MÉMOIRES DE LA S. M. F.

GÉRARD RAUZY

Ensembles de nombres algébriques et transformations rationnelles

Mémoires de la S. M. F., tome 25 (1971), p. 165-168

<http://www.numdam.org/item?id=MSMF_1971__25__165_0>

© Mémoires de la S. M. F., 1971, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (http://smf.emath.fr/Publications/Memoires/Presentation.html) 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/

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 165 à 168

ENSEMBLES DE NOMBRES ALGEBRIQUES ET TRANSFORMATIONS RATIONNELLES

par

G. RAUZY

-:-:-:-

Le but de l'exposé est de montrer sur quelques exemples que les transformations rationnelles transformant l'un dans l'autre certains ensembles de nombres algébriques ont généralement une forme assez simple, déterminée par des considérations topologiques.

Comme premier exemple rappelons qu'une fraction rationnelle f à coefficients dans une extension de $\mathbb{Q}$ qui pour tout $n \in \mathbb{N}$, prend pour valeur un entier algébrique est nécessairement un polynôme. En considérant alors f et $1/f$ on en déduit que si $f(n)$ est une unité algébrique pour $n \in \mathbb{N}$, f est constante. Mais, on peut améliorer ce résultat de la manière suivante :

- <u>si pour une infinité de $n \in \mathbb{N}$, $f(n)$ est une unité algébrique, alors f est constante.</u>

<u>Démonstration.</u> f prenant des valeurs algébriques pour une infinité de n, on peut toujours la supposer f à coefficients dans une extension finie de $\mathbb{Q}$ que l'on prendra galoisienne sur $\mathbb{Q}$ de groupe de Galois G. Si $\sigma \in G$, f_σ désigne la fraction obtenue en faisant agir σ sur les coefficients de f.

Pour $n \in \mathbb{N}$ les $f_\sigma(n)$ sont conjugués sur $\mathbb{Q}$ et pour une infinité de n, $\prod_{\sigma \in G} f_\sigma(n) = 1$, ce qui entraine que la valuation à l'infini de f_σ (qui est celle de chacune des f_σ) est égale à 0. En particulier $f_\sigma(n) \to \lambda_\sigma$ ($\lambda_\sigma \in K^*$) quand $n \to \infty$. Mais, si on suppose $f(n)$ entier algébrique dès que n est assez grand les coefficients de l'équation $\prod_{\sigma \in G} [x - f_\sigma(n)]$ sont des entiers rationnels bornés. Il n'y a qu'un nombre fini de telles équations, $f(n)$ prend une infinité de fois la même valeur, donc f est constante.

En utilisant des idées analogues, on peut étudier les fractions rationnelles laissant invariant l'ensemble des unités algébriques. De manière plus générale, soit K une extension algébrique finie de $\mathbb{Q}$, M un ensemble de valeurs absolues sur K vérifiant une formule du produit

$$x \neq 0 \Rightarrow \prod_{v \in M} |x|_v^{N_v} = 1 .$$

Soit S un ensemble fini de valeurs absolues, τ un élément de K distinct de 0 ou d'une racine de l'unité, f une fraction rationnelle à coefficients dans K,

on a :

- si pour une infinité de $n \in \mathbb{N}$, $f(\tau^n)$ est une S-unité, alors il existe une S-unité λ et un entier $k \in \mathbb{Z}$ tels que : $f(x) = \lambda x^k$.

Démonstration. Quitte à agrandir S on peut supposer que τ est une S-unité. On peut alors remplacer $f(x)$ par $g(x) = f(x)\, x^{-k}$ (sans changer les hypothèses) de manière à avoir g de valuation à l'infini nulle. Soit alors $v_o \in M$ tel que $|\tau|_{v_o} > 1$ (un tel v existe d'après la formule du produit puisque τ n'est pas une racine de l'unité). Quand $n \to \infty$, $|\tau^n|_{v_o} \to \infty$ et par conséquent : $|g(\tau^n) - \lambda|_{v_o} \to 0$ où $\lambda \in K^*$, et même

$$|g(\tau^n) - \lambda|_{v_o} < \frac{C_o}{|\tau^n|_{v_o}} \quad .$$

Pour une infinité de n , $g(\tau^n)$ est une S-unité. Evaluons sa hauteur, c'est-à-dire la quantité :

$$H(g(\tau^n)) = \prod_{v \in M} \max(1, |g(\tau^n)|_v^{N_v}) = \prod_{v \in S} \max(1, |g(\tau^n)|_v^{N_v}) .$$

Pour une valeur absolue quelconque v , si P est un polynôme on a dès que n assez grand

$$|P(\tau^n)|_v < C_1 |\tau^n|_v^{r_1} \quad \text{et} \quad |P(\tau^n)|_v \leq 1$$

sauf pour un ensemble fini de v , fixé lorsque sont connus les coefficients de P. La formule du produit montre alors que pour n assez grand on a une inégalité en sens inverse

$$|P(\tau^n)|_v > C_2 |\tau^n|_v^{r_2} \quad , \quad r_2 \in \mathbb{Z} \quad , \quad C_2 > 0 \quad .$$

Donc une formule analogue pour une fraction rationnelle. On a donc pour une infinité de $n \in \mathbb{N}$:

$$\begin{cases} |g(\tau^n) - \lambda|_{v_o} < \dfrac{C}{H(g(\tau^n))^{\varepsilon}} & \text{avec} \quad \varepsilon > 0 \\ g(\tau^n) \text{ S-unité} \end{cases}$$

Un argument classique, utilisant le théorème de Roth montre alors que pour une infinité de $n \in \mathbb{N}$ $g(\tau^n) = \lambda$, donc que g est constante. C.Q.F.D.

Le résultat précédent montre en particulier que, en désignant par T l'ensemble des nombres de Salem (c'est-à-dire l'ensemble des entiers algébriques supérieurs à 1 , dont tous les autres conjugués sont dans le disque unité, l'un au moins étant sur la circongérence), si une fraction rationnelle f à coefficients dans une

extension de $\mathbb{Q}$ est telle que : $f(T) \subset T$ on a nécessairement $f(x) = x^k$, $k \geq 1$ ou f est constante.

(Un argument beaucoup plus simple utilisant les propriétés particulières aux nombres de Salem pourrait d'ailleurs être utilisé).

Un résultat analogue existe pour l'ensemble S des nombres de Pisot (entiers algébriques supérieurs à 1 dont tous les autres conjugués sont intérieurs au disque unité) mais la méthode de démonstration est différente et repose principalement sur l'emploi du théorème de Rouché.

M. Liardet et Mme Ventadoux ont étendu ce résultat de la manière suivante : (C.R. Acad. Sc. Paris, t. 269, p. 181-183).

- Soit Θ_n l'ensemble des entiers algébriques dont n conjugués au plus sont extérieurs au disque unité si f est une fraction rationnelle non constante telle que : $f(\Theta_n) \subset \Theta_n$ alors il existe $m \in \mathbb{N}^*$ tel que : $f(x) = \pm x^m$.

On peut en employant les mêmes méthodes démontrer le résultat plus général suivant : soit $\mathcal{C}$ l'ensemble des compacts K de C tels que : $\forall Z \in K \quad \bar{Z} \in K$, et $K = \mathring{K}$ c'est-à-dire K est égal à la fermeture de son intérieur. Si $K \in \mathcal{C}$ nous désignons par $\Theta_m(K)$ l'ensemble des entiers algébriques ayant m conjugués au plus extérieurs à K. Et par $\Theta^\circ_m(K)$ l'ensemble des entiers algébriques ayant exactement m conjugués extérieurs à K.

Soient m,n deux entiers ≥ 1, K et H deux éléments de $\mathcal{C}$, f une fraction rationnelle à coefficients dans $\mathbb{Q}$ (ceci uniquement pour ne pas allonger l'énoncé). Alors :

- si $m \leq n$ il y a équivalence entre les propositions :

(i) $f(\Theta^\circ_m(K)) \subset \Theta_n(H)$

(ii) f est un polynôme à coefficients entiers et $f(K) \subset H$.

si $m > n$ aucune fraction rationnelle non constante ne vérifie la condition (i).

Des résultats de ce type se généralisent aisément à des fractions rationnelles de plusieurs variables ou en définissant des ensembles de nombres algébriques avec des conditions portant à la fois sur les valeurs absolues archimédiennes et non archimédiennes. Une autre généralisation plus délicate est d'étendre les résultats à des transformations algébriques. Citons, par exemple, le résultat suivant :

soit $F(x,y)$ un polynôme à 2 variables à coefficients algébriques tel que :

$$\forall \alpha \in S \qquad \exists \beta \in S \qquad F(\alpha,\beta) = 0 .$$

Alors, ou bien $\exists \theta \in S$ tel que identiquement on ait $F(x,\theta) = 0$

ou bien $\exists m \geq 1$ tel que identiquement on ait $F(x,x^m) = 0$.

La démonstration qui utilise des résultats sur l'irréductibilité en a été exposée au séminaire de Théorie des Nombres de Bordeaux en 1969.

Signalons enfin qu'il existe des résultats purement algébrique : par exemple, si m et k sont deux entiers premiers entre eux une condition nécessaire et suffisante pour qu'il existe $\theta \in \Theta_m^\circ$ tel que $\theta^k \in S$ est que 2 divise m et m divise $\varphi(k)$.

-:-:-:-

Faculté des Sciences de Marseille
Département de Mathématiques
Place Victor Hugo
13 - Marseille (3e) (France)