k't'} c_j \left(b^{k'} + c + i'\right) \\ &\Longrightarrow b^{k(t-t')} = \frac{\lambda m_{i',t'} b^{k't'} c_j \left(b^{k'} + c + i'\right)}{m_{i,t} b^{kt} c_j \left(b^k + c + i\right)} \in G \end{aligned}$$

l'image de $b^{t-t'}$dans le groupe K^*/G comme $b \notin H$, alors on déduit que $t = t'$ par conséquence la deuxiéme composante est constante pour tout élément L_l donc tout élément L_l est de la forme $L_l' \times \{t\}$.

Alors on a la relation suivante:

$$\sum g_{i,j,t} = 0 \qquad\qquad \text{pour } k \in E_2$$

La sommation étant faite sur les indices $s = (i,j,t)$ dans L_l on a t constant pour les indices de L_l donc on peut simplifier cette egalité par b^{kt} par conséquence on aura

$$\sum m_{i,t} c_j \left(b^k + c + i\right) = 0 \quad \text{avec } k \in E_2$$

la sommation est sur les indice s

Or $\sum_{(i,j) \in L_d'} m_{i,t} c_j \left(b^k + c + i\right)$ est le coefficient de x^t dans le polynôme
$Q(x) = \sum_{(i,j) \in L_d'} A(x+c) c_j \left(b^t + c + i\right)$ en réunissant ces relations pour les indices l tels que $L_l = L_l' \times \{t\}$ on aura

$$\sum_{i=0}^{k} A_i (x+c) u \left(b^k + c + i\right) = 0 \quad \text{avec } k \in E_2 \text{ et } \forall t$$

.

En prenant $x = -c$ par conséquent on aura $\sum_{i=0}^{k} A_i(0) u \left(b^k + c + i\right)$ donc $v(n) = 0$ pour $n = b^k + c$ et $k \in E_2$.

par conséquent on trouve une partie C de Γ tel que

$$C = \left\{ \quad n = b^k + c \quad , k \in E_2 \ \text{ tel que } v(n) = 0 \quad \right\}$$

$v(n) = 0$ pour $n \in C$ ce qui donne une contradiction car tout élément de C doit vérifier $v(n)$ non nul puisque C est une partie de l'ensemble Γ .donc Γ est une partie finie.

comme $\Omega = \Gamma \cup \Gamma^c$ avec Γ finie ,on déduit que $\Gamma^c = \{ n \in \Omega \; / \; v(n) = 0 \}$ est infinie doncc por tout n assez grand dans Ω on $v(n) = 0$.

Montrons que $S(x)$ posséde des pôles simples s'il n'est pas un polynôme ,d'aprés les propriétés algébriques d'une suite récurrente linéaire à coefficients constantes

$$u(n) = \sum_{j=1}^{k} P_j(n) \alpha_j^n$$

avec α_j sont algèbrique sur le corps K et meme les coefficients des polynômes de P_j.

On peut supposer que K contient tous les α_j pour $j = \overline{1,t}$ et les polynômes $P_j \in K[x]$.

Posons $\alpha'_j = 1/ \alpha_j$, donc α'_j sont des pôles de S .

Pour démontrer que les pôles sont simples il suffit donc de montrer que les polynômes P_j sont constants pour tout j.et comme oa le degrédes polynôme est $\tau_j - 1$ avec τ_j est la multiplicité des pôles de $S(x)$.

dire que la fraction rationnelle $S(x)$ posséde des pôles simples c'est dire que $\tau_j = 1 \; \forall i$ et donc les polynôme P_j sot des polynôme constants.

posons $v(n) = \sum\limits_{j=1}^{k} P_j(0) \alpha_j^n$ la suite $v(n\ )$ est une suite D-finie il en est de même pour la suite:

$$\begin{aligned} c(n) &= u(n) - v(n) \\ &= \sum_{j=1}^{k} (P_j(n) - P_j(0)) \alpha_j^n \end{aligned}$$

Alors on a la relation

$$\sum_{j=1}^{k} P_j(n) \alpha_j^n - \sum_{j=1}^{m} c_j(n) = 0 \qquad \text{pour tout } n \text{ assez grand}$$

On peut donc trouver un ensemble A de la forme:

$$A = \left\{ n \in \mathbb{N} \; / \; n = b^k + c \quad \text{avec } k \in \mathbb{N}, c \in \{0, ..., q\} \right\}$$

Pour tout n assez grand de lensemble A on a la relation :

$$\sum_{j=1}^{k} P_j(0) \alpha_j^n - \sum_{j=1}^{m} c_j(n) = 0$$

$$u(n) = \sum_{j=1}^{m} c_j(n)$$

Or on a

$$c(n) = 0 \qquad \text{pour tout } n \text{ assez grand de l'ensemble } A$$

Si l'on a choisit convenablement q il en résulte que $c(n) = 0$ pour n assez grand donc

$$u(n) = \sum_{j=1}^{k} P_j(0)\,\alpha_j^n \qquad \text{pour } n \text{ assez grand}$$

l'unicité de l'écriture montre que $P_j(x) = P_j(0)$ pour tout j et donc le polynôme P_j est constant et alors les pôles de S sont des pôles simples ce qui achève la démonstration du théorème. ∎

Théorème 3.1.2 *Soit $S(x) = \sum_{n\geq 0} u(n)\,x^n$ une série formelle algebrique à coefficients dans K tous non nuls on suppose que l'inverse au sens de Hadamard de S est encore une série algébrique*
Alors S est une fraction rationnelle.

Preuve.
On peut supposer que K est une extension de type fini sur $\mathbb{Q}$.

Soient $\alpha_1, ..., \alpha_r$ des éléments algèbriquements indépendants sur $\mathbb{Q}$ et θ un élément primitif de K donc on a: $K = \mathbb{Q}(\alpha_1, ..., \alpha_r)(\theta)$.

il existe un polynôme non nul $H \in \mathbb{Z}[x_1, ..., x_r]$ et des polynômes P_n, Q_n dans $\mathbb{Z}[x_1, ..., x_r, Y]$ tels que l'on ait pour tout $n \in \mathbb{N}$.

$$\begin{aligned} H(x_1, ..., x_r)^{n+1}\,u(n) &= P_n(x_1, ..., x_r,\ \theta) \text{ et} \\ H(x_1, ..., x_r)^{n+1}\,\frac{1}{u(n)} &= Q_n(x_1, ..., x_r, \theta) \end{aligned}$$

Soit R l'anneau $\mathbb{Z}\left[x_1, ..., x_r, \theta, \dfrac{1}{H(x_1, ..., x_r)}\right]$ .R est de type fini sur $\mathbb{Z}$ on a $u(n)$ est un élément inversible de l'anneau R pour tout n.

Comme l'ensemble R^* des éléments inversibles de R est un groupe de type fini .donc on peut appliquer le théorème 3.1.1 et on a donc la démonstration de ce théorème. ∎

3.2 Une généralisation du Théorème de Skolem-Mahler -Lech (de Bézivin)

Définition 3.2.1 *On dit qu'une partie E de $\mathbb{N}$ a une densité arithmétique égale à α si:*

$$\lim_{x \to +\infty} \frac{card\,(E \cap [0, x[)}{x} = \alpha$$

La densité arithmétique supérieure est définie par la limite supérieure dans cette formule.

Définition 3.2.2 *Soit M un espace topologique ,etant donné un point de M sur l'ensemble $E\,(p)$ défini par:*

$$E\,(p) = \{(U, f)\ \ /\ U \text{ est un voisinage ouvert de } p \text{ et } f \in C^{\infty}\}$$

on introduit la relation binaire

$$(U, f)\,\Re\,(U', f') \Leftrightarrow \exists U'' \text{ un voisinage de } p \text{ et } U'' \subset U \cap U' \text{ tel que } f_{|U''} = f'_{|U''}$$

Les élements du quotient $E\,(p)\,/\Re$ sont appelés germes au point p.

Lemme 3.2.1 *Soit $a\,(n)$ une suite d'éléments de K on suppose que cette suite vérifie une relation de récurrence linéaire à coefficients polynômes en la variable n de longueur h .*
Soit d un entier naturel non nul et r un entier naturel quelconque Alors la suite
$b\,(k) = a\,(kd + r)$ vérifie une relation de récurrence linéaire à coefficients polynômes en la variable n de longueur au plus h.

Preuve.

Soit R l'ensemble des germes à l'infini de suite de la forme $P\,(n)\,/Q\,(n)\ \ n \in \mathbb{N}$ où P et Q sont des polynômes à coefficients dans K avec Q non nul. Pour éviter les difficultés dues aux zéros éventuels appartenant à $\mathbb{N}$ du polynôme Q nous utilisons les germes à l'infini .
R est un corps isomorphe au corps des fractions rationnelles en la variable $x \in K$.
Soit Ω l'ensemble des germes à l'infini des suites d'éléments de K l'ensemble Ω est un espace vectoriel sur le corps R pour les opérations usuelles sur les suites ,le sous-espace vectoriel Σ de Ω engendré par les suites $a\,(n + j)$ avec $j \in \mathbb{N}$ est un sous-espace vectoriel de dimension

finie inférieure ou égale à h de plus Σ est engendré par les suites $a\left(n+j\right)$, $j=0,...,h-1$ soit s un élément de $\mathbb{N}$ il existe donc des $F_{t,i}$ $i=0,...,h-1$éléments de R tels que l'on ait :

$$a\left(n+t\right)=\sum F_{t,i}\left(n\right)a\left(n+i\right) \tag{3.2.1}$$

l'egalité ayant lieu dans Ω .

En prenant $n=sd$ et $t=jd+r$, $j=0,...,h$ dans (3.2.1) on montre que les suites $b\left(s+h\right)=a\left(sd+jd+r\right)$ appartiennent toutes à l'espace vectoriel engengré par les suites $a\left(sd+i\right),i=0,...,h-1$.Par conséquent il existe une relation entre ces suites $b\left(s+j\right)$ $j=0,...,h$ on en déduit une relation de récurrence linéaire à coefficients polynômes en la variable n pour la suite $b\left(n\right)$ de longueur au plus h ce qui démontre le lemme. ■

Définition 3.2.3 *Soit U un ouvert de $\mathbb{C}$,et soit l'équation différentielle :*

$$a_m y^{(m)}+a_{m-1}y^{(m-1)}+...+a_1 y'+a_0 y=0 \tag{3.2.2}$$

tout point $x\in U$ tel que $a_m\left(x\right)\neq 0$ est un point régulier de (3.2.2) et tout point $x\in U$ tel que $a_m\left(x\right)=0$ est un point singulier de (3.2.2) .

Il y a deux types de points singuliers:

i) les points singuliers réguliers:

Soit $x_0\in U$ tel que $a_m\left(x_0\right)=0$ on normalise l'équation (3.2.2) :

$$y^{(m)}+\frac{a_{m-1}}{a_m}y^{(m-1)}+...+\frac{a_1}{a_m}y'+\frac{a_0}{a_m}y=0 \tag{3.2.3}$$

L'équation (3.2.3) devient

$$y^{(m)}+b_{m-1}y^{(m-1)}+...+b_1 y'+b_0 y=0 \tag{3.2.4}$$

Ou $b_i=\dfrac{a_i}{a_m}$ $i\in\{0,...,m-1\}$.

Si b_{m-1} posséde au plus un pôle d'ordre 1 en x_0

.b_{m-2} posséde au plus un pôle d'ordre 2 en x_0

$\vdots$

b_{m-i} posséde au plus un pôle d'ordre i en x_0

avec $i=\overline{1,m}$.

on dit que x_0 est un point singulier régulier.

On obtient un résultat analogue au théorème de Skolem-Mahler -Lech qui est le théorème suivant :

Théorème 3.2.1 *Soit* $F(x) = \sum u(n)\, x^n$ *une série formelle à coefficients dans* K *,On suppose que* F *vérifie une equation différentielle* E *,linéaire homogéne à coefficients dans* $K[x]$ *telle que zero et le point à l'infini ne soient pas singuliers-irréguliers pour* E *il existe alors un entier naturel* d *non nul tel que pour tout* $r \in \{0, ..., d-1\}$ *on ait l'alternative suivante:*
i) *la suite* $u(kd+r)$ *est nulle à partir d'un certain rang.*
ii) *la densité arithmétique de l'ensemble*

$$\Omega_r = \{\ k \quad /\ u(kd+r) = 0\} \qquad \textit{est nulle}$$

Preuve.
Nous allons tout d'abord démontrer le théorème dans le cas où le corps de base est $\mathbb{C}$ puis nous traiterons le cas général d'un corps commutatif de caractéristique nulle quelconque.
i) Le corps de base est $\mathbb{C}$:
Comme le zéro n'est pas un point singulier-irrégulier pour l'equation différentielle alors la solution série formelle $F(x) = \sum u(n)\, x^n$ est une série entiere de rayon de convergence non nul.
Soit I l'ensemble de singularités dans $\mathbb{C}$ du germe de fonction analytique à l'origine .
Cet ensemble est fini .Nous définissons l'entier d comme étant le plus petit commun multiple des ordres des quotients de deux éléments dans I qui sont des racines de l'unité.

dans le cas où aucun de ces quotients n'est une racine de l'unité on prend $d = 1$.

Soit la fonction F_r , $r = \overline{0, d}$ définie par la relation

$$x^r F_r\left(x^d\right) = \sum F(\zeta x)\, \zeta^{-r} \tag{3.2.5}$$

la somation étant faite sur les racine $d - i\grave{e}me$ de l'unité.

les fonctions F_r sont analytiques au voisinage de l'origine et le developpement de Taylor à l'origine de F_r est

$$F_r(x) = d \sum u(kd+r)\, x^k \tag{3.2.6}$$

examinons les deux cas ;

a) Le cas ou les indices $r \in \{0, ..., d-1\}$ tel que la fonction F_r n'est aucune singularité à distance finie.

dans ce cas la fonction $F_r$est analytique dans tout $\mathbb{C}$;

Soit $\{A_1, ..., A_t\}$ un ensemble fini de points de $\mathbb{C}\setminus\{0\}$ contenant les singularités de l'équation différentielle E (sauf zero) et qui soit stable par toutes les applications ζx où ζ parcourt les racines $d-i\grave{e}me$ de l'unité .

On note B l'ouvert simplement connexe obtenu en enlevant de $\mathbb{C}$ les demi-droites $B_i = \{ zA_i \ / \ z \in \mathbb{R}\}$ avec $i = \overline{1,t}$ le germe $F(x)$ se prolonge dans B en une fonction analytique vérifiant encore E que nous notons encore F.

la fonction $F(x)$ a une criossance modérée quand x tend vers l'infini dans B_i d'aprés le théorème 3.2.1 , l'infini n'est pas singulier-irrégulier pour E par conséquent de la relation (3.2.5) il existe deux constantes $a_1$et a_2 telle que on ait

$$\left|F_r\left(x^d\right)\right| \leq a_1 |x|^{a_2}$$

pour x dans B et $|x|$ assez grand

donc F_r est analytique dans tout $\mathbb{C}$ il en resulte que F_r est un polynôme et montre que la suite $u(kd+r)$ est nulle a partir d'un certain rang.

b) Supposons que la fonction F_r posséde au moins une singularité à distance finie dans ce cas il nous faut démontrer que l'ensemble $\Omega_r = \{ k \ / \ u(kd+r) = 0\}$ est de densité arithmétique nulle.

Nous allons raisonner par l'absurde donc supposons que la densité arithmétique supérieure de l'ensemble Ω_r est non nulle .

D'aprés le théorème de **szemerdi** il existe une infinité de progressions arithmètiques de longueur s dans Ω_r et de même raison m par conséquent il existe un entier λ de l'ensemble $\{0, ..., m-1\}$ tel que l'on ait

$$km + \lambda \in \Omega_r$$

avec k appartenant à une infinité d'intervalles de longueur s .

On note $w(k) = v(km+\lambda)$ .la suite $w(k)$ est une suite récurrente linéaire à coefficients polynômes en la variable k (d'aprés le lemme 3.2.1 .).

pour les valeurs de k dans les intervalles déterminés précédément ;il en résulte que la suite $w(k)$ est nulle par conséquent la suite $w(k)$ est nulle à partir d'un certain rang.

donc la série

$$\sum v(km+h)\, x^k \qquad \text{est un polynôme}$$

D'où

$$\sum F_r(\zeta x)\, \zeta^{-1} \qquad \text{est un polynôme en } x$$

où ζ parcourt l'ensemble des racines $m - ième$ de l'unité.

On a si s est une singularité à distance finie de F_r il existe une autre singularité de F_r ,s' telle que $s \;/\; s'$ soit une racine $m - ième$ de l'unité.

Consédérons l'ensemble S' des singularités à distance finie de F_r est inclus dans l'ensemble formé des puissances $d - ième$ des éléments de S des singularités de la fonction F.

Soit b un point de $\mathbb{C}\setminus\{0\}$ qui ne soit pas de la forme s^d où s est une singularité non nulle de F.

Soit μ une racine $d - ième$ de v ,et H un ouvert simplement connexe contenant zéro et v qui est stable par toutes les applications λx où λ parcourt les racines $d - ième$ de l'unité et ne contenant aucune des singularités de F .

le germe $F(x)$ se prolonge à l'ouvert H en une fonction analytique que nous notons encore F.

D'aprés l'égalité (3.2.5) la fonction $F_r\left(x^d\right)$ se prolonge en une fonction analytique dans l'ouvert R image de l'ouvert H par l'application x^d qui est un ouvert connexe contenant zero et b.et donc b n'est pas une singularité de $F_r(x)$.

On a aucun des quotient s_1/s_2 avec $s_1$et s_2 dans S ne peut être une racine de l'unité autre que un.

et donc on a une contradiction , ce qui démontre le théorème dans le cas complexe .

ii) le cas d'un corps de caractéristique zéro :

Soit L le corps de type fini sur $\mathbb{Q}$ contenant tous les coefficients des polynôme qui intervienant dans l'équation E' .Ainsi que tous les coefficients $u(n)$ de la série formelle $F(x)$.

L est un corps isomorphe a un sous corps de $\mathbb{C}$, soit alors E' l'équation différentielle transformée de E par cet isomorphisme.

E' vérifie encore les conditions du théorème ,à l'aide des conditions sur les degrés et les valuations z -adique des polynômes coefficients de E , la série formelle F' transformée de F par l'isomorphisme vérifie E' par conséquence l'ensemble des indices des coefficients nuls est le même pour F et F' ce qui achéve la démonstration du théorème. ■

Remarque 3.2.1 *Si on remplace la condition* ***ii)*** *du théorème de Bézivin par* $\Omega_r = \{ \ k \quad / \ u\,(kd + r) = 0\}$ *est un ensemble fini on trouve un resultat analogue du théorème de Skolem-Mahler -Lech.*

Chapitre 4

Une généralisation du théorème de Skolem-Mahler-lech sur une variété affine

4.1 La forme algebrique linéaire d'une suite récurrente linéaire:

Dans ce paragraphe nous prouvons que le théorème de Skolem-Mahler -Lech peut être reformulé sous la forme algebrique linéaire.

Définition 4.1.1 *Soit K un corps commutatif et soit $f(x) = \sum\limits_{n \geq 0} u(n)\, x^n$ une série à coéfficients dans K .*

f est reconnaissable sur K s'il existe une matrice carrée $M = (m_{ij})_{1 \leq i,j \leq k}$ à coefficients dans K un vecteur ligne $\alpha = (\alpha_i)_{1 \leq i \leq k}$ et un vecteur colonne $\beta = (\beta_j)_{1 \leq j \leq k}$ également à coefficients dans K tel que pour tout $n \in \mathbb{N}$ on a

$$u(n) = \alpha M^n \beta$$

le triplet (α, M, β) est une représentation de f , les $\alpha_i, \beta_i, m_{ij}$ sont les coefficients de cette représentation et k est la dimension .

Schützenberger a montré qu'une série est rationelle si et seulement si elle est reconnaissable.

Théorème 4.1.1 *[25]**Schützenberger***
Soit $f(x)$ est une série rationnelle dans K alors il existe une matrice inversible M et deux vecteurs de colonne v, w est un polynôme P tels que

$$f(x) = P(x) + \sum_{i=0}^{\infty} \left(v^T M^i w\right) x^i$$

réciproquement ,on se donne une matrice inversible M et deux vecteurs colonnes v, w est la série

$$g(x) = \sum_{i=0}^{\infty} \left(v^T M^i w\right) x^i$$

est rationnelle.

Théorème 4.1.2 *[4]* ***Skolem_ Mahler -Lech second version***
Soit $\sum_{n=0}^{\infty} u(n) x^n$ une série rationnelle sur un corps K de caractéristique zero ,alors l'ensemble des entiers m tels que $u(n) = 0$ est la réunion d'un nombre fini de progressions arithmétiques et d'un ensemble fini

Nous donnons une généralisation "algebro-géométrique de ce théorème

Théorème 4.1.3 *[4]*
Soit K un corps de caractéristique zero et soit $\varphi : K^n \longrightarrow K^n$ une application linéaire inversible .soient $v \in K^n, W$ un sous-espace de K^n de dimension un alors l'ensemble des entiers m tels que $\varphi^m(v) \in W$ est la réunion d'un nombre fini de progressions arithmétiques et d'un ensemble fini.

Nous montrons maintenant l'équivalence entre le théorème4.1.3 et le théorème de Skolem-Mahler -Lech

Preuve.

i)Le théorème 4.1.3 implique le théorème de Skolem-Mahler -Lech:

Soit K un corps de caractéristique zéro.

en fixant une base pour K^n, considérons un automorphisme linéaire φ de K^n donné par la multiplication par une matrice inversible M .

un sous-espace W de K^n de codimension un est de la forme $\{ x / \ v^t x = 0\}$ pour tout vecteur v .

On a l'ensemble des entiers m tels que $\varphi^m (w) \in W$ est exactement l'ensemble des entiers m tels que $v^t M^m w = 0$ par le théorème de Schützenberger on trouve le théorème de Skolem-Mahler -Lech.

ii) Le théorème de Skolem-Mahler -Lech implique le théorème 4.13 :
soit $f(x) = \sum_{n \geq 0} u(n) x^n$ d'aprés le théoreme de Schützenberger 4.1.1 il exite une matrice inversible M et deux vecteurs colonnes v, w tels que

$$f(x) = P(x) + \sum_{i=0}^{\infty} \left(v^T M^i w\right) x^i$$

avec P est un polynôme de degré n
pour $n_0 > n$ on a

$$f(x) = \sum_{i=0}^{\infty} \left(v^t M^i w\right) x^i$$

Soit φ une application linéaire inversible et W défini comme dans l'implication i) donc l'ensemble des indices n tel que $\varphi^n (w) \in W$ est exactement l'ensemble des indices n tel que $u(n)$ est nul et donc on trouve Le théorème 4.1.3 ■

4.2 La conjecture Jacobienne:

Dans ce paragraphe nous présentons un rapport actualisé sur les résultats les plus importants concernant la conjecture jacobienne .

Définition 4.2.1 ***1)*** *Une application de polynômes est une application*

$$\begin{array}{rcl} F & = & (F_1, ..., F_n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n \\ (x_1, ..., x_n) & \longmapsto & (F_1(x_1, ..., x_n), ..., F_n(x_1, ..., x_n)) \end{array}$$

tel que $F_i \in \mathbb{C}[x] := \mathbb{C}[x_1, ..., x_n] \qquad i = \overline{1, n}$
2) *Soit R un anneau unitaire,on définit l'automorphisme polynômial comme suit* $Aut\left(IA_R^n\right)$

l'ensemble des applications polynômiales inversibles $\sigma = (f_1, ..., f_n) \in (R[x_1, ..., x_n])^n$ *avec la proprieté* $\sigma^{-1}(g_1, ..., g_n)$ *pour* $g_1, ..., g_n \in R[x_1, ..., x_n]$ *un élément* $\sigma \in Aut(IA_R^n)$ *est appelé automorphisme de* IA_R^n.

Remarque 4.2.1 *:*

Lorsque R est un corps les automorphismes lineaire sont un cas spécial de ceci dans le quel nous insistans sur le fait que tous les polynôme impliqués en définissant les application sont homogénes du degré un i.e il sont des applications linéaires inversibles.

Définition 4.2.2 *La matrice jacobienne de* $F = (f_1, ..., f_p)$ *en* $U = (x_1, ..., x_n)$ *est la matrice (dans la base canonique) de la différentielle de* F *de* U *,toutes les dérivées partielles étant prises en* U *est :*

$$J(F, U) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ \frac{\partial f_p}{\partial x_1} & \frac{\partial f_p}{\partial x_2} & \cdots & \frac{\partial f_p}{\partial x_n} \end{pmatrix}$$

Théorème 4.2.1 *Soit* $F : IR^n \longrightarrow IR^m$ *de classe* C^1 *sur un ouvert* U *de* IR^n *et* $G : IR^m \longrightarrow IR^p$ *de classe* C^1 *sur ouvert de* IR^m *alors* $G \circ F$ *est de classe* C^1*sur* U *et*

$$J_{G \circ F} = J_G \times J_F$$

Preuve.

On appelle $(f_1, ..., f_m)$ et $(g_1, ..., g_p)$ les composantes de F et de G.On note $U = (x_1, ..., x_n)$

$$\begin{aligned} F(U) &= (y_1, ..., y_m) = (f_1(U), ...f_m(U)) \\ &= (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \end{aligned}$$

d'autre part on a

$$\begin{aligned} G \circ F(U) &= G(F(U)) \begin{pmatrix} g_1(y_1, ..., y_m) \\ . \\ . \\ . \\ g_p(y_1, ..., y_m) \end{pmatrix} \\ &= \begin{pmatrix} g_1(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \\ . \\ . \\ . \\ g_p(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \end{pmatrix} \\ &= \begin{pmatrix} h_1(x_1, ..., x_n) \\ . \\ . \\ . \\ h_p(x_1, ..., x_n) \end{pmatrix} \end{aligned}$$

Ces composantes sont de classe C^1 pour alléger les notations on ne précise plus en quels points on prend ces dérivées partielles .

En appliquand le théorème de dérivation des fonctions composées on a :

$$\begin{aligned} \frac{\partial h_i}{\partial x_j} &= \frac{\partial g_i}{\partial y_1}\frac{\partial f_1}{\partial x_j} + \frac{\partial g_i}{\partial y_2}\frac{\partial f_2}{\partial x_j} + ... + \frac{\partial g_i}{\partial y_m}\frac{\partial f_m}{\partial x_j} \\ &= \left(\frac{\partial g_i}{\partial y_1}, \frac{\partial g_i}{\partial y_2}, ..., \frac{\partial g_i}{\partial y_m}\right) \begin{pmatrix} \frac{\partial f_1}{\partial x_j} \\ \frac{\partial f_2}{\partial x_j} \\ . \\ . \\ . \\ \frac{\partial f_n}{\partial x_j} \end{pmatrix} \text{‘} \end{aligned}$$

On reconnait bien sur le produit de la $i^{éme}$ ligne de la matrice jacobienne de G par la $\mathrm{j}^{\mathrm{éme}}$ colonne de la matrice jacobienne de F ce qui est l'élément $i^{éme}$ ligne $j^{éme}$ colonne de la matrice jacobienne de $G \circ F$. ■

4.2.1 La conjecture Jacobienne :

Nous rappelons le resultat suivant:

Théorème 4.2.2 *Soit K un corps algebriquement clôs de caractéristique zero.soit F : $K^n \longrightarrow K^n$ une application de polynôme si F est injective alors F est surjective et son inverse est une aplication de polynôme (i.e F est un automorphisme de polynôme donc la conjecture jacobienne est équivalente à:*
si $F(a) = F(b)$ pour certain $a, b \in \mathbb{C}^*$ alors $a = b$.

La conjecture jacobienne s'appelle aussi le problème de **O.KELLER.**

Proposition 4.2.1 *Si le degré du polynôme F est inférieur ou égal à deux alors la conjecture jacobienne est vraie.*

Preuve.
D'aprés le théorème 4.2.2 il suffit de montrer que F est injective .
on suppose que $F(a) = F(b)$ pour $a, b \in \mathbb{C}^n$ et $a \neq b$ .On définit

$$G(x) = F(x+a) - F(a)$$

donc G est un polynôme de degré inférieur ou égal à deux et $G(0) = 0$.
On pose $c = b - a$ ona $c \neq 0$ (car $a \neq b$) et $G(c) = 0$.

remarquons que $J(G(x)) = J(x+a)$ donc $J(G) \in \mathbb{C}^*$.

on écrit $G = G_{(1)} + G_{(2)}$ la décomposition en composantes homogènes

on considére

$$G(tc) = tG_{(1)}(c) + t^2 G_{(2)}(c)$$

on trouve

$$\begin{aligned} JG(tc) &= \frac{d}{dt} G(tc) \\ &= G_{(1)}(c) + 2tG_{(2)}(c) \\ &= cJ(G(tc)) \neq 0 \qquad\qquad (\text{car } JG \in \mathbb{C}^*) \end{aligned}$$

$\forall\ t \in \mathbb{C}$ comme $c \neq 0$ et $\det(JG) \in \mathbb{C}^*$ pour $t = \frac{1}{2} \Rightarrow G(c) \neq 0.$

contradiction avec $G(c) = 0$

donc F est injective. ■

Nous donnons les définitions necessaires

4.3 Espace affine projectif variété algebrique :

4.3.1 Espaces algébriques affines :

Définition 4.3.1 *Un n-espace affine est l'ensemble des n-uples* $(a_1, ..., a_n)$ *d'éléments* a_i *d'un corps K :*

$$IA^n(K) = \{a = (a_1, ..., a_n), a_i \in K\}$$

L'élément $a = (a_1, ..., a_n)$ *est un point de l'espace* $IA^n(K)$ *à n coordonnées.*

Définition 4.3.2 *Un ensemble algébrique d'un n-espace affine* $IA^n(K)$ *est l'ensemble H des zéros d'une famille de polynômes* $\{f_1 \ldots, f_d\}$ *de l'anneau* $K[X_1, ...X_n]$.

$$H = \{a = (a_1, ..., a_n); f_1(a) = f_2(a) = ... = f_d(a) = 0\} = H(f_1, ..., f_d)$$

Les ensembles algébriques permettent de déterminer une topologie spécifique.

4.4 Topologie de Zariski:

Définition 4.4.1 *La topologie de **Zariski** sur le n-espace affine* $IA^n(K)$ *est définie avec les ensembles algébriques comme sous ensembles fermés et leurs complémentaires comme des ouverts.*

Donc l'espace affine est un espace topologique avec la topologie de Zariski.

Définition 4.4.2 *Une variété algébrique affine est un sous espace irréductible et fermé d'un espace affine* $IA^n(K)$.

4.5 Plongement dans $\mathbb{Z}_p$:

Lemme 4.5.1 *Soit K une extension de type fini de $\mathbb{Q}$ et soit S un sous ensemble fini de K alors il existe un nombre premier p tel que K plonge dans $\mathbb{Q}_p$ tel que pour chaque élément de S on peut l'associé un élément de $\mathbb{Z}_p$.*

Preuve. voir [4] ■

4.6 Le théorème de Skolem-Mahler-lech sur une variété affine

Lemme 4.6.1 *Soit $\sigma = (F_1, ..., F_n) : IA^n_{\mathbb{Z}_p} \longrightarrow IA^n_{\mathbb{Z}_p}$ une application de polynomes surjectives tel que $F_1, ..., F_n \in \mathbb{Z}[x_1, ..., x_1]$ et qui a la propriété que son déterminant jacobien est une constante de norme p-adique égale a un alors il y a des entiers positifs j tels que $\sigma^j = (H_1, ..., H_n)$ a les deux propriétés suivantes :*
i) *$\sigma^j = (s_1, ..., s_n) = (s'_1, ..., s'_n)$ satisfait :*

$$s_i \equiv s'_i \bmod p \quad \text{pour } 1 \leq i \leq n \text{ et pour tout } (s_1, ..., s_n) \in \mathbb{Z}_p^n.$$

ii) *la jacobienne de $(H_1, ..., H_n)$ évaluée a $x_1 = s_1, ..., x_n = s_n$ est de la forme $I + pM$ pour une certaine matrice M avec des entiers dans $\mathbb{Z}_p$.*

Preuve.
Nous avons

$$\sigma(s_1, ..., s_n) = (F_1(s_1, ..., s_n), ..., F_n(s_1, ..., s_n))$$

avec $F_1, ..., F_n \in \mathbb{Z}[x_1, ..., x_1]$ comme les F_i ont des coéfficients dans $\mathbb{Z}_p$ donc nous avons

$$\sigma(s_1, ..., s_n) = (r_1, ...r_n) \quad \text{pour } r_1, ..., r_n \text{ dans } \mathbb{Z}_p$$

autrement dit

$$(r_1, ..., r_n) = \sigma(s_1, ..., s_n) \quad \text{et} \quad (r'_1, ..., r'_n) = \sigma(s'_1, ..., s'_n)$$

et

$$\begin{aligned} s_i &\equiv s_i' \,(\mathrm{mod}\, p\mathbb{Z}_p) \text{ pour } 1 \leq i \leq n \text{ alors} \\ r_i &\equiv r_i' \,(\mathrm{mod}\, p\mathbb{Z}_p) \text{ pour } 1 \leq i \leq n \end{aligned}$$

par conséquent il existe deux entiers l et k ,$k > l > 0$ tel que $\sigma^k(s_1, ..., s_n)$ et $\sigma^l(s_1, ..., s_n)$ ont les même cordonneés $\mathrm{mod}\, p$ pour chaque $(s_1, ..., s_n) \in \mathbb{Z}_p^n$. comme σ est surjective nous avons $\tau = \sigma^{k-l}$ a la propriétés que si $\tau(s_1, ..., s_n) = (s_1', ..., s_n')$ alors $s_1' \equiv s_1, ..., s_n' \equiv s_n \,(\mathrm{mod}\, p)$ .par conséquent n'importe qu'elle puissance de τ à cette propriété on note $J(\mu, s)$ le jacobien de l'application polynômiale μ à le point $s \in IA^n_{\mathbb{Z}_p}$.On note m l'ordre de $GLn(IF_p)$ alors $\forall s = (s_1, ..., s_n) \in IA^n_{\mathbb{Z}_p}$ on a d'aprés le théorème 4.2.1 :

$$\begin{aligned} J(\tau^m, s) &\equiv J\left(\tau, \tau^{m-1}(s)\right) J\left(\tau, \tau^{m-2}(s)\right) ... J(\tau, s) \\ &\equiv (J(\tau, s))^m \equiv I_n \,(\mathrm{mod}\, p\mathbb{Z}_p) \end{aligned}$$

et ona donc la démonstration du lemme. ■

Lemme 4.6.2 *[4]* ***p-adic analytic arc lemma***

Soient $\mu_1, ..., \mu_n$ des éléments de $\mathbb{Z}_p$ et $H_1, ..., H_n$ des polyn̂mes dans $\mathbb{Z}_p[x_1, ..., x_n]$ qui satisfont :

i) *$H_i(\mu_1, ..., \mu_n) \equiv \mu_i \,(\mathrm{mod}\, p)$ pour $i \in \{1, ..., n\}$.*

ii) *$\sigma(H_1, ..., H_n) : IA^n_{\mathbb{Z}_p} \longrightarrow IA^n_{\mathbb{Z}_p}$ est une application surjective avec son déterminant jacobien est une constante dans $\mathbb{Z}_p$ de norme égale à un .*

iii) *$J(H_1, ..., H_n)$ valué en $x_1 = \mu_1, ..., x_n = \mu_n$ est égle à $I_n + pM$ avec M une matrice ces éléments sont entiers dans $\mathbb{Z}_p$*

Alors :

il existe des séries entieres $f_1, ...f_n$ dans $\mathbb{Q}_p[[x]]$ qui converge dans la boule unité fermeé de $\mathbb{Q}_p$ et qui satisfait:

a) $f_i(x+1) = H_i(f_1(x), ..., f_n(x))$ pour $i = \overline{1, n}$

b) $f_i(0) = \mu_i$ pour $i = \overline{1, n}$

Théorème 4.6.1 [?]De Strassman

Soit $(K, |\ |)$ un corps valué et R son anneau de valuation et soit f une série entiere à *coefficients dans R on suppose qu'au moins un des coefficients est non nul (de sorte que f ne soit pas identiquement nul) et l'ordre des coefficients converge à 0 réspictivement à $|\ |$ alors f à seulement un nombre finie de zéros dans R.*

Théorème 4.6.2 *Soit K un corps de caractéristique zéro soit λ un point dans IA_K^n et soit σ un automorphisme de K^n,Si X est une sous variété de IA_K^n alors l'ensemble $\{m \in \mathbb{Z} \ / \ \sigma^m(\lambda) \in X\}$ est une réunion d'un ensemble fini de de progressions arithmétiques compléte et d'un ensemble fini.*

Preuve.

Nous regardons l'orbite d'un point $\lambda = (\lambda_1, ..., \lambda_n)$ par σ.

On écrit $\sigma = (H_1, ..., H_n)$ et $\sigma^{-1} = (G_1, ..., G_n)$ avec H_i et $G_i \in K[x_1, ..., x_n]$ pour $i \in \{1, ..., n\}$.

On choisit les polynômes $F_1, ..., F_n$ tq X est l'ensemble des zeros des polynôme $F_1, ..., F_n$.

Soit S l'ensemble qui contient les λ_i et les coefficients des H_i, G_i et F_i sans aucune perte de généralité on peut supposer que K est une extension de type fini de $\mathbb{Q}$ avec des générateurs dans S par le lemme 4.5.1 il existe des nombres premiers p tels que l'on a un plongement $K \hookrightarrow \mathbb{Q}_P$ qui associe a chaque élément de S un élément de $\mathbb{Z}_p$.

On peut supposer que $K = \mathbb{Q}_p$ et σ est la restriction d'un automorphisme de $IA_{\mathbb{Z}_p}^n$.

Donc $\sigma \in Aut(IA_{\mathbb{Z}_p}^n)$ avec le déterminant de la matrice jacobienne de σ est une constante de valeur absolue p-adique égale a un. $\lambda = (\lambda_1, ..., \lambda_n) \in IA_{\mathbb{Z}_p}^n$ et X est une sous variété de $IA_{\mathbb{Z}_p}^n$.

Soit $\tau = \sigma^j$ ici j est un entier positif et σ^j vérifie les deux propriétés du lemme 4.6.1 , soit i un entier $i \in \{0, ..., j-1\}$,$\tau^m(\sigma^i(\lambda))$ dans X pour un nombre infini de m ou il y a seulement un nombre fini de m pour lequel ceci se produit.Si le nombre de m est infini, nous avons $\tau^m(\sigma^i(\lambda)) \in X$ doit être dans X pour tout m. pour voir ceci nous remplaçons λ avec le $\sigma^i(\lambda)$ de sorte que le $\tau^n(\lambda)$ est dans X pour un nombre infini de n . on peut écrire $\tau = (H_1, ..., H_n)$ avec $H_1, ..., H_n$ sont dans $\mathbb{Z}_p[x_1, ..., x_n]$.

Par construction $H_i(\lambda_1, ..., \lambda_n) \equiv \lambda_i \pmod{p\mathbb{Z}_p}$ Par conséquent par Lemme 4.6.2 il existe des séries entiéres $f_1, ..., f_n \in \mathbb{Z}_p[[z]]$ qui converge dans la boule unité fermée d'unité de $\mathbb{Q}_p$

et qui satisfont

$$\begin{aligned} f_i(0) &= \lambda_i \text{ pour } i = \overline{1,n} \\ f_i(z+1) &= H_i\left(f_1(z), ..., f_n(z)\right) \text{ pour } i = \overline{0,n} \end{aligned}$$

Par la construction, $\tau^k(\lambda) = (f_1(k), ..., f_n(k))$ pour tout k dans $\mathbb{Z}$. l'orbite de q sous le τ intersecte X une infinité de fois .

On écrit $X = Z(Q_1, ..., Q_d)$ annulateur pour $i = \overline{1,d}$.

Définissons

$$P_i(z) := Q_i(f_1(z), ..., f_n(z)) \in \mathbb{Q}_p[[z]].$$

Comme $f_1, ..., f_n$ convergent sur le disque d'unité fermée.et $Q_1, ..., Q_d$ sont des polynômes, $P_i(z)$ sont des séries entières p-adique qui convergent sur le disque fermé d'unité pour$1 \leq i \leq d$.on a $P_i(m) = 0$ pour toutes $\tau^m(\lambda) \in X \subseteq Z(Q)$.Par conséquent $P_i(z)$ a un nombre infini de zéros à l'intérieur de la boule d'unité fermée .d'aprés le théorème de **Strassman** 4.6.1 $P_i(z)$ est identiquement nul. par consequence le $\tau^m(q)$ est dans $Z(Q_1, ..., Q_d) = X$ pour tout les entiers m par suite on a:

$$\left\{\sigma^{i+jm}(\lambda) \ / \ m \in \mathbb{Z}\right\} \subseteq X$$

Pour tout $0 \leq i \leq j$.ona

$$\left\{ \ m \in \mathbb{Z} \ / \ \sigma^{i+jm}(\lambda) \in X \ \right\}$$

est un ensemble fini ou l'ensemble de tous les entiers . ■

Théorème 4.6.3 *[27]**(Srinivas)***
Soit A une algébre fini sur un corps K alors il existe un nombre naturel $n = n(A)$ tel que si $N > n$ et $f : K[x_1, ..., x_N] \longrightarrow A$ et $g : K[x_1, ..., x_N] \longrightarrow A$ sont deux applications surjectives dans K algébre ,alors il existe un automorphisme de $K-$algébre
$\Phi : K[x_1, ..., x_N] \longrightarrow K[x_1, ..., x_N]$ *tel que*

$$f = g \circ \Phi$$

Théorème 4.6.4 *Soit Y une variété affine sur un corps K de caractéristique nulle, soient λ un point dans Y et σ un automorphisme de Y .Si X est une sous- variété de Y,alors l'ensemble $\{m \in \mathbb{Z} \ / \ \sigma^m(\lambda) \in X\}$ est une réunion d'un ensemble fini et de infinité de progressions arithmétique doublé .*

Preuve.

On note A l'anneau des fonctions régulières de Y et soit n l'entier comme dans le théorème de Srinivas 4.6.3 .

Comme A a un nombre fini de generateurs sur le corps K il existe un entier $N > n$ tels qu'il existe une surjection $g : K[x_1, ..., x_N] \longrightarrow A$,l'automorphisme σ de Y induit un automorphisme de $K-$algébre $\Psi : A \longrightarrow A$.

$$K[x_1, ..., x_N] \xrightarrow{g} A \xrightarrow{\Psi} A$$

On note f la composition .

D'aprés le théorème de Srinivas 4.6.3 il existe un automorphisme Φ de $K[x_1, ..., x_N]$ tel que

$$f = g \circ \Phi \Leftrightarrow \Psi \circ g = g \circ \Phi$$

Donc g induit un plongement $i : Y \hookrightarrow IA^n_K$ et Φ induit un automorphisme τ de IA^n_K .Alors on a

$$\tau \circ i = i \circ \sigma$$

Comme $\tau_{|Y} = \sigma$ et d'où

$$\Gamma = \{ m \ / \ \sigma^m(\lambda) \in X \} = \{ m \ / \ \tau^m(\lambda) \in X\}$$

On peut regarder la sous variété X de Y comme sous variété de IA^n_K et par le théorème 4.6.2 on déduit que Γ est une réunion d'un ensemble fini de progressions arithmétiques complétes et un ensemble fini. ■

Corollaire 4.6.1 *Soit Y une variété affine sur un corps K de caractéristique nulle,et soit σ un automorphisme de Y et soit λ un point dans IA^n_K Alors l'orbite de λ sous le σ est dense pour la topologie de Zariski si et seulement si pour chaque sous-variété propre X de Y l'ensemble $\{ m \ / \ \sigma^m(\lambda) \in X\}$ est fini .*

Preuve.

Supposons que l'ensemble $\{ m \ / \ \sigma^m(\lambda) \in X\}$ n'est pas dense dans Y.on note X la fermeture de Zariski de cet ensemble .

supposons qu'il existe une sous-variété propre X tels que $\{ m \ / \ \sigma^m(\lambda) \in X\}$ est infini alors par le théorème 4.6.4 il existe deux entiers i , j avec $j \geq 1$ tels que $\sigma^{i+jm}(\lambda) \in X$ pour tous m. donc on a

$$\{ \sigma^m(\lambda) \ / \ m \in \mathbb{Z}\} \subseteq \bigcup_{i=0}^{j-1} \sigma^i(X)$$

l'orbite est contenue dans un sous-ensemble fermé propre de Y et ainsi n'est pas dense pour la topologie de Zariski .

nous obtenons une contradiction immédiate ■

Proposition 4.6.1 *Soit p un nombre premier > 3 et $K = \overline{IF}_p(T)$ et soit l'application σ définit par :*

$$\begin{array}{rcl} \sigma & : & IA^2_{\mathbb{C}} \longrightarrow IA^2_{\mathbb{C}} \\ (x_1, x_2) & \rightsquigarrow & \sigma(x_1, x_2) = (Tx_1, (T+1)x_2) \end{array}$$

Alors pour $\lambda = (1,1)$ et $V = \{(a,b) \in K^2 / x_2 - x_1 = 1\}$,l'orbite $\sigma^j(\lambda)$ intersecte V infiniment defois, mais ne contient aucune progression arithmétique infinie.

Preuve. On a :
$\sigma^j(1,1) = \left(T^j, (T+1)^j\right)$
$\sigma^{p^d}(1,1) = \left(T^{p^d}, T^{p^d}+1\right) \in V \ \text{car}\left(T^{p^d}+1\right) - T^{p^d} = 1$
mais comme T est transcendante sur IF_p, la seule condition est $i + jm$ une puissance de p pour tout $m \geq 0$. qui est impossile. ■

Chapitre 5

Conclusion générale

Le théorème de Skolem-Mahler- Lech ne permet pas de déterminer effectivement tous les zeros d'une s.r.l.

Etant donné une suite récurrente linéaire existe t-il un algorithme permettant de trouver tous les indices n tel que la s.r.l soit nulle?

le théorème de Strassman permet de majorer le nombre de zéros d'une suite récurrente linéaire lorsque ce nombre est fini.

Bézivin propose les problémes suivants:

Dans chapitre 2 il serait intéressant dans le cas de la caractéristique non nulle de décrire explicitement ce qui passe quand l'ensemble des indices nuls d'une suite récurrente linéaire est infini et de densité nulle. en particulier peut-on décrire cet ensemble à l'aide de progressions géométriques comme dans l'exemple de Lech.

Dans le chapitre 3 il serait intéressant de savoir si l'on peut dans le théorème 3.1.1 remplacer l'hpothése " $a(n) = \sum_{j=1}^{m} c_j \ \forall n$ " par "$a(n) = \sum_{j=1}^{m} R_j(n)\, c_j(n) \ \forall n$ avec $R_j(n) \in K[x]$ pour tout j ".

-Il y a beaucoup de différentes preuves et généralisations du théorème de Skolem-Mahler-Lech touteses preuves emploient des méthodes p-adique d'une manière quelconque, bien que le résultat soit valide dans n'importe quel corps de caracteristique zéro.

Bibliographie

[1] **Y. Amice.** "*Interpolation p-adique*", Bull. Soc. math. France, 92, 1964, p. 117-180.

[2] **Y.Amice.** "*Les nombres p-adique*"1975 Presses universitaires de France.

[3] **D.Barsky** . "*Interpolation p-adique*"Seminare delang-pisot-poitou théorie des nombres, t9,.1967-1969 exp n°11 p1-11

[4] **J.P Bell .** "*A generalized Skolem-Mahler-Lech theorem for affine varieties.* Jason P. Bell. math.NT (math.AG).

[5] **B.BENZAGHOU** "*Algèbre de Hadamard*", Bull. Soc. Math. France 28 (1970), pp. 209-252.

[6] **J-P .BEZIVIN .** " *Factorisation de suites récurrentes linéaires et applications".* Bulletin de la Société Mathématique de France, 112 (1984), p. 365-376

[7] **J-P .BEZIVIN .** "*Une généralisation du théorème de Skolem-Mahler-Lech*", Quart. J. Math. Oxford, t. 40, 1989, p. 133-138.

[8] **J-P .BEZIVIN .** "*Suites récurrentes linéaires en caractéristique non nulle*". Bulletin de la Société Mathématique de France, 115 (1987), p. 227-239

[9] **J-P .BEZIVIN .** "*Sur un théorème de Polya*", J. Reine Angew. Math. 364 (1986), 60-68. MR 817638 | Zbl 0569.10004

[10] **J-P .BEZIVIN .** "*Quotient de fonctions entières et quotients de Hadamard de séries formelles*", Ann. Inst. Fourier, t. 39, 1989, p. 737-752.

[11] **N.BOURBAKI .** "*Algèbre commutative*" .ch6.§10.N°3 corrolaire 4

[12] **I.CIERLENCO , M.MIGNOTTE et F.PIRAS.** " S*uites récurrentes linéaires propriétés algébriques et arithmétiques*", Enseign. Maths, t. 33, 1987, p. 67-108.

[13] **G. Everest**, **A. van der Poorten, Alf, I. Shparlinski, T. Ward.** "*Recurrence sequences*". Mathematical Surveys and Monographs, 104. American Mathematical Society, Providence, RI, 2003.

[14] **Derlingue P** " *Equation différentielles à points singuliers réguliers* " lecture Notes in Maths N° 163.

[15] **V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, and A. A. Nechaev**. "*Linear recurring sequences over rings and modules*". J. of Math. Sci., 76(6):2793{2915, 1995.

[16] **LECH (C.)**. "*A note on recurring series*", Ark Mat., vol. 2, 1952, p. 417-421.

[17] **K. Mahler**. *Eine arithmetische Eigenshaft der Taylor-Koeffizienten rationaler Funktionen*. Proc. Kon. Nederlandsche Akad. v. Wetenschappen 38 (1935) 50–60.

[18] **K. Mahle**r. "*On the Taylor coefficients of rational functions*". Proc. Cambridge Philos. Soc. 52 (1956), 39–48.

[19] **K. Mahler**. Addendum to the paper "*On the Taylor coefficients of rational functions*". Proc. Cambridge Philos. Soc. 53 (1957), 544.

[20] **POLYA (G.).** "*Arithmetische Eigenschaften der Reihenenwicklungen rationaler Funktionen*", J. Reine Angew. Math., t. 151, 1921, p. 1-31.

[21] **Poken .J-**"*arithmetical proprties of the taylor coefficients of algebraic functions* ",Indag Math 21 (1959) ,202-210.

[22] **SZEMEREDI (E.).** "*On sets of integers containing no k elements in arithmetic progression*", Acta Math., vol. 27, 1975, p. 199-245.

[23] **R. Strassman.** ¨"*Uber den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen*". J. Reine Angew. Math. 159 (1928), 13–28; 65–66.

[24] **REUTENAUER (C.).** " *Sur les éléments inversibles de l'algèbre de Hadamard des séries rationnelles*", Bull. soc. Math. France., vol. 110, 1982,p.225-232

[25] **M.-P**. **Schützenberger**. "*On the certain synchronizing properties of certain prefix codes*". Inform. and Comput. 7 (1964), 23–36.

[26] **R.P. Stanley,** "*Differentiably finite power series"*, Eur. J. Comb. 1 (1980), 175-188.

[27] **Srinivas.V.** "*On the embedding dimension of an affine variety*". Math Ann. 289 (1991), 125–132.

[28] **T. Skolem.** "*Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen"*. C. r. 8 congr. scand. ʻa Stockholm (1934), 163–188.

[29] **VAN DER POORTEN (A. J.)**. "*Additive relations in number fields"*, Séminaire de théorie des nombres de Paris", 1982-1983, p. 259-266. Progress in Math., 1984, Birkhaüser-Boston.

[30] **J.P.Bézivin and Vichian Laohakosol**."*On the theorm Skolem-Mahler-Lech " Expo.Math.9 (1991),89-86*