

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

MOHAMED AMARA

Ensembles fermés de nombres algébriques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. n° 8, p. 1-8

http://www.numdam.org/item?id=SDPP_1963-1964__5__A6_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1963-1964, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ENSEMBLES FERMÉS DE NOMBRES ALGÈBRIQUES

par Mohamed AMARA

Introduction.

L'étude d'ensembles de nombres algébriques se ramènent, suivant une idée due à Salem à celle de familles de fractions rationnelles appartenant au corps $Z(x)$.

Nous serons amené dans la première partie de cet exposé, à étudier une famille remarquable de fractions rationnelles et d'en tirer dans la seconde partie des conclusions concernant certains ensembles de nombres algébriques, en particulier S_q en nous servant de la topologie de R et $S_q^{(p)}$ en nous servant de la topologie Q_p .

I. Familles compactes de fractions rationnelles.

Définition. - Nous désignons par $\mathfrak{F}(q, k, \delta)$ une famille de fractions rationnelles $\varphi(z) = \frac{A(z)}{Q(z)}$ telle que :

1° A et Q polynômes à coefficients entiers ; $A(0) \neq 0$ et $Q(0) = q \neq 0$ fixe.

2° $Q(z)$ possède dans $|z| \leq 1$ au plus $k \geq 0$ zéros tous situés dans la couronne $0 < \delta \leq |z| < 1$.

3° $|\varphi(z)| \leq 1, |z| = 1$.

THÉOREME I. - $\mathfrak{F}(q, k, \delta)$ est un ensemble compact pour la convergence uniforme sur la sphère de Riemann dans tout compact situé dans $|z| < 1$.

Démonstration.

A. Dans la première partie nous montrerons que nous pouvons extraire de la famille $\varphi(z)$ une suite qui converge uniformément sur la sphère de Riemann dans tout compact situé dans $|z| < 1$ vers une fraction

$$\frac{A^*(z)}{Q^*(z)} \quad \text{cù} \quad \begin{aligned} A^*(z) &= \sum_{j \geq 0} a_j^* z^j & q^j a_j^* &= \text{entier} \\ Q^*(z) &= q + \sum_j q_j^* z^j & q^{j-1} q_j^* &= \text{entier.} \end{aligned}$$

B. Comme a_j^* et q_j^* sont des nombres rationnels dont le dénominateur ne contient comme facteurs premiers que les nombres premiers divisant q , pour que a_j^* et q_j^* soient entiers, il suffit que

$$|a_j^*|_p \leq 1 \quad \text{et} \quad |q_j^*|_p \leq 1.$$

$$(A) \quad \varphi(z) = \sum u_n z^n \quad \text{pour} \quad |z| < \delta.$$

Posons

$$\psi(z) = \prod_{j=1}^k \frac{1 - \theta_j z}{\bar{\theta}_j - z}$$

$$\frac{1}{\theta_j} \quad \text{étant les racines de} \quad Q(z), \quad \delta \leq \frac{1}{|\theta_j|} < 1$$

$$f(z) = \psi(z) \cdot \varphi(z).$$

Nous pouvons extraire des familles ψ et f des suites telles que :

$$\psi \rightarrow \psi^* = \prod_j \frac{1 - \theta_j^* z}{\bar{\theta}_j^* - z} \quad 1 < |\theta_j^*| \leq \frac{1}{\delta}$$

$$f \rightarrow \psi^* \varphi^*.$$

Donc tout compact situé dans $|z| < \delta$, φ converge uniformément vers φ^* . De plus $\varphi^*(z)$ est méromorphe dans $|z| < 1$ et bornée au voisinage de $|z| = 1$.

$\varphi^* = \sum u_n^* z^n$, où $u_n^* = \lim u_n \implies u_n = u_n^*$ à partir d'un certain rang ($q^{n+1} u_n = \text{entier}$).

$$D_n = D_n^* \quad \text{à partir d'un certain rang.}$$

$$|q^{2n+1} D_n| = |q^{2n+1} D_n^*| \geq qc(\varepsilon) (q^2 \varepsilon)^n.$$

Or $q^{2n+1} D_n$ est un entier $\implies D_n^* = 0$ (quand on est assez loin dans la suite).

Ainsi $\varphi^* = \frac{A^*}{Q^*}$ et, en appliquant un résultat de Fatou, nous avons

$$A^* = \sum a_j^* z^j \quad q^j a_j^* = \text{entier}$$

$$Q^* = q + \sum q_j z^j \quad q^{j-1} q_j^* = \text{entier}$$

$$|\varphi^*(z)| \leq 1 \\ |z| < 1$$

d'où, en faisant tendre z vers un point de $|z| = 1$, nous avons

$$\begin{aligned} |\varphi^*(z)| &\leq 1 \\ |z| &= 1 \end{aligned}$$

$$u_0^* = \frac{A^*(0)}{q} = \lim u_0 \neq 0 \implies A^*(0) \neq 0.$$

(B) a. $|q_j^*|_p \leq 1$, $|q|_p = p^{-g}$.

Soit

- $j(n) =$ le plus petit entier tel que $|q_j|_p = p^{-b}$, $b \in (0, 1, \dots, g)$.
- $b_0 =$ le plus petit entier b tel que $\limsup_Q j(n) = \text{fini}$.
- $m_0 = \limsup j(b_0)$.

De la famille $\varphi(z)$, on peut extraire une suite telle que :

1° pour les polynômes correspondants on ait :

$$\lim j(b) = \infty \text{ si } b < b_0$$

$$j(b_0) = m_0.$$

2° que le polygone de Newton des $Q(z)$ soit fixe pour $0 \leq j \leq m_0$ (m_0, b_0) = sommet de ce polygone.

Dans Ω_p , les polynôme $Q(z)$ ont exactement m_0 zéros α_j situés dans $|q|_p \leq |z|_p \leq \gamma < 1$ ($\log_p \gamma$ étant la pente négative du côté du polygone aboutissant à gauche au sommet (m_0, b_0))

$$Q(z) = \beta(z) Q_1(z)$$

où

$$\beta(z) = \prod_{j=1}^{m_0} (1 - \alpha_j z) = 1 + \beta_1 z + \dots + \beta_{m_0} z^{m_0}.$$

Les polynômes $\beta(z)$ ayant leur polygone de Newton fixe, l'ensemble des zéros α_j est compacte.

Nous pouvons extraire une sous-suite partielle telle que :

$$\alpha_j^* = \lim \alpha_j \quad (\text{au sens } p\text{-adique}).$$

Posons

$$\beta^*(z) = \prod_{j=1}^{m_0} (1 - \alpha_j^* z) = 1 + \beta_1^* z + \dots + \beta_{m_0}^* z^{m_0}$$

$\beta_j^* = \lim \beta_j$ (au sens p -adique).

Considérons $\beta(z) \frac{A(z)}{Q(z)} = \sum v_n z^n$ analytique des $|z|_p < 1$

$$v_n = \sum_{j=n-m_0}^n u_j \beta_{n-j}$$

$$\lim v_n^* = \sum u_j^* \beta_{n-j}^* .$$

De plus, pour $z \in \hat{\Omega}_p$, $\gamma < |z|_p = \rho < 1$, nous avons :

$$\left| \beta \frac{A}{Q} \right|_p \leq \frac{1}{|q|_p} \quad (\text{uniformément})$$

ce qui nous donne $\beta^* \frac{A^*}{Q^*}$ analytique des $|z|_p < \rho$ et $\left| \beta^* \frac{A^*}{Q^*} \right|_p \leq \frac{1}{|q|_p}$.

Comme ρ est aussi voisin que l'on veut de 1, les seuls zéros de $Q^*(z)$ de $|z|_p < 1$ sont les zéros de $\beta^*(z)$. Les côtés à pentes négatives du polygone de Newton de $Q^*(z)$ coïncident ou sont au-dessus de ceux du polygone de Newton de $Q(z)$ pour $0 \leq j \leq m_0$. Ainsi que le polygone de $Q^*(z)$ est situé au-dessus de l'axe des t , et nous avons $|q_j^*|_p \leq 1$.

(B) b. $|a_j^*|_p \leq 1$. Soit $z \in \hat{\Omega}_p$ et $\gamma < |z|_p = \rho < 1$,

$$\left| \beta^* \frac{A^*}{Q^*} \right|_p \leq \frac{1}{|q|_p} \quad \text{et} \quad \left| \frac{Q^*}{\beta^*} \right|_p \leq \frac{|q|_p}{\rho^{m_0 - m_1}}$$

m_1 étant le nombre des $\frac{1}{\alpha_j^*}$ qui sont racines de $Q^*(z)$.

Ainsi

$$|A^*(z)| \leq \frac{1}{\rho^{m_0 - m_1}} .$$

Les inégalités de Cauchy donnent alors $|a_j^*|_p \leq \frac{1}{\rho^{m_0 - m_1 + j}}$.

En faisant tendre ρ vers 1, nous en déduisons :

$$|a_j^*|_p \leq 1 .$$

En utilisant les notations et résultats précédents, nous pouvons démontrer le lemme suivant :

LEMME 1. - Supposons que, pour les fonction de $\mathfrak{F}(q, k, \delta)$, le polygone de Newton de $Q(z)$, pour $0 \leq j \leq m_0$, soit formé d'un seul segment joignant le point $(0, g)$ au point (m_0, b_0) , que $g - b_0$ soit premier à m_0 , et que $|a_0|_p > p^{-\frac{(g-b_0)}{m_0}}$, toute fraction limite vérifiera les mêmes conditions.

2. Ensembles fermés de nombres algébriques.

A. Ensembles S_q .

Définition. - S_q : ensembles de nombres algébriques réels possédant les propriétés suivantes :

1° $\theta \in S_q$ si $\theta > 1$ et $\frac{1}{\theta}$ seul zéro situé dans $|z| \leq 1$ d'un polynôme $Q(z)$ à coefficients entiers rationnel tel $Q(0) = q$ fixe.

2° Il existe $A(z)$ à coefficients entiers tel que $A(1/\theta) \neq 0$, $|A(0)| \geq q$ et $|\frac{A(z)}{Q(z)}| \leq 1$, $|z| = 1$.

Remarque.

1° $q \geq 1$, car nous ne changeons pas θ en remplaçant $Q(z)$ par $-Q(z)$ ou $A(z)$ par $-A(z)$, $\Rightarrow S_q = S_{-q}$ et $A(0) \geq q$.

2° tout nombre algébrique $\theta > 1$, zéro d'un polynôme irréductible $P(z) = qz^s + \dots$, dont les conjugués sont situés dans $|z| < 1$ et dans la norme vérifie $|N(0)| \geq 1$, appartient à S_q .

Nous pouvons prendre dans ce cas :

$$A(z) = P(z)$$

$$Q(z) = z^s P(1/z)$$

sauf si

$$P = Q = qz^2 - az + q \quad (a \geq 2q + 1),$$

car nous prendrons alors dans ce cas

$$A(z) = qz^2 - bz + q \quad (2q \leq b \leq a - 1).$$

3° $Q(z)$ n'étant pas nécessairement primitif ou irréductible, donc $S_{q'} \subset S_q$ si q' divise q :

Ainsi que $S_1 = S \subset S_q$ ou S ensemble de Salem = inverses des nombres de PISOT-VIJAYARAGHAVAN.

THÉORÈME II. A : L'ensemble S_q est fermé.

Soit une suite $\theta \in S_q$ tendant vers un nombre θ' à chaque θ nous associons la fonction $\frac{A(z)}{Q(z)}$ qui sert à le définir et un nombre $\delta > 0$ tel que $|\theta| < \frac{1}{\delta}$ (pour $\theta \in S_q$).

L'ensemble des fractions $\frac{A(z)}{Q(z)}$ appartient à $\mathfrak{F}(q, 1, \delta)$ compact. Nous pouvons extraire une suite partielle tendant vers $\frac{A^*}{Q^*}$ telles que :

$$\frac{A^*}{Q^*} = u_0^* + u_1^* z + \dots$$

$$Q^*(0) = q$$

$$A^*(0) \geq q.$$

$\frac{A(z)}{Q(z)}$ ayant exactement un pôle dans $|z| < 1 \implies u_1^* \neq 0$ et par suite $u_1^* \neq 0$, aussi $\frac{A^*}{Q^*}$ a effectivement un pôle dans $|z| < 1$ et ce pôle ne peut être que $\frac{1}{\theta'}$.

A étant premier à Q^* , nous avons $A^*(1/\theta') \neq 0$.

Le théorème est ainsi démontré.

Remarque. - Si S'_q désigne l'ensemble dérivé de S_q nous pouvons démontrer que pour que $\theta \in S'_q$ il faut et il suffit que $A(z)$ ne soit pas le polynôme réciproque de $Q(z)$.

Détermination des 4 plus petits éléments de S_q . - Soit $\varphi_1(z)$, fraction rationnelle telle que :

$$\varphi_1(z) = 1 + \frac{1}{q} z + \frac{1}{q^2} z^2 + \dots \quad (\varphi(z) \in \mathfrak{F}(q, 1, \delta)).$$

nous avons alors :

$$\varphi_1(z) = \frac{q(1 - z^2)}{q - z - qz^2}$$

ou

$$\varphi_1(z) = \frac{q(1 - z^2) + \varepsilon z^n (q + z - qz^2)}{q - z - qz^2 + \varepsilon qz^n (1 - z^2)}.$$

Soit $\theta \in S_q$ et $\varphi(z)$ la fonction qui le caractérise

$$\varphi(z) = u_0 + u_1 z + u_2 z^2 + \dots$$

$$1^\circ \theta < 1 + \frac{1}{q} \implies u_0 = 1.$$

$$2^\circ \theta < \theta' \text{ racine de } qz^2 - z - q \implies u_1 = \frac{1}{q}.$$

$$3^\circ \theta < \hat{\theta} \text{ racine de } qz^3 + (q-2)z^2 - (q-1)z - q \implies u_2 = \frac{1}{q^2}.$$

Comme $\hat{\theta} < \theta' < 1 + \frac{1}{q}$, nous avons, pour tout nombre $\theta < \hat{\theta}$,

$$\varphi(z) = \frac{q(1-z^2) + z^n(q+z-qz^2)}{q-z-qz^2 + qz^n(1-z^2)}.$$

Nous avons aussi les quatre plus petits éléments de S_q :

$$\theta_1 \text{ zéro } > 1 \text{ de } qz^3 + (q-1)z^2 - qz - q$$

$$\theta_2 \text{ zéro } > 1 \text{ de } qz^4 - z^3 - q$$

$$\theta_3 \text{ zéro } > 1 \text{ de } qz^5 - z^4 - qz^3 + qz^2 - q$$

$$\hat{\theta} \text{ zéro } > 1 \text{ de } qz^3 + (q-2)z^2 - (q-1)z - q.$$

B. Ensemble $S_q^{(p)}$.

Définitions. - $S_q^{(p)}$ = ensemble des nombres algébrique p-adique possédant les propriétés suivantes :

1° $\theta \in S_q^{(p)}$ si $|\theta|_p > 1$ et $\frac{1}{\theta}$ seul zéro situé dans $|z|_p \leq 1$ d'un polynôme $Q(z)$ à coefficients entiers rationnels tel que $Q(0) = q \geq 2$, p premier divisant q et ne divisant pas q_1 .

2° Dans le corps des complexes C, $Q(z)$ a au plus k zéros dans $|z| \leq 1$ situés dans la couronne fixe $0 < \delta \leq |z| < 1$.

3° Il existe $A(z)$ à coefficients entiers rationnels tel que :

$$\left| \frac{A(z)}{Q(z)} \right| \leq 1, \quad |z| = 1; \quad A(1/\theta) \neq 0 \text{ et } |A(0)|_p > |q|_p.$$

THÉORÈME II. B. - L'ensemble $S_q^{(p)}$ est fermé dans Q_p .

Considérons une suite de nombre $\theta \in S_q$ tendant vers une limite θ' . Aux nombres θ , nous associons les fonctions $\frac{A(z)}{Q(z)}$ appartenant à $\mathfrak{E}(q, k, \delta)$ compact.

Nous pouvons extraire une suite partielle tendant vers $\frac{A^*}{Q^*}$ avec $Q^*(0) = q$.

De plus dans $\hat{\Omega}_p$ la fonction $(1 - \theta z) \frac{A(z)}{Q(z)}$ tend, pour $|z|_p \leq \rho < 1$, uniformément vers $(1 - \theta' z) \frac{A^*}{Q^*}$.

Nous avons dans ce cas

$$(m_0, b_0) = (1, 0), \quad |A(0)|_p > p^{-g} = p^{-(m_0 - b_0)/m_0}$$

et le polygone de $Q(z)$ est formé d'un seul côté pour $0 \leq j \leq m_0$. D'après le lemme 1, toute fonction limite vérifiera les mêmes conditions. Ainsi :

- 1° $Q^*(z)$ admet dans Ω_p un zéro et un seul situé dans $|z|_p < 1$.
- 2° $|A^*(0)|_p > |q|_p$.
- 3° $(1 - \theta' z) \frac{A^*}{Q^*}$ est analytique dans $|z|_p < 1$, ce qui nous donne $\frac{1}{\theta'}$ zéro de $Q^*(z)$, soit aussi $\theta' \in \Omega_p$.
- 4° $|\theta^*|_p = \frac{1}{|q|_p} \implies |q_1^*|_p = 1$.

Le théorème est ainsi démontré.

Application. - nombres " p-intégrable" et théorème de Chabauty.

Définition.

- 1° $\theta \in \Omega_p$ est dit " p-intégrable" s'il est zéro d'un polynôme

$$P(z) = p^g z^s + q_1 z^{s-1} + \dots + q_s$$

$q_j \in \mathbb{Z}$, $g \geq 1$ et p nombre premier ne divisant pas q .

- 2° Ensembles C : $\theta \in C$ si :

- a. θ " p-intégrable" et $|\theta_p| > 1$.
- b. $P(z)$ a tous ses zéros dans le corps C situés dans $|z| < 1$.

Théorème de Chabauty. - L'ensemble C est fermé dans p .

$$C = S_q^{(p)} \text{ avec } q = p^g.$$