Le théorème de Christol pour les séries généralisées

Auteur : Lèbre, Florelle
Promoteur(s) : Charlier, Emilie
Faculté : Faculté des Sciences
Diplôme : Master en sciences mathématiques, à finalité didactique
Année académique : 2025-2026
URI/URL : http://hdl.handle.net/2268.2/25512

Faculté des Sciences
Département de Mathématique

Le théorème de Christol pour les séries généralisées

Mémoire de fin d'études présenté en vue de l'obtention du titre de
Master en Sciences Mathématiques, à finalité didactique

Année académique 2025-2026

Auteur :
Florelle LEBRE

Promoteur :
Emilie CHARLIER

Introduction

L'histoire des mathématiques est jalonnée par la découverte de ponts inattendus entre des disciplines que tout semble séparer. Au 19e siècle, Isaac Newton et Victor Puiseux établissent un résultat fondamental : la clôture algébrique du corps des séries formelles $K((t))$ sur un corps de caractéristique nulle est entièrement décrite par les séries de Puiseux (les séries à exposants fractionnaires). Malheureusement, quand on veut poursuivre la réflexion en caractéristique positive, ce théorème s'effondre. Le corps des séries de Puiseux n'est plus algébriquement clos, des équations très simples en apparence n'y trouvent aucune solution, comme le polynôme mis en évidence par Chevalley $y^p - y = t^{-1}$. C'est alors que nait une réflexion inattendue en 1970 avec Gilles Christol. Poussé par les échecs des outils classiques pour décrire les éléments algébriques de $K((t))$ en caractéristique p, Christol se met à chercher une régularité ailleurs. Il commence alors à se questionner sur la nature des coefficients de séries formelles satisfaisant des équations différentielles ou algébriques, notamment à travers l'étude des diagonales de fractions rationnelles et sous l'angle de l'action de Frobenius. En manipulant algébriquement ces séries, Christol se rend compte que le fait d'être algébrique impose une condition de finitude très stricte sur les coefficients. C'est cette structure purement algébrique (un espace vectoriel de dimension finie stable pour certaines opérations) qui s'est avérée, dans un second temps, être exactement la définition d'un objet combinatoire bien connu. Après rencontre avec des spécialistes du sujet (Mendès, Rauzy et Kamae), le lien entre théorie des automates et algébricité se concrétise dans l'article [5] intitulé "Suites algébriques, automates et substitutions" où ils énoncent leur théorème : *Une série formelle est algébrique sur $\mathbb{F}_p(t)$ si et seulement si sa suite de coefficients est p-automatique.* Un nouveau monde s'éclaire alors pour les mathématiciens qui ne s'attendaient pas à trouver une réponse algorithmique à un problème d'algèbre. Une équation algébrique polynomiale peut être d'un degré arbitrairement grand, manipuler des structures hautement non linéaires et abstraites et pourtant, grâce au théorème de Christol, on sait désormais que toute cette complexité se résume à un ensemble fini d'états et de transitions simples (un automate fini déterministe avec sortie). L'infini algébrique est apprivoisé par la finitude de l'automate.
Le théorème de Christol est une avancée majeure dans la caractérisation d'éléments algébriques en caractéristique p, cependant il n'est pas suffisant pour décrire entièrement la clôture algébrique de $\mathbb{F}_q(t)$. Au début des années 2000, Kiran Kedlaya essaie de franchir une nouvelle étape en ce sens en généralisant ce lien combinatoire-algébrique à un corps de séries plus grand que celui des séries de Puiseux, le corps des séries de Laurent généralisées.

Ces séries sont à exposants dans les rationnels et ont leur support bien ordonné. Elles sont d'abord introduites par Hahn en 1908 puis étudiées en terme de valuation par Krull en 1932. Ce mémoire a pour but de présenter cette généralisation en se basant principalement sur deux articles de Kedlaya : "Finite automata and algebraic extensions of function fields" [12] paru en 2006 et "On the algebraicity of generalized power series" [13] publié en 2017.

Pour mener à bien cette étude, nous structurons notre propos en plusieurs étapes. Le premier chapitre met en lumière le contraste fondamental entre la caractéristique nulle et la caractéristique positive. Nous y voyons comment le théorème classique de Newton-Puiseux échoue en caractéristique p face au contre-exemple historique du polynôme de Chevalley. On pose ensuite le cadre formel nécessaire à la fusion de deux mondes. Côté automatique, on introduit les bases de la théorie des langages (alphabets, langages réguliers) et définit précisément les Automates Finis Déterministes avec Sortie (AFDO) qui caractérisent les suites automatiques. Côté algèbre, on met en lumière les polynômes additifs, structures cruciales en caractéristique p liées à l'endomorphisme de Frobenius. Enfin, on énonce le théorème de Christol classique et on pose le cadre de notre généralisation.
Le deuxième chapitre est dédié à la première moitié de notre théorème principal, à savoir le sens "automatique implique algébrique" dans le cadre des séries généralisées. Après avoir étendu les notations et démontré ce sens direct en traduisant les transitions de l'automate en relations polynomiales, nous basculons vers l'étude des propriétés de stabilité des séries p-quasi-automatiques. L'établissement de ces propriétés de stabilité nous fournit les outils nécessaires pour aborder, dans les chapitres suivants, le sens inverse "algébrique implique automatique".
Le troisième chapitre propose une preuve algorithmique et constructive du sens "algébrique implique automatique". Pour extraire un automate fini d'une relation polynomiale, nous déployons une machinerie combinant plusieurs outils classiques des mathématiques. Nous étudions d'abord les polynômes tordus, un outil standard d'algèbre non commutative. Nous introduisons ensuite les polygones de Newton, un outil traditionnel de la théorie des courbes planes et de la géométrie algébrique pour l'étude des singularités. Ils nous permettent ici de factoriser un polynôme en fonction de son polygone de Newton, ce qu'on appellera la factorisation par pente. En couplant ces concepts à la topologie des graphes de transitions (les automates en forme de saguaro), nous formalisons une version algébrique de l'algorithme de Newton. Ce procédé itératif permet de construire pas à pas la solution sous forme de série tout en garantissant la préservation de sa structure automatique à chaque étape.
Le chapitre final couronne le travail en exploitant l'ensemble des outils développés pour caractériser la structure de la clôture algébrique de $\mathbb{F}_q(t)$. En faisant intervenir des théorèmes profonds de l'algèbre locale comme le lemme de Krasner pour les corps valués complets et des arguments de séparabilité, l'étude de la clôture algébrique de $\mathbb{F}_q(t)$ vient conclure la démonstration de notre théorème généralisé.

Ce mémoire vise ainsi à offrir une vision synthétique et rigoureuse d'un domaine où la simplicité des automates rencontre la richesse des structures algébriques.

Table des matières

Chapitre 1

Motivation et théorème de Christol

L'objectif de ce premier chapitre est de poser les bases nécessaires pour la suite de notre étude. Le but de ce mémoire est de lier deux domaines qui semblent différents : l'algèbre en caractéristique positive et la théorie des langages et des automates.
Pour comprendre comment ces deux univers se rencontrent, nous allons procéder par étapes. Nous commençons par rappeler les notions algébriques de base pour voir pourquoi les outils classiques ne fonctionnent plus en caractéristique positive. C'est cet échec qui justifie l'introduction des automates et des langages pour chercher une régularité dans les coefficients des séries. Ensuite, la réunion de ces deux aspects se fera à travers le théorème de Christol classique. La démarche et les méthodes de preuve de ce théorème nous serviront de modèle pour la généralisation aux séries de Laurent généralisées que nous développerons dans ce travail.

1.1 Extension de champ et éléments algébriques

Cette section est consacrée aux rappels des définitions et propriétés fondamentales liées aux extensions de corps et à l'algébricité. Les démonstrations de ces résultats classiques sont omises et peuvent être consultées dans l'ouvrage [12].

Définition 1.1. Soient K et L des champs tels que $K \subseteq L$. Alors, $\alpha \in L$ est dit algébrique sur K s'il existe un polynôme non nul $P(t) \in K[t]$ tel que $P(\alpha) = 0$.

On dit que L est algébrique sur K si tout élément de L est algébrique sur K.

Lemme 1.2. *Soient K et L deux corps tels que $K \subseteq L$. Alors $\alpha \in L$ est algébrique sur K si et seulement s'il appartient à une sous-extension M de L (avec $K \subseteq M$) qui est de dimension finie en tant que K-espace vectoriel. La plus petite extension de K contenant α est notée $K(\alpha)$.*

Corollaire 1.3. *Soient K et L des champs tels que $K \subseteq L$. Si $[L : K] = \dim_K L$ est fini, alors L est algébrique sur K.*

Lemme 1.4. *Soient K et L des champs tels que $K \subseteq L$. Si $\alpha, \beta \in L$ sont algébriques sur K, alors $\alpha + \beta$, $\alpha\beta$ et si $\alpha \neq 0$, $\frac{1}{\alpha}$ sont aussi algébriques sur K.*

Définition 1.5. Un champ K est algébriquement clos si tout polynôme sur K se factorise complètement dans K.

Définition 1.6. Une clôture algébrique d'un champ K est une extension de champ L de K telle que L est algébriquement clos et minimal pour cette propriété.

Proposition 1.7. *Soit L une extension d'un champ K. L'ensemble des éléments de L algébriques sur K forme un sous-anneau de L.*

Définition 1.8. Soit K un champ de caractéristique $p > 0$. L'endomorphisme de Frobenius est $\sigma : K \to K$ $\alpha \mapsto \alpha^p$.

On termine la section en introduisant les notations d'usage. On note :

- $K[t]$ l'anneau commutatif des polynômes à coefficients dans K.
- $K[[t]]$ l'anneau commutatif des séries formelles à coefficients dans K.
- $K(t)$ le champ des fractions rationnelles de l'anneau $K[t]$.
- $K((t))$ l'ensemble des séries de Laurent (les séries où on autorise un nombre fini de degrés négatifs). On peut également le voir comme le champ des fractions de l'anneau $K[[t]]$.

1.2 Séries de Puiseux et polynôme de Chevalley

L'étude de la clôture algébrique de $K((t))$ sur un corps K de caractéristique nulle a donné lieu à un nouveau corps de séries : le corps de séries de Puiseux. Nous en donnons un aperçu, inspiré de [2] section 2.6.

Définition 1.9. Une série de Puiseux en t avec ses coefficients dans K est une série de la forme $x = \sum_{i \geq k} x_i t^{\frac{i}{n}}$ où $k \in \mathbb{Z}$, $x_i \in K$ et n est un entier strictement positif.

Deux séries de Puiseux $x_1 = \sum_{i \geq k} x_i t^{\frac{i}{n_1}}$ et $x_2 = \sum_{i \geq k} x_i t^{\frac{i}{n_2}}$ peuvent toujours être écrites comme des séries de Laurent en $t^{\frac{1}{n}}$ où n est le plus petit commun multiple de n_1 et n_2. Il est alors clair de comment additionner et multiplier des séries de Puiseux.

Exemple 1.10. Soient $x_1 = t^{\frac{1}{2}}$ et $x_2 = t^{\frac{2}{3}} - t^{\frac{1}{3}}$. Alors la somme des deux est $x_1 + x_2 = t^{\frac{1}{2}} + t^{\frac{2}{3}} - t^{\frac{1}{3}}$ et le produit est

$$x_1 x_2 = t^{\frac{3}{6}}(t^{\frac{4}{6}} - t^{\frac{2}{6}}) = t^{\frac{3}{6}+\frac{4}{6}} - t^{\frac{3}{6}+\frac{2}{6}} = t^{\frac{7}{6}} - t^{\frac{5}{6}}.$$

Définition 1.11. Le corps de toutes les séries de Puiseux est noté $K((t^{\frac{1}{\infty}})) = \cup_{n>0} K((t^{\frac{1}{n}}))$.

Définition 1.12. Si $x = x_1 t^{n_1} + x_2 t^{n_2} + \cdots \in K((t^{\frac{1}{\infty}}))$ avec $x_1 \neq 0$, $n_1 < n_2 < \ldots$ alors la valuation de x, noté $v(x)$ est n_1 et le coefficient initial de x, noté $\mathrm{In}(x)$ est x_1. Par convention, la valuation de 0 est ∞. Cette application de $K((t^{\frac{1}{\infty}}))$ dans $\mathbb{Q} \cup \{\infty\}$ satisfait $v(xy) = v(x) + v(y)$ et $v(x + y) \geq \min(v(x), v(y))$.

Le théorème suivant est dû à Puiseux mais souvent appelé le théorème de Newton-Puiseux, à retrouver par exemple dans [18].

Théorème 1.13. *Pour K un champ de caractéristique 0, la clôture algébrique de $K((t))$ est isomorphe à $K((t^{\frac{1}{\infty}}))$.*

Malheureusement, ce théorème n'est plus vrai en caractéristique positive comme l'a fait remarquer Chevalley, dont la preuve a été exposée dans [8].

Proposition 1.14. *Soit q une puissance d'un nombre premier p. Le polynôme $z^p - z - t^{-1} \in \mathbb{F}_q(t)[z]$ n'a pas de racines dans $\mathbb{F}_{q'}((t^{\frac{1}{n}}))$ pour toute puissance q' de q et tout entier strictement positif n.*

Démonstration. Procédons par l'absurde et supposons que $z = \sum_i z_i t^i \in \mathbb{F}_{q'}((t^{\frac{1}{n}}))$ est racine de ce polynôme. Alors, on a $z^p = \sum_i z_i^p t^{ip} = \sum_i z_{\frac{i}{p}}^p t^i$ et en injectant ces deux informations dans notre polynôme, on obtient $t^{-1} = \sum_i (z_{\frac{i}{p}}^p - z_i) t^i$. Comme z est une série de Laurent non nulle en $t^{\frac{1}{n}}$ pour un certain n strictement positif, il doit y avoir un plus petit indice i pour lequel $z_i \neq 0$. Si $i < \frac{-1}{p}$, alors $0 = z_i^p - z_{pi}$ et donc $z_{pi} \neq 0$, ce qui contredit la minimalité de i car dans ce cas $pi < i$. On obtient alors $z_{-1} = 0$, ce qui force $1 = z_{\frac{-1}{p}} = z_{\frac{-1}{p^2}} = \cdots$ et contredit le fait que $z \in \mathbb{F}_{q'}((t^{\frac{1}{n}}))$ pour un certain n. □

1.3 Notions de base de théorie des langages

Afin d'introduire le volet combinatoire du théorème de Christol, cette section formalise les outils élémentaires de la théorie des langages et des automates finis, supposés connus.

Soit Σ un ensemble fini qu'on appelle alphabet. Soit Σ^* l'ensemble des mots finis sur Σ. Un langage sur Σ est un sous-ensemble L de Σ^*. Pour des mots x et y, on note xy leur concaténation.

Un automate fini déterministe est un 5-uplet $M = (Q, \Sigma, \delta, q_0, F)$ où Q est un ensemble fini d'états, δ est la fonction de transition, q_0 l'unique état initial et F est un ensemble fini d'états finaux. Tout langage accepté par un automate fini est appelé régulier. C'est équivalent au fait de demander que le langage soit décrit par une expression régulière. Les langages réguliers sont stables par concaténation, union, complémentaire, miroir et intersection.

Soit L un langage sur Σ. On définit une relation d'équivalence sur Σ^* par $x \sim y$ si et seulement si pour tout $z \in \Sigma^*$, $xz \in L$ si et seulement si $yz \in L$.

Théorème 1.15 (Myhill-Nérode)**.** *Un langage L est régulier si et seulement si Σ^* admet un nombre fini de classes d'équivalence pour la relation $\sim$.*

1.4 Automates et fonctions automatiques

On introduit les fonctions automatiques. Pour ce faire, on définit ce qu'est un automate fini déterministe avec sortie.

Définition 1.16. Un automate fini déterministe avec sortie (AFDO) est un 6-uplet $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ où

- Q est un ensemble fini dont les éléments sont appelés les états,
- Σ est un ensemble fini, appelé l'alphabet et dont les éléments sont des lettres,
- δ est une fonction de $Q \times \Sigma$ dans Q, appelée fonction de transition,
- $q_0 \in Q$ est un état, appelé l'état initial,
- Δ est un ensemble, appelé l'alphabet de sortie,
- τ est une fonction de Q dans Δ, appelée fonction de sortie.

La fonction δ s'étend en une fonction $\delta^* : Q \times \Sigma^* \to Q$ par les règles

$$\delta^*(q, \varepsilon) = q$$

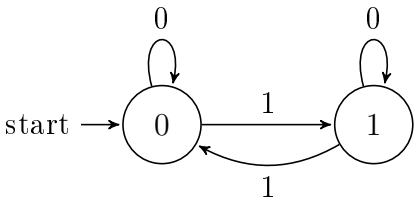
$$\delta^*(q, wa) = \delta(\delta^*(q, w), a)$$

pour tous $q \in Q, w \in \Sigma^*, a \in \Sigma$.

On obtient une fonction $f_M : \Sigma^* \to \Delta$ en posant $f_M(w) = \tau(\delta^*(q_0, w))$.

Définition 1.17. Soit Δ un ensemble fini. Une fonction $f : \mathbb{N} \to \Delta$ est b-automatique s'il existe un AFDO $M = (Q, \Sigma_b, \delta, q_0, \Delta, \tau)$ tel que $f(\mathrm{val}_b(w)) = f_M(w)$ pour tout $w \in \Sigma_b^*$, où $\Sigma_b = \{0, \ldots, b-1\}$ et $\mathrm{val}_b : \Sigma_b^* \to \mathbb{N}$ $w_n \ldots w_0 \mapsto \sum_{i=0}^{n} w_i b^i$.

Exemple 1.18. La suite de Thue-Morse définie par $f_n = s_2(n) \bmod 2$ pour tout $n \geq 0$ où s_2 représente la fonction "somme des chiffres en base 2", est 2-automatique. En effet, l'AFDO suivant la génère :



1.5 Polynômes additifs

Les polynômes additifs sont un outil de base en caractéristique p, directement lié à l'endomorphisme de Frobenius.

Définition 1.19. Si K est un champ de caractéristique $p > 0$, les polynômes additifs sont les polynômes de $K[t]$ de la forme $\sum_{i=0}^{n} c_i t^{p^i}$.

De tels polynômes ont le nom d'additif par la proposition suivante.

Proposition 1.20. *Soit $P(t)$ un polynôme non nul sur un champ K de caractéristique $p > 0$ et soit L la clôture algébrique de K. Les assertions suivantes sont équivalentes :*

a) Le polynôme $P(t)$ est additif.

b) L'équation $P(t+z) = P(t)+P(z)$ est valable comme identité formelle de polynômes.

c) Les zéros de P dans L forment un $\mathbb{F}_p$-vectoriel pour l'addition, tout zéro ayant la même multiplicité qui est une puissance de p.

L'étude des polynômes additifs est suffisante en caractéristique p pour caractériser les éléments algébriques par le lemme suivant.

Lemme 1.21. *Pour K et L des champs de caractéristique $p > 0$ tels que $K \subseteq L$ et $\alpha \in L$, α est algébrique sur K si et seulement si c'est un zéro d'un polynôme additif sur K.*

Démonstration. La condition est suffisante : il est évident que si α est zéro d'un polynôme additif sur K, alors α est algébrique sur K. La condition est nécessaire : si α est algébrique sur K, alors $\alpha, \alpha^p, \ldots$ ne peuvent pas tous être linéairement indépendants. Il doit alors exister une relation de la forme $c_0\alpha + c_1\alpha^p + \ldots + c_n\alpha^{p^n} = 0$ avec $c_0, \ldots, c_n \in K$ non tous nuls. Ce qui montre que α est zéro d'un polynôme additif, ce qui conclut la preuve. □

Définition 1.22. L'endomorphisme de Frobenius s'étend aux vecteurs de la façon suivante :

Soit v un vecteur de dimension n.

$$\sigma(v) = \begin{pmatrix} v_0^p \\ \vdots \\ v_{n-1}^p \end{pmatrix}$$

Le lemme suivant provient de [12] et est retranscrit dans [16]. Il nous sera très utile dans la suite pour traduire des systèmes d'équations polynomiales en systèmes matriciels et déduire l'algébricité de certaines composantes.

Lemme 1.23. *Soient K et L des champs de caractéristique $p > 0$ tels que $K \subseteq L$. Soient A et B des matrices carrées de dimension n à coefficients dans K avec au moins une des deux inversible et soit $w \in K^n$ un vecteur colonne. Supposons que $v \in L^n$ est un vecteur colonne tel que $A\sigma(v) + Bv = w$, où σ est l'endomorphisme de Frobenius. Alors, les éléments de v sont algébriques sur K.*

Démonstration. Supposons tout d'abord que A est inversible. Alors, on peut multiplier l'équation à gauche par A^{-1} et écrire notre relation sous la forme $\sigma(v) = -A^{-1}Bv + A^{-1}w$. En posant $U_1 = -A^{-1}B$ et $w_1 = A^{-1}w$, on peut généraliser notre équation sous la forme :

$$\sigma^i(v) = U_i v + w_i,$$

pour une matrice carrée U_i de dimension n sur K et $w_i \in K^n$, par stabilité de K sous l'action de l'endomorphisme de Frobenius. De tels vecteurs $\sigma^i(v)$ appartiennent tous au K-espace vectoriel $E = \{Cv + x \mid C \in M_n(K), x \in K^n\}$. Ce sous-espace $E \subset L^n$ est engendré sur K par les n vecteurs canoniques e_i et les n composantes de v via C. Ainsi,

la dimension de E sur K est au plus n^2+n, de dimension finie. Alors, pour un certain m plus grand que n^2+n, les vecteurs $v, \sigma(v), \sigma^2(v), \ldots$ sont linéairement dépendants sur K et on peut trouver $c_0, \ldots, c_m$ non tous nuls tels que

$$c_0 v + c_1\sigma(v) + \ldots + c_m\sigma^m(v) = 0$$

Chaque composante de v vérifiant une équation de ce type, en appliquant le lemme 1.21, on en déduit qu'elles sont algébriques sur K.

Supposons maintenant que B est inversible, alors on peut écrire notre équation sous la forme $B^{-1}A\sigma(v) + v = B^{-1}w$ c'est-à-dire, en isolant v, $v = -B^{-1}A\sigma(v) + B^{-1}w$. Par substitutions successives, on constate que, comme dans le cas où A était inversible (en inversant le sens des indices), pour un entier $m \geq 1$ fixé, les vecteurs $\sigma(v), \sigma^2(v), \ldots, \sigma^m(v)$ se trouvent tous dans un K-espace vectoriel de dimension au plus n^2+n. Alors, pour un certain m strictement supérieur à n^2+n, la famille $(\sigma(v), \ldots, \sigma^m(v))$ est linéairement dépendante sur K. On peut donc trouver des scalaires $c_1, \ldots, c_m \in K$ non tous nuls tels que

$$c_1\sigma(v) + \cdots + c_m\sigma^m(v) = 0$$

Chaque composante de v vérifiant une équation de ce type, en appliquant le lemme 1.21, on en déduit qu'elles sont algébriques sur K. □

1.6 Théorème de Christol

Nous sommes maintenant en mesure de présenter le théorème de Christol.

On considère $\mathbb{F}_q$ le champ à q éléments avec q une puissance d'un nombre premier p. En particulier, tout élément $x \in \mathbb{F}_q$ satisfait $x^q - x = 0$ et $\mathbb{F}_q$ est l'ensemble des racines de cette équation.

A chaque suite $u : \mathbb{N} \to \mathbb{F}_q$, on associe une série formelle $u(t) = \sum_{n\geq 0} u_n t^n$, où u_n est le n-ième terme de la suite u.

Le théorème de Christol est le suivant :

Théorème 1.24 (Christol)**.** *Une suite $u : \mathbb{N} \to \mathbb{F}_q$ est p-automatique si et seulement si la série formelle $u(t)$ est algébrique sur $\mathbb{F}_q(t)$.*

Exemple 1.25. Reprenons la suite f_n de Thue-Morse définie à l'exemple 1.18. Alors la série $\sum_{n=0}^{+\infty} f_n t^n \in \mathbb{F}_2[[t]]$ est 2-automatique donc algébrique par le théorème de Christol. En effet, on peut vérifier que f annule le polynôme $(1+t^3)z^2 + (1+t)^2 z + t = 0$.

Il existe plusieurs preuves de ce théorème. Pour but didactique, nous choisissons d'en montrer une du sens automatique implique algébrique qui utilise une méthode qu'on adaptera plus tard dans notre généralisation.

Ce qui suit provient des articles [5] et [4] de Christol.

Définition 1.26. Une partie $X \subset \mathbb{N}$ est p-reconnaissable si le langage $\{0^*\mathrm{rep}_p(x) : x \in X\}$ est régulier, c'est-à-dire accepté par un automate fini.

Le résultat suivant ainsi que sa démonstration est une version adaptée de [7].

Lemme 1.27. *Soit q une puissance d'un nombre premier p et soit $\mathbb{F}_q$ le corps à q éléments. Soit A un ensemble d'entiers positifs ou nuls p-reconnaissable, alors la série $f(t) = \sum_{n\in A} t^n$ de $\mathbb{F}_q[[t]]$ est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. L'ensemble A est p-reconnaissable, donc il existe un AFDO $M = (Q, \Sigma_p, \delta, q_0, \{0,1\}, \tau)$ qui accepte les représentations en base p des éléments de A (sort 1 si l'élément est dans A et 0 sinon). Pour chaque état $q_i \in Q$ avec $i \in \{0, \dots, r\}$, on définit la série

$$F_{q_i}(t) = \sum_{\substack{n\geq 0 \\ \delta^*(q_0, \mathrm{rep}_p(n)) = q_i}} t^n.$$

Montrons que F_{q_i} est algébrique sur $\mathbb{F}_q(t)$ pour tout $q_i \in Q$. En particulier, on aura $f = \sum_{\substack{q_i \in Q \\ \tau(q_i)=1}} F_{q_i}(t)$ algébrique sur $\mathbb{F}_q(t)$ par somme de séries algébriques.
On utilise la relation fondamentale $n = pm + j$ avec $j \in \{0, \dots, p-1\}$. On a alors $t^{pm+j} = (t^m)^p t^j$. La série devient

$$\begin{aligned}
F_{q_i}(t) &= \sum_{\substack{n\geq 0 \\ \delta^*(q_0, \mathrm{rep}_p(n)) = q_i}} t^n = \sum_{j=0}^{p-1} t^j \sum_{\substack{m\geq 0 \\ \delta^*(q_0, \mathrm{rep}_p(m)j) = q_i}} t^{pm} \\
&= \sum_{j=0}^{p-1} t^j \sum_{\substack{q'\in Q \\ \delta(q',j)=q_i}} \sum_{\substack{m\geq 0 \\ \delta^*(q_0,\mathrm{rep}_p(m))=q'}} t^{pm} = \sum_{j=0}^{p-1} t^j \sum_{\substack{q'\in Q \\ \delta(q',j)=q_i}} \left(\sum_{\substack{m\geq 0 \\ \delta^*(q_0,\mathrm{rep}_p(m))=q'}} t^m \right)^p \\
&= \sum_{\substack{q'\in Q \\ j\in\{0,\dots,p-1\} \\ \delta(q',j)=q_i}} t^j \left(F_{q'}(t)\right)^p
\end{aligned}$$

Alors, les $F_{q_i}(t)$ s'expriment en fonction de puissances p-ièmes de $F_{q'}(t)$. En posant

$$v = \begin{pmatrix} F_{q_0} \\ \vdots \\ F_{q_r} \end{pmatrix}, \quad \sigma(v) = \begin{pmatrix} F^p_{q_0} \\ \vdots \\ F^p_{q_r} \end{pmatrix}$$

et A une matrice carrée à coefficients dans $\mathbb{F}_q(t)$ telle que $a_{ij} = \sum_{\substack{l\in\{0,\dots,p-1\} \\ \delta(q_j,l)=q_i}} t^l$. Alors, notre équation s'écrit sous la forme matricielle $A\sigma(v) - v = 0$ et correspond aux hypothèses du lemme 1.23 avec $B = -Id$, $w = 0$. On en déduit que les éléments de v sont algébriques sur $\mathbb{F}_q(t)$. C'est-à-dire que $F_{q_i}(t)$ est algébrique sur $\mathbb{F}_q(t)$ pour tout $q_i \in Q$ et donc f est également algébrique sur $\mathbb{F}_q(t)$. □

Théorème 1.28. *Si une suite $u : \mathbb{N} \to \mathbb{F}_q$ est p-automatique alors la série formelle $u(t)$ est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. Pour tout $x \in \mathbb{F}_q$, on pose $A_x = \{n \geq 0 : u_n = x\}$, alors A_x est p-reconnaissable. Par le lemme, on a $f_x(t) = \sum_{n \in A_x} t^n$ est algébrique sur $\mathbb{F}_q(t)$. De plus, on a

$$u(t) = \sum_{n \geq 0} u_n t^n = \sum_{n \geq 0} \sum_{x \in \mathbb{F}_q} x \chi_{A_x}(n) t^n = \sum_{x \in \mathbb{F}_q} x f_x(t)$$

Donc $u(t)$ est algébrique en tant que combinaison linéaire de séries algébriques. □

On obtient des reformulations du théorème de Christol.

Théorème 1.29. *Un élément $\sum_{n=o}^{\infty} u_n t^n$ de $\mathbb{F}_q[[t]]$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si pour tout $c \in \mathbb{F}_q$, l'ensemble des représentations en base p des entiers n tels que $x_n = c$ est généré par un automate fini.*

Définition 1.30. Une série formelle $\sum_{n=0}^{\infty} u_n t^n \in \mathbb{F}_q[[t]]$ est p-automatique si la suite de ses coefficients $(u_n)_{n \geq 0}$ est une suite p-automatique à valeur dans $\mathbb{F}_q$.

Théorème 1.31. *Une série $\sum_{n=0}^{\infty} u_n t^n$ de $\mathbb{F}_q[[t]]$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si elle est p-automatique.*

1.7 Représentations valides en base b

L'objectif de ce travail est de généraliser le théorème de Christol classique que nous venons d'énoncer. Comme nous l'avons mis en évidence avec le contre-exemple du polynôme de Chevalley, le corps des séries de Puiseux s'avère insuffisant pour décrire entièrement la clôture algébrique de $K(t)$ en caractéristique positive. Pour franchir cette étape, nous devons aller plus loin en considérant des séries dotées d'exposants rationnels. Ce faisant, il devient indispensable d'étendre aux nombres rationnels les notions combinatoires qui interviennent dans le théorème de Christol, notamment en ce qui concerne la représentation en base.
Soient $b > 1$ un entier positif et $\Sigma = \Sigma_b = \{0, 1, \ldots, b-1, ", "\}$. On étend la notion de représentation en base aux nombres rationnels. Pour ce faire, on doit imposer une condition pour que les représentations soient cohérentes, notamment par rapport à la présence d'une virgule.

Définition 1.32. Un mot $s = s_1 s_2 \ldots s_n \in \Sigma^*$ est une représentation valide en base b si $s_1 \neq 0, s_n \neq 0$ et exactement un des $s_1, \ldots, s_n$ est égal à la virgule. Si s est une représentation valide en base b et si s_k est la virgule, alors on définit la valeur de s comme

$$\mathrm{val}_b(s) = \sum_{i=1}^{k-1} s_i b^{k-1-i} + \sum_{i=k+1}^{n} s_i b^{k-i}.$$

Il est évident que deux mots valides n'ont pas la même valeur. On peut donc définir sans ambiguïté s comme étant la représentation en base b de $\mathrm{val}_b(s)$.

Les automates finis ne pouvant traiter que des mots finis, nous restreignons notre étude aux rationnels possédant un développement fini (les rationnels b-adiques).

Définition 1.33. Soit S_b l'ensemble des rationnels b-adiques positifs ou nuls. C'est-à-dire les nombres de la forme $\frac{m}{b^n}$ pour des entiers m, n positifs ou nuls, ou encore les nombres rationnels positifs ou nuls qui ont un nombre fini de chiffres après la virgule lorsqu'ils sont écrits en base b.

Il est clair que l'ensemble des valeurs des représentations valides en base b est précisément S_b. Pour un élément $i \in S_b$, on note $\mathrm{rep}_b(i)$ sa représentation en base b.

Lemme 1.34. *L'ensemble des représentations valides en base b est un langage régulier.*

Exemple 1.35. Pour $b = 3$, on a $\Sigma_b = \{0, 1, 2, ", "\}$. Les représentations valides en base 3 doivent avoir les caractéristiques suivantes : elles commencent par 1, 2 ou ",", n'ont qu'une seule virgule et finissent par 1, 2 ou ",". L'automate qui accepte les représentations valides en base 3 est représenté à la figure 1.1.

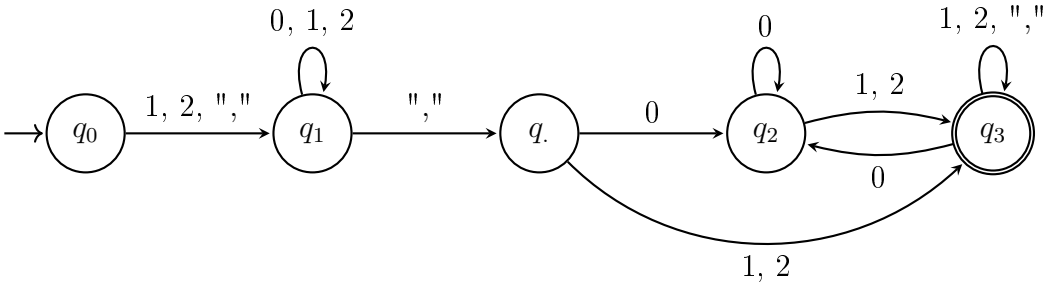


FIGURE 1.1 – Automate acceptant les représentations valides en base 3.

Définition 1.36. Soit M un AFD avec Σ_b comme alphabet. On dit qu'un état $q \in Q$ est pré-virgule (*resp.* post-virgule) s'il existe une représentation valide en base b $s = s_1 \dots s_n$, avec s_k qui est la virgule telle que si on pose $q_i = \delta(q_{i-1}, s_i)$, alors $q = q_i$ pour un $i < k$ (*resp.* $i \geq k$). Remarquons que si M accepte uniquement les représentations valides en base b, alors aucun état ne peut être pré-virgule et post-virgule.

1.8 Fonctions p-automatiques et ensembles p-reconnaissables

Comme pour la représentation en base, nous devons adapter la définition vue précédemment à notre ensemble d'intérêt.

Définition 1.37. Soit Δ un ensemble fini. Une fonction $f : S_p \to \Delta$ est p-automatique s'il existe un AFDO $M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$ tel que pour tout $i \in S_p$, $f(i) = f_M(\mathrm{rep}_p(i))$.

Exemple 1.38. On peut étendre la suite de Thue-Morse vue à l'exemple 1.18 aux représentations valides. Il nous suffit de considérer la fonction $f_{TM} : S_2 \to \{0,1\}$ $i \mapsto s_2(i) \mod 2$.

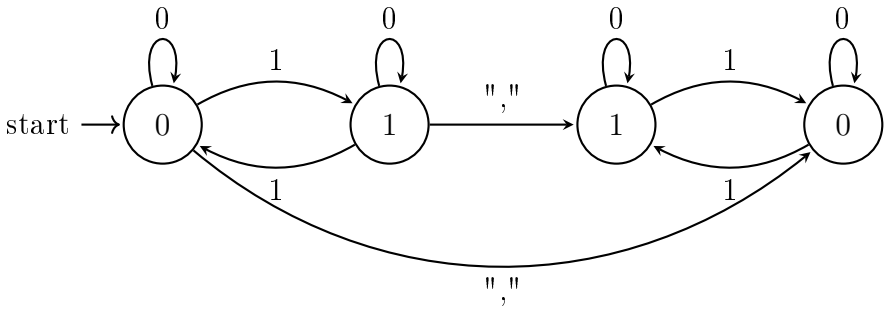


FIGURE 1.2 – AFDO acceptant f_{TM}

Définition 1.39. Un sous-ensemble S de S_p est p-reconnaissable si sa fonction caractéristique $\chi_S(s) = \left\{ \begin{smallmatrix} 1 \text{ si } s \in S \\ 0 \text{ sinon} \end{smallmatrix} \right.$ est p-automatique.

Exemple 1.40. L'ensemble S des nombres 2-adiques dont la représentation valide contient un nombre pair de 1 est 2-reconnaissable. En effet, sa fonction caractéristique est exactement la fonction f_{TM} de notre exemple précédent qui est 2-automatique.

1.9 Séries généralisées

Afin de réussir à généraliser le théorème de Christol, on s'intéresse à un corps plus large que celui des séries de Puiseux. Les séries qu'on considère sont appelées les séries généralisées.

Définition 1.41. Un ensemble bien ordonné est un ensemble muni d'une relation d'ordre tel que tous ses sous-ensembles non vides possèdent un plus petit élément pour cette relation d'ordre.

Proposition 1.42. *Tout sous-ensemble d'un ensemble bien ordonné est bien ordonné. Si E et F sont des ensembles bien ordonnés alors $E \cup F$, $E \cap F$ et $E+F = \{e+f : e \in E, f \in F\}$ sont bien ordonnés.*

Démonstration. Toutes ces propriétés sont des conséquences de l'interdiction de suites décroissantes infinies. Prouvons-le pour l'union.
On procède par l'absurde et on suppose qu'il existe une suite infinie strictement décroissante d'éléments de $E \cup F$, $x_0 > x_1 > \cdots$. Alors, par définition de l'union, chaque x_i est soit dans E soit dans F et comme la suite est infinie, au moins l'un des deux ensembles contient

une infinité de termes de la suite. Supposons sans perte de généralité que c'est E. On peut extraire une sous-suite $(x_{n_k})_{k\geq 0}$ uniquement composée d'éléments de E. Cette sous-suite reste strictement décroissante, ce qui contredit le bon ordre de E. □

Définition 1.43. Soient R un anneau arbitraire et G un groupe abélien, en notation additive, totalement ordonné. Etant donné une fonction $f : G \to R$, le support de f est l'ensemble des $g \in G$ tels que $f(g) \neq 0$.

Définition 1.44. Une série de Laurent généralisée sur R avec les exposants dans G est une fonction $f : G \to R$ dont le support est bien ordonné. Si le support est inclus dans $\{g \in G : g > 0, 0 \text{ est l'élément neutre de } G\} \cup \{0\}$, on appelle f une série généralisée.

On représente la série de Laurent généralisée f par $\sum_{g\in G} f(g)t^g$ et on note $R[[t^G]]$ et $R((t^G))$ les ensembles des séries généralisées et séries de Laurent généralisées sur R avec les exposants dans G.

Proposition 1.45. *On a les inclusions de corps suivantes*

$$K(t) \subset K((t)) \subset K((t^{\frac{1}{\infty}})) = \cup_{n>0} K((t^{\frac{1}{n}})) \subset K((t^{\mathbb{Q}}))$$

Remarque 1.46. Dans le cas qui nous intéresse, on travaille avec des fonctions $f : \mathbb{Q} \to \mathbb{F}_q$ et le champ des séries de Laurent généralisées qu'on considère est donc $\mathbb{F}_q((t^{\mathbb{Q}}))$.

Définition 1.47. La somme sur $R[[t^G]]$ et $R((t^G))$ se fait terme à terme tandis que le produit est défini, pour $f, h \in R[[t^G]]$ ou $R((t^G))$, par

$$fh(t) = \sum_{g\in G} \left(\sum_{\substack{s,u\in G \\ s+u=g}} f(s)h(u) \right) t^g.$$

Les éléments neutres de l'addition et de la multiplication sont respectivement les séries $0t^0$ et $1t^0$.

La condition du support bien ordonné nous permet d'avoir la somme et le produit bien définis sur $R[[t^G]]$ et $R((t^G))$, ce qui leur confère une structure d'anneaux. En effet, si S_1, S_2 sont des sous-ensembles bien ordonnés de G, alors pour tout $g \in G$, le nombre de 2-uplets $(s_1, s_2) \in S_1 \times S_2$ tels que $s_1 + s_2 = g$ est fini. Procédons par l'absurde et supposons qu'on en a une infinité, alors pour chaque s_i il y a une infinité de possibilités, toutes plus petites ou égales à g. Ce qui forme une suite infinie décroissante dans S_i, qui est bien ordonné. On a donc une contradiction. Enfin, le support du produit est inclus dans la somme des supports des séries de base qui est bien ordonné par stabilité des ensembles bien ordonnés.

De plus, cet ensemble est même un corps. Tout élément non nul peut être écrit $at^m(1-f)$ où $a \in R$, $m \in G$ et $f \in R((t^G))$ avec $f_0 = 0$. Alors, la série $\sum_{n=0}^{+\infty} f^n$ est bien définie et décrit l'inverse de $1 - f$.

Définition 1.48. Si $f = \sum_i f(i)t^i$ et $h = \sum_i h(i)t^i$ sont deux séries de Laurent généralisées, le produit terme à terme de ces séries $f \odot h = \sum_i f(i)h(i)t^i$ est également une série de Laurent généralisée appelée le produit d'Hadamard de f et h.

Définition 1.49. Soit $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$. On définit la racine p-ième, notée $x^{\frac{1}{p}}$, comme l'unique série y telle que $y^p = x$. Si $x = \sum_i x_i t^i$, alors sa racine p-ième est définie par $x^{\frac{1}{p}} = \sum_i x_i^{\frac{1}{p}} t^{\frac{i}{p}}$ où $x_i^{\frac{1}{p}}$ est l'unique racine p-ième de x_i dans $\mathbb{F}_q$.

Cette définition est valide. En effet, les coefficients sont bien dans $\mathbb{F}_q$ car $\mathbb{F}_q$ est un corps parfait donc tous ses éléments possèdent une unique racine p-ième et les exposants sont toujours dans $\mathbb{Q}$. De plus, le bon ordre du support est conservé car l'application $i \mapsto \frac{i}{p}$ est une bijection strictement croissante de $\mathbb{Q}$ dans $\mathbb{Q}$.

Le théorème suivant est démontré dans [14].

Théorème 1.50. *Si K est un champ algébriquement clos, alors $K((t^{\mathbb{Q}}))$ est aussi un champ algébriquement clos. En particulier, $\mathbb{F}_q((t^{\mathbb{Q}}))$ est un champ algébriquement clos.*

On termine la section en définissant la valuation sur $\mathbb{F}_q((t^{\mathbb{Q}}))$. L'introduction d'une valuation permet de munir le corps $\mathbb{F}_q((t^{\mathbb{Q}}))$ d'une structure ultramétrique, outil indispensable pour aborder les questions de convergence et de clôture algébrique que nous traiterons ultérieurement.

Définition 1.51. Soit A un anneau commutatif non nul. On appelle valuation de A une application de A vers un groupe abélien totalement ordonné $(G, +, <) \cup \{\infty\}$ vérifiant les propriétés suivantes :

1. Pour tout $x \in A$, $v(x) = \infty \Leftrightarrow x = 0$;
2. Pour tous $x, y \in A$, $v(xy) = v(x) + v(y)$;
3. Pour tous $x, y \in A$, $v(x + y) \geq \min(v(x), v(y))$.

La valuation est dite discrète si le groupe G est $\mathbb{Z}$.

Proposition 1.52. *Si v est une valuation sur A, on a les propriétés suivantes :*

1. *$v(1) = v(-1) = 0$;*
2. *Pour tout $x \in A$, $v(x) = v(-x)$;*
3. *Pour tous $x, y \in A$, $v(x + y) = \min(v(x), v(y))$ si $v(x) \neq v(y)$.*

Démonstration.

1. On a $v(x) = v(1x) = v(1) + v(x)$ d'où $v(1) = 0$. En utilisant la même logique, on a $v(1) = v((-1)(-1)) = v(-1) + v(-1)$ et comme $v(1) = 0$, on a aussi $v(-1) = 0$.
2. On le déduit du point 1 : $v(-x) = v((-1)x) = v(-1) + v(x) = v(x)$.
3. Supposons que $v(x) < v(y)$, alors $v(x + y) \geq v(x)$ par définition. De plus, on a $v(x) = v(x + y - y) \geq \min(v(x + y), v(y))$ ce qui implique $v(x) \geq v(x + y)$ car sinon cela contredirait l'hypothèse $v(x) < v(y)$. En combinant nos deux inégalités, on obtient $v(x + y) = v(x)$.

□

Définition 1.53. De la même manière que pour les séries de Puiseux, pour $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ non nul, on définit la valuation par $v(x)$ qui désigne le plus petit élément du support de x. On pose aussi $v(0) = +\infty$.

Définition 1.54. Cette valuation définit une distance sur $\mathbb{F}_q((t^{\mathbb{Q}}))$ de la manière suivante :

$$d(x,y) = 2^{-v(x-y)} \quad \forall x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$$

Proposition 1.55. *La distance définie sur $\mathbb{F}_q((t^{\mathbb{Q}}))$ est une distance ultramétrique.*

Démonstration. On vérifie seulement l'inégalité ultramétrique, les propriétés de base des distances étant évidentes par définition. Soient $x, y, z \in \mathbb{F}_q((t^{\mathbb{Q}}))$. Par les propriétés usuelles des valuations on a

$$\begin{aligned} & v(x-z) \geq \min(v(x-y), v(y-z))) \\ \Leftrightarrow\ & 2^{-v(x-z)} \leq 2^{-\min(v(x-y),v(y-z))} \\ \Leftrightarrow\ & d(x,z) \leq \max(d(x,y), d(y,z)) \end{aligned}$$

□

Le corps $\mathbb{F}_q((t^{\mathbb{Q}}))$ est alors un corps valué ultramétrique. Afin d'étudier les propriétés de convergence dans ce corps ainsi que dans ses futurs sous-corps, nous introduisons la notion générale de complétude sous la forme suivante :

Définition 1.56. Un champ valué ultramétrique K est complet pour la valuation v si pour n'importe quelle suite $(x_n)_{n\geq 0}$ telle que $v(x_n - x_{n+1})$ tend vers l'infini si n tend vers l'infini, il existe un élément $x \in K$ tel que $v(x_n - x)$ tend aussi vers l'infini si n tend vers l'infini.

Bien que cette définition semble plus faible en apparence que la convergence des suites de Cauchy, elle s'avère identique en pratique dans le contexte d'une valuation ultramétrique. En effet, une suite est de Cauchy si $v(x_n - x_m) \to +\infty$ si $n, m \to +\infty$ et on a l'inégalité $v(x_n - x_{n+p}) \geq \min_{i=n}^{n+p-1}\{v(x_i - x_{i+1})\}$. Ainsi, si $v(x_i - x_{i+1}) \to +\infty$, le minimum aussi et la suite est de Cauchy. L'autre sens est trivial puisque la condition de Cauchy doit être valable pour tout n, m donc en particulier pour $n, n+1$.

Autrement dit, un corps ultramétrique est complet pour la valuation v si toute suite de Cauchy converge dans K, la convergence d'une suite $(x_n)_n$ vers x étant définie par la condition $v(x_n - x) \to +\infty$.

Théorème 1.57. *Le corps $\mathbb{F}_q((t^{\mathbb{Q}}))$ muni de la distance ultramétrique induite par la valuation v est un espace ultramétrique complet.*

Démonstration. Soit $(x_n)_n$ une suite dans $\mathbb{F}_q((t^{\mathbb{Q}}))$ telle que $\lim_{n\to+\infty} v(x_{n+1} - x_n) = +\infty$. Chaque terme de cette suite est une série de Laurent généralisée, notons-les $x_n = \sum_i f_n(i)t^i$ où $\mathrm{supp}(x_n)$ est bien ordonné. Par définition, on a que pour tout $j \in \mathbb{Q}$, il existe un rang $N_j \geq 0$ tel que pour tout $n \geq N_j$, on a $v(x_{n+1} - x_n) > j$. On en déduit que $f_{n+1}(i) = f_n(i)$ pour tout $i < j$. On définit alors la série limite par $x = \sum_i f(i)t^i$ où $f(i) = \lim_{n\to+\infty} f_n(i)$.

On a directement par construction que $v(x - x_n) \to +\infty$. Il nous reste à vérifier que x est bien dans $\mathbb{F}_q((t^{\mathbb{Q}}))$. Supposons par l'absurde qu'il existe une suite infinie strictement décroissante $i_0 > i_1 > i_2 > \cdots$ d'éléments de $\mathrm{supp}(x)$. Par hypothèse, on sait qu'il existe un rang N suffisamment grand tel que pour tout $n \geq N$, on a $v(x_{n+1} - x_n) > i_0$. Cela implique que pour tout $n \geq N$ et pour tout exposant $i \leq i_0$, les coefficients de la suite stationnent, c'est-à-dire que $f_n(i) = f_N(i) = f(i)$. En particulier, pour tous les éléments de notre suite décroissante, on a $f_N(i_k) = f(i_k) \neq 0$. Par conséquent, la suite strictement décroissante $\{i_0, i_1, i_2, \dots\}$ est entièrement incluse dans $\mathrm{supp}(x_N)$, ce qui contredit le fait que x_N a un support bien ordonné. □

Nous avons démontré ici la complétude de Cauchy, qui suffit à l'étude des séries. Cependant, on peut trouver dans [11] qu'il est remarquable de noter que le corps $\mathbb{F}_q((t^{\mathbb{Q}}))$ vérifie une propriété encore plus forte : il est sphériquement complet. C'est-à-dire que toute suite décroissante de boules fermées non vides $B_0 \supseteq B_1 \supseteq B_2 \cdots$ a une intersection non vide.

Proposition 1.58. *Dans l'espace ultramétrique complet $\mathbb{F}_q((t^{\mathbb{Q}}))$, une série $\sum_n a_n$ avec $a_n \in \mathbb{F}_q((t^{\mathbb{Q}}))$ converge si et seulement si son terme général tend vers 0, c'est-à-dire si et seulement si $v(a_n) \to +\infty$ quand $n \to +\infty$.*

Démonstration. Supposons que la série converge, c'est-à-dire que la suite de ses sommes partielles $(S_n)_n$ converge. Alors, on a $S_n - S_{n-1} = a_n$ d'où $v(a_n) = v(S_n - S_{n-1}) \to +\infty$ quand $n \to +\infty$.
Supposons à présent que $v(a_n) \to +\infty$ et montrons que la suite $(S_n)_n$ converge. Par les propriétés ultramétriques, on a $v(S_m - S_n) = v(\sum_{k=n+1}^{m} a_k) \geq \min_{n+1 \leq k \leq m}\{v(a_k)\}$. Comme $v(a_k) \to +\infty$ pour $k \to \infty$, il en va de même pour $v(S_m - S_n)$ lorsque $m, n \to +\infty$. La suite $(S_n)_n$ est alors de Cauchy donc converge. □

1.10 Enoncé de notre résultat principal

Enonçons notre résultat principal. Le but est de fournir une généralisation du théorème de Christol dans le cas des séries de Laurent généralisées. Pour cela, commençons par adapter la notion de fonctions p-automatiques à notre contexte.

Définition 1.59. Soit q une puissance du nombre premier p et soit $f : \mathbb{Q} \to \mathbb{F}_q$ une fonction telle que son support S est bien ordonné. On dit que f définit une série de Laurent généralisée p-quasi-automatique si les conditions suivantes sont respectées :

a) Il existe des entiers a, b avec $a > 0$ tels que $f(\frac{i-b}{a})$ a son support inclus dans S_p.

b) Pour des entiers $a > 0$ et b qui vérifient l'assertion précédente, la fonction $f_{a,b} : S_p \to \mathbb{F}_q$ donnée par $f_{a,b}(i) = f(\frac{i-b}{a})$ est p-automatique.

Dans le cas où une série de Laurent généralisée p-quasi-automatique a son support inclus dans S_p, c'est-à-dire si le point a) est vérifié pour $a = 1, b = 0$, on dit que la série est p-automatique.

Théorème 1.60. *Soit q une puissance de p et $f : \mathbb{Q} \to \mathbb{F}_q$ une fonction dont le support est bien ordonné. Alors, la série de Laurent généralisée correspondante $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si elle est p-quasi-automatique.*

Corollaire 1.61. *La série de Laurent 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 pour tout $\alpha \in \mathbb{F}_q$, la série de Laurent généralisée $\sum_{i \in f^{-1}(\alpha)} t^i$ est algébrique sur $\mathbb{F}_q(t)$.*

Chapitre 2

Le sens automatique implique algébrique

On s'appuie sur les résultats de [12] et [16]. Le but est d'adapter le sens de démonstration qu'on a fait pour Christol dans le chapitre 1 à notre contexte étendu. On commence par un lemme de stabilité algébrique.

Lemme 2.1. *Soient des entiers a, b avec $a > 0$. La série $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si la série $\sum_i f(\frac{i-b}{a})t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. Pour montrer que ce résultat est valide peu importe les entiers a et b qu'on choisit, on commence par montrer que celui-ci est valide pour $a = 1$ et b quelconque puis pour $a > 1$ et $b = 0$. La réunion des deux cas nous donne le résultat pour des a et b quelconques. En effet, toute série de la forme $\sum_i f(\frac{i-b}{a})t^i$ peut s'écrire sous la forme $t^b \sum_i f(i)(t^a)^i$, alors le cas $a > 1, b = 0$ prouve que $\sum_i f(i)(t^a)^i$ est algébrique et le cas $a = 1, b$ quelconque prouve que le tout est algébrique, c'est-à-dire $\sum_i f(\frac{i-b}{a})t^i$ est algébrique.

Commençons par supposer que $a = 1$ et prenons b quelconque. On remarque que la série est alors $\sum_i f(i-b)t^i = \sum_i f(i)t^{i+b} = t^b \sum_i f(i)t^i$. Si $\sum_i f(i)t^i$ annule $P = \sum_{i=0}^n a_i z^i$, $a_i \in \mathbb{F}_q(t)$, alors le polynôme $Q = \sum_{i=0}^n a_i(\frac{z}{t^b})^i = \sum_{i=0}^n (a_i t^{-bi})z^i$ est tel que $a_i t^{-bi} \in \mathbb{F}_q(t)$ et est annulé par la série $t^b \sum_i f(i)t^i$. Inversement, si $\sum_i f(i-b)t^i = t^b \sum_i f(i)t^i$ annule le polynôme $Q = \sum_{i=0}^n a_i z^i$, alors le polynôme $P = \sum_{i=0}^n a_i(zt^b)^i = \sum_{i=0}^n (a_i t^{bi})z^i$ est tel que $a_i t^{bi} \in \mathbb{F}_q(t)$ et est annulé par la série $\sum_i f(i)t^i$.

Passons maintenant au cas $a > 1$ et $b = 0$. La série est $\sum_i f(\frac{i}{a})t^i = \sum_i f(i)t^{ai}$. On considère l'automorphisme τ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ définit par $\tau : \sum_i f(i)t^i \mapsto \sum_i f(i)t^{ai}$. Alors, comme $\mathbb{F}_q(t) \subset \mathbb{F}_q((t^{\mathbb{Q}}))$, on peut restreindre τ à $\mathbb{F}_q(t)$, τ reste un automorphisme et l'image de $\mathbb{F}_q(t)$ par τ^{-1} est incluse dans $\mathbb{F}_q(t^{\frac{1}{a}})$. On a alors, si $\sum_i f(i)t^i$ annule le polynôme $P = \sum_{i=0}^n a_i z^i$, $a_i \in \mathbb{F}_q(t)$, alors $Q = \sum_{i=0}^n \tau(a_i)z^i$ est tel que $\tau(a_i) \in \mathbb{F}_q(t)$ et est annulé par la série $\sum_i f(i)t^{ai} = \tau\left(\sum_i f(i)t^i\right)$. Inversement, si $\sum_i f(i)t^a$ annule le polynôme $Q = \sum_{i=0}^n a_i z^i$, $a_i \in \mathbb{F}_q(t)$, alors le polynôme $P = \sum_{i=0}^n \tau^{-1}(a_i)z^i$ est tel que $a_i^{\tau^{-1}} \in \mathbb{F}_q(t^{\frac{1}{a}})$ et est annulé par la série $\sum_i f(i)t^i$. Ce qui implique que cette série est algébrique sur $\mathbb{F}_q(t^{\frac{1}{a}})$. Or, $\mathbb{F}_q(t^{\frac{1}{a}})$ est de dimension finie sur $\mathbb{F}_q(t)$ car $t^{\frac{1}{a}}$ est racine du polynôme $z^a - t \in \mathbb{F}_q(t)[z]$,

irréductible sur $\mathbb{F}_q(t)$. Par le corollaire 1.3, $\mathbb{F}_q(t^{\frac{1}{a}})$ est algébrique sur $\mathbb{F}_q(t)$. On conclut que $\sum_i f(i)t^i$ est algébrique sur $\mathbb{F}_q(t)$, ce qu'on voulait. □

Nous voyons à présent le lemme qui est une adaptation de celui démontré par Christol, comme annoncé dans le chapitre 1.

Lemme 2.2. *Soit q une puissance d'un nombre premier p et soit S un sous-ensemble p-reconnaissable de S_p. Alors $\sum_{i\in S} t^i \in \mathbb{F}_q[[t^{\mathbb{Q}}]]$ est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. Par définition d'ensemble p-reconnaissable, on sait que χ_S est p-automatique donc il existe un AFDO $M = (Q, \Sigma, \delta, q_0, \{0,1\}, \tau)$ tel que pour tout $i \in S, \chi_S(i) = f_M(\mathrm{rep}_p(i))$. Comme $S \subset S_p$, on sait aussi que $\mathrm{rep}_p(i)$ est une représentation valide en base p.

Pour $n \geq 0$, soit $s'(n)$ la représentation en base p de n à laquelle on enlève la partie après la virgule ainsi que la virgule. Notons $Q_{pre} = \{q_0, \ldots, q_r\}$ les états pré-virgules, alors pour chaque état pré-virgule $q_i \in Q_{pre}$, soit T_{q_i} l'ensemble des entiers $n \geq 0$ tels que q_i est accessible depuis q_0 en lisant $s'(n)$:

$$T_{q_i} = \{n \geq 0 | \delta^*(q_0, s'(n)) = q_i\}.$$

Posons $f_{q_i}(t) = \sum_{j\in T_{q_i}} t^j$. Notons U_{q_i} l'ensemble des paires $(q', d) \in Q_{pre} \times \{0, \ldots, p-1\}$ telles que $\delta(q', d) = q_i$.

Alors, si $q_i \neq q_0$, on a :

$$f_{q_i}(t) = \sum_{(q',d)\in U_{q_i}} t^d f_{q'}(t)^p.$$

En effet, si $s'(j) = ud$ où $u \in \{0, \ldots, p-1\}^*, d \in \{0, \ldots, p-1\}$, alors $j = p.\mathrm{val}_p(u) + \mathrm{val}_p(d)$ et $\mathrm{val}_p(d) = d$. On peut alors réécrire $f_{q_i}(t)$:

$$\begin{aligned} f_{q_i}(t) &= \sum_{j\in T_{q_i}} t^j \\ &= \sum_{(q',d)\in U_{q_i}} \sum_{l\in T_{q'}} t^{pl+d} \\ &= \sum_{(q',d)\in U_{q_i}} t^d \sum_{l\in T_{q'}} (t^l)^p \\ &= \sum_{(q',d)\in U_{q_i}} t^d (f_{q'}(t))^p. \end{aligned}$$

Si $q_i = q_0$, on a

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

Par le lemme 1.23, f_{q_i} est algébrique sur $\mathbb{F}_q(t)$ pour chaque état pré-virgule q_i. On a

$$v = \begin{pmatrix} f_{q_0} \\ \vdots \\ f_{q_n} \end{pmatrix}, \quad \sigma(v) = \begin{pmatrix} f^p_{q_0} \\ \vdots \\ f^p_{q_n} \end{pmatrix}, \quad w = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Pour tout $i > 0$, on a $f_{q_i}(t) = \sum_{j=1}^{n} C_{i,j}(t) f_{q_j}(t)^p$, où $C_{i,j}(t)$ est la somme des t^d provenant des transitions qui vont de q_j vers q_i. En d'autres termes, $C_{i,j}(t) = \sum_{d:(q_j,d)\in U_{q_i}} t^d$.

On pose $A = -(C_{i,j})$ et on obtient la relation $v + A\sigma(v) = w$, respectant les conditions du lemme 1.23.

Pour $x \in S_p \cap [0,1[$, soit $s''(x)$ la représentation en base p de x à laquelle on enlève la partie avant la virgule. Notons $Q_{post} = \{q_{r+1}, \ldots, q_m\}$ l'ensemble des états post-virgules. Pour chaque état $q_i \in Q_{post}$, soit V_{q_i} l'ensemble des $x \in S_p \cap [0,1[$ tels que, à partir de q_i, la représentation est acceptée par l'automate.

$$V_{q_i} = \{x \in S_p \cap [0,1[: \delta^*(q_i, s''(x)) \text{ est final}\}.$$

Posons $g_{q_i}(t) = \sum_{j\in V_{q_i}} t^j$.

Alors, si q_i est non final, on a :

$$g_{q_i}(t)^p = \sum_{d=0}^{p-1} t^d g_{\delta(q_i,d)}(t).$$

En effet, si $s''(j) =, du$, alors $s''(jp) = d, u$ et $jp = d + \mathrm{val}_p(u)$. On peut alors écrire $g_{q_i}(t)^p$ sous la forme :

$$\begin{aligned} g_{q_i}(t)^p &= \left(\sum_{j\in V_{q_i}} t^j\right)^p = \sum_{j\in V_{q_i}} t^{jp} \\ &= \sum_{d=0}^{p-1} t^d \sum_{l\in V_{q'}} t^l \quad \text{où} \quad q' = \delta(q_i, d) \\ &= \sum_{d=0}^{p-1} t^d g_{\delta(q_i,d)}(t) \end{aligned}$$

Si q_i est final, on a

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

Par le lemme 1.23, g_{q_i} est algébrique pour chaque état post-virgule. On a

$$v = \begin{pmatrix} g_{q_r} \\ \vdots \\ g_{q_m} \end{pmatrix}, \quad \sigma(v) = \begin{pmatrix} g^p_{q_r} \\ \vdots \\ g^p_{q_m} \end{pmatrix},$$

w est le vecteur où $w_i = 1$ si q_i est final et 0 sinon.

Pour tout $i \in \{r+1, \dots, m\}$, on a $g_{q_i}(t)^p = \sum_{j=1}^{n} C_{i,j}(t) g_{q_j}(t)$, où $C_{i,j}(t)$ est la somme des t^d provenant des transitions qui vont de q_i vers q_j. En d'autres termes, $C_{i,j}(t) = \sum_{d:\delta(q_i,d)=q_j} t^d$.

On pose $B = -(C_{i,j})$. On obtient la relation $Bv + \sigma(v) = w$, respectant les conditions du lemme 1.23.

Finalement, notons que $\sum_{i \in S} t^i = \sum_{q_l, q_j} f_{q_l}(t) g_{q_j}(t)$, où la somme parcourt les états pré-virgules q_l et post-virgules q_j. Cette somme est algébrique sur $\mathbb{F}_p(t)$ par le lemme 1.4. On a donc le résultat. □

Théorème 2.3. *Soit $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série de Laurent généralisée p-quasi-automatique. Alors $\sum_i f(i)t^i$ est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. Choisissons des entiers a et b comme dans la définition 1.59. Pour chaque $\alpha \in \mathbb{F}_q$, soit S_α l'ensemble des $j \in S_p$ tels que $f(\frac{j-b}{a}) = \alpha$. Alors, chaque S_α est p-reconnaissable car $f_{a,b} : S_p \to \mathbb{F}_q \quad i \mapsto f(\frac{i-b}{a})$ est p-automatique par p-quasi-automaticité de $\sum_i f(i)t^i$. Par le lemme précédent, on obtient que $\sum_{j \in S_\alpha} t^j$ est algébrique sur $\mathbb{F}_q(t)$. De plus,

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

est aussi algébrique sur $\mathbb{F}_q(t)$ par le lemme 1.4. On conclut grâce au lemme 2.1. □

2.1 Stabilité des séries p-quasi-automatiques

On peut d'ores et déjà établir des propriétés de stabilité sur les séries p-quasi-automatiques. Ces propriétés nous seront d'une grande aide dans le chapitre 4. Les résultats suivants peuvent être retrouvés dans les articles [16] et [13].

Définition 2.4. On note $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$ le sous-ensemble de $\mathbb{F}_q((t^{\mathbb{Q}}))$ consistant en les éléments p-quasi-automatiques.

Remarque 2.5. Dans la suite, par soucis de clarté et pour simplifier les notations nous noterons les séries de Laurent généralisées $\sum_i x_i t^i$.

Lemme 2.6. *Soient $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$ alors leur somme $x + y \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$.*

Démonstration. Par définition de séries p-quasi-automatiques, on peut trouver des entiers a_1, b_1, a_2, b_2 tels que $\sum_i x_i t^{a_1 i + b_1}$ et $\sum_i y_i t^{a_2 i + b_2}$ soient p-automatiques. Alors, on peut trouver des entiers $a > 0$ et b communs tels que $x(t^a)t^b = \sum_{i \geq 0} x'_i t^i$ et $y(t^a)t^b = \sum_{i \geq 0} y'_i t^i$ sont toutes les deux p-automatiques en prenant le plus petit commun multiple de a_1 et a_2 pour trouver a et en prenant b de telle sorte que les supports sont bien dans S_p.

Comme les suites (x'_i) et (y'_i) sont p-automatiques, leur somme est toujours p-automatique (par construction de l'automate produit effectuant l'addition dans $\mathbb{F}_q$).

On conclut que la série $(x+y)(t^a)t^b$ est p-automatique. De plus, le support de $(x+y)(t^a)t^b$ étant inclus dans l'union des supports de $x(t^a)t^b$ et $y(t^a)t^b$, tous deux dans S_p, on a bien qu'il est lui aussi inclus dans S_p. Dès lors, $x+y$ est p-quasi-automatique par définition. □

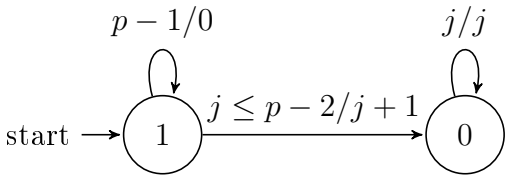
Lemme 2.7. *Soient $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$, alors leur produit d'Hadamard $x \odot y \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$.*

Démonstration. De la même manière que pour la somme, on peut se ramener à deux séries p-automatiques. Le produit terme à terme de suites p-automatiques est p-automatique par construction de l'automate produit dont les sorties sont définies par le produits des sorties des automates de départ dans le corps $\mathbb{F}_q$. On conclut que $x \odot y$ est p-quasi-automatique. □

Le lemme suivant est un mélange des résultats de la section 4.3 dans [1].

Lemme 2.8. *Soit $S \subset S_p$. Pour tous entiers a, b tels que $a > 0, b \geq 0$, S est p-reconnaissable si et seulement si $aS + b$ l'est.*

Démonstration. On construit un transducteur qui lit $\text{rep}_p(s)$ et rend $\text{rep}_p(s+1)$.



Alors, pour tout entier $b \geq 0$, S est p-reconnaissable si et seulement si $S + b$ l'est.
On construit à présent un transducteur qui lit $\text{rep}_p(s)$ et rend $\text{rep}_p(as)$. Pour cette opération, on a des retenues jusque $a-1$. Le transducteur est défini comme suit : $\Sigma = \Delta = \{0, \ldots, p-1\}$, $Q = \{0, \ldots, a-1\}$, $q_0 = 0$, $\delta(q, j) = \lfloor \frac{q+aj}{p} \rfloor$ et $\lambda(q, j) = q + aj \mod p$.
On a alors notre conclusion par stabilité des langages réguliers à la fois par l'application d'un transducteur (image directe) et par l'application d'un transducteur inverse (image réciproque). □

Proposition 2.9. *Pour $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ dont le support est inclus dans S_p et a, b des entiers avec $a > 0$, $b \geq 0$, x est p-automatique si et seulement si $\sum x_i t^{ai+b}$ l'est.*

Démonstration. Supposons que x est p-automatique et montrons qu'alors $x' = \sum_i x_i t^{ai+b} = \sum_i x_{\frac{i-b}{a}} t^i$ l'est aussi. On commence par vérifier que le support de x' est dans S_p.

$$\begin{aligned}
\text{supp}(x') &= \{i \in \mathbb{Q} : x_{\frac{i-b}{a}} \neq 0\} \\
&= \{i \in \mathbb{Q} : \frac{i-b}{a} \in \text{supp}(x)\} \\
&\subset \{i \in \mathbb{Q} : i \in aS_p + b\} \\
&\subset aS_p + b \subset S_p
\end{aligned}$$

On vérifie facilement que la suite des coefficients est toujours p-automatique car les transformations affines sur les indices $i \mapsto \frac{i-b}{a}$ ne changent pas l'automaticité par le lemme précédent.

L'autre sens se fait de façon similaire. □

Ce lemme nous assure que si le point b) de la définition 1.59 est vérifié pour un couple (a, b) qui vérifie le point a), alors il est vérifié pour n'importe quel couple (a', b').

Corollaire 2.10. *L'ensemble* $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$ *est un module sur* $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}} \cap \mathbb{F}_q((t))$.

Démonstration. $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$ est stable par addition par le lemme 2.6.

$\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}} \cap \mathbb{F}_q((t))$ est un anneau puisque c'est la clôture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t))$. En effet, une série p-quasi-automatique à exposants entiers se ramène, par un décalage t^b, à une série formelle p-automatique qui est algébrique sur $\mathbb{F}_q(t)$ d'après Christol. La série de Laurent initiale l'est donc aussi, puisque le décalage par un monôme préserve l'algébricité.

Il reste à vérifier que pour $x \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$, $y \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}} \cap \mathbb{F}_q((t))$, on a $xy \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$. Comme pour le lemme 2.6, on se ramène au cas où x et y sont p-automatiques (on omet de les noter $x(t^a)t^b$ et $y(t^a)t^b$ pour plus de clarté). On peut exprimer x comme une combinaison linéaire finie $\sum_i y_i z_i$ dans laquelle $y_i \in \mathbb{F}_q((t))$ correspond à la partie entière de x et est p-automatique et z_i correspond à la partie fractionnaire de x, à support dans $[0, 1)$ et est aussi p-automatique (par restriction de l'automate fini acceptant les représentations en base p des éléments du support de x).

Alors, $xy = \sum_i (yy_i)z_i$ est p-automatique. En effet, (yy_i) est p-automatique par produit de séries p-automatiques. Toute combinaison linéaire finie de cette forme est p-automatique par stabilité pour la somme et en construisant l'automate produit pour $(yy_i)z_i$ qui renvoie le produit du coefficient déterminé par yy_i pour la partie entière des représentations en base p des indices et le coefficient déterminé par z_i pour la partie fractionnaire de ces représentations.

Finalement, xy est bien p-quasi-automatique puisqu'après un décalage adéquat on s'est ramené à une série p-automatique. □

Chapitre 3

Preuve algorithmique

Dans ce chapitre, on donne une preuve algorithmique du sens algébrique implique automatique, principalement basée sur [12]. Plus tard, on prouvera ce même sens du théorème par une approche purement algébrique. Certaines notions vues dans ce chapitre seront alors utiles.

3.1 Polynômes tordus

De la même manière que nous avons réduit notre étude aux polynômes additifs au chapitre 1, nous adoptons ici une démarche analogue en introduisant les polynômes tordus, qui constitueront le cœur de notre machinerie algorithmique pour valider le théorème.
Soit K un champ de caractéristique p.

Définition 3.1. Soit $K\{F\}$ l'anneau non-commutatif dont les éléments sont des sommes formelles finies $\sum_{i=0}^{m} c_i F^i$, additionnés composante à composante et multipliés par la règle :

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

L'anneau $K\{F\}$ est appelé l'anneau polynomial tordu sur K.

Définition 3.2. Comme dans le cas polynomial, le degré d'un polynôme tordu non nul $\sum_i c_i F^i$ est le plus grand i tels que $c_i \neq 0$. Le degré du polynôme 0 est $-\infty$.

Proposition 3.3. *Le degré du produit de deux polynômes tordus non nuls est la somme de leurs degrés.*

En particulier, l'anneau $K\{F\}$ est intègre et non-commutatif.

Remarque 3.4. On peut associer à tout polynôme tordu $P(F) = \sum_i c_i F^i$ sur K un polynôme classique additif en une indéterminée z, défini par $P(F)(z) = \sum_i c_i z^{p^i} \in K[z]$.

On retrouve l'algorithme de division euclidienne.

Lemme 3.5. *Soient $S(F)$ et $T(F)$ des polynômes tordus sur K, avec $T(F)$ non nul de degré $d \geq 0$. Alors, il existe une unique paire $Q(F), R(F)$ de polynômes tordus sur K avec $\deg(R) < d$ tels que $S = QT + R$.*

Démonstration. Ecrivons $T(F) = \sum_{i=0}^{d} c_i F^i$ avec $c_d \neq 0$. L'existence se montre par induction sur le degré de S. Si $\deg(S) < d$, on prend $Q = 0$ et $R = S$. Supposons maintenant que $e \geq d$ et que le résultat est vrai pour tous les polynômes de degré strictement plus petit que e et montrons qu'alors c'est toujours vrai pour les polynômes de degré e. Soit aF^e le terme de plus haut degré de S, on veut se ramener à un polynôme de plus petit degré en soustrayant un multiple de T au polynôme S. On cherche b tel que $bF^{e-d}T$ ait aF^e comme terme de plus haut degré. Alors $b = \frac{a}{c_d^{p^{e-d}}}$ convient.

On définit alors $S_1 = S - (\frac{a}{c_d^{p^{e-d}}} F^{e-d})T$. Par construction, on a $\deg(S_1) < \deg(S)$, alors par hypothèse de récurrence on sait qu'il existe Q_1, R tels que $S_1 = Q_1 T + R$ avec $\deg(R) < d$. On a alors la conclusion : $S = (Q_1 + \frac{a}{c_d^{p^{e-d}}} F^{e-d})T + R$.

L'unicité provient du fait que si $S = QT + R = Q'T + R'$ sont deux décompositions de la forme voulue, alors $R - R' = (Q' - Q)T$. Le premier membre étant de degré strictement plus petit que celui de T et si $Q' - Q \neq 0$ le deuxième membre strictement plus grand, on obtient $Q = Q'$, et donc aussi $R = R'$. □

Lemme 3.6. *Soit L une clôture algébrique de K et soit $T(F) = \sum_{i=0}^{d} c_i F^i$ un polynôme tordu non nul de degré d sur K. Alors, le noyau $\ker(T)$ agissant sur L est un $\mathbb{F}_p$-espace vectoriel de dimension plus petite ou égale à d, avec l'égalité si et seulement si $c_0 \neq 0$.*

Démonstration. On a bien un $\mathbb{F}_p$-espace vectoriel puisqu'on peut voir $T(F)(z)$ comme un polynôme additif et en vertu de la proposition 1.20. En tant que polynôme en la variable z, $T(F)(z)$ est de degré p^d. Un polynôme de degré p^d possède au plus p^d racines distinctes dans L. Puisque le noyau $\ker(T)$ est un $\mathbb{F}_p$-espace vectoriel, son cardinal est donné par $p^{\dim_{\mathbb{F}_p}(\ker(T))}$. L'inégalité $p^{\dim_{\mathbb{F}_p}(\ker(T))} \leq p^d$ donne alors immédiatement $\dim_{\mathbb{F}_p}(\ker(T)) \leq d$. La dimension du noyau est donc bien au plus d. De plus, le nombre de racines est égal au degré du polynôme si et seulement si celui-ci est séparable. Un polynôme $P(z)$ est séparable si sa dérivée formelle $P'(z)$ n'est pas nulle. La dérivée de $T(F)(z)$ est c_0. Si $c_0 \neq 0$, alors la dérivée n'est pas nulle, le polynôme est séparable et possède exactement p^d racines distinctes. Dans ce cas, la dimension du noyau est exactement d. □

Proposition 3.7. *Soient $S(F)$ et $T(F)$ des polynômes tordus sur K, avec le coefficient constant de T non nul, et soit L une clôture algébrique de K. Alors, S est un multiple à gauche de T, c'est-à-dire qu'il existe $Q \in K\{F\}$ tel que $S = QT$, si et seulement si $\ker_L(T) \subset \ker_L(S)$.*

Démonstration. Commençons par la condition nécessaire. Si $S = QT$, alors $T(F)(z) = 0$ implique $S(F)(z) = 0$ d'où $\ker_L(T) \subset \ker_L(S)$.

Passons à la condition suffisante. Supposons que $\ker_L(T) \subset \ker_L(S)$ et écrivons $S = QT + R$. On a alors aussi $\ker_L(T) \subset \ker_L(R)$. Par le lemme précédent, $\ker_L(T)$ est un $\mathbb{F}_p$-espace vectoriel de dimension $\deg(T)$ puisque son coefficient constant est non nul. Si R est

non nul, alors $\ker_L(R)$ est un $\mathbb{F}_p$-espace vectoriel de dimension au plus $\deg(R) < \deg(T)$, ce qui contredit $\ker_L(T) \subset \ker_L(R)$. On a donc $R = 0$ et $S = QT$. □

3.2 Polygones de Newton

Pour étudier la structure d'un polynôme, une excellente approche consiste à utiliser les polygones de Newton. Cet outil combinatoire permet de traduire les coefficients du polynôme sous forme de graphiques convexes, ce qui s'avère particulièrement utile pour simplifier la recherche de racines ou la factorisation algorithmique. Au-delà du calcul formel, ils trouvent également de nombreuses applications en géométrie algébrique pour analyser les singularités de courbes ou encore dans l'étude des équations différentielles complexes. Reprenons la valuation sur $\mathbb{F}_q((t^{\mathbb{Q}}))$ définie à la section 1.9.

Définition 3.8. Etant donné un polynôme non nul $P(t) = \sum_i c_i t^i$ sur $K[t]$ pour un champ K muni d'une valuation v, on définit le polygone de Newton de P comme étant la frontière inférieure de l'enveloppe convexe de l'ensemble des points $(-i, v(c_i))$. Les pentes de ce polygone sont appelées les pentes de P. Pour $r \in \mathbb{Q}$, on définit la multiplicité de r comme pente de P comme étant la largeur (i.e la différence des abscisses des points extrémités) de l'unique segment du polygone de Newton de P de pente r, ou 0 si un tel segment n'existe pas. On déclare conventionnellement que ∞ peut être une pente et sa multiplicité comme pente du polynôme P est l'ordre d'annulation de P au point $t = 0$. On dit que P est pur de pente r si toutes les pentes finies de P sont égales à r.

Remarque 3.9. Le choix de prendre les points d'abscisse $-i$ vient du fait que dans ce cas, les pentes du polygone correspondent exactement aux valuations des racines de P. En effet, prenons $x \in K$ de valuation ρ et racine de P. Par définition, on a l'égalité $\sum_i c_i x^i = 0$. D'après les propriétés fondamentales des valuations ultramétriques, pour qu'une telle somme s'annule, la valuation minimale parmi tous les termes de la somme ne peut pas être atteinte par un unique terme (sinon, la valuation globale de la somme serait égale à cette valeur minimale, et non à $+\infty$). Il doit donc y avoir au moins deux termes, disons d'indices i et j, qui atteignent simultanément cette valuation minimale pour se compenser. La valuation de $c_i x^i$ est $v(c_i) + i\rho$. L'égalité de ces deux valuations, à savoir $v(c_i x^i) = v(c_j x^j)$, se traduit alors par $v(c_i) + i\rho = v(c_j) + j\rho$, c'est-à-dire $\rho = \frac{v(c_i) - v(c_j)}{j - i}$. On obtient que la valuation de x doit correspondre à la pente du segment reliant $(-i, v(c_i))$ à $(-j, v(c_j))$.

Exemple 3.10. Pour illustrer la théorie, on se place dans un cadre plus visuel. Construisons le polygone de Newton du polynôme $P(t) = 1 + 5t + \frac{1}{5}t^2 + 35t^3 + 25t^5 + 625t^6$ vu comme un polynôme à coefficients dans le corps $\mathbb{Q}_5$. La valuation que l'on utilise est donc la valuation 5-adique, c'est-à-dire, pour un nombre n, $v(n)$ est la plus grande puissance de 5 qui divise n. De plus, $v(\frac{m}{n}) = v(m) - v(n)$.

Les points à considérer sont :

$$A_0 = (0,0) \qquad A_3 = (-3,1)$$
$$A_1 = (-1,1) \qquad A_5 = (-5,2)$$
$$A_2 = (-2,-1) \qquad A_6 = (-6,4)$$

où A_4 n'est pas défini car $c_4 = 0$. Le polygone de Newton de P est la ligne brisée de sommets A_0, A_2, A_5, A_6 représentée à la figure 3.1

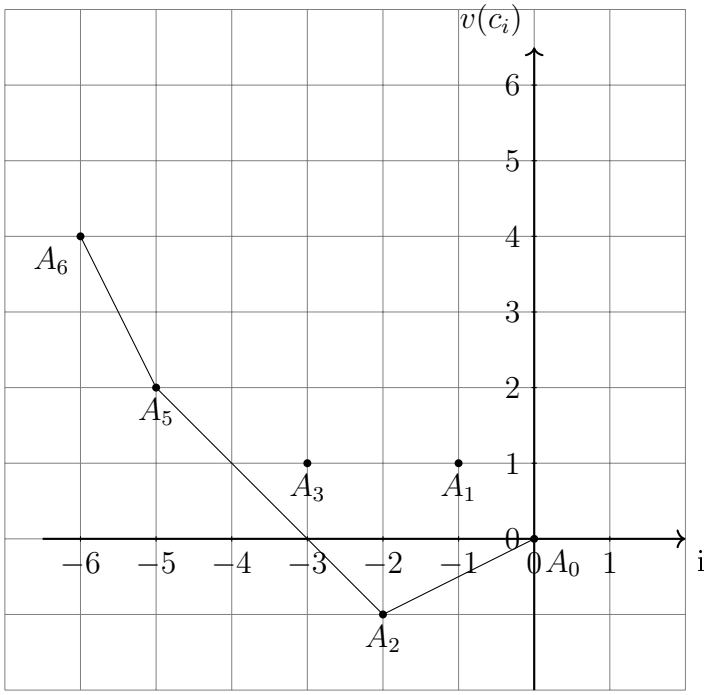


FIGURE 3.1 – Exemple de polygone de Newton

Le lemme suivant est un mélange des démonstrations qui peuvent être trouvées dans [12] et [9].

Lemme 3.11. *Soient P et Q des polynômes non nuls sur $\mathbb{F}_q((t^{\mathbb{Q}}))$. Alors, pour chaque $r \in \mathbb{Q} \cup \{\infty\}$, la multiplicité de r comme pente de PQ est la somme des multiplicités de r comme pente de P et Q.*

Démonstration. Supposons que $r \in \mathbb{Q}$. Ecrivons $P(z) = \sum_i c_i z^i$, $Q(t) = \sum_j d_j z^j$.
Notons $(-e, v(c_e)), (-f, v(c_f))$ les points extrêmes du segment possiblement dégénéré du polygone de Newton de P de pente r de multiplicité $f - e$. Notons $(-g, v(d_g)), (-h, v(d_h))$ les mêmes informations pour le polynôme Q, où la multiplicité de r est alors $h - g$. Alors, on a que e minimise $v(c_i) + ri$ et g minimise $v(d_j) + rj$. En effet, toute droite de pente r

a pour équation $y = rx + b$ et la droite de pente r du polygone de P passe par les points $(-e, v(c_e)), (-f, v(c_f))$. On en tire que $b = v(c_e) + re$ et comme cette droite est dans le polygone de Newton, cette valeur est bien la valeur minimale de $v(c_i) + ri$. Il en va de même pour Q.

On a $PQ(z) = \sum_k a_k z^k = \sum_k \sum_{i+j=k} c_i d_j z^k$. On veut étudier la valeur de $v(a_k) + rk$. Par les propriétés de valuation, on a $v(a_k) \geq \min_{i+j=k}\{v(c_i d_j)\}$ et $v(c_i d_j) + r(i + j) = v(c_i) + ri + v(d_j) + r_j$. Comme $v(c_i) + r_i \geq v(c_e) + re = v(c_f) + rf$ et $v(d_j) + rj \geq v(d_g) + rg = v(d_h) + rh$, on a toujours $v(c_i d_j) + r(i + j) \geq v(c_e) + re + v(d_g) + rg$.

On a alors plusieurs cas :

- $k = e+g$: $c_e d_g$ atteint le minimum, on a l'égalité $v(a_k)+rk = v(c_e)+re+v(d_g)+rg$.
- $k = f + h$: on a les mêmes conclusions pour $c_f d_h$.
- $k \notin [e+g, f+h]$: On a uniquement l'inégalité stricte puisqu'il est impossible d'avoir simultanément $i \in [e, f]$ et $j \in [g, h]$. Par conséquent, $v(c_i) + ri > v(c_e) + re$ ou $v(d_j) + rj > v(d_g) + rg$ d'où $v(a_k) + rk > v(c_e) + re + v(d_g) + rg$.

On trouve alors que la valeur minimale de $v(a_k)+rk$ est $v(c_e)+re+v(d_g)+rg$, c'est-à-dire la somme des valeurs minimales pour P et Q. Elle est atteinte pour $k = e+g$ et $k = f+h$ donc le segment reliant les points $(-(f + h), v(a_{f+h}))$ et $(-(e + g), v(a_{e+g}))$ est dans le polygone de Newton de PQ et de pente r. La multiplicité de r comme pente de PQ est alors $(f + h) - (e + g) = (f - e) + (h - g)$, qui sont les multiplicités de r comme pente de P et Q. □

Exemple 3.12. Reprenons notre exemple et vérifions que le procédé de chercher le minimum de $v(c_i) + ri$ nous rend bien le segment de pente r du polygone de Newton. On a $P(t) = 1 + 5t + \frac{1}{5}t^2 + 35t^3 + 25t^5 + 625t^6$, cherchons le segment de pente $\frac{1}{2}$ en minimisant la fonction $v(c_i) + \frac{1}{2}i$ pour $i \in \{0, 1, 2, 3, 5, 6\}$.

$$
\begin{array}{llll}
i = 0 & v(1) + \dfrac{1}{2}.0 = 0 & i = 3 & v(35) + \dfrac{1}{2}.3 = \dfrac{5}{2} \\
i = 1 & v(5) + \dfrac{1}{2}.1 = \dfrac{3}{2} & i = 5 & v(25) + \dfrac{1}{2}.5 = \dfrac{9}{2} \\
i = 2 & v(\dfrac{1}{5}) + \dfrac{1}{2}.2 = 0 & i = 6 & v(625) + \dfrac{1}{2}.6 = 7
\end{array}
$$

Le minimum est atteint en $i = 0$ et $i = 2$ ce qui nous dit que le segment $[(0, 0); (-2, -1)]$ est dans le polygone de Newton de P et de pente $\frac{1}{2}$, ce qu'on peut effectivement vérifier sur notre figure 3.1.

Corollaire 3.13. *Soit P un polynôme non nul sur $\mathbb{F}_q((t^{\mathbb{Q}}))$ qui se factorise en produit $Q_1 \cdots Q_n$ de polynômes purs. Alors, pour tout $r \in \mathbb{Q} \cup \{\infty\}$, la somme des degrés des Q_i pour i tel que Q_i a une pente r est égale à la multiplicité de r comme pente de P.*

Démonstration. Par définition, Q_i est pur de pente r si toutes ses pentes finies sont égales à r. Géométriquement, cela se représente par un unique segment dans le polygone de Newton, de pente r et dont la multiplicité vaut alors le degré du polynôme.

Par le lemme, la multiplicité de r comme pente de Q_iQ_j est la somme des multiplicités de r comme pente de Q_i et Q_j. Par induction, on obtient que la multiplicité de r comme pente de P est égale à la somme des multiplicités de r comme pente des polynômes Q_i. La multiplicité de r comme pente des polynômes Q_i étant exactement leur degré, on a la conclusion. □

L'étude des polygones de Newton nous donne la forme de la factorisation des polynômes. En vertu du corollaire 3.13 et de la remarque 3.9, chaque segment de pente r et de largeur m dans le polygone de Newton correspond à un facteur pur de degré m dont toutes les racines ont pour valuation r. Ainsi, un polynôme P peut être décomposé en un produit de facteurs $P = \prod_i P_{r_i}$, où chaque rupture de pente dans le polygone marque la transition vers un nouveau facteur algébrique. Cette décomposition est particulièrement puissante dans les corps valués complets, car elle permet de ramener l'étude d'un polynôme quelconque à celle de polynômes purs, beaucoup plus simples à manipuler.

Exemple 3.14. Dans notre exemple, l'étude du polygone de Newton révèle trois segments distincts, ce qui implique que P se factorise en trois polynômes purs : le premier dont la valuation des racines vaut $\frac{1}{2}$, le deuxième dont les racines sont de valuation -1 et le troisième avec des racines de valuation -2. Une factorisation de P est alors de la forme $P(t) = P_{\frac{1}{2}}(t)P_{-1}(t)P_{-2}(t)$ où le degré de chaque polynôme correspond à la multiplicité des pentes associées.

On cherche maintenant à utiliser les polygones de Newton pour affiner cette factorisation de tout polynôme non nul. Bien que le corps global $\mathbb{F}_q((t^{\mathbb{Q}}))$ soit complet, nous faisons le choix de restreindre nos résultats à un sous-corps K complet pour la valuation. Cette démarche répond à un impératif d'efficacité algorithmique : en confinant la preuve au sein d'un sous-corps adapté, on garantit que les facteurs obtenus posséderont exactement les mêmes types de coefficients que le polynôme de départ, sans nécessiter d'extensions de corps. Pour ce faire, on a besoin de quelques notions préalables.

Définition 3.15. Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v. Soient $r, s \in \mathbb{Q}$ tels que $r < s$ et $u \in (r, s)$ On définit le sous-ensemble S des séries $\sum_{j\in\mathbb{Z}} x_j z^j$ sur K telles que $v(x_j) + rj \geq 0$ pour tout $j \geq 0$ et $v(x_j) + sj \geq 0$ pour tout $j \leq 0$.

Proposition 3.16. *Le sous-ensemble S est un anneau.*

Démonstration. On commence par vérifier la stabilité pour l'addition. Soient $x = \sum_{j\in\mathbb{Z}} x_j z^j$ et $y = \sum_{j\in\mathbb{Z}} y_j z^j$ deux éléments de S. Alors $x + y = \sum_{j\in\mathbb{Z}}(x_j + y_j)z^j$. Comme $\mathbb{F}_q((t^{\mathbb{Q}}))$ est stable pour l'addition, on a bien que $x_j + y_j \in K$ pour tout j. Vérifions que cette série satisfait les conditions de S. Pour $j \geq 0$, on a

$$v(x_j + y_j) + rj \geq \min\{v(x_j), v(y_j)\} + rj = \min\{v(x_j) + rj, v(y_j) + rj\} \geq 0$$

car $v(x_j) + rj \geq 0$ et $v(y_j) + rj \geq 0$.
Pour $j \leq 0$, on a par le même raisonnement

$$v(x_j + y_j) + sj \geq \min\{v(x_j) + sj, v(y_j) + sj\} \geq 0$$

On conclut que $x + y \in S$.

Passons à la stabilité pour la multiplication. On a $xy = \sum_k c_k z^k = \sum_k \left(\sum_j x_j y_{k-j} \right) z^k$. On doit d'abord vérifier que le produit a un sens et que le coefficient c_k est bien dans K. Etant donné que K est complet pour la valuation v, il nous suffit de vérifier que $\sum_j x_j y_{k-j}$ converge, c'est-à-dire que $v(x_j y_{k-j})$ tend vers l'infini si j tend vers l'infini. Si $j \to +\infty$, on a $v(x_j) \geq -rj$. De plus, les contraintes de S nous donnent que pour tout indice n, on a $v(y_n) + un \geq 0$ car pour $n \geq 0$, $v(y_n) + un \geq v(y_n) + rn \geq 0$ et pour $n \leq 0$, $v(y_n) + un \geq v(y_n) + sn \geq 0$. On a alors, pour $j \to +\infty$,

$$v(x_j) + v(y_{k-j}) \geq -rj + (-u(k-j)) = (u-r)j - uk \to +\infty$$

car $u - r > 0$ vu que $u \in (r, s)$.
On procède de même pour $j \to -\infty$. On a $v(x_j) \geq -sj$ et $v(y_n) \geq -un$, et donc

$$v(x_j) + v(y_{k-j}) \geq -sj - u(k-j) = (u-s)j - uk \to +\infty$$

car $u - s < 0$ et $j < 0$. Au final, on a que $v(x_j y_{k-j}) \to +\infty$ pour tout $j \to \infty$ et la série converge. Le produit a donc un sens et on peut vérifier les conditions d'appartenance à S. On a $v(c_k) \geq \min_j \{v(x_j) + v(y_{k-j})\}$.

- Pour $k \geq 0$, on veut $v(c_k) + rk \geq 0$. On a

  $$v(x_j) + v(y_{k-j}) + rk = v(x_j) + rj + v(y_{k-j}) + r(k-j)$$

  Si $j \geq 0$, on a $v(x_j) + rj \geq 0$, pour $k \geq j$, $k - j \geq 0$ et $v(y_{k-j}) + r(k-j) \geq 0$ et pour $k \leq j$, $k - j \leq 0$ et $v(y_{k-j}) + r(k-j) \geq v(y_{k-j}) + s(k-j) \geq 0$.
  Si $j \leq 0$, on a $v(x_j) + rj \geq v(x_j) + sj \geq 0$ et $v(y_{k-j}) + r(k-j) \geq 0$ car $k - j \geq 0$.
  Alors, pour tout j, on a $v(x_j) + v(y_{k-j}) + rk \geq 0$ et en prenant le minimum sur j, on obtient $v(c_k) + rk \geq 0$ pour $k \geq 0$.
- Pour $k \leq 0$, on veut $v(c_k) + sk \geq 0$. On procède de la même manière que pour $k \geq 0$ et on conclut que $v(x_j) + v(y_{k-j}) + sk \geq 0$ pour tout j. En prenant le minimum sur j, on obtient $v(c_k) + sk \geq 0$ pour $k \leq 0$.

Finalement le produit xy appartient bien à S.
Les neutres pour l'addition et la multiplication sont respectivement 0 et 1, il est aisé de voir qu'ils appartiennent bien à S ce qui fait de S un anneau. □

Définition 3.17. On définit la valuation v_u sur S par la formule

$$v_u \left(\sum_{j \in \mathbb{Z}} x_j z^j \right) = \min_j \{v(x_j) + uj\}.$$

On vérifie que v_u définit bien une valuation. Tout d'abord il faut vérifier que v_u est bien défini et arrive bien dans $\mathbb{Q} \cup \{\infty\}$. L'ensemble $\{v(x_j) + uj\}$ est minoré pour tout j. En

effet, si $j \geq 0$, on a $v(x_j) + uj \geq (u-r)j \geq 0$ et si $j \leq 0$ on a $v(x_j) + uj \geq (u-s)j \geq 0$ donc l'ensemble est minoré par 0 pour tout j. Le minimum est bien atteint car si $j \to +\infty$, $v(x_j)+uj \to +\infty$ et si $j \to -\infty$, $v(x_j)+uj \to +\infty$ donc il n'y a qu'un nombre fini d'indices pour lesquels $v(x_j) + uj$ est en dessous d'un certain seuil, ce qui garantit l'existence d'un minimum. De plus, l'application v_u a bien son image dans $\mathbb{Q} \cup \{\infty\}$ car $v(x_j) \in \mathbb{Q} \cup \{\infty\}$ et $u \in \mathbb{Q}$ don chaque terme est dans $\mathbb{Q} \cup \{\infty\}$ d'où le minimum aussi.

Il nous reste à vérifier que v_u satisfait les trois propriétés des valuations :

1. $v_u(x) = +\infty \Leftrightarrow x = 0$:
   Supposons que $x = 0$, alors $x_j = 0$ pour tout j et $v(x_j) = v(0) = +\infty$. Alors $v_u(x) = \min_j\{v(x_j) + uj\} = +\infty$. Supposons maintenant que $v_u(x) = +\infty$, c'est-à-dire $v(x_j) + uj = +\infty$ pour tout j. Cela impose que $v(x_j) = +\infty$ puisque uj est une valeur finie. On conclut que $x_j = 0$ pour tout j et donc $x = 0$.
2. $v_u(x+y) \geq \min(v_u(x), v_u(y))$:
   On a $x + y = \sum_j (x_j + y_j) z^j$ et $v_u(x+y) = \min_j\{v(x_j + y_j) + uj\}$. Or, $v(x_j + y_j) \geq \min(v(x_j), v(y_j))$ car v est une valuation sur K. Alors, $v(x_j + y_j) + uj \geq \min(v(x_j) + uj, v(y_j) + uj)$ pour tout j. Cette inégalité reste vraie en prenant le minimum sur j, ce qui donne $\min_j\{v(x_j + y_j) + uj\} \geq \min\left(\min_j\{v(x_j) + uj\}, \min_j\{v(y_j) + uj\}\right)$ c'est-à-dire $v_u(x+y) \geq \min(v_u(x), v_u(y))$.
3. $v_u(xy) = v_u(x) + v_u(y)$:
   On a $xy = \sum_k \sum_{i+j=k} x_i y_j z^k$. Pour chaque k, on a $v(c_k)+uk = v(\sum_{i+j=k} x_i y_j)+uk \geq \min_{i+j=k}\{v(x_i) + v(y_j)\} + u(i+j) = \min_{i+j=k}\{v(x_i) + ui + v(y_j) + uj\}$ où pour tout j, $v(x_j) + uj \geq v_u(x)$ et $v(y_j) + uj \geq v_u(y)$ par définition de v_u. On obtient alors $v_u(xy) \geq v_u(x) + v_u(y)$.
   On montre l'autre inégalité. Supposons que $v_u(x) = \mu_x$ et $v_u(y) = \mu_y$. Par définition du minimum, on a pour tout i et j, $v(x_i) + ui \geq \mu_x$ et $v(y_j) + uj \geq \mu_y$ et il existe des plus petits indices i_0 et j_0 tels que $v(x_{i_0}) + ui_0 = \mu_x$ et $v(y_{j_0}) + uj_0 = \mu_y$. Regardons le coefficient du produit correspondant à $i_0 + j_0 = k_0$: $c_{k_0} = x_{i_0} y_{j_0} + \sum_{\substack{i+j=k_0 \\ i \neq i_0}} x_i y_j$.
   Regardons la valuation de $c_{k_0} z^{k_0}$, $v_u(c_{k_0} z^{k_0}) = v(c_{k_0}) + uk_0 = \min_{i+j=k_0}\{v(x_i y_j) + u(i+j)\}$. Pour $i = i_0, j = j_0$, on a $v(x_{i_0} y_{j_0}) + u(i_0 + j_0) = \mu_x + \mu_y$ par définition. Pour tout autre couple $(i,j) \neq (i_0, j_0)$, on a forcément $i > i_0$ ou $j > j_0$. Par définition de plus petits indices, on a alors $v(x_i y_j) + u(i+j) > \mu_x + \mu_y$. Alors $v(c_{k_0}) + uk_0 = \mu_x + \mu_y$. Comme $v_u(xy) = \min_k\{v(c_k) + uk\}$, on a en particulier $v_u(xy) \leq v(c_{k_0}) + uk_0$. On en déduit que $v_u(xy) \leq \mu_x + \mu_y = v_u(x) + v_u(y)$. En combinant nos deux inégalités, on trouve finalement $v_u(xy) = v_u(x) + v_u(y)$.

Lemme 3.18. *L'anneau S est complet pour la valuation v_u.*

Démonstration. Soit $(x_n)_n$ une suite de Cauchy dans S pour la valuation v_u. Par définition, pour tout $M > 0$, il existe $N > 0$ tel que pour tous $n, m > N$, $v_u(x_n - x_m) \geq M$. En isolant chaque coefficient d'indice j dans $x_n = \sum_i a_i z^i$, nous obtenons

$$\begin{aligned} v(a_j^{(n)} - a_j^{(m)}) + uj \geq v_u(x_n - x_m) \geq M \\ \Leftrightarrow v(a_j^{(n)} - a_j^{(m)}) \geq M - uj \end{aligned}$$

Pour un indice j fixé, la suite des coefficients $(a_j^{(n)})_n$ est une suite de Cauchy dans K. Puisque K est complet pour la valuation v, chaque suite de coefficients converge vers une limite $A_j \in K$. Considérons la série formelle limite $x = \sum_{j\in\mathbb{Z}} A_j z^j$. Pour prouver que S est complet pour la valuation v_u, on doit vérifier que x satisfait les conditions de croissances. Pour chaque n, nous savons que $x_n \in S$ donc pour tout $j \geq 0$, on a $v(a_j^{(n)}) \geq -rj$. Par continuité de la valuation v, l'inégalité est préservée par le passage à la limite pour n qui tend vers l'infini. On a $v(A_j) = \lim_{n\to+\infty} v(a_j^{(n)}) \geq -rj$. Le même raisonnement s'applique pour $j \leq 0$ avec s. Ainsi, x respecte les conditions et appartient bien à S. L'ensemble S est alors complet pour la valuation v_u. □

Lemme 3.19. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v. Soit P un polynôme non nul sur K et choisissons $u \in \mathbb{Q}$ qui n'apparait pas comme pente de P.*

Alors, il existe une factorisation $P = QR$, où Q est un polynôme sur K avec toutes ses pentes plus petites que u et R est un polynôme sur K avec toutes ses pentes plus grandes que u.

Démonstration. Prenons $r, s \in \mathbb{Q}$ tels que $r < s$ et $u \in (r, s)$ mais aucune pente de P n'appartient à cet intervalle.

Soit S l'anneau de séries formelles muni de la valuation v_u définis aux définitions 3.15 et 3.17. Étant donné $y = \sum_j y_j z^j \in S$, écrivons $f(y) = \sum_{j>0} y_j z^j$. On a alors $f(f(y)) = f(y)$. Notons $P(z) = \sum_{i=0}^{d} c_i z^i$, $d = \deg(P)$. Soit e l'unique entier qui minimise $v(c_i)+ui$ puisque u n'apparait pas comme pente de P et posons $x_0 = c_e^{-1} z^{-e} P(z) \in S$. On définit la suite $(x_h)_{h\geq 0}$ par la récurrence $x_{h+1} = x_h(1 - f(x_h))$ pour $h \geq 0$. Posons $l = v_u(x_0 - 1)$, on a $v_u(x_0 - 1) = v_u\left(\sum_{i\neq e}(c_e^{-1}c_i)z^{i-e}\right) = \min_{i\neq e}\{v(c_e^{-1}c_i) + u(i-e)\}$.
Or, $v(c_e^{-1}c_i) + u(i-e) = v(c_i) - v(c_e) + u(i-e)$ qui est strictement positif pour tout indice $i \neq e$ par définition de e : $v(c_i) + ui > v(c_e) + ue$. On a donc $l > 0$.
On montre par induction que $v_u(x_h) = 0$, $v_u(x_h - 1) \geq l$ et $v_u(f(x_h)) \geq (h+1)l$ pour tout h.

Cas de base : Pour $h = 0$, $v_u(x_0) = v_u(x_0 - 1 + 1) = \min(v_u(x_0 - 1), v_u(1)) = 0$ car $v_u(x_0 - 1) = l > 0$. On a directement la deuxième inégalité par définition de l et elle implique la troisième puisqu'on prend le minimum sur moins d'indices.

Induction : Supposons avoir les trois inégalités pour un certain h et montrons qu'alors on les a toujours pour $h + 1$. On a, en utilisant la définition de x_{h+1} et les hypothèses de récurrence :

$$\begin{aligned} v_u(x_{h+1}) &= v_u(x_h(1 - f(x_h))) \\ &= v_u(x_h) + v_u(1 - f(x_h)) \\ &= \min(v_u(1), v_u(f(x_h))) \\ &= 0 \end{aligned}$$

$$\begin{aligned} v_u(x_{h+1} - 1) &= v_u(x_h - x_h f(x_h) - 1) \\ &\geq \min\left(v_u(x_h - 1), v_u(x_h) + v_u(f(x_h))\right) \\ &\geq \min\left(l, (h+1)l\right) \geq l \end{aligned}$$

$$\begin{aligned} v_u(f(x_{h+1})) &= v_u(f(x_h - x_h f(x_h))) \\ &= v_u(f(x_h - f(x_h) + f(x_h) - x_h f(x_h))) \\ &= v_u(f(x_h) - f(f(x_h)) - f((x_h - 1)f(x_h))) \\ &= v_u(f((x_h - 1)f(x_h))) \\ &\geq v_u((x_h - 1)f(x_h)) \\ &\geq l + (h+1)l = (h+2)l \end{aligned}$$

où on a utilisé le fait que f est un opérateur linéaire et $v_u(f(y)) \geq v_u(y)$ puisque f ne sélectionne que la partie avec les indices positifs donc le minimum sur ceux-ci est forcément plus grand ou égal au minimum sur tous les indices initiaux de la série. On a alors nos trois résultats pour tout h. On en déduit que

$$v_u(x_{h+1} - x_h) = v_u(-x_h f(x_h)) = v_u(x_h) + v_u(f(x_h)) \geq (h+1)l.$$

Ce qui signifie que $v_u(x_{h+1} - x_h) \to +\infty$ si $h \to +\infty$. Alors la suite $(x_h)_{h\geq 0}$ converge vers une limite $x \in S$ puisque S est complet pour la valuation v_u par le lemme 3.18.

Par construction, $f(x) = 0$ car $f(x) = f(\lim_{h\to+\infty} x_h) = \lim_{h\to+\infty} f(x_h) = 0$ vu que $v_u(f(x_h)) \geq (h+1)l \to +\infty$, donc x n'a pas de puissances strictement positives de z. Par induction sur h, $z^e x_h$ n'a pas de puissances négatives de z. En effet, pour $h = 0$, $z^e x_0 = c_e^{-1} P(z)$ qui n'a pas de puissances négatives puisque P est un polynôme. Induction : si $z^e x_h$ n'a pas de puissances négatives de z, comme $z^e x_{h+1} = (z^e x_h)(1 - f(x_h))$ et que les deux facteurs n'ont pas de puissances négatives de z, alors $z^e x_{h+1}$ non plus. Alors, $z^e x$ n'a pas non plus de puissances négatives de z et est donc un polynôme en z de degré exactement e. En effet, x n'avait aucune puissance strictement positive de z et le multiplier par z^e décale toutes les puissances négatives donc le degré est plus petit ou égal à e et c'est exactement e car le terme indépendant de x_0 est $c_e^{-1} c_e = 1$. Comme $x \in S$, ses coefficients respectent les conditions sur les pentes. Les coefficients de $z^e x = \sum_{j=0}^{e} r_j z^j$ sont des décalages de ceux de $x = \sum_j a_j z^j$, le coefficient j de $z^e x$ correspond au coefficient $j - e$ de x avec $j - e \leq 0$. On a alors $v(a_{j-e}) + s(j-e) \geq 0$ ce qui implique $v(r_j) \geq -s(j-e)$. Regardons les pentes m du polygone de Newton de $z^e x$ reliant les points $(-j, v(r_j))$ au point extrémité $(-e, v(r_e))$. On a $m = \frac{v(r_e) - v(r_j)}{j-e}$. Or, on sait que $v(r_e) = v(1) = 0$ et $v(r_j) \geq -s(j-e)$, on trouve alors $v(r_e) - v(r_j) \leq s(j-e)$ c'est-à-dire $\frac{v(r_e) - v(r_j)}{j-e} \geq s$. Les pentes reliant n'importe quel point au point extrémité sont toutes plus grandes ou égales à s et comme le polygone de Newton prend l'enveloppe convexe inférieure des points, on a bien que toutes les pentes du polygones de $z^e x$ sont plus grandes ou égales à s.

De l'autre côté, on a $x = x_0(1 - f(x_0))(1 - f(x_1))\ldots$ tel que $x_0 x^{-1}$ a uniquement des puissances positives de z. Cependant, $z^{e-d} x_0 x^{-1}$ n'a pas de puissances positives de z puisque $z^{e-d} x_0 x^{-1} = z^{e-d}(c_e^{-1} z^{-e} P(z)) x^{-1} = c_e^{-1} z^{-d} P(z) x^{-1}$. Le polynôme $z^{-d} P(z)$ n'a aucune puissance strictement positive de z puisque $\deg(P) = d$ et x^{-1} n'a pas non plus de puissances positives sinon celles-ci ne seraient pas compensées dans le produit $x x^{-1}$ ce qui contredit la définition d'inverse. On en tire que $x_0 x^{-1}$ est un polynôme en z de degré exactement $d - e$, notons-le $\sum_{j=0}^{d-e} q_j z^j$. On a $x_0 x^{-1} \in S$ car $x_0 \in S$ et comme

$v_u(x-1) > 0$, on peut écrire $x = 1+\varepsilon$ avec $v_u(\varepsilon) > 0$ et x^{-1} est alors la série $\sum_{n=0}^{+\infty}(-\varepsilon)^n$ qui converge dans S donc $x^{-1} \in S$. Les indices j du polynôme x_0x^{-1} sont tous positifs donc on a $v(q_j) + rj \geq 0$. On regarde les pentes reliant les points $(-j, v(q_j))$ au point origine $(0, v(q_0))$. On a $m = \frac{v(q_j)-v(q_0)}{-j}$. Le terme indépendant q_0 de x_0x^{-1} est 1 donc on peut écrire $v(q_j) - v(q_0) \geq -rj$ et en divisant les deux termes par $-j$ qui est négatif on obtient $m = \frac{v(q_j)-v(q_0)}{-j} \leq \frac{-rj}{-j} = r$. Les pentes reliant n'importe quel point au point origine sont toutes plus petites ou égales à r. Par convexité du polygone de Newton, toutes les pentes du polygone de Newton de x_0x^{-1} sont plus petites ou égales à r.

On obtient la factorisation $P = QR$ avec $Q(z) = c_e x_0 x^{-1}$ et $R(z) = z^e x$ avec les conditions sur les pentes voulues. □

Corollaire 3.20. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v. Alors, tout polynôme monique P sur K admet une unique factorisation $Q_1 \dots Q_n$ en polynômes moniques sur K telle que chaque Q_i est pur de pente s_i et $s_1 < s_2 < \dots < s_n$.*

Démonstration. On a l'existence en itérant le lemme 3.19. Pour l'unicité, soit $P \in K[z]$ un polynôme monique. Supposons qu'il existe deux factorisations en polynômes moniques purs $P = Q_1 \cdots Q_n = Q'_1 \cdots Q'_m$ où, pour chaque facteur, les pentes associées sont strictement croissantes ($s_1 < s_2 < \cdots < s_n$ pour les Q_i, et $s'_1 < s'_2 < \cdots < s'_m$ pour les Q'_j). Par le corollaire 3.13, on sait que la multiplicité de r comme pente de P est égale à la somme des degrés des Q_i (*resp.* Q'_i) tel que Q_i (*resp.* Q'_i) a une pente r. Or, comme les pentes sont strictement croissantes dans les factorisations de P, si r est une pente de P alors il existe un unique Q_i (*resp.* Q'_i) de pente r. Comme toutes les pentes de P doivent se trouver dans les factorisations et vu la croissance stricte de celles-ci, on a forcément $m = n$ et $s_i = s'_i$ pour tout i. L'égalité $Q_i = Q'_i$ découle alors de l'unicité de la factorisation dans $K[z]$. En effet, soit $P = \prod_j R_j$ l'unique décomposition de P en facteurs irréductibles moniques dans $K[z]$. Puisque chaque R_j est irréductible, il est pur et possède une unique pente s_i. Par le corollaire 3.13, le produit de tous les R_j ayant pour pente s_i est un polynôme pur de pente s_i. De plus, pour chaque pente s_i, le polynôme Q_i (*resp.* Q'_i) est un polynôme pur dont le degré est égal à la multiplicité de la pente s_i dans P. Par conséquent, Q_i et Q'_i doivent tous deux être égaux au produit de tous les facteurs irréductibles R_j ayant pour pente s_i, d'où $Q_i = Q'_i$. □

Définition 3.21. On appelle la factorisation donnée par le corollaire 3.20, la factorisation par pentes du polynôme P.

On va maintenant appliquer ces concepts théoriques à l'anneau des polynômes tordus.

Remarque 3.22. Pour cette partie, on va utiliser le fait que pour K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$, la valuation v s'étend de façon unique sur toute clôture algébrique de K.

Lemme 3.23. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v. Soit P un polynôme monique et additif sur K et soit $Q_1 \dots Q_n z^{p^d}$ sa factorisation par pentes. Alors, $Q_n z^{p^d}$ est aussi additif.*

Démonstration. Soit L une clôture algébrique de K. Soient $s_1, \ldots, s_n$ les pentes de P et soit V l'ensemble des zéros de P dans L. Alors les valuations des éléments non nuls de V sont précisément $s_1, \ldots, s_n$ par la remarque 3.9.

De plus, Q_n est un polynôme pur de pente s_n et z^{p^d} a pour racine 0 de valuation ∞. On obtient qu'un élément $x \in V$ est un zéro de $Q_n z^{p^d}$ si et seulement si $v(x) \geq s_n$. Comme P est un polynôme additif, l'ensemble V est un $\mathbb{F}_p$-espace vectoriel. Si on note $W = \{x \in V : v(x) \geq s_n\}$, cet ensemble est un sous-ensemble de V stable par multiplication par un scalaire et par addition. Si $x, y \in W$, alors $v(x) \geq s_n$ et $v(y) \geq s_n$ et par les propriétés de valuation, $v(x+y) \geq \min(v(x), v(y)) \geq s_n$ d'où $x + y \in W$. De même, si $\lambda \in \mathbb{F}_p$ et $x \in W$, alors $v(\lambda x) = v(\lambda) + v(x) = v(x) \geq s_n$ car $v(\lambda) = 0$. L'ensemble W est alors un sous-espace vectoriel de V et le polynôme $Q_n z^{p^d}$ est donc additif par le lemme 1.20. □

Définition 3.24. Soit $P(F)$ un polynôme tordu sur K. Pour $r \in \mathbb{Q}$, on dit que $P(F)$ est pur de pente r si P a un terme indépendant non nul et le polynôme classique associé $\frac{P(F)(z)}{z}$ est pur de pente r. On dit conventionnellement que toute puissance de F est pure de pente ∞.

Exemple 3.25. Considérons le polynôme $P(F) = F - t \in \mathbb{F}_p((t))\{F\}$. Alors $P(F)$ est pur de pente $\frac{1}{p-1}$ car le terme indépendant de P est $-t$ qui est non nul et $\frac{P(F)(z)}{z} = z^{p-1} - t$ est pur de pente $\frac{v(-t)-v(1)}{p-1-0} = \frac{1}{p-1}$.

Proposition 3.26. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v et soit $P(F)$ un polynôme tordu monique sur K. Alors, il existe une factorisation $Q_1 \ldots Q_n$ de P en polynômes tordus moniques sur K, dans laquelle chaque Q_i est pur d'une certaine pente.*

Démonstration. Regardons tout d'abord le polynôme $P(F)(z)$, c'est un polynôme monique et additif sur K donc par le corollaire 3.20, il existe une factorisation de $P(F)(z)$ en polynômes moniques $Q_1 \ldots Q_n z^{p^d}$ telle que chaque Q_i est pur de pente s_i et $s_1 < s_2 < \ldots < s_n$. Par le lemme 3.23, on a que $Q_n z^{p^d}$ est aussi un polynôme additif. On peut alors l'écrire sous la forme $Q_n(z) z^{p^d} = R(F)(z)$ pour un polynôme tordu $R(F)$. On peut écrire $R(F) = (F^m + a_{m-1}F^{m-1} + \ldots + a_0)F^d$. On peut supposer que $d = 0$ sans perte de généralité.

Par la proposition 3.7, comme $\ker(R) \subset \ker(P)$ et que le terme indépendant de R est non nul (sinon on pourrait sortir une puissance de F et d serait alors différent de 0), on peut factoriser $P(F)$ sous la forme $P(F) = P_1(F)R(F)$ pour un $P_1(F)$ de plus petit degré que $P(F)$. Si $d \neq 0$, il suffit de recoller les termes de pentes infinies et garder le même résultat.
En itérant l'argument, on a la conclusion. □

Nous définissons le produit tensoriel d'espaces vectoriels. De plus amples informations sont données dans [6].

Définition 3.27. A tout couple d'espaces vectoriels E, F, on peut associer un troisième espace vectoriel G et une application bilinéaire T de $E \times F$ dans G possédant les propriétés suivantes :

a) $T(E \times F)$ engendre G. C'est-à-dire tout élément de G est somme d'éléments de la forme $T(x, y)$, $x \in E, y \in F$

b) pour toute base $(e_i)_{i\in I}$ de E et toute base $(f_j)_{j\in J}$ de F, la famille $(T(e_i, f_j))$ est une base de G.

L'espace G est appelé produit tensoriel de E et F et noté $E \otimes F$. On note $x \otimes y = T(x, y)$. Les éléments de $E \otimes F$ sont appelés tenseurs, ceux de la forme $x \otimes y$ sont dits décomposables de sorte que tout tenseur s'écrit comme somme de tenseurs décomposables.

Exemple 3.28. Si on prend $E = \mathbb{R}^2 = F$, le produit tensoriel de E et F est $E \otimes F = \mathbb{R}^2_2$ et l'application $T : E \times F \to E \otimes F$ $(x, y) \mapsto xy^T$. C'est-à-dire que pour tout élément $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in E$ et tout élément $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in F$, on a

$$x \otimes y = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} y_1 & y_2 \end{pmatrix} = \begin{pmatrix} x_1y_1 & x_1y_2 \\ x_2y_1 & x_2y_2 \end{pmatrix}$$

On peut vérifier les propriétés de T :

a) Toute matrice 2×2 peut être écrite comme somme d'éléments de la forme $T(x, y)$ pour $x \in E, y \in F$. Par exemple, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est la somme de $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

b) Soient $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ une base canonique de $E = F$. Les produits $e_i \otimes e_j$ pour $i, j \in \{1, 2\}$ sont donnés par

$$e_1 \otimes e_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad e_2 \otimes e_1 \qquad = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$e_1 \otimes e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad e_2 \otimes e_2 \qquad = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Ces quatre matrices forment bien la base canonique de $\mathbb{R}^2_2$ et on a bien $\dim(E \otimes F) = \dim E \times \dim F = 2.2 = 4$.

Remarque 3.29. Lorsque l'on souhaite préciser que E et F sont des espaces vectoriels sur un corps K, on note souvent l'espace produit $E \otimes_K F$. Cette notation rappelle que les scalaires de K commutent avec le produit tensoriel, c'est-à-dire que pour tout $\lambda \in K$, on a :

$$(\lambda x) \otimes y = x \otimes (\lambda y) = \lambda(x \otimes y)$$

Dans le cas qui nous intéresse et qu'on va utiliser, le produit tensoriel se simplifie. En effet, on va considérer le produit tensoriel par une extension de champs, ce qui simplifie notre produit tensoriel à une extension des scalaires.

Définition 3.30. Soit K un corps et L une extension de K. Pour tout K-espace vectoriel V, on appelle extension des scalaires de V à L (ou changement de base), notée V_L, le produit tensoriel de K-espaces vectoriels défini par $V_L = V \otimes_K L$. Cet espace V_L est muni d'une structure unique de L-espace vectoriel induite par la multiplication sur le second facteur, définie par $\lambda(v \otimes \beta) = v \otimes (\lambda\beta)$ pour tous $\lambda, \beta \in L$ et $v \in V$. En s'appuyant sur la propriété b) de la définition 3.27, si $(\epsilon_i)_{i\in I}$ est une base de V sur K, alors la famille $(\epsilon_i \otimes 1)_{i\in I}$ forme une base de ce nouveau L-espace vectoriel V_L. Tout élément de V_L s'écrit alors de manière unique comme une combinaison linéaire à coefficients dans L sous la forme $\sum_{i\in I} \epsilon_i \otimes \alpha_i$ où $\alpha_i \in L$.

Dans le cas qui nous intéresse, on considère un corps K qui est un sous-corps de $\mathbb{F}_q((t^{\mathbb{Q}}))$ et $\mathbb{F}_{q'}$ une extension de $\mathbb{F}_q$. Dans ce cas, faire le produit tensoriel $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ revient simplement à étendre le corps des constantes de $\mathbb{F}_q$ à $\mathbb{F}_{q'}$. Concrètement, les éléments de K sont des séries à coefficients dans $\mathbb{F}_q$, les éléments de $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ sont des séries de même nature, mais dont les coefficients s'autorisent désormais à vivre dans l'extension finie $\mathbb{F}_{q'}$.

Remarque 3.31. Le produit tensoriel considéré préserve la p-quasi-automaticité du corps de base. En effet, si une série de $\mathbb{F}_q((t^{\mathbb{Q}}))$ est p-quasi-automatique, l'extension des scalaires à une extension finie $\mathbb{F}_{q'}$ revient à introduire des combinaisons linéaires finies à coefficients dans $\mathbb{F}_{q'}$, ce qui préserve la structure d'automate et donc l'automaticité de la série.

Proposition 3.32. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$ complet pour la valuation v et soit $P(F)$ un polynôme tordu monique sur K, pur de pente 0. Alors, le polynôme $P(F)(z)$ se factorise complètement en facteurs linéaires sur $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ pour une certaine puissance q' de q.*

Démonstration. Notons $P(F) = \sum_{i=0}^{d} c_i F^i$ avec $c_d = 1$. Comme P est pur de pente 0, on doit avoir $\frac{v(c_d)-v(c_0)}{-d+0} = 0$ ce qui implique que $v(c_0) = 0$ et $v(c_i) \geq 0$ pour $1 \leq i \leq d-1$. Soit $a_i \in \mathbb{F}_q$ le terme indépendant de c_i, alors le polynôme $\sum_{i=0}^{d} a_i z^{p^i}$ a son terme indépendant a_0 non nul car $v(c_0) = 0$ donc le polynôme ne possède que des racines simples dans la clôture algébrique de $\mathbb{F}_q$, ces racines appartiennent donc à une extension finie de la forme $\mathbb{F}_{q'}$ pour une puissance q' de q. Il en a alors p^d distinctes dans $\mathbb{F}_{q'}$. Comme ces racines n'appartiennent pas nécessairement au corps de base K, on introduit le produit tensoriel $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ plutôt que de plonger globalement l'étude dans le grand corps des séries $\mathbb{F}_{q'}((t^{\mathbb{Q}}))$. Soit $r \in \mathbb{F}_{q'}$ une racine non nulle de $\sum_{i=0}^{d} a_i z^{p^i}$. Regardons le décalage $z + r$,
$P(F)(z+r) = \sum_{i=0}^{d} c_i (z+r)^{p^i} = \sum_{i=0}^{d} c_i z^{p^i} + \sum_{i=0}^{d} c_i r^{p^i}$. Comme on a pris r comme étant une racine de $\sum_{i=0}^{d} a_i z^{p^i}$, le terme constant du terme indépendant de $P(F)(z+r)$ est nul. Le polynôme $P(F)(z+r)$ a alors un terme indépendant de valuation strictement positive et son terme de plus haut degré a toujours une valuation nulle. On sait alors que $P(F)(z+r)$ possède au moins une pente strictement positive donc une racine e de valuation strictement positive. On a alors trouvé une racine $r' = e + r$ de $P(F)(z)$ avec $v(r'-r) > 0$, $r' \in K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$. L'existence de cette racine implique que le polynôme classique $P(F)(z)$ admet le facteur linéaire $(z - r')$ dans sa factorisation.

En itérant le même argument, on peut trouver une factorisation complète de $P(F)(z)$ en facteurs linéaires dans $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ puisque les racines de $\sum_{i=0}^{d} a_i z^{p^i}$ sont toutes distinctes, on trouve bien p^d facteurs linéaires distincts. □

Corollaire 3.33. *Soit K un sous-champ de $\mathbb{F}_q((t^{\mathbb{Q}}))$, contenant toutes les puissances fractionnaires de t et complet pour la valuation v et soit $P(F)$ un polynôme tordu monique sur K. Alors, pour une puissance q' de q, il existe une factorisation $Q_1 \dots Q_n$ de P en polynômes tordus moniques linéaires sur $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$.*

Démonstration. Procédons par induction sur le degré de P.

Il suffit de montrer que si P n'est pas linéaire, alors il est multiple à gauche d'un polynôme tordu linéaire sur $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ pour un q'. Par la proposition 3.26, P se factorise en polynômes tordus moniques et purs d'une certaine pente sur K. On peut alors se réduire au cas où P est pur d'une certaine pente s, quitte à travailler sur un des facteurs et procéder par récurrence.

On peut encore se réduire au cas où P est pur de pente 0. En effet, si P est pur de pente s, comme K contient toutes les puissances fractionnaires de t, on peut trouver un $\lambda \in K$ tel que $v(\lambda) = s$. Alors, en utilisant le changement de variables $z = \lambda.y$ et en normalisant le polynôme obtenu, celui-ci a pour coefficients $c'_i = \frac{c_i \lambda^{p^i}}{c_d \lambda^{p^d}}$ dont la valuation est $v(c'_i) = v(c_i) + p^i s - v(c_d) - p^d s$. Le polynôme P étant pur de pente s, tous les points du polygone se trouvent soit sur, soit au dessus du segment de pente s, la valeur de $v(c_i) + p^i s$ est constante pour tous les points du segment et strictement plus grande que cette constante pour les points au dessus de celui-ci. On obtient finalement $v(c'_i) = 0$ pour les points de P qui étaient sur le segment de pente s et $v(c'_i) > 0$ pour les autres points, ce qui signifie que P est pur de pente 0.

Par la proposition 3.32, $P(F)(z)$ se factorise complètement en facteurs linaires sur $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ pour une puissance q' de q. Choisissons un $\mathbb{F}_p$-sous-espace de l'ensemble des racines de $P(F)(z)$ de dimension 1. Par le lemme 1.20, cet ensemble forme les racines d'un polynôme additif monique linéaire $Q(F)(z)$ sur $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ pour un polynôme tordu $Q(F)$. Pour finir, on a $\ker(Q) \subset \ker(P)$ et $Q(F)(z)$ a p racines distinctes donc $Q(F)$ est un polynôme de la forme $F - \alpha$ avec $\alpha \neq 0$ sinon cela contredirait la condition des racines distinctes. Alors, par la proposition 3.7 il existe un polynôme tordu P_0 tel que $P = P_0 Q$ avec P_0 de plus petit degré que P. Ce qui complète l'induction nécessaire. □

3.3 Un peu de théorie des graphes

Dans cette section, nous étudions quel type d'automate pourrait accepter nos séries de Laurent généralisées. Nous commençons la section avec plusieurs définitions qui nous seront utiles.

Définition 3.34. Soit $M = (Q, \Sigma, \delta, q_0, \Delta)$ un AFD. Etant donné un état $q_1 \in Q$, un état $q \in Q$ est dit accessible depuis q_1 si $\delta^*(q_1, s) = q$ pour un mot $s \in \Sigma^*$, et non accessible depuis q_1 dans le cas contraire.

Si $q_1 = q_0$, on dit simplement que q est accessible ou non accessible.

Remarque 3.35. Tout état q pour lequel un état non accessible est accessible depuis q est lui-même non accessible.

Définition 3.36. Soit M un AFD. Un état $q \in Q$ est dit co-accessible s'il existe un état final accessible depuis q. Si ce n'est pas le cas, on dit que cet état est non co-accessible.

Définition 3.37. On qualifie d'émondé tout AFD qui ne contient aucun état non accessible et non co-accessible.

Remarque 3.38. Tout état accessible depuis un état non co-accessible est non co-accessible. Tout AFD peut toujours être émondé en enlevant ses états non accessibles et non co-accessibles sans changer le langage accepté par celui-ci.

Définition 3.39. Soit M un AFD avec $\Sigma_b = \{0, ..., b-1\}$ comme alphabet. On dit que M est bien formé (resp. bien ordonné) si le langage accepté par M est l'ensemble des représentations valides en base b des éléments d'un sous-ensemble arbitraire (resp. bien ordonné) de S_b.

Définition 3.40. Soit $G = (V, E)$. Un cycle minimal de G est un cycle qui ne passe qu'une seule fois par chaque sommet et dans lequel on ne peut pas trouver de cycle plus petit.

Exemple 3.41. Dans la figure ci-dessous, le cycle $(1, 2, 5, 4, 1)$ est minimal tandis que le cycle $(1, 2, 3, 6, 5, 4, 1)$ ne l'est pas car il contient $(1, 2, 5, 4, 1)$ et le cycle $(2, 3, 6, 5, 2)$ ne l'est pas car il contient $(3, 3)$.

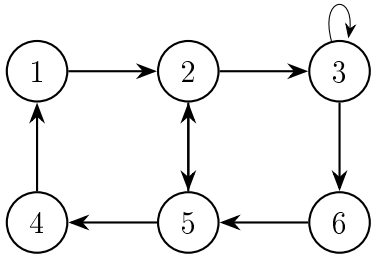


FIGURE 3.2 – Exemple de cycles

Définition 3.42. Un graphe orienté $G = (V, E)$ équipé d'un sommet distingué $v \in V$ est appelé un saguaro enraciné s'il satisfait :

1. Chaque sommet de G est sur au plus un cycle minimal.
2. Il existe des chemins orientés de v à chaque sommet de G.

Dans ce cas, on dit que v est une racine du saguaro.
Un cycle minimal d'un saguaro enraciné est appelé un lobe.
Une arête d'un saguaro enraciné est cyclique si elle est sur un lobe, acyclique sinon.

Exemple 3.43. Voici un exemple de saguaro enraciné. Dans ce cas, v est une racine du saguaro, les arêtes en bleu sont les arêtes cycliques et en rouge celles qui sont acycliques. Le saguaro contient 2 lobes : le cycle (B, C, D, B) et le cycle (E, F, G, H, E).
Chaque sommet est bien sur au plus un cycle minimal et on peut atteindre tous les sommets à partir de la racine v.

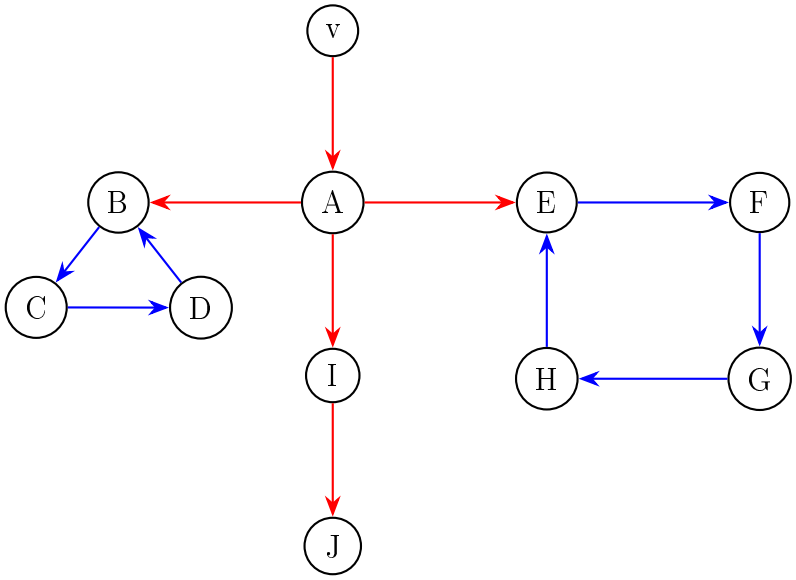


FIGURE 3.3 – Exemple de saguaro enraciné

Définition 3.44. Soit $G = (V, E)$ un saguaro enraciné. Un b-étiquetage approprié de G est une fonction $l : E \to \{0, ..., b-1\}$ avec les propriétés :

1. Si $v, w, x \in V$ et $vw, vx \in E$, alors $l(vw) \neq l(vx)$.
2. Si $v, w, x \in V$, $vw \in E$ est sur un lobe et $vx \in E$ n'est pas sur un lobe, alors $l(vw) > l(vx)$.

Exemple 3.45. La figure 3.4 est un exemple de saguaro enraciné muni d'un 2-étiquetage approprié. En effet, deux arêtes provenant d'un même sommet ont des valeurs distinctes et l'arête cyclique a une plus grande valeur que celle acyclique.

Théorème 3.46. *Soit M un AFD avec Σ_b comme alphabet, émondé et bien formé. Alors, M est bien ordonné si et seulement si pour tout état q post-virgule, le sous-graphe G_q du graphe de transition consistant en les états accessibles depuis q et co-accessibles est un saguaro enraciné de racine q, équipé d'un b-étiquetage.*

Démonstration. Commençons par supposer que M est bien ordonné. Soit q un état post-virgule de M. Alors, comme M est bien formé, le langage accepté par celui-ci est l'ensemble des représentations valides en base b d'un sous-ensemble de S_b. On en déduit que toute transition du sous-graphe G_q est étiquetée par des éléments de $\{0, \ldots, b-1\}$ puisqu'une représentation valide ne peut pas avoir plusieurs virgules.

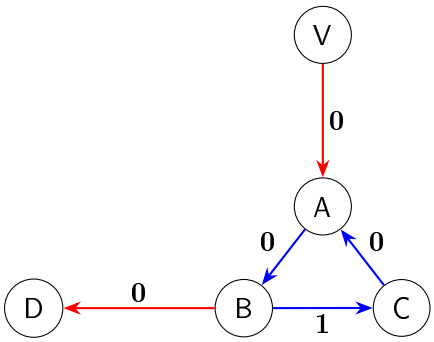


FIGURE 3.4 – Exemple de b-étiquetage approprié

Supposons qu'à partir de q on ait le choix entre une arête qui fait partie d'un cycle étiquetée par $s \in \{0, \dots, b-1\}$ et une autre arête qui ne fait pas partie d'un cycle vers un état co-accessible étiquetée par $s' \in \{0, \dots, b-1\}$, avec $s' \neq s$. Montrons que $s > s'$, ce qui prouvera la deuxième condition pour avoir un étiquetage approprié.
Soit $w \in \Sigma^*$ de longueur minimale tel que $\delta^*(q, sw) = q$, c'est-à-dire le mot obtenu en empruntant une fois le cycle au départ de q et après avoir lu s. Comme M est émondé, q est accessible donc on peut trouver un $w_0 \in \Sigma^*$ tel que $\delta^*(q_0, w_0) = q$.
Comme $\delta(q, s')$ est un état co-accessible, on peut trouver $w_1 \in \Sigma^*$ tel que $\delta^*(q, s'w_1) \in F$.
Alors, tous les mots $w_0 s' w_1$, $w_0 sws' w_1$, $w_0 swsws' w_1$, ... sont acceptés par M.
Procédons par l'absurde et supposons que $s' > s$. Alors, les mots ci-dessus acceptés par M forment les représentations valides en base b d'une suite décroissante infinie, ce qui contredit le fait que M est bien ordonné. En effet, comme $s' > s$, alors au premier rang où ils diffèrent, le premier nombre a un chiffre plus grand que le suivant dans sa représentation en base b, il est donc lui même plus grand. On conclut qu'on doit forcément avoir $s > s'$, l'option $s = s'$ étant rejetée par le déterminisme de M.
Cette dernière conclusion implique directement que le graphe G_q en question est un saguaro enraciné puisqu'on ne peut pas avoir un sommet sur deux cycles minimaux. Si tel était le cas, on pourrait appliquer le même raisonnement avec s, s' pour les deux premiers étiquetages des boucles, qui sont différents par le déterminisme de M. On pourrait alors les comparer et construire une suite infinie décroissante en bouclant sur la boucle de plus petit étiquetage.
Finalement, on a bien que G_q est un saguaro enraciné équipé d'un b-étiquetage approprié.

Passons maintenant à la condition suffisante et supposons que G_q est un saguaro enraciné muni d'un b-étiquetage approprié. Procédons par l'absurde et supposons que le langage accepté par M inclut une suite infinie décroissante notée $x_1, x_2, \dots$.
On dit que le m^e chiffre de la représentation en base b de x_i (en lisant de gauche à droite) est statique si $x_i, x_{i+1}, \dots$ ont tous le même m^e chiffre. Dans ce cas, la représentation de chaque x_i commence avec un segment initial, possiblement vide, de termes statiques et le nombre de termes statiques tend vers l'infini si i tend vers l'infini. Alors, il existe une unique suite infinie $s_1, s_2, \dots$ d'éléments de Σ telle que chaque segment initial de termes statiques apparaissant dans la représentation en base b d'un x_i a la forme $s_1 \dots s_m$ pour un

m dépendant de i. Le mot $s_1 s_2 \dots$ représente le mot limite de la suite des repésentations des x_i.
Comme on a une suite décroissante, le nombre de termes pré-virgules dans la représentation de chaque x_i est au plus le nombre de termes pré-virgules dans la représentation en base b de x_1. On en tire que la suite $s_1, s_2, \dots$ doit obligatoirement inclure une (et une seule) virgule. Définissons $q_m = \delta^*(q_0, s_1 \dots s_m)$. Alors, chaque q_m est co-accessible puisque $s_1 \dots s_m$ est la partie statique d'un des x_i dans le langage de M, donc on peut la compléter pour arriver dans un état final. De plus, par la remarque sur le nombre fini de termes pré-virgules dans les représentations des x_i, chaque q_m est aussi post-virgule pour m suffisamment grand.
Remarquons que seul un nombre fini de transitions post-virgules de q_m vers q_{m+1} peut être acyclique, sinon pour lire un mot infini on devrait obligatoirement repasser par des transitions déjà vues avant et elles feraient alors par définition partie d'un cycle.
Soit x_i dans la suite décroissante infinie dont les m premiers chiffres sont tous statiques, avec m assez grand tel que q_m soit post-virgule et la transition de q_n à q_{n+1} soit cyclique pour tout $n \geq m$ dans la représentation limite.
Soit $t_1 t_2 \dots \in \Sigma^*$ la représentation en base b de x_i. Comme la suite est décroissante et que la représentation de x_i n'est pas l'élément limite, il existe un plus petit entier $n > m$ tel que $s_n \neq t_n$ et cet entier n satisfait $s_n < t_n$. Cependant, la transition de q_n à q_{n+1} est cyclique donc l'inégalité $s_n < t_n$ contredit la définition de b-étiquetage approprié puisque t_n doit se trouver sur une arête acyclique par définition du saguaro enraciné.
On conclut qu'il ne peut exister de suite infinie décroissante. Donc M est bien ordonné. □

Remarque 3.47. Ce résultat nous permet d'affirmer que les automates associés à des saguaros enracinés muni d'un b-étiquetage approprié reconnaissent des séries de Laurent généralisées. En effet, ceux-ci reconnaissent des représentations valides en base b et le fait que M soit bien ordonné traduit la condition du support pour les séries de Laurent généralisées.

3.4 Stabilité du produit

Nous avons désormais les outils nécessaires pour démontrer la stabilité du produit de séries automatiques. Pour ce faire, nous avons besoin du lemme suivant.

Lemme 3.48. *Soit $n \in \mathbb{N}^*$ un naturel non nul. Soit $M = (Q, \Sigma, I, F, \delta)$ un automate fini non déterministe et $f : \Sigma^* \to \mathbb{Z}/n\mathbb{Z}$ la fonction qui, à un mot $w \in \Sigma^*$, associe le nombre de chemins acceptants (partant d'un état initial et arrivant à un état final après avoir lu w) réduit modulo n. Alors f est une fonction automatique.*

Démonstration. On construit un automate fini déterministe complet à sortie $M' = (Q', \Sigma', i', \delta', \Delta, \tau)$. Soit Q' l'ensemble des fonctions de Q dans $\mathbb{Z}/n\mathbb{Z}$ et $\Sigma' = \Sigma$. On définit $i' : Q \to \mathbb{Z}/n\mathbb{Z}$ la fonction qui associe 1 aux états initiaux et 0 aux autres états. On définit la fonction de transition de M' comme suit, si $g : Q \to \mathbb{Z}/n\mathbb{Z}$ et si $s \in \Sigma$,

alors $\delta'(g,s) : Q \to \mathbb{Z}/n\mathbb{Z}$ est la fonction donnée par $\delta'(g,s)(q) = \sum_{\delta(q',s)=q} g(q')$ où l'on somme sur l'ensemble des états q' de M qui aboutissent dans q lorsqu'on lit la lettre s dans l'automate M. La fonction de sortie est $\tau : Q' \to \mathbb{Z}/n\mathbb{Z} \quad g \mapsto \sum_{q\in F} g(q)$.

L'automate M' ainsi construit est déterministe. Pour n'importe quel mot w, il aboutit dans un état g_w qui stocke en mémoire le nombre de chemins arrivant dans chaque état de M. La fonction de sortie τ extrait alors la somme de ces chemins pour les états terminaux. Ainsi, $f(w) = \tau(g_w)$, ce qui prouve que f est une fonction automatique. □

Théorème 3.49. *Soient $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ p-automatiques (*resp. *p-quasi-automatiques), alors xy est p-automatique (*resp. *p-quasi-automatique).*

Démonstration. Pour cette démonstration on se place dans le sens de lecture de droite à gauche, c'est-à-dire que les zéros de tête sont les chiffres les moins significatifs.

On montre le cas automatique et on déduit le cas quasi-automatique en se ramenant à une série automatique avec un décalage.

Ecrivons x et y comme une $\mathbb{F}_q$-combinaison linéaire de séries généralisées de la forme $\sum_{i\in S} t^i$ pour un $S \subset S_p$. Par le lemme 2.6, si le produit de deux séries de cette forme est toujours p-automatique alors xy le sera aussi. Sans perte de généralité, nous pouvons dès lors supposer que $x = \sum_{i\in A_1} t^i$ et $y = \sum_{i\in A_2} t^i$. Notre but est alors de montrer que $xy = \sum_k c_k t^k$ est p-automatique, où

$$c_k = \#\{(i,j) \in A_1 \times A_2 : i + j = k\} \pmod p.$$

Cette série est p-automatique s'il existe un automate qui, à partir de la représentation en base p d'un indice k, calcule le nombre de paires (i,j) dont la somme fait k et rend ce résultat modulo p. Commençons par construire un automate qui accepte les paires de représentations en base p de couples d'indices de $A_1 \times A_2$. Soit S le sous-ensemble de $\Sigma_p^* \times \Sigma_p^*$ consistant en les paires (w_1, w_2) avec les propriétés suivantes :

a) w_1 et w_2 sont des mots de même longueur.

b) w_1 et w_2 ont chacun une unique virgule, à la même position.

c) Après avoir enlevé les zéros de tête et de queue, w_1 et w_2 deviennent les représentations miroirs valides en base p de certains éléments $i, j \in S_p$.

d) La paire (i,j) appartient à $A_1 \times A_2$.

Par le point a), on peut voir S comme un langage sur $\Sigma_p \times \Sigma_p$, qui de plus est régulier. Soit $M = (Q, \Sigma, \delta, q_0, F)$ un AFD qui accepte S, avec $\Sigma = \Sigma_p \times \Sigma_p$. C'est-à-dire que M accepte les paires (w_1, w_2) pour lesquelles w_i est une représentation en base p d'un élément de A_i, $i \in \{1,2\}$.

Construisons maintenant un automate qui à un entier k donné, va compter le nombre de paires possibles $(i,j) \in A_1 \times A_2$ telles que leur somme fait k. On définit un automate fini non déterministe (AFND) $M' = (Q', \Sigma', \delta', q_0', F')$ dans lequel δ' prend des valeurs multiples. Posons

- $Q' = Q \times \{0,1\}$, où $\{0,1\}$ désigne l'ensemble des retenues possibles venues des sommes précédentes

- $\Sigma' = \Sigma_p$
- $q'_0 = (q_0, 0)$
- $F' = F \times \{0\}$
- δ' est défini comme suit : pour $(q, i) \in Q'$ et $s \in \{0, \ldots, p-1\}$, on regarde chaque paire $(t, u) \in \{0, \ldots, p-1\} \times \{0, \ldots, p-1\}$ telle que s peut être obtenu par la somme de t, u et la retenue actuelle i, c'est-à-dire satisfaisant $t + u + i = s + p.i'$. Pour chacune des paires trouvées, $\delta'((q, i), s) = (q', i')$ où $q' = \delta(q, (t, u))$ et i' est la nouvelle retenue. Pour $(q, i) \in Q'$ et s égal à la virgule, on a $\delta((q, i), s) = (q', i)$ si $\delta(q, (s, s)) = q'$.

Supposons que w est un mot qui, après le retrait des zéros de tête et de queue, est la représentation miroir valide en base p d'un $z \in S_p$. Alors, le nombre de chemins acceptant w dans M' est égal au nombre de paires $(w_1, w_2) \in S$ dont la somme en base p avec retenue fait w, avec ses zéros de tête et de queue. Alors la fonction qui rend le nombre de chemin acceptant w dans M' modulo p est acceptée par un automate fini par le lemme 3.48.

Montrons à présent que l'automate est stable pour l'ajout de zéros de tête. Supposons que w commence par m zéros de tête, pour un m plus grand que le nombre d'états de M. Alors, tous w_1, w_2 dont la somme fait w doivent commencer par des zéros de tête. En effet, si ce n'était pas le cas, en exécutant $(w_1, w_2) \in S$ dans M certains états devraient se répéter durant les m premiers termes. Soient (b_1, b_2) les mots qui mènent pour la première fois dans un état déjà rencontré, soient (m_1, m_2) les mots entre la première et la deuxième itération d'état répété et soient (e_1, e_2) le reste des mots. Alors, $b_i e_i, b_i m_i e_i, b_i m_i m_i e_i, \ldots$ sont des représentations miroir en base p, avec possiblement des zéros de queue mais pas de tête, d'éléments $z_{0,i}, z_{1,i}, \ldots$ de A_i. De plus, ces nombres sont tous distincts : si b_i n'est pas vide, alors b_i commence avec un chiffre non nul tandis que si b_i est vide, alors m_i commence avec un chiffre non nul puisque w_1 et w_2 ne commencent pas par des zéros de tête.

Vérifions que pour tout j, on a $z_{j,0} + z_{j,1} = z$, ce qui signifie que peu importe le nombre de fois qu'on utilise la boucle m_i, la valeur de la somme reste constante et égale à z. C'est effectivement le cas car comme w commence avec m zéros et que $w_1 + w_2 = w$, on sait que les m premiers termes se somment à 0 et ces m premiers termes se retrouvent dans la portion $b_i m_i$. Comme w_1 et w_2 ne commencent pas par des zéros, il doit y avoir une retenue qui est propagée tout le long du bloc de 0 créé. On peut alors retirer le tronçon ou le répéter à volonté sans changer la valeur de la représentation en base p de la somme.

On a alors une infinité de paires $(z_{j,0}, z_{j,1})$ dont la somme fait z donc une des deux suites $z_{0,i}, z_{1,i}, \ldots$ est une suite infinie décroissante, ce qui est impossible car A_i est bien ordonné. On conclut que si w a m zéros de tête alors w_1 et w_2 commencent aussi par des zéros de tête. Le nombre de chemins acceptants de w est alors stable par ajout de zéros de tête, pour autant que w ait déjà m zéros de tête.

Il s'en suit que la fonction qui, à une représentation miroir valide en base p d'un nombre $k \in S_p$, associe la réduction modulo p du nombre de façons d'écrire $k = i + j$ avec $i \in A_1$ et $j \in A_2$ est automatique : on peut le calculer en ajoutant m zéros de tête et un zéro de queue à la représentation miroir puis exécuter le résultat dans M'.

Alors, xy est p-automatique, comme souhaité. □

Exemple 3.50. Regardons un exemple simple pour comprendre le fonctionnement des automates M et M'. Prenons la base 2 et les séries $x = \sum_{i\in\{1,2\}} t^i$ et $y = \sum_{j\in\{1\}} t^j$. Le produit est $xy = \sum_{i\in\{2,3\}} t^i$.

L'automate M est l'automate produit d'un automate M_1 qui accepte les représentations miroirs en base 2 de $A_1 = \{1, 2\}$ et de l'automate M_2 qui accepte les représentations miroirs en base 2 des éléments de $A_2 = \{1\}$. C'est-à-dire que M_1 accepte uniquement les mots de la forme $0^*, 10^*$ et M_2 ceux de la forme $0^*, 10^*$ et $0^*, 010^*$. L'automate M est représenté à la figure 3.5.

L'automate M' est l'automate produit de M avec l'automate I qui calcule les retenues possibles. L'automate I est représenté à la figure 3.6 et l'automate M' à la figure 3.7.

Cherchons le coefficient de t^2 dans le produit. En base 2, 2 se représente par 10 qu'on renverse en miroir et à laquelle on ajoute 2 zéros de tête et 1 zéro de queue, ce qui donne 00.010 à donner en entrée de M'.

Le seul chemin qui mène à l'état accepteur est celui qui lit les paires suivantes : $(0, 0) \to (0, 0) \to (., .) \to (1, 1) \to (0, 0) \to (0, 0)$ ce qui nous donne comme solution $w_1 = 00, 100$ et $w_2 = 00, 100$ qui sont bien dans A_1 et A_2 respectivement et dont la somme fait $00, 010$.

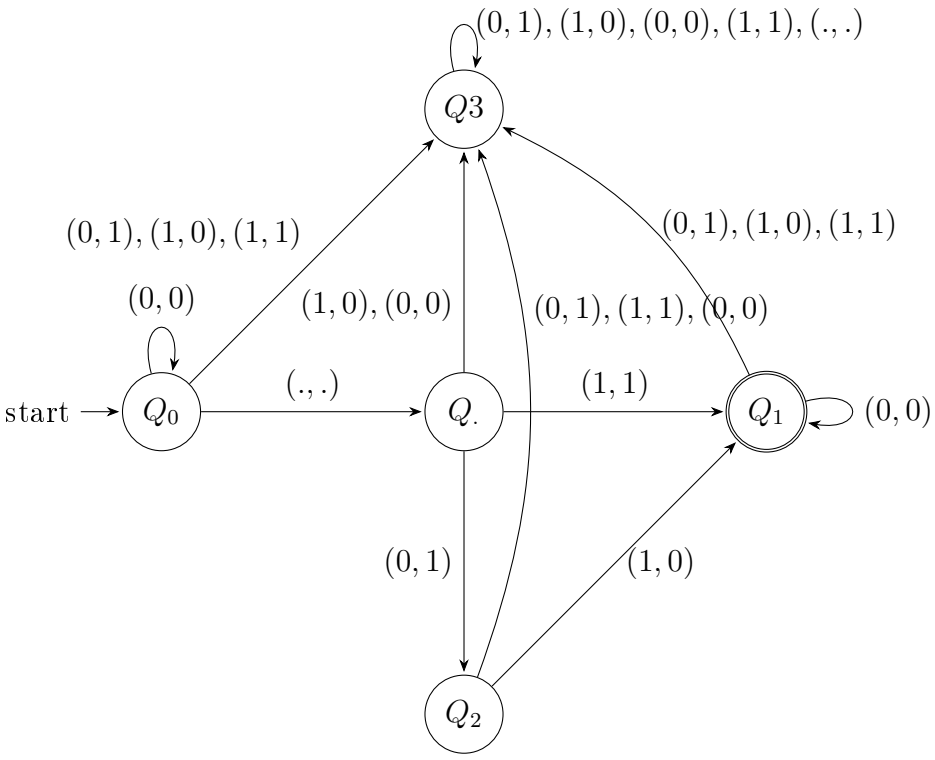


FIGURE 3.5 – L'automate M pour la base 2

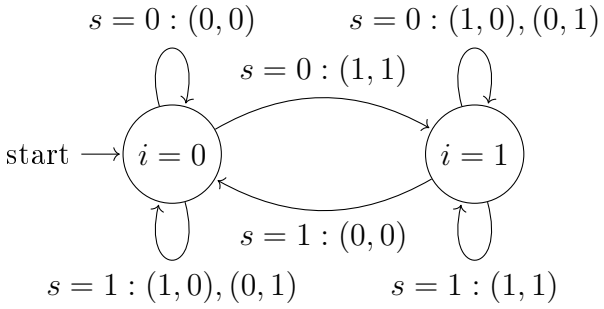


FIGURE 3.6 – L'automate I

3.5 Algorithme de Newton et résultat

Après avoir décomposé les opérateurs tordus par leurs pentes, nous abordons la phase finale de la preuve algorithmique : l'adaptation de l'algorithme de Newton. Pour entamer ce processus, nous partons de la factorisation de notre opérateur en facteurs moniques linéaires, qui donne lieu à un système d'équations de type Artin-Schreier généralisées ($z^p - az = b$) dont nous devons, dans un premier temps, vérifier qu'il est possible d'extraire les racines au sein de notre structure. Une fois cette résolubilité établie, la finalité de cette section sera d'introduire une méthode d'approximation afin d'identifier et d'isoler l'unique solution correspondant à notre série d'origine parmi la multiplicité des racines produites.

Lemme 3.51. *Pour tout $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ p-quasi-automatique dont le support est inclus dans $(-\infty, 0)$, il existe une série p-quasi-automatique $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ telle que $y^p - y = x$.*

Démonstration. Il suffit de montrer que $y = x^{\frac{1}{p}} + x^{\frac{1}{p^2}} + x^{\frac{1}{p^3}} + \cdots$ est p-quasi-automatique puisqu'on a bien que $y^p - y = (x^{\frac{1}{p}} + x^{\frac{1}{p^2}} + x^{\frac{1}{p^3}} + \cdots)^p - x^{\frac{1}{p}} + x^{\frac{1}{p^2}} + x^{\frac{1}{p^3}} + \cdots$
$= x + x^{\frac{1}{p}} + x^{\frac{1}{p^2}} + \cdots - x^{\frac{1}{p}} - x^{\frac{1}{p^2}} - x^{\frac{1}{p^3}} - \cdots = x$.

On sait que la série x est p-quasi-automatique, c'est-à-dire qu'on peut se ramener à une série p-automatique à support inclus dans S_p par un décalage $i \mapsto \frac{i-b}{a}$.

Notons $y = \sum_i y_i t^i = \sum_i x_i^{\frac{1}{p}} t^{\frac{i}{p}} + \sum_i x_i^{\frac{1}{p^2}} t^{\frac{i}{p^2}} + \cdots = \sum_j (x_{jp}^{\frac{1}{p}} + x_{jp^2}^{\frac{1}{p^2}} + \cdots) t^j$
d'où $y_i = x_{ip}^{\frac{1}{p}} + x_{ip^2}^{\frac{1}{p^2}} + \cdots$

Pour tout j fixé, la série $\sum_{i<-p^{-j}} y_i t^i$ est p-automatique. En effet, comme x est à support bien ordonné dans $(-\infty, 0)$, il existe une borne $N > 0$ telle que $x_m = 0$ pour tout $m < -N$. Pour n'importe quel indice $i < -p^{-j}$, la condition $ip^k < -N$ est satisfaite dès que $k > j + \log_p(N)$. Cela signifie que pour tous les indices i inférieurs à $-p^{-j}$, le coefficient y_i est une somme comportant un nombre fini de termes : $y_i = \sum_{k=1}^{K} x_{ip^k}^{\frac{1}{p^k}}$ avec $K = \lfloor j + \log_p(N) \rfloor$.
Comme x est p-automatique après décalage, chaque $x^{\frac{1}{p^k}}$ l'est aussi par stabilité sous l'action du Frobenius inverse. Alors y est p-automatique par somme de séries p-automatiques.

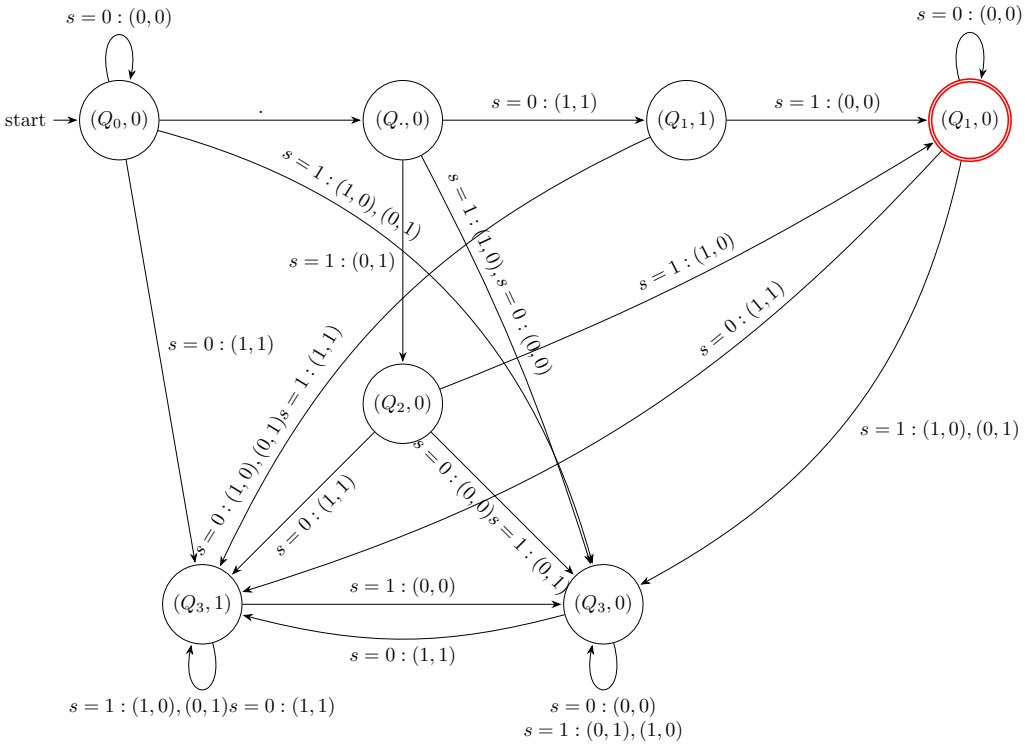


FIGURE 3.7 – Automate M'

Il reste à traiter le comportement de la série pour i appartenant à l'intervalle $[-p^{-j}, 0)$. Dans cette zone, l'argument de finitude ne tient plus : plus i se rapproche de zéro, plus le nombre de termes k tels que $ip^k \geq -N$ augmente. Pour garantir que y est globalement p-quasi-automatique, nous devons prouver que les coefficients y_i sont encore produits par un automate fini. Pour ce faire, nous allons fixer un indice $i \in [-1, 0)$ et analyser précisément la structure de la somme $y_{\frac{i}{p^k}}$ qui dépend des coefficients $x_i, x_{\frac{i}{p}}, x_{\frac{i}{p^2}}, \ldots$

Comme après un décalage x est p-automatique, il existe un automate qui à tout $n \in \mathbb{N}$ lit sa représentation en base p de gauche à droite et renvoie x_n. Pour évaluer les coefficients x_i, $x_{\frac{i}{p}}$, $x_{\frac{i}{p^2}}$, $x_{\frac{i}{p^3}}, \ldots$ à l'aide de l'automate fini associé à la série p-automatique x, nous utilisons le codage par la transformation $i \mapsto 1+i$. L'automate de x peut lire la représentation en base p de $1+i$ en omettant la virgule puisque ce sont des représentations finies elles se comportent comme des représentations de naturels. La transition de $1 + \frac{i}{p^k}$ à $1 + \frac{i}{p^{k+1}}$ se traduit en base p par l'ajout d'un chiffre $(p-1)$ en tête du développement (juste après la virgule). L'automate de x recevant en entrée des mots qui commencent par des suites de plus en plus longues de $(p-1)$, et le nombre d'états de cet automate étant fini, il existe nécessairement deux entiers distincts m et n (avec $m < n$) pour lesquels $y_{\frac{i}{p^m}} = y_{\frac{i}{p^n}}$. De

plus, on remarque la structure de récurrence suivante

$$y_{\frac{i}{p}} = x_i + x_{ip} + x_{ip^2} + \cdots = x_i + y_i$$
$$y_{\frac{i}{p^2}} = x_{\frac{i}{p}} + x_i + x_{ip} + \cdots = x_{\frac{i}{p}} + x_i + y_i = x_{\frac{i}{p}} + y_{\frac{i}{p}}$$

Alors, l'automate lit la représentation en base p de $1 + \frac{i}{p^m}$ et rend $y_{\frac{1}{p^m}}$ puisqu'on a

$$y_{\frac{i}{p^m}} = x_{\frac{i}{p^{m-1}}} + x_{\frac{i}{p^{m-2}}} + \cdots + x_{\frac{i}{p^n}} + \underbrace{y_{\frac{i}{p^n}}}_{=y_{\frac{i}{p^m}}}.$$

On obtient bien tous les coefficients de y car ils dépendent de ceux de x qui après décalage a son support dans S_p, les coefficients de y héritent donc de ce support.

Finalement, puisque y possède un support inclus dans S_p (après un décalage, comme pour x) et que la suite de ses coefficients est générée par un automate fini (soit par sommation directe, soit par bouclage sur les états) nous concluons que y est une série p-quasi-automatique. □

On établit la définition du binome de Newton généralisé.

Définition 3.52. Soit K un champ et soient $x, y \in K$. Pour tout réel r, si $v(x) < v(y)$, on a

$$(x+y)^r = \sum_{j=0}^{+\infty} \binom{r}{j} x^{r-j} y^k$$

où $\binom{r}{j} = \frac{r(r-1)\cdots(r-j+1)}{j!}$ est un coefficient binomial.

Remarque 3.53. Il est important de noter que le corps des séries p-quasi-automatiques n'est pas complet sous la valuation v. En effet, il est aisé de construire une suite de Cauchy d'éléments p-quasi-automatiques dont la limite ne l'est pas. Pour cela, considérons une série de Laurent généralisée infinie dont la suite des coefficients n'est pas automatique. Les troncatures successives de cette série à l'ordre k forment une suite de polynômes, donc des séries trivialement p-quasi-automatiques, qui constitue une suite de Cauchy sous la valuation v. Pourtant, sa limite est la série infinie d'origine, qui n'est pas automatique. Dans les résultats suivants, on se place dans le complété du champ des séries p-quasi-automatiques.

Lemme 3.54. *Soit $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ le complété, sous la valuation v, du champ des séries p-quasi-automatiques. Alors, pour tous $a, b \in R_q$ avec $a \neq 0$, l'équation $z^p - az = b$ a p solutions distinctes dans $R_{q'}$, pour une puissance q' de q.*

Démonstration. On commence par traiter le cas homogène : $b = 0$.

On doit résoudre $z^p - az = 0$, c'est-a-dire $z^{p-1} = a$ (sans compter la solution triviale $z = 0$). Cette équation a $p-1$ solutions distinctes dans $R_{q'}$. Notons $a = a_0 t^i (1+u)$ où $i \in \mathbb{Q}$ tel que $v(a) = i$, $a_0 \in \mathbb{F}_q$ est le coefficient du terme de plus bas degré et u est tel

que $v(u) > 0$ et représente le reste de la série après division par $a_0 t^i$. Choisissons q' tel que a_0 a ses racines $(p-1)$-ième dans $\mathbb{F}_{q'}$. Alors les solutions de $z^{p-1} = a$ sont données par $z = \beta t^{\frac{i}{p-1}}(1+u)^{\frac{1}{p-1}}$ pour toute racine $(p-1)$-ième β de a_0. Le terme $(1+u)^{\frac{1}{p-1}}$ peut être traité via la généralisation du binôme de Newton. On a alors $z = \beta t^{\frac{i}{p-1}} \sum_{j=0}^{+\infty} \binom{\frac{1}{p-1}}{j} u^j$. Cette expression est bien solution de l'équation puisque

$$z^{p-1} = \beta^{p-1}(t^{\frac{i}{p-1}})^{p-1} \left(\sum_{j=0}^{+\infty} \binom{\frac{1}{p-1}}{j} u^j \right)^{p-1} = a_0 t^i \left(\sum_{j=0}^{+\infty} \binom{1}{j} u^j \right) = a_0 t^i (1+u)$$

car $\binom{1}{j} = 0$ pour tout $j \geq 2$. De plus, ces solutions appartiennent bien à $R_{q'}$ puisque $\beta \in \mathbb{F}_{q'}$, les exposants $\frac{i}{p-1} \in \mathbb{Q}$ et la série est convergente puisque $v(u) > 0$ donc dans R_q et le tout est alors dans $R_{q'}$. Ce qui fait qu'en tout on a bien p solutions distinctes à l'équation de départ dans $R_{q'}$.

Le cas homogène étant traité, il ne nous reste plus qu'à traiter le cas où $a = 1$. En effet, en ayant le cas homogène, on trouve des solutions telles que $w^{p-1} = a$, alors avec un changement de variable $z = wy$, pour une équation générale $z^p - az = b$, on se ramène à une équation de la forme $(wy)^p - a(wy) = b$ qui se réduit à $y^p - y = B$ en divisant le tout par aw.

On cherche à résoudre $z^p - z = b$. Pour ce faire, on sépare b en b_- et b_+ où b_- est la partie de b dont le support est dans $(-\infty, 0)$ et b_+ celle dont le support est dans $[0, +\infty)$. Le cas b_- est précisément le lemme 3.51, qui nous donne l'existence d'une solution particulière p-quasi-automatique, notons-là z_-. Cette solution appartient trivialement à $R_{q'}$. Pour le cas b_+, considérons b_0 le terme indépendant de b_+ et prenons q' tel que l'équation $z^p - z = b_0$ a $c_1, \ldots, c_p \in \mathbb{F}_{q'}$ comme racines distinctes. Il nous reste alors à résoudre $z^p - z = b_+ - b_0$. Notons $V = b_+ - b_0$, on résout l'équation en itérant $z = z^p - V$. On obtient $z = -\sum_{j=0}^{+\infty} V^{p^j}$ et cette série converge car $v(V) > 0$. Les solutions de $z^p - z = b_+$ sont alors données par $c_i - \sum_{j=0}^{+\infty} (b_+ - b_0)^{p^j}$, exactement au nombre de p, distinctes et dans $R_{q'}$ car $c_i \in \mathbb{F}_{q'}$ et la série est convergente et appartient à R_q.

Les solutions globales de l'équation de départ sont alors $z_- + c_i - \sum_{j=0}^{+\infty} (b_+ - b_0)^{p^j}$ et il y en a bien p distinctes, toutes dans $R_{q'}$. □

Proposition 3.55. *Soit $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ le complété, sous la valuation v, du champ des séries p-quasi-automatiques, et soit R l'union des anneaux $R_{q'}$ pour toutes les puissances q' de q. Alors R est algébriquement clos.*

Démonstration. Par le lemme 1.21, il suffit de montrer que pour tout polynôme tordu monique $P(F)$ sur R_q, le polynôme $P(F)(z)$ se factorise complètement sur $R_{q'}$ pour un q'. Si $P(F)$ n'a pas de terme indépendant, on peut factoriser F à droite pour se ramener à un polynôme avec un terme indépendant non nul et donc, par le lemme 3.6, au cas où le polynôme $P(F)(z)$ n'a pas de zéros multiples. Pour factoriser de la sorte, on a besoin de savoir que R_q est parfait, ce qui est le cas puisque la racine p-ième d'une série p-quasi-automatique est elle-même p-quasi-automatique (par modification des sorties de l'automate

par l'endomorphisme de Frobenius), alors le corps R_q est clos pour l'opération $x \mapsto x^{\frac{1}{p}}$, c'est-à-dire R_q est parfait. On utilise la définition de polynôme tordu pour factoriser le F à droite et le fait que R_q soit parfait nous garantit d'obtenir à nouveau un polynôme sur R_q : si $P(F) = a_n F^n + \ldots + a_1 F$, on le factorise en $F(a_n^{\frac{1}{p}} F^{n-1} + \cdots + a_1^{\frac{1}{p}})$.

Par le corollaire 3.33, on peut écrire $P = Q_1 \ldots Q_n$ pour des polynômes tordus moniques linéaires $Q_1, \ldots, Q_n$ sur $R_q \otimes_{\mathbb{F}_q} \mathbb{F}_{q'} \simeq R_{q'}$. Notons $Q_i = F - c_i$ avec $c_i \in R_{q'}$, $c_i \neq 0$.

Le processus pour trouver les racines de $P(F)(z)$ peut alors être décrit comme le processus itératif pour résoudre le système suivant :

$$\begin{cases} z_1^p - c_1 z_1 = 0 \\ z_2^p - c_2 z_2 = z_1 \\ \vdots \\ z_n^p - c_n z_n = z_{n-1} \end{cases} \tag{3.1}$$

La première équation étant exactement le cas homogène du lemme 3.54, donnant p solutions distinctes dans R. Une fois z_1 obtenu, les équations suivantes suivent le cas général du lemme 3.54, donnant chacune p solutions distinctes dans R. Au total, le système admet p^n solutions distinctes et comme $P(F)$ est de degré n en F, cela correspond bien à un degré p^n en z pour $P(F)(z)$, ce qui signifie que $P(F)(z)$ se factorise complètement dans R. □

Théorème 3.56. *Soit $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série de Laurent généralisée qui est algébrique sur $\mathbb{F}_q(t)$. Alors x est p-quasi-automatique.*

Démonstration. La série x est algébrique sur $\mathbb{F}_q(t)$ donc elle est solution d'un polynôme à coefficients dans $\mathbb{F}_q(t)$. Cependant, dans ce cas, x pourrait être une racine multiple du polynôme, ce qui arrive si celui-ci est de la forme $\sum_i a_i z^{pi}$. Alors, on prend la racine p-ième, ce qui nous ramène à un polynôme $P(z) = \sum_i a_i^{\frac{1}{p}} z^i$ à coefficient dans $\mathbb{F}_q(t^{\frac{1}{p}})$. Si ce polynôme a denouveau des racines multiples, on itère la procédure. Comme le degré du polynôme est fini, la procédure va forcément s'arrêter et on finira par obtenir un polynôme qui n'a que des racines simples.

Prenons $c \in \mathbb{Q}$ tel que $c > v(x - x')$ pour toute autre racine $x' \neq x$ de P. Par la proposition 3.55, le complété R pour la valuation du champ des séries p-quasi-automatiques est algébriquement clos et on a $\mathbb{F}_q(t) \subset R$ donc toute série algébrique sur $\mathbb{F}_q(t)$ appartient en particulier à R. On obtient alors $x \in R$, on peut alors trouver une série y p-quasi-automatique telle que $v(x - y) \geq c$ par définition de R.

Les racines du polynôme $P(z+y)$ sont de la forme $x'-y$ pour x' qui sont les racines de P. On a $v(x-y) \geq c$ et pour $x' \neq x$, $v(x'-y) = v((x'-x)+(x-y)) = \min(v(x'-x), v(x-y)) < c$ et comme les valuations des racines donnent les pentes du polygone de Newton par la remarque 3.9, on en tire que $P(z + y)$ a exactement une racine de pente au moins c, à savoir $x - y$.

De plus, par le théorème 2.3, y est algébrique sur $\mathbb{F}_q(t)$. Soit K l'extension finie $\mathbb{F}_q((t))(y)$. Alors K est complet sous la valuation v car c'est une extension finie d'un corps

complet. Par le corollaire 3.20, on peut factoriser $P(z+y)$ en polynômes purs linéaires dont le dernier est celui de pente au moins c. Les coefficients de la factorisation restant dans K, on obtient $x - y \in K$ et finalement $x \in K$.

Soit m le degré du polynôme minimum de y sur $\mathbb{F}_q(t)$. Alors $\{1, y, \ldots, y^{m-1}\}$ est une base de K et on obtient la décomposition suivante pour $j = 0, \ldots, m-1$:

$$y^{p^j} = \sum_{i=0}^{m-1} a_{i,j} y^i \quad a_{i,j} \in \mathbb{F}_q(t) \subset \mathbb{F}_q((t)) \tag{3.2}$$

Les $a_{i,j}$ sont alors trivialement algébriques sur $\mathbb{F}_q(t)$.

La série x étant algébrique sur $\mathbb{F}_q(t)$, elle génère une extension de dimension finie. On peut alors prendre n minimal tel que $x, x^p, \ldots, x^{p^n}$ soient linéairement dépendants sur $\mathbb{F}_q(t)$, donc aussi sur $\mathbb{F}_q((t))$. On a aussi $x \in K$, ce qui nous donne la décomposition suivante :

$$x^{p^j} = \sum_{l=0}^{m-1} b_{l,j} y^l \quad b_{l,j} \in \mathbb{F}_q((t)) \tag{3.3}$$

En élevant cette dernière équation à la puissance p et en appliquant (3.2) puis en comparant avec l'utilisation de (3.3), on obtient

$$\begin{aligned}(x^{p^j})^p &= \sum_{l=0}^{m-1} b_{l,j}^p y^{lp} = \sum_{l=0}^{m-1} b_{l,j}^p \left(\sum_{i=0}^{m-1} a_{i,l} y^i \right) = \sum_{i=0}^{m-1} \left(\sum_{l=0}^{m-1} b_{l,j}^p a_{i,l} \right) y^i \\ &= \sum_{i=0}^{m-1} b_{i,(j+1)} y^i\end{aligned}$$

et par unicité de la décomposition, on obtient les équations

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

Soit $c_0 x + \ldots + c_n x^{p^n} = 0$ une relation linéaire sur $\mathbb{F}_q(t)$ que nous pouvons normaliser en posant $c_0 = 1$. Alors, les c_i sont trivialement algébriques sur $\mathbb{F}_q(t)$.
On peut aussi écrire $x = -c_1 x^p - \cdots - c_n (x^{p^{n-1}})^p = \sum_{j=0}^{n-1} -c_{j+1} (x^{p^j})^p$. En combinant (3.2) et (3.3) à ceci, on a

$$\begin{aligned}x = \sum_{i=0}^{m-1} b_{i,0} y^i &= \sum_{j=0}^{n-1} -c_{j+1} (x^{p^j})^p \\ &= \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{l,j}^p y^{pl} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{l,j}^p a_{i,l} y^i\end{aligned}$$

et par unicité de la décomposition

$$b_{i,0} = \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{l,j}^p a_{i,l}$$

Au final, on a un système d'équations liant les $b_{i,j}$ comme dans le lemme 1.23 avec $B = Id$, $w = 0$ et

$$v = \begin{pmatrix} b_{0,0} \\ \vdots \\ b_{m-1,0} \\ \vdots \\ \vdots \\ b_{m-1,n-1} \end{pmatrix}, \quad A = \begin{pmatrix} c_1 M_a & c_2 M_a & \cdots & c_n M_a \\ -M_a & 0 & \cdots & 0 \\ 0 & -M_a & \cdots & 0 \\ \vdots & & & \\ 0 & \cdots & -M_a & 0 \end{pmatrix}$$

avec $M_a = (a_{i,l})_{0 \leq i,l \leq m-1}$. Ce qui nous permet de conclure que chaque $b_{i,j}$ est algébrique sur $\mathbb{F}_q(t)$. Par le théorème de Christol, chaque $b_{i,j}$ est p-automatique et $x = \sum_{i=0}^{m-1} b_{i,0} y^i$ est p-quasi-automatique par stabilité des séries p-quasi-automatiques. □

3.6 Résumé de la procédure

Donnée : Une série x satisfaisant une équation algébrique $P(x) = 0$ où $P \in \mathbb{F}_q(t)[z]$.
Question : Comment construire un automate fini qui, recevant la représentation en base p d'un indice $i \in \mathbb{Q}$, produit le coefficient x_i ?

1. Puisque l'étude directe des racines d'un polynôme quelconque est complexe, on utilise la structure d'anneau polynomial tordu $K\{F\}$. On cherche un polynôme additif $Q(z)$ (correspondant à un polynôme tordu $R(F)$) qui admet x comme racine. Si P n'est pas additif, on construit Q comme un multiple à gauche de P dans l'anneau des opérateurs.
2. À l'aide des polygones de Newton, on analyse les valuations des racines de $R(F)$. Le théorème de factorisation par pentes permet de décomposer $R(F)$ de degré n en F en un produit de n facteurs tordus linéaires de la forme $(F - a_i)$ sur une extension finie. Le problème se réduit alors à la résolution successive de systèmes d'équations d'Artin-Schreier généralisées : $z^p - a_i z = b$
3. Il suffit alors de résoudre des équations du type $z^p - az = b$ à coefficients dans le complété des séries p-quasi-automatiques.
4. Le système fournit p^n solutions potentielles (les racines de Q). Pour isoler notre solution cible x, on calcule une approximation y à une précision suffisante (grâce aux pentes du polygone de Newton) telle qu'un unique candidat x vérifie cette proximité. On construit l'automate associé à cette approximation y.
5. On trouve alors un automate qui calcule x puisque x s'exprime en fonction de y et des coefficients du système.

Chapitre 4

Clôture algébrique de $\mathbb{F}_q(t)$

Dans ce chapitre, nous déterminons la clôture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t^{\mathbb{Q}}))$, qui nous permet de prouver le sens algébrique implique automatique de notre théorème. Cette section développe certains résultats de [13].

Proposition 4.1. *Soit L un langage régulier de représentations valides en base p tel que $\mathrm{val}_p(L) = \{\mathrm{val}_p(s) : s \in L\}$ est bien ordonné. Alors tout point d'accumulation de $\mathrm{val}_p(L)$ est rationnel.*

Démonstration. Soit $s_1, s_2, \ldots \in L$ une suite de mots tels que $\mathrm{val}_p(s_1), \mathrm{val}_p(s_2), \ldots$ converge vers un $r \in \mathbb{R}$. Alors il existe un unique mot infini s tel que la longueur du préfixe commun entre s et s_i tend vers l'infini si i tend vers l'infini. Ce mot peut être vu comme la représentation en base p de r.

Comme L est un langage régulier, il est accepté par un automate fini. Alors, il existe un état q qui est visité une infinité de fois par les préfixes de s. Or, étant donné que $\mathrm{val}_p(L)$ est bien ordonné, par le théorème 3.46, pour tout état q accessible, le sous-graphe G_q des états accessibles depuis q est un saguaro enraciné muni d'un p-étiquetage approprié. Alors, le chemin suivi par l'automate pour lire s à partir de l'état q doit nécessairement finir dans un unique cycle. Si le chemin pour lire s empruntait une arête qui n'est pas sur le cycle de q, alors comme l'état q est visité une infinité de fois par les préfixes de s, il serait alors sur deux cycles ce qui contredit la définition de saguaro enraciné. On obtient que s est ultimement périodique et r est rationnel. □

Définition 4.2. Pour $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ et $r \in \mathbb{R}$, on définit la r-troncature de x comme étant la série $\sum_{i<r} x_i t^i$. On la note $x_{(r)}$.

Lemme 4.3. *Si $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est p-quasi-automatique, alors toute troncature de x l'est aussi.*

Démonstration. Par définition de p-quasi-automatique, il existe des entiers $a > 0, b$ tels que le support $S = \{i \in \mathbb{Q} : x_{\frac{i-b}{a}} \neq 0\}$ est inclus dans S_p et la série $x' = \sum_i x_{\frac{i-b}{a}} t^i$ est p-automatique. Par la proposition 4.1, en prenant $L = \{\mathrm{rep}_p(j) : j \in S\}$, on a $\sup\{i \in S : i < r\} \in \mathbb{Q}$ donc on peut se réduire au cas où $r \in \mathbb{Q}$.

Montrons que la série $x_{(r)}$ décalée par les mêmes entiers a et b, qu'on notera $x'_{(r)}$, est p-automatique. Le produit d'Hadamard de deux séries p-automatiques est encore p-automatique. Alors, en écrivant $x'_{(r)} = x' \odot \mathbb{1}_{<r}$, on peut conclure car $\{\mathrm{rep}_p(i) : i < r, i \in S_p\}$ est un langage régulier sur Σ_p. En effet, on peut effectuer la comparaison d'un nombre en base p avec la représentation ultimement périodique d'un rationnel en base p par un automate fini. La suite des coefficients de $x'_{(r)}$ est alors p-automatique. Pour finir, le support de $x'_{(r)}$ est inclus dans S et donc dans S_p et on a prouvé que $x'_{(r)}$ était p-automatique ce qui signifie que la série initiale $x_{(r)}$ est p-quasi-automatique pour les mêmes entiers a, b que x. □

Le résultat suivant est un résultat analogue au lemme 3.51 mais on se focalise ici sur l'existence d'un automate pour y, sans le construire.

Lemme 4.4. *Si $x \in \mathbb{F}_q((t^{\mathbb{Q}}))_{\mathrm{aut}}$ et $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ satisfont $y^p - y = x$, alors toute troncature de y est p-quasi-automatique.*

Démonstration. On peut supposer que le support de x est contenu soit dans $(-\infty, 0)$ soit dans $(0, +\infty)$ quitte à séparer la série sous la forme $x = x_1 + x_2$ avec x_1 dont le support est dans $(-\infty, 0)$ et x_2 dont le support est dans $(0, +\infty)$ et traiter les deux séparément. La série à support dans $(-\infty, 0)$ est p-quasi-automatique car c'est une troncature d'une série p-quasi-automatique. Alors, la série à support dans $(0, +\infty)$ l'est forcément aussi par le lemme 2.6. Chercher y tel que $y^p - y = x$ revient alors à chercher y_1 dont le support est dans $(-\infty, 0)$ et y_2 dont le support est dans $(0, +\infty)$ tels que $y_1^p - y_1 = x_1$ et $y_2^p - y_2 = x_2$.

- Support dans $(0, +\infty)$:
  En itérant la relation $y = y^p - x$, on obtient pour tout n

  $$y = y^{p^n} - x^{p^{n-1}} - \cdots - x^p - x$$

  Avec cette écriture, pour n assez grand, seulement un nombre fini de puissances de x va contribuer à n'importe quelle troncature, l'automaticité est alors préservée.

- Support dans $(-\infty, 0)$:
  On se réduit au cas où x est à support dans $(-1, 0)$. En effet, le support de x étant bien ordonné, toute partie non-vide admet un minimum, c'est-à-dire que le support est inclus dans $(-N, 0)$ pour un certain N. En prenant $b = 0$ et $a = N$, la proposition 2.9 nous assure qu'on obtient une nouvelle série x à support dans $(-1, 0)$ et p-quasi-automatique. La relation $y^p - y = x$ est alors toujours vraie mais porte sur des séries à support dans $(-1, 0)$.
  De la même manière que pour le cas du support positif, en itérant la relation $y^p = y + x$, on obtient pour tout n

  $$y = y^{\frac{1}{p^n}} + x^{\frac{1}{p^{n-1}}} + \cdots + x^{\frac{1}{p^2}} + x^{\frac{1}{p}}.$$

  On pose $\tilde{x} = tx$ et $\tilde{y} = t^{\frac{1}{p}} y$ de sorte que $\tilde{x}$ soit à support dans $(0, 1)$, puisque x était à support dans $(-1, 0)$ et $\tilde{y}$ dans $(-1 + \frac{1}{p}, \frac{1}{p})$ puisque y était à support dans $(-1, 0)$.

Avec ces définitions, on a la relation $\tilde{y}^p - t^{\frac{p-1}{p}}\tilde{y} = \tilde{x}$. Cette dernière relation découle directement de nos définitions et de la relation initiale :

$$\begin{aligned}\tilde{y}^p - t^{\frac{p-1}{p}}\tilde{y} &= ty^p - t^{\frac{p-1}{p}}t^{\frac{1}{p}}y \\ &= ty^p - ty \\ &= t(y^p - y) = tx = \tilde{x}\end{aligned}$$

On déduit alors que $\tilde{y}$ doit avoir son support inclus dans $(0, \frac{1}{p})$ pour que la relation soit valide. En effet, si $\tilde{y}$ avait une plus petite puissance négative t^α, alors $\tilde{y}^p$ aurait $t^{p\alpha}$ comme puissance minimum et $t^{\frac{p-1}{p}}\tilde{y}$ aurait $t^{\alpha+\frac{p-1}{p}}$ comme puissance minimum. Celles-ci ne se compenseraient pas alors que $\tilde{x}$ a un support strictement positif. Quitte à passer à un décalage, on peut supposer que le support de $\tilde{x}$ est inclus dans S_p. Il en va alors de même pour celui de $\tilde{y}$. De plus, comme x est p-quasi-automatique, $\tilde{x}$ est toujours p-quasi-automatique par la proposition 2.9. Notons $\tilde{x} = \sum_i \tilde{x}_i t^i$, $\tilde{y} = \sum_i \tilde{y}_i t^i$ et définissons $X, Y \in \mathbb{F}_q[[t]]$ dont les coefficients sont définis par les formules $X_{\mathrm{val}_p(s)} = \tilde{x}_{\mathrm{val}_p(,s^R)}$ et $Y_{\mathrm{val}_p(s)} = \tilde{y}_{\mathrm{val}_p(,s^R)}$, $s \in (\Sigma_p^* \backslash 0\Sigma_p^*)$.
On a alors que X est p-automatique par stabilité du miroir pour les suites automatiques puisque x est p-automatique car son support est dans S_p.

Si on écrit les indices en base p, la relation $\tilde{y}^p - t^{\frac{p-1}{p}}\tilde{y} = \tilde{x}$ se traduit par une relation entre les coefficients qui ne génère pas de retenues puisque $\tilde{y}$ est à support dans $(0, \frac{1}{p})$.
On peut alors formellement inverser l'identité afin d'obtenir une nouvelle relation faisant intervenir X, Y : $Y^{\frac{1}{p}} - t^{p-1}Y = X$.
En effet, l'opération qui à $\tilde{y}$ associe $\tilde{y}^p$ revient à ajouter un zéro au poids faible de la représentation en base p. Prendre le miroir de cette représentation permet que ce zéro soit au poids fort, ce qui se traduit par l'opération qui à Y associe $Y^{\frac{1}{p}}$.
L'opération $t^{\frac{p-1}{p}}\tilde{y}$ ajoute $\frac{p-1}{p}$ à l'indice i. Pour la représentation en base p, cela se traduit par le fait de passer, si $i = 0, d_1d_2d_3\ldots$ à $0, d_1d_2d_3\ldots + 0, (p-1)$. Comme $\tilde{y}$ est à support dans $(0, \frac{1}{p})$, le d_1 de toute représentation en base p de ses indices est obligatoirement 0. On ne produit donc aucune retenue. En prenant le miroir de la représentation, ce chiffre devient celui de poids le plus faible. Cela revient à avoir ajouté $p-1$ à l'indice i dans Y, ce qui se traduit par l'opération $t^{p-1}Y$.
En élevant notre nouvelle identité à la puissance p, on obtient $Y - t^{p(p-1)}Y^p = X^p$. On a un polynôme additif $P(z) = z - t^{p(p-1)}z^p$. La série $X \in \mathbb{F}_q[[t]]$ est p-automatique, donc algébrique sur $\mathbb{F}_q(t)$ par le théorème de Christol, d'où X^p l'est aussi. Alors, X^p est zéro d'un polynôme à coefficients dans $\mathbb{F}_q(t)$, notons-le Q.
On a $Q(X^p) = 0 = Q(P(Y))$. Alors, $Q \circ P$ est un polynôme à coefficients dans $\mathbb{F}_q(t)$, on déduit finalement que Y est algébrique sur $\mathbb{F}_q(t)$. Par le théorème de Christol, Y est p-automatique. Alors, $\tilde{y}$ est p-automatique par stabilité de l'opération miroir et parce que son support est dans S_p. On déduit que y est p-quasi-automatique donc toutes ses troncatures également.

□

Remarque 4.5. Le lemme qu'on vient d'établir fonctionne aussi dans le cas où toutes les troncatures de x sont p-quasi-automatiques. En effet, dans la démonstration, en étudiant les troncatures de y, on a jamais besoin de x tout entier.

Corollaire 4.6. *Soit $P(F)$ un polynôme tordu non nul à coefficient dans $\mathbb{F}_q$. Si $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ sont tels que x est p-quasi-automatique et $P(F)(y) = x$, alors toute troncature de y est p-quasi-automatique.*

Démonstration. Cas de base : $P(F) = F - \mu$, $\mu \in \mathbb{F}_q$. L'équation devient $y^p - \mu y = x$. Si $\mu = 0$, on a simplement $y = x^{\frac{1}{p}}$ qui reste p-quasi-automatique par stabilité des automates pour un décalage et sous composition de la fonction de sortie avec le Frobenius inverse. Si $\mu = 1$, le lemme 4.4 nous permet de conclure. Si $\mu \neq 1$, on peut se ramener à une équation du type du lemme 4.4 par un changement de variable. En effet, on peut trouver $w \in \mathbb{F}_{q'}$ tel que $w^{p-1} = \mu$ pour q' une puissance de q, en résolvant l'équation homogène. Alors, en posant $y = wz$, on obtient $w^p z^p - \mu w z = x$ qui se réduit à $z^p - z = x'$ avec $x' = (\mu w)^{-1} x$ toujours p-quasi-automatique. Par le lemme 4.4, toute troncature de z est p-quasi-automatique et il en va de même pour $y = wz$ par stabilité sous la multiplication par une constante. Le cas général se réduit au cas de base par factorisation par pentes du polynôme en polynômes linéaires par le corollaire 3.33. On a $P(F)(y) = (F - \mu_n) \cdots (F - \mu_1)(y) = x$ avec $\mu_i \in \mathbb{F}_q \otimes_{\mathbb{F}_q} \mathbb{F}_{q'} \simeq \mathbb{F}_{q'}$. On résout étape par étape : on pose $z_1 = (F - \mu_{n-1}) \circ \ldots \circ (F - \mu_1)(y)$. Alors $(F - \mu_n)(z_1) = x$, ce qui implique par le cas de base que toute troncature de z_1 est p-quasi-automatique. Ensuite, on pose $z_2 = (F - \mu_{n-2}) \circ \ldots \circ (F - \mu_1)(y)$. Alors $(F - \mu_{n-1})(z_2) = z_1$, ce qui implique par le cas de base que toute troncature de z_2 est p-quasi-automatique. On itère le procédé jusqu'à obtenir $(F - \mu_1)(y) = z_{n-1}$ et conclure que toute troncature de y est p-quasi-automatique. □

Lemme 4.7. *Supposons que $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ a son support inclus dans S_p et est algébrique sur $\mathbb{F}_q((t))$. Alors toute troncature de x est p-automatique.*

Démonstration. Traitons le résultat pour le cas où le support de x est non borné, le cas borné étant trivial. En effet, si le support était borné, il serait en particulier fini et x serait un polynôme à exposants rationnels donc p-automatique. Il s'en suit que toutes ses troncatures le sont également par le lemme 4.3.

Pour $r \in \mathbb{R}$, soit $x_{(r)}$ la r-troncature de x. Soit S l'ensemble des $r \in \mathbb{R}$ tels que $x_{(r)}$ est p-automatique. L'ensemble S est non-vide car il contient $(-\infty, 0]$ puisque pour tout $i \in (-\infty, 0]$, $x_{(i)} = 0$ et 0 est p-automatique. Comme le support de x est bien ordonné, S ne peut pas admettre de maximum. En effet, si tel était le cas, notons $r = \max(S)$, c'est-à-dire qu'on a $x_{(r)}$ p-automatique et pour tout $r' > r, x_{(r')}$ n'est pas p-automatique. Comme le support est bien ordonné et non borné, l'ensemble $\{r'' \in supp(x) : r'' > r\}$ est non vide, donc admet un minimum r'. Dans ce cas, on a que pour tout $s \in (r, r'), x_{(s)} = x_{(r)}$. On obtient finalement $x_{(s)}$ p-automatique avec $s > r$, une contradiction.

Supposons dès lors que S admet une borne supérieure finie $r = \sup(S)$ qui n'appartient pas à S et montrons qu'on arrive à une contradiction. Puisque x est algébrique sur $\mathbb{F}_q((t))$, il existe un polynôme non nul $P(t) = \sum_{j=0}^{d} P_j t^{p^j}$ avec $P_j \in \mathbb{F}_q((t))$ tel que $P(x) = 0$ par le

lemme 1.21. Soit v la valuation sur $\mathbb{F}_q((t^{\mathbb{Q}}))$. On définit la constante $c = \min_{0\leq j\leq d}\{v(P_j) + rp^j\}$. Pour chaque j, on note Q_j le coefficient de t^{c-rp^j} dans P_j. On construit $Q(t) = \sum_{j=0}^{d} Q_j t^{p^j}$. Le polynôme Q est non-nul par définition de c puisqu'au moins un indice j vérifie le minimum voulu et le coefficient de $t^{v(P_j)}$ est non nul dans P_j par définition de la valuation. On veut écrire la c-troncature de $P_j x^{p^j}$ qui va faire intervenir des troncatures de x. Pour ce faire, on commence par écrire le produit :

$$P_j x^{p^j} = \left(\sum_m P_{j,m} t^m\right)\left(\sum_k x_k t^k\right)^{p^j} = \sum_{m,k} P_{j,m} x_k^{p^j} t^{m+kp^j}$$

Ensuite, on ne garde que les termes où l'exposant de t est plus petit que c et on isole x :

$$\sum_{\substack{m,k\\ m+kp^j<c}} P_{j,m} x_k^{p^j} t^{m+kp^j} = \sum_m P_{j,m} t^m \left(\sum_{k<\frac{c-m}{p^j}} x_k t^k\right)^{p^j} = \sum_m P_{j,m} t^m (x_{(\frac{c-m}{p^j})})^{p^j}$$

Pour finir, par définition de la valuation et de la constante c, on a que $P_j = \sum_m P_{j,m} t^m = \sum_{m\geq v(P_j)} P_{j,m} t^m = \sum_{m\geq c-rp^j} P_{j,m} t^m$. Au final, on obtient que la c-troncature de $P_j x^{p^j}$ est $\sum_{m\geq c-rp^j} P_{j,m} t^m (x_{\frac{c-m}{p^j}})^{p^j}$. On observe qu'elle s'écrit sous la forme $y_j + z_j$ où

- $y_j = Q_j t^{c-rp^j} (x_{(r)})^{p^j}$ (terme en $m = c - rp^j$)
- z_j est p-automatique par hypothèse. En effet, z_j fait intervenir des l-troncatures de x avec $l < r = \sup(S)$ puisqu'on a l'équivalence suivante : $m > c - rp^j \Leftrightarrow \frac{c-m}{p^j} < r$.

Puisque $\sum_{j=0}^{d} P_j x^{p^j} = 0$, on en déduit que $y = \sum_{j=0}^{d} y_j = -\sum_{j=0}^{d} z_j$. Chaque z_j étant p-automatique, leur somme y reste p-automatique. On a

$$y = \sum_{j=0}^{d} Q_j t^{c-rp^j} (x_{(r)})^{p^j}$$

<u>1^{er} cas :</u> Le polynôme Q est un monôme. Alors, $y = Q_j t^{c-rp^j} (x_{(r)})^{p^j}$ et $(x_{(r)})^{p^j}$ est p-automatique donc $x_{(r)}$ l'est aussi.
<u>2^e cas :</u> Le polynôme Q n'est pas un monôme. Dans ce cas, Q est une combinaison linéaire de puissances de Frobenius appliquées à la série $x_{(r)}$ et qui est égale à une série p-automatique : $t^{-c}y = Q(t^{-r}x_{(r)})$. Alors, $x_{(r)}$ est lui-même p-automatique par le corollaire 4.6.

Dans les deux cas, on aboutit à la conclusion que $r \in S$, ce qu'on a dit être impossible. L'ensemble S est alors non borné, ce qui signifie que toutes les troncatures de x sont p-automatiques. □

Avant de passer au corollaire, nous avons besoin d'une propriété sur les séries de $\mathbb{F}_q((t^{\mathbb{Q}}))$ algébriques sur $\mathbb{F}_q((t))$. Cette propriété est notamment énoncée dans [8].

Proposition 4.8. *Soit K un clôture algébrique de $\mathbb{F}_q$. Tout élément x de la clôture algébrique de $\mathbb{F}_q((t))$ dans $K((t^{\mathbb{Q}}))$ a les propriétés suivantes :*

1. *Le support de x est inclus dans $\frac{1}{m}\mathbb{Z}[p^{-1}]$ pour un entier m positif premier avec p.*
2. *Les coefficients de x sont dans un sous-champ fini $\mathbb{F}_{q'}$ de K.*

Corollaire 4.9. *Si $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q((t))$ et à support borné, alors x est p-quasi-automatique.*

Démonstration. Comme x est algébrique sur $\mathbb{F}_q((t))$, on sait que son support est inclus dans $\frac{1}{m}\mathbb{Z}[\frac{1}{p}]$, où m est un entier premier avec p. En posant $x' = \Sigma_i x_i t^{mi+N}$, où N est tel que le $m$supp(x) est inclus dans $(-N, +\infty)$, on obtient que le support de x' est dans S_p.

Alors, par le lemme 4.7, toute troncature de x' est p-automatique. Comme le support est borné, pour un r assez grand on a $x'_{(r)} = x'$, d'où x' est p-automatique. C'est-à-dire x est p-quasi-automatique puisqu'après un décalage adéquat on a trouvé une série x' p-automatique dont le support est inclus dans S_p. □

On définit deux notions d'algèbre qui nous seront utiles pour définir et démontrer le lemme de Krasner. Ces informations peuvent être retrouvées dans [17].

Définition 4.10. Soit $(K, |\cdot|)$ un corps valué. On dit que K est complet si toute suite de Cauchy de K converge vers un élément de K.

Définition 4.11. Soit K un corps et L une extension de K. Un élément $\alpha \in L$ est dit séparable sur K si son polynôme minimal $P \in K[t]$ ne possède que des racines simples dans la clôture algébrique $\overline{K}$. L'extension L est dite séparable si tous ses éléments sont séparables.

Définition 4.12. Soit L/K une extension de corps de caractéristique $p > 0$. Un élément $x \in L$ est dit radiciel sur K s'il existe un entier $n > 0$ tel que $x^{p^n} \in K$. Une extension algébrique L/K est une extension radicielle ou purement inséparable si tous ses éléments sont radiciels sur K.

Proposition 4.13. *Soit $(K, |\cdot|)$ un corps valué complet et soit $\overline{K}$ la clôture algébrique de K. Il existe alors une unique valeur absolue sur $\overline{K}$ prolongeant $|\cdot|$.*

Lemme 4.14 (Krasner)**.** *Soit K un corps valué complet ultramétrique et $\overline{K}$ une clôture algébrique de K. Soient α et β deux éléments de $\overline{K}$ tels que α est séparable sur K et tels que $|\alpha - \beta| < \min\{|\alpha - \alpha_i| : 2 \leq i \leq d\}$ où $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ sont les conjugués distincts de α sur K. Alors $K(\alpha) \subset K(\beta)$.*

Démonstration. Soit L l'extension engendrée par tous les conjugués de α, c'est-à-dire que L est le corps de rupture du polynôme minimum de α. Alors, l'extension L est normale sur K donc aussi sur l'extension intermédiaire $K(\beta)$. De plus, tous les générateurs de L sont séparables sur K donc sur $K(\beta)$, ce qui signifie que L est séparable sur $K(\beta)$. On conclut que $L/K(\beta)$ est une extension normale et séparable, donc de Galois. Par définition, le

groupe $\mathrm{Gal}(L/K(\beta))$ fixe les éléments de $K(\beta)$. Il suffit de prouver que α est fixé par tous les éléments de $\mathrm{Gal}(L/K(\beta))$. Soit $\varphi \in \mathrm{Gal}(L/K(\beta))$, $\varphi(\alpha) = \alpha_i$ pour un $i \in \{1, \ldots, d\}$. On a

$$\begin{aligned} |\varphi(\alpha) - \alpha| &= |\varphi(\alpha) - \beta + \beta - \alpha| = |\varphi(\alpha) - \varphi(\beta) + \beta - \alpha| \\ &\leq \sup\{|\varphi(\alpha - \beta)|, |\beta - \alpha|\} = |\beta - \alpha| \end{aligned}$$

car par unicité du prolongement de la valeur absolue de K à son extension algébrique L, la norme est invariante par l'action du groupe de Galois $\mathrm{Gal}(L/K(\beta))$. On a donc $|\varphi(x)| = |x|$ pour tout $x \in L$, d'où $|\varphi(\alpha - \beta)| = |\alpha - \beta|$. Cette inégalité combinée à notre hypothèse nous donne $|\varphi(\alpha) - \alpha| < |\alpha - \alpha_i|$ pour $2 \leq i \leq d$. La seule possibilité est alors $\varphi(\alpha) = \alpha$ et finalement $\alpha \in K(\beta)$. □

Pour appliquer ceci à notre contexte, on pose $|x - y| = d(x, y) = 2^{-v(x-y)}$.

Lemme 4.15. *Supposons que $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q((t))$. Alors, pour $r \in \mathbb{R}$ suffisamment grand, la r-troncature $x_{(r)}$ de x est p-quasi-automatique, algébrique sur $\mathbb{F}_q(t)$ et génère une extension finie de $\mathbb{F}_q((t))$ contenant x.*

Démonstration. On cherche à appliquer le lemme de Krasner. Pour ce faire, on a besoin que l'élément $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ soit séparable sur $\mathbb{F}_q((t))$. Si ce n'est pas le cas, on sait qu'il existe un $j \geq 0$ tel que x^{p^j} soit séparable sur $\mathbb{F}_q((t))$. Dans ce cas, prouver que la r-troncature de x^{p^j} génère la même extension que x^{p^j} suffit pour le prouver pour x puisque l'opérateur de Frobenius est un automorphisme. Quitte à remplacer x par x^{p^j}, on peut donc supposer que x est séparable sur $\mathbb{F}_q((t))$.

Comme le support de x est bien ordonné et que x est algébrique sur $\mathbb{F}_q((t))$, il existe des entiers a et b tels que $x' = \sum_i x_{\frac{i-b}{a}} t^i$ a son support inclus dans S_p. Par le lemme 4.7, pour tout $r \in \mathbb{R}$, $x'_{(r)}$ est p-automatique d'où $x_{(r)}$ est p-quasi-automatique. On obtient, par le théorème 2.3 que $x_{(r)}$ est algébrique sur $\mathbb{F}_q(t)$.

Pour r suffisamment grand, on peut appliquer le lemme de Krasner au polynôme minimum de x pour voir que x et $x_{(r)}$ génèrent la même extension de $\mathbb{F}_q((t))$. En effet, $v(x - x_{(r)})$ tend vers l'infini si r tend vers l'infini, c'est-à-dire $|x - x_{(r)}|$ tend vers 0 et on a $|x - \alpha_i| > 0$ pour tout α_i les autres racines du polynôme minimum de x. Pour r assez grand, on a alors $|x - x_{(r)}| < \min\{|x - \alpha_i| : 2 \leq i \leq d\}$. Par le lemme de Krasner, on déduit que $\mathbb{F}_q((t))(x) \subset \mathbb{F}_q((t))(x_{(r)})$. L'autre inclusion étant évidente par définition, on obtient $\mathbb{F}_q((t))(x) = \mathbb{F}_q((t))(x_{(r)})$. □

Le résultat suivant est à retrouver dans [6].

Proposition 4.16. *Soit M un sous-espace vectoriel de E, l'espace vectoriel $E/M \otimes F$ est isomorphe à l'espace vectoriel $(E \otimes F)/\Gamma(M)$ où $\Gamma(M)$ est le sous-espace vectoriel de $E \otimes F$ engendré par les éléments de la forme $m \otimes y$ avec $m \in M, y \in F$.*

Définition 4.17. Soit P un polynôme non constant sur le corps K. On appelle corps de décomposition de P sur K une extension L de K telle que dans $L[t]$, P est produit de facteurs de degré 1 et le corps L est minimal pour cette propriété (c'est-à-dire que les racines de P engendrent L).

Théorème 4.18 (premier théorème d'isomorphie). *Si $\varphi : G_1 \to G_2$ est un homomorphisme, alors l'application $\tilde{\varphi} : G_1/\ker(\varphi) \to \varphi(G_2)$ définie par $\tilde{\varphi}(x\ker(\varphi)) = \varphi(x)$ est un isomorphisme.*

De même que l'extension des scalaires nous a servis dans la partie algorithmique pour travailler dans le corps le plus optimal possible, le produit tensoriel réapparaît ici comme l'outil naturel pour faire cohabiter l'extension finie E et le corps F'. Construire le produit $E \otimes_F F'$ permet de créer un espace d'accueil commun. Dès lors qu'on montre qu'il s'agit encore d'un corps, on peut suivre et contrôler précisément le comportement de nos éléments algébriques face à cette extension.

Lemme 4.19. *Soit $F \subset F'$ une inclusion de champs tels que F est algébriquement clos dans F'. Soit E une extension finie de F.*

a) L'anneau $E' = E \otimes_F F'$ est encore un champ.

b) Le champ E est algébriquement clos dans E', où on voit l'inclusion $E \subset E'$ via le plongement canonique $i : E \to E \otimes F'$ $x \mapsto x \otimes 1_{F'}$.

Démonstration. a) Supposons que $E = F(y)$ pour un $y \in E$. Cela suffit pour traiter le cas où E/F est une extension séparable par le théorème de l'élément primitif.

Soit $P \in F[t]$ le polynôme minimum de y sur F. Dans tout champ algébriquement clos contenant F, les zéros de P sont algébriques sur F. En conséquence, pour toute factorisation de P en polynômes moniques dans $F'[t]$, les coefficients des facteurs sont aussi algébriques sur F puisqu'ils sont des sommes/ produits des zéros de P. Comme F est algébriquement clos dans F', ces coefficients sont dans F. Donc si P se factorise dans F', il se factorisait déjà dans F. On conclut que P est irréductible dans $F'[t]$. On a alors l'isomorphisme $E \simeq F[t]/\langle P\rangle$ par le premier théorème d'isomorphie en considérant l'isomorphisme $\Phi : F[t] \to E \quad Q(t) \mapsto Q(y)$ où $\ker\Phi = \langle P\rangle$, $\mathrm{Im}\Phi = F(y) = E$.

On a alors, en appliquant 4.16

$$\begin{aligned} E' = E \otimes_F F' &\simeq F[t]/\langle P\rangle \otimes_F F' \\ &\simeq (F[t] \otimes_F F')/\Gamma(\langle P\rangle) \\ &\simeq F'[t]/\langle P\rangle \end{aligned}$$

qui est un champ vu que P est irréductible sur $F'[t]$, ce qui fait de $\langle P\rangle$ un idéal maximal.

Si l'extension était purement inséparable, par définition, tout élément $y \in E$ vérifie $y^{p^n} = a$ pour n minimal avec $a \in F$. Le polynôme minimum est $P(t) = t^{p^n} - a$. Si ce polynôme n'était pas irréductible sur F, on aurait un polynôme de plus petit degré qui annule y de la forme $(t-y)^d$ ce qui impliquerait qu'une plus petite puissance de p de y appartiendrait à F contredisant la minimalité du n choisi. Alors, si a n'a pas de racine p^n-ième dans F', le polynôme $t^{p^n} - a$ ne possède pas de racine dans F' donc il reste irréductible sur F'. Alors $E' = E \otimes F' \simeq F'[t]/\langle(t^{p^n} - a)\rangle$ est un champ. Si a possédait une racine p^n-ième dans F', notons-la β, alors β étant algébrique sur F, il appartiendrait à F car F est algébriquement clos dans F'. Ce qui contredirait l'irréductibilité de $t^{p^n} - a$ sur F.

b) Soit $x \in E'$ algébrique sur E. Montrons que $x \in E$.

Soit $Q \in E[t]$ le polynôme minimum de x sur E. Considérons E_1 le corps de décomposition de Q sur E. C'est une extension finie de F qui vérifie le premier point, c'est-à-dire pour laquelle $E_1' = E_1 \otimes_F F'$ est un champ. Le polynôme Q se factorise en facteurs linéaires dans $E_1[t]$. Puisque x est racine de Q et que Q est scindé dans E_1, x appartient nécessairement à E_1. Cependant, x appartient aussi à $E' = E \otimes_F F'$. On regarde alors l'intersection $E_1 \cap (E \otimes_F F')$ au sein du champ E_1'. On a $E_1 \subset E_1'$ correspond aux éléments qui n'ont aucune composante dans F'. D'autre part, $E \otimes_F F' \subset E_1 \otimes_F F'$ car $E \subset E_1$ et ces éléments s'écrivent $\sum_i a_i \otimes f_i'$, $a_i \in E$, $f_i' \in F'$. Un tel élément appartient à E_1 si $a_i = 0$ pour tout $i > 0$ et $a_0 \in E_1$. Dans l'intersection, on retrouve uniquement les éléments de la forme $a_0 \otimes 1 \in E$, c'est-à-dire $E_1 \cap (E \otimes_F F') = E$. Finalement, $x \in E$ et E est bien algébriquement clos dans E'.

Si l'extension E/F est purement inséparable, le raisonnement s'adapte de la manière suivante. Par définition, pour tout élément $x \in E'$, il existe $m > 0$ tel que $x^{p^m} \in E$. Considérons l'extension $E_1 = E(x)$. C'est une extension finie de E, et par transitivité, une extension finie de F. On peut alors appliquer le point a) à E_1 : $E_1' = E_1 \otimes_F F'$ est un champ. Puisque x appartient à E_1 par construction et que x est également dans E' par hypothèse, on se retrouve à nouveau dans la situation où l'on doit examiner l'intersection $E_1 \cap (E \otimes_F F')$. La conclusion se fait de la même manière que pour le premier cas.

□

Corollaire 4.20. *Soient $F \subset F' \subset F''$ des inclusions de champs. Supposons que $x, y \in F''$ sont algébriques sur F et $x \in F'(y)$. Posons $m = [F'(y) : F']$ et écrivons $x = \sum_{i=0}^{m-1} a_i y^i$ avec $a_i \in F'$. Alors, les a_i sont eux-mêmes algébriques sur F.*

Démonstration. On peut supposer que F est algébriquement clos dans F'. Si ce n'est pas le cas, on considère la clôture algébrique de F dans F'. Par le lemme 4.19, comme $F(y)$ est une extension finie de F puisque y est algébrique sur F, on a que $F(y) \otimes_F F'$ est un champ et $F(y)$ est algébriquement clos dans $F(y) \otimes_F F'$. De plus, $F(y) \otimes_F F' = F'(y)$ car si $P \in F[t]$ est le polynôme minimum de y, on a $F(y) \otimes_F F' \simeq F[t]/\langle P \rangle \otimes_F F' \simeq F'[t]/\langle P \rangle \simeq F'(y)$. Comme $x \in F'(y)$ est algébrique sur F par hypothèse, il l'est aussi sur $F(y)$ (puisque $F \subset F(y)$). Il s'en suit que $x \in F(y)$ car $F(y)$ est algébriquement clos dans $F'(y)$. Alors, $x = \sum_{i=0}^{m-1} a_i y^i \in F(y)$ et $a_i \in F$. Si F n'était pas algébriquement clos dans F', on arriverait à la conclusion que $a_i \in \overline{F}$, c'est-à-dire algébriques sur F. □

Le résultat suivant conclut la démonstration de notre théorème initial puisque la description de la clôture algébrique nous donne exactement ce que nous voulions montrer.

Théorème 4.21. *La clôture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t^{\mathbb{Q}}))$ est $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$.*

Démonstration. Par le théorème 2.3, $\mathbb{F}_q((t^{\mathbb{Q}}))_{\text{aut}}$ est inclus dans la clôture algébrique. Il reste à prouver la réciproque.

Soit $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ algébrique sur $\mathbb{F}_q(t)$. Par le lemme 4.15, il existe une troncature y de x qui est p-quasi-automatique, algébrique sur $\mathbb{F}_q(t)$ et génère une extension finie de $\mathbb{F}_q((t))$

contenant x. Notons que toute puissance de y a un support borné et est alors p-quasi-automatique par le corollaire 4.9. Comme $x \in \mathbb{F}_q((t))(y)$, on peut appliquer le corollaire 4.20 pour écrire x comme $\sum_{i=0}^{m-1} a_i y^i$ pour $m = [\mathbb{F}_q((t))(y) : \mathbb{F}_q((t))]$ et des a_i dans la clôture algébrique de $\mathbb{F}_q(t)$ dans $\mathbb{F}_q((t))$. Par le théorème de Christol, chaque a_i est p-automatique. Enfin, par le corollaire 2.10, x est p-quasi-automatique. □

Bibliographie

[1] Jean-Paul Allouche et Jeffrey Shallit, *Automatic sequences*, Cambridge University Press, 2003.

[2] Saugata Basu, Richard D. Pollack et M-F Roy, *Algorithms in real algebraic geometry*, Second Edition. Vol. 10, Algorithms and Computation in Mathematics, Springer, Berlin, 2006.

[3] Jean Berstel et Christophe Reutenauer, *Noncommutative rational series with applications*, 1re éd. Vol. v.Series Number 137, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, New York, 2010.

[4] Gilles Christol, *Ensembles presque periodiques k-reconnaissables*, Theoretical computer science **9** (1979), n° 1, p. 141-145.

[5] Gilles Christol, *Suites algébriques, automates et substitutions*, Bulletin de la S.M.F **108** (1980), p. 401-419.

[6] Jean Dieudonné, *Sur les produits tensoriels*, Annales scientifiques de l'École normale supérieure **64** (1947), p. 101-117.

[7] Kiran S Kedlaya, *Christol's theorem and its analoguefor generalized power series, part 1*, slides, disponible via l'URL `<http://math.ucsd.edu/~kedlaya/slides/>`.

[8] Kiran S Kedlaya, *Christol's theorem and its analoguefor generalized power series, part 2*.

[9] Kiran S Kedlaya, "Newtons Polygons", eng, in : *p-adic differential equations*, Second edition., Cambridge studies in advanced mathematics ; 198, Cambridge University Press, Cambridge, United Kingdom ; New York, NY, 2022, chap. 2, ISBN : 1-009-27565-8.

[10] Kiran S Kedlaya, *Power series and p-adic algebraic closures*, Journal of number theory **89** (2001), n° 2, p. 324-339.

[11] Kiran S Kedlaya, *Topics in Algebraic Geometry*, disponible via l'URL `<https://kskedlaya.org/18.727/notes.html>`.

[12] Kiran S. Kedlaya, *Finite automata and algebraic extensions of function fields*, Journal de theorie des nombres de bordeaux **18** (2006), n° 2, p. 379-420.

[13] Kiran S. Kedlaya, *On the algebraicity of generalized power series*, Beiträge zur Algebra und Geometrie **58** (2017), n° 3, p. 499-527.

[14] Kiran S. Kedlaya, *The algebraic closure of the power series field in positive characteristic*, Proceedings of the American Mathematical Society **129** (2001), n° 12, p. 3461-3470.

[15] Serge Lang, *Algèbre*, 3e éd., 2002.

[16] Christophe Rose, *Extensions finies du corps Fq(t) et automates finis* (Federico Pellarin, éds), Mémoire, 2006.

[17] Benjamin Schraen, *Théorie des nombres* (Université Paris-Saclay, éds), Notes de cours.

[18] Jean-Pierre Serre, *Corps locaux*, Hermann, 1968.