

---

# Automates finis et développements dans les corps des fonctions en caractéristique positive

---

## Rapport de stage

Master “Mathématiques et Applications”

2-ème année Recherche

Université Claude Bernard Lyon 1

**Alina FIRICEL**

---

Sous la direction de **Boris ADAMCZEWSKI**

Septembre 2007



# Table des matières

<b>Introduction</b>	<b>1</b>
<b>I Théorème de Christol</b>	<b>4</b>
I.1 Automates finis et suites automatiques . . . . .	4
I.1.1 Définitions . . . . .	4
I.1.2 Exemples de suites automatiques . . . . .	7
I.1.3 Noyau d'une suite automatique et condition de non automaticité . . .	10
I.2 Théorème de Christol . . . . .	11
I.2.1 Préliminaires algébriques . . . . .	11
I.2.2 Exemples de séries formelles algébriques . . . . .	13
I.2.3 Le théorème de Christol . . . . .	15
I.2.4 Comparaison avec le développement $b$ -adique des nombres réels . . .	20
I.3 Application du théorème de Christol . . . . .	22
<b>II Généralisation du théorème de Christol</b>	<b>25</b>
II.1 Présentation du théorème de Kedlaya . . . . .	25
II.1.1 Séries formelles de Hahn–Mal'cev–Neumann . . . . .	26
II.1.2 Automates finis revisités et séries quasi- $p$ -automatiques . . . . .	28
II.1.3 Un exemple de série de Hahn algébrique . . . . .	30
II.2 Préliminaires algébriques . . . . .	32
II.2.1 Systèmes d'équations semi-linéaires . . . . .	32
II.2.2 Polygone de Newton . . . . .	33
II.2.3 Polynômes tordus et factorisation . . . . .	36
II.3 Démonstration du théorème de Kedlaya . . . . .	36
II.3.1 Preuve de la première implication du théorème . . . . .	36
II.3.2 L'ensemble $K_q$ est un corps . . . . .	40
II.3.3 Clôture topologique et clôture algébrique . . . . .	44
II.3.4 Preuve de la seconde implication du théorème . . . . .	47
<b>Conclusions</b>	<b>50</b>
<b>A Polynômes additifs et démonstration du lemme II.2.3</b>	<b>52</b>
<b>B Polynômes tordus et démonstration de la proposition II.2.3</b>	<b>54</b>

# Introduction

La suite des chiffres du développement d'un nombre irrationnel, comme  $\sqrt{2}$ , dans une base entière est source de nombreux problèmes. Nos connaissances sur ce sujet sont pour le moins limitées et la plupart de ces questions restent encore sans réponse.

De façon assez surprenante, lorsque l'on choisit d'additionner et de multiplier sans retenue, il devient possible de décrire les représentations des nombres algébriques : c'est le théorème de Christol. Ici, l'expression "additionner et multiplier sans retenue" doit s'entendre comme suit : au lieu d'étudier l'algébricité sur le corps  $\mathbb{Q}$  du nombre réel  $\sum_{n \geq 0} \frac{a_n}{p^n}$ , on s'intéresse à l'algébricité de la série formelle  $f(t) = \sum_{n \geq 0} a_n t^n \in \mathbb{F}_p((t))$  sur le corps de fractions rationnelles à coefficients dans  $\mathbb{F}_p$ ,  $p$  désignant un nombre premier.

Le théorème de Christol donne une caractérisation simple et combinatoire de l'algébricité des séries formelles à coefficients dans le corps fini  $\mathbb{F}_q$ , énoncée en termes d'automates finis. Il s'énonce de la façon suivante : la série formelle  $f$  est algébrique sur  $\mathbb{F}_p((t))$  si, et seulement si, la suite  $(a_n)_{n \geq 0}$  peut être engendré par un  $p$ -automate fini. La première partie de ce mémoire a pour objet l'étude de ce théorème.

Un exemple illustrant ce résultat est donné par la série de Thue-Morse :

$$T(t) = t + t^2 + t^4 + t^7 + t^8 + t^{11} + \dots$$

C'est la somme des puissances de  $t$  dont l'exposant a une écriture binaire comportant un nombre pair de chiffres 1 : cette série formelle est 2-automatique. Par conséquent, si l'on considère cette série comme une série de Laurent sur un corps fini de caractéristique 2, elle est algébrique. Plus précisément, elle vérifie l'équation

$$(1+t)^3 T(t)^2 + (1+t)^2 T(t) + t = 0.$$

Le théorème de Christol peut s'appliquer dans de nombreuses situations ; il permet en particulier d'obtenir des résultats de transcendance pour des analogues définis par Carlitz des fonctions logarithme, exponentielle, gamma ou zeta. Suivant cette approche, nous donnerons à la fin de la première partie de ce mémoire une démonstration de la transcendance de l'analogue du nombre  $\pi$  ; cette série peut être décrite par le produit infini suivant :

$$\prod_{j=1}^{\infty} \left( 1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X} \right).$$

Malheureusement, le corps  $\mathbb{F}_p((t))$  est loin d'être algébriquement clos et le théorème de Christol n'offre donc qu'une description incomplète des éléments algébriques sur  $\mathbb{F}_p(t)$ .

En effet, il existe des polynômes à coefficients dans  $\mathbb{F}_p(t)$  qui n'ont aucune racine dans le corps de séries formelles  $\mathbb{F}_p((t))$ . Par exemple, le polynôme d'Artin-Schreier

$$P(X) = X^p - X - \frac{1}{t}$$

n'a pas de racine dans le corps  $\mathbb{F}_p((t))$ .

Ses racines sont les séries de la forme

$$x = c + t^{-1/p} + t^{-1/p^2} + \dots \quad \text{pour } c = 0, 1, 2, \dots, p-1.$$

Elles font partie d'un corps bien plus gros, le corps des séries formelle généralisées (ou séries de Hahn) à coefficients dans  $\mathbb{F}_p$ , que l'on note  $\mathbb{F}_p((t^{\mathbb{Q}}))$ .

Ces séries ont été introduites par Hahn en 1907 et elles peuvent être vues comme les sommes formelles de la forme

$$\sum_{i \in I} x_i t^i,$$

où l'ensemble  $I$  est un ensemble bien ordonné des rationnels (c'est-à-dire qu'on ne peut pas extraire une sous-suite infinie strictement décroissante de l'ensemble  $I$ ).

Dans la deuxième partie de ce mémoire, nous donnerons une description en termes d'automates de la clôture algébrique de  $\mathbb{F}_p(t)$  dans le corps des séries de Hahn. Cette extension du théorème de Christol fait l'objet d'un travail récent de Kedlaya [9]. Plus précisément, cette clôture algébrique est caractérisée comme l'ensemble des séries quasi- $q$ -automatiques, c'est-à-dire que quitte à effectuer une affinité rationnelle sur les exposants, leurs dénominateurs deviennent tous des puissances de  $p$  et les coefficients peuvent alors être calculés par un automate fini à partir de l'écriture en base  $p$  de ces exposants (écriture finie après la virgule puisque, le dénominateur est, justement, une puissance de  $p$ ).

# I Théorème de Christol

Le but de la première partie de ce mémoire est de démontrer le théorème de Christol, qui donne une équivalence entre une propriété algébrique d'une série formelle et une propriété combinatoire de la suite de ses coefficients. Nous commençons avec quelques rappels sur les automates finis et les suites automatiques, puis sur les séries formelles. Nous donnons ensuite quelques exemples de séries formelles algébriques dont les coefficients sont des suites automatiques. Nous démontrons alors le théorème de Christol et donnons enfin une application de ce théorème. Plus précisément, nous allons démontrer la transcendance de la fonction  $\Pi_q$  de Carlitz sur le corps  $\mathbb{F}_q(X)$ .

## I.1 Automates finis et suites automatiques

### I.1.1 Définitions

Dans cette partie, on définit certaines notions élémentaires à propos des automates finis déterministes, puis on rappelle quelques résultats fondamentaux les concernant.

On appellera alphabet tout ensemble fini. Les éléments d'un alphabet sont traditionnellement appelés lettres, symboles ou encore caractères.

Considérons maintenant un alphabet  $\Sigma$ . On appelle mot sur  $\Sigma$  toute suite finie d'éléments de  $\Sigma$ . L'ensemble des mots sur  $\Sigma$  est noté  $\Sigma^*$ .

On appelle langage sur l'alphabet  $\Sigma$  un sous-ensemble de  $\Sigma^*$ . On définit l'opération de concaténation de deux mots  $a = a_1a_2 \dots a_m$  et  $b = b_1b_2 \dots b_n$  étant le mot obtenu par juxtaposition :  $ab = a_1a_2 \dots a_mb_1b_2 \dots b_n$ . C'est une opération associative.

L'ensemble  $\Sigma^*$ , muni de la concaténation, forme un monoïde libre. Son élément neutre est le mot vide, qu'on note en général  $\epsilon$ .

**Définition I.1.1.** Un automate fini déterministe (DFA)  $M$  est un quintuplet  $M = (Q, \Sigma, \delta, q_0, F)$  dans lequel :

- $Q$  est l'ensemble fini des états (la mémoire de l'automate)
- $\Sigma$  est l'alphabet fini sur lequel sont construits les mots à reconnaître : l'automate recevra comme donnée un mot de  $\Sigma^*$  sur lequel il réalisera un certain type de calcul.
- $\delta : Q \times \Sigma \rightarrow Q$  est la fonction de transition de l'automate  $M$ . Elle décrit le mode de fonctionnement de l'automate.  
Elle définit dans quel état l'automate va passer quand il se trouve dans un état  $q$  et lit une lettre  $x$  (ou s'il va éventuellement se bloquer).  
Le qualificatif déterministe correspond au fait que pour un couple  $(q, x)$  donné :
  - soit la fonction est définie et l'automate passe dans l'état unique  $q'$  spécifié par la fonction de transition ( $q' = \delta(q, x)$ ).
  - soit elle n'est pas définie et l'automate se bloque.
- $q_0 \in Q$  est l'état initial de l'automate  $M$ . C'est l'état dans lequel l'automate se trouve lorsqu'il commence à travailler.
- $F \subset Q$  est l'ensemble des états terminaux (ou états finaux) de l'automate  $M$ .

Pour formaliser le calcul d'un automate fini déterministe  $M$ , on définit l'extension  $\delta^*$  de la fonction  $\delta$  aux mots de  $\Sigma^*$  de la manière suivante :

- $\forall q \in Q, \delta^*(q, \epsilon) = q$ , où  $\epsilon$  est le mot vide.
- $\forall q \in Q, \forall x \in \Sigma, \forall u \in \Sigma^*, \delta^*(q, ux) = \delta(\delta^*(q, u), x)$ .

Un mot  $w$  de  $\Sigma^*$  est reconnu par l'automate fini déterministe  $M$  si  $\delta^*(q_0, w) \in F$  (la fonction  $\delta^*$  est donc définie en  $(q_0, w)$  et lui associe un élément de  $F$ ). Le langage  $L(M)$  reconnu par l'automate est donc

$$\{u \in \Sigma^*, \text{ tel que } \delta^*(q_0, u) \in F\}.$$

Un langage est appelé régulier si, est seulement si, il est accepté par un automate fini.

Pour représenter de façon très intuitive un automate fini déterministe  $M = (Q, \Sigma, \delta, q_0, F)$ , on peut utiliser un graphe de transition constitué des éléments suivants :

- Un ensemble de sommets (chaque sommet représente un élément de  $Q$ ).
- Un ensemble d'arcs entre les sommets valués par un symbole de  $\Sigma$  (un arc entre les états  $q$  et  $q'$  valué par le symbole  $s$  signifie que  $\delta(q, s) = q'$ ).
- L'état initial  $q_0$  est marqué par une flèche entrante.
- Les états finaux  $F$  sont marqués par un double cercle.

**Exemple I.1.1.** On considère le DFA  $M = (Q, \Sigma, \delta, q_0, F)$  suivant :

- $Q = \{1, 2\}$
- $\Sigma = \{a, b\}$
- $\delta(1, a) = 1, \delta(1, b) = 2, \delta(2, a) = 1, \delta(2, b) = 2$
- $q_0 = 1$
- $F = \{2\}$

Cet automate peut être représenté sur la figure 1 :

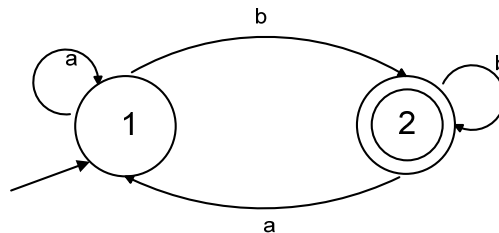


FIG. 1 – Un automate fini déterministe

Il est facile de voir que le langage reconnu par cet automate est constitué exactement des mots composés de  $a$  et de  $b$  qui se terminent par un  $b$ .

**Définition I.1.2.** Un automate fini avec sortie (DFAO)  $M$  est un 6-uple  $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$  dans lequel :

- $Q, \Sigma, \delta, q_0$  sont définis comme pour les DFA ;
- $\Delta$  est l'alphabet de sortie ;
- $\tau : Q \rightarrow \Delta$  est la fonction de sortie.

Pour un DFAO  $M$  on définit la fonction  $f_M : \Sigma^* \rightarrow \Delta$  de la manière suivante :

$$f_M(w) = \tau(\delta(q_0, w)).$$

Cette fonction est appelée fonction d'état fini. La seule différence entre les DFAO et les DFA est la façon d'appeler les états : ici  $(q/a)$  indique que la sortie associée à l'état  $q$  est le symbole  $a$ .

**Exemple I.1.2.** On considère le DFAO  $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$  suivant :

- $Q = \{(q_0, 0), (q_1, 1)\}$
- $\Sigma = \{0, 1\}$
- $\delta((q_0, 0), 0) = (q_0, 0), \delta((q_0, 0), 1) = (q_1, 1), \delta((q_1, 1), 0) = (q_1, 1), \delta((q_1, 1), 1) = (q_0, 0)$
- $q_0 = (q_0, 0)$
- $\Delta = \{0, 1\}$
- $\tau(q_0) = 0, \tau(q_1) = 1$

Cet automate peut être représenté de la façon suivante :

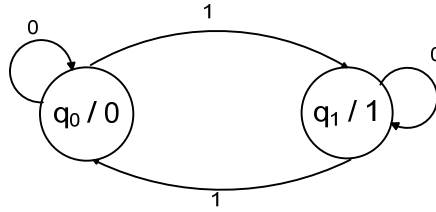


FIG. 2 – Un automate fini déterministe avec sortie

On peut remarquer que cet automate calcule la somme modulo 2 des bits d'entrée. Par exemple, si on entre le mot  $w = 01110$ , en faisant la transition par l'automate,  $f_M(w) = 1$ .

Dans la suite, on va étudier la fonction d'état fini pour des entrées données par la représentation des entiers en base  $k$ , c'est à dire que l'alphabet  $\Sigma$  considéré est  $\Sigma_k = \{0, 1, \dots, k-1\}$ ,  $k \geq 2$ . On parlera alors d'un  $k$ -DFAO.

Pour un mot  $w = b_1 b_2 \dots b_r$ , on notera

$$[w]_k = \sum_{1 \leq i \leq r} b_i k^{r-i}.$$

De même, pour un entier  $N = \sum_{0 \leq i \leq t} a_i k^i$ ,  $a_t \neq 0$  et  $0 \leq a_i < k$ ,

$$(N)_k = a_t a_{t-1} \dots a_1 a_0.$$

**Définition I.1.3.** Une suite  $(a_n)_{n \geq 0}$  sur l’alphabet  $\Delta$  est  $k$ -automatique s’il existe un  $k$ -DFAO  $M = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$  tel que  $a_n = \tau(\delta(q_0, w))$ ,  $\forall n \geq 0$  et  $\forall w$  avec  $[w]_k = n$ .

Autrement dit, une suite est  $k$ -automatique si son  $n$ -ième terme est engendré par une machine à états finis, lisant en entrée le développement de  $n$  en base  $k$ .

Si  $M$  est le DFAO de la définition précédente, on dit alors que  $M$  engendre la suite  $(a_n)_{n \geq 0}$ .

### I.1.2 Exemples de suites automatiques

Nous donnons maintenant quelques exemples de suites automatiques, ainsi que les automates qui les engendrent.

#### Exemple I.1.3. La suite de Thue–Morse.

La suite de Thue–Morse, notée ici  $\mathbf{t} = (t_n)_{n \geq 0}$  calcule le nombre de “1” modulo 2 dans la représentation de  $n$  en base 2.

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

En se plaçant dans l’alphabet  $\{0, 1\}$ , la suite de Thue–Morse est 2-automatique car elle est engendrée par l’automate suivant :

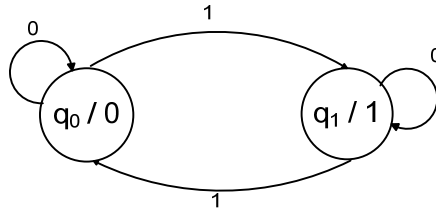


FIG. 3 – Automate engendrant la suite de Thue–Morse

Pour le démontrer, on remarque que l’état  $q_0$  représente la lecture d’une entrée avec un nombre pair de 1 (donc 0 modulo 2) et l’état  $q_1$  représente la lecture d’une entrée avec un nombre impair de 1 (donc 1 modulo 2).

**Remarque.** Cette suite, introduite initialement par Axel Thue au début du XX-ième siècle, possède des propriétés très intéressantes en termes de répétitions.

Il est facile de vérifier que sur un alphabet à deux lettres il n’existe pas de mots infinis “sans carré”. Un mot sans carré est un mot qui ne contient aucun motif de la forme  $XX$ . On peut naturellement se demander s’il contient des “chevauchements”, c’est-à-dire des motifs de la forme  $WWx$ , où  $W$  est un mot(fin) et  $x$  la première lettre de  $W$ . Par exemple, le mot *ananas* contient le chevauchement *anana*.

En 1912, Thue a montré que la suite  $\mathbf{t}$  ne contient aucun chevauchement. A fortiori, elle ne contient pas de “cube”, c’est-à-dire, aucun motif de la forme  $XXX$ .

**Exemple I.1.4. La suite de Rudin–Shapiro.**

Toujours en base 2, on peut définir la suite  $s_n = (-1)^{r_n}$ , où  $r_n$  compte le nombre d’occurrences de “11” dans l’écriture binaire de  $n$ .

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

Alors cette suite est 2-automatique car elle est engendrée par l’automate suivant :

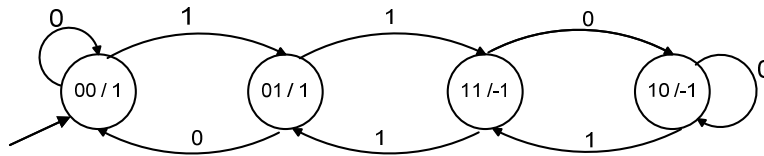


FIG. 4 – Automate engendrant la suite de Rudin–Shapiro

**Remarque.** Cette suite est apparue comme réponse à une question posée en 1950 par Salem. Si  $\mathbf{u} = (u_n)_{n \geq 0}$  est une suite infinie à valeurs dans  $\{-1, 1\}$ , que peut on dire de la quantité :

$$F_N(\mathbf{u}) = \sup_{\theta \in \mathbb{R}} \left| \sum_{n=0}^{N-1} u(n)e^{2i\pi n\theta} \right|$$

lorsque  $N$  tend vers l’infini ? En majorant trivialement, puis en minorant la norme  $L^\infty$  par la norme  $L^2$ , on obtient :

$$\sqrt{N} \leq F_N(\mathbf{u}) \leq N.$$

Par ailleurs, on peut démontrer que, pour presque toute suite  $\mathbf{u}$ , on a :

$$F_N(\mathbf{u}) \leq \sqrt{N \log N}.$$

Shapiro en 1951, puis indépendamment Rudin en 1952, ont construit une suite  $\mathbf{s}$  “explicité”, pour laquelle on a :

$$F_N(\mathbf{s}) \leq C\sqrt{N}.$$

Ultérieurement, Brillhart et Carlitz ont prouvé que cette suite peut être définie par  $s_n = (-1)^{r_n}$ , où  $r_n$  représente le nombre de 11 (avec chevauchements éventuels) dans le développement binaire de  $n$ . En particulier, on a vu que cette suite est 2-automatique.

### Exemple I.1.5. La suite des entiers de Cantor.

Maintenant voyons un exemple d'une suite 3-automatique. La suite des entiers de Cantor, notée ici  $\mathbf{c} = (c_n)_{n \geq 0}$  est définie de la façon suivante :

$$c_n = \begin{cases} 1 & \text{si } (n)_3 \text{ ne contient que les chiffres 0 et 2} \\ 0 & \text{si } (n)_3 \text{ contient le chiffre 1.} \end{cases}$$

En se plaçant maintenant dans l'alphabet  $\{0, 1, 2\}$ , la suite des entiers de Cantor est 3-automatique car elle est engendrée par l'automate décrit par la figure 5.

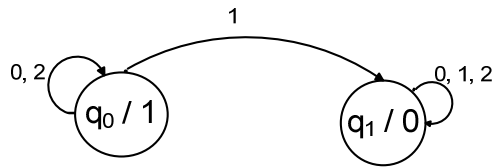


FIG. 5 – Automate engendrant la suite des entiers de Cantor

**Remarque.** Cette suite est en forte relation avec l'ensemble de Cantor (ou ensemble triadique de Cantor), qui est un sous-ensemble remarquable de la droite réelle construit par le mathématicien allemand Georg Cantor. Il est construit de manière itérative à partir du segment  $[0, 1]$ , en enlevant le tiers central ; puis on réitère l'opération sur les deux segments restants, et ainsi de suite. Il s'agit d'un ensemble fermé de  $[0, 1]$ , d'intérieur vide.

Il admet aussi une interprétation en terme de développement des réels en base 3. Pour cette raison, il est parfois noté  $K_3$ .

On peut le définir via l'écriture en base 3 : tout réel  $x \in [0, 1]$  s'écrit de manière :  $x = \sum_{n=1}^{\infty} \frac{x_n}{3^n}$  avec  $x_n \in \{0, 1, 2\}$ . On écrit alors  $x = 0, x_1x_2x_3x_4x_5 \dots$ . Cette écriture est unique à ceci près : on peut remplacer  $1000000 \dots$  par  $0222222 \dots$  (et  $2000000 \dots$  par  $1222222 \dots$ ) à la fin d'une écriture, de la même manière que  $0,999999 \dots = 1$  en base 10. L'ensemble des entiers de Cantor est formé des réels de  $[0, 1]$  ayant une écriture en base 3 ne contenant que des 0 et des 2. C'est à dire

$$K_3 = \left\{ x = \sum_{n=1}^{\infty} \frac{x_n}{3^n}, \quad x_n \in \{0, 2\} \right\}.$$

Donc  $1/3$  est dans cet ensemble, puisqu'il admet les deux écritures  $0,1000 \dots$  et  $0,02222 \dots$  en base 3, tout comme  $2/3$  également ( $0,2000 \dots$  ou  $0,12222 \dots$ ). Parmi les nombres admettant un développement propre et un développement impropre, il n'en existe aucun dont les deux écritures vérifient la propriété demandée.

Cet ensemble a de nombreuses propriétés. Par exemple, on sait qu'il est de mesure nulle, qu'il a la puissance du continu ainsi que beaucoup d'autres propriétés topologiques.

### I.1.3 Noyau d'une suite automatique et condition de non automaticité

Nous allons à présent introduire une notion très importante pour les suites automatiques : le  $k$ -noyau. Ce terme a été introduit par O. Salon en 1986.

**Définition I.1.4.** Soit  $k \geq 2$  un entier. Le  $k$ -noyau d'une suite  $(a_n)_{n \geq 0}$  est l'ensemble des sous-suites du type  $(a_{k^i n + j})_{n \geq 0}$  avec  $i \geq 0$  et  $0 \leq j \leq k^i$ .

### Exemple I.1.6. La suite de Thue–Morse.

011010011001011010010...

Soit  $t_n$  le  $n$ -ième terme de la suite de Thue–Morse. Alors,

$$t_{2n} = t_n \quad \text{et} \quad t_{2n+1} = 1 - t_n.$$

Ainsi, on a

$$t_{2^i n + j} = t_n \quad \forall n \geq 0 \quad \text{ou} \quad t_{2^i n + j} = 1 - t_n \quad \forall n \geq 0.$$

Le 2-noyau de la suite de Thue–Morse ne contient que 2 suites : la suite de Thue–Morse et sa “renversée”.

Rappelons dans la suite une propriété caractéristique des suites automatiques. Il s'agit d'un résultat dû à Eilenberg [7].

**Théorème I.1.1.** *Une suite est  $k$ -automatique si, et seulement si, son  $k$ -noyau est fini.*

Remarquons que ce théorème implique qu'une suite automatique ne prend qu'un nombre fini des valeurs. Par ailleurs, on voit facilement qu'une suite ultimement périodique est  $k$ -automatique, pour tout entier  $k \geq 2$ .

Une autre propriété assez utile est le théorème suivant, dû à Eilenberg :

**Théorème I.1.2.** *Pour tout entier  $m \geq 1$ , une suite  $(a_n)_{n \geq 0}$  est  $k$ -automatique si, et seulement si, elle est  $k^m$ -automatique.*

Nous admettrons les deux résultats précédents qui sont, par exemple, démontrés dans [2].

Le théorème suivant permet en général de montrer la non automaticité de certaines suites.

**Théorème I.1.3.** *Soit  $k$  un entier  $\geq 2$  et soit  $\mathbf{a} = (a_n)_{n \geq 0}$  une suite automatique engendrée par le  $k$ -DFAO  $(Q, \Sigma, \delta, q_0, \Delta, \tau)$ . Soient  $v, w \in \{0, 1, \dots, k-1\}$ . Alors, la suite  $(a_{[vw^i]_k})_{i \geq 0}$  est ultimement périodique.*

*Démonstration.* C'est trivial si la longueur de  $w$  est nulle. On peut donc supposer dans la suite que  $|w| \geq 1$  et posons ainsi  $w = w_0 w_1 \dots w_{r-1}$  pour un entier  $r \geq 1$ . De même, soit  $v = v_0 v_1 \dots v_{s-1}$ , avec  $s \geq 1$  et définissons :

$$x_0 x_1 x_2 \dots = v_0 v_1 \dots v_{s-1} (w_0 w_1 \dots w_{r-1})^\omega.$$

Pour  $i \geq 1$ , on définit  $q_i := \delta(q_0, x_0 x_1 x_2 \dots x_{i-1})$ . Puisque la suite  $\mathbf{a}$  est automatique, l'ensemble des états  $\{q_i : i \geq 0\}$  est fini.

De même, l'ensemble  $\{(q_i; i \bmod r) : i \geq s\}$  est fini. Mais si  $i \geq s$ , l'état suivant  $q_{i+1}$  est complètement déterminé par  $q_i$  et  $i \bmod r$ , car :

$$\begin{aligned} q_{i+1} &= \delta(q_0, x_0 x_1 x_2 \dots x_i) = \delta(\delta(q_0, x_0 x_1 x_2 \dots x_{i-1}), x_i) \\ &= \delta(q_i, x_i) = \delta(q_i, w_{(i-s) \bmod r}). \end{aligned}$$

Comme il y a au plus  $|Q| \cdot r$  possibilités pour  $(q_i, i \bmod r)$ , à partir d'un certain rang, la suite devient périodique (de période au plus  $|Q| \cdot r$ ). □

**Corollaire I.1.1.** *Si  $(a_n)_{n \geq 0}$  est  $k$ -automatique, alors les sous-suites  $(a_{k^n})_{n \geq 0}$  et  $(a_{k^n - 1})_{n \geq 0}$  sont ultimement périodiques.*

*Démonstration.* Puisque  $(k^n)_k = \underbrace{10 \dots 0}_n$ , on retrouve le résultat du théorème précédent.

Cela correspond au cas particulier  $v = 1$  et  $w = 0$ .

De même, puisque  $(k^n - 1)_k = \underbrace{1 \dots 1}_n$ , on reconnaît  $v = \epsilon$  et  $w = 1$ . Par conséquent, les suites sont ultimement périodiques. □

## I.2 Théorème de Christol

Nous allons maintenant démontrer le théorème de Christol. Pour cela, nous commençons avec quelques préliminaires sur les séries formelles et nous allons donner quelques exemples.

### I.2.1 Préliminaires algébriques

Dans cette partie, nous rappelons quelques définitions et résultats élémentaires concernant les séries formelles.

Soit  $R$  un anneau commutatif. On note  $R[X]$  l'ensemble des polynômes à coefficients dans  $R$ . Alors  $R[X]$  forme un anneau commutatif pour l'addition et la multiplication usuelles d'élément neutre 1. Dans le cas particulier où  $R = K$  est un corps,  $K[X]$  représente un anneau commutatif intègre. Ainsi on peut considérer le corps des fractions de  $K[X]$ , noté  $K(X)$ ; il contient toutes les fractions rationnelles :  $\frac{f}{g}$ , où  $f, g \in K[X]$  et  $g \neq 0$ .

L'anneau des séries formelles sur  $K$  de la variable  $X$ , noté  $K[[X]]$  est l'ensemble des sommes infinies de la forme  $\sum_{n \geq 0} a_n X^n$ , où les coefficients  $a_n$  sont des éléments de  $K$ . L'addition et la multiplication sont définies comme pour les séries entières :

Si  $A(X) = \sum_{i \geq 0} a_i X^i$  et  $B(X) = \sum_{i \geq 0} b_i X^i$  alors :

$$A(X) + B(X) = \sum_{i \geq 0} (a_i + b_i) X^i$$

et

$$A(X)B(X) = \sum_{n \geq 0} \left( \sum_{i+j=n} a_i b_j \right) X^n.$$

On définira les éléments unités de l'anneau  $K[[X]]$  comme étant les séries formelles  $A(X) = \sum_{i \geq 0} a_i X^i$  avec  $a_0 \neq 0$ .

Si  $K$  est un corps,  $K[[X]]$  désigne un domaine intègre. Donc c'est possible de considérer le corps des fractions  $K((X))$ . Ce corps coïncide avec le corps des séries de Laurent, qui sont les séries de la forme  $A(X) = \sum_{i \geq a} a_i X^i$ , pour un certain entier  $a$ . On remarque qu'une telle expression a un nombre infini des puissances positives de  $X$ , mais seulement un nombre fini de puissances négatives.

Parfois, on écrit  $X = \frac{1}{T}$ , où  $T$  est une indéterminée. Dans ce cas, une analogie avec l'écriture en base  $k$  d'un nombre réel apparaît. En effet, on peut mettre en correspondance la série formelle  $\sum \frac{a_n}{T^n}$  et le nombre réel  $\sum \frac{a_n}{k^n}$  car, si on note  $T = k$ , alors un nombre réel a un développement comprenant un nombre fini de puissances positives de  $k$ , mais éventuellement une infinité des puissances négatives.

Dans la suite de cette étude, on considère  $K$  étant le corps fini à  $q$  éléments, noté en général  $\mathbb{F}_q$  et  $q$  représentant une puissance d'un nombre premier  $p$ . Nous rappelons l'égalité fondamentale suivante :

Etant donné  $A(X) = \sum_{n \geq 0} a_n X^n \in \mathbb{F}_q((X))$ , alors

$$A(X^q) = A(X)^q. \quad ((P))$$

On termine ces rappels par la notion d'algébricité d'une série formelle, définition analogue à la notion d'algébricité d'un nombre réel.

**Définition I.2.1.** Une série formelle  $f(X) = \sum_{n \geq 0} a_n X^n \in K[[X]]$  est algébrique sur  $K(X)$  s'il existe un entier  $d \geq 1$  et des polynômes  $A_0(X), \dots, A_d(X) \in K[X]$ , non tous nuls, tels que :

$$A_0 + A_1 f + A_2 f^2 + \dots + A_d f^d = 0$$

Un premier exemple est la série  $f(X) = X + X^2 + \dots = \sum_{i \geq 0} X^{2^i}$  qui est algébrique sur  $\mathbb{F}_2(X)$  car  $f(X)^2 + f(X) + X = 0$ .

## I.2.2 Exemples de séries formelles algébriques

Dans la partie précédente, on a évoqué quelques exemples de suites automatiques. Nous allons à présent démontrer que les séries formelles associées à ces suites sont algébriques. Plus précisément, on va démontrer que la série dont la suite des coefficients est la suite de Thue–Morse (vue à valeurs dans  $\mathbb{F}_2$ ) est algébrique sur le corps  $\mathbb{F}_2(X)$ . De même, on démontrera l’algébricité sur  $\mathbb{F}_2(X)$  de la série formelle associée à la suite de Rudin–Shapiro (vue à valeurs dans  $\mathbb{F}_2$ ), ainsi que l’algébricité sur  $\mathbb{F}_3(X)$  de la série formelle associée à la suite des entiers de Cantor (vue à valeurs dans  $\mathbb{F}_3$ ).

**La suite de Thue–Morse.** La suite de Thue–Morse, notée  $(t_n)_{n \geq 0}$  calcule le nombre de “1” modulo 2 dans la représentation de  $n$  en base 2. La suite de Thue–Morse est 2-automatique. La définition de la suite  $(t_n)_{n \geq 0}$  implique que  $t_{2n} = t_n$  et  $t_{2n+1} = 1 + t_n$  (1).

Nous allons démontrer dans la suite que la série formelle  $T(X) = \sum_{n \geq 0} t_n X^n$ , est algébrique sur  $\mathbb{F}_2(X)$ .

$$\begin{aligned}
 T(X) &= \sum_{n \geq 0} t_{2n} X^{2n} + \sum_{n \geq 0} t_{2n+1} X^{2n+1}, \text{ séparant les indices pairs et impairs} \\
 &= \sum_{n \geq 0} t_n X^{2n} + \sum_{n \geq 0} (1 + t_n) X^{2n+1}, \text{ en utilisant la propriété (1)} \\
 &= T(X^2) + XT(X^2) + \sum_{n \geq 0} X^{2n+1} \\
 &= T(X^2) + XT(X^2) + \frac{X}{1 - X^2} \\
 &= (1 + X)T(X^2) + \frac{X}{1 - X^2}.
 \end{aligned}$$

Ainsi, en regroupant les termes et en utilisant l’égalité (P), on obtient le résultat suivant :

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

et par conséquent, la série formelle  $T(X)$  est bien algébrique sur  $\mathbb{F}_2(X)$ .

**Remarque.** Le fait qu’on se place dans un corps de caractéristique positive est très important ; ceci nous a permis de trouver une équation vérifiée par la série  $T(X)$ . En effet, si on regarde la série  $T(X)$  comme élément de  $\mathbb{C}((X))$ , elle n’est cette fois plus algébrique : elle est non seulement transcendante mais même hypertranscendante. Nous rappelons qu’une série formelle  $F(X)$  à coefficients dans un corps  $K$  est hypertranscendante si, et seulement si, elle et toutes ses dérivées sont linéairement indépendantes sur  $K(X)$ . Autrement dit, il n’existe pas une équation différentielle du type  $P(X, F(X), F'(X), \dots, F^{(k)}(X)) = 0$ , où  $P$  est un polynôme à coefficients dans le corps  $K(X)$  et  $k$  est un entier positif.

**La suite de Rudin–Shapiro.** Soit  $(s_n)_{n \geq 0}$  la suite de Rudin–Shapiro. Elle calcule le nombre d’occurrences de “11” modulo 2 dans la représentation de  $n$  en base 2. La définition

de la suite  $(s_n)_{n \geq 0}$  implique que  $s_{2n} = s_n$  et  $s_{4n+1} = s_n$  et  $s_{4n+3} = s_{2n+1} + 1$ . (2)

Nous allons démontrer que la serie formelle associée,  $S(X) = \sum_{n \geq 0} s_n X^n$ , est algébrique sur  $\mathbb{F}_2(X)$ .

Pour cela, on écrit

$$S(X) = \sum_{n \geq 0} s_{2n} X^{2n} + \sum_{n \geq 0} s_{2n+1} X^{2n+1}, \text{ en écrivant suivant les indices pairs et impairs}$$

et, en notant

$$T(X) = \sum_{n \geq 0} s_{2n+1} X^n,$$

on obtient

$$S(X) = S(X^2) + XT(X^2) = S(X^2) + XT(X^2) = S(X)^2 + XT(X)^2. \quad (3)$$

D'autre part, en utilisant la remarque précédente sur la suite  $(s_n)_{n \geq 0}$ ,

$$\begin{aligned} T(X) &= \sum_{n \geq 0} s_{4n+1} X^{2n} + \sum_{n \geq 0} s_{4n+3} X^{2n+1} \\ &= \sum_{n \geq 0} s_n X^{2n} + X \sum_{n \geq 0} (s_{2n+1} + 1) X^{2n}. \end{aligned}$$

Par conséquent, on obtient :

$$T(X) = S(X)^2 + XT(X)^2 + \frac{X}{1-X^2} = S(X)^2 + XT(X)^2 + \frac{X}{(1+X)^2}. \quad (4)$$

En additionnant les relations (3) et (4), il vient :

$$S(X) + T(X) = \frac{X}{(1+X)^2}$$

et donc

$$S(X)^2 + T(X)^2 = \frac{X^2}{(1+X)^4}$$

ce qui implique que

$$S(X) = S(X)^2 + X \left( S(X)^2 + \frac{X^2}{(1+X)^4} \right).$$

Finalement, en terminant le calcul, on obtient la relation suivante, ce qui démontre l'algébricité de la série  $S(X)$  :

$$(1+X)^5 S(X)^2 + (1+X)^4 S(X) + X^3 = 0.$$

**La suite des entiers de Cantor.** Rappelons que la suite des entiers de Cantor, notée  $(c_n)_{n \geq 0}$ , est définie de la façon suivante :

$$c_n = \begin{cases} 1 & \text{si } (n)_3 \text{ ne contient que les chiffres 0 et 2} \\ 0 & \text{si } (n)_3 \text{ contient le chiffre 1.} \end{cases}$$

C'est une suite 3-automatique. La définition de la suite  $(c_n)_{n \geq 0}$  implique que  $c_{3n} = c_n = c_{3n+2}$  et  $c_{3n+1} = 0$ .

Nous allons démontrer dans la suite que la série formelle associée,  $C(X) = \sum_{n \geq 0} c_n X^n$ , est algébrique sur  $\mathbb{F}_3(X)$ .

$$\begin{aligned} C(X) &= \sum_{n \geq 0} c_{3n} X^{3n} + \sum_{n \geq 0} c_{3n+1} X^{3n+1} + \sum_{n \geq 0} c_{3n+2} X^{3n+2} \\ &= \sum_{n \geq 0} c_n X^{3n} + \sum_{n \geq 0} c_n X^{3n+2}. \end{aligned}$$

Donc

$$C(X) = C(X^3) + X^2 C(X^3)$$

et par conséquent

$$(1 + X^2)C(X)^3 - C(X) = 0.$$

Ainsi la série formelle  $C(X)$  est algébrique sur  $\mathbb{F}_3(X)$ .

Nous venons de présenter quelques exemples de séries algébriques dont les suites des coefficients sont automatiques. La première partie de ce mémoire a pour but de démontrer qu'il s'agit en fait d'un phénomène tout à fait général, comme l'explique le théorème de Christol.

### I.2.3 Le théorème de Christol

Nous allons démontrer à présent le théorème principal de cette première partie du mémoire.

**Théorème I.2.1** (Christol). *Soit  $p$  un nombre premier. Soit  $\Delta$  un ensemble fini, non vide, et  $\mathbf{a} = (a_i)_{i \geq 0}$  une suite à valeurs dans  $\Delta$ . Alors la suite  $\mathbf{a}$  est  $p$ -automatique si, et seulement si, il existe un entier strictement positif  $n$  et une application injective  $\beta : \Delta \rightarrow \mathbb{F}_{p^n}$  telle que la série formelle  $\sum_{i \geq 0} \beta(a_i) X^i$  est algébrique sur le corps  $\mathbb{F}_{p^n}(X)$ .*

**Définition I.2.2.** On définit la transformation linéaire  $\Lambda_r$  sur l'ensemble des séries formelles à coefficients dans le corps fini à  $q$  éléments,  $\mathbb{F}_q$ , et  $r$  un entier tel que  $0 \leq r < q$  :

$$\Lambda_r : \begin{array}{ccc} \mathbb{F}_q[[X]] & \longrightarrow & \mathbb{F}_q[[X]] \\ \sum_{i \geq 0} a_i X^i & \longmapsto & \sum_{i \geq 0} a_{qi+r} X^i \end{array}$$

Cet opérateur est appelé l'opérateur de Cartier.

Afin de démontrer le théorème principal, nous aurons besoin des trois lemmes.

**Lemme I.2.1.** *On a les propriétés suivantes :*

a) *Si  $A$  est une série formelle à coefficients dans  $\mathbb{F}_q$ , alors*

$$A(X) = \sum_{i \geq 0} a_i X^i = \sum_{0 \leq r < q} X^r \Lambda_r(A(X))^q.$$

b) *Si  $G$  et  $H$  sont deux séries formelles à coefficients dans  $\mathbb{F}_q$ , alors*

$$\Lambda_r(G^q H) = G \Lambda_r(H).$$

*Démonstration.* a) On a :

$$\begin{aligned} A(X) &= \sum_{i \geq 0} a_i X^i \\ &= \sum_{0 \leq r < q} \sum_{i \geq 0} a_{qi+r} X^{qi+r} && \text{en groupant les indices } i \text{ suivant leurs valeurs modulo } q \\ &= \sum_{0 \leq r < q} X^r \left( \sum_{i \geq 0} a_{qi+r} X^i \right)^q \\ &= \sum_{0 \leq r < q} X^r \Lambda_r(A(X))^q && \text{par définition de l'opérateur } \Lambda_r. \end{aligned}$$

b) Soient

$$G(X) = \sum_{k \geq 0} g_k X^k$$

et

$$H(X) = \sum_{j \geq 0} h_j X^j.$$

Alors

$$\begin{aligned} \Lambda_r(G^q H) &= \Lambda_r \left( \left( \sum_{k \geq 0} g_k X^k \right)^q \left( \sum_{j \geq 0} h_j X^j \right) \right) \\ &= \Lambda_r \left( \left( \sum_{k \geq 0} g_k X^{qk} \right) \left( \sum_{j \geq 0} h_j X^j \right) \right). \end{aligned}$$

Ainsi, en développant le produit de deux séries dans la parenthèse, on obtient :

$$\begin{aligned}
\Lambda_r(G^q H) &= \Lambda_r \left( \sum_{i \geq 0} X^i \sum_{k,j \geq 0, qk+j=i} g_k h_j \right) = \sum_{i \geq 0} X^i \left( \sum_{k,j \geq 0, qk+j=qi+r} g_k h_j \right) \\
&= \sum_{i \geq 0} X^i \left( \sum_{0 \leq k \leq i} g_k h_{q(i-k)+r} \right) = \sum_{k \geq 0} g_k X^k \left( \sum_{i \geq k} h_{q(i-k)+r} X^{i-k} \right) \\
&= \sum_{k \geq 0} g_k X^k \left( \sum_{i \geq 0} h_{qi+r} X^i \right) = \left( \sum_{k \geq 0} g_k X^k \right) \left( \sum_{i \geq 0} h_{qi+r} X^i \right) \\
&= G \Lambda_r(H).
\end{aligned}$$

□

**Lemme I.2.2.** *Une série formelle  $A(X) = \sum_{i \geq 0} a_i X^i \in \mathbb{F}_q[[X]]$  est algébrique sur  $\mathbb{F}_q(X)$  si, et seulement si, il existe des polynômes  $B_0(X), B_1(X), \dots, B_t(X)$ , non tous nuls, tels que :*

$$B_0 A + B_1 A^q + B_2 A^{q^2} + \dots + B_t A^{q^t} = 0.$$

De plus, on peut supposer que  $B_0 \neq 0$ .

*Démonstration.* La première partie du lemme est connue sous le nom de lemme d'Ore. Si  $A$  est algébrique, alors les séries  $A, A^q, A^{q^2}, \dots$  ne peuvent pas être toutes linéairement indépendantes et donc il existe des polynômes  $B_0(X), B_1(X), \dots, B_t(X)$ , non tous nuls, tels que :

$$B_0 A + B_1 A^q + B_2 A^{q^2} + \dots + B_t A^{q^t} = 0.$$

Réciproquement, si une telle relation existe, alors  $A$  est algébrique par définition.

Maintenant, il reste à montrer qu'on peut trouver une telle relation avec  $B_0 \neq 0$ . Supposons :

$$B_0 A + B_1 A^q + B_2 A^{q^2} + \dots + B_t A^{q^t} = 0$$

avec  $t$  minimal et soit  $j$  le plus petit indice tel que  $B_j(X) \neq 0$ . Le but est de montrer que  $j = 0$ . D'après le lemme I.2.1,

$$B_j = \sum_{0 \leq r < q} X^r (\Lambda_r(B_j))^q.$$

Ce dernier est non nul, donc il existe un  $r$  tel que  $\Lambda_r(B_j) \neq 0$ . Puisque  $\sum_{j \leq i \leq t} B_i A(X)^{q^i} = 0$ , en appliquant l'opérateur  $\Lambda_r$  et le résultat obtenu au lemme I.2.1, on obtient la relation suivante :

$$\sum_{j \leq i \leq t} \Lambda_r(B_i) A^{q^{i-1}} = 0.$$

Supposons que  $j \neq 0$ . On obtiendrait alors une nouvelle relation, dans laquelle le coefficient de  $A^{q^{j-1}}$  est non nul, ce qui contredirait la minimalité de  $t$ . Donc  $j = 0$  et par conséquent  $B_0$  est non nul. □

**Lemme I.2.3.** Soit  $\mathbf{a} = (a_i)_{i \geq 0}$  une suite à valeurs dans  $\mathbb{F}_q$ . Alors  $\mathbf{a}$  est  $q$ -automatique si, et seulement si, il existe une famille de séries formelles  $\mathcal{F}$  telle que :

a)  $A(X) = \sum_{i \geq 0} a_i X^i \in \mathcal{F}$

b) pour toute série  $g$  de  $F$  et pour tout  $r$ ,  $0 \leq r < q$ ,  $\Lambda_r(g) \in \mathcal{F}$ .

*Démonstration.* La suite  $\mathbf{a}$  est  $q$ -automatique si, et seulement si, le  $q$ -noyau  $N_q(\mathbf{a})$  est fini, donc si, et seulement si,  $N_q(\mathbf{a}) = \{\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \dots, \mathbf{a}^{(d)}\}$ , avec  $\mathbf{a}^{(1)} = \mathbf{a}$  et  $\mathbf{a}^{(i)} = (a_n^{(i)})_{n \geq 0}$ , pour un certain entier  $d$ .

“ $\implies$ ” Posons

$$\mathcal{F} = \left\{ \sum_{n \geq 0} a_n^{(i)} X^n : 1 \leq i \leq r \right\}$$

Il est clair que  $\mathcal{F}$  est finie et  $\mathcal{F}$  contient la série  $A(X) = \sum_{n \geq 0} a_n^{(1)} X^n = \sum_{n \geq 0} a_n X^n$ . On vérifie la stabilité de la famille  $\mathcal{F}$  par rapport à l'opérateur  $\Lambda_r$ . Soit  $g(X) = \sum_{n \geq 0} a_n^{(i_0)} X^n$  appartenant à  $\mathcal{F}$ . Alors

$$\Lambda_r(g(X)) = \Lambda_r\left(\sum_{n \geq 0} a_n^{(i_0)} X^n\right) = \sum_{n \geq 0} a_{qn+r}^{(i_0)} X^n \in \mathcal{F}$$

car  $(a_{qn+r}^{(i_0)})_{n \geq 0}$  appartient au  $q$ -noyau, donc cette série est égale à l'un des  $\mathbf{a}^{(i)}$ .

“ $\impliedby$ ” Comme  $A(X) = \sum_{i \geq 0} a_i X^i \in \mathcal{F}$ , en appliquant plusieurs fois la stabilité de  $\Lambda_r$ , pour tous les  $r$  tels que  $0 \leq r < q$ , on démontre que chaque série  $\sum_{n \geq 0} a_n^{(i)} X^n \in \mathcal{F}$ . Comme  $\mathcal{F}$  est finie, il existe un nombre fini d'indices  $i$ , donc un nombre fini de  $a_n^{(i)}$ . Ainsi le  $q$ -noyau  $N_q(\mathbf{a})$  est fini. □

*Démonstration du théorème de Christol.* “ $\implies$ ” Soient  $p$  un nombre premier et  $\mathbf{a} = (a_n)_n$  une suite  $p$ -automatique. On choisit un entier  $n$  assez grand, de sorte que le cardinal de l'ensemble  $\Delta$  est inférieur à  $p^n$ . Soit  $\beta : \Delta \rightarrow \mathbb{F}_{p^n}$  une application injective. On peut supposer sans perte de généralité que  $\Delta \subseteq \mathbb{F}_{p^n}$  et nous allons démontrer que la série  $\sum_{i \geq 0} a_i X^i$  est algébrique sur  $\mathbb{F}_{p^n}(X)$ .

Comme la suite  $\mathbf{a} = (a_i)_{i \geq 0}$  est  $p$ -automatique, elle est aussi  $q$ -automatique, où  $q = p^n$  et donc le  $q$ -noyau  $N_q(\mathbf{a})$  est fini. Ainsi on pose  $(\mathbf{a}) = \{\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \dots, \mathbf{a}^{(d)}\}$ , avec  $\mathbf{a}^{(1)} = \mathbf{a}$  et  $\mathbf{a}^{(i)} = (a_n^{(i)})_{n \geq 0}$ .

Définissons les séries  $A_j(X) = \sum_{n \geq 0} a_n^{(j)} X^n$ , pour tous les entiers  $j$ ,  $1 \leq j \leq d$ . Ainsi :

$$A_j(X) = \sum_{0 \leq r < q} \sum_{m \geq 0} a_{qm+r}^{(j)} X^{qm+r} = \sum_{0 \leq r < q-1} X^r \sum_{m \geq 0} a_{qm+r}^{(j)} X^{qm}.$$

Comme  $(a_{qm+r}^{(j)})_{m \geq 0}$  est toujours un élément du  $q$ -noyau, il est égal à l'un des  $\mathbf{a}^{(i)}$ ,  $1 \leq i \leq d$ . Ceci montre que chaque  $A_j(X)$  est une  $\mathbb{F}_q(X)$ -combinaison linéaire des séries  $A_i(X^q)$ . Autrement dit,  $A_j(X)$  appartient au  $\mathbb{F}_q(X)$ -espace vectoriel engendré par les séries  $A_i(X^q)$  :

$$\forall j \in [1, d], \quad A_j(X) \in \langle A_1(X^q), A_2(X^q), \dots, A_d(X^q) \rangle.$$

Mais ceci implique :

$$\forall j \in [1, d], \quad A_j(X^q) \in \langle A_1(X^{q^2}), A_2(X^{q^2}), \dots, A_d(X^{q^2}) \rangle$$

et par transitivité :

$$\forall j \in [1, d], \quad A_j(X) \in \langle A_1(X^{q^2}), A_2(X^{q^2}), \dots, A_d(X^{q^2}) \rangle.$$

Ainsi

$$\forall j \in [1, d], \quad A_j(X), A_j(X^q) \in \langle A_1(X^{q^2}), A_2(X^{q^2}), \dots, A_d(X^{q^2}) \rangle.$$

Ceci implique que

$$\forall j \in [1, d], \quad A_j(X^q), A_j(X^{q^2}) \in \langle A_1(X^{q^3}), A_2(X^{q^3}), \dots, A_d(X^{q^3}) \rangle$$

et donc

$$\forall j \in [1, d], \quad A_j(X), A_j(X^q), A_j(X^{q^2}) \in \langle A_1(X^{q^3}), A_2(X^{q^3}), \dots, A_d(X^{q^3}) \rangle.$$

On peut itérer ce raisonnement et on obtient finalement :

$$\forall j \in [1, d], \quad A_j(X), A_j(X^q), A_j(X^{q^2}), \dots, A_j(X^{q^d}) \in \langle A_1(X^{q^{d+1}}), A_2(X^{q^{d+1}}), \dots, A_d(X^{q^{d+1}}) \rangle.$$

Or, la dimension de ce dernier, vu comme un  $\mathbb{F}_q(X)$ -espace vectoriel, est au plus égale à  $d$ . Par conséquent, les séries  $A_j(X), A_j(X^q), A_j(X^{q^2}), \dots, A_j(X^{q^d})$ , où  $j \in [1, d]$ , ne peuvent pas être linéairement indépendantes sur  $\mathbb{F}_q(X)$ .

En particulier, pour  $j = 1$ , les séries  $A(X), A(X^q), A(X^{q^2}), \dots, A(X^{q^d})$  sont liées, donc il existe une relation :

$$B_0A + B_1A^q + B_2A^{q^2} + \dots + B_dA^{q^d} = 0$$

où les polynômes  $B_0(X), B_1(X), \dots, B_d(X)$  ne sont pas tous nuls.

Par définition,  $A$  est algébrique sur  $\mathbb{F}_q(X) = \mathbb{F}_{p^n}(X)$  et la première implication du théorème de Christol est ainsi démontrée.

“ $\Leftarrow$ ” On suppose maintenant que la série  $A(X) = \sum_{i \geq 0} a_i X^i$  est algébrique sur  $\mathbb{F}_q(X)$ , avec  $q = p^n$  et on va démontrer que la suite  $\mathbf{a} = (a_i)_{i \geq 0}$  est  $q$ -automatique, donc aussi  $p$ -automatique (d’après le théorème 1.2).

D’après le lemme I.2.2, il existe des polynômes  $B_0(X), B_1(X), \dots, B_t(X)$ ,  $B_0 \neq 0$ , tels que :

$$B_0A + B_1A^q + B_2A^{q^2} + \dots + B_tA^{q^t} = 0.$$

Comme  $B_0 \neq 0$ , on peut poser  $G = \frac{A}{B_0}$ . Ainsi la relation précédente devient :

$$G + G^q B_1 B_0^{q-2} + \dots + G^{q^t} B_t B_0^{q^t-2} = 0$$

et donc

$$G = - \sum_{1 \leq i \leq t} G^{q^i} B_i B_0^{q^i - 2} = \sum_{1 \leq i \leq t} C_i G^{q^i}, \quad \text{avec } C_i = -B_i B_0^{q^i - 2}.$$

Soit  $N = \max(\deg B_0, \max_i \deg C_i)$ . Définissons la famille  $\mathcal{H}$  de séries formelles de la façon suivante :

$$\mathcal{H} = \{H \in \mathbb{F}_q[[X]] : H = \sum_{0 \leq i \leq t} D_i G^{q^i} \text{ avec } D_i \in \mathbb{F}_q[X] \text{ et } \deg D_i \leq N\}.$$

C'est une famille finie car le nombre de polynômes à coefficients dans  $\mathbb{F}_q$  et de degré inférieur ou égal à  $N$  est fini.

De plus,  $\mathcal{H}$  contient aussi la série formelle  $A(X) = \sum_{i \geq 0} a_i X^i$  car  $A = B_0 G$  et  $\deg B_0 \leq N$ .

Afin d'appliquer le lemme I.2.3 et de conclure donc que la suite  $\mathbf{a}$  est  $q$ -automatique, il reste à démontrer que pour toute  $H \in \mathcal{H}$  et pour tout  $r$ ,  $0 \leq r < q$ ,  $\Lambda_r(H) \in \mathcal{H}$ .

Soit  $H \in \mathcal{H}$  et soit  $r$ ,  $0 \leq r < q$ .

$$\begin{aligned} \Lambda_r(H) &= \Lambda_r \left( D_0 G + \sum_{1 \leq i \leq t} D_i G^{q^i} \right) = \Lambda_r \left( D_0 \sum_{1 \leq i \leq t} C_i G^{q^i} + \sum_{1 \leq i \leq t} D_i G^{q^i} \right) \\ &= \Lambda_r \left( \sum_{1 \leq i \leq t} (D_0 C_i + D_i) G^{q^i} \right) = \sum_{1 \leq i \leq t} \Lambda_r \left( (D_0 C_i + D_i) G^{q^i} \right) \\ &= \sum_{1 \leq i \leq t} \Lambda_r (D_0 C_i + D_i) G^{q^{i-1}}. \end{aligned}$$

Cette série appartient à  $\mathcal{H}$  si, et seulement si,  $\deg \Lambda_r(D_0 C_i + D_i) \leq N$ . Comme  $\deg D_0$ ,  $\deg D_i$ ,  $\deg C_i$  sont au plus  $N$ ,  $D_0 C_i + D_i$  est un polynôme de degré au plus  $2N$  et donc  $\Lambda_r(D_0 C_i + D_i)$  est un polynôme de degré au plus  $\frac{2N}{q}$ , donc au plus  $N$ , car  $q \geq 2$ .

Ainsi la famille  $\mathcal{H}$  remplit toutes les conditions du lemme I.2.3, et par conséquent la suite  $\mathbf{a}$  est  $q$ -automatique, donc  $p$ -automatique. Cela termine cette démonstration.  $\square$

#### I.2.4 Comparaison avec le développement $b$ -adique des nombres réels

Il est intéressant de contraster le théorème de Christol avec un résultat de la même nature concernant les nombres réels automatiques.

Comme nous venons de voir, le théorème de Christol affirme qu'une série formelle  $\sum_i a_i X^i \in \mathbb{F}_p((X))$  est algébrique sur le corps  $\mathbb{F}_p(X)$  si, et seulement si, elle est automatique.

En ce qui concerne les nombres réels, on distingue deux situations, selon que le nombre est rationnel ou irrationnel.

Par exemple, on considère le nombre dont le développement binaire est la suite de Thue–Morse étudiée précédemment :  $\mathbf{t} = 0.110100110010110\dots$

Ce nombre, appelé aussi la constante de Prouhet–Thue–Morse, est donc égal à :

$$\tau = \sum_i \frac{t_i}{2^{i+1}} = 0,412454033640\dots$$

Il est irrationnel et 2-automatique, puisque la suite de Thue–Morse est une suite infinie, non ultimement périodique, 2-automatique. De plus, en 1929, K. Mahler a démontré que le nombre  $\tau$  est transcendant.

Il est bien connu qu’un nombre est rationnel si et seulement si son développement dans une base entière  $b$  est ultimement périodique. En particulier, un tel développement peut être engendré par un automate fini.

On peut alors se demander si le développement en base  $b$  d’un nombre algébrique irrationnel peut être également engendré par un automate fini. Cette question a été posée en 1968 par Cobham [5] qui a conjecturé que la réponse doit être négative.

En 1988, Loxton et van der Poorten ont annoncé ce résultat : les nombres irrationnels algébriques ne peuvent pas être automatiques (c’est-à-dire le développement en base  $b$  d’un nombre irrationnel algébrique ne peut pas être engendré par un  $k$ -DFAO). Malheureusement, en 1993, Becker a remarqué que leur démonstration est en fait incomplète. Depuis, cet énoncé est parfois appelé conjecture de Cobham–Loxton–van der Poorten.

En 2006, Boris Adamczewski et Yann Bugeaud ont démontré ce résultat [1] en utilisant une méthode complètement différente basée sur le théorème du sous-espace de Schmidt.

Par conséquent, contrairement à ce qui se passe avec les séries formelles qui sont algébriques si, et seulement si, elles sont automatiques, le comportement des nombres réels est plutôt différent. Un nombre irrationnel algébrique ne peut pas être automatique. Ou, autrement dit, un nombre irrationnel automatique est transcendant. Par exemple, on peut conclure ainsi qu’il n’existe pas d’automate fini qui calcule les décimales de la racine carrée de 2.

### I.3 Application du théorème de Christol

En 1935 Carlitz a introduit la fonction connue sous le nom de “fonction zeta de Carlitz”, analogue à la “fonction zeta de Riemann”.

On rappelle que la fonction zeta de Riemann est définie pour tous les nombres complexes  $s$ ,  $\Re(s) > 1$ , de la manière suivante :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

La fonction zeta de Carlitz est définie, par analogie, de la façon suivante :

$$\zeta : \mathbb{N}^* \rightarrow \mathbb{F}_q \left[ \left[ \frac{1}{X} \right] \right]; \quad \zeta(n) = \sum_{\substack{P \in \mathbb{F}_q[X] \\ P \text{ unitaire}}} \frac{1}{P^n}$$

De plus, il existe une série formelle de Laurent appelée  $\Pi_q$  telle que :

$$\forall n \equiv 0 \pmod{q-1}, n \neq 0, \exists r_n \in \mathbb{F}_q(X), \zeta(n) = \Pi_q^n r_n.$$

Cette série peut être décrite par le produit infini suivant :

$$\Pi_q = \prod_{j=1}^{\infty} \left( 1 - \frac{X^{q^j} - X}{X^{q^{j+1}} - X} \right).$$

**Remarque.** Cette propriété est similaire aux résultats classiques des valeurs de la fonction zeta de Riemann pour les entiers pairs. En effet, il est connu que si  $s$  est pair,  $\zeta(s) = \pi^s r$ , où  $r$  est un nombre rationnel. Par exemple,  $\zeta(2) = \frac{\pi^2}{6}$  et  $\zeta(4) = \frac{\pi^4}{90}$ . Par contre ce résultat ne reste plus vrai pour les entiers impairs. Ainsi, la série  $\Pi_q$  est bien un analogue naturel du réel  $\pi$ .

On peut se demander si cette série de Laurent  $\Pi_q$  est transcendante sur  $\mathbb{F}_q(X)$ , par analogie au nombre  $\pi$ , qui est transcendant sur le corps des rationnels  $\mathbb{Q}$ . De même, ces questions apparaissent pour les valeurs de la fonction  $\zeta$  de Carlitz, par analogie avec les valeurs de la fonction  $\zeta$  de Riemann.

Actuellement, dans l'étude de transcendance des fonctions  $\zeta$  ou  $\Pi_q$  de Carlitz, plusieurs méthodes sont connues. La première démonstration est due à Wade [12], dans les années quarante. Il a démontré plusieurs résultats de transcendance, et en particulier, celle de la série formelle  $\Pi_q$ . La méthode utilisée ressemble à une méthode classique de transcendance de nombres réels sur le corps des rationnels. Cette méthode a été ensuite étendue par Dammame et Hellegouarch [6], qui ont démontré la transcendance de  $\zeta(n)$ , pour tout  $n \in \mathbb{N}^*$ . Une autre démonstration, due à de Mathan et Cherif [4], repose sur une méthode d'approximation diophantienne, et essentiellement sur le calcul des mesures d'irrationalité des valeurs de la fonction  $\zeta$  de Carlitz. La méthode la moins élémentaire de transcendance de ces fonctions de Carlitz, qui utilise les modules de Drinfeld, a été développée par Yu.

A l'aide des modules de Drinfeld, il a démontré [13] que :  $\zeta(n)$  est transcendant pour tout  $n \in \mathbb{N}^*$  et que  $\frac{\zeta(n)}{\Pi_q^n}$  est transcendant pour tout  $n \neq 0 \pmod{q-1}$ .

Une dernière méthode pour démontrer la transcendance de certaines séries formelles est basée sur l'utilisation du théorème de Christol. Elle a été en particulier développée par Allouche et Berthé (voir par exemple [2, 3, 10]).

Nous allons à présent démontrer la transcendance de  $\Pi_q$  en utilisant cette dernière approche.

**Théorème I.3.1.** *La fonction  $\Pi_q$  de Carlitz est transcendante sur  $\mathbb{F}_q(X)$ .*

*Démonstration.* Par l'absurde, nous supposons que la fonction  $\Pi_q$  est algébrique sur  $\mathbb{F}_q(X)$ . En utilisant les propriétés d'algébricité, sa dérivée,  $\Pi'_q$  est aussi algébrique et donc le quotient  $\frac{\Pi'_q}{\Pi_q}$  l'est aussi. Mais :

$$\begin{aligned} \frac{\Pi'_q}{\Pi_q} &= \sum_{k \geq 1} \left( \frac{1}{1 - \frac{X^{q^k} - X}{X^{q^{k+1}} - X}} \right) \left( \frac{(X^{q^{k+1}} - X) - (X^{q^k} - X)}{(X^{q^{k+1}} - X)^2} \right) \\ &= \sum_{k \geq 1} \frac{1}{X^{q^{k+1}} - X} \\ &= \left( \sum_{k \geq 1} \frac{1}{X^{q^k} - X} \right) - \frac{1}{X^q - X}. \end{aligned}$$

Ceci implique que la série

$$B = \sum_{k \geq 1} \frac{1}{X^{q^k} - X}$$

est aussi algébrique. Mais

$$\begin{aligned} B &= \sum_{k \geq 1} \frac{1}{X^{q^k} - X} = \sum_{k \geq 1} \frac{1}{X^{q^k} (1 - (\frac{1}{X})^{q^k - 1})} \\ &= \sum_{k \geq 1} \frac{1}{X^{q^k}} \sum_{n \geq 0} \left( \frac{1}{X} \right)^{n(q^k - 1)} = \frac{1}{X} \sum_{k \geq 1} \frac{1}{X^{q^k} - 1} \sum_{n \geq 0} \left( \frac{1}{X} \right)^{n(q^k - 1)} \\ &= \frac{1}{X} \sum_{\substack{n \geq 0 \\ k \geq 1}} \left( \frac{1}{X} \right)^{(n+1)(q^k - 1)} = \frac{1}{X} \sum_{\substack{k \geq 1 \\ n \geq 1}} \left( \frac{1}{X} \right)^{n(q^k - 1)} \\ &= \frac{1}{X} \sum_{m \geq 1} \left( \frac{1}{X} \right)^m \sum_{\substack{k, n \geq 1 \\ n(q^k - 1) = m}} 1 = \frac{1}{X} \sum_{m \geq 1} \left( \frac{1}{X} \right)^m \sum_{\substack{k \geq 1 \\ q^k - 1 | m}} 1. \end{aligned}$$

Cette dernière expression peut aussi être écrite sous la forme

$$B = \frac{1}{X} \sum_{m \geq 1} \left( \frac{1}{X} \right)^m c(m)$$

en posant

$$c(m) = \sum_{\substack{k \geq 1 \\ q^k - 1 | m}} 1.$$

$B$  est algébrique sur  $\mathbb{F}_q(X)$  et donc la série

$$\sum_{m \geq 1} c(m) \left( \frac{1}{X} \right)^m$$

est aussi algébrique, ce qui, d'après le théorème de Christol, implique que la suite  $(c(m))_{m \geq 1}$  est  $q$ -automatique.

D'après le corollaire I.1.1, la suite  $(c(q^n - 1))_{n \geq 0}$  est ultimement périodique. Mais

$$c(q^n - 1) = \sum_{\substack{k \geq 1 \\ q^k - 1 | q^n - 1}} 1 = \sum_{\substack{k \geq 1 \\ k | n}} 1 = d(n)$$

où  $d(n)$  représente le nombre de diviseurs de  $n$ .

Ainsi, la suite  $d(n)$  est ultimement périodique et donc la suite  $(d(n) \bmod q)_{n \geq 1}$  l'est aussi. Comme  $q$  est une puissance du nombre premier  $p$ , alors la suite  $(d(n) \bmod p)_{n \geq 1}$  est également ultimement périodique. Cela implique qu'il existe des entiers  $t \geq 1$ ,  $n_0 \geq 0$  tels que pour tous les entiers  $n \geq n_0$  et  $i \geq 1$ , on a :

$$d(n + it) \equiv d(n) \pmod{p}.$$

On choisit  $i = ni'$  et alors  $d(n(1 + i't)) \equiv d(n) \pmod{p}$  pour tout  $i' \geq 1$ .

D'après le théorème de Dirichlet, on peut trouver  $i' \geq 1$  tel que  $1 + i't = p'$  est un nombre premier. Pour  $n = p'$  on obtient alors :

$$d(p'^2) \equiv d(p') \pmod{p}.$$

Mais  $d(p'^2) = 3$  et  $d(p') = 2$  et donc  $3 \equiv 2 \pmod{p}$ , ce qui est absurde. On obtient ainsi une contradiction avec la supposition que  $\Pi_q$  est algébrique, ce qui termine cette démonstration.  $\square$

## II Généralisation du théorème de Christol

La deuxième partie de ce mémoire consiste à étudier un résultat récent de Kedlaya [9]. Il s'agit d'une généralisation du théorème de Christol au corps des séries formelles de Hahn.

### II.1 Présentation du théorème de Kedlaya

Le théorème de Christol démontré dans la première partie du mémoire donne une description concrète des éléments de  $\mathbb{F}_q((t))$  qui sont algébriques sur  $\mathbb{F}_q(t)$  ; il montre, comme nous l'avons vu, qu'une série est algébrique sur  $\mathbb{F}_q(t)$  si, et seulement si, la suite de ses coefficients est  $q$ -automatique. Puisque le corps  $\mathbb{F}_q((t))$  est loin d'être algébriquement clos, le théorème de Christol n'offre qu'une description incomplète des éléments algébriques sur  $\mathbb{F}_q(t)$ .

En effet, il existe des polynômes à coefficients dans  $\mathbb{F}_q(t)$  qui n'ont pas de racines dans le corps de séries formelles  $\mathbb{F}_q((t))$ . Par exemple, le polynôme d'Artin–Schreier

$$P(X) = X^p - X - \frac{1}{t}$$

n'a pas de racines dans le corps  $\mathbb{F}_q((t))$ , ni même dans le corps de Puiseux :  $\bigcup_{i=1}^{\infty} \mathbb{F}_q((t^{1/i}))$ .

**Remarque.** Puiseux a montré que si  $K$  est un corps de caractéristique 0, alors tout polynôme unitaire de degré  $n$  à coefficients dans  $K(t)$  se factorise complètement sur  $L((t^{1/n}))$  pour  $L$  une extension finie de  $K$  et  $n$  un entier positif. Ainsi, pour un corps algébriquement clos  $K$  de caractéristique 0, le corps  $\bigcup_{i=1}^{\infty} K((t^{1/i}))$  est aussi algébriquement clos et contient en particulier la clôture de  $K(t)$ .

On peut d'ailleurs remarquer que le polynôme d'Artin–Schreier  $P$  possède, formellement, les racines suivantes :

$$x = c + t^{-1/p} + t^{-1/p^2} + \dots, \quad \text{pour } c = 0, 1, 2, \dots, p-1.$$

Il se factorise donc complètement dans le corps des séries de Hahn  $\mathbb{F}_q((t^{\mathbb{Q}}))$  (voir définition II.1.3).

Dans un article récent [9], Kedlaya généralise le théorème de Christol, en se plaçant dans le corps des séries formelles de Hahn pour déterminer la clôture algébrique de  $\mathbb{F}_p(t)$ . Pour cela, il définit la notion de quasi- $p$ -automaticité. Une série formelle généralisée  $\sum_{i \in I} x_i t^i$  est quasi- $p$ -automatique si elle est telle que, si on effectue une affinité rationnelle sur les exposants de  $t$ , leurs dénominateurs deviennent des puissances de  $p$  et les coefficients peuvent alors être calculés par un  $p$ -automate fini.

Plus précisément, cette partie a pour but de démontrer le théorème suivant.

**Théorème II.1.1** (Kedlaya). *Soit  $q$  une puissance du nombre premier  $p$  et soit  $f : \mathbb{Q} \longrightarrow \mathbb{F}_q$  une fonction à support bien ordonné.*

*Alors la série généralisée  $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est algébrique sur  $\mathbb{F}_q(t)$  si, et seulement si, elle est quasi- $p$ -automatique.*

Cette partie est organisée comme suit. Nous commençons par présenter le théorème de Kedlaya. Pour cela, nous faisons quelques rappels sur les séries de Hahn et sur les séries quasi- $p$ -automatiques. Pour mieux appréhender ce résultat, nous l'illustrons en étudiant un exemple de série de Hahn algébrique. Ensuite, nous rappelons quelques outils algébriques, qui nous serviront, dans la dernière partie du mémoire, à démontrer le théorème de Kedlaya.

### II.1.1 Séries formelles de Hahn–Mal’cev–Neumann

Nous commençons tout d’abord par la définition générale des séries formelles généralisées.

**Définition II.1.1.** Un groupe abélien  $G$  est *totalelement ordonné* s’il existe une relation binaire “ $>$ ” telle que, pour tous  $a, b, c \in G$  :

$$\begin{aligned} a &\not> b; \\ a &\not> b, b &\not> a \Rightarrow a = b; \\ a &> b, b > c \Rightarrow a > c; \\ a &> b &\Leftrightarrow a + c > b + c. \end{aligned}$$

**Définition II.1.2.** Un sous-ensemble  $S$  de  $G$  est *bien ordonné* si tout sous-ensemble de  $S$  a un plus petit élément. Ceci est équivalent à dire qu’il n’existe pas une suite infinie décroissante dans  $S$ .

On peut déduire aisément les propriétés suivantes des ensembles bien ordonnés d’un groupe  $G$  totalelement ordonné :

(a) Si  $S_1, S_2, \dots, S_n$  sont des sous-ensembles de  $G$ , alors l’ensemble  $S_1 + S_2 + \dots + S_n = \{s_1 + s_2 + \dots + s_n; s_i \in S_i\}$  est aussi bien ordonné.

(b) Si  $S_1, S_2, \dots, S_n$  sont des sous-ensembles de  $G$ , alors pour tout  $x \in G$ , l’ensemble  $\{(s_1, s_2, \dots, s_n) \in S_1 \times S_2 \times \dots \times S_n \text{ tel que } s_1 + s_2 + \dots + s_n = x\}$  est fini.

(c) Si  $S$  est un sous-ensemble de  $P = \{a \in G; a > 0\}$ , alors  $\tilde{S} = \bigcup_{n=1}^{\infty} S^{+n}$  (où  $S^{+n} = \underbrace{S + S + \dots + S}_n = \underbrace{\{s + s + \dots + s\}}_n; s \in S$ ) est aussi bien ordonné.

**Définition II.1.3.** Soit  $R$  un anneau commutatif et  $G$  un groupe abélien totalelement ordonné. On note  $R((t^G))$  l’ensemble de tous les éléments de la forme  $f = \sum_{\alpha \in G} r_{\alpha} t^{\alpha}$  telle que :

- $r_{\alpha} \in G$ , pour tout  $\alpha \in G$ .
- le support de  $f$ , c’est à dire l’ensemble  $\{\alpha / r_{\alpha} \neq 0\}$ , est bien ordonné.

On définit les lois “+” et “×” de la manière suivante :

$$\sum_{\alpha \in G} r_{\alpha} t^{\alpha} + \sum_{\alpha \in G} s_{\alpha} t^{\alpha} = \sum_{\alpha \in G} (r_{\alpha} + s_{\alpha}) t^{\alpha}$$

$$\sum_{\alpha \in G} r_{\alpha} t^{\alpha} \times \sum_{\alpha \in G} s_{\alpha} t^{\alpha} = \sum_{\alpha \in G} \sum_{\beta \in G} (r_{\beta} s_{\alpha - \beta}) t^{\alpha}.$$

Dans ce cas, l'ensemble  $R((t^G))$ , muni des deux lois définies précédemment, constitue un anneau qu'on appelle *l'anneau des séries formelles généralisées de  $R$  à exposants dans  $G$*  ou *l'anneau des Séries de Hahn–Mal'cev–Neumann à coefficients dans  $R$  et à exposants dans  $G$* .

**Remarque.** Grâce aux propriétés ci-dessus, la somme et le produit sont bien définis et donc  $R((t^G))$  est bien un anneau. Un élément non nul, i.e. une série de  $R((t^G))$  est une unité de l'anneau si, et seulement si, son premier coefficient est non nul. En particulier, si  $R$  est un corps, alors  $R((t^G))$  est aussi un corps. De plus, si  $K$  est un corps algébriquement clos et  $G$  est un groupe divisible, alors  $K((t^G))$  est algébriquement clos [8].

Dans la suite du mémoire, on s'intéresse au cas où  $K$  est le corps fini à  $q$  éléments ( $q$  sera partout une puissance du nombre premier  $p$ , sauf mention contraire) et  $G$  est le groupe divisible des rationnels  $\mathbb{Q}$ . On obtient alors la suite des inclusions suivante :

$$\mathbb{F}_q(t) \subset \mathbb{F}_q((t)) \subset \mathbb{F}_q((t^{\mathbb{Q}})).$$

Le corps  $\mathbb{F}_q((t^{\mathbb{Q}}))$  n'est pas algébriquement clos, mais par contre  $(\bigcup_{n \geq 1} \mathbb{F}_{p^n})((t^{\mathbb{Q}}))$  l'est, puisque  $\bigcup_{n \geq 1} \mathbb{F}_{p^n}$  est la clôture algébrique de  $\mathbb{F}_p$ .

De plus, le corps  $\mathbb{F}_q((t^{\mathbb{Q}}))$  est un corps valué, c'est-à-dire il est muni d'une valuation

$$v : \mathbb{F}_q((t^{\mathbb{Q}})) \rightarrow \mathbb{R} \cup \{\infty\};$$

pour une série  $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ ,  $v(x)$  étant défini comme le plus petit élément du support de  $x$  et, on pose  $v(0) = \infty$ .

Il est facile de voir que cette fonction vérifie bien les conditions nécessaires pour être une valuation :

- $\forall x \in \mathbb{F}_q((t^{\mathbb{Q}})), v(x) = \infty \Leftrightarrow x = 0$
- $\forall x, y \in \mathbb{F}_q((t^{\mathbb{Q}})), v(xy) = v(x) + v(y)$
- $\forall x, y \in \mathbb{F}_q((t^{\mathbb{Q}})), v(x - y) \geq \min \{v(x), v(y)\}$ .

Le corps des séries de Hahn  $\mathbb{F}_q((t^{\mathbb{Q}}))$  est donc un corps topologique (avec la distance donnée par la valuation qui se définit par la fonction  $(x, y) \rightarrow \exp(-(x - y))$ ).

## II.1.2 Automates finis revisités et séries quasi- $p$ -automatiques

Dans cette partie, on définit la notion d'automaticité pour une fonction définie sur  $\mathbb{Q}$  et, ultérieurement, on définit la notion de quasi-automaticité. Dorénavant, on utilisera l'alphabet (d'entrée) suivant :

$$\Sigma_{k,\bullet} = \{0, 1, 2, \dots, k-1, \bullet\}.$$

On note  $L(k)$  le langage contenant les mots de  $\Sigma_{k,\bullet}^*$ , ayant une seule occurrence du symbole “ $\bullet$ ” (le point) et dont la première et la dernière lettre sont non nulles. Celui-ci est un langage régulier (c'est le langage des développements valides en base  $k$ ) (voir [2] comme référence).

Soit  $S_k$  l'ensemble des nombres rationnels  $k$ -adiques positifs, c'est à dire :

$$S_k = \left\{ \frac{a}{k^b}; a, b \in \mathbb{Z}, a \geq 0 \right\}.$$

**Remarque.** En fait, il existe une bijection entre  $L(k)$  et  $S_k$ , définie de la façon suivante :

$$\begin{aligned} [\bullet] : L(k) &\longrightarrow S_k \\ s_1 s_2 \dots s_{i-1} \bullet s_{i+1} \dots s_n &\longrightarrow \sum_{j=1}^{i-1} s_j k^{i-1-j} + \sum_{j=i+1}^n s_j k^{i-j} \end{aligned}$$

où  $s_1, s_2, \dots, s_{i-1}, s_{i+1}, \dots, s_n \in \{0, 1, \dots, k-1\}$ .

L'expression

$$\sum_{j=1}^{i-1} s_j k^{i-1-j} + \sum_{j=i+1}^n s_j k^{i-j}$$

sera notée dans la suite  $v(s)$ . Aussi, le développement en base  $k$  d'un rationnel  $p$ -adique  $v \in S_k$  sera noté  $s(v)$ .

Kedlaya définit d'une manière un peu différente la notion d'automaticité d'une fonction.

**Définition II.1.4.** Soit  $\Delta$  un ensemble fini. Une fonction  $f : S_k \longrightarrow \Delta$  est  $k$ -automatique s'il existe un DFAO  $M$ , dont l'alphabet d'entrée est  $\Sigma_k$  et l'alphabet de sortie est  $\Delta$  telle que pour tout  $v \in S_k$ ,  $f(v) = f_M(s(v))$ .

Un ensemble  $S \subset S_k$  est dit  $k$ -régulier si sa fonction caractéristique :

$$\chi_S(s) = \begin{cases} 1 & \text{si } s \in S \\ 0 & \text{sinon} \end{cases}$$

est  $k$ -automatique.

Dans ce cas, on remarque que la fonction  $f : S_k \longrightarrow \Delta$  est  $k$ -automatique si, et seulement si, l'ensemble  $f^{-1}(d)$  est  $k$ -régulier, pour tout  $d \in \Delta$  (voir [2]).

Ensuite, on dit qu'une fonction  $f : \mathbb{Q} \longrightarrow \Delta$  est  $k$ -automatique si son support est inclus dans  $S_k$  et si sa restriction à  $S_k$  est  $k$ -automatique.

Pendant la transition d'un mot dans un automate, on peut différencier deux types d'états, selon le sous-mot qui apparaît avant le point “•” et celui qui se trouve après :

**Définition II.1.5.** Soit  $M$  un DFAO (l'alphabet d'entrée est toujours  $\Sigma_k$ ). On dit qu'un état  $q \in Q$  est *prévirgulaire* (respectivement *postvirgulaire*) s'il existe un développement valide en base  $k$  :  $s = s_1s_2\dots s_k\dots s_n$  avec  $s_k = \text{“•”}$  tel que si  $q_i = \delta(q_{i-1}, s_i)$  alors  $q = q_i$  pour  $i < k$  (respectivement  $i \geq k$ ).

Autrement dit, pendant la transition dans l'automate du mot  $s$ , un état  $q$  prévirgulaire (respectivement postvirgulaire) apparaît avant (respectivement après) la transition du “•” de  $s$ . On remarque que si  $L(M)$  ne contient que les développements valides, aucun état ne peut pas être à la fois prévirgulaire et postvirgulaire.

**Exemple II.1.1.** Pour  $w \in L(2)$  on définit la fonction

$$f([w]_2) = \begin{cases} 0 & \text{s'il existe un nombre pair d'occurrences de “1” dans } w \\ 1 & \text{sinon.} \end{cases}$$

Alors la fonction  $f : S_2 \rightarrow \{0, 1\}$  est 2-automatique car elle est engendrée par la machine à états finis représentée par la figure 6 (l'alphabet d'entrée étant  $\{0, 1, \bullet\}$  et l'alphabet de sortie  $\{0, 1\}$ ). Cette machine associe au mot  $w$ , le nombre de “1” qui apparaît dans  $w$  réduit modulo 2.

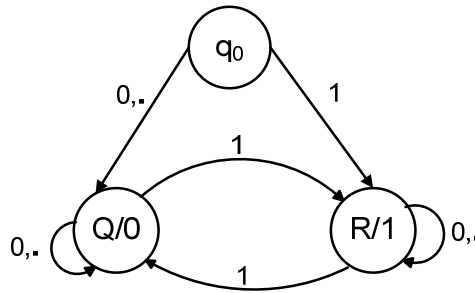


FIG. 6 – Une machine à états finis avec l'alphabet d'entrée  $\Sigma_2$  et l'alphabet de sortie  $\{0, 1\}$

**Définition II.1.6.** Soit  $f : \mathbb{Q} \rightarrow \Delta$  une fonction dont le support  $S$  est bien ordonné. Alors  $f$  est quasi- $k$ -automatique s'il existe des entiers  $a > 0$  et  $b$  tels que :

- (a) l'ensemble  $aS + b = \{ai + b; i \in S\} \subset S_k$
- (b) la fonction

$$f_{a,b} : S_k \longrightarrow \Delta \\ x \longmapsto f\left(\frac{x-b}{a}\right)$$

est  $k$ -automatique.

Nous dirons que la série formelle généralisée  $\sum_i f(i)t^i$  est quasi- $p$ -automatique si la fonction  $f$  est quasi- $p$ -automatique.

Désormais, l'ensemble des séries quasi- $p$ -automatiques est noté  $K_p$ .

**Remarque.** Si la condition (b) est vraie pour un couple de paramètres  $(a, b)$  satisfaisant à la condition (a), alors (b) est vraie pour tous les entiers  $a$  et  $b$  satisfaisant à cette première condition. Pour démontrer cela, on introduit le lemme suivant.

**Lemme II.1.1.** *Soit  $S$  un sous-ensemble de  $S_k$ . Alors pour tout  $r \in \mathbb{N}$  et pour tout  $s \in S_k$ ,  $S$  est  $k$ -régulier si, et seulement si :*

$$rS + s = \{rx + s : x \in S\}$$

*est  $k$ -régulier.*

Justifions à présent la remarque précédente, qui sera très utile dans la suite du mémoire et soient  $a, b$  tels que  $f_{a,b}(x) = f\left(\frac{x-b}{a}\right)$  est  $p$ -automatique et soient  $a', b'$  vérifiant (a). Montrons que  $f_{a',b'}$  reste encore  $p$ -automatique.

La fonction  $f_{a,b}$  est  $p$ -automatique si, et seulement si, l'ensemble  $f_{a,b}^{-1}(d)$  est  $p$ -régulier, pour tout  $d \in \Delta$ . Mais

$$f\left(\frac{x-b}{a}\right) = d \iff x \in af^{-1}(d) + b$$

et donc ce dernier ensemble est aussi régulier et par l'application deux fois du lemme précédent, l'ensemble  $a'f^{-1}(d) + b'$  est aussi  $p$ -régulier. Le même raisonnement implique que  $f\left(\frac{x-b'}{a'}\right)$  est  $p$ -automatique et donc que  $f_{a',b'}$  est automatique.

### II.1.3 Un exemple de série de Hahn algébrique

Considérons la série formelle généralisée

$$F(t) = t^{-1/p} + t^{-1/p^2} + \dots \in \mathbb{F}_q((t^{\mathbb{Q}})).$$

On a déjà vu qu'elle est *algébrique* sur le corps  $\mathbb{F}_p(t)$  car elle est racine du polynôme d'Artin-Schreier

$$x^p - x - \frac{1}{t}.$$

Nous allons montrer dans la suite qu'elle est aussi *quasi- $p$ -automatique*.

En effet, la série  $F(t)$  peut être écrite de la forme :  $F(t) = \sum_i f(i)t^i$  avec

$$f(i) = \begin{cases} 1 & \text{si } i = -\frac{1}{p^n}, \forall n \geq 0 \\ 0 & \text{sinon.} \end{cases}$$

- Le support de  $f$  est l'ensemble

$$S = \left\{ -\frac{1}{p^n}, n \geq 0 \right\}.$$

Il s'agit d'un ensemble bien ordonné.

- Le couple d'entiers  $(a, b)$  qui apparaît dans la définition correspond ici au couple  $(1, 1)$ . En effet, l'ensemble

$$S + 1 = \left\{ 1 - \frac{1}{p^n} = \frac{p^n - 1}{p^n}, n \geq 0 \right\}$$

est inclus dans l'ensemble  $S_p$  des nombres rationnels  $p$ -adiques positifs.

De plus, le développement en base  $p$  de  $1 - \frac{1}{p^n}$  est de la forme  $0.\underbrace{(p-1)(p-1)\dots(p-1)}_{n \text{ fois}}$ .

La fonction  $f_{1,1} : S_p \rightarrow \mathbb{F}_p$  définie par l'expression :

$$f_{1,1}(i) = \begin{cases} 1 & \text{si } i = 1 - \frac{1}{p^n}, \forall n \geq 0 \\ 0 & \text{sinon} \end{cases}$$

est  $p$ -automatique au sens de Kedlaya car elle est engendrée par l'automate suivant :

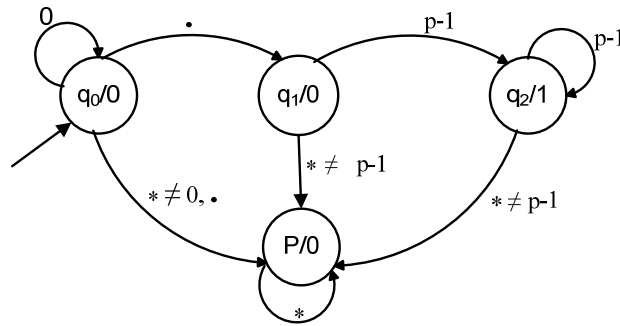


FIG. 7 – Un automate engendrant la fonction  $f_{1,1}$ , l'alphabet d'entrée étant  $\Sigma_{p,\bullet}$  et l'alphabet de sortie étant  $\{0, 1\}$  ; \* est un symbole de  $\Sigma_{p,\bullet}$

## II.2 Préliminaires algébriques

Dans cette partie, nous donnons quelques notions algébriques, qui nous seront utiles pour démontrer le théorème de Kedlaya.

### II.2.1 Systèmes d'équations semi-linéaires

Le lemme suivant est très utile dans la preuve des deux implications du théorème de Kedlaya. Il jouera un rôle important pour démontrer l'algébricité de certains éléments sur le corps  $\mathbb{F}_p(t)$ .

**Lemme II.2.1.** *Soient  $K \subseteq L$  deux corps de caractéristique  $p$ . Soient  $A, B \in M_{m,n}(K)$ , au moins une inversible et soit  $w$  un vecteur colonne à coefficients dans  $K$  ( $w \in K^n$ ). Si  $v \in L^n$  tel que  $Av^\sigma + Bv = w$ , où  $\sigma$  représente le morphisme de Frobenius,  $\sigma : x \mapsto x^p$ , alors les coefficients de  $v$  sont tous algébriques sur  $K$ .*

*Démonstration.* Nous allons distinguer deux cas selon que  $A$  ou  $B$  est inversible.

- Supposons que  $A$  est inversible.

Alors on peut écrire  $v^\sigma + A^{-1}Bv = A^{-1}w$ . Si on note  $U_1 = -A^{-1}B$  et  $w_1 = A^{-1}w$ , il vient :  $v^\sigma = U_1v + w_1$ . En raisonnant par récurrence sur  $i = 1, 2, \dots$ , on obtient :

$$v^{\sigma^i} = U_i v + w_i,$$

où  $U_i \in M_{n,n}(K)$  et  $w_i \in K^n$ . Les vecteurs  $v^{\sigma^i}$  engendrent un espace vectoriel de dimension au plus  $n^2 + n$ . Par conséquent, il existe un entier  $m$  et  $c_0, c_1, \dots, c_m$  dans  $K$ , non tous nuls, tels que

$$c_0 v + c_1 v^\sigma + \dots + c_m v^{\sigma^m} = 0.$$

D'après le lemme d'Ore, chaque coefficient du vecteur  $v$  est algébrique sur  $K$ .

- Supposons que  $B$  est inversible.

On peut supposer sans perte de généralité que toutes les racine  $p$ -ièmes des éléments de  $L$  appartiennent à  $L$  (i.e. que le corps  $L$  est parfait). Dans cette situation, le morphisme de Frobenius  $\sigma : L \rightarrow L$  est bijectif.

Soit  $K'$  l'ensemble des  $x \in L$  tel qu'il existe un entier  $i$  pour lequel  $x^{\sigma^i} \in K$ . Alors  $\sigma' : K' \rightarrow K'$  est aussi bijective et chaque élément de  $K'$  est algébrique sur  $K$ . Comme dans le premier cas, on peut maintenant écrire :  $v^{\sigma^{-i}} = U_i v + w_i$ , pour  $i = 1, 2, \dots$  avec  $U_i \in M_{n,n}(K')$  et  $w_i \in K'^n$ . De même, on conclut que les coefficients de  $v$  sont algébriques sur  $K'$ .

Mais chaque élément  $\alpha \in L$  algébrique sur  $K'$  est algébrique sur  $K$ . En effet, si  $\alpha$  est algébrique, alors  $d_0 + d_1 \alpha + \dots + d_m \alpha^m = 0$ , pour des  $d_i \in K'$  non tous nuls. Comme  $d_0, d_1, \dots, d_m$  sont dans  $K'$ , on peut trouver un entier  $i$  tel que  $d_0^{\sigma^i}, d_1^{\sigma^i}, \dots, d_m^{\sigma^i}$  sont dans  $K$ . Ainsi

$$d_0^{\sigma^i} + d_1^{\sigma^i} \alpha^{p^i} + \dots + d_m^{\sigma^i} \alpha^{mp^i} = 0$$

Donc  $d_0^{\sigma^i} + d_1^{\sigma^i} X^{p^i} + \dots + d_m^{\sigma^i} X^{mp^i}$  est un polynôme à coefficients dans  $K$  qui admet  $\alpha$  comme racine. Par conséquent,  $\alpha$  est algébrique sur  $K$ .

Finalement, puisque tous les coefficients de  $v$  sont dans  $L$  et qu'ils sont algébriques sur  $K'$ , le raisonnement précédent implique qu'ils sont également algébriques sur  $K$ . □

## II.2.2 Polygone de Newton

Un outil important dans l'étude des corps valués est *le polygone de Newton*. Dans ce paragraphe, on s'intéresse au corps des séries formelles généralisées  $\mathbb{F}_q((t^{\mathbb{Q}}))$  muni de la valuation

$$v : \mathbb{F}_q((t^{\mathbb{Q}})) \rightarrow \mathbb{R} \cup \{\infty\}.$$

Rappelons que pour une série  $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ ,  $v(x)$  est défini comme le plus petit élément du support de  $x$  et que, par convention,  $v(0) = \infty$ .

Pour un polynôme  $P(z) = \sum_{i=0}^n c_i z^i$  à coefficients dans le corps  $\mathbb{F}_q((t^{\mathbb{Q}}))$  on définit le polygone de Newton de  $P$  comme étant l'enveloppe convexe inférieure de l'ensemble des points  $\{(0, \infty), (-n, \infty)\} \cup \{-i, v(c_i), 0 \leq i \leq n\}$ . Donc le polygone de Newton est formé par deux axes verticaux et un ensemble de segments des droites de différentes pentes. On appelle pentes du polynôme  $P$  les pentes de son polygone de Newton. On définit sa multiplicité (ou la largeur) la longueur de la projection sur l'axe des abscisses du segment ayant une pente égale à  $r$ . Si un nombre rationnel  $r$  n'est pas une pente du polynôme, alors on dit, par convention, que sa multiplicité est 0.

On dit de plus qu'un polynôme  $P$  est *de pente pure égale à  $r$*  si toutes ses pentes sont égales à  $r$ . Autrement dit, le polygone de Newton est formé par l'axe vertical  $x = -n$ , un segment de droite de pente  $r$  et l'axe vertical  $x = 0$ . Par convention,  $\infty$  peut être considéré comme pente de  $P$  et sa multiplicité est égale à l'ordre de 0 comme racine de  $P$ .

**Exemple II.2.1.** Considérons le polynôme  $P(z) = c_0 + c_1 z + c_2 z^2 + c_3 z^3 + c_4 z^4 + c_5 z^5$ , où les coefficients  $c_i$  sont les séries formelles généralisées suivantes :

$$\begin{array}{ll} c_0 = t^1 + t^2 + t^3 + \dots & \text{donc } v(c_0) = 1 \\ c_1 = t^{3/2} + t^2 + t^{5/2} + \dots & \text{donc } v(c_1) = 3/2 \\ c_2 = t^{1/2} + t^{3/4} + t^{5/6} + \dots & \text{donc } v(c_2) = 1/2 \\ c_3 = t^{7/2} + t^{9/2} + t^{11/2} + \dots & \text{donc } v(c_3) = 7/2 \\ c_4 = t^2 + t^4 + t^6 + \dots & \text{donc } v(c_4) = 2 \\ c_5 = t^5 + t^{10} + t^{15} + \dots & \text{donc } v(c_5) = 5. \end{array}$$

Le polygone de Newton de  $P$  est alors représenté sur la figure 8.

Il est formé des deux axes verticaux :  $x = -5$  et  $x = 0$  et des trois segments de pentes :  $-3, -3/4, 1/4$  et de multiplicités respectivement égales à 1, 2, 2.

Nous allons prouver maintenant une proposition exprimant une relation entre les pentes du polygone de Newton et les racines du polynôme.

**Proposition II.2.1.** *Soit  $P$  un polynôme de degré  $n$  à coefficients dans  $\mathbb{F}_q((t^{\mathbb{Q}}))$ . Si  $u$  est une racine de  $P$ , alors il existe un segment dans le polygone de Newton de pente  $v(u)$ .*

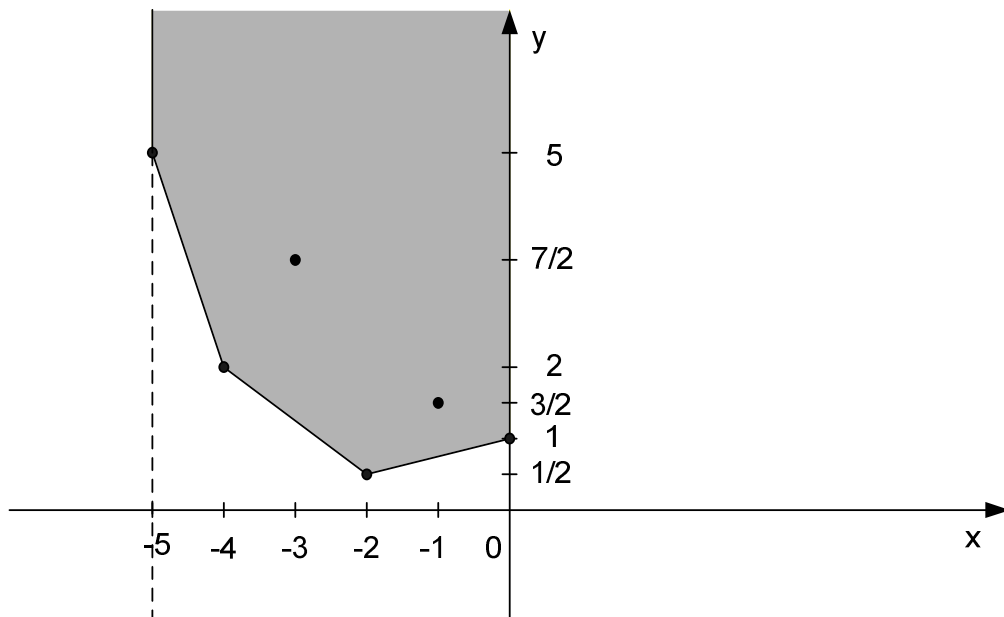


FIG. 8 – Polygone de Newton

*Démonstration.* Soit  $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ , avec  $a_i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ . Si  $u$  est une racine de  $P$ , alors :

$$a_0 + a_1u + a_2u^2 + \cdots + a_nu^n = 0$$

et par conséquent  $v(a_0 + a_1u + a_2u^2 + \cdots + a_nu^n) = v(0) = \infty$ .

Si  $\min_k v(a_ku^k)$  est uniquement déterminé, alors  $v(a_0 + a_1u + a_2u^2 + \cdots + a_nu^n) = v(a_ku^k) = +\infty$  ce qui est absurde. Donc il existe deux entiers  $i$  et  $j$  comprises entre 0 et  $n$ ,  $i \neq j$  tels que  $v(a_iu^i) = v(a_ju^j) = \min \{v(a_ku^k), 0 \leq k \leq n\}$ . Par définition d'une valuation,  $v(a_iu^i) = v(a_i) + iv(u)$  et  $v(a_ju^j) = v(a_j) + jv(u)$ . Par conséquent,

$$v(u) = \frac{v(a_j) - v(a_i)}{i - j}$$

et donc  $v(u)$  est la pente du segment des extrémités  $(-i, v(a_i))$  et  $(-j, v(a_j))$ .

Il reste maintenant à démontrer que ce segment appartient au polygone de Newton. Pour cela, on considère la droite de pente  $v(u)$  à laquelle ce segment appartient :

$$y = v(u)x + v(a_iu^i) = v(u)x + v(a_ju^j).$$

Elle intersecte l'axe des ordonnées  $Oy$  dans le point  $(0, v(a_iu^i)) = (0, v(a_ju^j))$ . De plus cette valuation est minimale et donc tous les points des coordonnées  $(-k, v(a_k))$  sont soit au dessus, soit sur cette droite. Par conséquent, le segment  $[(-i, v(a_i)), (-j, v(a_j))]$  est inclus dans le polygone de Newton. □

Le lemme suivant décrit une propriété des multiplicités des pentes d'un produit de deux polynômes.

**Lemme II.2.2.** Soient  $P$  et  $Q$  deux polynômes non nuls à coefficients dans  $\mathbb{F}_q((t^{\mathbb{Q}}))$ . Alors, pour chaque  $r \in \mathbb{Q} \cup \{\infty\}$ , la multiplicité de  $r$  comme pente de  $PQ$  est la somme de multiplicités de  $r$  comme pente de  $P$  et comme pente de  $Q$  respectivement.

*Démonstration.* Si  $r = \infty$ , la multiplicité de  $r$  est égale à l'ordre d'annulation du polynôme  $PQ$  en 0 et le lemme est clair.

On suppose par la suite que  $r \in \mathbb{Q}$ . Soient  $P(z) = \sum_i c_i z^i$  et  $Q(z) = \sum_j d_j z^j$ . Soient  $(-e, v(c_e))$  et  $(-f, v(c_f))$  (respectivement  $(-g, v(d_g))$  et  $(-h, v(d_h))$ ) les points extrêmes du segment de droite de pente  $r$ , du polygone de Newton de  $P$  (respectivement de  $Q$ ). Donc la multiplicité de  $r$  comme pente de  $P$  (respectivement de  $Q$ ) est égale à  $(e-f)$  (respectivement à  $(g-f)$ ).

On a alors :

$$v(c_i) + ri \geq v(c_e) + re = v(c_f) + rf$$

$$v(d_j) + rj \geq v(d_g) + rg = v(d_h) + rh,$$

l'inégalité étant stricte si  $i \notin [e, f]$  ou si  $j \notin [g, h]$ .

Donc pour chaque  $k$ ,

$$\min_{i+j=k} \{v(c_i d_j) + rk\} \geq v(c_e) + re + v(d_g) + rg$$

l'inégalité étant stricte si  $k \notin [f+h, e+g]$ , si  $k = e+g$  et  $i \neq e$  ou, si  $k = f+h$  et  $i \neq h$ .

Si on écrit le polynôme  $R(z) = P(z)Q(z) = \sum_{k=i+j} a_k z^k$ , il vient :

$$\min_k \{v(a_k) + rk\} \geq v(c_e) + re + v(d_g) + rg$$

égalité étant obtenue pour  $k = f+h$  et  $k = e+g$ , mais pas pour  $k \notin [f+h, e+g]$ . Par conséquent, la multiplicité de  $r$  comme pente de  $R$  est égale à  $e+g-(f+h) = (e-f)+(g-h)$ , ce qui termine la démonstration. □

**Corollaire II.2.1.** Soit  $P(z)$  un polynôme non nul à coefficients dans  $\mathbb{F}_q((t^{\mathbb{Q}}))$  qui se factorise sous la forme  $Q_1 Q_2 \dots Q_n$ ,  $Q_i$  des polynômes de pentes pures. Alors, pour chaque  $r \in \mathbb{Q} \cup \{\infty\}$ , la somme de degrés de tous les  $Q_i$  ayant une pente  $r$ , est égale à la multiplicité de  $r$  comme pente de  $P$ .

De façon analogue à la factorisation d'un polynôme en produit de facteurs irréductibles, on peut factoriser les polynômes à coefficients dans un corps valué en produit de polynômes de pentes pures (cf. [9]).

**Proposition II.2.2.** Soit  $K$  un sous-corps de  $\mathbb{F}_q((t^{\mathbb{Q}}))$  complet pour la valuation  $v$ . Alors tout polynôme unitaire  $P$  à coefficients dans le corps  $K$  admet une unique factorisation  $P = Q_1 Q_2 \dots Q_n$ , où chaque  $Q_i$  est un polynôme unitaire, de pente pure égale à  $s_i$  avec de plus,  $s_1 < s_2 < \dots < s_n$ .

### II.2.3 Polynômes tordus et factorisation

Pour un corps  $K$  de caractéristique  $p > 0$ , on définit l'anneau non commutatif des polynômes tordus à coefficients dans  $K$ , noté  $K\{F\}$ , l'ensemble des sommes de la forme  $\sum_{i=0}^n c_i F^i$ , muni de l'addition habituelle, notée “+” et de la multiplication suivante, notée “ $\times$ ” :

$$\sum_{i=0}^n c_i F^i \times \sum_{j=0}^m d_j F^j = \sum_{k=0}^{m+n} \left( \sum_{i+j=k} c_i d_j^{p^i} \right) F^k.$$

Le degré d'un polynôme  $\sum_{i=0}^n c_i F^i$  est le plus grand  $i$  tel que le coefficient  $c_i \neq 0$ . Par convention,  $\deg(0) = -\infty$ . Le degré du produit de deux polynômes non nuls est la somme des degrés des polynômes.

Les polynômes tordus à coefficients dans un corps  $K$  peuvent être vus comme des opérateurs additifs agissant, sur tout corps  $L$  contenant  $K$ , de la façon suivante :

$$\left( \sum_{i=0}^n c_i F^i \right) (z) = \sum_{i=0}^n c_i z^{p^i}.$$

Le noyau de cette application a la propriété suivante (cf. annexe A) :

**Lemme II.2.3.** *Soit  $L$  une clôture algébrique de  $K$ . Soit  $T(F) = \sum_{i=0}^d c_i F^i$  un polynôme tordu non nul de degré  $d$ , à coefficients dans  $K$ . Alors le noyau de  $T$  est un  $\mathbb{F}_p$ -espace vectoriel de dimension  $\leq d$ , avec égalité si, et seulement si, le coefficient constant du polynôme  $T$  est non nul.*

On a aussi la propriété suivante sur la factorisation d'un polynôme tordu (cf. annexe B) :

**Proposition II.2.3.** *Soit  $K$  un sous-corps de  $\mathbb{F}_q((t^{\mathbb{Q}}))$  contenant toutes les puissances rationnelles de  $t$  et complet pour la valuation  $v$ . Soit  $P(F)$  un polynôme tordu à coefficients dans  $K$ . Alors, pour toute puissance  $q'$  de  $q$ , il existe une factorisation du polynôme  $P$  sous la forme d'un produit  $P = Q_1 Q_2 \cdots Q_n$ , où les  $Q_i$  sont des polynômes tordus unitaires et linéaires sur  $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ .*

## II.3 Démonstration du théorème de Kedlaya

Dans cette partie, nous démontrons le théorème de Kedlaya. La preuve de la première implication de ce théorème reste dans le même esprit que celle du théorème de Christol, contrairement à la démonstration de la seconde implication qui utilise des outils complètement différents.

### II.3.1 Preuve de la première implication du théorème

Dans cette partie, nous démontrons que si une série généralisée  $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est quasi- $p$ -automatique, alors elle est algébrique sur  $\mathbb{F}_q(t)$ .

Pour démontrer cette implication on aura besoin des deux lemmes suivants.

**Lemme II.3.1.** Soient  $a$  et  $b$  des entiers et  $a > 0$ . Alors  $\sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est algébrique sur  $\mathbb{F}_q(t)$  si, et seulement si,  $\sum_i x_{ai+b} t^i$  est algébrique sur  $\mathbb{F}_q(t)$ .

Un élément  $\tau \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$  peut être vu comme un automorphisme de  $\mathbb{F}_q(t)$  et  $\mathbb{F}_q((t^{\mathbb{Q}}))$  en définissant l'action suivante :

$$\left( \sum_i x_i t^i \right)^\tau = \sum_i x_i^\tau t^i.$$

On remarque que si  $\sigma \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$  est le morphisme de Frobenius, alors  $x^p = x^\sigma$  si  $x \in \mathbb{F}_q$ , mais  $x^p \neq x^\sigma$  si  $x \in \mathbb{F}_q(t)$  ou  $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$  car l'automorphisme introduit précédemment n'agit que sur les coefficients du polynôme (respectivement de la série).

*Démonstration.* Il suffit de démontrer l'équivalence pour  $a = 1$  puis pour  $b = 0$ . En effet, le cas général est couvert par applications successives de ces cas particuliers.

- Supposons que  $a = 1$ .

Si  $x = \sum_i x_i t^i$  est algébrique sur  $\mathbb{F}_q(t)$ , alors par définition, il existe un polynôme  $P(z) \in \mathbb{F}_q(t)[z]$  tel que  $P(x) = 0$ . La série  $x' = \sum_i x_{i+b} t^i = \sum_i x_i t^{i-b}$  est alors racine du polynôme  $P(z t^b)$  et donc  $x'$  est aussi algébrique sur  $\mathbb{F}_q(t)$ .

Réciproquement, si  $x' = \sum_i x_{i+b} t^i$  est racine d'un polynôme  $P(z)$  à coefficients dans  $\mathbb{F}_q(t)$ , alors la série  $x = \sum_i x_i t^i = t^b x'$  est racine de  $P(z t^{-b})$  et donc  $x$  est algébrique.

- Supposons que  $b = 0$ . Nous devons distinguer deux cas selon que  $a = p$  ou que  $(a, p) = 1$ .

- Supposons que  $a = p$ .

Si la série  $x = \sum_i x_i t^i$  est racine d'un polynôme  $P(z) = \sum_j c_j z^j \in \mathbb{F}_q(t)(z)$ , alors  $x' = \sum_i x_{pi} t^i = \sum_i x_i t^{i/p}$  est racine du polynôme

$$\sum_j c_j^\sigma z^{pj} \in \mathbb{F}_q(t)(z).$$

Réciproquement, si  $x'$  est racine d'un polynôme  $Q(z) = \sum_j d_j z^j \in \mathbb{F}_q(t)(z)$ , alors  $x$  est racine de  $\sum_j (d_j^p)^{\sigma^{-1}} z^j \in \mathbb{F}_q(t)(z)$  et donc  $x$  est aussi algébrique sur  $\mathbb{F}_q(t)$ .

- Supposons que  $(a, p) = 1$ .

Si  $x = \sum_i x_i t^i$  est racine d'un polynôme  $P(z) = \sum_j c_j z^j$ , alors  $x' = \sum_i x_{ai} t^i = \sum_i x_i t^{i/a}$  est racine du polynôme

$$\sum_j c_j^{\tau^{-1}} z^j \in \mathbb{F}_q(t^{1/a})(z)$$

où  $\tau$  est l'automorphisme défini de la façon suivante :

$$\tau : \begin{array}{ccc} \mathbb{F}_q((t^{\mathbb{Q}})) & \rightarrow & \mathbb{F}_q((t^{\mathbb{Q}})) \\ \sum_i x_i t^i & \mapsto & \sum_i x_i t^{ai} \end{array}.$$

D'ailleurs, on peut remarquer que  $\tau$  agit aussi sur le corps  $\mathbb{F}_q(t)$ .

Par conséquent,  $x'$  est algébrique sur  $\mathbb{F}_q(t^{1/a})$ . Mais ce dernier est une extension finie de  $\mathbb{F}_q(t)$  et comme toute extension finie est algébrique, alors  $x'$  est algébrique sur  $\mathbb{F}_q(t)$ .

Réciproquement, on suppose que la série  $x'$  est racine de  $Q(z) = \sum_j d_j z^j \in \mathbb{F}_q(t)(z)$ . Alors  $x$  est racine de

$$\sum_j d_j^r z^j \in \mathbb{F}_q(t)(z)$$

et par conséquent la série est algébrique sur  $\mathbb{F}_q(t)$ . □

**Lemme II.3.2.** *Si  $S$  un sous-ensemble  $p$ -régulier de  $S_p$ , alors la série formelle généralisée  $\sum_{i \in S} t^i \in \mathbb{F}_p[[t^{\mathbb{Q}}]]$  est algébrique sur  $\mathbb{F}_p(t)$ .*

*Démonstration.* On considère l'ensemble  $L = \{s(v), v \in S\}$ . Puisque  $S$  est régulier, il existe un automate déterministe  $M = (Q, \Sigma, \delta, q_0, F)$  qui accepte le langage  $L$ .

Pour  $n \geq 0$ , on note  $s'(n)$  le sous-mot du développement en base  $p$  de  $n$  qui apparaît avant le point (ou la virgule). Pour chaque état prévirgulaire  $q \in Q$ , on considère :

- l'ensemble  $T_q = \{n \geq 0 \text{ tels que } \delta^*(q_0, s'(n)) = q\}$
- la fonction  $f(q) = \sum_{i \in T_q} t^i$
- l'ensemble  $U_q = \{(q', d) \in Q \times \{0, 1, \dots, p-1\} \text{ tels que } \delta(q', d) = q\}$

On peut alors remarquer que si  $q \neq q_0$ , alors

$$f(q) = \sum_{(q', d) \in U_q} t^d f(q')^p$$

et si  $q = q_0$  alors

$$f(q_0) = 1 + \sum_{(q', d) \in U_{q_0}} t^d f(q')^p.$$

Ceci nous fournit une équation du type  $Bv = w + Av^\sigma$  ( $\sigma$  étant toujours le morphisme de Frobenius), en notant  $v$  le vecteur dont les coefficients sont les  $f(q_i)$ , sur tous les états prévirgulaires  $q_i$  et  $B$  la matrice identité (donc une matrice inversible). Ainsi on remplit toutes les conditions du lemme II.2.1 et on peut donc conclure que  $f(q)$  est algébrique sur  $\mathbb{F}_q(t)$ , pour tout état prévirgulaire  $q$ .

Pour  $x \in S_p \cap [0, 1[$ , on note  $s''(x)$  le sous-mot du développement en base  $p$  de  $x$  qui apparaît après le point. Pour tout état postvirgulaire  $q$ , on considère maintenant :

- l'ensemble  $V_q = \{x \in S_p \cap [0, 1[ \text{ tels que } \delta^*(q, s''(x)) \in F\}$
- la fonction  $g(q) = \sum_{i \in V_q} t^i$ .

De même, on peut remarquer que si  $q \notin F$  (c'est à dire que  $q$  n'est pas un état acceptant), alors

$$g(q)^p = \sum_{d=0}^{p-1} t^d g(\delta(q, d))$$

et si  $q \in F$ , alors

$$g(q)^p = 1 + \sum_{d=0}^{p-1} t^d g(\delta(q, d)).$$

Comme précédemment, on utilise le lemme II.2.1, avec  $A$  la matrice identité et  $v$  le vecteur dont les coefficients sont les  $g(q)$ , pour chaque état postvirgulaire  $q$ . Par conséquent,  $g(q)$  est algébrique pour chaque état postvirgulaire  $q$ .

On veut démontrer que la série  $\sum_{i \in S} t^i$  est algébrique. Pour cela, il faut remarquer que cette série peut s'écrire en fonction de  $f$  et  $g$  de la manière suivante :

$$\sum_{\substack{q \text{ prévirgulaire,} \\ q' \text{ postvirgulaire}}} f(q)g(q').$$

Puisque une somme finie d'éléments algébriques est aussi algébrique, la série formelle généralisée  $\sum_{i \in S} t^i$  est algébrique sur  $\mathbb{F}_p(t)$ , ce que l'on voulait démontrer.  $\square$

*Preuve du théorème du Kedlaya (implication  $\Leftarrow$ ).* Nous voulons démontrer que toute série formelle généralisée  $F = \sum_i f(i)t^i \in \mathbb{F}_p[[t^{\mathbb{Q}}]]$  quasi- $p$ -automatique est algébrique sur  $\mathbb{F}_q(t)$ .

Puisque  $F$  est quasi- $p$ -automatique, il existe deux entiers  $a$  et  $b$ ,  $a$  strictement positif, tels que  $aS + b \subset S_p$  ( $S$  est toujours le support de la fonction  $f$ ) et la fonction  $f_{a,b}(x) = f\left(\frac{x-b}{a}\right)$  est  $p$ -automatique. Ceci implique que l'ensemble  $f_{a,b}^{-1}(\alpha)$  est régulier, pour tout  $\alpha \in \mathbb{F}_q$ . Donc l'ensemble

$$S_\alpha = \left\{ j, \text{ tel que } f\left(\frac{j-b}{a}\right) = \alpha \right\}$$

est  $p$ -régulier.

D'après le lemme II.3.1, il suffit de démontrer que la série  $\sum_i f(ai + b)t^i$  est algébrique, car cela implique que la série  $\sum_i f(i)t^i$  est aussi algébrique.

Mais

$$\sum_i f(ai + b)t^i = \sum_j f(j)t^{\frac{j-b}{a}} = \sum_{\alpha \in \mathbb{F}_q} \alpha \left( \sum_{j \in S_\alpha} t^j \right).$$

Puisque l'ensemble  $S_\alpha$  est  $p$ -régulier, le lemme II.3.2 implique que la série  $\sum_{j \in S_\alpha} t^j$  est algébrique sur  $\mathbb{F}_p(t)$  et donc sur  $\mathbb{F}_q(t)$  (car  $\mathbb{F}_q(t)$  est une extension finie de  $\mathbb{F}_p(t)$ ). La série  $\sum_i f(ai + b)t^i$  est donc algébrique et  $\sum_i f(i)t^i$  l'est aussi. La première implication du théorème II.1.1 est ainsi démontrée.  $\square$

### II.3.2 L'ensemble $K_q$ est un corps

Dans cette partie, nous allons démontrer que l'ensemble des séries quasi- $p$ -automatiques, que l'on note  $K_q$ , est un sous-corps de  $\mathbb{F}_q((t^{\mathbb{Q}}))$ . De plus, il contient  $\mathbb{F}_q(t)$  et il est inclus dans la clôture intégrale de  $\mathbb{F}_q(t)$  (car toutes les séries quasi- $p$ -automatiques sont algébriques sur  $\mathbb{F}_q(t)$ ).

Pour cela, nous devons donc démontrer les propositions suivantes :

P1. La somme de deux éléments de  $K_q$  est aussi dans  $K_q$ .

Si  $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$  sont  $p$ -automatiques (respectivement quasi- $p$ -automatiques), alors  $x+y$  est aussi  $p$ -automatique (respectivement quasi- $p$ -automatique).

P2. Le produit de deux éléments de  $K_q$  est aussi dans  $K_q$ .

Si  $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$  sont  $p$ -automatiques (respectivement quasi- $p$ -automatiques), alors  $x \cdot y$  est aussi  $p$ -automatique (respectivement quasi- $p$ -automatique).

P3. Tout élément non nul de  $K_q$  est inversible.

Si  $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est quasi- $p$ -automatique, alors il existe un élément  $x^{-1}$ , aussi quasi- $p$ -automatique tel que  $x \cdot x^{-1} = 1$ .

*Preuve de P1.* Pour démontrer cette propriété, il suffit de traiter le cas de l'automaticité, car la quasi-automaticité se déduit immédiatement d'après le lemme II.1.1.

Soient donc  $x = \sum_i x_i t^i$  et  $y = \sum_i y_i t^i$  deux séries  $p$ -automatiques. Cela implique que les fonctions  $i \rightarrow x_i$  et  $i \rightarrow y_i$  sont  $p$ -automatiques. Par conséquent, la fonction  $i \rightarrow (x_i, y_i)$  l'est aussi et, ultérieurement, la fonction  $i \rightarrow x_i + y_i$  l'est également. Donc la série  $x + y$  est  $p$ -automatique (pour plus de détails, il existe une preuve complète dans [2] page 166).  $\square$

*Preuve de P2.* On peut de nouveau supposer que les deux séries sont  $p$ -automatiques. On va démontrer que le produit est aussi automatique. La quasi-automaticité se déduit du lemme II.1.1.

• Soient  $x = \sum_i x_i t^i$  et  $y = \sum_i y_i t^i$  deux séries formelles généralisées dans  $\mathbb{F}_q((t^{\mathbb{Q}}))$ . On peut aussi les écrire comme une  $\mathbb{F}_q$ -combinaison linéaire de séries de la forme  $\sum_{i \in S} t^i$  pour  $S \subset S_p$ . Si le produit de deux telles séries est  $p$ -automatique, alors le produit  $x \cdot y$  est  $p$ -automatique (car, d'après P1., une somme d'éléments  $p$ -automatiques est encore  $p$ -automatique).

On peut donc supposer sans perte de généralité que  $x = \sum_{i \in A_1} t^i$  et  $y = \sum_{i \in A_2} t^i$ , où  $A_1$  et  $A_2$  sont deux sous-ensembles de  $S_p$ , donc bien ordonnés.

Le produit vaut alors

$$x \cdot y = \sum_{\substack{k = i + j \\ i \in A_1, j \in A_2}} a_k t^k$$

où  $a_k$  est le nombre de façons d'écrire  $k$  comme somme de deux éléments  $i \in A_1$  et  $j \in A_2$ , pris modulo  $p$ .

- Pour prouver que le produit  $x \cdot y$  est  $p$ -automatique, on doit donc démontrer que la suite  $(a_k)_k$  est  $p$ -automatique.

Rappelons déjà la définition d'un automate fini non déterministe (NFA) :

**Définition II.3.1.** Un automate fini non déterministe (NFA) est un quintuplet  $M = (Q, \Sigma, \delta, q_0, F)$  où tous les paramètres sont définis comme dans le cas d'un DFA, mise à part la fonction de transition

$$\delta : Q \times (\Sigma \cup \epsilon) \rightarrow P(Q).$$

La fonction de transition  $\delta$  reçoit ici comme argument un état de  $Q$  et un symbole de  $\Sigma$  et elle rend comme résultat une partie de  $Q$ . Les automates finis non déterministes sont donc tels qu'à partir d'un état donné il peut y avoir zéro, une ou plusieurs transitions pour un symbole d'entrée donné. Pour un mot  $w = s_1 s_2 \dots s_n$  on appelle *un chemin acceptant pour  $w$*  la suite des états  $q_1, q_2, \dots, q_n$  tels que  $q_i \in \delta(q_{i-1}, s_i)$  pour  $i = 1, \dots, n$  et  $q_n \in F$ . Le langage accepté par  $M$  est l'ensemble des mots  $w \in \Sigma^*$  pour lesquels il existe un chemin acceptant.

Pour les automates non déterministe on a la propriété suivante, démontrée dans [9] :

**Lemme II.3.3.** Soit  $n$  un entier strictement positif. Soit  $M = (Q, \Sigma, \delta, q_0, F)$  un NFA et  $f : \Sigma^* \rightarrow \mathbb{Z}/n\mathbb{Z}$  la fonction qui à un mot  $w \in \Sigma^*$  associe le nombre de chemins acceptant pour  $w$  dans  $M$  modulo  $n$ . Alors  $f$  est une fonction automatique.

- L'idée de la démonstration de l'automatisme de la suite  $a_k$  est de trouver un NFA qui "calcule" toutes les sommes possibles  $k = i + j$ , avec  $i \in A_1$  et  $j \in A_2$ . D'après le lemme précédent, on sait que la fonction comptant, pour une entrée  $k$ , le nombre de chemins acceptant modulo  $p$  dans cet automate, est automatique et le résultat sera ainsi démontré.

- Construction de l'automate non déterministe

On souhaite réaliser l'addition avec retenue de deux nombres écrits en base  $p$  en partant de la droite vers la gauche. Donc on veut considérer plutôt les miroirs des mots qui constituent les développements en base  $p$  des nombres qu'on veut ajouter.

On considère pour l'instant l'ensemble  $S \subset \Sigma_{p,\bullet}^* \times \Sigma_{p,\bullet}^*$ , formé des couples  $(w_1, w_2)$  avec les propriétés suivantes :

- $|w_1| = |w_2|$ ,
- $w_1$  et  $w_2$  se terminent par un 0,
- $w_1$  et  $w_2$  ont un seul point situé dans la même position,
- $w_1$  et  $w_2$  sont les miroirs des écritures en base  $p$  de  $i \in A_1$  et  $j \in A_2$  respectivement.

$S$  est un ensemble régulier et donc il existe un automate  $M = (Q, \Sigma_{p,\bullet}^* \times \Sigma_{p,\bullet}^*, \delta, q_0, F)$  qui accepte  $S$ .

À partir de là, nous allons construire un automate non déterministe  $M'$ , qui accepte un mot  $w$  si, et seulement si,  $w$  peut être écrit comme somme de  $w_1$  et  $w_2$ , où  $(w_1, w_2)$  est un couple accepté par l'automate déterministe  $M$ .

Pour cela, il suffit de considérer  $M' = (Q', \Sigma', \delta, q_0, F)$  avec

$$\begin{aligned} Q' &= Q \times \{0, 1\} \\ \Sigma' &= \Sigma_{p, \bullet} \\ q'_0 &= (q_0, 0) \\ F' &= F \times \{0\}. \end{aligned}$$

Les états de  $M'$  sont les couples  $(q, i) \in Q \times \{0, 1\}$ . Chaque tel couple est formé d'un état de l'automate déterministe  $M$  et d'un entier 0 ou 1 indiquant la présence d'une éventuelle retenue lors de l'addition. Définissons maintenant la fonction de transition  $\delta'$  de la manière suivante :

- pour un état  $(q, i) \in Q'$  et  $s \in \{0, 1, \dots, p-1\}$ , on pose  $(q', 0) \in \delta'((q, i), s)$  (respectivement  $(q', 1) \in \delta'((q, i), s)$ ) s'il existe un couple  $(t, u) \in \{0, 1, \dots, p-1\} \times \{0, 1, \dots, p-1\}$  tel que  $t+u+i < p$  (respectivement  $t+u+i \geq p$ ) et  $t+u+i \equiv s[p]$  et tel que  $\delta(q, (t, u)) = q'$ ,
- pour un état  $(q, i) \in Q'$  et  $s = \bullet$ , on pose  $(q', i) \in \delta'((q, i), s)$  si  $\delta(q, (s, s)) = q'$  (de sorte que  $(q', 1-i)$  n'est jamais inclus dans  $\delta'((q, i), s)$ ).

Lorsque l'on rentre un mot  $w$  dans  $M'$  et après sa lecture par l'automate, celui-ci nous dit si le mot peut s'écrire comme une somme de deux éléments  $w_1$  et  $w_2$ ,  $(w_1, w_2)$  étant un couple de  $S$  (accepté donc par  $M$ ). Les états acceptants sont donc les états de la forme  $(q, 0)$ , où  $q$  est un état final de  $M$ . Notons que  $(q, 1)$  n'est jamais un état acceptant car on ne veut pas qu'à la fin de l'addition il reste une retenue en suspend.

**Remarque.** Si  $w$  est un mot accepté par  $M'$ , le nombre de chemins acceptants par  $w$  dans  $M'$  est égal au nombre, considéré modulo  $p$ , de couples  $(w_1, w_2) \in S$  tels que  $w_1 + w_2 = w$ .

Il ne faut pas oublier qu'on veut trouver l'ensemble de sommes  $k = i + j$ . Par contre, pendant la lecture d'un mot  $w$  par l'automate  $M'$ , on trouve des couples  $(w_1, w_2)$  tels que  $w_1 + w_2 = w$ , où  $w_1$  et  $w_2$  sont de la même longueur (et pas plus longs) que  $w$ . Cela peut poser des problèmes. Par exemple, en base 5 :

$$\begin{aligned} k &= 2 \cdot 314 \\ i &= 1 \cdot 4012013 \\ j &= 0 \cdot 4122432 \\ k &= i + j. \end{aligned}$$

Ainsi, si on s'intéresse au nombre  $k = 2.314$ , il existe des entiers  $i$  et  $j$  dont le développement est arbitrairement long et dont la somme vaut  $k$ , mais l'automate  $M'$  ne peut pas les trouver.

Par contre, on ne peut pas avoir une infinité de tels  $i$  et  $j$  dont la somme vaut  $k$ . En effet  $i$  et  $j$  appartiennent chacun à des ensembles bien ordonnés ( $A_1$  et  $A_2$ ), or si on avait une infinité de tels couples  $(i, j)$ , soit l'ensemble des  $i$ , soit l'ensemble des  $j$ , contiendrait une suite infinie décroissante, ce qui ne se peut, donc il existe quand même un nombre fini des tels couples  $i$  et  $j$  tels que  $i + j = k$ .

- Pour calculer le nombre total de tels couples, il suffit alors d'ajouter un nombre  $m = |Q|$  de zéros à la fin de l'écriture en base  $p$  de  $k$  pour que l'automate "trouve" bien tous les  $i \in A_1$  et  $j \in A_2$  dont la somme vaut  $k$ . C'est-à-dire que, avec les hypothèses qu'on a sur  $A_1$  et  $A_2$ , si deux nombres  $i$  et  $j$  ont pour somme un nombre  $k$  ayant  $n$  chiffres,  $i$  et  $j$  ne peuvent avoir plus de  $n + m$  chiffres.

Pour prouver cela, on considère un mot  $w$  qui commence par  $m$  zéros (n'oublions pas que  $w$  est le miroir du développement de  $k$  en base  $p$ , donc si celui ci se termine par  $m$  zéros, alors  $w$  commence par  $m$  zéros). Nous allons montrer que, dans ce cas, tous les couples  $(w_1, w_2)$  dont la somme vaut  $w$ , sont tels que  $w_1$  et  $w_2$  commencent chacun par un 0 (donc les développements de  $i$  et  $j$  se terminent tous deux par zéro). Cela implique que si on ajoute encore un 0 (ou autant qu'on veut) à l'écriture en base  $p$  de  $k$  (qui se termine déjà par  $m$  zéros), le nombre des chemins acceptant par  $w$  dans  $M'$  ne change pas, et ainsi on trouve le nombre total des couples avec la propriété désirée.

Il reste donc à démontrer l'assertion suivante :

- Si un mot  $w$  commence par  $m = |Q|$  zéros, alors tous les couples  $(w_1, w_2)$ , dont la somme vaut  $w$ , sont tels que  $w_1$  et  $w_2$  commencent chacun par un 0.

Par l'absurde, si  $w_1$  commence par une lettre différente de 0. D'après le lemme de l'étoile, à la lecture de  $(w_1, w_2)$  par l'automate  $M$ , on passe forcément deux fois par le même état, disons  $q$ , avant  $m$  coups (car la longueur de  $w_i$  est plus grande que  $m$ , le nombre d'états de  $M$ ). On peut alors écrire  $(w_1, w_2) = (b_1 w'_1 e_1, b_2 w'_2 e_2)$ , où  $(b_1, b_2)$  est le mot lu avant l'apparition de l'état  $q$ ,  $(w'_1, w'_2)$  le mot lu entre les deux passages par l'état  $q$  et  $(e_1, e_2)$  le mot restant entre l'état  $q$  et l'état final. Dans ce cas, tous les mots :

$$(b_1 e_1, b_2 e_2), (b_1 w'_1 e_1, b_2 w'_2 e_2), (b_1 w'_1 w'_1 e_1, b_2 w'_2 w'_2 e_2), \dots$$

sont des mots acceptés par l'automate  $M$ .

Ces mots représentent les écritures inverses en base  $p$  d'une infinité de nombres  $(i_n, j_n)$  de  $A_1 \times A_2$ . Comme  $b_1$  ne commence par 0, on peut remarquer que les  $i_n$  sont tous différents. De plus  $i_n + j_n = k$ . Cela implique qu'on peut extraire une sous-suite infinie strictement décroissante de l'ensemble  $A_i$ , ce qui est impossible car il s'agit d'un ensemble bien ordonné.  $\square$

On a démontré que l'ensemble des séries quasi- $p$ -automatiques,  $K_q$ , est un anneau. Pour démontrer que celui-ci est bien un corps, il reste à démontrer la dernière propriété, P3.

*Preuve de P3.* Tout d'abord, on remarque que tout élément de  $\mathbb{F}_q(t)$  est aussi dans  $K_q$ . Pour prouver cela, considérons  $x \in \mathbb{F}_q(t)$ . Alors  $x$  s'écrit aussi de la forme

$$x = \sum_{k=0}^{\infty} c_k t^k,$$

où la suite  $(c_k)_k$  est ultimement périodique et donc  $p$ -automatique. Ainsi  $x$  est  $p$ -automatique et est inclus dans  $K_q$ .

Dans la preuve de cette proposition on utilise la première implication du théorème de Kedlaya. Si une série est quasi-automatique, elle sera algébrique sur  $\mathbb{F}_q(t)$ . Soit donc

$x \in \mathbb{F}_q(t)$ . Il existe alors un polynôme à coefficients dans  $\mathbb{F}_q(t)$ ,  $P(z) = c_0 + c_1z + \cdots + c_nz^n$  qui a  $x$  comme racine. De plus, on peut supposer que  $c_0, c_n \neq 0$ . Donc :

$$c_0 + c_1x + \cdots + c_nx^n = 0.$$

Cela implique que  $x \cdot (c_1 + c_2x + \cdots + c_nx^{n-1}) = -c_0$  et par conséquent

$$x^{-1} = - \underbrace{c_0^{-1}}_{\in \mathbb{F}_q(t)} (c_1 + \cdots + c_nx^{n-1}).$$

Puisque tout élément de  $\mathbb{F}_q(t)$  est aussi dans  $K_q$ , le terme de droite est bien contenu dans  $K_q$ . Finalement, on a bien que l'inverse d'une série quasi-automatique est toujours une série quasi-automatique et donc  $K_q$  est un corps. □

### II.3.3 Clôture topologique et clôture algébrique

Dans cette partie nous allons démontrer que le complété topologique (pour la valuation  $v$ ) du corps des séries formelles généralisées quasi- $p$ -automatiques est algébriquement clos. Plus précisément, nous voulons démontrer la proposition suivante.

**Proposition II.3.1.** *Soit  $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$  le complété (pour la valuation  $v$ ) du corps de séries quasi- $p$ -automatiques. Soit  $R = \cup_{q'} R_{q'}$ , l'union portant sur toutes les puissances  $q'$  de  $q$ . Alors le corps  $R$  est algébriquement clos.*

**Remarque.** Autrement dit, si on considère une série formelle généralisée  $x$  algébrique sur  $\mathbb{F}_q(t)$ , on peut toujours trouver  $q'$ , une puissance de  $q$ , et une série  $y \in \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ , quasi- $p$ -automatique aussi proche que l'on veut de  $x$  (au sens de la distance induite par la valuation  $v$ ). Ce résultat jouera un rôle important pour démontrer la deuxième implication de la preuve du théorème de Kedlaya.

Afin de démontrer cette proposition, nous allons utiliser les lemmes suivantes.

**Lemme II.3.4.** *Soit  $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  une série quasi- $p$ -automatique. De plus, on suppose que le support de  $x$  est inclus dans  $] -\infty, 0[$ . Alors l'équation  $y^p - y = x$  admet une solution  $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$  quasi- $p$ -automatique.*

La preuve du lemme II.3.4 peut être vue dans [9].

**Lemme II.3.5.** *Soit  $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$  le complété (pour la valuation  $v$ ) du corps de séries quasi- $p$ -automatiques. Alors il existe une puissance de  $q$ ,  $q'$ , telle que l'équation :*

$$z^p - az = b \quad a, b \in R_q \quad a \neq 0$$

*a p racines distinctes dans  $R_{q'}$ .*

*Démonstration du lemme II.3.5.* Tout d'abord, on résout l'équation dans le cas particulier  $b = 0$ . On doit donc montrer que l'équation  $z^{p-1} = a$  a  $(p-1)$  racines distinctes dans  $R_{q'}$ , pour une certaine puissance de  $q, q'$ . On peut écrire  $a = a_0 t^i (1+u)$ , avec  $a_0 \in \mathbb{F}_q, i \in \mathbb{Q}$  et  $v(u) > 0$ . On choisit  $q'$  tel que  $z^{p-1} = a_0$  a toutes les racines dans  $\mathbb{F}_{q'}$  et on pose

$$z = a_0^{1/(p-1)} t^{i/(p-1)} \sum_{j=0}^{\infty} \binom{1/(p-1)}{j} u^j$$

pour toutes les racines  $p$ -ièmes de  $a_0$ , notées ici  $a_0^{1/(p-1)}$ .

Maintenant on revient sur le cas où  $b$  est une série quelconque de  $R_q$ . D'après le paragraphe précédent, on peut supposer que  $a = 1$  et il suffit donc de résoudre l'équation :

$$z^p - z = b.$$

**Remarque.** Ceci est une équation d'Artin-Schreier. Si  $b$  est un élément d'un corps  $K$  de caractéristique  $p$ , le corps de décomposition du polynôme  $X^p - X = b$  au-dessus de  $K$  est appelé *extension d'Artin-Schreier*. Si on peut déterminer une racine  $z$  de ce polynôme, alors on peut déterminer toutes les autres racines. En effet, les racines du polynôme sont  $z, z+1, z+2, \dots, z+p-1$ . Elles sont toutes distinctes, donc le corps de décomposition est séparable. C'est une extension cyclique de degré  $p$  de  $K$ , le groupe de Galois étant engendré, par exemple, par le morphisme  $z \rightarrow z+1$ . Le théorème d'Artin-Schreier affirme que toute extension cyclique de degré  $p$  d'un corps de caractéristique  $p$  est une extension d'Artin-Schreier.

Afin de résoudre l'équation  $z^p - z = b$ , on peut écrire la série formelle généralisée  $b$  sous la forme  $b = b_+ + b_-$ , où  $b_+$  est une série dont le support est inclus dans  $[0, \infty[$  et  $b_-$  est une série dont le support est inclus dans  $] -\infty, 0]$ . Nous allons traiter les deux cas séparément.

À présent, on considère l'équation  $z^p - z = b_+$ . Soit  $b_0$  le terme constant de  $b_+$  et soit  $q'$  tel que le polynôme  $z^p - z = b_0$  a toutes les racines, disons  $c_1, c_2, \dots, c_p$  dans le corps  $\mathbb{F}_{q'}$ . Alors les séries  $z_i$  définies de la manière suivante :

$$z_i = c_i - \sum_{j=0}^{\infty} (b_+ - b_0)^{p^j}$$

sont bien les solutions de l'équation  $z^p - z = b_+$ .

Il reste maintenant à résoudre l'équation  $z^p - z = b_-$ . D'après le lemme II.3.4, il existe une solution  $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$  quasi- $p$ -automatique.

Finalement, les  $p$  solutions de l'équation  $z^p - z = b$  sont de la forme  $y + z_i$ , où  $y$  est la solution de l'équation précédente et les  $z_i$ , pour  $i = 1, 2, \dots, p$  sont les solutions de l'équation  $z^p - z = b_+$ .  $\square$

*Démonstration de la proposition II.3.1.* D'après le lemme d'Ore, il suffit de prouver que pour tout polynôme tordu  $P(F) \in R_q\{F\}$ , de degré  $n$ , le polynôme  $P(F)(z)$  se factorise complètement sur  $R_{q'}$ ,  $q'$  désignant une puissance de  $q$ . De plus,  $R_q$  est parfait et on peut alors factoriser  $F$ , s'il apparaît ; ainsi on obtiendrait un polynôme dont le coefficient constant est non nul. D'après le lemme II.2.3 ceci équivaut au fait que  $P(F)(z)$  n'a pas de racines multiples (en effet, le noyau de  $P$ , considéré comme une application sur  $R_{q'}$ , est de dimension égale au degré de  $P(F)$ , donc ce noyau a  $p^n$  éléments).

D'après la proposition II.2.3 on peut factoriser le polynôme  $P = Q_1Q_2 \dots Q_n$ , où les  $Q_i$  désignent des polynômes tordus, unitaires, à coefficients dans  $R_{q'}$  (pour une puissance  $q'$  de  $q$ ). On écrit donc  $Q_i = F - c_i$ ,  $c_i \neq 0$ .

Nous allons démontrer que le polynôme  $P(F)(z)$ , polynôme de degré  $p^n$  en la variable  $z$ , a ses  $p^n$  racines dans une extension finie de  $R_q$ , notée désormais  $R_{q'}$ . Il faut donc résoudre l'équation :

$$Q_1Q_2 \dots Q_n(F)(z) = (F - c_1)(F - c_2) \dots (F - c_n)(z) = 0.$$

Cela nous amène à résoudre le système d'équations suivant :

$$\begin{aligned} z_1^p - c_1z_1 &= 0 \\ z_2^p - c_2z_2 &= z_1 \\ &\vdots \\ z_n^p - c_nz_n &= z_{n-1} \end{aligned}$$

Si on démontre que toute équation de ce système admet  $p$  racines distinctes dans  $R_{q'}$ , alors le système aura bien  $p^n$  racines distinctes (de plus, il n'y a pas une même racine pour deux équations du système) comme souhaité.

Finalement, à l'aide du lemme II.3.5 le système considéré précédemment admet donc bien  $p^n$  racines distinctes contenues dans une extension  $R_{q'}$  de  $R_q$ . Cela implique donc que le polynôme  $P(F)(z) = (F - c_1)(F - c_2) \dots (F - c_n)(z)$  se factorise complètement sur ce corps et la proposition est ainsi démontrée. □

### II.3.4 Preuve de la seconde implication du théorème

Dans cette partie, nous allons démontrer la deuxième implication du théorème de Kedlaya : si  $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est algébrique sur  $\mathbb{F}_q(t)$ , alors  $x$  est une série quasi- $p$ -automatique.

Pour cela on va procéder en plusieurs étapes :

- La première étape consiste à démontrer que  $x$  est contenu dans une extension finie du corps de séries formelles  $\mathbb{F}_{q'}((t))$  et, plus précisément,  $x \in \mathbb{F}_{q'}((t))(y)$ , où  $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$  est une série quasi- $p$ -automatique. Donc  $x$  s'écrit de la forme

$$x = \sum_{i=0}^{m-1} b_i y^i,$$

avec les  $b_i \in \mathbb{F}_{q'}((t))$ .

On veut se placer dans une extension finie de  $\mathbb{F}_{q'}((t))$ , puisque c'est un corps complet pour la valuation  $v$  et on peut appliquer plusieurs propriétés des corps locaux (corps valués complets).

- Nous allons démontrer ensuite que les  $b_i$  sont algébriques sur  $\mathbb{F}_{q'}(t)$ .

- La dernière étape consiste à appliquer le théorème de Christol. Les  $b_i$ , étant algébriques, ils sont donc  $p$ -automatiques et à fortiori quasi- $p$ -automatiques. Par conséquent, la série  $x$ , est une combinaison finie d'éléments quasi- $p$ -automatiques et elle est donc elle-même quasi- $p$ -automatique.

*Démonstration du théorème II.1.1. Etape 1.* Puisque  $x$  est algébrique sur  $\mathbb{F}_q(t)$ , il existe un polynôme  $P \in \mathbb{F}_q(t^{1/p^m})$  qui admet  $x$  comme racine simple. Si  $x$  est algébrique, alors  $x^{p^m}$  l'est aussi. Quitte à remplacer  $x$  par  $x^{p^m}$ , on peut donc supposer sans perte de généralité que  $x$  est une racine simple d'un polynôme  $P(z)$  à coefficients dans le corps  $\mathbb{F}_q(t^{1/p})$ .

Si  $x'$  est une racine de  $P$  différente de  $x$ , alors  $v(x - x') < +\infty$ . Puisque  $P$  n'a qu'un nombre fini de racines et que  $x$  est une racine simple, il existe une constante  $c \in \mathbb{Q}$  telle que  $c > v(x - x')$ , pour toute racine  $x' \neq x$ .

Par la proposition II.3.1, pour tout  $c \in \mathbb{Q}$ , il existe une puissance  $q'$  de  $q$  et  $y \in \mathbb{F}_{q'}((t^{\mathbb{Q}}))$  une série quasi- $p$ -automatique tels que  $v(x - y) \geq c$ .

Le polynôme  $P(z + y)$  a une unique racine de valuation supérieure à  $c$ , plus précisément,  $v(x - y) \geq c$  et toutes les autres racines  $x' - y$  ont des valuations inférieures à  $c$ .

La série quasi- $p$ -automatique  $y \in \mathbb{F}_{q'}((t^{\mathbb{Q}}))$  est aussi algébrique sur  $\mathbb{F}_{q'}(t)$  par la première implication du théorème de Kedlaya. Soit  $K$  l'extension de  $\mathbb{F}_{q'}((t))$  obtenue en ajoutant  $y$ . C'est une extension finie (car  $y$  est algébrique sur  $\mathbb{F}_{q'}(t)$  et  $\mathbb{F}_{q'}(t) \subset \mathbb{F}_{q'}((t))$ ) qui est donc complète pour la valuation  $v$ .

On peut appliquer maintenant la proposition II.2.2. Le polynôme  $P(z + y)$  se factorise uniquement sous la forme du produit  $Q_1 Q_2 \dots Q_n$ , avec  $Q_i(z) \in K(z)$ , unitaire de pente  $s_i$ . De plus,  $s_1 < s_2 < \dots < s_n$ . Puisque  $x - y$  est une racine de valuation supérieure à  $c$ , et comme toutes les autres racines ont des valuations inférieures à  $c$ , la proposition II.2.1 implique que le polygone de Newton de  $P(z + y)$  contient un segment de pente égale à  $v(x - y)$ . Il s'agit bien sûr de la pente  $s_n$  et alors  $Q_n(z) = z - (x - y)$ . Puisque  $Q_n \in K[z]$ ,  $x - y \in K$ . D'autre part  $y \in K$  par définition de l'extension  $K$  et donc la série  $x$  est également contenue dans  $K$ .

Soit  $m$  le degré du polynôme minimal de  $y$  sur  $\mathbb{F}_{q'}(t)$ . Alors  $[\mathbb{F}_{q'}((t))(y) : \mathbb{F}_{q'}((t))] = m$  et les éléments  $1, y, \dots, y^{m-1}$  constitue une base de  $K$ . Donc tout élément peut s'écrire comme une  $\mathbb{F}_{q'}((t))$ -combinaison lineaire de la forme :  $\alpha_0 + \alpha_1 y^1 + \dots + \alpha_{m-1} y^{m-1}$ . En particulier,  $x$  étant un élément de  $K$ , il admet une telle écriture.

*Etape 2.* Tout élément de  $K$  s'écrit comme une  $\mathbb{F}_{q'}((t))$ -combinaison lineaire des éléments  $1, y, \dots, y^{m-1}$ . Puisque les  $y^{pj}$  sont aussi dans  $K$ , alors :

$$y^{pj} = \sum_{i=0}^{m-1} a_{ij} y^i,$$

pour  $j = 0, 1, \dots, m - 1$  et  $a_{ij} \in \mathbb{F}_{q'}((t))$ . De plus, les  $a_{ij}$  sont algébriques sur  $\mathbb{F}_{q'}(t)$ .

Soit  $n$  le plus petit entier tel que  $x, x^p, \dots, x^{p^n}$  soient linéairement dépendants sur  $\mathbb{F}_{q'}((t))$  (un tel  $n$  existe d'après le lemme d'Ore). Donc il existe des  $c_i \in \mathbb{F}_{q'}((t))$  tels que

$$c_0 x + c_1 x^p + \dots + c_n x^{p^n} = 0.$$

On peut de plus supposer que  $c_0 = 1$  et alors on remarque que les  $c_i$  sont algébriques sur  $\mathbb{F}_{q'}(t)$ .

De plus,  $x^{p^j} \in K$ , pour tous les  $j = 0, 1, \dots, n - 1$ , donc il existe des  $b_{ij} \in \mathbb{F}_{q'}((t))$  tels que :

$$x^{p^j} = \sum_{i=0}^{m-1} b_{ij} y^i.$$

En calculant de deux façons le terme  $x^{p^{j+1}}$ , on en déduit que

$$b_{i(j+1)} = \sum_{l=0}^{m-1} b_{lj}^p a_{il}.$$

les  $c_j$  et les  $a_{ij}$ . D'un coté,  $x = x^{p^0} = \sum_{i=0}^{m-1} b_{i0} y^i$ . D'autre part,

$$\begin{aligned}
x &= \sum_{j=0}^{n-1} -c_{j+1} \left( x^{p^j} \right)^p \\
&= \sum_{j=0}^{n-1} -c_{j+1} \left( \sum_{i=0}^{m-1} b_{ij} y^i \right)^p \\
&= \sum_{j=0}^{n-1} -c_{j+1} \sum_{i=0}^{m-1} b_{ij}^p y^{pi} \\
&= \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} \sum_{l=0}^{m-1} -c_{j+1} b_{ij}^p a_{li} y^l.
\end{aligned}$$

En identifiant maintenant les coefficients des puissances de  $y$  dans les deux expressions, on obtient :

$$b_{i0} = \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{lj}^p a_{il}.$$

De plus, puisque

$$b_{i(j+1)} = \sum_{l=0}^{m-1} b_{lj}^p a_{il},$$

on peut calculer les  $b_{ij}$ , pour tous les  $j = 0, 1, \dots, n-1$  et  $i = 0, 1, \dots, m-1$ .

Cela nous conduit à un système d'équations de la forme

$$Id \cdot v = A \cdot v^\sigma,$$

où  $\sigma$  est le morphisme de Frobenius,  $A$  une matrice dont les coefficients sont des combinaisons des  $a_{il}$  et  $c_j$ , donc des éléments algébriques sur  $\mathbb{F}_{q'}(t)$  et  $v$  est le vecteur dont les coefficients sont les  $b_{ij}$ . On peut alors appliquer le lemme II.2.1, la matrice identité étant bien sûr inversible.

Par conséquent, les coefficients du vecteur  $v$  sont algébriques sur  $\mathbb{F}_{q'}(t)$ . En particulier les  $b_{i0}$  sont aussi algébriques sur  $\mathbb{F}_{q'}(t)$ .

*Etape 3.* Nous pouvons à présent appliquer le théorème de Christol, démontré dans la première partie du mémoire. Les  $b_{i0}$  sont des séries formelles à coefficients dans  $\mathbb{F}_{q'}$  algébriques sur  $\mathbb{F}_{q'}(t)$ . Par conséquent, elles sont aussi  $p$ -automatiques. Puisque  $x = \sum_{i=0}^{m-1} b_{i0} y^i$  et puisque le produit (respectivement la somme) d'éléments quasi- $p$ -automatiques reste quasi- $p$ -automatique,  $x$  est quasi- $q'$ -automatique, donc quasi- $p$ -automatique, ce qui achève la démonstration du théorème.  $\square$

## Conclusions

Dans ce mémoire nous avons décrit et démontré deux résultats importants utilisant les automates finis afin de déterminer l’algébricité ou la transcendance de certaines séries formelles, classiques ou généralisées. Plus précisément, nous avons démontré, dans la première partie de cette étude, le théorème de Christol qui stipule qu’une série formelle à coefficients dans un corps fini de caractéristique positive  $p$  est algébrique sur le corps  $\mathbb{F}_p(t)$  si, et seulement si, la suite de ses coefficients est  $p$ -automatique. Dans la deuxième partie, nous avons étendu ce théorème aux séries formelles de Hahn, en démontrant qu’une série formelle de Hahn appartenant à  $\mathbb{F}_p((t^{\mathbb{Q}}))$  est algébrique sur le corps  $\mathbb{F}_p(t)$  si, et seulement si, elle est quasi- $p$ -automatique au sens de Kedlaya.

Les résultats qui peuvent être obtenus à partir de ces deux théorèmes prouvent bien l’efficacité de cette méthode. Nous avons vu, par exemple, à la fin de la première partie de ce mémoire, comment le théorème de Christol permet de démontrer la transcendance de la série formelle  $\Pi_q$  introduite par Carlitz. Cette série est l’analogie dans ce contexte du nombre réel  $\pi$ . De même, le théorème de Christol peut s’appliquer pour obtenir la transcendance d’autres analogues définis par Carlitz des fonctions logarithme, exponentielle, gamma ou zeta. Cette approche, que l’on appelle parfois la méthode “automatique”, a donné lieu à de nombreux travaux (voir par exemple [2, 3, 10]).

Les théorèmes de Christol et de Kedlaya ont d’autres applications très intéressantes comme, par exemple, un résultat sur le produit de Hadamard. Ce dernier est défini, pour deux séries formelles  $A = \sum_i a_i X^i$  et  $B = \sum_i b_i X^i \in K[[X]]$ ,  $K$  désignant un corps, par :

$$A \odot B = \sum_i a_i b_i X^i.$$

Une application assez directe du théorème de Christol pour les séries formelles (respectivement du théorème de Kedlaya pour les séries de Hahn) s’énonce alors de la façon suivante.

**Théorème II.3.1.** *Si  $A$  et  $B$  sont deux séries formelles algébriques sur  $\mathbb{F}_q(X)$ , alors le produit de Hadamard  $A \odot B$  est aussi algébrique.*

Le produit de Hadamard a été introduit par Hadamard en 1899. Le théorème précédent a été démontré par Furstenberg en 1967. Un autre théorème démontré aussi par Furstenberg, en forte relation avec le produit de Hadamard, est le théorème suivant.

**Théorème II.3.2.** *Une série de Laurent à coefficient dans un corps fini est algébrique si, et seulement si, elle est diagonale d’une série rationnelle en deux variables commutatives.*

Nous rappelons que la diagonale d’une série  $F(X, Y) = \sum_{m \geq m_0, n \geq n_0} a_{m,n} X^m Y^n$  est définie comme étant la série

$$DF(X) = \sum_{k \geq \max\{m_0, n_0\}} a_{k,k} X^k.$$

Ce résultat est valable pour les séries formelles ordinaires. Il serait intéressant de savoir s'il existe un résultat analogue pour les séries de Hahn.

Il serait également intéressant de savoir s'il est possible d'utiliser le théorème de Kedlaya pour prouver la transcendance de certains analogues de nombres réels, et d'étendre ainsi la méthode "automatique" mentionnée précédemment.

## A Polynômes additifs et démonstration du lemme II.2.3

**Définition A.0.2.** Soient  $K$  un corps de caractéristique positive  $p$  et  $P$  un polynôme à coefficients dans  $K$ . On dit que  $P$  est un polynôme additif s'il est de la forme :

$$P(z) = c_0z + c_1z^p + \dots + c_nz^{p^n},$$

où  $c_0, c_1, \dots, c_n \in K$ .

**Lemme A.0.6.** Soient  $K$  un corps de caractéristique positive  $p$  et  $r_1, r_2, \dots, r_n \in K$ . Le déterminant de la matrice suivante (appelé aussi déterminant de Moore)

$$\begin{pmatrix} r_1 & r_2 & \dots & r_n \\ r_1^p & r_2^p & \dots & r_n^p \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{p^{n-1}} & r_2^{p^{n-1}} & \dots & r_n^{p^{n-1}} \end{pmatrix}$$

est nul si, et seulement si, les  $r_1, r_2, \dots, r_n$  sont linéairement dépendants dans le corps  $\mathbb{F}_p$ .

*Démonstration.* Ce déterminant peut être considéré comme un polynôme à coefficients dans  $\mathbb{F}_p$ , en variables  $r_1, r_2, \dots, r_n$ . Il est divisible par toutes les formes linéaires

$$c_1r_1 + c_2r_2 + \dots + c_nr_n,$$

$c_1, c_2, \dots, c_n \in \mathbb{F}_p$ , pas tous nuls. Ceci implique qu'il est aussi divisible par le produit de toutes ces expressions, donc par :

$$\prod_{(c_1, c_2, \dots, c_n) \in \mathbb{F}_p^n \setminus (0, 0, \dots, 0)} c_1r_1 + c_2r_2 + \dots + r_nc_n.$$

D'autre part, le déterminant est un polynôme homogène, de degré égal à  $p^{n-1} + \dots + p^2 + p + 1$ . Ainsi, le déterminant de Moore est égal à

$$\prod_{(c_1, c_2, \dots, c_n) \in \mathbb{F}_p^n \setminus (0, 0, \dots, 0)} c_1r_1 + c_2r_2 + \dots + r_nc_n$$

multiplié par une constante. Par conséquent, il est nul si, et seulement si, ce produit est nul, donc si, et seulement si, les  $r_1, r_2, \dots, r_n$  sont linéairement dépendants dans le corps  $\mathbb{F}_p$ .  $\square$

**Proposition A.0.2.** Soit  $P(z)$  un polynôme, non nul à coefficients dans un corps  $K$  de caractéristique  $p > 0$  et soit  $L$  une clôture algébrique de  $K$ . Alors on a l'équivalence :

(a)  $P(z)$  est un polynôme additif.

(b)  $P(y + z) = P(y) + P(z)$ , pour tous  $y, z \in L$ .

(c) Les racines de  $P$  dans  $L$  forment un  $\mathbb{F}_p$ -espace vectoriel et elles ont toutes la même multiplicité. Plus précisément, c'est une puissance de  $p$ .

*Démonstration.* L'implication (a) $\Rightarrow$ (b) est claire.

(c) $\Rightarrow$ (a)

Soit  $V \subset L$  l'ensemble des racines de  $P$  et soit  $p^e$  leur multiplicité commune. Soit  $Q(z)$  le déterminant de Moore dans les variables  $z^{p^e}, r_1^{p^e}, r_2^{p^e}, \dots, r_m^{p^e}$ . D'après le lemme A.0.6 les racines de  $Q$  sont les éléments de  $V$ , chacune apparaît avec une multiplicité au moins égale à  $p^e$ . Mais  $\deg Q = p^{e+m} = \deg P$ , donc la multiplicité des racines de  $Q$  doit être exactement  $p^e$ . Donc  $P = Q \times \text{constante}$  et, puisque  $Q$  est additif,  $P$  l'est aussi.

(b) $\Rightarrow$ (c)

Etant donnée la proposition (b), on peut démontrer facilement que les racines de  $P$  dans  $L$  forment un  $\mathbb{F}_p$ -espace vectoriel. De plus, si  $r$  est une telle racine, alors  $P(z+r) = P(z)$  et par conséquent, les racines occurrent avec une même multiplicité dans  $P$ .

Il reste à montrer que cette multiplicité commune, notée  $n$ , est exactement une puissance de  $p$ .

Soit  $V$  l'ensemble des racines de  $P$  et soient  $r_1, r_2, \dots, r_m$  les générateurs de  $\mathbb{F}_p$ -espace vectoriel  $V$ . Soit  $Q(z)$  le déterminant de Moore dans les variables  $z, r_1, r_2, \dots, r_m$ . Le raisonnement précédemment implique que  $Q$  n'a pas de racines multiples et donc que  $P(z) = \text{constante} \times Q(z)^n$ .

Supposons par l'absurde que  $n$  n'est pas une puissance de nombre premier. Alors les polynômes  $(y+z)^n$  et  $y^n + z^n$  ne sont pas identiquement égaux ( car  $\binom{n}{p^i}$  n'est pas divisible par  $p$ , donc il n'est pas nul dans un corps de caractéristique  $p$ , pour le plus grand  $i$  tel que  $p^i$  divise  $n$  ). Donc il existe des  $y, z \in L$  tels que  $(y+z)^n \neq y^n + z^n$ . Puisque  $L$  est algébriquement clos,  $Q : L \rightarrow L$  est une application surjective. Ainsi on peut choisir  $y, z \in L$  tels que  $(Q(y) + Q(z))^n \neq Q(y)^n + Q(z)^n$  et comme  $Q$  est additif,  $P(y+z) \neq P(y) + P(z)$ , ce qui contredit l'hypothèse. Par conséquent,  $n$  est une puissance de  $p$ . □

*Démonstration du lemme II.2.3.* Le noyau est un  $\mathbb{F}_p$ -espace vectoriel car  $T(F)$  est un opérateur additif et alors on peut appliquer A.0.2. De plus  $T(F)(z)$  est un polynôme de degré  $p^d$  et donc la dimension du  $\mathbb{F}_p$ -espace vectoriel est inférieure ou égale à  $d$ . L'égalité est obtenue si, et seulement si, le polynôme en variable  $z$ ,  $T(F)(z)$ , n'a pas de racines multiples; donc, si, et seulement si, sa dérivée est non nulle, donc  $c_0 \neq 0$  (puisque la caractéristique est  $p$ , la dérivée est bien égale à  $c_0$ ). □

## B Polynômes tordus et démonstration de la proposition II.2.3

**Lemme B.0.7.** Soient  $S(F)$  et  $T(F)$  deux polynômes tordus à coefficients dans  $K$ ,  $T(F)$  non nul, de degré égal à  $d \geq 0$ . Il existe alors un unique couple de polynômes tordus à coefficients dans  $K$ ,  $Q(F)$  et  $R(F)$ ,  $\deg(R) < d$ , tel que  $S = QT + R$ .

*Démonstration.* L'existence se déduit par récurrence sur le degré de  $S$ . Pour démontrer l'unicité, on suppose par l'absurde qu'il existe deux couples  $(Q, R)$  et  $(Q', R')$  tels que  $S = QT + R = Q'T + R'$ . Ceci implique que  $R - R' = (Q' - Q)T$ . Mais, puisque  $\deg(R - R') < \deg(T)$ , alors  $R - R' = 0$ .  $\square$

**Lemme B.0.8.** Soient  $S(F)$  et  $T(F)$  deux polynômes tordus à coefficients dans  $K$ , tel que le coefficient constant de  $T(F)$  est non nul. Soit  $L$  une clôture algébrique de  $K$ . Alors  $S$  est un multiple "gauche" de  $T$ , c'est à dire, il existe  $Q \in K\{F\}$  tel que  $S = QT$ , si, et seulement si,  $\ker_L(T) \subseteq \ker_L(S)$ .

**Remarque.** Ici  $\ker_L(P)$  signifie le noyau de l'opérateur  $P$ , c'est à dire l'ensemble de  $z \in L$  tels que  $P(F)(z) = 0$

*Démonstration.* Si  $S = QT$ , alors  $T(F)(z) = 0 \Rightarrow S(F)(z) = 0$ . D'où

$$\ker_L(T) \subseteq \ker_L(S).$$

Réciproquement, si  $\ker_L(T) \subseteq \ker_L(S)$ , nous écrivons, d'après le lemme B.0.7,  $S = QT + R$ . Ainsi

$$\ker_L(T) \subseteq \ker_L(R).$$

D'après le lemme B.0.8,  $\ker_L(T)$  est un  $\mathbb{F}_p$ -espace vectoriel de dimension égale à  $\deg(T)$ . Mais si, par l'absurde,  $R \neq 0$ , alors  $\ker_L(R)$  était un  $\mathbb{F}_p$ -espace vectoriel de dimension  $\deg(R) < \deg(T)$ , ce qui contredirait l'inclusion  $\ker_L(T) \subseteq \ker_L(R)$ . Donc  $R = 0$  et  $S = QT$ .  $\square$

Dans ce paragraphe, on utilise le fait que, pour tout sous-corps  $K$  de  $\mathbb{F}_q((t^\mathbb{Q}))$ , il existe une unique manière de prolonger la valuation  $v$  à toute clôture algébrique du corps  $K$  ( cf. [11] ).

**Lemme B.0.9.** Soit  $K$  un sous-corps de  $\mathbb{F}_q((t^\mathbb{Q}))$ , complet pour la valuation  $v$ . Soit  $P$  un polynôme unitaire additif à coefficients dans  $K$  et soit  $Q_1 Q_2 \dots Q_n t^{p^d}$  sa factorisation en produit de polynômes de pentes pures. Alors  $Q_n t^{p^d}$  est aussi additif.

*Démonstration.* Grâce à la proposition A.0.2, nous devons démontrer que les racines du polynôme  $Q_n t^{p^d}$  forment un  $\mathbb{F}_p$ -espace vectoriel et, de plus, toutes ses racines doivent avoir la même multiplicité, une puissance de  $p$ .

Soit  $L$  une clôture de  $K$  et soient  $V$  l'ensemble de racines du polynôme  $P$  dans  $L$ . Celui-ci est un espace vectoriel, toujours d'après la proposition A.0.2. Soient  $s_1 < s_2 < \dots < s_n$  les

pentés des polynômes  $Q_1, Q_2, \dots, Q_n$ . D'après la proposition II.2.1, les valuations possibles des racines de  $P$  se retrouvent parmi les pentés de  $P$ , donc elles sont parmi les  $s_1, s_2, \dots, s_n$ . De plus, un élément de  $V$  est une racine de  $P$  si, et seulement si,  $v(x) \geq s_n$ . Cet ensemble constitue un  $\mathbb{F}_p$ -sous-espace vectoriel de  $V$ . De plus, chaque racine est de multiplicité égale à  $p^d$ . D'après la proposition A.0.2,  $Q_n t^{p^d}$  est un polynôme additif.  $\square$

**Définition B.0.3.** Soit  $P(F)$  un polynôme tordu à coefficients dans  $\mathbb{F}_q((t^{\mathbb{Q}}))$ . Pour  $r \in \mathbb{Q}$ , on dit que  $P(F)$  est de pente pure égale à  $r$  si on a les conditions suivantes :

- le coefficient constant de  $P$  est non nul,
- le polynôme en variable  $z$  :

$$\frac{P(F)(z)}{z}$$

est de pente pure égale à  $r$ .

Par convention, toute puissance de  $F$  est un polynôme de pente pure égale à  $\infty$ .

**Proposition B.0.3.** Soit  $K$  un sous-corps de  $\mathbb{F}_q((t^{\mathbb{Q}}))$ , complet pour la valuation  $v$ . Soit  $P(F)$  un polynôme tordu, unitaire, à coefficients dans  $K$ . Alors il existe une factorisation de  $P$  sous la forme  $P = Q_1 Q_2 \dots Q_n$ , avec chaque  $Q_i \in K\{F\}$  unitaire, de pente pure.

*Démonstration.* On considère la factorisation du polynôme additif

$$P(F)(z) = T_1 T_2 \dots \underbrace{T_n z^{p^d}}_{R(z)}.$$

D'après le lemme B.0.9, le polynôme  $R(z)$  est additif et, par conséquent, il existe un polynôme tordu  $Q$  tel que  $R(z) = Q(F)(z)$ . Les racines de  $R(z)$  sont aussi des racines pour  $P(F)(z)$  et donc  $\ker_L(Q) \subseteq \ker_L(P)$ . D'après le lemme B.0.8,  $P$  est un multiple gauche de  $Q$ , c'est à dire, il existe un polynôme  $P_1$ , de degré inférieur à  $P$  tel que  $P = P_1 Q$ . On répète le procédé jusqu'à obtenir la décomposition voulue.  $\square$

**Proposition B.0.4.** Soit  $K$  un sous-corps de  $\mathbb{F}_q((t^{\mathbb{Q}}))$ , complet pour la valuation  $v$ . Soit  $P(F)$  un polynôme tordu, unitaire, à coefficients dans  $K$ , de pente pure égale à 0. Alors le polynôme  $P(F)(z)$  se factorise en produit de polynômes linéaires sur  $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ , pour une puissance  $q'$  de  $q$ .

*Démonstration.* Soit  $P(F) = c_d F^d + c_{d-1} F^{d-1} + \dots + c_1 F + c_0$ ,  $c_i \in \mathbb{F}_q((t^{\mathbb{Q}}))$  et posons  $c_d = 1$ .

Puisque  $P$  a une unique pente égale à 0 et  $v(c_d) = 0$ , alors les valuations des termes extrêmes sont nécessairement nulles. Donc  $v(c_0) = v(c_d) = 0$  et  $v(c_i) \geq 0$  pour tous les  $1 \leq i \leq d-1$ .

Soit  $a_i \in \mathbb{F}_q$  le coefficient constant de la série  $c_i$ , pour  $1 \leq i \leq d$  et on choisit  $q'$  une puissance de  $q$  telle que le polynôme :

$$z^{p^d} + a_{d-1} z^{p^{d-1}} + \dots + a_1 z^p + a_0 z$$

ait toutes les  $p^d$  racines distinctes dans le corps  $\mathbb{F}_{q'}$ .

Soit  $r \in \mathbb{F}_{q'}$  une telle racine, non nulle. Considérons le polynôme

$$P(F)(z+r) = c_0(z+r) + c_1(z+r)^p + \cdots + c_d(z+r)^{p^d}.$$

Les racines de ce polynôme sont égales aux  $r' - r$ , pour toute  $r'$  racine de  $P(F)(z)$ . Nous allons démontrer que ce polynôme admet une racine dans  $\mathbb{F}_{q'}$  et, par conséquent,  $P(F)(z)$  aura aussi une racine dans  $\mathbb{F}_{q'}$ .

Pour cela, regardons le polygone de Newton de

$$P(F)(z+r) = c_d z^{p^d} + \cdots + c_1 z^p + c_0 z + \underbrace{(c_0 r + c_1 r^p + \cdots + c_d r^{p^d})}_{\text{terme constant}}.$$

On a vu que  $v(c_d) = v(c_0) = 1$  et toutes les autres  $v(c_i) \geq 0$ . Nous remarquons que la valuation du terme constant du polynôme  $P(F)(z+r)$  est strictement positive. En effet :  $v(c_0 r + c_1 r^p + \cdots + c_d r^{p^d}) = v((c_0 - a_0)r + (c_1 - a_1)r^p + \cdots + (c_d - a_d)r^{p^d})$  et la valuation de chaque  $(c_i - a_i)$  est strictement positive, puisqu'il n'existe pas de terme constant et que  $v(c_i) \geq 0$ .

Il est clair alors que le polygone de Newton est constitué de deux axes verticaux :  $x = -d$ ,  $x = 0$ , un segment de droite de pente 0 ( plus précisément le segment dont les extrémités sont les points  $(-d, 0)$  et  $(-1, 0)$ ) et un segment de droite de pente strictement positive (celui dont les extrémités sont les points  $(-1, 0)$  et  $(0, v(\text{terme constant de } P(F)(z+r)))$ ).

Donc le polynôme admet deux pentes, une égale à 0 et une strictement positive, disons égale à un rationnel  $m$  positif. De plus, la multiplicité de  $m$  est égale à 1. D'après le corollaire II.2.1, la factorisation du polynôme  $P(F)(z+r)$  en produit de polynômes de pentes pures contient un seul polynôme linéaire (de degré 1). Alors ce polynôme a une racine dans  $\mathbb{F}_{q'}$  et donc  $P(F)(z)$  aussi.

Si on enlève le facteur linéaire de la factorisation de  $P(F)(z+r)$ , il nous reste un polynôme dont le polygone de Newton contient un seul segment de droite, de pente 0. On peut donc recommencer le même procédé avec ce nouveau polynôme de pente pure égale à 0. On continue alors jusqu'à trouver toutes les autres racines. Ainsi le polynôme  $P(F)(z)$  se factorise complètement sur  $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ .  $\square$

*Démonstration de la proposition II.2.3.* Il s'agit d'une conséquence immédiate de la proposition B.0.4.  $\square$

## Références

- [1] B. Adamczewski & Y. Bugeaud, On the complexity of algebraic numbers I. Expansions in integer bases, *Annals of Math.* 165 (2007), 447–465.
- [2] J.-P. Allouche & J. Shallit, *Automatic Sequences : Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.
- [3] V. Berthé, Fonctions de Carlitz et automates. Entropies conditionnelles, Thèse de l'Université de Bordeaux, 1994.
- [4] H. Cherif, B. de Mathan, Irrationality measures of Carlitz zeta values in characteristic  $p$ , *J. Number Theory* 44 (1993), 260–272
- [5] A. Cobham, On the Hartmanis-Stearns problem for a class of tag machines, *Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory*, Schenectady, New York (1968), 51–60
- [6] G. Damamme et Y. Hellegouarch, Propriétés de transcendance des valeurs de la fonction zêta de Carlitz, *C. R. Acad. Sci. Paris, Série 1* 307 (1988), 635–637
- [7] S. Eilenberg, *Automata, languages, and machines*, Vol. A, Academic Press, 1974
- [8] I. Kaplanasky, Maximal fields with valuations, *Duke Math. J.* 9 (1942), 303–321
- [9] K. Kedlaya, Finite automata and algebraic extensions of function fields, *J. Théor. Nombres Bordeaux* 18 (2006), 379–420.
- [10] F. Pellarin, Aspects de l'indépendance algébrique en caractéristique non nulle. [d'après Anderson, Brownawell, Denis, Papanikolas, Thakur, Yu,...], séminaire Bourbaki 973, mars 2007.
- [11] J.-P. Serre, *Local Fields*, Springer-Verlag, 1979.
- [12] L.J. Wade, Certain quantities transcendental over  $GF(p_n)(x)$ , *Duke Math. J.* 8 (1941), 701–720.
- [13] J. Yu, Transcendence and Special Zeta Values in Characteristic  $p$ , *Annals of Math.* 134 (1991), 1–23.