ENS RENNES

École Normale Supérieure de Rennes

RAPPORT DE STAGE DE MATHÉMATIQUES DE M1

effectué à l'ICJ

09 mai 2022 - 08 juillet 2022, 9 semaines

Automaticité et algébricité des séries formelles

Le théorème de Skolem-Mahler-Lech en caractérisique non-nulle

---

Brian Flanagan

2e année, magistère de mathématiques de l'ENS Rennes

Institut Camille Jordan
Institut Camille Jordan
Université Claude Bernard Lyon 1
43 boulevard du 11 novembre 1918
F-69622 Villeurbanne Cedex

Encadrant à l'ICJ
Boris Adamczewski
Directeur de recherche

Table des matières

À l'instar des langages rationnels en informatique, on peut définir en théorie des nombres les suites (resp. les ensembles) automatiques comme étant les suites (resp. les ensembles) reconnues par un automate fini. Il apparait grâce à un théorème de Gilles Christol que cette notion d'automaticité est particulièrement adaptée à la description des séries entières algébriques sur les corps finis.
Outre la démonstration de ce théorème, ainsi que certaines de ses généralisations et corollaires, on se propose surtout dans ce mémoire de regarder les liens plus subtils existant entre automaticité et algébricité des séries de Laurent en caractéristique non-nulle, par une généralisation étonnante du théorème de Skoler-Mahler-Lech démontrée par Harm Derksen.

1 Introduction

1.1 Quelques généralités sur les suites et les séries formelles

Remarque. Dans toute la suite de ce mémoire, on verra souvent une suite définie sur un corps comme une série formelle, et inversement.

Définition 1.1.1 (Suites et ensembles périodiques)
Soit $a = (a_n)_{n\in\mathbb{N}}$ une suite quelconque. La suite a est dite :

i. périodique de période $r \in \mathbb{N}^*$ si pour tout entier $n \in \mathbb{N}$, $a_n = a_{n+r}$.

ii. ultimement périodique de période $r \in \mathbb{N}^*$ s'il existe un entier n_0 tel que pour tout entier $n \geqslant n_0$, $a_n = a_{n+r}$.

Un sous-ensemble X de $\mathbb{N}$ est dit périodique (resp. ultimement périodique) si la suite caractéristique $(\mathbb{1}_X(n))_{n\in\mathbb{N}}$ associée est périodique (resp. ultimement périodique).

Remarque. Les ensembles périodiques non vides de période $a \in \mathbb{N}^*$ sont exactement les unions finies de progressions arithémtiques de la forme $a\mathbb{N} + b$, $b < a$ (une telle progression arithmétique où $b < a$ sera dite "complète"). Tandis que les ensembles ultimement périodiques sont exactement les ensembles égaux à un ensemble fini à un ensemble périodique.

Définition 1.1.2 (Suite récurrente linéaire)
Soit K un corps quelconque et $a = (a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ une suite à valeurs dans K. La suite a est dite récurrente linéaire d'ordre inférieur ou égal à $d \in \mathbb{N}$ s'il existe des éléments $\gamma_0, \ldots, \gamma_{d-1} \in K$ tel que :

$$\forall n \in \mathbb{N},\ \gamma_0 a_n + \gamma_1 a_{n+1} + \cdots + \gamma_{d-1} a_{n+d-1} = a_{n+d}$$

Le plus petit entier d tel que a vérifie une telle relation est appelé l'ordre de a.

Relions maintenant cette notion aux séries formelle, afin de travailler plus librement par la suite.

Définition 1.1.3 (Séries rationnelles, algébriques)
Une série de Laurent $f \in K((X))$ est dite,

i. rationnelle s'il existe des polynômes $P, Q \in K[X]$ tels que $f = P/Q$.

ii. algébrique s'il existe un entier r et des polynômes $P_0, \ldots, P_r$ tels que

$$P_r f^r + \cdots + P_1 f + P_0 = 0.$$

Théorème 1.1.4 (Caractérisation des séries rationnelles)
Soit K un corps quelconque et $f(X) = \sum_{n\in\mathbb{N}} a_n X^n$ une série formelle sur K. La série f est rationnelle de dénominateur de degré supérieur ou égal au degré du numérateur si et seulement si la suite a donnée par ses coefficients est récurrente linéaire.

Preuve. Supposons que f est algébrique et s'écrit $f = P/Q$, où P, Q sont des polynômes sur K. On a donc la relation $Qf = P$. Posons $Q = \sum_{i=0}^{d-i} \gamma_i X^i$ de degré d et notons $n_0 \leqslant d$ le degré de P. Par

identification des coefficients, pour tout entier n, on a $\sum_{i=0}^{d} \gamma_{d-i} a_{n+d-i} = 0$, c'est-à-dire, puisque $\gamma_d \neq 0$:

$$a_{n+d} = -\frac{1}{\gamma_d} \left(\gamma_0 a_n + \gamma_1 a_{n+1} + \cdots \gamma_{d-1} a_{n+d-1}\right)$$

Réciproquement, si la suite $(a_n)_{n\in\mathbb{N}}$ des coefficients de f est récurrente linéaire, en posant $Q = -X^d + \gamma_0 X^{d-1} + \cdots \gamma_1 X + \gamma_{d-1}$, on a bien que Qf est un polynôme de degré inférieur ou égal à Q et donc que f est rationnelle.

Remarque. Après la caractérisation des séries rationnelles, la prochaine étape serait de savoir quelles suites donnent des séries algébriques. La tâche est plus ardue et est un des principaux objets de ce mémoire (sur les corps de caractéristique non nulle).

1.2 Suites et ensembles automatiques

Définition 1.2.1 (Automate fini à sortie)
Un automate finie à sortie est un uplet $\mathcal{A} = (\Sigma, Q, q_0, \delta, \Delta, \tau)$ où Σ et Δ sont des alphabets finis, Q est un ensemble fini (l'ensemble des états), $q_0 \in Q$ est l'état initial. À cela on ajoute une fonction de transition $\delta : Q \times \Sigma \to Q$ et une fonction de sortie $\tau : Q \to \Delta$.

Exemple 1.2.2

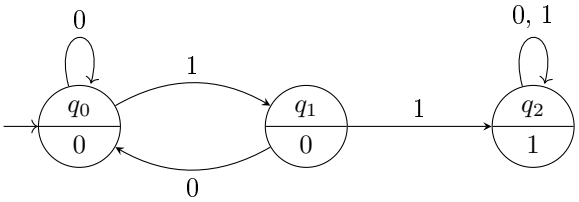


FIGURE 1 – Un exemple d'automate
Ici, $k = 2$, $Q = \{q_0, q_1, q_2\}$, $\delta(q_0, 0) = \delta(q_1, 0) = q_0, \delta(q_0, 1) = q_1, \delta(q_1, 0) = \delta(q_2, 0) = \delta(q_2, 1) = q_2$, $\Delta = \{0, 1\}$, $\tau(q_0) = \tau(q_1) = 0, \tau(q_2) = 1$

Définition 1.2.3 (Suite p-automatique)
Soit $p \geqslant 2$ un entier un $(a_n)_{n\in\mathbb{N}}$ une suite quelconque. Pour un entier n, notons $\langle n \rangle_p$ sa décomposition en base p (avec le chiffre le plus significatif à gauche). La suite $(a_n)_{n\in\mathbb{N}}$ est dite p-automatique s'il existe un automate finie à sortie sur l'alphabet $A_p = \{0, \ldots, p-1\}$ produisant la suite $(a_n)_{n\in\mathbb{N}}$.
Plus précisément, la suite $(a_n)_{n\in\mathbb{N}}$ est p-automatique s'il existe un automate fini à sortie $\mathcal{A} = (A_p, Q, q_0, \delta, \Delta, \tau)$ tel que pour tout entier $n \in \mathbb{N}$:

$$a_n = \tau(\delta(q_0, \langle n \rangle_p))$$

Remarque. On a étendu la définition de la fonction de transition à $Q \times \Sigma^*$ et non plus seulement à $Q \times \Sigma$. On définit la fonction de transition généralisée aux mots comme suit, par récurrence. Pour une lettre $a \in \Sigma$ et un mot $w \in \Sigma^*$ et un état q, on définit $\delta(q, aw) = \delta(\delta(q, a), w)$.
Ceci correspond à une lecture de gauche à droite des mots, mais on aurait tout aussi bien pu prendre la convention opposée : $\delta(q, aw) = \delta(\delta(q, w), a)$. Un résultat classique de théorie des automates indique qu'une suite est p-automatique par lecture de gauche à droite si et seulement si elle est p-automatique par lecture de droite à gauche. Dans la plupart des cas, nous suivront la première convention.

Exemple 1.2.4 (Suite de Thue-Morse)
La suite de Thue-Morse est une des suites automatiques les plus célèbres. On la définit comme suit. Étant donné un entier n, soit t_n la somme de ses chiffres en base 2 modulo 2.
On a $t_0 = 0,\ t_1 = 1,\ t_2 = 1,\ t_3 = 0,\ t_4 = 1, \ldots$ La suite $t = (t_n)_{n\in\mathbb{N}}$ est la suite de Thue-Morse. Elle est 2-automatique, puisqu'elle est engendrée par l'automate donné en figure 2.
Il est à noter que la suite de Thue-Morse est donnée par le même automate, que l'on lise les mots de

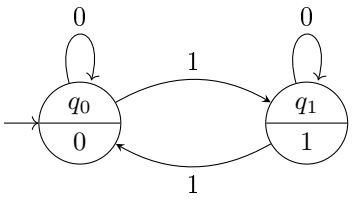


FIGURE 2 – Automate de Thue-Morse
Ici, $p = 2$, $Q = \{q_0, q_1\}$, $\delta(q_0, 0) = q_0, \delta(q_0, 1) = q_1, \delta(q_1, 0) = q_1, \delta(q_1, 1) = q_0$, $\Delta = \{0, 1\}$, $\tau(q_0) = 0, \tau(q_1) = 1$

gauche à droite ou de droite à gauche.

Exemple 1.2.5 (Progressions arithmétiques) Considérons deux entiers naturels $b < a$. La progression arithmétique $a\mathbb{N} + b$ est p-automatique pour tout $p \geqslant 2$. Pour le voir, on va construire un p-automate qui convient.
On pose $Q = \mathbb{Z}/a\mathbb{Z}$, $q_0 = 0$ et la fonction de transition suivante :

$$f : \begin{cases} Q \times A_p & \longrightarrow Q \\ (x, l) & \longmapsto px + p \mod a \end{cases}$$

On considère également l'alphabet de sortie $\Delta = \{0, 1\}$ et la fonction de sortie :

$$\tau : \begin{cases} Q & \longrightarrow \Delta \\ x & \longmapsto 1 \text{ ssi } x = b \end{cases}$$

Par exemple, la figure 3 ce que donne une telle description pour la progression arithmétique $4\mathbb{N} + 1$ en base 3.

Le résultat suivant est classique en théorie des automates.

Théorème 1.2.6 (Caractérisation des suites automatiques par le p-noyau)
Soit $p \geqslant 2$ un entier et $a = (a(n))_{n\in\mathbb{N}}$ une suite quelconque. On intrdoduit le p-noyau de a :

$$\mathcal{N}_p(a) = \{(a(p^r n + j))_{n\in\mathbb{N}} \mid r \in \mathbb{N}, 0 \leqslant j < p^r\}$$

La suite a est p-automatique si et seulement si son p-noyau est fini.

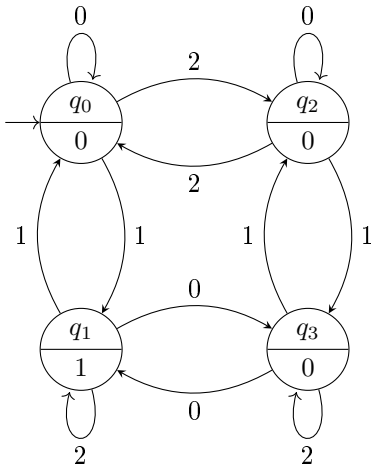


FIGURE 3 – 3-automate produisant la progression arithmétique $4\mathbb{N}+1$.

Preuve. Supposons tout d'abord que la suite a est p-automatique et donnons-nous un automate $\mathcal{A} = (A_p, Q, q_0, \delta, \Delta, \tau)$ la produisant de droite à gauche (et non de gauche à droite comme habituellement). Soit r un entier naturel et $j < p^r$. Considérons $w = \langle j \rangle_p$ l'écriture de j en base p, que l'on a éventuellement complétée par des zéros à gauche de sorte que w soit de longueur r.
Pour tout $n \in \mathbb{N}$, on a l'identité : $\langle p^r n + j \rangle_p = \langle n \rangle_p w$. De sorte que :

$$a(p^r n + j) = \tau(\delta(q_0, \langle p^r n + j \rangle_p)) = \tau(\delta(q_0, \langle n \rangle_p w)) = \tau(\delta(\delta(q_0, w), \langle n \rangle_p))$$

Ainsi, la suite $(a(p^r n + j))_{n\in\mathbb{N}}$ est la suite produite de droite à gauche par l'automate

$$\mathcal{A}_j^r = (A_p, Q, \delta(q_0, w), \delta, \Delta, \tau)$$

(on a seulement modifié l'état initial de $\mathcal{A}$).
Or, l'ensemble des $\{\mathcal{A}_j^r \mid r \in \mathbb{N}, j < p^r\}$ est fini, puisque $\mathcal{A}$ possède un nombre fini d'états. Le p-noyau de a est donc nécessairement lui aussi fini (à un automate correspond une suite du p-noyau).

Réciproquement, supposons que le p-noyau de a est fini. Construisons explicitement un automate produisant a de droite à gauche. Considérons l'ensemble des états $Q = \mathcal{N}_p(a)$ et l'état initial $q_0 = (a(n))_{n\in\mathbb{N}}$.
Pour un état $(a(p^r n + j))_{n\in\mathbb{N}}$ et une lettre $t \in \{0, \dots, p-1\}$, on pose

$$\delta((a(p^r n + j))_{n\in\mathbb{N}}, t) = (a(p^{r+1} n + p^r t + j))_{n\in\mathbb{N}}$$

ce qui est bien défini, puisque si $(a(p^r n + j))_{n\in\mathbb{N}} = (a(p^s n + i))_{n\in\mathbb{N}}$, alors en remplaçant n par $pn + t$, on a bien $(a(p^{r+1} n + p^r t + j))_{n\in\mathbb{N}} = (a(p^{s+1} n + p^s t + i))_{n\in\mathbb{N}}$. Enfin, on considère la fonction de sortie τ définie par :

$$\tau((a(p^r n + j))_{n\in\mathbb{N}}) = a(j)$$

À nouveau, elle est bien définie, puisque si $(a(p^r n + j))_{n\in\mathbb{N}} = (a(p^s n + i))_{n\in\mathbb{N}}$, alors en particulier, $a(j) = a(i)$. Ainsi, pour un entier j dont l'écriture en base p est $\langle j \rangle_p = w_{r-1} \dots w_0$, on a :

$$\begin{aligned}
\tau(\delta(q_0, \langle j \rangle_p)) &= \tau(\delta(\underbrace{\delta(q_0, w_0)}_{(a(pn+w_0))_{n\in\mathbb{N}}}, w_{r-1} \dots w_1)) \\
&= \tau(\delta(\underbrace{\delta(\delta(q_0, w_0), w_1)}_{(a(p^2 n + pw_1 + w_0))_{n\in\mathbb{N}}}, w_{r-1} \dots w_2)) \\
&= \dots = \tau((a(p^r n + j))_{n\in\mathbb{N}}) = a(j)
\end{aligned}$$

L'automate que l'on a construit produit donc bien la suite a de droite à gauche.

Remarque. Sur un ensemble X on note T_j^k l'opérateur de $X^{\mathbb{N}}$ sur lui-même, défini par :

$$\forall a = (a(n))_{n\in\mathbb{N}} \in X^{\mathbb{N}},\ \forall n \in \mathbb{N}, T_j^k a(n) = a(kn+j)$$

De sorte que si l'on note Θ le monoïde engendré par les $T_j^k, j = 0, 1, \ldots, k-1$, une suite est k- automatique si et seulement si son orbite sous l'action de Θ est finie.
Cette notion est cependant plus adaptée aux suites automatiques qu'aux ensembles automatiques. Si S est un sous-ensemble de $\mathbb{N}$ et si χ_S est sa suite caractéristique, on a :

$$T_j^k \chi_S = (\chi_S(kn+j))_{n\in\mathbb{N}} = \chi_{\frac{(S-j)}{k}\cap\mathbb{N}}$$

Si bien que si l'on introduit l'opérateur $L_j^k : \mathbb{N} \to \mathbb{N}, n \mapsto kn+j$, on a :

$$T_j^k \chi_S = \chi_{(L_j^k)^{-1}S}$$

Ainsi, un ensemble $S \subset \mathbb{N}$ est k-automatique si et seulement si l'ensemble

$$\mathcal{N}_k(S) = \left\{(L_{j_1}^k)^{-1} \cdots (L_{j_r}^k)^{-1} S \mid r \in \mathbb{N}, 0 \leqslant j_1, \ldots j_r < k\right\}$$

est fini. Une stratégie courante pour montrer qu'une suite (resp. un ensemble) est k-automatique sera donc d'inclure cette suite (resp. cet ensemble) dans un ensemble fini stable par les T_j^k (resp. les $(L_j^k)^{-1}$).

Corollaire 1.2.7 Soit $S \subset \mathbb{N}$ et $k \in \mathbb{N}^*$. L'ensemble S est p-automatique si et seulement si les ensembles $(L_j^k)^{-1}S$ sont p-automatiques pour tout $0 \leqslant j < k$.

Preuve. On observe que pour des entiers naturels r et $i < p^r$ donnés, on a l'égalité :

$$(L_i^{p^r})^{-1} S = \bigcup_{j=0}^{N-1} (L_j^k)^{-1} (L_i^{p^r})^{-1}$$

Ainsi, l'ensemble $\mathcal{N}_p(S) = \left\{(L_i^{p^r})^{-1} S \mid r \in \mathbb{N}, 0 \leqslant i < k\right\}$ est fini si et seulement si l'ensemble :

$$\left\{(L_j^k)^{-1}(L_i^{p^r})^{-1} S \mid r \in \mathbb{N}, 0 \leqslant i < k, 0 \leqslant j < k\right\}$$

est fini. En outre, pour $0 \leqslant j < k$, le p-noyau de $(L_j^k)^{-1}S$ est :

$$\left\{(L_i^{p^r})^{-1}(L_j^k)^{-1} S \mid r \in \mathbb{N}, 0 \leqslant i < k\right\}$$

Or, pour r fixé, si $p^r n + i = km + j$, alors :

$$L_i^{p^r} L_n^k = L_{p^r n+i}^{kp^r} = L_{km+j}^{kp^r} = L_j^k L_m^{p^r}$$

Donc le p-noyau de S est fermé si et seulement si les p-noyaux des $(L_j^k)^{-1}S$ sont finis.

On peut aisément transposer certaines propriétés des langages rationnels aux ensembles k-automatiques, comme c'est le cas dans [AS03].

Théorème 1.2.8 (Quelques propriétés de stabilité des ensembles automatiques)
Une union finie d'ensembles k-automatiques est k-automatique, et tout ensemble fini est k-automatique.

Nous ne démontrerons pas le théorème suivant, qui est ardu mais fondamental. Une preuve assez longue est donnée par Allouche et Shallit [AS03]. Elle comporte une erreur, remarquée et corrigée par Rigo et Waxweiler [RW09]. Une preuve plus courte a récemment été donnée par Krebs [Kre18].

Théorème 1.2.9 (Cobham)
Soient k, l deux entiers premiers entre eux. Une suite $(a_n)_{n\in\mathbb{N}}$ est à la fois k-automatique et l-automatique si et seulement elle est ultimement périodique. Dans ce cas, elle est p-automatique pour tout entier p.

2 Séries de Laurent algébriques

Dans toute cette section, on travaillera sur un corps K de caractéristique non nulle et étant donné un sous-ensemble V de K, et on notera $V^{\langle p\rangle}$ l'image de V par le morphisme de Frobenius, c'est-à-dire :

$$V^{\langle p\rangle} = \{f^p \in K \mid f \in V\}$$

2.1 Opérateurs de Cartier et séries algébriques

Définition 2.1.1 (Opérateurs de Cartier)
Soit K un corps parfait de caractéristique p et $i \in \{0, \dots, p-1\}$. On définit l'opérateur de Cartier $\Lambda_i : K[[X]] \to K[[X]]$ sur les séries formelles à coefficients dans K comme suit :

$$\forall f(X) = \sum_{n\in\mathbb{N}} a(n)X^n \in K[[X]],\ \Lambda_i(f) = \sum_{n\in\mathbb{N}} a(pn+i)^{1/p}X^n$$

On note Ω le monoïde engendré par les $\Lambda_1, \dots, \Lambda_{p-1}$ et pour une série formelle $f \in K[[X]]$, on désignera par $\Omega(f)$ l'orbite de f sous l'action de Ω.

Remarque.

— Sur $\mathbb{F}_p$, on peut réécrire la définition des opérateurs de Cartier : $\Lambda_i(f) = \sum_{n\in\mathbb{N}} a(pn+i)X^n$.
— Dans ce cas, l'orbite $\Omega(f)$ d'une série formelle f est égale à son noyau $mathcalN_p(f)$.
— La définition des opérateurs de Cartier et les propriétés qu'on donnera à leur sujet se généralisent sans douleur au cas multidimensionnel (sauf mention contraire).
Plus précismément, pour $\boldsymbol{i} \in \{0, \dots, p-1\}^d$ et $f \in K[[\boldsymbol{X}]]$, on définit :

$$\Lambda_{\boldsymbol{i}}(f) = \sum_{\boldsymbol{n}\in\mathbb{N}^d} a(p\boldsymbol{n}+\boldsymbol{i})\boldsymbol{X}^{\boldsymbol{n}}$$

De même, cette définition s'étend à $K((X))$ (que X désigne une ou plusieurs indéterminées). Mais nous préciserons l'extension de cette définition après le lemme suivant.

Lemme 2.1.2 (Quelques propriétés des opérateurs de Cartier)
Soit K un corps parfait de caractéristique p.

i. Les opérateurs de Cartier sont semi-linéaires :

$$\forall f, g \in K[[X]], \forall \lambda \in K,\ \Lambda_i(\lambda f + g) = \lambda^{1/p}\Lambda_i(f) + \Lambda_i(g)$$

ii. On dispose de la décomposition suivante :

$$\forall f \in K[[X]],\ f = \sum_{i=0}^{p-1} X^i \Lambda_i(f)^p$$

Et cette décomposition est de plus unique.

iii. $\forall f, g \in K[[X]],\ \Lambda_i(fg^p) = \Lambda_i(f)g$

iv. Pour un polynôme $P \in K[X]$, $\deg(\Lambda_i(P)) \leqslant \deg(P)/p$. Dans le cas multidimensionnel, le degré est remplacé par le maximum des degrés en chaque indéterminée.

Preuve.

ii. Soit $f = \sum_{n\in\mathbb{N}} a(n)X^n$ une série formelle. On peut écrire :

$$\begin{aligned} f(X) &= \sum_{i=0}^{p-1}\sum_{n\in\mathbb{N}} a(pn+i)X^{pn+i} = \sum_{i=0}^{p-1} X^i \sum_{n\in\mathbb{N}} \left(a(pn+i)^{1/p}X^n\right)^p \\ &= \sum_{i=0}^{p-1} X^i \left(\sum_{n\in\mathbb{N}} a(pn+i)^{1/p}X^n\right)^p = \sum_{i=0}^{p-1} X^i \Lambda_i(f)^p \end{aligned}$$

De plus, cette décomposition est unique, puisque $1, X, X^2, \ldots, X^{p-1}$ forme une famille libre de $K[[X]]$ en tant que $K[[X]]^{\langle p\rangle}$-espace vectoriel.

iii. On remarque : $fg^p = \sum_{i=0}^{p-1} X^i\Lambda_i(f)^p g^p = \sum_{i=0}^{p-1} X^i\left(\Lambda_i(f)g\right)^p$, et donc par unicité de la déomposition ii., on obtient bien l'égalité voulue.

✌

Remarque. Revenons à notre volonté d'étendre la définition des opérateurs de Cartier aux séries de Laurent, qui demande un peu plus d'astuce que le cas multidimensionnel. Soit donc $f = a/b \in K((X))$, avec $a, b \in K[[X]]$. On remarque que : $a/b = ab^{p-1}/b^p$ avec $ab^{p-1} \in K[[X]]$. On a alors :

$$f = \frac{a}{b} = \frac{ab^{p-1}}{b^p} = \frac{1}{b^p}\sum_{i=0}^{p-1} X^i\Lambda_i(ab^{p-1})^p = \sum_{i=0}^{p-1} X^i\left(\frac{\Lambda_i(ab^{p-1})}{b}\right)^p$$

On pose donc $\Lambda_i(f) = \dfrac{\Lambda_i(ab^{p-1})}{b} \in K((X))$. Les opérateurs sont ainsi bien définis sur $K((X))$, puisque si $f = a/b = c/d \in K((X))$ avec $a, b, c, d \in K[[X]]$, alors en utilisant le point iii. du lemme 2.1.2, on a :

$$d\Lambda_i(ab^{p-1}) = \Lambda_i(ad^pb^{p-1}) = \Lambda_i(cbd^{p-1}b^{p-1}) = b\Lambda_i(cd^{p-1})$$

Les résultats énoncés plus haut se généralisent sans peine aux séries de Laurent formelles, puisque l'on dispose toujours d'une décomposition similaires à celle donnée au point i. du lemme 2.1.2.

On est maintenant armés pour énoncer le théorème suivant, qui va nous permettre d'exhiber le lien fort qui existe entre séries de Laurent algébriques et opérateurs de Cartier.

Théorème 2.1.3 (Lemme d'Ore)
Soit K un corps parfait de caractéristique p et soit f une série de Laurent formelle à coefficients dans K algébrique sur $K(X)$. Il existe un entier $d \in \mathbb{N}^*$ et des polynômes $P_0, \ldots, P_d \in K[X]$ tels que :

$$P_0 f + P_1 f^p + P_2 f^{p^2} + \cdots + P_d f^{p^d} = 0$$

et $P_0 \neq 0$.

Preuve. Puisque f est algébrique sur $K(X)$, le $K(X)$-espace vectoriel engendré par $\{1, f, f^2, \ldots\}$ est de dimension finie. En particulier, le $K(X)$-espace vectoriel engendré par $\{f, f^p, f^{p^d}, \ldots\}$ l'est lui aussi. Par conséquent, il existe un entier $d \in \mathbb{N}^*$ et des polynômes $P_0, \ldots, P_d$ non tous nuls tels que :

$$P_0 f + P_1 f^p + P_2 f^{p^2} + \cdots + P_d f^{p^d} = 0 \qquad (\star)$$

Considérons maintenant r l'indice minimal tel que $P_r \neq 0$ parmi les équations de type $(\star)$. Supposons par l'absurde que $r > 0$. Ainsi, il existe un entier $d \geqslant r$ et des polynômes $P_r, \ldots, P_d$ tels que :

$$P_r f^{p^r} + \cdots + P_d f^{p^d} = 0$$

et $P_r \neq 0$. Puisque P_r est non nul, il existe un indice $i \in \{0, \ldots, p-1\}$ tel que $\Lambda_i(P_r) \neq 0$, en vertu de la décomposition du point ii. du lemme 2.1.2. Par conséquent, en appliquant Λ_i à l'équation précédente, on obtient par le point iii. du lemme 2.1.2. (puisque $r > 0$) :

$$\Lambda_i(P_r) f^{p^{r-1}} + \cdots + \Lambda_i(P_d) f^{p^{d-1}} = 0$$

On obtient donc une équation du type $(\star)$ avec le $(r-1)$-ème coefficient non nul, ce qui contredit la définition de r. Par conséquent, $r = 0$, ce qui achève la démonstration.

✌

Remarque. L'intérêt d'une telle équation est de pouvoir facilement y appliquer les opérateurs de Cartier. Si l'on réussit à renormaliser une telle équation et avoir $P_0 = 1$, on observe que :

$$\Lambda_i(f) + \Lambda_i(P_1) f + \Lambda_i(P_2) f^p + \cdots + \Lambda_i(P_d) f^{p^{d-1}} = 0$$

Donc si f est une combinaison linéaire à coefficients dans $K_{\leqslant d}[X]$ de $f, f^p, f^{p^2}, \ldots, f^{p^d}$, alors $\Lambda_i(f)$ l'est également.
Ainsi, si f est algébrique et si l'on considère le K-espace vectoriel composé de ces combinaisons linéaires, on peut espérer qu'il soit stable sous l'action de Ω. Le théorème suivant de Sharif et Woodcock [SW88] va préciser cette idée et lui donner une réciproque.

Théorème 2.1.4 (Sharif et Woodcock)
Soit K un corps parfait de caractéristique p et soit $f \in K((X))$. La série de Laurent f est algébrique sur $K(X)$ si et seulement s'il existe un sous K-espace vectoriel V de $K((X))$ de dimension finie contenant f et stable sous l'action de Ω.

Preuve. Supposons tout d'abord que f est algébrique sur $K(X)$. D'après le lemme d'Ore, on dispose de polynômes $P_0, \ldots, P_d \in K[X]$ avec P_0 non nul tels que :

$$P_0 f + P_1 f^p + P_2 f^{p^2} + \cdots + P_d f^{p^d} = 0$$

Suivant notre idée de renormaliser cette équation, posons $g = f/P_0 \in K((X))$. De sorte que :

$$g = -\sum_{i=1}^{d} P_i P_0^{-2} f^{p^i} = -\sum_{i=1}^{d} P_i P_0^{p^i - 2} (f/P_0)^{p^i}$$

En posant $Q_i = -P_i P_0^{p^i - 2} \in K[X]$, on obtient la relation $(\star)$: $g = \sum_{i=1}^{d} Q_i g^{p^i}$.
Notons maintenant $M = \sup(\deg P_0, \deg Q_i, i = 1, \ldots, d)$ et posons, comme annoncé dans la remarque du lemme d'Ore :

$$V = \left\{ h = \sum_{i=0}^{d} R_i g^{p^i} \in K((X)) \mid R_i \in K_{\leqslant M}[X], i = 1, \ldots, d \right\}$$

Cet espace vectoriel est un sous K-espace vectoriel de $K((X))$. Il contient f puisque $f = P_0 g$ et est stable sous l'action de Ω. En effet, si $h = \sum_{i=0}^{d} R_i g^{p^i} \in V$, alors en utilisant les points i. et iii. du lemme 2.1.2 et en utilisant la relation $(\star)$, on obtient :

$$\Lambda_j(h) = \Lambda_j\left(R_0 g + \sum_{i=1}^{d} R_i g^{p^i}\right) = \Lambda_j\left(\sum_{i=1}^{d} (R_0 Q_i + R_i) g^{p^i}\right) = \sum_{i=1}^{d} \Lambda_j\left((R_0 Q_i + R_i)\right) g^{p^{i-1}}$$

D'après le point iv. du lemme 2.1.2, les $\Lambda_j\left((R_0 Q_i + R_i)\right)$ sont de degré au plus $2M/p \leqslant M$ et donc $\Lambda_j(h)$ appartient bien à V.

Réciproquement, supposons qu'il existe un sous K-espace vectoriel V de $K((X))$ de dimension finie contenant f et stable par Ω. On va montrer que f est algébrique.
Pour cela, notons n la dimension de V (sur K) et fixons $\mathcal{B}$ une base de V. On considère alors G le $K(X)$-espace vectoriel engendré par les :

$$\prod_{g \in \mathcal{B}} g^{s_g}, \quad (s_g)_{g \in \mathcal{B}} \in \mathbb{N}^{\mathcal{B}} \setminus (0, \dots, 0)$$

Puisque $f \in V = \operatorname{Vect}_K \mathcal{B}$, par la formule du binôme, les f^m sont des éléments de G, quel que soit l'entier m. Par conséquent, si l'on montre que G est de dimension finie sur $K(X)$, il est clair que f sera algébrique. C'est donc ce que nous allons tacher de faire.
Pour cela introduisons V_1 le $K(X)$-espace vectoriel engendré par V et V_2 le $K(X)$-espace-vectoriel engendré par l'image de V par le morphisme de Frobenius. Plus précisément :

$$V_1 = \operatorname{Vect}_{K(X)} V \quad \text{et} \quad V_2 = \operatorname{Vect}_{K(X)} \{h^p \mid h \in V_1\} = \operatorname{Vect}_{K(X)} V_1^{\langle p \rangle}$$

On va montrer que V_1 et V_2 sont en fait égaux. Puisque V_1 est de dimension au plus $n = \dim_{K(X)} V$ (il admet une famille génératrice de cardinal n), on peut s'en donner une base $\mathcal{C} = (c_1, \dots, c_r)$, de sorte que pour un élément $h = \sum_{i=1}^{r} h_i c_i \in V_1$, on a : $h^p = \sum_{i=1}^{r} h_i^p c_i^p$.
Si bien que $(c_1^p, \dots, c_r^p)$ engendre V_2 et donc : $\dim_{K(X)} V_2 \leqslant \dim_{K(X)} V_1 \leqslant n$. Il nous suffit donc de montrer que V est inclu dans V_2, ce qui montrera que V_1 est inclu dans V_2 et donc par égalités de dimensions que $V_1 = V_2$. C'est bien le cas, puisque si $h \in V$, on peut écrire : $h = \sum_{i=0}^{p-1} X^i \underbrace{\Lambda_i^p(h)}_{\in V} \in V_2$.
Revenons maintenant à l'espace G. Si $g \in \mathcal{B} \subseteq V \subseteq V_1$, alors $g^p \in V_2 = V_1$. Par conséquent, un tel g^p est une combinaison linéaire sur $K(X)$ des éléments de $\mathcal{B}$. Il s'en suit donc que G est engendré par les :

$$\prod_{g \in \mathcal{B}} g^{s_g}, \quad (s_g)_{g \in \mathcal{B}} \in \{0, \dots, p-1\}^{\mathcal{B}} \setminus (0, \dots, 0)$$

et est donc bien de dimension finie ! Les opérateurs de Cartier ont ici été essentiel, puisqu'ils permettent d'écrire une série de Laurent en fonction de séries Laurent mises à la puissance p, ce qui implique une sorte de périodicité dans les puissances des séries de Laurent.

✌

On en déduit immédiatement le corollaire suivant, qui est plus précis.

Corollaire 2.1.5
Soit K un corps parfait de caractéristique p.
Une série de Laurent $f \in K((X))$ est algébrique si et seulement si le $K(X)$-espace vectoriel engendré par $\Omega(f)$ est de dimension finie.

Ceci nous permet de démontrer le résultat suivant sur l'algébricité des séries de Laurent.

Théorème 2.1.6 (Algébricité et produit de Hadamard)
Soit K un corps parfait de caractéristique p. Soient $f, g \in K((X))$ deux séries de Laurent algébriques sur $K(X)$. Leur produit de Hadamard $f * g$ est également algébrique sur $K(X)$.

Preuve. Puisque f (resp. g) est algébrique, l'espace $V = \mathrm{Vect}_{K(X)} \Omega(f)$ (resp. $W = \mathrm{Vect}_{K(X)} \Omega(g)$) est de dimension finie. Par conséquent, l'espace $V * W$ engendré par les produits de Hadamard des éléments de f et de g est lui aussi de dimension finie. Il est alors facile de se convaincre qu'il contient $f * g$ et est stable par l'action de Ω. Ceci montre bien que $f * g$ est algébrique d'après le théorème de Sharif et Woodcock.

✌

Remarque. Ce résultat est faux sur un corps de caractéristique nulle, puisque $\sum_{n\in\mathbb{N}} \binom{2n}{n} X^n = \sqrt{1-4X}$ est algébrique sur $\mathbb{Q}(X)$, tandis que $\sum_{n\in\mathbb{N}} \binom{2n}{n}^2 X^n$ ne l'est pas [SW88].

2.2 Le théorème de Christol et ses applications

Avant d'énoncer le résultat principal de cette section, nous avons d'abord besoin d'un lemme technique.

Lemme 2.2.1 (Opérateurs de Cartier et p-noyau)
Soit K un corps fini de caractéristique p et $f = \sum_{n\in\mathbb{N}} a_n X^n \in K[[X]]$ une série formelle.

$$|\mathcal{N}_p(f)| < +\infty \quad \text{ssi} \quad |\Omega(f)| < +\infty$$

Preuve. Considérons l'ensemble suivant :

$$\mathcal{M}_p(f) = \left\{ \sum_{n\in\mathbb{N}} a(p^j n + r)^{p^i} X^n \mid i \in \mathbb{Z}, j \in \mathbb{N}, r < p^j \right\}$$

qui contient à la fois $\mathcal{N}_p(f)$ et $\Omega_p(f)$, de sorte que s'il est fini, l'un et l'autre le sont également.
En outre, si l'on note $q = p^e$ le cardinal de K, on peut écrire l'ensemble $\mathcal{M}_p(f)$ sous la forme :

$$\mathcal{M}_p(f) = \left\{ \sum_{n\in\mathbb{N}} a(p^j n + r)^{p^i} X^n \mid |i| < e, j \in \mathbb{N}, r < p^j \right\}.$$

Supposons maintenant que $\mathcal{N}_p(f)$ est fini, de sorte que pour un entier $N \geqslant 0$ suffisamment grand, on peut écrire :

$$\mathcal{N}_p(f) = \left\{ \sum_{n\in\mathbb{N}} a(p^j n + r) X^n \mid j \leqslant N, r < p^j \right\}$$

Soit $|i| < e, j \in \mathbb{N}, r < p^j$. Pour un certain $j' \geqslant N$ et $r' < p^{j'}$, on a $\sum_{n\in\mathbb{N}} a(p^j n + r') X^n = \sum_{n\in\mathbb{N}} a(p^{j'} n + r) X^n$ et donc $\sum_{n\in\mathbb{N}} a(p^j n + r)^{1/p^i} X^n = \sum_{n\in\mathbb{N}} a(p^{j'} n + r')^{1/p^i} X^n$. L'ensemble $\mathcal{M}_p(f)$ est donc fini, puisque l'on peut borner les indices i, j et r dans sa définition.

Réciproquement, supposons que $\Omega(f)$ est fini. L'ensemble

$$\widetilde{\mathcal{M}}_p(f) = \left\{ \sum_{n\in\mathbb{N}} a(p^j n + r)^{p^i/p^j} X^n \mid i \in \mathbb{Z}, j \in \mathbb{N}, r < p^j \right\}$$

est donc lui aussi fini (à nouveau, l'indice i ne parcoure pas réellement $\mathbb{Z}$ tout entier). Or il est clair que $\widetilde{\mathcal{M}}_p(f) = \mathcal{M}_p(f)$, ce qui conclue la démonstration.

Théorème 2.2.2 (Christol)
Soit K un corps fini de caractéristique p. Une série formelle $f \in K[[X]]$ est algébrique sur $K(X)$ si et seulement si la suite de ses coefficients est p-automatique.

Preuve. Puisqu'un corps fini de caractéristique p est parfait, on va pouvoir appliquer le théorème Sharif et Woodcock. Soit f une série formelle. Le corps K étant fini, il équivalent de dire qu'un ensemble est fini et que le K-espace vectoriel qu'il engendre est de dimension finie. Si bien que :
f est algébrique sur $K(X)$ si et seulement si $\Omega(f)$ engendre un espace vectoriel de dimension fini si et seulement si $\Omega(f)$ est fini si et seulement si $\mathcal{N}_p(f)$ est fini si et seulement si la suite des coefficients de f est p-automatique.

Exemple 2.2.3 Puisqu'une série rationnelle est algébrique, le théorème de Christol nous indique que sur un corps fini, les suites récurrentes linéaires sont des exemples particuliers de suites automatiques.

Exemple 2.2.4 Dans les faits, il n'est pas difficile de trouver une équation satisfaite par une suite automatique. Il n'y a qu'à regarder l'automate !
Par exemple, dans le cas de la suite de Thue-Morse $(t_n)_{n\in\mathbb{N}}$ définie à l'exemple 1.2.4, on remarque que lorsque l'on part de l'état 0 ou de l'état 1, en lisant un 0 on reste sur le même état, alors qu'en lisant un 1, on change d'état. Puisque l'on lit de gauche à droite, lire un 0 revient à doubler la valeur du mot, tandis que lire un 1 revient à doubler la valeur du mot et ajouter 1 (par exemple $3 = 2\times 1+1$ s'écrit 11 en binaire et 1 s'écrit 1). On en déduit les relations $t_{2n} = t_n$ et $t_{2n+1} = t_n + 1 \mod 2$. Si bien que sur $\mathbb{F}_2$:

$$\begin{aligned} T &= \sum_{n=0}^{+\infty} t_n X^n = \sum_{n=0}^{+\infty} t_{2n} X^{2n} + \sum_{n=0}^{+\infty} t_{2n+1} X^{2n+1} \\ &= \sum_{n=0}^{+\infty} t_n X^{2n} + \sum_{n=0}^{+\infty} (t_n+1) X^{2n+1} \\ &= \left(\sum_{n=0}^{+\infty} t_n X^n\right)^2 + X\left(\sum_{n=0}^{+\infty} t_n X^n\right)^2 + X\left(\sum_{n=0}^{+\infty} X^n\right)^2 \\ &= T^2 + XT^2 + \frac{X}{(1+X)^2} \end{aligned}$$

Si bien que T vérifie l'équation :

$$(1+X)^3T^2 + (1+X)T + T = 0$$

De même, on va lire l'automate décrit dans l'exemple 1.2.2. Notons $(s_n)_{n\in\mathbb{N}}$ la suite produite par l'automate (sur $\mathbb{F}_2$) et notons S la série correspondante.
Tout d'abord, on remarque que lire un 0 peut changer l'état (de q_1 à q_0 par exemple), mais ne change pas la valeur de la sortie. De sorte que l'on a la relation $r_{2n} = r_n$. De la même manière, lire un 0 puis un 1 ne change pas la sortie, donc $r_{4n+1} = r_n$. Enfin, lire deux 1 à la suite fait nécessairement aboutir à

l'état q_2, si bien que $r_{4n+3} = 1$. On a donc :

$$\begin{aligned} S &= \sum_{n=0}^{+\infty} s_n X^n = \sum_{n=0}^{+\infty} s_{2n} X^{2n} + \sum_{n=0}^{+\infty} s_{2n+1} X^{2n+1} \\ &= \sum_{n=0}^{+\infty} s_n X^{2n} + X \left(\sum_{n=0}^{+\infty} s_{4n+1} X^{2n} + \sum_{n=0}^{+\infty} s_{4n+3} X^{2n+1} \right)^2 \\ &= S^2 + X \left(\sum_{n=0}^{+\infty} s_n X^{2n} + \sum_{n=0}^{+\infty} X^{2n+1} \right)^2 \\ &= S^2 + X \left(S^2 + \frac{X}{(1+X)^2} \right)^2 = S^2 + XS^4 + \frac{X^3}{(1+X)^4} \end{aligned}$$

Donc S vérifie l'équation :

$$X(1+X)^4 S^4 + (1+X)^4 R^2 + (1+X)^4 R + X^3 = 0$$

Remarque. Le théorème de Christol est fondamental, puisqu'il exhibe sur les corps finis un véritable pont entre l'étude des séries algébriques et des suites automatiques, deux domaines qui avaient à priori peu à voir. Ceci permet notamment de démontrer la transcendance de séries formelles sur $\mathbb{Q}(X)$ est le suivant [AS03].

Théorème 2.2.5 (L'agébricité passe aux corps finis)
Soit $f \in \mathbb{Z}[[X]]$ une série formelle à coefficients entiers. Si f est algébrique sur $\mathbb{Q}(X)$, alors pour tout nombre premier p, la projection f_p de f sur $\mathbb{F}_p[[X]]$ est algébrique sur $\mathbb{F}(X)$.

Preuve. Considérons des polynômes $P_0, \ldots, P_d \in \mathbb{Q}[X]$ tels que :

$$P_0 + P_1 f + P_2 f^2 + \cdots + P_d f^d = 0$$

Quitte à multiplier les P_i par un entier bien choisi, on peut les supposer à coefficients entiers. Fixons un nombre premier p.
Quitte à diviser les P_i par p plusieurs fois, on peut supposer que leurs projections $\widetilde{P}_i$ sont non toutes nulles. Par conséquent, on dispose d'une relation :

$$\widetilde{P}_0 + \widetilde{P}_1 f_p + \widetilde{P}_2 f_p^2 + \cdots + \widetilde{P}_d f_p^d = 0$$

non triviale et f_p est donc algébrique sur $\mathbb{F}_p(X)$.

✌

On peut se servir de ce principe pour démontrer assez facilement un théorème de Fatou sur le corps des rationnels, comme l'a fait Allouche [All99].

Théorème 2.2.6 (Fatou)
Soit $f(X) = \sum_{n \in \mathbb{N}} a_n X^n \in \mathbb{Q}[[X]]$ une série entière dont les coefficients prennent un nombre fini de valeurs. Cette série entière est soit rationnelle, soit transcendante sur $\mathbb{Q}(X)$.

Preuve. Considérons un entier $M \in \mathbb{N}$ tel que les Ma_n soient entiers et un entier $K \in \mathbb{N}$ tel que les $Ma_n + K$ sont positifs (c'est possible puisque les a_n sont en nombre fini). La série $g = Mf + \dfrac{K}{1-X}$ est alors à coefficients $(b_n)_{n\in\mathbb{N}}$ entiers naturels bornés et a la même algébricité que f sur $\mathbb{Q}(X)$.
Supposons que f est algébrique. Il nous suffit de montrer qu'elle est rationnelle pour conclure. Puisque f est algébrique, g l'est aussi. Soient donc p et q deux nombres premiers distincts majorant strictement les coefficients de g. Ainsi, les projections de g dans $\mathbb{F}_p$ et dans $\mathbb{F}_q$ sont elles aussi algébriques et ont les mêmes coefficients que g. Par conséquent, d'après le théorème de Christol, la suite $(b_n)_{n\in\mathbb{N}}$ est à la fois p-automatique et q-automatique. Puisque p et q sont distincts, le théorème de Cobham nous indique que la suite $(b_n)_{n\in\mathbb{N}}$ est ultimement périodique, c'est-à-dire que g est rationnelle, et donc que f est rationnelle.

✌

Exemple 2.2.7
Le théorème de Fatou peut par exemple servir à démontrer sans heurts la transcendance de certaines séries lacunaires.
Considérons par exemple la série indicatrice des carrés parfaits $f = \sum_{n\in\mathbb{N}} X^{n^2}$. D'après le théorème de Fatou, si cette série est algébrique, c'est qu'elle est rationnelle, *i.e.* que la suite de ses coefficients est récurrente linéaire d'ordre d à partir d'un certain rang, d'après le théorème 1.1.4. Or, pour tout entier n suffisamment grand, on a :

$$n^2 < n^2 + d < (n+1)^2$$

ce qui contredit le fait que la suite caractéristique des carrés parfaits soit récurrente linéaire (tous ses termes seraient nuls à partir d'un certain rang). La série f est donc transcendante (à noter que l'on peut en réalité se passer d'outils aussi puissants pour le démontrer, cf Example 5.5.1 de [AS03]).
Plus généralement, on déduit du théorème de Fatou que si une série lacunaire (entendue comme une série comportant uniquement des 1 et des 0 parmi ses coefficients) est algébrique, alors soit c'est un polynôme, soit le nombre de ses coefficients successifs nuls est borné. La série $\sum_{n\in\mathbb{N}} X^{n!}$ est donc par exemple elle aussi transcendante.

3 Zéros des coefficients des séries algébriques

3.1 Le théorème de Skolem-Mahler-Lech

Dans un corps de caractéristique nulle, on connait depuis longtemps la forme que prennent les ensembles des zéros des suites récurrentes linéaires (c'est-à-dire des séries rationnelles). Le théorème suivant a d'abord été démontré en 1933 par Skolem sur $\mathbb{Q}$, puis étendu en 1935 par Mahler au corps des réels algébriques, pour être enfin généralisé à tout corps de caractéristique nul par Lech en 1953. C'est pour cette raison qu'il porte leurs trois noms. Une courte preuve en est donné dans [Eve+03], tandis que Hansel en donne une preuve plus longue et plus élémentaire [Han86].

Théorème 3.1.1 (Skolem-Mahler-Lech)
Soit $\mathbb{K}$ un corps de caractéristique nulle et $a \in \mathbb{K}^{\mathbb{N}}$ une suite récurrente linéaire à coefficients dans $\mathbb{K}$. L'ensemble $\mathcal{Z}(a) = \{n \in \mathbb{N} \mid a_n = 0\}$ est ultimement périodique.

Remarque. Il n'est pas très difficile de voir que la réciproque du théorème est juste. En effet, si on se donne une union finie de progressions d'arithmétiques complètes quelconque, on peut la ré-écrire comme une union finie de progressions arithmétiques de même période en considérant le ppcm des périodes et en décomposant certaines progressions arithmétiques. Par exemple, on peut écrire :

$$(2\mathbb{N}+1) \cup (3\mathbb{N}+0) = (6\mathbb{N}+1) \cup (6\mathbb{N}+3) \cup (6\mathbb{N}+5) \cup (6\mathbb{N}+0) \cup (6\mathbb{N}+3)$$

C'est d'ailleurs pour cette raison que l'on impose parfois une écriture des progressions arithmétiques avec la même période dans l'énoncé du théorème de Skolem-Mahler-Lech, mais cette formulation est

équivalente à celle que l'on a donné.
Étant donc donné une union finie de progressions arithmétiques complètes de même période, disons $\bigcup_{i=0}^{d}(r\mathbb{N}+b_i)$, il suffit de considérer la suite périodique $(a_n)_{n\in\mathbb{N}}$ de période r et de premiers termes $a_j = 0$ si j est égal à l'un des b_i et $a_j = 1$ sinon, pour $j < r$. Pour une union finie de singletons et de progressions arithmétiques quelconque, il suffit de voir que multiplier une suite rationnelle par un X^s et lui ajouter un polynôme ne modifie pas son caractère rationnel (ceci permet de modifier un nombre fini de termes de la suite).

Exemple 3.1.2 Le théorème de Skolem-Mahler-Lech n'est cependant plus vérifié en caractéristique $p > 0$. Aux progressions arithmétiques et aux ensembles finis, il faut ajouter une nouvelle classes d'ensembles pathologiques appelés "p-nested sets" par Derksen [Der07]. En effet, le morphisme de Frobenius fait apparaître de nombreux contre-exemples au théorème de Skolem-Mahler-Lech énoncé en caractéristique nulle. On peut par exemple se placer sur le corps $\mathbb{F}_p(X)$ et considérer la suite a définie par :

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

Cette suite est bien récurrente linéaire, puisqu'elle est annulée par $(E - X - 1)(E - X)(E - 1)$ (cf définition 3.2.1). En outre, pour tout entier $k \in \mathbb{N}$, on a :

$$a(p^k) = X^{p^k} + 1 - X^{p^k} - 1 = 0$$

Si bien que $\mathcal{Z}(a) = \{1, p, p^2, p^3, \ldots\}$ à cause du (ou grâce au) morphisme de Frobenius. L'ensemble $\mathcal{Z}(a)$ n'est donc pas ultimement périodique.

3.2 Quelques propriétés des séries rationnelles

Détaillons quelques résultats sur les suites récurrentes linéaires, principalement tirés d'Everest, van der Poorten, Shparlinski, Ward [Eve+03] et de Derksen [Der07], afin de faciliter leur étude plus tard. Dans cette partie, on travaille sur un corps K quelconque, sauf mention contraire.

Définition 3.2.1 (Polynôme minimal d'une suite récurrente linéaire)
Soit K un corps quelconque. On définit sur l'espace $K^{\mathbb{N}}$ des suites à valeur dans K l'opérateur de translation :

$$E : \begin{cases} K^{\mathbb{N}} & \longrightarrow K^{\mathbb{N}} \\ (a_n)_{n\in\mathbb{N}} & \longmapsto (a_{n+1})_{n\in\mathbb{N}} \end{cases}$$

Soit $a \in K^{\mathbb{N}}$ récurrente linéaire. Par hypothèse il existe un polynôme $P \in K[X]$ tel que $P(E)(a) = 0$. On se donne donc $\mathcal{I}_a$ l'idéal des polynômes qui appliqués à E annulent a :

$$\mathcal{I}_a = \{P \in \mathbb{K}[X] \mid P(E)(A) = 0\}$$

et l'on s'en donne le générateur unitaire P_a, appelé le polynôme minimal de la suite récurrente linéaire a.

Exemple 3.2.2 Le polynôme minimal d'une suite périodique de période p première est le polynôme $X^p - 1$. En général, si une suite $a = (a(n))_{n\in\mathbb{N}}$ vérifie une relation de récurrence :

$$\gamma_0 a(n) + \cdots + \gamma_{d-1} a(n+d-1) = a(n+d)$$

et que l'on impose que d soit minimal, alors $P_a = X^d - \gamma_{d-1}X^{d-1} - \cdots - \gamma_0$.

Remarque. Soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire. Quitte à considérer la clôture algébrique de K, on peut supposer que P_a est scindé. On le décompose donc :

$$P_a(X) = \prod_{i=1}^{r}(X - \alpha_i)^{m_i}$$

où les α_i sont distincts. D'après le lemme des noyaux, on peut écrire :

$$\operatorname{Ker} P_a(E) = \bigoplus_{i=1}^{r} \operatorname{Ker}((E-\alpha_i)^{m_i})$$

Par conséquent, il existe des suites $b_i \in \operatorname{Ker}((E-\alpha_i)^{m_i})$, $i = 1, 2, \ldots, r$ telles que $a = b_1 + \cdots + b_r$.
En outre, chacune de ces suites b_i est par définition annulée par $(E-\alpha_i)^{m_i}$ et on peut montrer par récurrence que :

$$\forall n \in \mathbb{N},\ b_i(n) = \sum_{j=0}^{m_i-1} \binom{n}{j} \beta_{i,j} \alpha_i^n$$

pour des éléments $\beta_{i,j} \in K$ fixés et en utilisant la formule vérifiée pour tout entiers naturels m, n et $k \leqslant m$:

$$\sum_{j=0}^{m} \binom{n+j}{k} \binom{m}{j} (-1)^{m-j} = 0$$

Pour démontrer cette formule, on peut par exemple s'intéresser aux coefficient d'ordre k du polynôme $(X+1)^n X^m = (X+1)^n((X+1)-1)^m$, ou simplement demander à Dounia Darkaoui (dounia.darkaoui@ens-rennes.fr).
Si bien que l'on peut écrire :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{r} \sum_{j=0}^{m_i-1} \beta_{i,j} \binom{n}{j} \alpha_i^n \qquad (\star)$$

On remarque que si par exemple $\alpha_1 = 0$, la suite b_1 est nulle à partir d'un certain rang et n'affecte donc plus a.
En outre, s'il existe $i \neq j$ pour lesquels il existe un entier k tel que $\alpha_i^k = \alpha_j^k$, alors pour tout $t < k$:

$$b_i(kn+t) = \sum_{s=0}^{m_i-1} \beta_{i,s} \binom{n}{s} \alpha_i^t (\alpha_i^k)^n \quad \text{et} \quad b_j(kn+t) = \sum_{s=0}^{m_i-1} \beta_{j,s} \binom{n}{s} \alpha_j^t \underbrace{(\alpha_j^k)^n}_{=(\alpha_i^k)^n}$$

Si bien que quitte à modifier les $\beta_{i,j}$, on peut réécrire chacune des suites $(a(kn+t))_{n\in\mathbb{N}}$ sous la forme $(\star)$ avec $r-1$ au lieu de r, et l'ensemble de ces sous-suites forment en quelque sorte une partition de la suite a. Enfin, si P_a est à racines simples, c'est-à-dire que les m_i sont tous égaux à 1, on peut écrire plus simplement a sous la forme :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{r} \beta_i \alpha_i^n \qquad (\star\star)$$

où $\beta_1, \ldots, \beta_r \in K$.
On aboutit donc assez naturellement aux définitions suivantes.

Définition 3.2.3 (Suite basique, non-dégénérée, simple)
Soit a une suite récurrente linéaire et l'on considère P_a son polynôme minimal, que l'on suppose scindé, quitte à travailler sur la clôture algébrique de notre corps de base. On dit que a est :

i. basique si 0 n'est pas une racine de P_a.
ii. non-dégénérée si les racines de de P_a sont non nulles et telles que le quotient de deux racines distinctes n'est pas une racine de l'unité.
iii. simple si P_a est à racines simples.

Lemme 3.2.4 (Stabilité par sous-progression arithmétique)
Soit $j < k$ deux entiers naturels. On rappelle que l'endomorphisme T_j^k sur l'espace $K^{\mathbb{N}}$ des suites à valeurs dans K, est défini par :

$$\forall a \in K^{\mathbb{N}},\ \forall n \in \mathbb{N}, T_j^k a(n) = a(kn + j)$$

Soit $a \in K^{\mathbb{N}}$ récurrente linéaire d'ordre d. La suite $T_j^k a$ est récurrente linéaire d'ordre au plus d.

Preuve. Dans cette démontration et dans la suite, on notera $\mathrm{Res}_Y(P(Y), Q(Y))$ le résultant par rapport à la variable Y de P et Q.
Notons donc $Q_a(X) = \mathrm{Res}_Y(Y^k - X, P_a(Y))$ et $U_a(X) = \mathrm{Res}_Y(Y^{k-1} + Y^{k-2}X + \cdots + X^{k-1}, P_a(Y))$.
Au signe près, les polynômes $Q_a(X)$ et $U_a(X)$ sont unitaires de degrés respectifs au plus d et $d(k-1)$.
En effet, la variable X apparait d fois dans la matrice dont $Q_a(X)$ est le déterminant. En outre, on a :

$$Y^k - X^k = (Y - X)(Y^{k-1} + Y^{k-2}X + \cdots + X^{k-1})$$

Donc : $Q(X^k) = \mathrm{Res}_Y(Y^k - E^k, P_a(Y^k)) = \mathrm{Res}_Y(Y - E, P_a(Y)U_a(X) = P_a(X)U_a(X)$. En particulier, $U_a(X)$ est bien de degré au plus $d(k-1)$. Grâce à cette relation, on obtient :

$$Q_a(E)T_j^k a = T_j^k Q(E^k)a = T_j^k U_a(E)P_a(E)a = 0$$

où l'on utilisé le fait que $E \circ T_j^k = T_j^k \circ E^k$. Ceci prouve bien que $T_j^k a$ est récurrente linéaire d'ordre au plus d (qui majore le degré de Q).

✌

Remarque. Les T_j^k sont en quelque sorte les équivalents pour les suites des opérateurs de Cartier. On a démontré dans le lemme 2.2.1 que sur un corps fini, le p-noyau d'une série formelle était fini si et seulement son orbite sous Ω était finie. Or, le p-noyau n'est autre que l'orbite sous l'action du monoïde engendré par les T_j^p. Ainsi, dans les corps finis, si les T_j^k et les opérateurs de Cartier diffèrent techniquement, ils ne sont pas si éloignés moralement. On a d'ailleurs la relation suivante, pour une série formelle $f = \sum a(n)X^n$ sur un corps K de caractéristique p :

$$\sum_{n\in\mathbb{N}} (T_j^p a)(n)X^{pn} = \left(\sum_{n\in\mathbb{N}} a(pn + j)^{1/p} X^n\right)^p = \Lambda_j(f)^p$$

Maintenant que l'on a démontré que les suites récurrentes étaient stables par par passage aux T_j^k, on peut utiliser ces opérateurs pour "réduire" nos suites, comme on a commencé à le faire informellement plus tôt.

Théorème 3.2.5 (Réduction des suites récurrentes linéaires)
Soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire.

i. Il existe un entier i tel que $E^i a$ est basique.
ii. Si a est basique, alors il existe un entier naturel k tel que pour tout $0 \leqslant j < k$, la suite $T_j^k a$ est récurrente linéaire.
iii. Si de plus K est de caractéristique non nulle p, alors on peut choisir k tel que $T_j^k a$ est en outre simple pour tout entier $0 \leqslant j < k$.

Preuve.

i. Pour un certain entier i, on peut écrire $P_a(X) = X^i Q(X)$, où X ne divise pas Q. De sorte que $Q(E)E^i a = P_a(E)a = 0$, si bien que $E^i a$ est basique.

ii. Décomposons $P_a = P_a(X) = \prod_{i=1}^{r}(X-\alpha_i)^{m_i}$. Pour un certain entier k, tous les quotients α_i/α_j qui sont des racines de l'unité sont des racines k-ièmes de l'unité. De sorte qu'un polynôme dont les racines seraient parmi les $\alpha_1^k, \dots, \alpha_r^k$ vérifierait la condition de non-dégénérescence.
Le polynôme $Q_a(X) = \mathrm{Res}_Y(Y^k - X, P_a(Y))$ a pour racines les $\alpha_1^k, \dots, \alpha_r^k$, et donc les suites $T_j^k a,\ j = 0, 1, \dots, k-1$ (dont Q_a est un polynôme annulateur) sont non-dégénérées.

iii. Notons $\gamma_1, \dots, \gamma_s$ les éléments distincts de $\alpha_1^k, \dots, \alpha_r^k$ et donnons-nous $q \geqslant d$ une puissance de p. De sorte que si l'on pose $U(X) = \prod_{i=1}^{s}(X-\gamma_i^q)$, alors $U(X^q) = \prod_{i=1}^{r}(X^q-\gamma_i^q) = \prod_{i=1}^{r}(X-\gamma_i)^q$ est divisible par $Q_a(X)$ (c'est un polynôme de degré au plus d dont les racines sont les γ_i).
Or, $P_a(X)$ divise $Q(X^k)$ (d'après la démonstration du lemme précédent) et donc P_a divise $U(X^{qk})$. Par conséquent, pour tout entier $0 \leqslant j < qk$:

$$U(E)T_j^{qk}a = T_j^{qk}U(E^{qk})a = 0$$

Par définition de U, les suites $T_j^{qk}a$ sont donc simples et non-dégénérées.

✌

Outre la simplification algébrique de leur écriture, réduire une suite récurrente linéaire en une suite non-dégénéres permet en quelque sorte de maîtriser l'ensemble de ses zéros, et d'en retirer les classes d'ensembles "simples" comme les progressions arithmétiques, pour se concentrer sur les cas pathologiques. On appelle ces ensembles dont on veut se débarasser les ensembles équilibrés. Plus précsiément, un ensemble d-équilibré est un ensemble de la forme :

$$\{m_0 + \varepsilon_1 m_1 + \cdots + \varepsilon_d m_d \mid \varepsilon_1, \dots, \varepsilon_d \in \{0,1\}\}$$

Où $m_0 \in \mathbb{N}$ et $m_1, \dots, m_d \in \mathbb{N}^*$

Lemme 3.2.6
Soit $a \in K^{\mathbb{N}}$ une suite non-nulle récurrente linéaire d'ordre d.

i. Si K est de caractéristique nulle et si a est non-dégénérée, alors $\mathcal{Z}(a)$ ne contient pas d'ensemble $(d-1)$-équilibré.

ii. Si K est de caractéristique $p > 0$ et si a est simple et non-dégénérée, alors $\mathcal{Z}(a)$ ne contient pas d'ensemble $(d-1)$-équilibré.

Preuve. Dans un corps de caractéristique quelconque, supposons que

$$S = \{m_0 + \varepsilon_1 m_1 + \cdots + \varepsilon_{d-1} m_{d-1} \mid \varepsilon_1, \dots, \varepsilon_{d-1} \in \{0,1\}\} \subset \mathcal{Z}(a)$$

On décompose le polynôme minimal de a, $P_a = \prod_{i=1}^{d}(X-\alpha_i)$ et l'on pose $Q = X^{m_0}\prod_{i=1}^{d-1}(X^{m_1}-\alpha_i^{m_i})$.

Dans les cas i. et ii. pour $i < d$, le polynôme $X - \alpha_i$ ne divise pas $\frac{X^{m_i}-\alpha_i^{m_i}}{X-\alpha_i}$.
En effet, dans le cas i. si $\alpha_d^{m_i} = \alpha_i^{m_i}$, alors $\alpha_d = \alpha_i$ (on est en caractéristique nulle). Or, $X^{m_i} - \alpha_i$ a pour dérivée $m_i X^{m_i-1}$ et donc puisque 0 n'est pas racine de $X^{m_i} - \alpha_i$ (la suite a est basique), il est à racines simples. Par conséquent, α_d ne peut pas être racine de $\frac{X^{m_i}-\alpha_i^{m_i}}{X-\alpha_i}$.
Dans le cas ii. puisque la suite est simple et non-dégénérée, α_d/α_i n'est pas une racine de l'unité et donc $\alpha_d^{m_i} \neq \alpha_i^{m_i}$.

Le polynôme P_a divise donc $Q(X)(X-\alpha_d)$, mais ne divise pas $Q(X)$, puisque :

$$\frac{Q(X)}{P(X)} = \frac{1}{X-\alpha_d}X^{m_0}\prod_{i=1}^{d-1}\frac{X^{m_i}-\alpha_i^{m_i}}{X-\alpha_i}$$

On a $(E-\alpha_d)Q(E)a = 0$, c'est-à-dire que la suite $Q(E)a$ est annulée par $E-\alpha_d$. Donc il existe un élément $\beta \in K$ (quitte à l'augmenter) tel que $Q(E)a(n) = \beta\alpha_d^n$ pour tout entier n.
Si un entier i est tel que le coefficient d'ordre i de Q est non nul, c'est qu'il s'écrit sous la forme $i = m_0 + \varepsilon_1 m_1 + \cdots + \varepsilon_{d-1}m_d d - 1$ et donc qu'il appartient à S. Par hypothèse, on a donc $a(i) = 0$.
Or, $\beta = Q(E)a(0)$, et c'est donc une combinaison linéaire de $a(i), i \in S$. Par conséquent, $\beta = 0$, si bien que $Q(E)a = 0$, ce qui est impossible puisque P_a ne divise pas Q.

✌

3.3 Une première généralisation de Skolem-Mahler-Lech

3.3.1 Free frobenius spliting

Avant toute chose, nous allons énoncer et démontrer un lemme algébrique technique, à la base de ce que Derksen [Der07] appelle le "Free Frobenius splitting". Pour cela, on va travailler sur une extension finiment engendrée K de $\mathbb{F}_p$.
On rappelle que le corps $K^{\langle p\rangle}$ est le sous-corps de K correspondant à l'image de K par le morphisme de Frobenius. On a alors l'égalité : $[K : K^{\langle p\rangle}] \cdot [K^{\langle p\rangle} : \mathbb{F}_p] = [K : \mathbb{F}_p] < +\infty$, si bien que $\mathbb{F}_p \subset K^{\langle p\rangle} \subset K$ sont des extensions finies. On peut donc se donner une base $h_1, \ldots, h_m$ de K en tant que $K^{\langle p\rangle}$-espace vectoriel, de sorte que :

$$K = K^{\langle p\rangle}h_1 \oplus \cdots \oplus K^{\langle p\rangle}h_m$$

On peut donc définir $\pi_i : K \to K,\ i = 1, 2, \ldots, m$ par la relation :

$$\forall f \in K, f = \sum_{i=1}^{m} \pi_i(f)^p h_i$$

Cette relation n'est pas sans rappeler celle du point ii. du lemme 2.1.2 sur les opérateurs de Cartier. Cette fois-ci, on effectue le splitting sur K directement, plutôt que sur $K[[X]]$ (ou $K^{\mathbb{N}}$). Il est donc naturel de voir que l'on a la relation :

$$\forall f, g \in K, \pi_i(g^p f) = g\pi_i(f)$$

Lemme 3.3.1 (Une borne bien utile)
Soit V un sous $\mathbb{F}_p$-espace vectoriel de K de dimension finie n contenant 1. Pour tout entier l, on a l'inclusion :

$$V^l \subset (V^{\lfloor l/p\rfloor})^{\langle p\rangle} V^{n(p-1)}$$

où en général, pour deux sous-espace vectoriels de K, VW désigne l'espace engendré par les $vw, v \in v, w \in W$.

Preuve. Donnons-nous $(e_1, \ldots, e_n)$ une base de V. Puisque V contient 1, l'espace V^l est engendré par les produits finis d'au plus l élements e_i. Soit $f = e_1^{a_1} \cdots e_n^{a_n}$ un de ces générateurs, avec donc $a_1 + \cdots + a_n \leqslant l$. Pour tout $1 \leqslant i \leqslant n$, on peut décomposer $a_i = pb_i + c_i$ avec $b_i \in \mathbb{N}$ et $0 \leqslant c_i < p$. Par conséquent :

$$f = (\underbrace{e_1^{b_1} \cdots e_n^{b_n}}_{=\, u \,\in\, V^{\lfloor l/p\rfloor}})^p \cdot (\underbrace{e_1^{c_1} \cdots e_n^{c_n}}_{=\, v \,\in\, V^{n(p-1)}}) \in (V^{\lfloor l/p\rfloor})^{\langle p\rangle} V^{n(p-1)}$$

En effet, il est clair que $\sum c_i \leqslant n(p-1)$ et puisque $p\sum b_i = \sum a_i - \sum c_i \leqslant l$, on a bien $\sum b_i \leqslant \lfloor l/p\rfloor$.
À noter que si l'on n'avait pas supposé que $1 \in V$, il aurait fallut s'assurer que ces inégalités soient des égalités, ce qui ne semble pas réalisable.

✌

Nous sommes maintenant près à énoncer et démontrer le lemme à la base du "free Frobenius splitting".

Lemme 3.3.2 (Derksen)
Soit V un sous $\mathbb{F}_p$-espace vectoriel de K de dimension finie. Il existe $V \subset W \subset K$ un sous $\mathbb{F}_p$-espace vectoriel de dimension finie tel que :

$$\forall 1 \leqslant i \leqslant m,\ \pi_i(VW) \subset W$$

Preuve. On va tout d'abord chercher à augmenter l'espace V pour travailler plus facilement par la suite.
Quitte à augmenter V en un espace V', on peut supposer que V contient $1, h_1, \dots, h_m$ ainsi que les générateurs de K en tant sur-corps de $\mathbb{F}_p$. En effet, si l'on démontre que l'on a un espace de dimension finie W contenant V' (qui est lui-même bien de dimension finie) tel que pour tout i, $\pi_i(V'W) \subset W$ alors on a $V \subset V' \subset W$ et les inclusions :

$$\pi_i(VW) \subset \pi_i(V'W) \subset W$$

pour $i = 1, 2, \dots, m$. Le fait que V contienne 1 implique qu'en général, $V^l \subset V^{l+1}$ (ce qui ne serait pas vrai sinon), inclusion dont nous nous servirons de nombreuses fois par la suite. Donnons-nous maintenant A l'anneau engendré par V. Puisque V contient les h_i, on a l'inclusion de $A^{\langle p \rangle}$-modules suivante :

$$A^{\langle p \rangle} h_1 \oplus \cdots \oplus A^{\langle p \rangle} h_m \subset A$$

En outre, V (et donc A également) engendrent K en tant que $\mathbb{F}_p$-espace vectoriel. Par conséquent, tout élément de K s'écrit comme un produit fini d'éléments de A et d'inverses (dans K) d'éléments de A. Ainsi, pour tout élément $h \in K$, il existe un élément $g \in A$ tel que $gh \in A$. On va utiliser ce fait pour montrer que le $A^{\langle p \rangle}$-module $M = A/(A^{\langle p \rangle} h_1 \oplus \cdots \oplus A^{\langle p \rangle} h_m)$ est un module de torsion.

Soit $f \in A$. Puisque $A \subset K$, on a l'égalité $f = \sum_{i=1}^{m} \pi_i(f)^p h$. Or, pour tout $1 \leqslant i \leqslant m$, il existe un élément $g_i \in A$ tel que $\pi_i(f) g_i \in A$. Si l'on pose $g = g_1 \cdots g_m$, on obtient que $g^p f \in A^{\langle p \rangle} h_1 \oplus \ldots \oplus A^{\langle p \rangle} h_m$. Par conséquent, en considérant un tel élément de A pour chaque générateur de A en tant que $A^{\langle p \rangle}$-module (qui sont en nombre fini par hypothèse) et en considérant leur produit, on dispose d'un élément $g \in A$ tel que pour tout $f \in A$, $g^p f \in A^{\langle p \rangle} h_1 \oplus \cdots \oplus A^{\langle p \rangle} h_m$. C'est bien ce que l'on recherchait.
Ainsi, si l'on localise A par rapport à g (ce qui revient à localiser par rapport à g^p), on obtient :

$$A_g = A_{g^p} = (A_g)^{\langle p \rangle} h_1 \oplus \ldots \oplus (A_g)^{\langle p \rangle} h_m$$

De même que précédemment, on peut supposer que V contient g^{-1}. Par ce que l'on vient de montrer, cela implique que $A = A_g$ et donc que l'on a l'égalité de $A^{\langle p \rangle}$-modules :

$$A^{\langle p \rangle} h_1 \oplus \cdots \oplus A^{\langle p \rangle} h_m = A$$

On a désormais le bon espace vectoriel V pour attaquer pour de bon la preuve. D'après le lemme 3.3.1, si n est la $\mathbb{F}_p$-dimension de V, on a pour tout entier l l'inclusion :

$$V^l \subset (V^{\lfloor l/p \rfloor})^{\langle p \rangle} V^{n(p-1)}$$

Notons maintenant $(e_1, \dots, e_n)$ une base de V. Par définition, l'espace $V^{n(p-1)}$ est engendré par les $e_1^{k_1} \cdots e_n^{k_n}$, avec $\sum k_i = n(p-1)$.

Notons $\underline{k} = (k_1, \dots, k_n)$. On écrit : $e_1^{k_1} \cdots e_n^{k_n} = \sum_{i=1}^{m} \pi_i(e_1^{k_1} \cdots e_n^{k_n})^p h_i$. Or, $\pi_i(e_1^{k_1} \cdots e_n^{k_n})$ est un élément de $A = A^{\langle p \rangle} h_1 \oplus \cdots \oplus A^{\langle p \rangle} h_m$. C'est donc un élément de $V^{C_{i,\underline{k}}}$ pour une certaine constante $C_{i,\underline{k}}$. C'est le cas, car V engendre A (en tant qu'anneau), donc tout élément de A est contenu dans un V^l.
Ainsi, si l'on considère $C = \max_{i,\underline{k}} C_{i,\underline{k}}$, on a l'inclusion :

$$V^{n(p-1)} \subset (V^C)^{\langle p \rangle} h_1 \oplus \cdots \oplus (V^C)^{\langle p \rangle} h_m$$

Ainsi, on obtient :

$$V^l \subset (V^{\lfloor l/p \rfloor})^{\langle p \rangle} V^{n(p-1)} \subset (V^{\lfloor l/p \rfloor + C})^{\langle p \rangle} h_1 \oplus \ldots \oplus (V^{\lfloor l/p \rfloor + C})^{\langle p \rangle} h_m$$

Si l'on trouve un entier l tel que :

$$V^l \subset (V^{l-1})^{\langle p \rangle} h_1 \oplus \ldots \oplus (V^{l-1})^{\langle p \rangle} h_m$$

Alors en considérant $W = V^{l-1}$, on aura bien $V \subset W$ et $\pi_i(VW) = \pi_i(V^l) \subset V^{l-1} = W$, ce qui concluera la preuve.
Étant donné le travail que l'on a déjà fourni, il parait naturel de chercher un entier l tel que $l - 1 \geqslant \lfloor l/p \rfloor + C$. Il suffit donc de considérer $l \geqslant l/p + C + 1$, *i.e.* $l \geqslant p(C+1)/(p-1)$.

✌

3.3.2 Un premier théorème de Derksen

Nous allons dans cette section démontrer le théorème suivant, du à Derksen [Der07]. C'est une première étape vers la généralisation du théorème de Skolem-Mahler-Lech en caractéristique p.

Théorème 3.3.3 (Derksen)
Soit K une extension finiment engendrée de $\mathbb{F}_p$ et $a \in K^{\mathbb{N}}$ une suite récurrente linéaire. L'ensemble $\mathcal{Z}(a)$ est p-automatique.

Preuve. En utilisant le théorème 3.2.5, le résultat n'a besoin d'être démontré que pour les suites simples, basiques et non-dégénérées. En effet, un ensemble reste p-automatique quitte à en modifier un nombre fini de termes, donc on peut la supposer basique. De plus, pour tout entier $k \geqslant 2$, un ensemble S est p-automatique si et seulement si les ensembles $(L_j^k)^{-1}S$, $j = 0, 1, \ldots, k-1$ le sont, donc puisque l'on travaille en caractéristique p, on peut supposer que a est simple et non-dégénérée.

On écrit donc : $\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$, avec les $\alpha_i, \beta_i \in K\backslash\{0\}$, quitte à augmenter K.

Tout d'abord, on se ramène au cas où K une extension finiment engendrée sur $\mathbb{F}_p$. En effet, a est toujours une suite récurrente linéaire basique, simple et non-dégénérée sur le sous-corps K_0 de K engendré par les β_i et les α_i, donc quitte à remplacer K par K_0, on peut supposer que K est finiment engendré sur $\mathbb{F}_p$.

Considérons maintenant le sous $\mathbb{F}_p$-espace vectoriel de K suivant, qui est de dimension finie :

$$V = \mathrm{Vect}_{\mathbb{F}_p}\left\{\alpha_i^j, \beta_i \in K \mid 1 \leqslant i \leqslant d, 0 \leqslant j < p\right\}$$

Soit W l'espace vectoriel donné par le lemme 3.3.2 appliqué à V. Notons a_i la suite $(\alpha_i^n)_{n\in\mathbb{N}}$, de sorte que $a = \sum_{i=1}^{d} \beta_i a_i$. D'une façon similaire au théorème de Sharif et Woodcock, on veut un espace vectoriel contenant a qui soit de dimension finie et ayant de bonnes propriétés de stabilité. On s'intéresse donc à l'espace :

$$U = Wa_1 + Wa_2 + \cdots + Wa_d$$

En étendant la définition des π_i aux suites (en les appliquant coordonnée par coordonnée), pour tout $1 \leqslant i \leqslant m$ et $0 \leqslant j < p$, on a l'inclusion : $\pi_i(T_j^p U) \subset U$. En effet, pour tout $1 \leqslant k \leqslant d$:

$$\pi_i T_j^p(Wa_k) = \pi_i(W \cdot (\alpha_k^{pn+j})_{n\in\mathbb{N}}) = \pi_i(W \underbrace{\alpha^j}_{\in V} \cdot ((\alpha^n)_{n\in\mathbb{N}})^p) \subset \pi_i(WV)a_k \subset Wa_k$$

Considérons maintenant $\mathcal{W}$ la collection des ensembles de la forme :

$$\bigcap_{i=1}^{r} \mathcal{Z}(b_i)$$

où r décrit $\mathbb{N}$ et les b_i décrivent U. L'ensemble $\mathcal{Z}(a)$ appartient trivialement à $\mathcal{W}$, puisque $a \in U$ et $\mathcal{W}$ est fini, car U l'est (l'espace W est un $\mathbb{F}_p$ espace vectoriel de dimension finie). Donc si l'on parvient à montrer que $\mathcal{W}$ est stable par les $(L_i^p)^{-1}$, il en résultera que $\mathcal{Z}(a)$ est p-automatique.

Soit $S = \bigcap_{j=1}^{r} \mathcal{Z}(b_j) \in \mathcal{W}$ et $0 \leqslant i < p$. On écrit :

$$(L_i^p)^{-1}(\mathcal{Z}(b_j)) = \mathcal{Z}(T_i^p b_j) = \bigcap_{k=1}^{m} \mathcal{Z}(\underbrace{\pi_k(T_i^p b_j)}_{\in U}) \in \mathcal{W}$$

En effet, un élément de K est nul si et seulement si ses projections selon les π_k sont toutes nulles. Par conséquent, puisque $\mathcal{W}$ est stable par intersection finie, on obtient :

$$(L_i^p)^{-1}S = \bigcap_{j=1}^{r} (L_i^p)^{-1}\mathcal{Z}(b_j) \in \mathcal{W}$$

Cela conclue la preuve !

3.3.3 Extension aux séries algébriques

À partir d'une reformulation du théorème de Sharif et Woodcock [SW88], Adamczewski et Bell [AB12] ont étendu le théorème 3.3.3 de Derksen aux séries algébriques en plusieurs variables, en utilisant à nouveau le free Frobenius splitting.

Théorème 3.3.4 (Une reformulation du théorème de Sharif et Woodcock)
Soit K un corps parfait de caractéristique p et une suite d-dimensionnelle $a \in K^{\mathbb{N}^d}$ telle que la série formelle f à d indéterminées dont les coefficients forment la suite a est algébrique sur $K(\boldsymbol{X})$.
Il existe un entier naturel m et des suites d-dimensionelles $a_1, \dots, a_m$ sur K telles que :

i. Les séries formelles $f_i = \sum_{\boldsymbol{n} \in \mathbb{N}^d} a_i(\boldsymbol{n}) \boldsymbol{X}^{\boldsymbol{n}}$, $i = 1, 2, \dots, m$ forment une base de $\mathrm{Vect}_K\, \Omega(f)$.

ii. $f_1 = f$

iii. Si une suite d-dimensionnelle b sur K est telle que la série formelle correspondante g appartient à $\mathrm{Vect}_K\, \Omega(f)$, alors pour tout $\boldsymbol{j} \in \{0, 1, \dots, p-1\}^d$, $T^p_{\boldsymbol{j}} b \in K a_1^p + \cdots + K a_m^p$.

Preuve. Puisque f est algébrique, le théorème 2.1.4 nous indique que $\mathrm{Vect}_K\, \Omega(f)$ est de dimension finie. Par conséquent, il existe des suites d-dimensionnelles $a_1, \dots, a_m$ sur K telles que les séries correspondantes $f_1, \dots, f_m$ forment une base de $\mathrm{Vect}_K\, \Omega(f)$ et on peut imposer que $f_1 = f$. Soit maintenant b une suite d-dimensionnelle sur K telle que la série formelle correspondante g appartient à $\mathrm{Vect}_K\, \Omega(f)$. On peut écrire :

$$g(\boldsymbol{X}) = \sum_{\boldsymbol{j} \in \{0, \dots, p-1\}^d} \boldsymbol{X}^{\boldsymbol{j}} \Lambda_{\boldsymbol{j}}(g(\boldsymbol{X}))^p$$

Puisque $g \in \mathrm{Vect}_K(\Omega(f))$, qui est stable par les opérateurs de Cartier, $\Lambda_{\boldsymbol{j}}(g(\boldsymbol{X})) \in K f_1 + \cdots + K f_m$ et donc $\Lambda_{\boldsymbol{j}}(g(\boldsymbol{X}))^p \in K f_1^p + \cdots + K f_m^p$. Or, pour $\boldsymbol{j} \in \{0, \dots, p-1\}^d$ et $\boldsymbol{n} \in \mathbb{N}^d$, le coefficient d'ordre $p\boldsymbol{n}$ de $\Lambda_{\boldsymbol{j}}(g(\boldsymbol{X}))^p$ est égal à $T^p_{\boldsymbol{j}} b(\boldsymbol{n})$, si bien que :

$$T^p_{\boldsymbol{j}} b(\boldsymbol{n}) \in K a_1(\boldsymbol{n})^p + \cdots + K a_m(\boldsymbol{n})^p$$

Ce qui conclue la preuve.

Théorème 3.3.5 (Adamczewski et Bell)
Soit K un corps de caractéristique $p > 0$ et $f \in K[[\boldsymbol{X}]]$ une série formelle d-dimensionnelle algébrique. L'ensemble $\mathcal{Z}(f) \subset \mathbb{N}^d$ est p-automatique.

Preuve. La preuve est très proche de la preuve initiale de Derksen et se base sur le lemme 3.3.2. Considérons tout d'abord des suites $a_1, \dots, a_m \in K^{\mathbb{N}^d}$, telles que décrites dans le théorème 3.3.4. D'après la propriété iii. pour tout $1 \leqslant i \leqslant m$ et $\boldsymbol{j} \in \{0, \dots, p-1\}^d$, il existe des éléments $\lambda(i, \boldsymbol{j}, k), k = 1, \dots, m$ tel que :

$$T^p_{\boldsymbol{j}} a_i = \sum_{k=1}^{m} \lambda(i, \boldsymbol{j}, k) a_k^p$$

On peut se ramene au cas où K est une extension finiment engendré de $\mathbb{F}_p$. En effet, si K_0 est le sous-corps de K engendré par les coefficients des $f_1, \dots, f_m$ et par les $\lambda(i, \boldsymbol{j}, k)$, alors K_0 est finiment engendrée sur $\mathbb{F}_p$. C'est le cas puisque, $f_1, \dots, f_m$ étant algébriques sur $K(\boldsymbol{X})$, leurs coefficients sont contenus dans

une extension finiment engendrée de $\mathbb{F}_p$. Donc quitte à remplacer K_0 par K, on peut supposer que K est finiment engendré sur $\mathbb{F}_p$.
Considérons maintenant le sous $\mathbb{F}_p$-espace vectoriel de K suivant, qui est de dimension finie suivant :

$$V = \mathrm{Vect}_{\mathbb{F}_p}\left\{1, \lambda(i, \boldsymbol{j}, k) \in K \mid 1 \leqslant i, k \leqslant m, \boldsymbol{j} \in \{0, \dots, p-1\}^d\right\}$$

Soit W l'espace vectoriel donné par le lemme 3.3.2 appliqué à V. On intrdoduit l'espace suivant :

$$U = Wa_1 + Wa_2 + \cdots + Wa_m$$

Cet espace contient $a = 1 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_m$ (et en général, il contient les a_j). De plus, pour tout $1 \leqslant i \leqslant m$ et $\boldsymbol{j} \in \{0, \dots, p-1\}^d$, on a l'inclusion : $\pi_i(T_{\boldsymbol{j}}U) \subset U$. En effet, pour tout $1 \leqslant k \leqslant d$, $T^p_{\boldsymbol{j}} a_k \in Va_1^p + \cdots + Va_m^p$ et donc :

$$\begin{aligned}\pi_i T^p_{\boldsymbol{j}}(Wa_k) &\subset \pi_i(WVa_1^p + \cdots + WVa_m^p) \\ &\subset \pi_i(WV)a_1^p + \cdots + \pi_i(WV)a_m^p \subset Wa_1 + \cdots + Wa_m = U\end{aligned}$$

Considérons maintenant $\mathcal{W}$ la collection des ensembles de la forme :

$$\bigcap_{i=1}^{r} \mathcal{Z}(b_i)$$

où r décrit $\mathbb{N}$ et les b_i décrivent U. L'ensemble $\mathcal{Z}(a)$ appartient trivialement à $\mathcal{W}$, puisque $a \in U$ et $\mathcal{W}$ est fini, car U l'est (l'espace W est un $\mathbb{F}_p$ espace vectoriel de dimension finie). Donc si l'on parvient à montrer que $\mathcal{W}$ est stable par les $(L^p_{\boldsymbol{i}})^{-1}$, il en résultera que $\mathcal{Z}(a)$ est p-automatique.
Soit $S = \bigcap_{j=1}^{r} \mathcal{Z}(b_j) \in \mathcal{W}$ et $0 \leqslant i < p$. On écrit :

$$(L^p_{\boldsymbol{i}})^{-1}(\mathcal{Z}(b_j)) = \mathcal{Z}(T^p_{\boldsymbol{i}} b_j) = \bigcap_{k=1}^{m} \mathcal{Z}(\underbrace{\pi_k(T^p_{\boldsymbol{i}} b_j)}_{\in U}) \in \mathcal{W}$$

En effet, un élément de K est nul si et seulement si ses projections selon les π_k sont toutes nulles. Par conséquent, puisque $\mathcal{W}$ est stable par intersection finie, on obtient :

$$(L^p_{\boldsymbol{i}})^{-1} S = \bigcap_{j=1}^{r} (L^p_{\boldsymbol{i}})^{-1} \mathcal{Z}(b_j) \in \mathcal{W}$$

Ce qui conclue la preuve.

Remarque. Ce théorème généralise à la fois le théorème de Derksen (théorème 3.3.3) et le sens direct du théotrème de Christol (théorème 2.2.2).
Pour le théorème de Derksen, il s'agit simplement de remarquer qu'une série rationelle est en particulier algébrique.
Pour le théorème de Christol, si $f(\boldsymbol{X})$ est une série algébrique sur un corps fini $\mathbb{F}_q$, on a montré que les ensembles $\mathcal{Z}(f(\boldsymbol{X}) - \lambda/(1 - \boldsymbol{X}))$, λ décrivant $\mathbb{F}_q$ sont p-automatiques. Leurs suites caractéristiques χ_λ le sont donc aussi, si bien que la suite $\sum_{\lambda \in K} \lambda \chi_\lambda$ est p-automatique. C'est exactement la suite des coefficients de f.

3.4 Une généralisation plus fine de Skolem-Mahler-Lech

Dans la suite, nous nous baserons principalement sur l'article [Der07] de Harm Derksen.

3.4.1 Propriété de l'automate d'un ensemble de zéros

On commence par observer un certain nombre de propriétés de l'automate produisant un ensemble de la forme $\mathcal{Z}(a)$, avec a une suite récurrente linéaire. Plus précisément, on va s'intéresser à l'automate construit à partir du p-noyau de $\mathcal{Z}(a)$. Rigoureusement, ses états sont les $(\chi(p^r n + j))_{n\in\mathbb{N}}$, où χ est la suite caractéristique de $\mathcal{Z}(a)$, mais on va les remplacer par les ensembles $(L_j^{p^r})^{-1}\mathcal{Z}(a)$ pour simplifier notre écriture.
Pour une suite récurrente linéaire simple et non dégénérée a, on définit le niveau $\ell(\mathcal{Z}(a))$ de $\mathcal{Z}(a)$ comme le plus petit entier naturel d tel que l'on peut écrire :

$$\mathcal{Z}(a) = \mathcal{Z}(b_1) \cap \mathcal{Z}(b_2) \cap \ldots \cap \mathcal{Z}(b_r)$$

où $b_1, \ldots, b_r \in K^{\mathbb{N}}$ sont des suites récurrentes linéaires simples et non-dégénérées d'ordre au plus d.
Le niveau de $\mathbb{N} = \mathcal{Z}(0)$ est 0, tandis que le niveau de $\varnothing = \mathcal{Z}(1)$ est 1. Si $\mathcal{Z}(a) \neq \varnothing, \mathbb{N}$, alors $\ell(Z(a)) \geqslant 2$, puisqu'une suite récurrente d'ordre au plus 1 est de la forme $(\gamma_0^n)_{n\in\mathbb{N}}$ (et son ensemble de zéros est donc soit $\varnothing$, soit $\mathbb{N}$).
Puisque les états de l'automate produisant a sont eux-même des ensembles de zéros de suites récurrentes linéaires (on a $(L_j^k)^{-1}\mathcal{Z}(a) = \mathcal{Z}(T_j^k a)$ et $T_j^k a$ est récurrente linéaire), on peut s'intéresser aux relations entre les niveaux des états.

Lemme 3.4.1
Soit K un corps de caractéristique $p > 0$ et soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire simple, non-dégénérée et non nulle d'ordre d. Soit $\mathcal{A}$ l'automate construit à partir du p-noyau de S.

i. Soient $Q, R \in \mathcal{N}_p(\mathcal{Z}(a))$. S'il existe un chemin dans $\mathcal{A}$ de Q à R, alors $\ell(Q) \geqslant \ell(R)$.
ii. Soient $Q, R \in \mathcal{N}_p(\mathcal{Z}(a))$ tel que $\ell(Q) \geqslant 2$. S'il existe dans $\mathcal{A}$ deux chemins distincts de Q à R de même longueur, alors $\ell(Q) > \ell(R)$.
iii. $\mathbb{N}$ n'est pas un état de l'automate $\mathcal{A}$.

Preuve. Écrivons $Q = \bigcap_{i=1}^{s} \mathcal{Z}(b_i)$, avec $b_1, \ldots, b_s$ sont des suites récurrentes linéaires simples non-dégénérées d'ordre au plus $d = \ell(Q)$.

i. Supposons qu'il existe un chemin dans $\mathcal{A}$ de Q à R. Ainsi, $R = (L_j^{p^r})^{-1}Q$ pour des entiers naturels r et $j < p^r$. Par conséquent, on a :

$$R = (L_j^{p^r})^{-1}\left(\bigcap_{i=1}^{s} \mathcal{Z}(b_i)\right) = \bigcap_{i=1}^{s} (L_j^{p^r})^{-1} Z(b_i) = \bigcap_{i=1}^{s} \mathcal{Z}(T_j^{p^r} b_i)$$

Et donc, d'après le lemme 3.2.4, le niveau $\ell(R)$ de R est bien inférieur ou égal à $\ell(Q)$.

ii. Supposons qu'il existe deux chemins distincts dans $\mathcal{A}$ de Q à R, de même longueur r. Dès lors, pour deux entiers $j, k \leqslant p^r$, on a $R = (L_j^{p^r})^{-1}Q = (L_k^{p^r})^{-1}Q$. Par conséquent, on a :

$$R = \bigcap_{i=1}^{s} \mathcal{Z}(T_j^{p^r} b_i) \quad \text{et} \quad R = \bigcap_{i=1}^{s} \mathcal{Z}(T_k^{p^r} b_i)$$

En intersectant R avec lui-même on obtient :

$$R = \bigcap_{i=1}^{s} \left(\mathcal{Z}(T_j^{p^r} b_i) \cap \mathcal{Z}(T_k^{p^r} b_i)\right)$$

On souhait maintenant écrire chaque intersection $\mathcal{Z}(T_j^{p^r} b_i) \cap \mathcal{Z}(T_k^{p^r} b_i)$ comme l'intersection des zéros de suites récurrentes linéaires d'ordre au plus $d-1$, ce qui achèvera de montrer que $\ell(R) \leqslant d - 1 < d = \ell(Q)$. Pour cela, démontrons le résultat suivant.

Lemme 3.4.2
Soit a une suite récurrente linéaire simple et non-dégénérée d'ordre $d \geqslant 2$. Si r est un entier naturel et $j, k < p^r$ sont deux entiers naturels distincts, alors il existe deux suites b et c récurrentes linéaires d'ordre au plus $d-1$ telles que :

$$\mathcal{Z}(T_j^{p^r} a) \cap \mathcal{Z}(T_k^{p^r} a) = \mathcal{Z}(b) \cap \mathcal{Z}(c)$$

Preuve. Puisque a est simple et non-dégérénrée, il existe des éléments $\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d \in K$ tels que :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

Par conséquent,

$$\forall n \in \mathbb{N},\ T_j^{p^r} a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^j (\alpha_i^{p^r})^n \quad \text{et} \quad T_k^{p^r} a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^k (\alpha_i^{p^r})^n$$

Puisque $d \geqslant 2$, on peut définir $b = \alpha_1^k T_j^{p^r} a - \alpha_1^j T_k^{p^r} a$ et $c = \alpha_2^k T_j^{p^r} a - \alpha_2^j T_k^{p^r} a$. Si bien que b et c sont d'ordre au plus $d-1$ (on a pour chacune d'entre elles annulé une des composantes de la suite a). En outre, on l'égalité suivante :

$$\forall n \in \mathbb{N},\ \begin{pmatrix} b(n) \\ c(n) \end{pmatrix} = \begin{pmatrix} \alpha_1^k & -\alpha_1^j \\ \alpha_2^k & -\alpha_2^j \end{pmatrix} \begin{pmatrix} T_j^{p^r} a(n) \\ T_k^{p^r} a(n) \end{pmatrix}$$

Et :

$$\det \begin{pmatrix} \alpha_1^k & -\alpha_1^j \\ \alpha_2^k & -\alpha_2^j \end{pmatrix} = -\alpha_1^k \alpha_2^j + \alpha_2^k \alpha_1^j$$

Ce déterminant est non, nul car a est non-dégénérée et donc (α_1/α_2) n'est pas une racine de l'unité. En particulier, puisque $k \neq j$, $(\alpha_1/\alpha_2)^{k-j} \neq 1$. Par conséquent, le vecteur ${}^t\begin{pmatrix} b(n) & c(n) \end{pmatrix}$ s'annule si et seulement si le vecteur ${}^t\begin{pmatrix} T_j^{p^r} a(n) & T_k^{p^r} a(n) \end{pmatrix}$ s'annule. Ainsi :

$$\mathcal{Z}(T_j^{p^r} a) \cap \mathcal{Z}(T_k^{p^r} a) = \mathcal{Z}(b) \cap \mathcal{Z}(c)$$

✌

La démonstration de ce lemme conclue la démonstration du point ii.

iii. Si $\mathbb{N}$ est un état de $\mathcal{A}$, alors c'est qu'il existe un entier r et un entier $j < p^r$ tel que $\mathbb{N} = (L_j^r)^{-1} \mathcal{Z}(a)$. Par conséquent, $\mathcal{Z}(a)$ contient l'ensemble $p^r\mathbb{N} + j$, ce qui contredit le lemme 3.2.6.

✌

Montrons maintenant un résultat sur la structure même de l'automate donné par le p-noyau des zéros d'une suite récurrente linéaire, simple et non-dégénérée.

Lemme 3.4.3
Soit a une suite récurrente linéaire, simple et non-dégénérée. Notons $\mathcal{A}$ l'automate donné par le p-noyau de $\mathcal{Z}(a)$.
Un état Q est dit cyclique s'il existe un mot w non trivial (c'est-à-dire non vide) tel que $\delta(Q, w) = Q$.
Soit Q un état cyclique non vide. Il existe un mot w_0 tel que pour mot w, si $\delta(Q, w) = Q$, alors il existe un entier k tel que $w = w_0^k$. Ce mot w_0 est appelé le cycle élémentaire de Q.

Preuve. Considérons tout d'abord w_0 un mot longueur minimale tel que $\delta(Q, w_0) = Q$. Considérons u un mot tel que $\delta(Q, u) = Q$ et écrivons $u = y w_0^r$, où y est un mot dont w_0 n'est pas suffixe. Supposons par l'absurde que $y \neq \varepsilon$.
Posons $m = |w_0|$ et $n = |y|$. Les mots w_0^n et y^m sont donc de même longueur et étiquettent tout deux des chemins de Q vers lui-même. Or, on a trivialement $\ell(Q) = \ell(Q)$, donc d'après la réciproque du point ii. du lemme 3.4.1, on a nécessairement $w_0^n = y^m$. Par hypothèse sur w_0, le mot y est plus long que w_0, et donc w_0 est un suffixe de y, contradiction.

✌

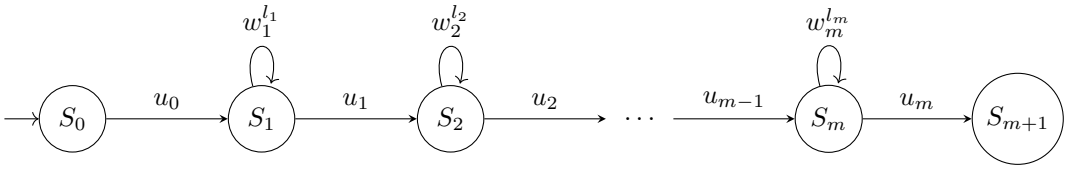
Nous sommes à présents prêts pour caractériser plus finement la forme que prend l'ensemble des zéros d'une suite récurrente linéaire. Dans la suite, on considérera les ensembles de la forme :

$$U_p(u_0, \dots, u_m; w_1, \dots, w_m) = \left\{ [u_m w_m^{k_m} u_{m-1} w_{m-1}^{k_{m-1}} \cdots u_1 w_1^{k_1} u_0]_p \in \mathbb{N} \mid k_1, \dots, k_m \in \mathbb{N} \right\}$$

où $u_0, \dots, u_m, w_1, \dots, w_m$ sont des mots sur l'alphabet $\{0, \dots, p-1\}$.

Théorème 3.4.4 (Derksen)
Soit K un corps de caractéristique $p > 0$ et $a \in K^{\mathbb{N}}$ une suite récurrente linéaire simple et non-dégénérée d'ordre d. L'ensemble $\mathcal{Z}(a)$ est une union finie d'ensembles de la forme $U_p(u_0, \dots, u_m; w_1, \dots, w_m)$, avec $m \leqslant d-1$.

Preuve. Soit $n \in \mathcal{Z}(a)$ et $w = \langle n \rangle_p$. Dans l'automate $\mathcal{A}$ donné par le p-noyau de $\mathcal{Z}(a)$, notons $Q = \delta(\mathcal{Z}(a), w)$ l'état auquel on aboutit en donnant n en entrée.
Puisque $n \in \mathcal{Z}(a)$, on a $\tau(Q) = 1$. Or, si $Q = (L_j^{p^r})^{-1}\mathcal{Z}(a)$ pour $r \in \mathbb{N}, j < p^r$, d'après la cinstruction de $\mathcal{A}$, on a $1 = \tau(Q) = \chi_{\mathcal{Z}(a)}(j)$, si bien que $0 \in (L_j^{p^r})^{-1}\mathcal{Z}(a) = Q$. En particulier, $Q \neq \varnothing$. Puisqu'en outre $Q \neq \mathbb{N}$, il advient que $\ell(Q) \geqslant 2$.
Maintenant, dans le chemin étiquetté par w et partant de $S_0 = \mathcal{Z}(a)$, notons (s'il existe) S_1 le premier sommet cyclique depuis lequel il n'existe pas de chemin jusqu'à S_0. En général, on note S_j le premier sommet cyclique apparaissant dans le chemin après S_{j-1} depuis lequel il n'existe pas de chemin jusqu'à S_{j-1}. De sorte que l'on défini $S_1, \dots, S_m$ de cette manière (le nombre de tels états est fini, puisque le nombre d'états de $\mathcal{A}$ est fini et que l'on considère des états nécessairement distincts) et l'on note $Q = S_{m+1}$. Pour $0 < j < m+1$, notons w_j le cycle élémentaire de S_j, de sorte que l'on a décomposé le chemin étiquetté par w sous la forme suivante :



où les u_i sont des mots sur l'alphabet $\{0, \dots, p-1\}$ et les l_i sont des entiers naturels (éventuellement nuls). Il est à noter que les chemins étiquettés par les u_i et partant de S_i passent par des sommets distincts.
On peut donc écrire $w = u_m w_m^{l_m} u_{m-1} w_{m-1}^{l_{m-1}} \cdots u_1 w_1^{l_1} u_0$ et donc $n \in U_p(u_0, \dots, u_m; w_1, \dots, w_m)$. On va maintenant montrer que m est majoré par $d-1$. On obtiendra alors que $\mathcal{Z}(a)$ s'écrit comme une union finie d'ensembles de la forme $U_p(u_0, \dots, u_m; w_1, \dots, w_m)$. En effet, il existe un nombre fini de mots tels que les u_i qui étiquettent un chemin passant par des sommets distincts (le nombre de sommets est fini dans $\mathcal{A}$, et le nombre de chemin sans cycles est donc lui aussi borné). De même, il existe un nombre fini de mots étiquettant un cycle élémentaire, plus précisément au plus autant que de sommets. Par conséquent, si d est majoré, il existe un nombre fini d'ensembles de la forme $U_p(u_0, \dots, u_m; w_1, \dots, w_m)$ tel qu'on l'a construit.
Montrons donc que $m \leqslant d-1$. Dans la construction précédente, on considère $0 < j < m+1$. Les mots $w_j^{|w_{j+1}|}u_j$ et $u_j w_{j+1}^{|w_j|}$ étiquettent chacun un chemin de S_j à S_{j+1}, et ces deux chemins sont distincts et de même longueur. D'après le point ii. du lemme 3.4.1, on a donc $\ell(S_j) > \ell(S_{j+1})$. En outre, on a $\ell(S_0) \geqslant \ell(S_1)$ et $\ell(S_m) \geqslant \ell(S_{m+1})$. Donc :

$$d = \ell(\mathcal{Z}(a)) = \ell(S_0) \geqslant \ell(S_1) > \ell(S_2) > \ldots > \ell(S_m) \geqslant \ell(S_{m+1}) = \ell(Q) \geqslant 2$$

Ainsi, $m \leqslant d-1$.

✌

Remarque. Dans l'article de Derksen [Der07], ce résultat est énoncé avec la borne $d-2$, et non $d-1$. Une lacune dans la démonstration empêche en réalité d'obtenir cette borne, puisqu'il est énoncé dans l'article que $\ell(S_0) > \ell(S_1)$, ce qui n'est à priori pas justifié.
La borne $d-2$ semble cependant juste, puisque Derksen et Masser ont généralisé le théorème de Derksen en dimension supérieure par une autre approche dans [DM15].

3.4.2 Les ensembles p-normaux

Définition 3.4.5 (p-nested set élémentaire)
Soit $q = p^r$, avec $r \in \mathbb{N}^*$. Soit $d \in \mathbb{N}^*$ et $c_0, c_1, \ldots, c_d \in \mathbb{Q}$ tels que :

i. $\forall 0 \leqslant i \leqslant d,\ (q-1)c_i \in \mathbb{Z}$

ii. $c_0 + c_1 + \cdots + c_d \in \mathbb{Z}$

iii. $\forall 1 \leqslant i \leqslant d,\ c_i \neq 0$

On définit :

$$\widetilde{S}_q(c_0; c_1, \ldots, c_d) = \{c_0 + c_1 q^{k_1} + \cdots + c_d q^{k_d} \mid k_1, k_2, \ldots, k_d \in \mathbb{N}\}$$

Et on pose :

$$S_q(c_0; c_1, \ldots, c_d) = \widetilde{S}_q(c_0; c_1, \ldots, c_d) \cap \mathbb{N}$$

Un tel ensemble est appelé un p-nested set élémentaire d'ordre d.

Remarque. Les conditions sur les c_i imposent que $\widetilde{S}_q(c_0; c_1, \ldots, c_d$ est un sous-ensemble de $\mathbb{Z}$, et pas seulement de $\mathbb{Q}$ comme c'était le cas à priori. En effet, si $k_1, \ldots, k_d \in \mathbb{N}$, alors :

$$\begin{aligned}
(q-1)(c_0 + c_1 q^{k_1} + \cdots + c_d q^{k_d}) &= (q-1)c_0 + \sum_{i=0}(q-1)c_i q^{k_i} \mod (q-1) \\
&\overset{\text{i.}}{=} (q-1)c_0 + \sum_{i=0}(q-1)c_i \mod (q-1) \\
&= (q-1)(c_0 + \ldots + c_d) \mod (q-1) \\
&\overset{\text{ii.}}{=} 0 \mod (q-1)
\end{aligned}$$

Par conséquent, $c_0 + c_1 q^{k_1} + \cdots + c_d q^{k_d}$ est nécessairement un entier (et pas seulement un rationnel).

Nous allons montrer que les ensembles $\mathcal{Z}(a)$ peuvent s'écrire comme des unions finies d'ensembles p-normaux et de progressions arithmétiques, à un ensemble fini près. Cette écriture par les ensemble p-normaux est plus facile à manier que celle par les ensembles de la forme $U_p(u_0, \ldots, u_m; w_1, \ldots, w_m)$, parce qu'ils évitent de passer par l'écriture en base p et qu'ils apparaissent plus naturellement, comme on le voit dans le lemme suivant.

Lemme 3.4.6 (Contre-exemples à Skolem-Mahler-Lech en caractéristique p)
Soit K un corps de caractéristique $p > 0$ et soit $q = p^r$ une puissance de p. Considérons la suite $a \in \mathbb{K}^{\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

où $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d$ sont des éléments de $\overline{K}$ la clôture algébrique de K. S'il existe des éléments $c_0, \ldots, c_1, \ldots, c_r \in \mathbb{Z}$ tels que :

$$0 = \sum_{i=1}^{d} ((\beta_i \alpha_i^{c_0}) \otimes \alpha_i^{c_1} \otimes \cdots \otimes \alpha_i^{c_r}) \in \underbrace{\overline{K} \oplus_{\mathbb{F}_q} \overline{K} \oplus_{\mathbb{F}_q} \cdots \oplus_{\mathbb{F}_q} \overline{K}}_{r+1 \text{ fois}}$$

alors $S_q(c_0; c_1, \ldots, c_r) \subset \mathrm{Z}(a)$.

Preuve. Considérons $\varphi : \overline{K} \to \overline{K}$ le morphisme de Frobenius, ainsi que l'aplication $\mathbb{F}_q$-linéaire $\psi : \overline{K} \oplus_{\mathbb{F}_q} \overline{K} \oplus_{\mathbb{F}_q} \cdots \oplus_{\mathbb{F}_q} \overline{K} \to \overline{K}$ définie par

$$\forall \lambda_0, \ldots, \lambda_r \in \overline{K},\ \psi(\lambda_0 \otimes \cdots \otimes \lambda_r) = \lambda_0 \cdots \lambda_r.$$

De sorte que

$$\begin{aligned} a(c_0 + c_1 q^{k_1} + \cdots + c_r q^{k_r}) &= \sum_{i=1}^{d} \beta_i \alpha_i^{c_0 + c_1 q^{k_1} + \cdots + c_r q^{k_r}} \\ &= \sum_{i=1}^{d} \beta_i \psi(\alpha_i^{c_0} \otimes \alpha_i^{c_1 q^{k_1}} \otimes \cdots \otimes \alpha_i^{c_r q^{k_r}}) \\ &= \sum_{i=1}^{d} \psi((\beta_i \alpha_i^{c_0}) \otimes \varphi^{k_1}(\alpha_i^{c_1}) \otimes \cdots \otimes \varphi^{k_r}(\alpha_i^{c_r})) \\ &= \psi \circ (\mathrm{id} \otimes \varphi^{k_1} \otimes \cdots \otimes \varphi^{k_r}) \left(\sum_{i=1}^{d} ((\beta_i \alpha_i^{c_0}) \otimes \alpha_i^{c_1} \otimes \cdots \otimes \alpha_i^{c_r}) \right) \\ &= 0 \end{aligned}$$

On va utiliser le lemme suivant pour réduire notre étude aux suites simples et non-dégénérées.

Lemme 3.4.7
Soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire, $d \in \mathbb{N}$ et $k \geqslant 2$. Si les ensembles de zéros $\mathcal{Z}(T_j^k a)$, $j = 0, \ldots, k-1$ non triviaux s'écrivent à un ensemble fini près comme des unions de p-nested sets élémentaires d'ordre au plus d, alors $\mathcal{Z}(a)$ s'écrit à un ensemble fini près comme union finie de p-nested sets élémentaires d'ordre au plus r et de progression arithmétiques.

Preuve. On a l'égalité ensembliste suivante :

$$\mathcal{Z}(a) = \bigcup_{j=0}^{k-1} L_j^k(\mathcal{Z}(T_j^k a))$$

Soit $j \in \{0, \ldots, k-1\}$. Si $T_j^k a = 0$, alors $\mathcal{Z}(T_j^k a) = \mathbb{N}$ et donc $L_j^k(\mathcal{Z}(T_j^k a)) = k\mathbb{N} + j$.
Sinon, par hypothèse $\mathcal{Z}(T_j^k a)$ est à un ensemble fini près une union de p-nested sets élémentaires d'ordre au plus d. Or, si $c_0, \ldots, c_d \in \mathbb{Q}$ vérifient les conditions de la définition 3.4.5, alors :

$$L_j^k S_q(c_0; c_1, \ldots, c_d) = S_q(j + kc_0; kc_1, \ldots, k_c d)$$

Donc $\mathcal{Z}(a)$ est bien de la forme annoncée.

Remarque. D'après le lemme 3.2.5, on peut choisir k tel que les $T_j^k a$, $j = 0, \ldots, k-1$ soient simples et non-dégénérées. Il nous suffit donc d'étudier ces suites et le lemme précédent généralise le résultat aux suites récurrentes linéaires quelconques.

Lemme 3.4.8
Soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire simple et non-dégénérée. On suppose qu'il existe q une puissance de p et des rationnels r, s tel que à partir d'un certain rang, $r + sq^n \in \mathcal{Z}(a)$.
L'ensemble $\{r + sq^n \mid n \in \mathbb{N}\} \cap \mathbb{N}$ est inclu dans $\mathcal{Z}(a)$.

Preuve. On va d'abord se ramener au cas où $r = 0$ et $s = 1$. Puisque a est simple et non-dégénérée, on peut écrire :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

Soit un entier naturel non nul N tel que Nr et Ns soient entiers. Pour tout entier $1 \leqslant i \leqslant d$, on se donne λ_i une racine N-ième de α_i (éventuellement dans la clôture algébrique de K), c'est-à-dire que $\lambda_i^N = \alpha_i$.

Puisque pour $i \neq j$, le quotient α_i/α_j n'est pas une racine de l'unité, le quotient λ_i/λ_j ne l'est pas non plus et donc la suite $b \in K^{\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N},\ b(n) = \sum_{i=1}^{d} \beta_i \lambda_i^n$$

est simple et non-dégénérée et est telle que : $\forall n \in \mathbb{N},\ b(Nn) = a(n)$ et donc $b(Nr+(Ns)q^n) = a(r+sq^n)$. On s'est ramené au cas où r et s étaient entiers. On définit ensuite la suite c définie par :

$$\forall n \in \mathbb{N},\ c(n) = b(Nr + (Ns)n) = \sum i = 1^d \beta_i \lambda_i^{Nr} (\lambda_i^{Ns})^n$$

Cette suite est également simple et non-dégénérée. En outre, on a $a(r + sq^n) = b(Nr + Nsq^n) = c(q^n)$, donc on a bien la réduction que l'on cherchait.
On peut donc travailler sur une suite $a \in K^{\mathbb{N}}$ récurrente linéaire, simple et non-dégénérée définie par :

$$\forall n \in \mathbb{N},\ a(n) = \sum_{i=1}^{d} \beta_i \alpha_i^n$$

telle qu'il existe un range m à partir duquel $a(q^n) = 0$. On fixe l'élément suivant de $K \oplus_{\mathbb{F}_q} K$:

$$x = \sum_{i=1}^{d} (\beta_i \otimes \alpha_i)$$

Notons φ le morphisme de Frobenius et $\psi : K \otimes_{\mathbb{F}_q} K \to K$ défini par $\psi(\lambda \otimes \mu) = \lambda\mu$ pour $\lambda, \mu \in K$ et étendu par linéarité à $K \otimes_{\mathbb{F}_q} K$. On a alors :

$$\psi \circ (\mathrm{id} \otimes \varphi^n)(x) = \psi\left(\sum_{i=1}^{d} \beta_i \otimes \alpha_i^{q^n}\right) = \sum_{i=1}^{d} \beta_i \alpha_i^{q^n} = a(q^n)$$

Ainsi, si l'on montre que x est nul, on aura montré que la suite a s'annule en tous les $q^n,\ n \in \mathbb{N}$. Supposons donc que x est non nul. Donnons-nous $e \in \mathbb{N}$ minimal tel que x s'écrit sous la forme :

$$x = \sum_{i=1}^{e} \delta_i \otimes \gamma_i$$

Par hypothèse, pour tout $n \geqslant m$, on a :

$$0 = a(q^n) = \psi \circ (\mathrm{id} \otimes \varphi^n)(x) = \sum_{i=1}^{d} \delta_i \gamma_i^{q^n}$$

Définissons maintenant pour tout $1 \leqslant j \leqslant e$ la suite $c_j \in K^{\mathbb{N}}$ par :

$$c_j(n) = \gamma_j^{q^n}$$

De sorte que pour tout $n \in \mathbb{N}$:

$$\left(\sum_{j=1}^{e} \delta_j E^m c_j\right)(n) = \sum_{j=1}^{e} \delta_j \gamma_j^{q^{m+n}} = a(q^{n+m}) = 0$$

Donc pour tout $n \geqslant m$, la famille $(E^n c_1, \ldots, E^n c_e)$ est liée sur K. On se donne donc j maximal tel que la famille $(E^n c_1, \ldots, E^n c_{j-1})$ est libre pour tout $n \in \mathbb{N}$. Cet entier existe car par hypothèse sur x, γ_1 est non nul et donc la famille $(E^n c_1)$ est libre pour tout $n \in \mathbb{N}$. De plus, on a $j - 1 < e$.
Pour un entier n suffisamment grand, la famille $(E^n c_1, \ldots, E^n c_j)$ est donc liée. On a donc :

$$E^n c_j = \sum_{i=1}^{j-1} \varepsilon_i E^n c_i$$

avec $\varepsilon_1, \dots, \varepsilon_{j-1} \in K$, car la famille $(E^n c_1, \dots, E^n c_{j-1})$ est libre. En appliquant le morphisme de Frobenius, on a alors :

$$E^{n+1}c_j = (E^n c_j)^q = \sum_{i=1}^{j-1} \varepsilon_i^q (E^n c_i)^q = \sum_{i=1}^{j-1} \varepsilon_i^q E^{n+1} c_i$$

Si en revance on applique l'opérateur E, on obtient :

$$E^{n+1}c_j = \sum_{i=1}^{j-1} \varepsilon_i E^{n+1} c_i$$

Donc :

$$\sum_{i=1}^{j-1} (\varepsilon_i^q - \varepsilon_i) E^{n+1} c_i = 0$$

Par indépendance des $E^{n+1}c_i$, $i = 1, \dots, j-1$ sur K, on obtient donc $\varepsilon_i^q = \varepsilon_i$ pour $i = 1, \dots, j-1$. Ainsi, $\varepsilon_1, \dots, \varepsilon_{j-1} \in \mathbb{F}_q$. Dès lors, la famille $(E^n c_1, \dots, E^n c_j)$ est liée sur $\mathbb{F}_q$ et non plus seulement sur K. En passant à la racine q^n-ième, on obtient que la famille $(c_1, \dots, c_j)$ est elle aussi liée sur $\mathbb{F}_q$. En particulier, la famille $(\gamma_1, \dots, \gamma_j) = (c_1(0), \dots, c_j(0))$ est donc liée sur $\mathbb{F}_q$, ce qui contredit la minimalité de e.
Par conséquent, x est nul et donc $a(q^n) = 0$ pour tout $n \in \mathbb{N}$.

Théorème 3.4.9 (Derksen)
Soit $a \in K^{\mathbb{N}}$ une suite récurrente linéaire simple et non dégénérée d'ordre d. L'ensemble de ses zéros $\mathcal{Z}(a)$ est une union finie de p-nested sets d'ordre au plus $d-1$.

Preuve. D'après le théorème 3.4.4, $\mathcal{Z}(a)$ s'écrit comme une union d'ensemble de la forme

$$U_p(u_0, \dots, u_m; w_1, \dots, w_m),$$

où $m \leqslant d-1$. Soit donc un tel ensemble. Notons r_i la longueur du mot w_i et $r = \text{ppcm}(r_1, \dots, r_m)$. On peut alors écrire :

$$U_p(u_0, \dots, u_m; w_1, \dots, w_m) = \bigcup_{0 \leqslant l_1 < k_1, \dots, 0 \leqslant l_m < k_m} U_p(u_0, u_1 w_1^{l_1} \dots, u_m w_m^{l_m}; w_1^{k_1}, \dots, w_m^{k_m})$$

où $k_i = r/r_i$, $i = 1, 2, \dots, m$. Ainsi, $\mathcal{Z}(a)$ s'écrit comme une union d'ensembles de la forme

$$U_p(u_0, \dots, u_m; w_1, \dots, w_m)$$

où $w_1, \dots, w_m$ sont de même longueur. Considérons un tel ensemble et notons r la longueur des w_i. On va l'inclure dans un p-nested set élémentaire, lui-même contenu dans $\mathcal{Z}(a)$.
Soit donc $q = p^r$ et t_i la longueur de u_i pour $i = 0, 1, 2, \dots, m$. On a en outre, pour $k_0, \dots, k_m \in \mathbb{N}$:

$$\begin{aligned}
[u_m w_m^{k_m} \cdots u_1 w_1^{k_1} u_0]_p &= \sum_{i=0}^{m} [u_i]_p p^{t_0+\cdots+t_{i-1}} q^{k_1+\cdots+k_i} + \sum_{i=1}^{m} [w_i]_p p^{t_0+\cdots+t_{i-1}} \left(\frac{q^{k_i}-1}{q-1}\right) q^{k_1+\cdots+k_{i-1}} \\
&= \underbrace{([u_0]_p - [w_1]p^{t_0}\frac{1}{q-1})}_{=\ c_0} \\
&\quad + \sum_{i=1}^{m-1} \underbrace{p^{t_0+\cdots+t_{i-1}}([u_i]_p + \frac{1}{q-1}[w_i]_p - \frac{1}{q-1}[w_{i+1}]_p p^{t_i})}_{=\ c_i} q^{k_1+\cdots+k_i} \\
&\quad + \underbrace{p^{t_0+\cdots+t_{m-1}}([u_m]_p + \frac{1}{q-1}[w_m]_p)}_{=\ c_m} q^{k_1+\cdots+k_m}
\end{aligned}$$

Ainsi, en fixant les $c_0, \dots, c_m \in \mathbb{Q}$ comme au dessus, et puisque les k_i décrivent $\mathbb{N}$, on a l'égalité :

$$U_p(u_0, \dots, u_m; w_1, \dots, w_m) = \{c_0 + c_1 q^{l_1} + \cdots + c_m q^{l_m} \mid 0 \leqslant l_1 \leqslant l_2 \leqslant \cdots \leqslant l_m\} \subset S_q(c_0; c_1, \dots, c_m)$$

En effet, pour tout $i = 0, 1, \dots, m$, $(q-1)c_i \in \mathbb{Z}$ et $c_0 + c_1 + \ldots + c_m = [u_m u_{m-1} \cdots u_0]_p \in \mathbb{Z}$. Certains c_i sont potentiellement nuls, il suffit de les éliminer et d'abaisser m (qui reste dond toujours inférieur ou égal à $d-1$). Cependant, on a nécessairement $c_m > 0$.

Montrons maintenant que $\mathcal{Z}(a)$ contient $S_q(c_0; c_1, \dots, c_m)$. Soit donc $l_1, \dots, l_m \in \mathbb{N}$ tels que la somme $c_0 + c_1 q^{l_1} + \cdots + c_m q^{l_m} \in \mathbb{N}$. On souhaite montrer que cette somme appartient à $\mathcal{Z}(a)$.
En appliquant le lemme 3.4.8 avec $r = c_0 + c_1 q^{l_1} + \cdots + c_{m-1} q^{l_{m-1}}$ et $s = c_m$, il nous suffit de montrer quà partir d'un certain rang N,

$$c_0 + c_1 q^{l_1} + \cdots + c_m q^{l_m+n} \in \mathcal{Z}(a)$$

Montrons-le par récurrence sur $D = \mathrm{Card}\{i \in \{1, \dots, m-1\} \mid l_i > l_{i+1}\}$. Le cas initial où $D = 0$ a déjà été traité (c'est le cas $l_1 \leqslant l_2 \leqslant \cdots \leqslant l_m$). Si en revanche $D > 0$, alors il existe $i \in \{1, \dots, m-1\}$ tel que $l_i > l_{i+1}$. Puisque $c_m > 0$, pour un entier N suffisamment grand, on a :

$$c_{i+1} q^{l_{i+1}} + \cdots + c_{m-1} q^{l_{m-1}} + c_m q^{l_m+N} > 0$$

Et donc pour tout $M \geqslant l_i - l_{i+1}$, par récurrence :

$$(c_1 q^{l_1} + \cdots + q_i^{l_i}) + (c_{i+1} q^{l_{i+1}+M} + \cdots + c_{m-1} q^{l_{m-1}+M} + c_m q^{l_m+M+N}) \in \mathcal{Z}(a)$$

Le lemme 3.4.8 nous permet de conclure que $c_0 + c_1 q^{l_1} + \cdots + c_m q^{l_m+n} \in \mathcal{Z}(a)$ pour tout $n \geqslant N$. Ce qui conclue la preuve.

✌

Remarque. Bien que l'on ait aboutit à une description assez fine (et assez naturelle en vertu du lemme 3.4.6), la réciproque du théorème 3.4.9 est toujours une question ouverte.

Bibliographie

[AB12] Boris Adamczewski et Jason Bell. "On vanishing coefficients of algebraic power series over fields of positive characteristic". In : *Inventiones mathematicae* 187 (2012), p. 243-393.

[All99] Jean-Paul Allouche. "Transcendence of formal power series with rational coefficients". In : *Theoretical Computer Science* 218.1 (1999), p. 143-160. issn : 0304-3975.

[AS03] Jean-Paul Allouche et Jeffrey Shallit. *Automatic Sequences : Theory, Applications, Generalizations*. Cambridge University Press, 2003.

[Der07] Harm Derksen. "A Skolem–Mahler–Lech theorem in positive characteristic and finite automata". In : *Inventiones mathematicae* 168.1 (2007), p. 175-224.

[DM15] H. Derksen et D. Masser. "Linear equations over multiplicative groups, recurrences, and mixing II". In : *Indagationes Mathematicae* 26.1 (2015), p. 113-136. issn : 0019-3577.

[Eve+03] G. Everest et al. *Recurrence Sequences*. Mathematical surveys and monographs. American Mathematical Society, 2003. isbn : 9780821833872.

[Han86] G. Hansel. "Une démonstration simple du théorème de Skolem-Mahler-Lech". In : *Theoretical Computer Science* 43 (1986), p. 91-98. issn : 0304-3975.

[Kre18] Thijmen Krebs. "A More Reasonable Proof of Cobham's Theorem". In : *International Journal of Foundations of Computer Science* 32 (jan. 2018). doi : 10.1142/S0129054121500118.

[RW09] Michel Rigo et Laurent Waxweiler. "A note on syndeticity, recognizable sets and Cobham's theorem". In : *CoRR* abs/0907.0624 (juill. 2009).

[SW88] Habib Sharif et Christopher F. Woodcock. "Algebraic Functions Over a Field of Positive Characteristic and Hadamard Products". In : *Journal of the London Mathematical Society* s2-37.3 (1988), p. 395-403. issn : 0024-6107.