Séminaire Delange-Pisot-Poitou.
Théorie des nombres

KHYRA GÉRARDIN

Séries rationnelles

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 2 (1974-1975), exp. n° G1, p. G1-G6

<http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
16e année, 1974/75, n° G1, 6 p.

28 octobre 1974

SÉRIES RATIONNELLES

par Khyra GÉRARDIN

1. Rappels sur les algèbres d'un monoïde libre.

Soient $X = (x_1 \dots x_p)$ un ensemble fini appelé alphabet dont les éléments s'appellent des lettres, X^* le monoïde libre qu'il engendre. Les éléments de X^* s'appellent des mots ; on notera e le mot vide de X^*. Le produit dans X^* est la concaténation. Si $f , g \in X^*$, $f * g$ revient à écrire g à droite de f. On notera $|f|$ la longueur du mot f, c'est-à-dire le nombre d'occurences de lettres de X dans f. On munit X^* d'une relation d'ordre de la manière suivante : $f \leqslant g$ si $|f| \leqslant |g|$ et si $|f| = |g|$ alors f précède g lexicographiquement, étant entendu que $x_1 < x_{i-1} < x_i < \dots < x_p$.

Dans le cas où $p = 1$, le monoïde libre commutatif est isomorphe à $\underset{\sim}{N}$ additif. Il est connu que dans ce cas X^* est cyclique.

Soient A un anneau commutatif unitaire, K son anneau de quotients. On notera $A\langle\langle X\rangle\rangle$ l'algèbre large du monoïde libre X^*. Les éléments de $A\langle\langle X\rangle\rangle$ s'écrivent :

$$a = \sum_{f\in X^*}(a , f)f \quad \text{où} \quad (a , f) \in A , \quad \forall f \in X^* .$$

On définit la somme et le produit dans $A\langle\langle X\rangle\rangle$ de la manière suivante : Si

$$a = \sum_{f\in X^*}(a , f)f \qquad b = \sum_{f\in X^*}(b , f)f ,$$

alors,

$$a + b = \sum[(a , f) + (b , f)]f .$$

Le produit de Cauchy est défini de la manière suivante :

$$a \times b = \sum_{f\in X^*} [\sum_{gh=f}(a , g) \times (b , h)]f .$$

Cette dernière expression a un sens car, X^* étant un monoïde libre, chaque mot f n'a qu'un nombre fini de factorisations en produit de deux mots qui le précèdent.

La série 0 est celle dont tous les coefficients sont nuls. La série 1 est celle dont le seul coefficient non nul est le coefficient de l'élément neutre qui est égal à 1. Il est immédiat que $A\langle\langle X\rangle\rangle$ est une algèbre non commutative si $|X|>2$. La sous-algèbre des polynômes se note $A\langle X\rangle$.

$$a \in A\langle X\rangle \Longleftrightarrow a = \sum(a , f)f ;$$

il n'existe qu'un nombre fini de coefficients (a , f) non nuls.

Si $(a , e) = 0$, on dit que la série a est quasi inversible. Sa quasi-inverse a^* est définie de la manière suivante :

$$a^* = a + a^* a = a + aa^* .$$

Si a est quasi inversible, on vérifie facilement que $1 + a$ est inversible dans l'anneau $A\langle\langle X\rangle\rangle$. Si $a = \sum(a , f)f$, on notera Support de a, ou Supp a,

$$\text{Supp } a = \{f/(a , f) \neq 0\} .$$

Dans $A\langle\langle X\rangle\rangle$, on définit aussi le produit d'Hadamard. Si

$$a = \sum(a , f)f \qquad b = \sum(b , f)f ,$$

alors,

$$a \odot b = \sum[(a , f) \times (b , f)]f .$$

Il est facile de vérifier que, munie du produit Hadamard, l'algèbre $A\langle\langle X\rangle\rangle$ est une algèbre commutative, non intègre, dont l'élément neutre est la série

$$\sum_{f\in X^*} f .$$

2. Propriétés topologiques de $A\langle\langle X\rangle\rangle$ et $A\langle X\rangle$.

Si $a , b \in A\langle\langle X\rangle\rangle$, on définit une distance de la manière suivante :

$$d(a,b) = \begin{cases} 0 & \text{si } a = b . \\ e^{-i} & \text{où } i \text{ est l'indice du 1er coefficient non nul de } a-b . \end{cases}$$

Munie de cette distance, l'algèbre $A\langle\langle X\rangle\rangle$ est un espace ultramétrique.

Si a est une série formelle, on notera l'ordre de la série l'indice du 1er coefficient non nul de a.

Pour tout $n \geq 0$, soit $\mathfrak{a}_n$ l'ensemble des séries formelles d'ordre $\geq n$. Si $a \in \mathfrak{a}_n$ et $b \in A\langle\langle X\rangle\rangle$, il est immédiat que ab et ba appartiennent à $\mathfrak{a}_n$. $\mathfrak{a}_n$ est un idéal bilatère de $A\langle\langle X\rangle\rangle$. Si $m \geq n$, on a : $\mathfrak{a}_m \subseteq \mathfrak{a}_n$. Les idéaux $\mathfrak{a}_n$ forment une base de voisinages de 0. L'anneau $A\langle\langle X\rangle\rangle$, muni de cette topologie, est complet. L'anneau des polynômes $A\langle X\rangle$ est partout dense dans $A\langle\langle X\rangle\rangle$ qui est son complété.

3. Définition d'un ensemble rationnellement clos.

Soit B un sous-ensemble de $A\langle\langle X\rangle\rangle$. B est dit rationnellement clos si, $\forall\, a\in B$, a quasi inversible, alors $a^* \in B$. a^* étant bien entendu la quasi-inverse de a.

4. Séries rationnelles $S(1)$.

On notera $A^{RAT}\langle\langle X\rangle\rangle$ la plus petite algèbre de $A\langle\langle X\rangle\rangle$ qui contienne X, et qui est rationnellement close.

Caractérisation des séries rationnelles $S(1)$.

PROPOSITION. - $a \in R^{AT}\langle\langle X\rangle\rangle$ si, et seulement si, il existe un entier $N \geq 1$, une représentation μ de X^* dans $M_N(A)$, une matrice P de $M_N(A)$, telle que l'on ait

$$a = \sum_f (a\ ,\ f) f = \sum_f (\mathrm{Tr}\ P\ \mu f) f\ .$$

Cas particuliers. - $X = 1 \Longrightarrow X^* = \underset{\sim}{N}$. $A = \underset{\sim}{Z}$. On a alors la définition habituelle des séries rationnelles. Rappelons la caractérisation usuelle des séries rationnelles,et montrons que les deux proposition coïncident : si $a = \sum_{n\geq 0} a_n X^n$, a est une série rationnelle si, et seulement si, il existe deux entiers h , $n_0 \geq 1$, h entiers $\lambda_1 \dots \lambda_h$, tels que pour tout $n \geq n_0$ on ait :

$$a_{n+h} = \lambda_1\ a_{n+h-1} + \dots + \lambda_i\ a_{n+h-i} + \dots + \lambda_h\ a_n\ .$$

Démonstration de l'équivalence des deux définitions. - Si

$$a = \sum_{n\geq 0} a_n\ X^n = \sum_{n\geq 0} (\mathrm{Tr}\ P\ M^n) X^n\ ,$$

où P et M sont des matrices de $M_N(\underset{\sim}{Z})$ pour un certain $N \geq 1$, la matrice M vérifie son polynôme caractéristique. Donc la suite $(\mathrm{Tr}\ P\ M^n)_{n\geq 0}$ vérifie une relation de récurrence.

Réciproque. - Si

$$a = \sum_{n\geq 0} a_n\ X^n = \frac{R(X)}{1 - S(X)} \qquad R\ ,\ S \in \underset{\sim}{Z}[X]\ ,$$

on examine le cas où P est un polynôme :

$$a = a_0 + a_1\ X + \dots + a_p\ X^p\ .$$

Soit M la matrice nilpotente de $M_{p+1}(\underset{\sim}{Z})$ définie de la manière suivante. Si $e_1 \dots e_{p+1}$ est une base de l'espace $\underset{\sim}{Q}^{p+1}$, on a :

$$\begin{aligned} &Me_1 = 0 \\ &M_{e_i}^{i} = e_{i-1} \qquad \forall\ 2 \leq i < p \\ &M_{e_{p+1}} = a_1\ e_1 + a_2\ e_2 + \dots + a_p\ e_p\ . \end{aligned}$$

Soit P la matrice de $\underset{\sim}{Z}\ M_{p+1}(\underset{\sim}{Z})$,

$$P = \begin{pmatrix} a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \dots & & & \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

On vérifie facilement que

$$\mathrm{Tr}\ P\ M^i = a_i \qquad \forall\ i \leq p\ .$$

$$\mathrm{Tr}\ P\ M^j = 0 \qquad \forall\ j > p\ .$$

Le cas où $a = R(X)/(1 - S(X))$ se ramène facilement à celui-ci : soient

$(P\ ,\ M)$ le couple de matrices associées au polynôme R ,

$(Q\ ,\ N)$ le couple de matrices associées au polynôme S .

On suppose que, $(Q, N) \in M_s(\underset{\sim}{Z})$. Soit N_u la matrice de $M_S(\underset{\sim}{Z})$ dont tous les éléments sont nuls à l'exception de ceux de la 1ère colonne égaux à ceux de la dernière colonne de N.

Soit $N' = N + N_u$. De la même manière, on définit la matrice M_u. Si

$$(P, M) \in M_r(\underset{\sim}{Z}),$$

M_u est la matrice $r \times s$ dont les éléments de la 1ère colonne sont égaux à ceux de la dernière colonne de M, les autres étant nuls.

Soit T la matrice $\begin{pmatrix} M & M_u \\ 0 & N' \end{pmatrix}$. On vérifie que le couple de $M_{r+s}(\underset{\sim}{Z})$, formé de la matrice u, où

$$u = \begin{pmatrix} a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \cdots & & & \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

et T représente la série a, c'est-à-dire que l'on a :

$$a = \sum_{n \geq 0} a_n X^n = \sum_{n \geq 0} (\mathrm{Tr}\, u\, T^n) X^n .$$

L'équivalence des deux démonstration est faite.

Caractérisation des séries rationnelles. – Soit $a = \sum (a, f) f$.

Déterminant de Hankel, en variables non commutatives [1]. – On notera $H_{f,g}$ le déterminant de Hankel dont les lignes et les colonnes sont les coefficients des termes g, $g \leq f$, dans l'ordre de X^*.

PROPOSITION 1 [1]. – Une série est rationnelle si, et seulement si, les déterminants de Hankel sont nuls à partir d'un certain mot f de X^*.

Problèmes posés par les séries rationnelles. – Il est immédiat que si a et b sont des séries rationnelles, leur produit d'Hadamard, $a \odot b = c$, est une série rationnelle. Si μ (et resp. v) est la représentation associée à la série a (resp. b) alors $\mu \otimes \nu$ est la représentation associée à la série c.

Problème. – Etant données deux séries rationnelles a et c, à quelles conditions la série b, définie par la relation $a \odot b = c$, est-elle rationnelle ?

Principaux résultats obtenus, en commutatif étendu en non commutatif.

Pour CANTOR-UCHIYAMA :

$$\sum_{n \geq 0} P(n) a_n X^n \text{ rationnelle} \Longleftrightarrow \sum_{n \geq 0} a_n X^n \text{ rationnelle.}$$

Pour Martine PATHIAUX :

$$\sum_n \frac{a_n X^n}{P(n)\mu_1^n + P_2(n)\mu_2^n} \text{ avec } \sum_n a_n X_n \text{ rationnelle : } \frac{a_n X^n}{P(n)\mu_1^n + P_2(n)\mu_2^n} \text{ entier algé-}$$

brique pour tout n.

Alors

$$\sum_n \frac{a_n X^n}{P(n)\mu_1^n + P_2(n)\mu_2^n} \quad \text{rationnelle.}$$

Pour BENZAGOU :

$$\sum_{n\geq 0} a_n X^n \ \text{Hadamard inversible} \Longleftrightarrow \sum_{n\geq 0} a_n X^n = \sum_{0\leq i<m} \frac{\mu_i X^i}{1 - c_i X^m} .$$

5. K-langages. Automates. Séries rationnelles.

Soit X^* un monoïde libre engendré par un ensemble fini X .

Définition du produit dans $\mathcal{P}(X^*)$.

- Si A , $B \in \mathcal{P}(X^*)$, alors $A \times B = \{ab \ ; \ a \in A \ , \ b \in B\}$.
- Si $A \in \mathcal{P}(X^*)$, alors $A^* = \{e\} \cup A \cup \ldots \cup A^n \cup \ldots$

Définition. - Une partie B de X^* est une partie rationnellement close si $A \subset B$, alors $A^* \subset B$.

K-langages. - La famille des K-langages sur X^* est la plus petite famille contenant X qui est stable par union, produit, et qui est rationnellement close. On se place dans le cas où $A = \mathbb{Z}$. Soient $a = \sum_f (a \ , \ f)f$ et $b = \sum_f (b \ , \ f)f$, deux séries positives, c'est-à-dire $(a,f) \geq 0$, $\forall f$, et $(b,f) \geq 0$, $\forall f$. On notera $\mathcal{A}$ (resp. $\mathcal{B}$) le support de a (resp. b) . On a alors :

$\mathcal{A} \cup \mathcal{B}$ est le support de $a + b$.

$\mathcal{A} \times \mathcal{B}$ est le support de $a \times b$.

Si a est quasi inversible et a^* sa quasi-inverse, alors $\mathcal{A}^*$ est le support de $\mathcal{A}^*$.

$\mathcal{A} \cap \mathcal{B}$ est le support de $a \odot b$.

Liens K-langages-séries rationnelles. - Les K-langages sont les supports des séries rationnelles positives.

6. Automates.

Définition d'un automate. - Un automate est défini par la donnée de trois ensembles U , X , N , et de deux applications s et t .

$$\begin{tikzcd} & U \\ U \times X \arrow[ur, "t"] \arrow[dr, "s"'] & \\ & N \end{tikzcd}$$

U est l'ensemble des états.

X l'ensemble des entrées.

N l'ensemble des sorties.

t l'application de transfert.

s l'application de sortie.

Soit X^* le monoïde libre engendré par X . On "prolonge" la fonction t à $U^* \times X^*$ de la manière suivante

$T(a , e) = a , \quad \forall a \in U , \quad e$ le mot vide de X^* .

$T(a , x) = t(a , x) , \quad x \in X , \quad a \in U$.

$T(a , xp) = T(t(a , x) , p) , \quad a \in U , \quad xp \in X^* , \quad x \in X$.

Soit N^* le monoïde libre engendré par N . On prolonge s en S de la manière suivante :

$$U \times X^* \xrightarrow{S} N^*$$

$S(a , e) = e' , \quad e'$ étant le mot vide de N^* .

$S(a , x) = s(a , x) , \quad \forall a \in U , \quad x \in X$.

$S(a , xp) = s(a , x).S(t(a , x) , p) , \quad a \in U , \quad x \in X , \quad p \in X^*$.

On suppose X fini. Soit $a_0 \in U$, $F \subset U$, F ensemble fini. Une partie régulière A de X^* est associée à un état a_0 d'un automate sans sortie :

$$A = \{f \; ; \; T(a_0 , f) \in F\} .$$

A est le langage d'un automate par rapport à l'état initial a_0 et au sous-ensemble F des états finaux.

PROPOSITION. - Le langage d'un automate à états finis, associé à un état initial $a_0 \in U$, est un K-langage.

BIBLIOGRAPHIE

[1] FLIESS (Michel). - Sur certaines familles de séries formelles, Thèse Sc. math. Univ. Paris-7, 1972.

(Texte reçu le 28 octobre 1974)

Khyra GÉRARDIN
12 rue Beccaria
75012 PARIS