Séminaire Dubreil.
Algèbre et théorie
des nombres

Marthe Hugot

Caractérisation des nombres de R. Salem

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 1 (1958-1959), exp. n° 5, p. 1-8

<http://www.numdam.org/item?id=SD_1958-1959__12_1_A5_0>

Faculté des Sciences de Paris
-:-:-:-

Séminaire P. DUBREIL,
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)

Année 1958/59
-:-:-:-

15 décembre 1958

CARACTÉRISATION DES NOMBRES DE R. SALEM

par Mlle Marthe HUGOT

THUE a montré [8], en utilisant le principe des tiroirs de Dirichlet, que si, étant donné un nombre $\theta > 1$, on a $\theta^n = u_n + \varepsilon_n$, où u_n est un entier rationnel, et où $|\varepsilon_n| < C\rho^n$ avec $0 < \rho < 1$, alors θ est un nombre algébrique. En utilisant la fonction analytique

$$f(z) = \sum_0^\infty u_n z^n ,$$

C. PISOT [2] a montré que dans ces conditions, θ est un entier algébrique dont les conjugués sont en module strictement inférieurs à 1 ; puis il a montré qu'étant donné un nombre algébrique $\alpha > 1$, si $\lambda\alpha^n = u_n + \varepsilon_n$, où $|\varepsilon_n| < 1$, et si les ε_n ont un nombre fini de points d'accumulation, α est un entier algébrique dont les conjugués ont leur module ≤ 1. R. SALEM a distingué l'ensemble S des nombres θ dont les conjugués sont en module strictement < 1, et l'ensemble T des nombres σ, ayant au moins un conjugué de module 1 [6] et [7], il a montré que S est fermé, alors que T ne l'est pas, puisque tout nombre $\theta \in S$ peut être considéré comme limite d'une suite de nombres $\sigma_\mu \in T$, mais on ne sait pas si l'ensemble T admet d'autres points limites. On connait peu de propriétés des nombres σ, mais certaines sont assez voisines de celles des nombres θ.

En généralisant convenablement la méthode utilisée par THUE [8], C. PISOT a montré le théorème suivant [4] :

THÉORÈME 1. - *Soient α et λ deux nombres réels supérieurs à 1. Posons $\lambda\alpha^n = u_n + \varepsilon_n$; si pour tout $n \geq 0$, on a*

$$\varepsilon_n \leq \frac{1}{2e\,\alpha(\alpha+1)(1+\operatorname{Log}\lambda)}$$

alors α et λ sont algébriques et α est soit un nombre θ, soit un nombre σ.

Soit ϵ la borne supérieure des ε_n : cherchons s'il existe des entiers rationnels $a_0, a_1, \dots, a_k$ où $|a_i| \leq a$ et tels que pour $n \geqslant n_0$

$$v_n = a_0 u_n + a_1 u_{n+1} + \dots + a_k u_{n+k} = 0$$

on a

$$-(u_{n+1} - \alpha u_n) = a_0(\varepsilon_{n+1} - \alpha \varepsilon_n) + \dots + a_k(\varepsilon_{n+k+1} - \alpha \varepsilon_{n+k})$$

d'où

$$|u_{n+1} - \alpha u_n| \leq a(k+1)(\alpha + 1)\,\epsilon \quad ,$$

donc si l'on a

$$a(k+1)(\alpha + 1)\,\epsilon < 1 \tag{1}$$

$u_n = 0$ entraînera $u_{n+1} = 0$.

Posons :

$$w_0 = b_0|u_0| + \dots + b_k|u_k|$$

où $b_0, b_1, \dots, b_k$ sont des entiers rationnels vérifiant $0 \leq b_j \leq a$.

$$w_0 \leq a(k+1)|u_k| = a(k+1)|\lambda \alpha^k + \varepsilon_k|$$

d'où en tenant compte de (1) :

$$w_0 \leq a\lambda(k+1)\,\alpha^k + \frac{1}{\alpha + 1} < (a+1)\,\lambda(k+1)\,\alpha^k - 1 \quad .$$

Il y a $(a+1)^{k+1}$ combinaisons possibles de b_0 , donc si

$$(a+1)^{k+1} \geqslant (k+1)(a+1)\lambda \alpha^k$$

ou

$$(a+s)^k \geqslant (k+1)\lambda \alpha^k \tag{2}$$

w_0 prendra la même valeur pour deux systèmes différents de b_j et par différence entre ces deux expressions on obtiendra $v_0 = 0$. Donc si l'on peut trouver α et k vérifiant (1) et (2), on aura $v_n = 0 \ \forall\, n$, donc α est algébrique,

ainsi que λ qui appartient au corps de α .

On peut prendre pour k et a les entiers définis respectivement par :

$$k - 1 \leq \text{Log } \lambda < k$$

$$a < 2\alpha \lambda^{y_k} \leq a + 1 \quad .$$

En effet si l'on considère la droite d'équation $y_1 = \frac{x}{k} + \text{Log } (1 + k)$ et la courbe d'équation $y_2 = 1 + \text{Log } (1 + x)$, qui se coupent au point $x = k$, pour $x = k - 1$ on a $y_1 < y_2$, ce qui a lieu pour toute valeur de x telle que $k - 1 \leq x < k$ et en particulier pour $x = \text{Log } \lambda$; k étant choisi, on peut prendre pour a le nombre indiqué plus haut. On a alors :

$$\varepsilon < \frac{1}{2e\alpha(\alpha+1)(1+\text{Log } \lambda)}$$

α et λ sont donc algébriques, et d'après le théorème de Fatou, α est un entier algébrique ; d'autre part $\sum \varepsilon_n z^n$ converge à l'intérieur du cercle unité, donc α ne peut être qu'un nombre θ ou un nombre σ . Si $\alpha \in S$, ε_n a un nombre fini de valeurs limites, et si $\alpha \in T$, ε_n est partout dense sur un segment entourant 0 .

En utilisant une méthode voisine, nous allons démontrer le théorème suivant :

THÉORÈME. - <u>Un nombre θ ou σ est zéro d'un polynôme dont les coefficients sont des entiers rationnels qui lui sont inférieurs en valeur absolue.</u>

Auparavant nous allons démontrer que :

THÉORÈME 2. - <u>Il y a des nombres θ dans tout corps algébrique, alors qu'il n'y a de nombres σ que dans l'extension quadratique des corps totalement réels.</u>

1. <u>Nombres θ [5]</u> .

La démonstration est une application du théorème de Minkowski :

Soient n formes linéaires à coefficients réels

$$y_1 = a_{11} x_1 + a_{12} x_2 + \ldots + a_{1n} x_n$$

$$y_n = a_{n1} x_1 + \ldots + a_{nn} x_n$$

où $D = \det(a_{ij}) \neq 0$, si $|\delta_1 \ \delta_2 \ \dots \ \delta_n| \geqslant |D|$, il existe un système d'entiers rationnels $x_1 \ \dots \ x_n$ vérifient

$$|y_1| \leq \delta_1 \qquad |y_n| \leq \delta_n \ .$$

Le théorème est valable pour des formes à coefficients complexes, à condition d'y faire figurer, en même temps qu'une forme à coefficients imaginaire, la forme imaginaire conjuguée et qu'elles soient toutes deux rendues inférieures au même nombre.

Soit un corps de degré k , une base minimale $\omega_1 \ , \ \omega_2 \ , \ \dots \ , \ \omega_k$ de ce corps, $\Delta = (\det(\omega_i^{(\alpha)}))^2$ le discriminant du corps.

$$\begin{aligned}
\theta &= u_1 \omega_1 + \dots + u_k \omega_k \\
\theta_2 &= u_1 \omega_1^{(2)} + \dots + u_k \omega_k^{(2)} \\
&\vdots \qquad\qquad\qquad \vdots \\
\theta_k &= u_1 \omega_1^{(k)} + \dots + u_k \omega_k^{(k)}
\end{aligned}$$

Peut-on avoir : $|\theta| \leq M \ ; \quad |\theta_2| \leq \delta < 1 \ \dots \ |\theta_k| \leq \delta < 1$?

D'après le théorème de Minkowski, on pourra trouver des entiers rationnels $u_1 \ \dots \ u_n$, vérifiant le système I . Si $M \delta^{k-1} \geqslant \sqrt{|\Delta|}$.

Les nombres $\theta \ , \ \theta_2 \ , \ \dots \ , \ \theta_k$ ainsi obtenus sont des entiers algébriques donc $|\theta \ \theta_2 \ \dots \ \theta_k| \geqslant 1$ donc $\theta > 1$ et $\theta \in S$.

2. Nombres σ .

R. SALEM [6] a montré que σ est racine d'un polynôme réciproque de degré $2s$, dont toutes les racines sauf σ et $\frac{1}{\sigma}$ sont sur le cercle unité.

En effet soit $P(z)$ le polynôme irréductible déterminant σ . Il a au moins une racine α de module 1 , or $\alpha \neq \pm 1$ sinon $P(z)$ ne serait pas irréductible, donc $\bar{\alpha} = \frac{1}{\alpha}$ est aussi racine de $P(z)$, on en déduit que $P(z)$, qui a deux racines inverses et est irréductible, est un polynôme réciproque de degré pair.

D'autre part, soient $\sigma \ , \ \frac{1}{\sigma} \ , \ \sigma_2 \ , \ \bar{\sigma}_2 \ , \ \dots \ , \ \sigma_s \ , \ \bar{\sigma}_s$ les conjugués de σ ; posons

$$\gamma = \sigma + \frac{1}{\sigma}$$

$$\gamma_2 = \sigma_2 + \overline{\sigma_2} = \sigma_2 + \frac{1}{\sigma_2}$$

$$\vdots$$

$$\gamma_s = \sigma_s + \overline{\sigma_s} = \sigma_s + \frac{1}{\sigma_s}$$

$\gamma_1\ \gamma_2 \ldots\ \gamma_3$ sont des entiers algébriques réels et l'on a

$$|\gamma| > 2$$

$$|\gamma_2| < 2$$

$$\vdots$$

$$|\gamma_s| < 2$$

On en déduit qu'il n'existe de nombres σ que dans l'extension quadratique des corps totalement réels.

THÉORÈME 3. - Un nombre θ ou σ est zéro d'un polynôme dont les coefficients sont des entiers rationnels qui lui sont inférieurs en valeur absolue [5].

1° Cas d'un nombre θ. - Soit $|\theta_s| \leq |\theta_{s-1}| \ldots \leq |\theta_2| < 1 \leq p < \theta < p + 1$.

Posons

$$u_n = \theta^n + \theta_2^n + \ldots + \theta_s^n$$

$$= \theta^n + \varepsilon_n$$

où u_n est un entier rationnel et où

$$\varepsilon_n = \theta_2^n + \ldots + \theta_s^n$$

$$|\varepsilon_n| \leq (s - 1)\ |\theta_2|^n$$

On cherche s'il existe un rang n_o tel que pour $n \geq n_o$ on ait :

$$v_n = a_o\, u_n + a_1\, u_{n+1} + \ldots + a_k\, u_{n+k}$$

les a_j étant des entiers rationnels tels que $|a_j| \leq p$

$$v_{n+1} - \theta v_n = a_o(\varepsilon_{n+1} - \theta \varepsilon_n) + \ldots + a_k(\varepsilon_{n+k+1} - \theta \varepsilon_{n+k})$$

d'où

$$|v_{n+1} - \theta v_n| \leq (k+1)\, p(1+\theta)(S-1)|\theta_2|^n$$

Si

$$(3) \qquad p(k+1)(1+\theta)(s-1)|\theta_2|^n < 1 \quad .$$

$v_n = 0$ entraîne $v_{n+1} = 0$.

Il suffit de trouver un rang m tel que $v_n = 0$ et que l'inégalité (3) soit vérifiée.

Posons, comme dans la démonstration du théorème 1

$$w_n = b_o|u_n| + \ldots + b_k|u_{n+k}| \quad \text{avec} \quad 0 \leq b_j \leq p$$

$$|w_n| \leq (p+1)(k+1)\theta^{n+k} - 1 \quad .$$

De la même manière on voit que w_n prendra la même valeur pour deux systèmes différents de b_j si

$$(4) \qquad (p+1)^k > (p+1)(k+1)\theta^{n+k}$$

On peut toujours trouver deux entiers n et k vérifiant (3) et (4) ; en effet : (3) équivaut à

$$(3') \qquad n > \frac{\mathrm{Log}(k+1)}{|\mathrm{Log}\,|\theta_2||} + \mathrm{Log}\,\frac{[p(s-1)(1+\theta)]}{|\mathrm{Log}|\theta_2||}$$

et (4) à

$$(4') \qquad n < k\,\frac{\mathrm{Log}(\frac{p+1}{\theta})}{\mathrm{Log}\theta} - \frac{\mathrm{Log}(k+1)}{\mathrm{Log}\theta}$$

et pour k assez grand (3') et (4') peuvent être vérifiées simultanément.

2° Cas d'un nombre σ .

Soit un nombre θ du corps de $\sigma + \frac{1}{\sigma}$, d'après le théorème 2, on peut choisir θ de telle sorte que :

$$|\theta_2| \leq \gamma \ \ldots \ |\theta_s| \leq \gamma \qquad |\theta| \leq \frac{\sqrt{\Delta}}{\gamma^{s-1}}$$

Δ étant le discriminant des corps.

Posons :

$$u_n = \theta(\sigma^n + \frac{1}{\sigma^n}) + \theta_2(\sigma_2^n + \bar{\sigma}_2^n) + \ldots + \theta_s(\sigma_2^n + \bar{\sigma}_s^n)$$

u_n est un entier rationnel et

$$u_n = \theta\, \sigma^n + \varepsilon_n$$

où

$$\varepsilon_n = \frac{\theta}{\sigma^n} + \theta_2(\sigma_2^n + \bar{\sigma}_2^n) + \ldots + \theta_s(\sigma_s^n + \bar{\sigma}_s^n)$$

$$|\varepsilon_n| \leq 2(s-1)\gamma + \frac{\sqrt{\Delta}}{\gamma^{s-1}\sigma^n}$$

Nous cherchons une relation de récurrence de type précédent ; par un calcul analogue on obtient

$$|v_{n+1} - \sigma v_n| \leq p(k+1)(1+\sigma)\left[2\gamma(s-1) + \frac{\sqrt{\Delta}}{\gamma^{s-1}\sigma^n}\right]$$

si $p < \sigma < p+1$.

Donc si

$$p(k+1)(1+\sigma)2\gamma(s-1) < \frac{1}{2} \tag{5}$$

et

$$p(k+1)(1+\sigma)\frac{\sqrt{\Delta}}{\gamma^{s-1}\sigma^m} < \frac{1}{2} \tag{6}$$

sont vérifiées, on aura $v_n = 0$ pour tout $n > m$. La recherche d'un rang m tel que $v_m = 0$ conduit, comme précédemment à l'inégalité :

$$(p+1)^k > (k+1)\,\sigma^{n+k} \tag{7}$$

(5), (6) et (7) permettent alors comme précédemment de déterminer n et k .

On a ainsi montré que si α est un nombre θ ou σ , il est racine du polynôme, non nécessairement irréductible :

$$P(z) \equiv a_o z^k + a_1 z^{k-1} + \ldots + a_k = 0 \quad \text{où} \quad |a_j| \leq p \ .$$

D'autre part un nombre θ ou σ de valeur absolue supérieure à $(p + 1)$ ne peut être racine d'un tel polynôme en effet :

$$\frac{P(z)}{a_o} = z^k + \lambda_1 z^{k-1} + \ldots + \lambda_k = a$$

où $\lambda_1 \ldots \lambda_k$ sont des nombres rationnels tels que $|\lambda_j| \leq p$.

Si on avait $P(\alpha) = 0$ et $|\alpha| > p + 1$, on aurait

$$(p + 1)^k < |\alpha^k| < p \frac{|\alpha|^k - 1}{|\alpha| - 1} < |\alpha^k| - 1$$

ce qui est impossible.

BIBLIOGRAPHIE

[1] HUGOT (Mlle M.) et PISOT (C.). - Sur certains entiers algébriques, C. R. Acad. Sc. Paris, t. 246, 1958, p. 2831-2833.

[2] PISOT (Charles). - Sur une propriété caractéristique de certains entiers algébriques, C. R. Acad. Sc. Paris, t. 202, 1936, p. 892-894.

[3] PISOT (Charles). - Sur la répartition modulo 1 des puissances successives d'un même nombre, C. R. Acad. Sc. Paris, t. 204, 1937, p. 312-314.

[4] PISOT (Charles). - La répartition modulo 1 et les nombres algébriques, Ann. Sc. Norm. Sup. Pisa, 2e série, t. 7, 1938, p. 205-248.

[5] PISOT (Charles). - Répartition (mod 1) des puissances successives de nombres réels, Comment. Math. Helvet, t. 19, 1946-1947, p. 153-160.

[6] SALEM (Raphaël). - A remarkable class of algebraic integers, Proof of a conjecture of Vijayaraghavan, Duke math. J., t. 11, 1944, p. 103-108.

[7] SALEM (Raphaël). - Power series with integral coefficients, Duke math. J., t. 12, 1945, p. 153-172.

[8] THUE (Axel). - Über eine Eigenschaft, die keine transcendente Grösse haben kann, Skr. Vidensk. i Kristiania, I Mat. - nat. Kl., t. 2, 1912, n° 20, 15 p.