Extensions finies du corps $\mathbb{F}_q(t)$ et automates finis

Christophe Rose

Mémoire de M2 rédigé sous la direction de
Federico Pellarin

M2 « Algèbre et Géométrie » de l'université Paris 6 – Pierre et Marie Curie
Année universitaire 2006/2007

Introduction

Ce texte est le résumé d'un article écrit par Kiran S. Kedlaya en 2005 sur les racines des polynômes de $\mathbb{F}_q(t)[X]$ et les automates finis, où $\mathbb{F}_q(t)$ est l'ensemble des fractions rationnelles à une indéterminée t sur un corps fini $\mathbb{F}_q$. Les automates finis sont des machines abstraites utilisées pricipalement en informatique, dans le cadre de la reconnaissance des langages.

On se donne K un corps (commutatif), et P un polynôme dont les coefficients sont dans $K(t)$. Il faut commencer par définir dans quel corps on cherche les racines de P.

Prenons $1 + t \in K(t)$, avec K de caractéristique 0. Pour définir la racine carrée de ce polynôme, on peut utiliser les développements en série entière. Ainsi, la série formelle :

$$\sum_{n=0}^{+\infty} \frac{\frac{1}{2} \cdot \frac{-1}{2} \cdots (\frac{1}{2} - n)}{n!} t^n$$

a pour carré le polynôme $1 + t$.

Par contre, le polynôme t n'a pas de racine carrée dans les séries entières $K[[t]] = \left\{\sum_{n\in\mathbb{N}} a_n t^n | a_n \in K\right\}$, ni même dans les séries de Laurent $K((t)) = (K[[t]])[1/t]$.

Les séries de Puiseux en l'indéterminée t sont définies comme l'ensemble $K((t^{1/\infty})) = \bigcup_{n\geq 1} K((t^{1/n}))$ dont les éléments sont les séries de Laurent en $t^{1/n}$ pour un certain entier n. Les séries de Puiseux sur K forment un corps.

Un théorème de Puiseux [Ser79, Chapitre 2.4] dit que si K est algébriquement clos et de caractéristique 0, alors l'ensemble des séries de Puiseux à une indéterminée sur le corps K est algébriquement clos.

Ce théorème est faux en caractéristique $p > 0$. En effet, Chevalley a montré que le polynôme $X^p - X - t^{-1}$ n'a pas de racine dans $\overline{\mathbb{F}_p}((t^{1/\infty}))$. Ce phénomène est propre aux extensions algébriques L/K de dimension p telles que L et K ont le même corps résiduel.

Si on essaye quand même de résoudre l'équation, on trouve une « somme » de la forme $t^{-1/p} + t^{-1/p^2} + \ldots + c$ avec $c \in \mathbb{F}_p$.

Pour donner un sens à cette somme, il faut se placer dans un corps encore plus grand, le corps des séries de Hahn $\mathbb{F}_p((t^{\mathbb{Q}}))$. Ce corps est un ensemble de séries formelles dont les exposants sont rationnels, avec une certaine condition pour que la valuation, l'addition et la multiplication soient bien définies. Nous définirons précisément les séries de Hahn dans le deuxième chapitre.

Le corps des séries de Hahn $K((t^{\mathbb{Q}}))$ est algébriquement clos dès que K est algébriquement clos. Nous chercherons donc les éléments algébriques sur

$\mathbb{F}_q(t)$ dans le corps des séries de Hahn $\mathbb{F}_{q'}((t^{\mathbb{Q}}))$ sur une extension finie $\mathbb{F}_{q'}$ de $\mathbb{F}_q$ (q' étant une puissance assez grande de q, qui est lui-même la puissance d'un nombre premier p).

Le théorème de Christol dit qu'une série entière de $\mathbb{F}_q[[t]]$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si elle est *p-automatique*, c'est-à-dire que ses coefficients sont engendrés d'une certaine manière par un automate fini.

Ce théorème transforme le problème de savoir si une série entière est algébrique ou transcendante sur $\mathbb{F}_q(t)$ en un problème d'informatique, sur les automates finis. On a alors accès à toute une théorie sur les automates finis et les langages rationnels pour résoudre des problèmes dont l'énoncé est purement algébrique.

Le théorème de Kedlaya, dont nous donnerons deux preuves ici (l'une essentiellement théorique et l'autre plus pratique), est une généralisation du théorème de Christol. Il permet de transformer le problème de savoir si une série de Hahn de $\mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique ou transcendante sur $\mathbb{F}_q(t)$ en un problème sur les automates finis.

La preuve constructive du théorème de Kedlaya permet même, à partir d'un polynôme de $\mathbb{F}_q(t)[X]$, de calculer explicitement ses racines.

Après des préliminaires sur les automates finis puis en algèbre, nous énoncerons et nous démontrerons dans le troisième chapitre les théorèmes de Christol et de Kedlaya.

Dans les deux derniers chapitres, nous étudierons la décomposition des polynômes tordus, ce qui nous permettra de donner une preuve constructive du théorème de Kedlaya.

Table des matières

1 Préliminaires sur les automates finis

Ce chapitre va nous permettre de rappeler des notions sur les automates finis, ainsi que de fixer les notations.

Pour décrire un algorithme qui calcule la valeur $f(x)$ d'une fonction f en un rationnel x, on peut utiliser une « machine » qui prend en entrée x et qui renvoie en sortie $f(x)$.

Les automates finis sont des machines qui lisent des suites finies de lettres (les *mots*) et qui renvoient une valeur dans un ensemble fini, généralement $\{0,1\}$. Ils sont d'usage commun en informatique. Entre autres, ils sont très efficaces pour rechercher une chaîne de caractères dans une autre.

Les automates peuvent aussi prendre des rationnels en entrée : si b est un entier supérieur ou égal à 2, l'écriture en base b d'un rationnel positif est une suite (parfois infinie) de chiffres contenant une virgule.

1.1 Automates finis et langages rationnels

Définition. On se donne un ensemble A fini et non vide, qu'on appelle l'*alphabet*. Ses éléments sont appelés les *lettres*. Pour i un entier naturel, on écrit les éléments du produit cartésien A^i par juxtaposition : ainsi (a,b,b) est écrit abb. On les appelle les *mots* de *longueur* i. Il n'y a qu'un seul mot de longueur 0, qu'on note ε.

Définition. On note $A^* = \bigcup_{i\in\mathbb{N}} A^i$ l'ensemble des mots sur l'alphabet A. On dit également que A^* est l'*étoile* de A. Si $u = u_1 \dots u_m$ et $v = v_1 \dots v_n$ sont deux mots, le *concaténé* de u et de v est le mot $uv = u_1 \dots u_m v_1 \dots v_n$ obtenu par juxtaposition des lettres.

Ainsi, $\varepsilon u = u\varepsilon = u$ pour tout mot $u \in A^*$.

Définition. On appelle *langage* (sur l'alphabet A) un sous-ensemble quelconque de A^*.

- Si L et M sont deux langages, on note $LM = \{uv | u \in L, v \in M\}$ le langage dont les éléments sont les concaténés des mots de L avec les mots de M.
- On note $(L|M) = L \cup M$ l'union ensembliste de L et de M.
- On note $L^* = \bigcup_{i\in\mathbb{N}} L^i = \{\varepsilon\} \cup L \cup LL \cup LLL \cup \dots$ l'*étoile* du langage L.

Ainsi, l'ensemble des mots A^* est l'étoile du langage noté A des mots à une lettre.

Un langage peut être vu comme un élément de $\mathcal{P}(A^*)$. Nous allons désormais nous intéresser à une certaine classe de langages, c'est-à-dire un sous-

ensemble de $\mathcal{P}(A^*)$.

Définition. On note $\mathrm{Rat}(A)$ le plus petit sous-ensemble $\mathcal{L}$ de $\mathcal{P}(A^*)$ qui vérifie les propriétés suivantes :

- $\emptyset \in \mathcal{L}$ et $\forall a \in A, \{a\} \in \mathcal{L}$
- $\forall L,M \in \mathcal{L}, LM \in \mathcal{L}$
- $\forall L,M \in \mathcal{L}, (L|M) \in \mathcal{L}$
- $\forall L,M \in \mathcal{L}, L^* \in \mathcal{L}$

Cet ensemble est appelé la *classe des langages rationnels* (ou *réguliers*) sur l'alphabet A.

Ainsi, tout langage formé d'un nombre fini de mots est un langage rationnel.

Pour décrire un langage rationnel, on utilise des expressions dites *expressions rationnelles*, qui reprennent les notations ci-dessus. Une définition rigoureuse d'expression rationnelle est donnée dans [AS03, Chapitre 1.3] ou dans [Sak03, Chapitre 1.4.1].

Par exemple, pour $A = \{a,b\}$ on note ab^* le langage $\{a,ab,abb,\ldots\}$ des mots formés par la concaténation d'un a puis d'un nombre quelconque de b, $(a|b|ab)$ le langage à trois éléments $\{a,b,ab\}$, et $a(a|b)^*b$ ou aA^*b l'ensemble des mots qui commencent par a et qui finissent par b.

Remarque. Pour des raisons de concision, a peut dénoter la lettre a, le mot à une lettre a, et également le langage $\{a\}$.

Définition. Un *automate fini* (*non-déterministe*) est un quintuplet $M = (Q,A,I,F,\delta)$ où :

- Q est un ensemble fini (l'ensemble des *états* de l'automate) ;
- A est un ensemble fini non vide (l'*alphabet d'entrée*) ;
- I et F sont des sous-ensembles de Q (les *états initials* et les *états finals*) ;
- δ est un sous-ensemble de $Q \times A \times Q$ (la *fonction de transition*).

On note $q_0 \xrightarrow{a} q_1$ si $(q_0,a,q_1) \in \delta$. Le *graphe de transition* de l'automate est le graphe dont les sommets sont les éléments de Q, et où les arêtes sont étiquetées par des éléments de A. Il y a une arête d'un élément q_0 de Q à un autre élément q_1 de Q, étiquetée par $a \in A$ si et seulement si $q_0 \xrightarrow{a} q_1$.

Généralement, on dessine aussi des flèches qui rentrent à chaque état de I et des flèches qui sortent de chaque état de F, ces flèches n'étant pas étiquetées.

Comme exemple, voici le graphe de transition de l'automate $(\{q_0,q_1\}, \{0,1\}, \{q_0\}, \{q_0\}, \{(q_0,0,q_0),(q_0,1,q_1),(q_1,0,q_1),(q_1,1,q_0)\})$.

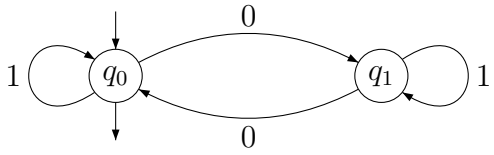

FIG. 1 – *Exemple d'automate (automate de Thue-Morse)*

Définition. On étend l'ensemble $\delta \subset Q \times A \times Q$ à l'ensemble $\delta^* \subset Q \times A^* \times Q$ défini de la façon suivante : si u est un mot de longueur n, alors $(q_0,u,q_n) \in \delta^*$ si et seulement s'il existe des états $q_1, \ldots, q_{n-1}$ tels que $q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} \ldots \xrightarrow{u_{n-1}} q_{n-1} \xrightarrow{u_n} q_n$. On écrit alors $q_0 \xrightarrow{u} q_n$.

Définition. On dit qu'un mot $u \in A^*$ est *reconnu* par l'automate s'il existe des états $i \in I$ et $f \in F$, tels que $i \xrightarrow{u} f$. On dit qu'un langage L est *reconnu* par un automate si cet automate reconnaît tous les mots de L et ne reconnaît aucun autre mot de A^*. Deux automates sont dit *équivalents* s'ils reconnaissent le même langage.

Remarque. Pour tout alphabet A, il existe un automate à un état qui reconnaît le langage A^* tout entier, à savoir $M = (Q,A,Q,Q,Q \times A \times Q)$, où Q est un ensemble à un élément.

Exemple. L'automate de Thue-Morse reconnaît le langage sur l'alphabet $\{0,1\}$ des mots qui contiennent un nombre pair de 1. Ce langage est rationnel, il peut être décrit par l'expression $(0^*10^*1)^*0^*$.

On peut dire qu'une expression rationnelle *engendre* un langage (rationnel), tandis qu'un automate *reconnaît* un langage.

Définition. Un automate fini (non-déterministe) est dit *complet* (respectivement *déterministe*) si pour tout $q \in Q$ et tout $a \in A$, il y a au moins (au plus) un $q' \in Q$ tel que $q \xrightarrow{a} q'$, et si I est de cardinal supérieur ou égal (inférieur ou égal) à 1.

Remarque. Selon la définition, un automate fini déterministe est un automate fini non-déterministe vérifiant certaines conditions.

Si M est un automate fini déterministe, on peut définir δ non seulement comme un sous-ensemble de $Q \times A \times Q$ mais également comme une fonction dont l'ensemble de définition est contenu dans $Q \times A$ et dont l'ensemble d'arrivée est Q, qui à un élément $(q,a) \in Q \times A$ associe (s'il existe) l'unique q' tel que $(q,a,q') \in \delta$.

On peut alors définir δ^* comme une fonction dont l'ensemble de définition est contenu dans $Q \times A^*$ et dont l'ensemble d'arrivée est Q, qui à un élément $(q,u) \in Q \times A^*$ associe (s'il existe) l'unique q' tel que $(q,u,q') \in \delta^*$.

Notons que si l'automate fini est déterministe et complet, alors l'ensemble de définition des deux fonctions δ et δ^* sont respectivement $Q \times A$ et $Q \times A^*$.

Il existe un algorithme simple, dont l'implémentation est rapide et nécéssite peu de mémoire, pour voir si un mot $u \in A^*$ est reconnu par un automate déterministe complet.

On part de l'état initial, puis on lit successivement de gauche à droite chaque lettre du mot. À chaque lettre a lue, on passe de l'état q à l'état $\delta(q,a)$.

On se retrouve après avoir lu toutes les lettres dans un certain état q'. Si cet état est final, alors le mot u est reconnu par l'automate. Sinon, u n'est pas reconnu par l'automate.

Avec des automates finis non déteministes pas forcément complets, on peut utiliser une variante de cet algorithme. La différence est qu'on ne garde pas en mémoire un seul état, mais un ensemble d'états. Cela explique la terminologie déterministe/non-déterministe.

Tout automate fini non-déterministe est équivalent à un automate complet. Pour construire un automate complet qui reconnaît le même langage, il suffit d'ajouter à l'automate de départ un état *puits* $p \notin Q$ qui n'est ni initial, ni final, et à chaque couple (q,a) tel que $\{q\} \times \{a\} \times Q \cap \delta = \emptyset$, de rajouter la transition $q \xrightarrow{a} p$.

Si un automate fini est complet, et si tout état de cet automate est final, alors le langage reconnu par cet automate est A^*.

Si un automate fini déterministe et complet reconnaît le langage L, l'automate obtenu en changeant F en $Q \backslash F$ est toujours un automate déterministe complet qui reconnaît le langage $A^* \backslash L$.

Définition. On fixe un automate fini non-déterministe $M = (Q,A,I,F,\delta)$. Un état q est dit *accessible* s'il existe $i \in I$ et un mot $u \in A^*$ tel que $i \xrightarrow{u} q$. Un état q est dit *co-accessible* s'il existe $f \in F$ et un mot $u \in A^*$ tel que $q \xrightarrow{u} f$. Un automate est dit *propre* si tous ses états sont accessibles et *émondé* si de plus tous ses états sont co-accessibles.

En prenant un automate fini et en retirant une partie de ses états qui ne sont pas à la fois accessibles et co-accessibles, on obtient un automate équivalent. Si on rend propre un automate complet, il reste complet. Mais si on le rend émondé, il n'est généralement plus complet car tout état puits n'est pas co-accessible.

Le théorème qui suit est un résultat fondamental en théorie des automates. Pour une démonstration complète, voir [AS03, Théorème 4.1.5] ou

[Sak03, Chapitre 1.2].

Théorème 1.1 (Kleene). *Soit A un alphabet et L un langage sur cet alphabet. Alors les trois propositions suivantes sont équivalentes :*

- *le langage L est rationnel ;*
- *il existe un automate fini déterministe $M = (Q,A,I,F,\delta)$ qui reconnaît L ;*
- *il existe un automate fini non-déterministe $M = (Q,A,I,F,\delta)$ qui reconnaît L.*

Une conséquence de ce théorème est que pour tout automate fini non-déterministe, il existe un automate fini équivalent qui est propre, complet et déterministe.

Une autre conséquence est que la classe des langages rationnels $\mathrm{Rat}(A)$ est non seulement stable par concaténation, union finie et étoile, mais aussi par complémentaire et par intersection finie.

La proposition suivante, appelée *lemme de l'étoile* ou *lemme de pompage* permet de caractériser les langages rationnels. Elle est très utile pour montrer qu'un langage n'est pas rationnel.

En fait, nous ne donnons qu'une seule forme de cette proposition. Il y a d'autres énoncés plus complexes, qui proviennent tous de la simple transcription en termes de langages du fait qu'un automate ne possède qu'un nombre fini d'états.

Proposition 1.2. *Soit $L \subset A^*$ un langage rationnel. Il existe un entier N tel que pour tout mot $u \in L$ de longueur supérieure à N, u se factorise en $u = vwx$ où vw est de longueur inférieure à N, w n'est pas le mot vide, et tel que $vw^*x \subset L$.*

Démonstration. Soit $M = (Q,A,\{i\},F,\delta)$ un automate fini déterministe complet et propre qui reconnaît le langage L. Soit N le cardinal de Q. Fixons un mot $u \in L$ de longueur strictement supérieure à N. En lisant les $N+1$ premières lettres de u, on passe au moins deux fois par l'un des états $q \in Q$. En lisant u en entier, on passe de i à $f \in F$.

u se décompose donc en $u = vwx$, où vw est de longueur inférieure ou égale à $N+1$, w n'est pas de longueur nulle, et $i \xrightarrow{v} q \xrightarrow{w} q \xrightarrow{x} f$. On en déduit que pour tout $u_n = vw^nx$ avec $n \in \mathbb{N}$, $i \xrightarrow{u_n} f$. Par conséquent $vw^*x \subset L$. □

Cette répétition n'est pas sans rappeler la répétition d'une suite de chiffres dans le développement infini d'un rationnel dans une certaine base b.

Exemple. Prenons deux exemples sur l'alphabet $A = \{a,b\}$.

Le langage $L = \{a^n b^n | n \in \mathbb{N}\}$ n'est pas rationnel. Si le contraire était vrai, il existerait des entiers N, $i \leq N$ et $j > 0$ tels que $a^N b^N = a^i a^j a^{N-i-j} b^N$ et $a^{N+xj} b^N \in L$ pour tout entier $x \geq -1$, ce qui amène une contradiction.

Le langage M formé des mots contenant le même nombre de a et de b n'est pas rationnel. En effet, s'il l'était, alors l'intersection de M et du langage (a^*b^*), égale à L, serait rationnelle, ce qui n'est pas le cas.

Définition. Soit A un alphabet, u un mot sur A et L un langage quelconque sur A. On appelle $u^{-1}L = \{v \in A^* | uv \in L\}$ le *quotient à gauche* de L par u ou encore le *résiduel* de L par u.

Le théorème suivant permet de construire à partir d'un langage rationnel un automate formé du nombre minimal d'états possible. La preuve est écrite dans [AS03, Théorème 4.1.8] ou dans [Sak03, Chapitre 1.3.3].

Théorème 1.3 (Myhill-Nerode). *Un langage L sur un alphabet A est rationnel si et seulement si lorsque u parcourt A^*, il n'y a qu'un nombre fini de langages du type $u^{-1}L$ différents.*

Dans ce cas, il existe un automate fini déterministe complet propre reconnaissant L, dont les états sont étiquetés par ces $u^{-1}L$, et qui — à renommage des états près — possède strictement moins d'états que tout autre automate fini déterministe équivalent.

Cet automate est $M = (\{u^{-1}L | u \in A^*\}, A, \{L\}, \{u^{-1}L | u \in L\}, \delta)$ où pour tout mot $u \in A^*$ et toute lettre $a \in A$, $u^{-1}L \xrightarrow{a} (ua)^{-1}L$.

Définition. Soit $M = (Q,A,I,F,\delta)$ un automate fini non-déterministe. L'*automate miroir* de M est l'automate $\overline{M} = (Q,A,F,I,\overline{\delta})$, où $\overline{\delta}$ est l'ensemble des $(q',a,q) \in Q \times A \times Q$ tels que $(q,a,q') \in \delta$. Soit $u = u_1 \dots u_n$ un mot de longueur n sur un alphabet A. Le *retourné* (ou *miroir*) du mot u est le mot $\overline{u} = u_n \dots u_1$ de longueur n. Soit L un langage sur l'alphabet A. Le *miroir* du langage L est le langage $\overline{L}$ formé des retournés des mots de L.

La proposition suivante est donnée sans preuve.

Proposition 1.4. *Si un automate M reconnaît le langage L, alors l'automate miroir $\overline{M}$ reconnaît le langage miroir $\overline{L}$.*

L'ensemble des langages rationnels est donc stable par miroir.

1.2 Généralisation des automates

À l'aide de la fonction caractéristique d'un sous-ensemble L de A^*, on peut voir les automates finis comme des fonctions de A^* dans $\{0,1\}$. Les *automates à sortie* assouplissent les conditions sur l'ensemble d'arrivée.

Définition. Un *automate (fini déterministe complet) à sortie* est un 6-uplet

$(Q,A,\{i\},\delta,\Delta,\tau)$ où :

- Q est un ensemble fini (l'ensemble des *états*) ;
- A est un ensemble fini (*l'alphabet d'entrée*) ;
- $\{i\}$ est un sous ensemble de Q de cardinal 1 (*l'état initial*) ;
- δ est une fonction de $Q \times A$ dans Q (*la fonction de transition*) ;
- Δ est un ensemble fini (*l'ensemble de sortie*) ;
- τ est une fonction de Q dans Δ (*la fonction de sortie*).

On associe à cet automate la fonction $f : A^* \to \Delta$ qui à un mot u associe $\tau(q)$ où q est l'état tel que $i \xrightarrow{u} q$.

Définition. Soient A et Δ des ensembles finis. Une fonction $f : A^* \to \Delta$ est dite *automatique* s'il existe un automate à sortie $(Q,A,\{i\},\delta,\Delta,\tau)$ associé à cette fonction.

Remarque. Si $f : A^* \to \Delta$ est une fonction automatique et si L est un langage rationnel, on dit également que la restriction de f à L, $f_{|L} : L \to \Delta$ est une fonction automatique.

La fonction caractéristique d'un langage rationnel est évidemment automatique. Inversement, si $f : A^* \to \Delta$ est une fonction automatique, alors tous les langages $f^{-1}(d)$ pour $d \in \Delta$ sont rationnels.

On aura aussi besoin d'une autre variante d'automates, les transducteurs. Pour des démonstrations complètes, voir [AS03, Chapitre 4.3] ou [Sak03, Chapitre 4].

Définition. Un *transducteur* (fini déterministe complet) est un 6-uplet $T = (Q,A,\{i\},\delta,B,\lambda)$ où :

- Q est un ensemble fini (l'ensemble des états) ;
- A est un ensemble fini (l'alphabet d'entrée) ;
- $\{i\}$ est un sous ensemble de Q de cardinal 1 (l'état initial) ;
- δ est une fonction de $Q \times A$ dans Q (la fonction de transition) ;
- B est un ensemble fini (l'alphabet de sortie) ;
- λ est une fonction de $Q \times A$ dans B^* (la fonction de sortie).

Définition. Si $T = (Q,A,\{i\},\delta,B,\lambda)$ est un transducteur, on appelle *fonction de transduction* (ou *fonction de traduction*) la fonction $\varphi_T : A^* \to B^*$ définie de la manière suivante : si $u = u_1 \dots u_n$ est un mot de A^*, et si on note $i = q_0 \xrightarrow{u_1} q_1 \xrightarrow{u_2} \dots \xrightarrow{u_n} q_n$, alors $\varphi_T(u) = \lambda(q_0,u_1) \dots \lambda(q_{n-1},u_n)$.

Une propriété utile des transducteurs est énoncée ci-dessous. Elle est prouvée dans [AS03, Théorèmes 4.3.6 et 4.3.8].

Proposition 1.5. *Soit T un transducteur. Si $L \subset A^*$ est un langage rationnel, alors $f_T(L) = \{f_T(u) | u \in L\}$ est un langage rationnel sur l'alphabet B.*

Si $M \subset B^*$ est un langage rationnel, alors ${f_T}^{-1}(M) = \{u \in A^* | f_T(u) \in M\}$ est un langage rationnel sur A.

Exemple. Prenons le transducteur d'alphabet d'entrée et de sortie $\{a,b,c\}$, dont la fonction de sortie est

$$\lambda : \begin{cases} (q_0,a) \mapsto \varepsilon & (q_0,b) \mapsto b & (q_0,c) \mapsto c \\ (q_1,a) \mapsto aa & (q_1,b) \mapsto \varepsilon & (q_1,c) \mapsto ac \\ (q_2,a) \mapsto aba & (q_2,b) \mapsto abb & (q_2,c) \mapsto ca \end{cases}$$

et dont le graphe de transition est donné par la figure suivante. Alors la fonction de transition effectue une recherche/remplacement, qui transforme toutes les occurences du mot *abc* par le mot *ca*.

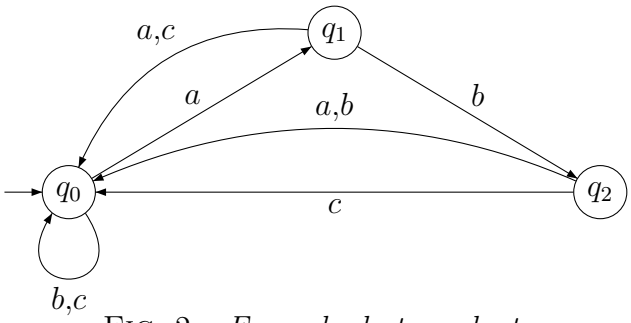

FIG. 2 – *Exemple de transducteur*

1.3 Écritures en base b et reconnaissance

Les automates à sortie sont associés à des fonctions dont l'ensemble de départ est un langage de mots et dont l'ensemble d'arrivée est fini.

Comme nous allons travailler avec des fonctions de $\mathbb{Q}$ dans le corps fini $\mathbb{F}_q$, le problème sera de voir $\mathbb{Q}$ comme un ensemble de mots.

Définition. Fixons b un entier naturel supérieur ou égal à 2, qu'on appelle la *base*. On note $S_b = \mathbb{Q}^+ \cap \mathbb{Z}[1/b]$ l'ensemble des nombres rationnels positifs qui ont un nombre fini de chiffres après la virgule lorsqu'ils sont écrits en base b.

Définition. Soit $A_b = \{"0"; \ldots; "b-1"; ","\}$ un alphabet à $b+1$ lettres, et Σ_b le langage sur A_b défini par l'expression rationnelle :

$$((1|...|b-1)(0|...|b-1)^*|\varepsilon)(",")((0|...|b-1)^*(1|...|b-1)|\varepsilon)$$

C'est l'ensemble des mots de A_b^* qui ne contiennent qu'une seule virgule, et qui ne commencent ni ne se terminent par 0.

On voit facilement que l'ensemble des écritures des éléments de S_b est contenu dans le langage Σ_b, quitte à prendre la convention que 0 s'écrit ",", que les nombres entiers se terminent par une virgule et que les éléments plus petits que 1 commencent par une virgule.

Inversement, à un élément de Σ_b de la forme u,v, on lui associe sa *valeur* : $\sum_{i=1}^{m} u_i b^{m-i} + \sum_{i=1}^{n} v_i b^{-i}$, qui est un élément de S_b.

Définition. Un sous-ensemble de $\mathbb{Q}$ est dit *b-rationnel* (ou *b-régulier*) s'il est inclus dans S_b et si l'ensemble des écritures en base b de ses éléments forme un langage rationnel.

Définition. Une fonction $f : S_b \to \Delta$ (où Δ est un ensemble fini) est dite *b-automatique* s'il existe un automate à sortie qui à l'écriture d'un élément $x \in S_b$ en base b renvoie $f(x)$. Une suite $(a_i)_{i\in\mathbb{N}}$ est dite *b-automatique* s'il existe un automate à sortie qui à l'écriture d'un entier i en base b renvoie a_i.

Proposition 1.6. *Si $f : S_b \to \Delta_f$ et $g : S_b \to \Delta_g$ sont deux fonctions b-rationnelles et si $O : \Delta_f \times \Delta_q \to \Delta$ est une fonction quelconque, alors $h : S_b \to \Delta : x \mapsto O(f(x),g(x))$ est b-rationnelle.*

Proposition 1.7. *Soit S un sous-ensemble de S_b, et r et s deux entiers naturels avec $r > 0$ tels que $rS + s$ est inclus dans S_b. Alors S est b-rationnel si et seulement si $rS + s$ est b-rationnel.*

Démonstration. Il existe un transducteur qui calcule la transformation affine $x \mapsto rx + s$ sur les retournés des écritures des nombres, comme dans [AS03, Lemmes 4.3.9 et 4.3.11]. Comme le miroir d'un langage rationnel est toujours un langage rationnel, cette proposition résulte du lemme sur les transducteurs.

□

Remarque. Il n'existe pas de transducteur qui à partir des écritures directes calcule une multiplication par un nombre qui n'est pas une puissance de b, ou une addition par un nombre non nul. Cela vient du fait qu'un transducteur n'a qu'un nombre fini d'états, et que les retenues se propagent de droite à gauche sur les écritures directes.

2 Préliminaires algébriques

2.1 Conditions générales d'algébricité

Nous commençons par des rappels élémentaires d'algèbre bien connus. Pour des définitions et des démonstrations rigoureuses, voir [Bou81].

Définition. Soit L/K une extension de corps quelconques. On dit qu'un

élément x de L est *algébrique sur* K s'il vérifie l'une des propriétés équivalentes de la proposition suivante :

Proposition 2.1. *Soit L/K une extension de corps, et x un élément de L. Alors les assertions suivantes sont équivalentes :*

- *il existe un polynôme P de $K[X]$, non nul, tel que $P(x) = 0$;*
- *$K[x]$ est un K-espace vectoriel de dimension finie ;*
- *$K[x] = K(x)$;*
- *$K(x)$ est un K-espace vectoriel de dimension finie ;*
- *la suite $(x^i)_{i\in\mathbb{N}}$ est linéairement liée sur K ;*
- *si $(P_i)_{i\in\mathbb{N}}$ est une suite de polynômes de $K[X]$ linéairement indépendante sur K, alors la suite $(P_i(x))_{i\in\mathbb{N}}$ est linéairement liée sur K.*

Remarque. Si K est un corps de caractéristique p, et si on prend la suite de polynômes $P_i = X^{p^i}$, on obtient le *lemme d'Ore* : un élément $x \in L$ est algébrique sur K si et seulement s'il est racine d'un polynôme de la forme $\sum_{j=0}^{n} a_j X^{p^j}$. Nous verrons dans le chapitre 4 les propriétés de ces polynômes, appelés les *polynômes additifs*.

Proposition 2.2. *Soit L/K une extension de corps. Si x et y sont deux éléments de L qui sont algébriques sur K, alors leur somme $x + y$ et leur produit xy sont des éléments de L algébriques sur K.*

Si x est un élément non nul du corps L, alors son inverse $1/x$ est un élément de L algébrique sur K.

Définition. Si L/K est une extension de corps, on dit que L est *algébrique sur* K (ou que l'extension L/K est algébrique) si tous ses éléments sont algébriques sur K. Un corps K est dit *algébriquement clos* si tout polynôme non nul de $K[X]$ admet au moins une racine dans K. Soit L/K est une extension de corps, on dit que L est une *clôture algébrique* de K si l'extension L/K est algébrique et si L est algébriquement clos.

Remarque. En utilisant le lemme de Zorn, on peut montrer que tout corps possède une clôture algébrique, et que si L et L' sont deux clôtures algébrique de K, elles sont K-isomorphes. On dira parfois « la » clôture algébrique d'un corps, qu'on notera $\overline{K}$.

Proposition 2.3. *Soit L/K une extension de corps. Si L est un K-espace vectoriel de dimension finie, alors L/K est une extension algébrique.*

Soit $M/L/K$ des extensions de corps. Si L est algébrique sur K, alors tout élément $x \in M$ algébrique sur L est algébrique sur K.

Remarque. Une extension algébrique n'est pas forcément de degré fini. Si K est un corps quelconque, sa clôture algébrique $\overline{K}$ n'est pas forcément un K-espace vectoriel de dimension finie. Par exemple, $\overline{\mathbb{Q}}$ n'est pas une extension finie sur $\mathbb{Q}$.

Pour faire des calculs à partir de la donnée d'un automate, nous aurons besoin d'associer à chaque état une certaine valeur. Il est nécéssaire de généraliser les conditions d'algébricité à des vecteurs à n coordonnées, où n est le nombre d'états de l'automate.

Définition. Soit L/K une extension de corps de caractéristique $p > 0$. L'*endomorphisme de Frobenius* $\sigma : L \to L : x \mapsto x^p$ se généralise aux vecteurs. Pour $(x_1, \ldots, x_n)$ un vecteur de L^n, on note $(x_1, \ldots, x_n)^\sigma = ({x_1}^\sigma, \ldots, {x_n}^\sigma)$.

Lemme 2.4. *Soit L/K une extension de corps de caractéristique $p > 0$, $v \in L^n$ et $w \in K^n$ deux vecteurs, et A et B deux matrices carrées de K de dimensions $n \times n$ dont au moins une est inversible.*

Si l'équation $Av^\sigma + Bv = w$ est vérifiée, alors les composantes de v sont algébriques sur K.

Démonstration. Si A est inversible, on peut se ramener au cas où A est la matrice identité I_n.

Il suffit alors de remarquer que le K-sous-espace vectoriel de L^n engendré par les v^{σ^i} est contenu dans le K-espace vectoriel $\{Cv + x | C \in \mathcal{M}_n(K), x \in K^n\}$ de dimension finie.

Dans le cas où seule la matrice B est inversible, on prend $\overline{L}$ une clôture algébrique de L et $\overline{K}$ une clôture algébrique de K contenue dans $\overline{L}$. L'endomorphisme de Frobenius est alors inversible.

Par le même raisonnement, on voit que les composantes de v sont algébriques sur $\overline{K}$, et donc sur K.

□

2.2 Les séries de Hahn

Nous allons généraliser les séries formelles en les écrivant sous la forme $\sum_{i \in \mathbb{Q}} x_i t^i$. En réalité, on pourrait considérer à la place de $\mathbb{Q}$ un groupe abélien totalement ordonné quelconque, mais nous n'en aurons pas besoin par la suite.

Pour des définitions et des preuves détaillées, voir [Pas77, Chapitre 13].

Définition. Un ensemble totalement ordonné E est dit *bien ordonné* si l'une des assertions équivalentes est vérifiée :

- tout sous-ensemble non vide de E possède un minimum ;
- il n'existe pas de suite strictement décroissante à valeur dans E ;
- toute suite décroissante de E est stationnaire.

Par exemple, les ensembles $\mathbb{Z}$, $\mathbb{R}$, $[0; +\infty[$, $\mathbb{Q}$, $\mathbb{Q} \cap [0; 1]$, $\{p^{-i} | i \in \mathbb{N}\}$ ne sont pas bien ordonnés. Par contre, tout sous-ensemble minoré de $\mathbb{Z}$, comme $\mathbb{N}$, est bien ordonné, ainsi que l'ensemble $\{1 - p^{-i} | i \in \mathbb{N}\}$.

À partir de maintenant, on ne considère que les sous-ensembles de $\mathbb{Q}$. Par abus, on prendra la convention que l'ensemble vide possède un minimum $+\infty$.

Proposition 2.5. *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.

Définition. Soit K un corps on appelle *série de Hahn* sur le corps K (ou *série de Hahn-Mal'cev-Neumann*) une série formelle $\sum_{i\in\mathbb{Q}} f(i)t^i$ où f est une fonction de $\mathbb{Q}$ vers K dont le *support* $\mathrm{Supp}(f) = \{i \in \mathbb{Q} | f(i) \neq 0\}$ est bien ordonné. On appelle *valuation* d'une série de Hahn $\sum_{i\in\mathbb{Q}} f(i)t^i$ le minimum du support de la fonction f.

Proposition 2.6. *Si $x = \sum x_i t^i$ et $y = \sum y_i t^i$ sont deux séries de Hahn, on définit leur somme comme la série formelle $x + y = \sum (x_i + y_i)t^i$. Cette somme est une série de Hahn. L'addition est associative et commutative, de neutre $0_K t^0$.*

Démonstration. Le support de cette série formelle est un sous-ensemble de $\mathrm{Supp}(f) \cup \mathrm{Supp}(g)$, avec $f : i \mapsto x_i$ et $g : i \mapsto y_i$. C'est donc un ensemble bien ordonné.

□

Proposition 2.7. *Si $x = \sum x_i t^i$ et $y = \sum y_i t^i$ sont deux séries de Hahn, on définit leur produit comme la série formelle $xy = \sum_{k\in\mathbb{Q}} \left(\sum_{i+j=k} x_i y_j \right) t^k$. Ce produit — dit de convolution — est bien défini et c'est une série de Hahn. La multiplication est associative et commutative, de neutre $1_K t^0$, et elle est distributive sur l'addition.*

Démonstration. Fixons un rationnel k. Notons les fonctions de $\mathbb{Q}$ dans K, $f : i \mapsto x_i$, $g : i \mapsto y_i$, $g' : i \mapsto y_{k-i}$.

Soit k un rationnel fixé. L'ensemble des i tels que x_i et y_{k-i} sont simultanément non nuls est à la fois dans un ensemble bien ordonné $\mathrm{Supp}(f)$ mais aussi dans un ensemble dont tout sous-ensemble possède un maximum $\mathrm{Supp}(g')$.

Or il est facile de vérifier qu'un ensemble totalement ordonné dont tout sous-ensemble possède un minimum et un maximum est forcément un ensemble fini. En effet, on suppose par l'absurde qu'il est infini, on prend son plus grand élément, puis son deuxième plus grand, puis son troisième, et on obtient une suite infinie strictement décroissante.

Pour tout k, la somme $\sum_{i+j=k} x_i y_j$ est une somme finie. Le produit de convolution est donc bien défini.

De plus, le support de cette série formelle est contenu dans $\mathrm{Supp}(f) + \mathrm{Supp}(g)$, donc c'est un ensemble bien ordonné. Le produit de deux séries de Hahn est donc une série de Hahn.

□

Remarque. La définition de valuation v d'une série de Hahn est compatible avec les définitions de l'addition et de la multiplication. Ainsi, $v(x+y) \geq \min(v(x),v(y))$ et $v(xy) = v(x) + v(y)$.

Proposition 2.8. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite de séries de Hahn telles que $v(u_n)$ tend vers $+\infty$ lorsque n tend vers l'infini. Alors la série $\sum_{n\in\mathbb{N}} u_n$ converge (pour la valutation v) vers une série de Hahn.*

Démonstration. Fixons un rationnel k quelconque. Il n'y a qu'un nombre fini de u_n qui possèdent des termes en $a_i t^i$ avec $i \leq k$. La somme des u_n est donc une série formelle $x = \sum_{i\in\mathbb{Q}} f(i)t^i$.

Fixons maintenant E un sous-ensemble de $\mathrm{Supp}(f)$. Si E est non vide, alors il possède au moins un élément k_0. Soit N un entier tel que pour tout $n \geq N$, $v(u_n) > k_0$. Si on appelle $U = \sum_{n=0}^{N} u_n$, qui est une série de Hahn, alors $E \cap]-\infty; k_0]$ est non vide et il est contenu dans le support de U. Par conséquent, $E \cap]-\infty; k_0]$ possède un minimum, donc E également. Il en résulte que $\mathrm{Supp}(f)$ est bien ordonné.

□

Une série de Hahn peut se décomposer en $x = at^i(1+u)$, où $a \in K$, $i \in \mathbb{Q}$ et u est une série de Hahn de valuation strictement positive. D'après la proposition 2.8, la série $a^{-1}t^{-i}(1 - u + u^2 - u^3 + \ldots)$ converge. C'est une série de Hahn, qui est l'inverse de x.

Les séries de Hahn forment donc un corps qu'on note $K((t^{\mathbb{Q}}))$.

Proposition 2.9. *Si K est un corps et t une indéterminée, alors $K(t) \subset K((t)) \subset K((t^{1/\infty})) = \bigcup_{n\in\mathbb{N}^*} K((t^{1/n})) \subset K((t^{\mathbb{Q}}))$.*

Définition. Si $x = \sum x_i t^i$ et $y = \sum y_i t^i$ sont deux séries de Hahn, le produit terme à terme de ces séries $x \odot y = \sum x_i y_i t^i$ est également une série de Hahn, appelée *produit de Hadamard* de x et de y.

2.3 Séries de Hahn et algébricité

Nous commençons par une proposition prouvée dans [Ked01]. Pour le cas général où l'on remplace $\mathbb{Q}$ par un groupe abélien totalement ordonné G, elle est prouvée dans [Kap42].

Proposition 2.10. *Si K est un corps algébriquement clos, alors le corps des séries de Hahn $K((t^{\mathbb{Q}}))$ est algébriquement clos.*

Par exemple, $\overline{\mathbb{F}_p}((t^{\mathbb{Q}}))$ est un corps algébriquement clos.

Dans toute la suite, nous considérerons les séries de Hahn de $\mathbb{F}_q((t^{\mathbb{Q}}))$, où $q = p^e$, p étant un nombre premier et $e > 0$.

Proposition 2.11. *Soit $a > 0$ et b deux entiers, et $x = \sum_{i\in\mathbb{Q}} f(i)t^i$ une série de Hahn. Considérons la série $x' = \sum_{i\in\mathbb{Q}} f(i)t^{ai+b} = \sum_{i\in\mathbb{Q}} f(-b + i/a)t^i$. Alors x' est une série de Hahn. De plus, x est algébrique sur $\mathbb{F}_q(t)$ si et seulement si x' est algébrique sur $\mathbb{F}_q(t)$.*

Démonstration. Prouvons d'abord l'assertion pour $a = 1$ et b quelconque.

Si x est annulé par le polynôme $P = \sum_{i=0}^n a_i X^i$, alors $Q = \sum_{i=0}^n a_i(X/t^b)^i = \sum_{i=0}^n (a_i t^{-bi})X^i$ annule la série $x' = \sum f(i)t^{i+b} = xt^b$.

Inversement, si $x' = xt^b$ est annulé par le polynôme $Q = \sum_{i=0}^n a_i X^i$, alors $P = \sum_{i=0}^n a_i(Xt^b)^i = \sum_{i=0}^n (a_i t^{bi})X^i$ annule la série x.

Prouvons désormais l'assertion pour $b = 0$ et pour $a > 0$ quelconque. Appelons τ l'automorphisme de $\mathbb{F}_q((t^{\mathbb{Q}}))$ donné par $\tau : x = \sum x_i t^i \mapsto x^\tau = \sum x_i t^{ai}$. Alors τ agit sur $\mathbb{F}_q(t)$, et l'image de $\mathbb{F}_q(t)$ par τ^{-1} est incluse dans $\mathbb{F}_q(t^{1/a})$, qui est de dimension finie sur $\mathbb{F}_q(t)$.

Si x est annulé par le polynôme $P = \sum_{i=0}^n a_i X^i$, alors

$$Q = \sum_{i=0}^n {a_i}^\tau X^i$$

annule la série $x' = \sum f(i)t^{ai} = x^\tau$.

Inversement, si x' est annulé par le polynôme $Q = \sum_{i=0}^n a_i X^i$, alors

$$P = \sum_{i=0}^n {a_i}^{\tau^{-1}} X^i$$

annule la série x, et x est algébrique sur $\mathbb{F}_q(t^{1/a})$, donc sur $\mathbb{F}_q(t)$.

Les deux résultats démontrent la proposition.

□

Corollaire 2.12. *On peut aussi supposer que $a > 0$ et b sont deux rationnels dans la proposition ci-dessus.*

Démonstration. La fonction $x \mapsto z = \frac{a}{a'}x + \frac{b}{b'} = \frac{ab'x+a'b}{a'b'}$ est la composée de la fonction $x \mapsto y = (ab')x + (a'b)$ avec la réciproque de la fonction $z \mapsto y = (a'b')z$.

□

Le fait d'appliquer une transformation affine sur les exposants des termes d'une série formelle s'appelle la *décimation*. On peut, grâce à la décimation, passer d'une série de Puiseux à une série entière.

3 Théorèmes principaux

Dans tout le reste du chapitre, p est un nombre premier et $q = p^e$ une puissance de p avec e non nul. Il y a exactement un corps à q éléments à isomorphisme près.

3.1 Énoncés des théorèmes

Définition. Soit $x = \sum_{i\in\mathbb{N}} x_i t^i$ une série entière dans $\mathbb{F}_q[[t]]$. Elle est dite *p-automatique* si la suite $(x_i)_{i\in\mathbb{N}}$ est p-automatique.

Définition. Soit $x = \sum_{i\in\mathbb{Q}} f(i)t^i = \sum_{i\in\mathbb{Q}} x_i t^i$ une série de Hahn dans $\mathbb{F}_q((t^{\mathbb{Q}}))$. Elle est dite *$p$-quasi-automatique* si les deux assertions suivantes sont vérifiées :

1. Il existe $a > 0$ et b deux entiers tels que $f((i-b)/a)$ a son support inclus dans S_p, c'est-à-dire qu'il est formé de rationnels positifs qui s'écrivent avec un nombre fini de chiffres après la virgule en base p.
2. Pour des entiers $a > 0$ et b qui vérifient l'assertion précédente, la fonction $f((i-b)/a)$ est p-automatique.

Si une série de Hahn p-quasi-automatique a son support inclus dans S_p (c'est-à-dire que la première assertion est vérifiée pour $a = 1$ et $b = 0$), alors on dit qu'elle est *p-automatique*.

Remarque. Par le lemme 1.7 si la deuxième assertion est vérifiée pour certains $a > 0$ et b entiers, elle l'est pour tous entiers $a > 0$ et b qui vérifient la première assertion. Noter aussi que le support d'une série de Hahn (l'ensemble des $i \in \mathbb{Q}$ tels que $x_i \neq 0$) vérifie la propriété suivante : l'ensemble des écritures en base p de ses éléments forme un langage p-rationnel.

Proposition 3.1. *Si on regarde $x \in \mathbb{F}_q(t)$ comme un élément de $\mathbb{F}_q((t^{\mathbb{Q}}))$, alors x est une série p-quasi-automatique.*

Démonstration. Regardons x comme un série de Laurent. On peut supposer, par multiplication avec certain t^b, que x est une série entière de la forme $\sum_{i\in\mathbb{N}} x_i t^i$ avec x_0 non nul. Nous allons montrer que x est p-automatique. Écrivons $x = \frac{a_0+a_1t+\ldots+a_mt^m}{b_0+b_1t+\ldots+b_nt^n}$ avec $a_0 \neq 0$ et $b_0 \neq 0$.

Pour tout $k \in \mathbb{N}$, $a_k = \sum_{i+j=k} b_i x_j = \sum_{i=0}^{k} b_i x_{k-i}$. En particulier, pour tout $k > m$, $0 = b_0x_k + \ldots + b_nx_{k-n}$. La suite $(x_k)_{k\in\mathbb{N}}$ est donc linéaire récurrente à partir d'un certain rang. Mais comme cette suite est à valeurs dans le corps fini $\mathbb{F}_q$, elle est périodique à partir d'un certain rang.

Il existe donc une série entière $y = \sum y_i t^i$, avec $(y_i)_{i\in\mathbb{N}}$ périodique de période N, telle que $x - y$ est un polynôme en t.

Soit $M = (\{0,\ldots,N-1\}, \{0,\ldots,p-1\}, \{0\}, \delta, \mathbb{F}_q, \tau)$, tel que $a \xrightarrow{b} (ap+b \mod N)$, et τ associe à un entier a la valeur commune des y_{a+kN} pour k entier quleconque. C'est un automate à sortie, à N états, qui à partir de l'écriture sans la virgule finale d'un entier i en base p, donne y_i.

La série y est donc p-automatique, et il en va de même de x, car en ajoutant ou en retirant à un langage rationnel un nombre fini de mots, on obtient un langage rationnel.

□

Proposition 3.2. *Si $x,y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ sont deux séries p-quasi-automatiques, alors leur somme $x+y$ est également une série de Hahn p-quasi-automatique. Si de plus x et y sont p-automatiques, alors $x+y$ également.*

Démonstration. Supposons que x et y sont toutes les deux p-automatiques. Les fonctions $i \mapsto x_i$ et $i \mapsto y_i$ sont p-automatiques, et par le lemme 1.6, la fonction $i \mapsto x_i + y_i$ est p-automatique, donc $x+y$ est p-automatique.

Si $x(t)$ et $y(t)$ sont p-quasi-automatiques, on peut trouver des entiers $a > 0$ et b communs tels que $x(t^a) \cdot t^b$ et $y(t^a) \cdot t^b$ sont toutes les deux p-automatiques. Donc $(x+y)(t^a) \cdot t^b$ est p-automatique, ce qui prouve que $x+y$ est p-quasi-automatique.

□

Remarque. De la même manière, on peut prouver que le produit de Hadamard de deux séries de Hahn p-quasi-automatiques est une série de Hahn p-quasi-automatique.

Il est plus difficile de prouver que le produit de deux séries p-quasi-automatiques est p-quasi-automatique. On peut voir ceci comme une conséquence du théorème de Kedlaya. Nous verrons dans le dernier chapitre une méthode pour le prouver directement par des arguments de théorie des automates.

Nous pouvons maintenant énoncer les deux théorèmes principaux ainsi que leurs corollaires.

Théorème 3.3 (Christol). *Une série entière $x \in \mathbb{F}_q[[t]]$ est p-automatique si et seulement si elle est algébrique sur le corps $\mathbb{F}_q(t)$.*

Théorème 3.4 (Kedlaya). *Une série de Hahn $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est p-quasi-automatique si et seulement si elle est algébrique sur le corps $\mathbb{F}_q(t)$.*

On peut remarquer que le théorème de Kedlaya est une généralisation du théorème de Christol.

Corollaire 3.5. *Une série de Hahn $x = \sum_{i\in\mathbb{Q}} f(i)t^i$ est algébrique sur $\mathbb{F}_q(t)$ si et seulement si pour chaque $\alpha \in \mathbb{F}_q$ non nul, la série de Hahn $\sum_{i\in f^{-1}(\{\alpha\})} t^i$ est algébrique.*

Corollaire 3.6. *Soient x,$y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ deux séries de Hahn algébriques sur $\mathbb{F}_q(t)$. Alors leur produit de Hadamard $x \odot y$ est algébrique sur $\mathbb{F}_q(t)$.*

3.2 Automatique implique algébrique

Pour démontrer le sens automatique $\Longrightarrow$ algébrique, la méthode utilisée dans la preuve du théorème de Christol peut être étendue pour le théorème de Kedlaya. Nous traiterons directement le cas du théorème de Kedlaya, ce qui montrera alors le même sens pour le théorème de Christol.

Grâce à la proposition 2.11, il suffit de prouver que toute série de Hahn $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ qui est p-automatique est algébrique sur $\mathbb{F}_q(t)$. Et comme :

$$x = \sum_{i \in \mathbb{Q}} x_i t^i = \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \alpha \left(\sum_{i \in f^{-1}(\{\alpha\})} t^i \right)$$

on peut se ramener au cas où les coefficients de la série de Hahn sont 0 ou 1. Il existe alors un sous-ensemble $S \subset S_p$ de rationnels positifs ayant un nombre fini de chiffres après la virgule en base p, tels que $x = \sum_{i \in S} t^i$.

Donnons nous maintenant un automate déterministe complet propre $M = (Q, A_p, \{i\}, F, \delta)$ à alphabet d'entrée $A_p = \{"0"; \ldots; "p-1"; ","\}$, qui reconnaît le langage des écritures en base p des éléments de S. Ce langage est inclus dans le langage Σ_p des écritures de rationnels de S_p. Par hypothèse, il est p-rationnel.

Définition. Soit $q \in Q$ un état de l'automate M. Il est appelé *pré-virgule* s'il est co-accessible et s'il peut être atteint en lisant un mot qui ne comporte pas de virgule. Il est appelé *post-virgule* s'il est co-accessible et s'il ne peut être atteint que par des mots contenant au moins une virgule.

Remarque. Les états post-virgule de M sont précisément les états atteints en lisant des mots contenant exactement une virgule. De plus, tous les états finals sont post-virgule. En effet, l'automate ne reconnaît que des mots contenant une unique virgule.

Proposition 3.7. *Si $x = \sum_{i \in S} t^i$ est une série de Hahn de $\mathbb{F}_{\mathfrak{q}}((t^{\mathbb{Q}}))$ qui est p-automatique, et si $M = (Q, A_p, \{q_0\}, F, \delta)$ est un automate fini déterministe complet propre qui reconnaît le langage des écritures en base p des éléments de S, alors x est algébrique sur $\mathbb{F}_{\mathfrak{q}}(t)$.*

Le principe de la preuve est de se ramener au cas où il n'y a qu'une transition de l'automate étiquetée par une virgule, puis de traiter l'étude de deux cas : les automates qui n'ont qu'un seul état pré-virgule, l'état initial, et les automates qui n'ont qu'un état post-virgule, l'unique état final. Les séries

associées à ces deux types d'automates on leur support inclus respectivement dans $[0;1[$ et $\mathbb{N}$.

Démonstration. Pour tout état pré-virgule $q \in Q$, soit F_q l'ensemble des entiers naturels n tels qu'en lisant leur écriture en base p sans la virgule finale, on passe de l'état initial de l'automate à l'état q.

Écrivons $f(q) = \sum_{i \in F_q} t^i$. Si q n'est pas l'état initial,

$$f(q) = \sum_{q' \xrightarrow{d} q} f(q')^p t^d$$

tandis que si q est l'état initial[1],

$$f(q) = 1 + \sum_{q' \xrightarrow{d} q} f(q')^p t^d$$

les sommes portant sur les transitions d'un état quelconque $q' \in Q$ (forcément pré-virgule) à l'état q par une lettre d (qui ne peut pas être une virgule).

Considérons le vecteur $v = (f(q))$ de coordonnées $f(q)$ pour chaque état pré-virgule q, ainsi que $v^\sigma = (f(q)^p)$. Par le lemme 2.4, les $f(q)$ sont algébriques sur $\mathbb{F}_\mathfrak{q}(t)$ pour tout état pré-virgule q.

Pour tout état post-virgule $q \in Q$, soit G_q l'ensemble des rationnels de $S_p \cup [0;1[$, tels qu'en lisant l'écriture sans la virgule initiale du rationnel x à partir de l'état q, on tombe sur un état final.

Écrivons $g(q) = \sum_{i \in G_q} t^i$. Si q n'est pas un état final,

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

tandis que si q est un état final[2],

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

Toujours par le lemme 2.4, les $g(q)$ sont algébriques sur $\mathbb{F}_\mathfrak{q}(t)$ pour tout état post-virgule q.

Finalement, on écrit que $x = \sum_{i \in S} t^i = \sum_{q \xrightarrow{,} q'} f(q)g(q')$, où la somme est portée sur tous les transitions d'un état pré-virgule q à un état post-virgule q' par une virgule. Cela montre que x est algébrique sur $\mathbb{F}_\mathfrak{q}(t)$.

□

1. Il n'y a pas de transition partant de l'état initial qui soit étiquetée par 0.
2. Il n'y a pas de transition étiquetée par 0 qui aboutit à un état final.

On en déduit qu'une série de Hahn p-quasi-automatique de $\mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q(t)$, et qu'une série entière p-automatique de $\mathbb{F}_q[[t]]$ est algébrique sur $\mathbb{F}_q(t)$.

3.3 Démonstration du théorème de Christol

Il reste maintenant à prouver les implications algébrique $\Longrightarrow$ automatique des deux théorèmes. Les preuves utilisés pour prouver le théorème de Christol, avec les séries entières, ne se généralisent pas aux séries de Hahn.

De plus, la démonstration du théorème de Kedlaya qui nous allons donner dans ce chapitre, ainsi qu'une autre démontration que nous donnerons dans le dernier chapitre, utilisent toutes les deux le théorème de Christol.

Une preuve du théorème de Christol est donnée dans [CKFR80]. Nous allons donner une preuve qui utilise les diagonales de Furstenberg, voir [Fur01].

L'idée de cette démonstration est de voir les séries entières algébriques sur $\mathbb{F}_q(t)$ comme des « traces » de fractions rationelles à plusieurs variables.

Définition. Soit $f(t_1,\ldots,t_m) = \sum c_{i_1,\ldots,i_m} {t_1}^{i_1}\cdots {t_m}^{i_m}$ une série de Laurent à m inconnues sur un corps K. On appelle *diagonale* de f la série de Laurent à une inconnue sur le corps K définie par $\Delta f(t) = \sum c_{i,\ldots,i} t^i$.

Lemme 3.8. *Une série entière de $\mathbb{F}_q[[t]]$ algébrique sur $\mathbb{F}_q(t)$ est annulée par un certain polynôme $a_0X + a_1X^p + \ldots + a_nX^{p^n}$ de $\mathbb{F}_q[t][X]$ avec a_0 non nul.*

Démonstration. Soit $f(t)$ cette série entière. Il existe des polynômes de $\mathbb{F}_q[t]$ tels que $a_l(t)f^{p^l} + \ldots + a_n(t)f^{p^n} = 0$, avec $a_l(t)$ et $a_n(t)$ non nuls.

Si $l > 0$, alors tous les monômes des f^{p^i} ont un exposant divisible par p. Le polynôme $a_0(t)$ possède un monôme d'exposant congru à $i \mod p$ avec $i < p$.

On considère alors les polynômes $a'_l,\ldots,a'_n$ obtenus en ne gardant que les monômes d'exposants congrus à $i \mod p$. En divisant le tout par t^i, on obtient une relation de la forme $a_l''(t^p)f^{p^l} + \ldots + a_n''(t^p)f^{p^n}$.

Comme l'automorphisme de Frobenius est bijectif dans $\mathbb{F}_q$, on passe la relation ci-dessus à l'inverse de l'automorphisme de Frobenius, et on trouve la relation $b_l(t)f^{p^{l-1}} + \ldots + b_n(t)f^{p^{n-1}}$.

Comme le polynôme $b_l(t)$ est non nul, on est passé d'une puissance de f en p^l à une puissance de f en p^{l-1}. Après itération, on aboutit à $l = 0$.

□

Lemme 3.9. *Une série entière de $\mathbb{F}_q[[t]]$ algébrique sur $\mathbb{F}_q(t)$ est la diagonale d'une fraction rationnelle à deux variables.*

Démonstration. On reprend les notations du lemme précédent, et on suppose que $f(t)$ est annulée par le polynôme $a_0X + \ldots + a_nX^{p^n}$ avec a_0 non nul.

Pour un entier $h > 0$, on écrit $f(t) = R(t)+t^h\varphi(t)$, avec $R(t)$ un polynôme en t et $\varphi(t)$ une série entière en t qui n'a pas de termes en t^0. Alors on a la relation suivante :

$$a_0(t)t^h\varphi(t) + \ldots + a_n(t)t^{hp^n}\varphi^{p^n}(t) = S(t)$$

où $S(t)$ est un polynôme en t. Pour h assez grand, on peut diviser la relation par une certaine puissance de t, tel que $a_0(t)$ ne s'annule plus en 0, et où $S(t)$ reste un polynôme.

On trouve donc un polynôme à deux variables $P \in \mathbb{F}_q[t,X]$ tel que $P(t,\varphi(t)) = 0$ et $\frac{\partial P}{\partial X} = a_0(0) \neq 0$. Soit $Q \in \mathbb{F}_q((t))[X]$ la série de Laurent à deux variables telle que $P(t,X) = (X - \varphi(t))Q(t,X)$.

En faisant une dérivée « logarithmique » en X, on obtient :

$$\frac{1}{P}\frac{\partial P}{\partial X}(t,X) = \frac{1}{X - \varphi(t)} + \frac{1}{Q}\frac{\partial Q}{\partial X}(t,X)$$

puis en multipliant par X^2 et en remplaçant t par tX, on obtient :

$$\frac{X^2}{P(tX,X)}\frac{\partial P(tX,X)}{\partial X}(tX,X) = \frac{X^2}{X - \varphi(tX)} + \frac{X^2}{Q(tX,X)}\frac{\partial Q}{\partial X}(tX,X)$$

Comme on a :

$$\Delta\left(\frac{X^2}{X - \varphi(tX)}\right) = \Delta\left(\frac{X}{1 - X^{-1}\varphi(tX)}\right) = \Delta\left(\sum_{n=0}^{+\infty} X^{-n+1}\varphi^n(tX)\right) = \Delta(\varphi(tX)) = \varphi$$

et :

$$\left(\frac{X^2}{Q(tX,X)}\frac{\partial Q}{\partial X}(tX,X)\right)$$

de diagonale nulle (pour chacun de ses monômes $c_{i,j}t^iX^j$, si $c_{i,j}$ est non nul alors $j > i$), cela prouve que φ est la diagonale de la fraction rationnelle à deux variables suivante :

$$\left(\frac{X^2}{P(tX,X)}\frac{\partial P}{\partial X}(tX,X)\right)$$

et par conséquent, f est aussi la diagonale d'une fraction rationnelle.

□

Lemme 3.10. *Le produit de Hadamard (terme à terme) des diagonales de deux fractions rationnelles à plusieurs variables est la diagonale d'une fraction rationnelle à plusieurs variables.*

Démonstration. Si $\sum x_i t^i = \Delta(P(X_1,\ldots,X_m))$ et $\sum y_i t^i = \Delta(Q(X_1,\ldots,X_n))$, alors la fraction rationnelle :

$$R(X_1,\ldots,X_m,X_{m+1},\ldots,X_{m+n}) = P(X_1,\ldots,X_m)Q(X_{m+1},\ldots,X_{m+n})$$

a pour diagonale $\sum x_i y_i t^i$.

□

Lemme 3.11. *Si $x = \sum_{i\in S} t^i \in \mathbb{F}_q[[t]]$, une série entière à coefficients dans $\{0;1\}$ est la diagonale d'une fraction rationnelle à plusieurs variables, alors x est p-automatique.*

Démonstration. Soient P et Q deux polynômes à m variables tels que $x = \Delta\frac{P}{Q}$. Pour tous n et h entiers naturels tels que $n < p^h$, on a la relation suivante :

$$\frac{P}{Q} = \frac{PQ^{p^h-1}}{Q^{p^h}} = \frac{PQ^{p^h-1}}{Q({X_1}^{p^h},\ldots,{X_m}^{p^h})}$$

Si on note $R_{n,h}$ le monôme obtenu à partir de PQ^{p^h-1} à qui l'on a appliqué la transformation linéaire suivante :

$$\begin{array}{rcl} {X_1}^{n+k_1p^h}\cdots{X_m}^{n+k_mp^h} & \mapsto & {X_1}^{k_1}\cdots{X_m}^{k_m} \\ \text{les autres monômes} & \mapsto & 0 \end{array}$$

alors $\Delta\frac{R_{n,h}}{Q} = \sum_{i\in u^{-1}S} t^i \in \mathbb{F}_q[[t]]$, où l'on a noté $u^{-1}S$ l'ensemble des valeurs de $u^{-1}L = \{v \in {A_p}^* | uv \in L\}$, où L est le langage des écritures des éléments de S, et u le mot de longueur h qui est l'écriture en base p de l'entier n.

Mais il n'y a qu'un nombre fini de $R_{n,h}$ possibles car leur degré est borné :

$$mn + p^h \deg(R_{n,h}) \leq \deg(P) + (p^h - 1)\deg(Q)$$

Le langage L n'a qu'un nombre fini de résiduels, et par le théorème 1.3, il est p-rationnel, donc l'ensemble S est p-automatique. La série x est donc p-automatique.

□

Lemme 3.12. *Si $x = \sum_{i\in\mathbb{N}} x_i t^i \in \mathbb{F}_q[[t]]$ est la diagonale d'une fraction rationnelle à deux variables, alors x est p-automatique.*

Démonstration. Remarquons tout d'abord que pour $\alpha \in \mathbb{F}_q$ la série $\sum_{i\in\mathbb{N}} \alpha t^i = \frac{\alpha}{1-t}$ est la diagonale d'une fraction rationnelle à une variable. Pour tout $\alpha \in \mathbb{F}_q$, considérons la série entière $y_\alpha = \sum_{i\in\mathbb{N}} \left(1-(x_i-\alpha)^{q-1}\right) t^i$. Alors $x = \sum_{\alpha\in\mathbb{F}_q} \alpha y_\alpha$. Comme les y_α sont des diagonales de fractions rationnelles à plusieurs variables, elles sont p-automatiques, donc x également.

□

Le théorème de Christol est une conséquence directe de tous ces lemmes.

3.4 Démonstration du théorème de Kedlaya

La démonstration que nous allons exposer ici est la première que Kedlaya a donné, en 2001. Elle est très théorique et utilise, en plus du théorème de Christol, un autre résultat démontré par Kedlaya. Il a donné une autre preuve en 2005, qui est plus algorithmique. Nous exposerons cette dernière dans le dernier chapitre.

On fixe p un nombre premier et $q \neq 1$ une puissance de p.

Définition. Si c est un entier positif, on note T_c le sous-ensemble de S_p formé des rationnels positifs dont l'écriture en base p n'a qu'un nombre fini de chiffres après la virgule, et qui a au plus c chiffres différents de $p-1$ après la virgule.

Le résultat suivant est montré dans l'article [Ked01, Théorème 15].

Théorème 3.13. *La série de Hahn $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ est algébrique sur $\mathbb{F}_q((t))$ si et seulement si les deux assertions suivantes sont vérifiées :*

1. *il existe des entiers $a > 0$, b et $c \geq 0$ tels que le support de $\sum x_{(i-b)/a} t^i$ est contenu dans T_c.*
2. *pour certains a, b et c qui vérifient la première assertion, il existe des entiers positifs M et N telle que toute suite $\left(x_{(u_n-b)/a}\right)_{n\in\mathbb{N}}$ avec $(u_n)_{n\in\mathbb{N}} = (b_f \dots b_0, a_0 \dots a_d (p-1) \dots (p-1) a_{d+1} \dots a_e)$ où l'on a ajouté n fois le chiffre $p-1$ à $b_f \dots b_0, a_0 \dots a_e \in T_c$, est périodique de période divisant N à partir du rang M.*

Dans ce cas, la deuxième assertion est vérifiée pour tout triplet d'entiers (a,b,c) vérifiant la première.

Remarque. Supposons vrai le théorème de Kedlaya. Si la série x est p-quasi-automatique, alors elle est algébrique sur $\mathbb{F}_q(t)$, donc sur $\mathbb{F}_q((t))$. Par conséquent, elle vérifie les deux assertions de l'énoncé ci-dessus.

La première assertion montre que si une série de Hahn est p-quasi-automatique, la décimation permet de supposer que son support est contenu non seulement dans S_p (cas des séries de Hahn p-automatiques), mais également dans l'un des T_c. La deuxième assertion est juste une conséquence du lemme de l'étoile.

Exemple. Considérons la série $x = t^0 + t^{0,1} + t^{0,11} + t^{0,111} + \ldots$. Pour $a = 1$ et $b = 0$, son support est dans S_p, mais il n'est dans aucun T_c. Cette série est quand même algébrique sur $\mathbb{F}_p((t))$, car elle vérifie les assertions de l'énoncé pour $a = p - 1$, $b = 0$ et $c = 0$. C'est une racine du polynôme $X^p - tX - 1$.

Lemme 3.14. *Soit $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ dont le support est dans $]0;1] \cap \mathbb{Q} \cap T_c$ pour un certain entier naturel c. Supposons que x soit algébrique sur $\mathbb{F}_q((t))$ avec M et N vérifiant les assertions de l'énoncé du théorème 3.13. Alors les trois assertions suivantes sont vraies :*

- *x est p-automatique ;*
- *x est algébrique sur $\mathbb{F}_q(t)$;*
- *il existe un ensemble fini déterminé par q, c, M et N contenant x.*

Démonstration. D'après le théorème 3.13, avec $a = 1$ et $b = 0$, toute suite $(x_{u_n})_{n\in\mathbb{N}}$ du type $(u_n) = (0,a_0 \ldots a_d(p-1)\ldots(p-1)a_{d+1}\ldots a_e)$ est périodique de période divisant N à partir du rang M.

Soit $\alpha \in \mathbb{F}_q$. Considérons le langage $L_\alpha \subset \Sigma_p$ des écritures de rationnels i tels que $x_i = \alpha$.

Chaque résidu $u^{-1}L_\alpha$ possède la propriété suivante : si un mot $v \in u^{-1}L_\alpha$ possède une suite consécutive de $M + r + sN$ fois le chiffre $p - 1$ (avec r et s des entiers positifs quelconques), alors le mot v' obtenu en remplaçant cette suite par une suite consécutive de $M + r + s'N$ fois le chiffre $p - 1$ (où s' est un entier positif quelconque) appartient aussi à $u^{-1}L_\alpha$.

Les résidus sont donc caractérisés par leurs éléments qui sont des mots de longueur au plus $c + M$, il y en a donc un nombre fini. D'après le théorème de Nerode, le langage L_α est rationnel.

Par conséquent, x est p-automatique. Et avec le sens direct du théorème de Kedlaya 3.7, x est algébrique sur $\mathbb{F}_q(t)$.

De plus, comme il n'y a qu'un nombre fini de résidus, x ne peut prendre qu'un nombre fini de valeurs.

□

Lemme 3.15. *Soient $x_1, \ldots, x_m$ des séries de Hahn vérifiant les hypothèses du lemme précédent. Si ces séries sont $\mathbb{F}_q((t))$-linéairement liées, alors elles sont $\mathbb{F}_q$-linéairement liées.*

Démonstration. Si on a une relation de la forme $c_1x_1 + \ldots + c_mx_m = 0$ avec $c_1, \ldots, c_m$ des séries de Laurent, on commence par ramener tous ces coefficients au même dénominateur. On peut supposer que les $c_1, \ldots, c_m$ sont des séries entières. En divisant par une puissance judicieuse de t, on peut même supposer qu'il y a au moins une série entière de terme constant non nul.

Comme les séries de Hahn $x_1, \ldots, x_m$ ont leur support dans $]0;1]$, la relation $c_1x_1 + \ldots + c_mx_m = 0$ entraine que $c_1(0)x_1 + \ldots + c_m(0)x_m = 0$. Comme les $c_i(0) \in \mathbb{F}_q$ ne sont pas tous non nuls, les séries de Hahn $x_1, \ldots, x_m$ sont linéairement liées sur $\mathbb{F}_q$.

□

Nous pouvons maintenant démontrer le sens algébrique $\Longrightarrow$ automatique du théorème de Kedlaya.

Proposition 3.16. *Soit $x = \sum_{i \in \mathbb{Q}} x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série de Hahn qui est algébrique sur $\mathbb{F}_q(t)$. Alors x est p-quasi-automatique.*

Démonstration. La série x étant algébrique sur $\mathbb{F}_q((t))$, elle vérifie les assertions du théorème 3.13 pour les entiers a, b, c. Soit $x' = \sum x_i' t^i$ avec $x_i' = x_{(i-b)/a}$, et $y = x' - x_0' t^0$. Alors y est algébrique sur $\mathbb{F}_q(t)$, et a son support dans T_c. De même, pour tout entier positif m, y^{q^m} est algébrique sur $\mathbb{F}_q(t)$ et a son support dans T_c.

Par conséquent, les séries $y, \ldots, y^{q^m}$ vérifient la deuxième assertion du théorème 3.13 pour certains entiers communs M et N. Soit V l'ensemble des éléments de $\mathbb{F}_q((t^{\mathbb{Q}}))$ qui sastisfont les hypothèses du lemme 3.14. Alors V est un ensemble fini et un $\mathbb{F}_q$-espace vectoriel, dont tous les éléments sont p-automatiques et algébriques. Soit $v_1, \ldots, v_r$ une $\mathbb{F}_q$-base de V ; par le lemme 3.15, les vecteurs $v_1, \ldots, v_r$ sont aussi linéairement indépendants sur $\mathbb{F}_q((t))$.

En séparant les coefficients de y selon les segments $]j; j+1]$, on peut écrire $y = \sum_{j=0}^{+\infty} w_j t^j$, avec chaque w_j dans V. Comme V n'a qu'un nombre fini d'éléments, y est une combinaison linéaire sur $\mathbb{F}_q((t))$ d'éléments de V. De la même façon, on trouve que les $y, \ldots, y^{q^m}$ sont des combinaisons linéaires sur $\mathbb{F}_q((t))$ d'éléments de V.

Pour $i = l, \ldots, m$, écrivons $y^{q^i} = \sum_{j=1}^{r} a_{i,j} v_j$, avec $a_{i,j} \in \mathbb{F}_q[[t]]$. Par le lemme 3.15, les $a_{i,j}$ sont déterminés de manière unique. De la même façon, pour $h = 1, \ldots, r$, on peut écrire $v_h^q = \sum_{j=1}^{r} b_{h,j} v_j$ de manière unique avec $b_{h,j} \in \mathbb{F}_q[[t]]$. Et comme les supports des v_j sont bornés, on a même $b_{h,j} \in \mathbb{F}_q[t]$

Nous allons maintenant montrer que pour $i = l, \ldots, m$ et $j = 1, \ldots, r$, les $a_{i,j}$ sont algébriques sur $\mathbb{F}_q(t)$.

Pour $i = l+1, \ldots, m$ et $j = 1, \ldots, r$, $a_{i,j} = \sum_{h=1}^{r} b_{h,j} a_{i-1,h}^q$. Cherchons maintenant une relation de ce type avec $i = l$. Par le lemme d'Ore, il existe un polynôme $P = \sum_{i=l}^{m} c_i X^{q^i}$ annulant y qui a ses coefficients dans $\mathbb{F}_q(t)$, avec c_l et c_m non nuls. On peut aussi supposer que $c_l = 1$. Comme $y^{q^l} = -c_{l+1} y^{q^{l+1}} - \ldots - c_m y^{q^m} = \left(-c_{l+1} y^{q^l} - \ldots - c_m y^{q^{m-1}}\right)^q$, on obtient :

$$\sum_{j=1}^{r} a_{l,j}v_j = \sum_{i=l}^{m-1} -c_{i+1}\left(\sum_{h=1}^{r} a_{i,h}v_h\right)^q = \sum_{i=l}^{m-1} -c_{i+1}\left(\sum_{h=1}^{r}\sum_{j=1}^{r} a_{i,h}^q b_{h,j}v_j\right)$$

En considérant les coefficients de cette équation dans la base $v_1,\ldots,v_r$, on obtient pour tout $j = 1,\ldots,r$ une équation de la forme :

$$a_{l,j} = \sum_{i=l}^{m-1}\sum_{h=1}^{r} d_{i,h,j}a_{i,h}^q$$

où tous les $d_{i,h,j} = -c_{i+1}b_{h,j}$ sont dans $\mathbb{F}_q(t)$.

En considérant v le vecteur de coordonnées les $a_{i,j}$ pour $i = l,\ldots,m$ et $j = 1,\ldots,r$, on obtient une relation de la forme $v = Bv^q$, où B est une matrice à coefficients dans $\mathbb{F}_q(t)$. Par le lemme 2.4, tous les $a_{i,j}$ sont algébriques sur $\mathbb{F}_q(t)$. Comme tous les $a_{i,j}$ sont dans $\mathbb{F}_q(t)((t))$, le théorème de Christol 3.3 s'applique, et tous les $a_{i,j}$ sont p-automatiques.

Nous allons maintenant démontrer que $y^{q^l} = \sum_{j=1}^{r} a_{l,j}v_j$ est p-automatique. Par la proposition 3.2, il suffit de prouver que si w et x sont deux séries de Hahn p-automatiques dont les supports sont contenus respectivement dans $\mathbb{N}$ et $[0;1[$, alors leur produit wx est une série de Hahn p-automatique.

En effet, on peut se restreindre au cas où les séries w et x sont à valeurs dans $\{0;1\}$. Si ces séries sont reconnues respectivement par les automates à sortie M_w et M_x, on considère M un automate à sortie[3] qui à une écriture en base p de la forme $b_f\ldots b_0,a_0\ldots a_e$, renvoie 1 si les automates M_w et M_x renvoient tous les deux 1 en lisant respectivement les mots $b_f\ldots b_0$, et $,a_0\ldots a_e$, et 0 sinon. L'automate M reconnaît alors la série wx.

Comme y^{q^l} est p-automatique, y est p-quasi-automatique. Il en va de même de x', puis de x.

□

Les propositions 3.7 et 3.16 donnent une preuve complète du théorème de Kedlaya 3.4. Nous donnerons dans le dernier chapitre une preuve plus constructive de la proposition 3.16.

3. Pour créer M, on peut « brancher » l'automate M_w qui n'a que des états pré-virgule avec l'automate M_x qui n'a que des états post-virgule.

4 Polynômes tordus et polynômes additifs

Ce chapitre va permettre de voir un polynôme annulateur d'une certaine série x comme un opérateur qui annule x. Toutes les propositions de cette sections sont assez classiques. Elles sont traitées par exemple dans [Gos96].

4.1 Propriétés de base

Définition. Soit K/F une extension de corps, et σ un F-endomorphisme de K. On définit l'ensemble $K\{\tau\}$ l'ensemble des polynômes munis de la somme usuelle et du produit défini comme ceci :

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

Les règles de commutation sont les suivantes : les éléments de K commutent entre eux, les puissances pures de τ commutent entre elles, et si $x \in K$, $\tau \cdot x = \sigma(x) \cdot \tau$.

Proposition 4.1. *L'ensemble $K\{\tau\}$ muni de la somme et du produit forme un anneau intègre non-commutatif, qu'on appelle l'ensemble des* polynômes tordus. *De plus, si $P,Q \in K\{\tau\}$ sont de dimensions respectives m et n, alors leur somme est de degré inférieur ou égal à $\min(m,n)$ et leur produit est de degré $m+n$.*

Si on prend K un corps de caractéristique $p > 0$, K est un $\mathbb{F}_p$-espace vectoriel et possède le $\mathbb{F}_p$-endomorphisme $\sigma : x \mapsto x^p$ de K, l'endomorphisme de Frobenius.

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

Tout polynôme tordu peut être vu comme un polynôme additif et inversement. Comme toute série de Hahn $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ algébrique sur $\mathbb{F}_q(t)$ est annulé par un polynôme additif, il est aussi annulé par un polynôme tordu. Il existe un polynôme tordu P tel que $P(\sigma)(x) = 0$.

Le reste du chapitre va nous permettre de voir comment « scinder » les polynômes tordus comme on scinde les polynômes usuels.

Proposition 4.2. *Soit K un corps de caractéristique p, et $\overline{K}$ sa clôture algébrique. Soit P un polynôme de $K[X]$. Alors les assertions suivantes sont équivalentes :*

- *P est additif ;*
- *$P(X+Y) = P(X) + P(Y)$ dans $K[X,Y]$;*
- *$P(x+y) = P(x) + P(y)$ pour tous $x,y \in \overline{K}$;*

– *l'ensemble des racines de P forme un $\mathbb{F}_p$-espace vectoriel de $\overline{K}$, et ses racines ont la même multiplicité p^e une puissance de p.*

Proposition 4.3. *Si P et Q sont des polynômes tordus avec Q non nul, alors il existe une unique paire de polynômes tordus A et B avec $\deg(B) < \deg(Q)$, tels que $P = AQ + B$.*

Proposition 4.4. *Soit $P(\tau)$ et $Q(\tau)$ deux polynômes tordus. Notons $P(z)$ et $Q(z)$ leurs polynômes additifs associés.*

Si le coefficient constant de $Q(\tau)$ n'est pas égal à 0, alors $P(\tau)$ est un multiple à gauche de $Q(\tau)$ — il existe $A \in K\{\tau\}$ tel que $P = AQ$ — si et seulement si $P(z)$ est un multiple de $Q(z)$.

4.2 Polygones de Newton et séparation par pente

Soit le problème suivant : on connaît les coefficients d'un polynôme dans un corps valué. On aimerait avoir des précisions sur les valuations de ses racines (éventuellement dans un corps de décomposition de ce polynôme).

Ici, le corps valué sera $\mathbb{F}_q((t^{\mathbb{Q}}))$.

Définition. Si $P(z) = \sum c_i z^i$ est un polynôme non nul à coefficients dans $\mathbb{F}_q((t^{\mathbb{Q}}))$, on définit le *polygone de Newton* de P la frontière basse de l'enveloppe convexe de l'ensemble des points $(-i, v(c_i))$. Les pentes de ce polygone sont appelés les *pentes* de P. Pour $r \in \mathbb{Q}$, on appelle *multiplicité* de la pente r de P la largeur (différence des abscisses des extrémités) du segment de pente r du polygone de Newton de P. On dit que P est *pur de pente r* si toutes les pentes sont égales à r. Par convention, $+\infty$ peut aussi être une pente : sa multiplicité en tant que pente du polynôme $P(z) = \sum_{i=0}^{m} c_i z^i$ est le plus petit entier l tel que $c_l \neq 0$.

Remarque. Si on multiplie un polynôme P par une constante a de valuation r, le polygone de Newton de aP est le polygone de Newton de P qu'on a translaté de r unités vers le haut. Ses pentes avec multiplicités sont les mêmes. Et si on considère le polynôme $P(aX)$, on obtient un polygone de Newton dont toutes les pentes sont augmentées de r.

Proposition 4.5. *Soient P et Q deux polynômes non nuls. Le polynôme PQ a pour pentes l'union des pentes de P et de Q. La multiplicité d'une pente r est égale à la somme des multiplicités des pentes r dans P et dans Q.*

Démonstration. Pour $r = +\infty$, c'est évident. Pour r quelconque, on commence par se ramener au cas où $u = 0$, et où les valuations de P et de Q sont nulles, c'est-à-dire qu'ils sont dans l'anneau des entiers et qu'ils possède au moins une composante de valuation 0.

Il suffit de considérer les projetés de P et de Q dans le corps résiduel, puis de considérer :

$$\overline{PQ} = \left(\sum_{i=m}^{m'} a_i X^i\right)\left(\sum_{j=n}^{n'} b_i X^i\right) = \sum_{k=m+n}^{m'+n'}\left(\sum_{i+j=k} a_i b_j\right) X^k$$

Comme $c_{m+n} = a_m b_n$ et $c_{m'+n'} = a_{m'} b_{n'}$ sont non nuls, cela veut dire que PQ a une pente 0 de multiplicité $(m'+n') - (m+n) = (m'-m) + (n'-n)$, la somme des multiplicités des pentes de 0 des polynômes P et Q.

□

Ainsi, dans un corps valué algébriquement clos, si un polynôme a une pente r de multiplicité m, alors il a exactement m racines (comptées avec leur multiplicités) de valuation égale à r.

Proposition 4.6. *Soit K un corps valué, complet pour cette valuation. Si P est un polynôme non nul de $K[X]$ alors on peut le décomposer en un produit de polynômes $P = P_1 \dots P_n$, où les P_i sont purs pour une certaine pente.*

Nous pouvons maintenant parler de la décomposition des polynômes tordus.

Définition. On définit les pentes des polynômes tordus comme les pentes des polynômes additifs associés. Un polynôme tordu $P(\tau)$ est dit *pur de pente* r si le polynôme $P(z)/z$ n'a qu'une seule pente r.

Théorème 4.7. *Soit K un sous-corps de $\mathbb{F}_q((t^{\mathbb{Q}}))$ contenant tous les t^r pour $r \in \mathbb{Q}$ et complet pour la valuation v. Soit $P(\tau)$ un polynôme tordu non nul de $K\{\tau\}$. Alors P se factorise en un produit de polynômes tordus $P = Q_1 \cdots Q_n$ où chaque Q_i est pur pour une certaine pente.*

De plus, il existe q' une puissance de q tel que $P(\tau)$ se décompose en produit de polynômes tordus de degré 1 sur le corps $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$.

5 Approche pratique et algorithmique

Ce chapitre est consacré à l'approche concrète et algorithmique des théorèmes énoncés jusqu'ici.

5.1 Automates et séries de Hahn

Le sens automatique $\Longrightarrow$ algébrique du théorème affirme qu'une série de Hahn p-quasi-automatique est algébrique. Avant de chercher un polynôme à partir d'un automate sur l'alphabet A_p, il faut vérifier si cet automate correspond bien à une série de Hahn.

On commence par voir si cet automate ne reconnaît que des mots de Σ_p, c'est-à-dire qu'il ne reconnaît que des écritures d'éléments de $S_p = \mathbb{Q}^+ \cap \mathbb{Z}[1/p]$. C'est un problème simple d'automates finis.

Proposition 5.1. *On se donne l'automate fini déteministe $M = (Q,A,\{i\},F,\delta)$. On considère $Q_1 \subset Q$ l'ensemble des états accessibles uniquement avec des chiffres et $Q_2 \subset Q$ l'ensemble des états co-accessibles par des chiffres.*

Alors le langage reconnu par M est dans Σ_p si et seulement si toutes les assertions suivantes sont vérifiées :

- *il n'y a pas de transition étiquetée par 0 qui parte de l'état initial ou qui arrive à un état final ;*
- *l'état initial est dans Q_1, et les états finals sont tous dans Q_2 ;*
- *les ensembles Q_1 et Q_2 sont disjoints ;*
- *toute transition étiquetée par une virgule est une transition d'un état de Q_1 à un état de Q_2.*

Démonstration. Il suffit de traduire le fait que Σ_p est le langage des mots contenant une unique virgule, et qui ne commencent ni ne terminent par 0.

Notons qu'on peut calculer Q_1 et Q_2 par un nombre fini d'étapes, car s'il existe un mot qui fait passer d'un état q à un état q', il en existe un de longueur au plus $|Q|$. C'est une conséquence du lemme de l'étoile.

□

Supposons maintenant que nous avons un automate, qui reconnaît un langage inclus dans Σ_p. On cherche à savoir si cet automate est associé à une série de Hahn.

Comme dans la preuve du sens direct du théorème de Kedlaya (proposition 3.7), on peut supposer qu'il n'y a qu'une transition étiquetée par une virgule, et qu'il n'y a qu'un seul état pré-virgule[4]. On peut aussi supposer que l'automate est déterministe, complet et propre.

Alors l'automate est associé à une série de Hahn si et seulement si toute transition n'appartient qu'à au plus un cycle, et si pour tout couple de transitions $q \xrightarrow{s} q'$ qui est sur un cycle et $q \xrightarrow{t} q''$ qui n'est pas sur un cycle, $s > t$.

Exemple. Soit l'automate de sortie suivant, où la fonction de sortie vaut 1 s'il y a une flèche sortante et 0 sinon. Il correspond à l'expression $t^{0,c} + t^{0,abc} + t^{0,ababc} + \ldots$. Si $a > c$, alors les exposants forment une suite strictement croissante, et l'expression est une série de Hahn. Si $a < c$, alors les exposants forment une suite strictement décroissante, et l'expression n'est pas une série de Hahn.

4. Les automates qui ont un unique état post-virgule calculent des séries entières à support dans $\mathbb{N}$, qui est bien ordonné.

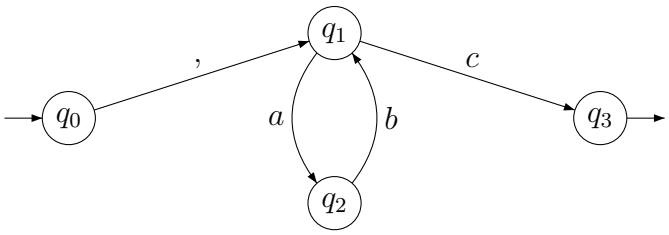

FIG. 3 – *Exemple d'automate à sortie*

5.2 Multiplication des séries p-quasi-automatiques

La proposition 3.2 dit que la somme de deux séries p-quasi-automatiques est p-quasi-automatique. Nous allons voir de manière « automatique » pourquoi c'est encore vrai avec le produit.

Lemme 5.2. *Soit $n \in \mathbb{N}^*$ un entier naturel non nul. Soit $M = (Q,A,I,F,\delta)$ un automate fini non-déterministe, et $f : A^* \to \mathbb{Z}/n\mathbb{Z}$ la fonction qui à un mot $w \in A^*$ 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. Nous construisons un automate fini déterministe complet à sortie $M' = (Q',A', \{i'\},\delta',\Delta',\tau')$.

Soit Q' l'ensemble des fonctions de Q dans $\mathbb{Z}/n\mathbb{Z}$, et $A' = A$. On définit $i' : Q \to \mathbb{Z}/n\mathbb{Z}$ la fonction qui associe 1 aux état initiaux et 0 aux autres états. On définit la fontion de transition de M' comme suit. Si $g : Q \to \mathbb{Z}/n\mathbb{Z}$ et si $s \in A$, alors $\delta'(g,s) : Q \to \mathbb{Z}/n\mathbb{Z}$ est la fonction donnée par :

$$\delta'(g,s)(q) = \sum_{q' \xrightarrow{s} q} g(q')$$

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

La fonction f est alors associée à l'automate M'.

□

Proposition 5.3. *Soient $x,y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ des séries de Hahn p-automatiques (respectivement p-quasi-automatiques). Alors leur produit xy est p-automatique (repectivement p-quasi-automatique).*

Par décimation, il suffit de prouver le cas p-automatique. Comme pour la preuve de la proposition 3.2, nous utiliserons les écritures retournées en base p.

Écrivons x et y comme combinaison $\mathbb{F}_q$-linéaire de séries de Hahn à coefficients dans $\{0;1\}$. Si le produit de deux séries de cette forme est toujours p-automatique, alors xy est p-automatique.

On peut donc supposer sans perte de généralité que $x = \sum_{i \in S_x} t^i$ et $y = \sum_{i \in S_y} t^i$. Considérons L le sous-ensemble de $A_p^* \times A_p^*$ constitué des couples (w_x,w_y) ayant les propriétés suivantes.

1. Les mots w_x et w_y ont la même longueur.
2. Les mots w_x et w_y terminent tous les deux par 0.
3. Les mots w_x et w_y ont tous les deux une unique virgule, située à la même position.
4. Après avoir retiré les zéros à gauche et à droite, w_x et w_y deviennent des écritures retournées en base p de rationnels $i,j \in S_p$.
5. Le couple (i,j) appartient à $S_x \times S_y$.

Par la première propriété, on peut voir L comme un langage sur $A_p \times A_p$. C'est clairement un langage rationnel. Soit $M = (Q,A,\{q_0\},F,\delta)$ un automate déterministe complet et propre qui reconnaît le langage L, avec $A = A_p \times A_p$.

Définissons un automate fini non-déterministe $M' = (Q',A',I',F',\delta')$ de la façon suivante. Posons[5] $Q' = Q \times \{0;1\}$ et $A' = A_p$. Posons également $I' = \{(q_0,0)\}$ et $F' = F \times \{0\}$.

On définit les transitions de M' de la manière suivante. Considérons les transitions $q \overset{(t,u)}{\to} q'$ dans l'automate M. Si $i \in \{0;1\}$, alors soit $t+u+i < p$ et on inclut $(q,i) \overset{t+u+i}{\to} (q',0)$ dans δ', soit $t+u+i \geq p$ et on inclut $(q,i) \overset{t+u+i-p}{\to} (q',1)$ dans δ'.

Considérons les transitions $q \overset{(,)\times(,)}{\to} q'$ dans l'automate M. Pour $i \in \{0;1\}$ on inclut les transitions $(q,i) \overset{.}{\to} (q',i)$ dans δ'. On n'inclut aucune autre transition.

Le nombre de chemins qui acceptent w avec l'automate M' est égal aux nombres de couples $(w_x,w_y) \in L$ dont la somme (par addition usuelle en base p avec retenues) vaut w. Par le lemme précédent, ce nombre de chemins modulo p est une fonction automatique.

Par conséquent, la fonction qui, étant donnée l'écriture renversée en base p d'un rationnel $k \in S_p$, calcule la réduction modulo p du nombre de façons d'écrire $k = i + j$ avec $i \in S_x$ et $j \in S_y$ est une fonction p-automatique. Donc xy est p-automatique.

5. On adjoint à l'automate la possibilité de « garder en mémoire » la retenue.

5.3 Résolution d'équations polynômiales

Pour démontrer constructivement le sens algébrique $\Longrightarrow$ automatique du théorème de Kedlaya, nous devons montrer pourquoi l'ensemble des séries p-quasi-automatiques est stable par extraction de racines.

Lemme 5.4. *Pour toute série de Hahn p-quasi-automatique $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ à support dans $]-\infty;0[$, il existe une série de Hahn $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ telle que $y^p - y = x$.*

Démonstration. On peut prendre $y = x^{1/p} + x^{1/p^2} + \ldots$, si l'on prouve que cette formule définit une série de Hahn qui est p-quasi-automatique. Par décimation, on peut supposer que x est p-automatique.

Écrivons $y = \sum y_i t^i$. Fixons $i < 0$, il existe un entier N tel que pour tout $n \geq N$, $i < v(x)/p^n$. Les coefficients de y inférieurs à $v(x)/p^n$ coincident avec les coefficients de $x^{1/p} + \ldots + x^{1/p^n}$. Par conséquent, $\mathrm{Supp}(y) \cap]-\infty; i]$ est bien ordonné. Cela montre que $\mathrm{Supp}(y)$ est bien ordonné, et donc que y est une série de Hahn.

Comme $y_i = x_{ip} + x_{ip^2} + \ldots$, pour tout j fixé, la série $\sum_{i<-p^{-j}} y_i t^i$ est p-automatique. De même, pour $i \in [-1;0[$, la suite x_i,$x_{i/p}$,x_{i/p^2},... est engendrée en faisant lire les écritures en base p de $1+i$,$1+i/p$,$1+i/p^2$,... par un automate fini. Il existe donc des entiers m et n tels que pour tout $i \in [-1;0[$, $y_{ip^{-m}} = y_{ip^{-n}}$.

À partir d'ici, nous pouvons construire un automate à sortie qui en lisant l'écriture en base p de $1+i$, retourne y_i. En effet, on part de l'automate qui reconnaît $\sum_{i<-p^{-n}} y_i t^i$; si $i \geq -p^{-n}$, alors $1 + i \geq 1 - p^{-n}$, et l'écriture en base p commence par n fois le chiffre $p-1$. Nous pouvons donc revenir à l'état où se trouvait l'automate après m fois le chiffre $p-1$. Comme $y_{ip^{-m}} = y_{ip^{-n}}$, on finit par calculer le bon coefficient.

Par conséquent, y est p-quasi-automatique.

□

Lemme 5.5. *Soit $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ le complété pour la valuation v de l'anneau des séries p-quasi-automatiques. Alors pour tout a,$b \in R_q$ avec $a \neq 0$, il existe q' une puissance de q telle que l'équation $z^p - az = b$ possède p racines dans $R_{q'}$.*

Démonstration. Commençons par montrer que pour $b = 0$, l'équation $z^{p-1} = a$ possède $p-1$ solutions disctintes dans un certain $R_{q'}$. Écrivons $a = a_0 t^i(1+u)$, où $a_0 \in \mathbb{F}_q$, $i \in \mathbb{Q}$ et $v(u) > 0$. Choisissons q' de sorte que a_0 ait toutes ses racines $p-1$-ièmes dans $\mathbb{F}_{q'}$. Alors pour toute racine $p-1$-ième μ de a_0, la série :

$$z = \mu t^{i/(p-1)} \sum_{j=0}^{+\infty} \begin{pmatrix} j \\ 1/(p-1) \end{pmatrix} u^j$$

convient.

Supposons maintenant b quelconque. Par l'argument précédent, on peut se ramener au cas $a = 1$. On peut alors séparer $b = b_- + b_+$, où b_- a son support inclus dans $]-\infty; 0[$ et b_+ a son support inclus dans $[0; +\infty[$, et traiter les cas $b = b_-$ et $b = b_+$ séparément. Le premier cas est précisément le lemme précédent. Pour le deuxième cas, on considère b_0 le coefficient constant de b_+, et on choisit q' tel que l'équation $z^p - z = b_0$ a p racines distinctes $c_1, \ldots, c_p \in \mathbb{F}_{q'}$. Alors les séries :

$$z = c_i - \sum_{j=0}^{+\infty} b^{p^j}$$

conviennent.

□

Lemme 5.6. *Soit $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ le complété pour la valutation v de l'anneau des séries p-quasi-automatiques, et $R = \bigcup_{e \in \mathbb{N}^*} R_{q^e}$ l'union des anneaux R_{q^e} pour les puissances de q. Alors tout polynôme non nul à coefficients dans R se scinde dans R.*

Démonstration. Par le lemme d'Ore, il suffit de prouver que pour tout polynôme tordu $P(\tau) \in R_q\{\tau\}$, le polynôme additif $P(z)$ est scindé sur $R_{q'}$ pour un certain q'.

Comme R_q est stable par racine p-ième, on peut se débarasser des facteurs τ à droite, et se ramener au cas où $P(\tau)$ a un coefficient constant non nul, ou de façon équivalente, au cas où $P(z)$ n'a pas de racine multiple.

Par le théorème 4.7, on peut décomposer $P(\tau) = Q_1 \cdots Q_n$ en produit de polynômes tordus $Q_i = \tau - c_i$ de degré 1, sur un certain $R_{q'}$. La recherche des solutions de $P(z)$ peut être décrite comme la recherche des solutions du système d'équations :

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

où les racines de $P(z)$ sont précisément les valeurs possibles de z_n. En appliquant plusieurs fois le lemme précédent, on trouve que le système a p^n solutions distinctes, et donc que $P(z)$ est scindé sur un certain $R_{q'}$.

□

Proposition 5.7. *Soit $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ une série de Hahn algébrique sur $\mathbb{F}_q(t)$. Alors x est p-quasi-automatique.*

Démonstration. Il existe un polynôme $P(z)$ sur $\mathbb{F}_q(t^{1/p^m})$ pour un certain entier m, tel que x est une racine de P de multiplicité 1. En remplaçant x par x^{p^m}, on peut se ramener au cas où $m = 1$. Prenons[6] $c \in \mathbb{Q}$ tel que $c > v(x - x')$ pour toute racine $x' \neq x$ de P.

Par le lemme précédent, il existe q' une puissance de q et une série p-quasi-automatique $y \in \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ telle que $v(x - y) \geq c$. Le polynôme $P(z + y)$ a alors exactement une pente supérieure ou égale à c, c'est même $v(x - y)$.

Par la proposition 3.7, y est algébrique sur $\mathbb{F}_q(t)$. Appelons K l'extension finie de $\mathbb{F}_{q'}((t))$ obtenue en y adjoignant y. Alors K est complet pour la valuation v, et par la proposition 4.6, on peut diviser $P(z+y)$ par son unique facteur de pente au moins c. Donc $x - y \in K$, et par conséquent $x \in K$.

Soit m le degré du polynôme minimal de y sur $\mathbb{F}_q(t)$. Pour $j = 0, \ldots, m-1$, écrivons $(y^j)^p = \sum_{i=0}^{m-1} a_{i,j} y^i$, avec $a_{i,j} \in \mathbb{F}_q((t))$. Alors les $a_{i,j}$ sont algébriques sur $\mathbb{F}_q(t)$. Soit n le plus petit entier tel que les $x, \ldots, x^{p^n}$ soient linéairement liés sur $\mathbb{F}_q((t))$. Écrivons $x^{p^j} = \sum_{i=0}^{m-1} b_{i,j} y^i$ avec $b_{i,j} \in \mathbb{F}_q((t))$.

On obtient alors les équations :

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

pour $j = 0, \ldots, n-1$.

Écrivons $c_0 x + \ldots + c_n x^{p^n} = 0$, où les $c_i \in \mathbb{F}_q((t))$ et $c_0 = 1$. Alors les c_i sont algébriques sur $\mathbb{F}_q(t)$. Si on écrit $x = -c_1 x^p - \ldots - c_n (x^{p^{n-1}})^p$, on obtient les équations :

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

et donc :

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

6. En utilisant par exemple le polygone de Newton de $P(z + x)$.

On obtient alors un système d'équations en les $b_{i,j}$ pour $i = 0, \ldots, m-1$ et $j = 0, \ldots, n$ comme dans le lemme 2.4. Par conséquent tous les $b_{i,j}$ sont algébriques sur $\mathbb{F}_q(t)$. D'après le théorème de Christol 3.3, tous les $b_{i,j} \in \mathbb{F}_q[[t]]$ sont p-automatiques, et donc $x = \sum_{i=0}^{m-1} b_{i,0} y^i$ est p-quasi-automatique.

□

Conclusion

Le principal intérêt du théorème de Kedlaya est de pouvoir décrire explicitement les racines des polynômes de $\mathbb{F}_q(t)[X]$. C'est pour cela que la preuve constructive du théorème est fondamentale.

Rappelons la méthode pour décrire, à partir d'un polynôme $P \in \mathbb{F}_q(t)[X]$, les séries de Hahn qui annulent ce polynôme.

- On commence, en considérant les X, X^p, X^{p^2}... par trouver un polynôme additif Q qui est multiple de P, et le polynôme tordu $R(\tau)$ correspondant à Q.
- On décompose alors sur le complété de l'un des corps $\mathbb{F}_{q'}(t)$ le polynôme tordu $R(\tau)$ en produit de polynômes tordus de degré 1, de la forme $\tau - a$.
- Il suffit alors de résoudre des équations du type $z^p - az = b$, dans l'un des complétés des corps $\mathbb{F}_{q'}((t^{\mathbb{Q}}))$.
- On peut calculer les racines avec une certaine précision. Si x est une racine dont on connaît une bonne approximation y et un automate qui calcule y, alors on peut exprimer x comme un polynôme en y.
- On trouve alors un automate qui calcule x.
- Après avoir trouvé toutes les racines x de Q, on calcule tous les $P(x)$ pour connaître les racines de P.

Cette méthode pour décomposer les polynômes de $\mathbb{F}_q(t)[X]$ a été la première proposée par Kedlaya. En théorie, toutes les étapes peuvent être effectuées algorithmiquement. Mais à chaque étape, le nombre de données à traiter augmente, parfois exponentiellement. Par exemple, à partir d'un polynôme de degré n, on trouve un polynôme additif de degré p^n.

Pour décomposer rapidement des polynômes de $\mathbb{F}_q(t)[X]$, on peut par exemple améliorer la méthode précédente. Si on fait les calculs en retirant les termes à grands exposants, ou en ne considérant qu'un certain nombre d'états pour les automates, il est possible qu'on puisse trouver rapidement des approximations des racines. Après plusieurs essais, on tombe éventuellement sur la valeur exacte.

On peut aussi chercher des méthodes complètement différentes, comme essayer de résoudre « automatiquement » des équations plus complexes que les simples équations du type $z^p - az = b$.

Références

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

[Bou81] N. Bourbaki. *Algèbre chapitres 4 à 7*. Éléments de mathématiques. Dunod, 1981.

[CKFR80] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, 108:401–419, 1980.

[Fur01] Harry Furstenberg. Algebraic functions over finite fields. *Journal of Algebra*, 7:271–277, 2001.

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1996.

[Kap42] Irving Kaplansky. Maximal fields with valuations. *Duke Mathematical Journal*, 9:303–321, 1942.

[Ked01] Kiran S. Kedlaya. Power series and p-adic algebraic closures. *Journal of Number Theory*, 89:324–339, 2001.

[Pas77] Donald S. Passman. *The Algebraic Structure of Group Rings*. Wiley, 1977.

[Sak03] Jacques Sakarovitch. *Éléments de théorie des automates*. Vuibert, 2003.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer-Verlag, 1979.