ACTA ARITHMETICA
XV (1969)

Nombres transcendants et ensembles normaux

par

M. MENDÈS FRANCE (Paris)

Here I am
Stoned again.
K. Botto

1. Introduction. Comprendre les rapports qui existent entre les notions de nombres transcendants et de nombres normaux semble être un problème difficile. Le but de cet article est de tenter de jeter un pont entre ces deux concepts.

2. Ensembles normaux. Soit $\Lambda = (\lambda_n)$ une suite infinie de nombres réels. Un nombre réel x est dit Λ-normal si la suite $x\Lambda = (x\lambda_n)$ est équirépartie modulo 1. On note par $B(\Lambda)$ l'ensemble des nombres Λ-normaux.

Un ensemble E est dit *ensemble normal élémentaire* s'il existe une suite Λ telle que $E = B(\Lambda)$. Une intersection dénombrable d'ensembles normaux élémentaires s'appelle un *ensemble normal d'ordre infini* ou, plus brièvement, un *ensemble normal.*

Donnons quelques exemples d'ensembles normaux:

(i) L'ensemble vide $\emptyset$ est un ensemble normal élémentaire comme on le voit en choisissant pour Λ une suite constante.

(ii) $\boldsymbol{R} - \{0\}$ est un ensemble normal élémentaire. En effet, on choisit $\Lambda = (\sqrt{n})$, (résultat dû à Fejér).

(iii) L'ensemble des nombres irrationnels $\boldsymbol{R}-\boldsymbol{Q}$ est un ensemble normal élémentaire ($\Lambda = \boldsymbol{N}$).

(iv) L'ensemble des nombres normaux en base g ($g \geqslant 2$ entier) est un ensemble normal élémentaire et l'ensemble des nombres normaux par rapport à toutes les bases (nombres complètement normaux) est un ensemble normal.

Nous démontrons le théorème suivant:

THÉORÈME. *Le complémentaire de tout corps algébrique réel de degré fini est un ensemble normal élémentaire.*

Ce résultat admet le corollaire suivant:

COROLLAIRE. *L'ensemble des nombres réels transcendants est un ensemble normal.*

En effet, l'ensemble des nombres transcendants réels est l'intersection dénombrable des complémentaires des corps algébriques réels de degré fini.

3. Démonstration du théorème.

LEMME 1. *Soit φ une fonction réelle de la variable réelle x, périodique et de période 1 et telle qu'il existe deux nombres $\alpha > 0$ et $\beta < \infty$ vérifiant*

$$(\forall x \in [0,1]), \quad \alpha x^2(1-x)^2 < 1-\varphi(x) < \beta x^2(1-x)^2.$$

Soit θ un nombre réel supérieur à 1. Alors θ est un nombre de Pisot-Vijayaraghavan, si, et seulement si, le produit infini

$$\prod_{k=0}^{\infty} \varphi(x\theta^k)$$

converge pour au moins un nombre réel $x \neq 0$ (qui est nécessairement dans $\boldsymbol{Q}(\theta)$).

Ce résultat est une simple reformulation d'un résultat classique de Mr Pisot [2]. Nous emploierons ce lemme dans le cas où $\varphi(x) = |\cos \pi x|$.

Introduisons quelques notations. Appelons $e_p(n)$ le $(p+1)^e$ chiffre de l'entier non négatif n écrit dans le système à base 2. Soit $c = (c_n) \in \boldsymbol{R}^{\boldsymbol{N}}$ une suite infinie de nombres réels. On pose

$$\lambda_n(c) = \sum_{p=0}^{\infty} e_p(n) c_p$$

et, en particulier,

$$\lambda_n(\theta) = \sum_{p=0}^{\infty} e_p(n) \theta^p.$$

La suite de terme général $\lambda_n(c)$ (resp. $\lambda_n(\theta)$) sera notée Λ_c (resp. Λ_θ). On aura à considérer les translatées de la suite c: $Tc = (c_{n+1}), \ldots$ $\ldots, T^\nu c = (c_{n+\nu})$.

Enfin, on définit les moyennes de Weyl,

$$M_c(x) = \limsup_{n\to\infty} \left| \frac{1}{n} \sum_{k=0}^{n-1} \exp 2i\pi x \lambda_k(c) \right|.$$

Nous aurons à nous servir du lemme suivant démontré dans [1]:

LEMME 2. *Pour tout entier $\nu \geqslant 1$, on a*

$$M_c(x) = M_{T^\nu c}(x) \prod_{k=0}^{\nu-1} |\cos \pi x c_k|$$

$$M_c(x) \leqslant \prod_{k=0}^{\infty} |\cos \pi x c_k|.$$

Démonstration du théorème. Soit K un corps algébrique réel et soit $\theta \in K$ un nombre de Pisot-Vijayaraghavan ayant le degré du corps; on sait qu'il en existe [2]. Montrons que

$$\complement K \subset B(\Lambda_\theta). \tag{1}$$

En effet, soit $x \in \complement K$. D'après le lemme 2, la moyenne de Weyl $M_\theta(qx)$ (q entier positif) vérifie l'inégalité

$$M_\theta(qx) \leqslant \prod_{k=0}^{\infty} |\cos \pi q x \theta^k|.$$

Or x n'appartient pas au corps de θ. Le lemme 1 montre alors que $M_\theta(qx) = 0$. Il s'ensuit que $x \in B(\Lambda_\theta)$. Ainsi

$$\complement K \subset B(\Lambda_\theta). \tag{2}$$

Soit maintenant $x \in K$. Montrons que $x \notin B(\Lambda_\theta)$. Puisque x est un nombre algébrique, il existe un entier rationnel non nul q tel que $y = qx$ soit un entier algébrique.

La première formule du lemme 2 montre que les deux suites $y\Lambda_\theta$ et $y\theta^\nu \Lambda_\theta$ ($\nu > 0$ entier fixé) sont, ou bien toutes deux équiréparties modulo 1, ou bien toutes deux non équiréparties modulo 1. Or, par le choix de θ, la quantité $y\theta^n$ tend vers 0 modulo 1 quand n croît indéfiniment, et ceci avec une décroissance exponentielle. Il s'ensuit que pour ν suffisamment grand, la suite $y\theta^\nu \Lambda_\theta$ n'est pas dense modulo 1. Le nombre y (et par suite x) n'est donc pas Λ_θ-normal. Ainsi

$$\complement K \supset B(\Lambda_\theta).$$

Cette inclusion associée avec (2) établit l'égalité (1) et le théorème.

4. Exercices et problèmes ouverts.

1° Montrer que $\boldsymbol{Z} - \{0\}$ est un ensemble normal élémentaire. (Considérer la suite Λ_c où $c = \dfrac{1}{2^{p+1}}$.)

Un certain nombre de problèmes naturels se posent en rapport avec l'étude précédente, problèmes dont je ne connais pas la solution.

2° Montrer qu'il existe un ensemble normal qui ne soit pas un ensemble normal élémentaire.

3° Donner une caractérisation des ensembles normaux. Il est facile de voir qu'un ensemble normal E ne contient pas 0, que si m est un entier non nul, alors $mE = \{mx \mid x \in E\}$ est contenu dans E, et qu'enfin E est,

soit de mesure nulle, soit de mesure pleine. Ces conditions sont-elles suffisantes? (Cela m'étonnerait.)

4° Si A et B sont deux ensembles normaux, en est-il de même de $A \cup B$? Sinon, trouver un ensemble normal C non trivial (différent de $\boldsymbol{R}-\{0\}$ ou $\boldsymbol{R}-\boldsymbol{Q}$) qui contienne $A \cup B$.

5° Est-il vrai qu'un nombre complètement normal soit nécessairement transcendant? Ce problème, vraisemblablement très difficile est à l'origine de cette étude.

Travaux cités

[1] M. Mendès France, *Deux remarques concernant l'équirépartition des suites*, Acta Arith. 14 (1968), p. 163-167.

[2] Ch. Pisot, *La répartition modulo 1 et les nombres algébriques*, Ann. Sc. Norm. Sup. Pisa, Série 2, 7 (1938), p. 205-248 (Thèse Sc. Paris, 1938).

Reçu par la Rédaction le 29. 3. 1968

ACTA ARITHMETICA
XV (1969)

A refinement of a theorem of Schur on primes in arithmetic progressions III

by

J. Wójcik (Warszawa)

I have given in [4] a purely algebraic proof of the following specia case of Dirichlet's theorem on arithmetic progression: Let $l^2 \equiv 1 \bmod m$, $m = p^\nu n$, where p is a prime, $\nu > 0$, $p \nmid n$, $l \equiv 1$ or $p \bmod n$. Then there exist infinitely many primes $\equiv l \bmod m$.

The aim of this paper is to extend this result. The proof, again purely algebraic, is based on the well known upper estimate for the number of genera in a cyclic field of prime degree.

Notation: Q is the rational field, m — any positive integer, E_m — the multiplicative group of rationals congruent to 1 mod m, ζ_m — mth primitive root of unity, $P_m = Q(\zeta_m)$.

For any two fields k and K, $k \subset K$, N_{Kk} is the norm from K to k. $(K; k)$ is the degree of K over k, $|k| = (k : Q)$.

For any two abelian groups J and G, $J \subset G$, $|G|$ is the order of G, G/J the quotient group, $(G : J) = |G/J|$.

The term *group of rationals* mod m *prime to* m denotes any set $G \subset Q$ such that 1) $E_m \subset G$, 2) G is multiplicative group, 3) any element of G is prime to m. (Clearly G/E_m is a group of residue classes mod m prime to m.) We say that a field $k \subset P_m$ is invariant with respect to group G if it is invariant with respect to automorphism $\zeta_m \to \zeta_m^n$ of P_m for any integer $n \in G$.

Theorem 1. *Let G, J be groups of rationals* mod m *prime to m and let J be a proper subgroup of G. There exist infinitely many primes in $G \setminus J$.*

Lemma 1. *Let G, J be groups of rationals* mod m *prime to m and let J be a subgroup of G of prime index. Let k be a maximal subfield of P_m invariant with respect to G. There exists a prime ideal $\mathfrak{p}$ in k prime to m such that $N\mathfrak{p}$ does not belong to J.*

Proof. Let K be a maximal subfield of P_m invariant with respect to J. We have:

$$(K : k) = (G/E_m : J/E_m) = (G : J) = l, \quad \text{where } l \text{ is a prime.}$$