

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

GEORGES RHIN

Généralisation d'un théorème de I. M. Vinogradov à un corps de séries formelles sur un corps fini

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 11, n° 1 (1969-1970), exp. n° 14, p. 1-8

http://www.numdam.org/item?id=SDPP_1969-1970__11_1_A10_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1969-1970, 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/>

GÉNÉRALISATION D'UN THÉORÈME DE I. M. VINOGRADOV [5]
 À UN CORPS DE SÉRIES FORMELLES SUR UN CORPS FINI

par Georges RHIN

D'après [5], la suite $p\alpha$, où p décrit la suite croissante des nombres premiers, est équirépartie modulo 1 si, et seulement si, α est irrationnel. Nous généralisons ce théorème à un corps de séries formelles sur un corps fini.

1. Notations et rappels.

Soit F_q le corps fini à q éléments, de caractéristique $p \neq 2$. Nous désignons par \mathfrak{F} le corps des fractions $F_q(x)$. On munit \mathfrak{F} de la valeur absolue ultramétrique discrète, dite "0-adique", en posant pour tout polynôme non nul A de $F_q[x]$, dont on désigne le degré par $d^\circ A$,

$$|A| = q^{-d^\circ A}.$$

Le complété \mathfrak{F}_0 de \mathfrak{F} pour la valeur absolue "0-adique" est le corps $F_q\{x^{-1}\}$ des séries formelles

$$\theta = \sum_{n=-\infty}^{+\infty} a_n x^{-n}, \quad a_n \in F_q \text{ et } a_n = 0 \text{ pour } n < n_\theta.$$

On désigne par \mathfrak{O} l'idéal de valuation de \mathfrak{F}_0 qui est l'ensemble des séries formelles

$$\theta = \sum_{n=1}^{\infty} a_n x^{-n}, \quad a_n \in F_q.$$

On définit l'homomorphisme \mathfrak{K}_0 du groupe additif \mathfrak{F}_0^+ sur le groupe additif \mathfrak{O}^+ par

$$\mathfrak{K}_0\left(\sum_{n=-\infty}^{+\infty} a_n x^{-n}\right) = \sum_{n=1}^{+\infty} a_n x^{-n}.$$

$\mathfrak{K}_0(\theta)$ sera ici la "partie fractionnaire" de θ . Nous considèrerons la mesure de Haar du groupe additif localement compact \mathfrak{F}_0^+ normalisée par

$$\text{mes } \mathfrak{O} = 1.$$

La mesure d'une boule $\mathfrak{B} = \alpha + \mathfrak{O}^d$ sera donc égale à q fois son rayon, c'est-à-dire,

$$\text{mes } \mathfrak{B} = q^{1-d}.$$

CARLITZ [1] a donné la définition de l'équirépartition modulo 1 dans \mathfrak{F}_0 .

Définition 1. - Une suite $(\alpha_n)_{n \geq 1}$ d'éléments de \mathfrak{F}_0 est dite équirépartie modulo 1 dans \mathfrak{F}_0 si la suite $(\mathcal{K}_0(\alpha_n))_{n \geq 1}$ est équirépartie dans le groupe compact \mathfrak{P}^+ .

Soit ψ un caractère différent de 1 du groupe additif F_q^+ , et soit e_0 le caractère de \mathfrak{F}_0^+ , défini par

$$e_0\left(\sum_{n=-\infty}^{+\infty} a_n x^{-n}\right) = \psi(a_1).$$

Alors $e_0(H \cdot)$ pour $H \in F_q[x]$ décrit l'ensemble des caractères e du groupe additif \mathfrak{F}_0^+ tels que

$$e(\theta) = e(\mathcal{K}_0(\theta)).$$

Ces caractères forment un sous-groupe du dual de \mathfrak{F}_0^+ isomorphe au dual de \mathfrak{P}^+ .

On a alors le critère de Weyl [4] :

PROPOSITION 1. - La suite $(\alpha_n)_{n \geq 1}$ d'éléments de \mathfrak{F}_0 est équirépartie modulo 1 dans \mathfrak{F}_0 si, et seulement si,

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N e_0(H\alpha_n) = 0, \quad \forall H \in F_q[x]^*.$$

2. Énoncé du théorème principal.

Soit un ordre sur F_q . Nous définissons l'ordre Ω suivant sur $F_q[x]^*$.

DÉFINITION 2. - Soient $A = a_n x^n + \dots + a_0$, et $B = b_m x^m + \dots + b_0$, deux éléments de $F_q[x]^*$ tels que $a_n \neq 0$ et $b_m \neq 0$, alors

$$A \leq B \text{ pour } \Omega \text{ si } n < m \text{ ou si } n = m,$$

et

$$(a_n, \dots, a_0) \leq (b_n, \dots, b_0)$$

pour l'ordre lexicographique à gauche sur F_q^{n+1} déduit de l'ordre sur F_q .

Soit $(P_n)_{n \geq 1}$ la suite croissante (pour l'ordre Ω) des polynômes unitaires irréductibles de $F_q[x]$. Nous démontrons alors le théorème suivant.

THÉORÈME 1. - La suite $(P_n \alpha)_{n \geq 1}$ est équirépartie modulo 1 si, et seulement si, $\alpha \notin \mathfrak{F}$.

Si $\alpha \in \mathfrak{F}$, $\alpha = \frac{A}{B}$, où A et B sont deux éléments de $F_q[x]$, et $B \neq 0$, alors en prenant $H = B$ dans le critère de Weyl, il vient

$$\frac{1}{N} \sum_{n=1}^N e_0(BP_n \alpha) = 1 ,$$

car, d'après la définition de e_0 , $e_0(F_q[x]) = 1$, et ici

$$BP_n \alpha \in F_q[x] \text{ pour tout } n .$$

Donc la suite $(P_n \alpha)_{n \geq 1}$ n'est pas équirépartie modulo 1 .

Si $\alpha \notin \mathfrak{F}$, pour tout $H \in F_q[x]^*$, $\beta = H\alpha \notin \mathfrak{F}$. En utilisant le développement en fraction continue de β [4], on montre que, pour tout τ entier assez grand, il existe deux éléments A et Q de $F_q[x]$ tels que

$$(A, Q) = 1 \quad (\text{i. e. } A \text{ et } Q \text{ sont étrangers}),$$

$$0 < |Q| \leq q^\tau \quad \text{et} \quad \left| \beta - \frac{A}{Q} \right| < \frac{q^{-\tau}}{|Q|} .$$

Soit N un entier ; alors il existe γ entier tel que $|P_N| = q^\gamma$.

Nous prenons alors ε réel ($0 < \varepsilon < \frac{1}{10}$) et $\tau = \gamma - [\gamma^\varepsilon]$. La démonstration sera différente selon les trois cas suivants.

$$q^{\gamma^\varepsilon} \leq |Q| \leq q^\tau$$

$$\gamma^{24\varepsilon} < |Q| < q^{\gamma^\varepsilon}$$

$$|Q| \leq \gamma^{24\varepsilon} .$$

Les deux premiers cas se traitent en adaptant à \mathfrak{F}_0 les techniques des sommes trigonométriques de I. M. VINOGRADOV [5]. Le dernier cas nécessite une généralisation à \mathfrak{F}_0 d'un théorème de Siegel [2].

3. Énoncé du théorème de Siegel.

Soient R, Q, L trois éléments de $F_q[x]^\tau$, et γ un entier, tels que : R soit unitaire de degré γ et $(L, Q) = 1$.

$\pi(\gamma)$ désigne le nombre de polynômes unitaires irréductibles de $F_q[x]$, et $\Phi(Q)$ l'indicateur d'Euler de Q , c'est-à-dire le nombre de polynômes unitaires A de $F_q[x]$, tels que $d^\circ A = d^\circ Q$ et $(A, Q) = 1$. Pour k entier, $\pi(R, Q, L, k)$ désigne le nombre de polynômes irréductibles unitaires P de $F_q[x]$ tels que

$$|P - R| < q^{\gamma-k} ,$$

et Q divise $P - L$ dans $F_q[x]$.

THÉOREME 2 (SIEGEL). - Soit $u > 0$, alors pour tout polynôme Q de $F_q[x]^*$, et k entier, tels que

$$|Q| \leq \gamma^u \quad \text{et} \quad k^4 \leq \gamma ,$$

nous avons

$$\left| \pi(R, Q, L, k) - \frac{\pi(\gamma)}{q^k \Phi(Q)} \right| \leq c(u) q^{\gamma - \sqrt{\gamma}},$$

où $c(u)$ est une constante positive qui ne dépend que de u .

Nous montrerons successivement comment la démonstration du troisième cas se ramène au théorème 2, puis comment la démonstration du théorème 2 nécessite la recherche, dans le plan complexe, des régions où les fonctions $L(\cdot, \lambda)$, introduites par D. R. HAYES [3], ne s'annulent pas.

4. Le troisième cas se ramène au théorème 2.

Soit \mathfrak{M} l'ensemble des polynômes unitaires de $F_q[x]$. Nous définissons la relation d'équivalence suivante sur \mathfrak{M} :

Définition 3. - Soit k entier, et soient A et B deux éléments de \mathfrak{M} de même degré γ

$$A \mathcal{R}_{(k)} B \iff |A - B| < q^{\gamma - k}.$$

$\mathcal{R}_{(k)}$ partage des polynômes de \mathfrak{M} de degré γ en q^k classes d'équivalence de cardinal $q^{\gamma - k}$. Nous avons la relation suivante entre $\mathcal{R}_{(k)}$ et l'ordre Ω :

PROPOSITION 2. - Si R_1 et R_2 sont deux éléments de même degré tels que $R_1 < R_2$ pour Ω , alors quels que soient les polynômes A et B , tels que

$$A \mathcal{R}_{(k)} R_1 \text{ et } B \mathcal{R}_{(k)} R_2,$$

nous avons $A < B$.

Nous pouvons donc ordonner les représentants des classes modulo $\mathcal{R}_{(k)}$, et si $|P_N| = q^\gamma$, il existe ℓ entier, $1 \leq \ell \leq q^k$, tel que si $R_1 < R_2 < \dots < R_{\frac{k}{q}}$ désignent les représentants de degré γ ,

$$S_N = \sum_{n=1}^N e_o(P_n) = \sum_{|P| \leq q^{\gamma-1}} e_o(P) + \sum_{i=1}^{\ell-1} \sum_{P \in \mathcal{R}_{(k)} R_i} e_o(P) + o\left(\sum_{P \in \mathcal{R}_{(k)} R_\ell} 1\right).$$

Il suffit alors de montrer que

$$\sum_{|P| \leq q^{\gamma-1}} e_o(P) = o(\pi(\gamma - 1) + \pi(\gamma - 2) + \dots + \pi(1)),$$

$$S_N(R_i) = \sum_{P \in \mathcal{R}_{(k)} R_i} e_o(P) = o(\pi(\gamma) q^{-k}),$$

et de prendre k tel que

$$\pi(R_\ell, 1, 1, k) = o(\pi(\gamma)).$$

Pour vérifier la dernière propriété, nous prenons $k = [\gamma^\epsilon]$, donc

$$|\pi(R_i, 1, 1, k) - \pi(\gamma) \times q^{-[\gamma^\epsilon]}| \leq c(24\epsilon)_q \gamma^{-\sqrt{\gamma}}$$

d'après le théorème 2. Ce choix de k convient, car $\pi(\gamma)$ est équivalent à $\gamma^{-1} q^\gamma$.

En partageant les polynômes de degré $\gamma - 1, \gamma - 2, \dots$ en classes d'équivalence modulo $\mathfrak{R}_{(k)}$, on se ramène à n'étudier que des sommes du type $S_N(R_i)$.

Posons $\beta = \frac{A}{Q} + \frac{\theta}{QT}$ où $|T| = q^T$ et $|\theta| < 1$. Alors, si $P \in \mathfrak{R}_{(k)} R_i$, nous avons

$$P_\beta = \frac{PA}{Q} + \frac{R_i \theta}{QT} + \frac{(P - R_i)\theta}{QT} \quad \text{et} \quad \frac{(P - R_i)\theta}{QT} \in \mathfrak{P}^2,$$

donc

$$S_N(R_i) = e_o\left(\frac{R_i \theta}{QT}\right) \sum_{P \in \mathfrak{R}_{(k)} R_i} e_o\left(\frac{PA}{Q}\right),$$

et

$$S_N(R_i) = e_o\left(\frac{R_i \theta}{QT}\right) \sum_{\substack{(L, Q)=1 \\ |L| < |Q|}} \sum_{\substack{P \in \mathfrak{R}_{(k)} R_i \\ Q \text{ divise } P-L}} e_o\left(\frac{AL}{Q}\right),$$

et, puisque $|e_o\left(\frac{R_i \theta}{QT}\right)| = 1$, il vient

$$|S_N(R_i)| = \left| \sum_{\substack{(L, Q)=1 \\ |L| < |Q|}} \pi(R_i, Q, L, k) e_o\left(\frac{AL}{Q}\right) \right|.$$

En utilisant le théorème 2,

$$|S_N(R_i)| \leq \frac{\pi(\gamma)}{q^k \phi(Q)} \left| \sum_{\substack{(L, Q)=1 \\ |L| < |Q|}} e_o\left(\frac{AL}{Q}\right) \right| + \phi(Q) q^{\gamma - \sqrt{\gamma}}.$$

Sachant que

$$\sum_{\substack{(L, Q)=1 \\ |L| < |Q|}} e_o\left(\frac{AL}{Q}\right) = \mu(Q),$$

où μ est la fonction de Möbius (et donc $|\mu(Q)| \leq 1$) et que

$$|Q|^{1/2} \leq |\phi(Q)| \leq |Q|,$$

on voit que

$$S_N(R_i) = o(\pi(\gamma) q^{-k}).$$

5. Introduction des fonctions $L(\cdot, \chi)$

Soit \mathcal{R} une relation d'équivalence sur \mathcal{M} , telle que le quotient \mathcal{M}/\mathcal{R} soit un demi-groupe et que le groupe $\mathcal{G}(\mathcal{R})$ des éléments inversibles soit fini d'ordre $g(\mathcal{R})$. Soit $\hat{\mathcal{G}}$ le dual de $\mathcal{G}(\mathcal{R})$, et on définit [3] les caractères sur \mathcal{M} .

Définition 4. - Soit $\chi \in \hat{\mathcal{G}}$, on définit l'homomorphisme χ de \mathcal{M} dans les nombres complexes de module 1 par

$$\chi(G) = \chi(\bar{G}) \text{ si la classe } \bar{G} \text{ est inversible,} \\ = 0 \text{ sinon.}$$

Soient $\chi_0 = 1, \chi_1, \dots, \chi_{g-1}$ les caractères relatifs à \mathcal{R} . On étend à \mathcal{M} la relation $\mathcal{R}_{(k)}$:

Si A et B sont deux éléments de \mathcal{M} de degrés respectifs n et m , on pose

$$A \mathcal{R}_{(k)} B \iff |x^m A - x^n B| < q^{m+n-k}.$$

Alors $g(\mathcal{R}_{(k)}) = q^k$. Si $H \in \mathcal{M}$, soit \mathcal{R}_H la relation

$$A \mathcal{R}_H B \iff H \text{ divise } A - B.$$

Alors $\mathcal{G}(\mathcal{R}_H) = \mathcal{G}(H)$.

Nous définissons la relation $\mathcal{R}_{(k)H} = \mathcal{R}_{(k)} \cap \mathcal{R}_H$.

Alors, si $(H, L) = 1$, \bar{L} est inversible dans $\mathcal{G}(\mathcal{R}_{(k)H})$.

PROPOSITION 3. - Si $\chi_0, \chi_1, \dots, \chi_{g-1}$ avec $g = g(\mathcal{R}_{(k)H}) = q^k \mathcal{G}(H)$ sont les caractères relatifs à $\mathcal{R}_{(k)H}$, nous avons

$$\pi(R, H, L, k) = \sum_{|P|=q^\gamma} \frac{1}{g} \sum_{i=0}^{g-1} \bar{\chi}_i(L) \chi_i(P).$$

En effet, si \bar{P} n'est pas inversible, $\chi_i(P) = 0$, et si \bar{P} est inversible,

$$\frac{1}{g} \sum_{i=0}^{g-1} \bar{\chi}_i(L) \chi_i(P) = \frac{1}{g} \sum_{i=0}^{g-1} \chi_i(\bar{P} \cdot \bar{L}^{-1}),$$

et cette expression est l'intégrale de Haar sur $\hat{\mathcal{G}}$ du caractère $\chi_i \mapsto \chi_i(\bar{P} \cdot \bar{L}^{-1})$ de $\hat{\mathcal{G}}$. Cette intégrale est égale à 1 si Q divise $P - L$, et à 0 sinon. En posant,

$$\pi(\gamma, \chi_i) = \sum_{|P|=q^\gamma} \chi_i(P),$$

nous obtenons

$$\pi(R, H, L, k) = \frac{1}{g} \sum_{i=0}^{g-1} \bar{\chi}_i(L) \pi(\gamma, \chi_i).$$

On démontre que

$$\pi(\gamma) - \pi(\gamma, \kappa_0) = \sum_{\substack{P \\ \bar{P} \text{ non inversible}}} 1 \leq 2g,$$

et donc

$$\left| \pi(R, H, L, k) - \frac{\pi(\gamma)}{q^k \varphi(H)} \right| \leq 2 + \frac{1}{g} \sum_{i=1}^{g-1} |\pi(\gamma, \kappa_i)|.$$

Il suffit alors de démontrer que, pour $1 \leq i \leq g-1$, $|\pi(\gamma, \kappa_i)| \leq c(u)q^{\gamma-\sqrt{\gamma}}$.
Nous posons

$$L(s, \kappa) = \sum_{G \in \mathbb{F}^*} \frac{\kappa(G)}{|G|^s} \quad s = \sigma + it \text{ et } \sigma > 1,$$

et nous obtenons, si $a \geq 1$,

$$\pi(\gamma, \kappa_i) = \frac{-1}{2\gamma\pi i \log^2 q} \int_{a-i\infty}^{a+i\infty} \frac{q^{(\gamma+1)s} - q^{\gamma s}}{s^2} \frac{L'(s, \kappa)}{L(s, \kappa)} ds + O(\gamma q^{\gamma/2}),$$

ce qui ramène la démonstration du théorème 2 à l'étude des régions de \mathbb{C} où les fonctions $L(\cdot, \kappa)$ ne s'annulent pas.

6. Autres résultats.

Nous démontrons aussi le théorème suivant :

THÉORÈME 3. - Soit f un polynôme à coefficients dans \mathfrak{F}_0 , de degré k
($2 \leq k < p$),

$$f(X) = \alpha_0 + \alpha_1 X + \dots + \alpha_k X^k.$$

Si il existe un entier s ($2 \leq s \leq k$) tel que $\alpha_s \notin \mathfrak{F}$ et tel que, si $(A_i)_{i \geq 1}$ désigne le développement en fraction continue de α_s , la suite A_i soit bornée, alors la suite $(f(P_n))_{n \geq 1}$ est équirépartie modulo 1 dans \mathfrak{F}_0 .

BIBLIOGRAPHIE

- [1] CARLITZ (L.). - Diophantine approximation in fields of characteristic p ,
Trans. Amer. math. Soc., t. 72, 1952, p. 187-207.
- [2] ESTERMANN (T.). - Introduction to modern prime number theory. - Cambridge, at
the University Press, 1952 (Cambridge Tracts in Mathematics and mathematical
Physics, 41).
- [3] HAYES (D. R.). - The distribution of irreducibles in $GF[q, x]$, Trans. Amer.
math. Soc., t. 117, 1965, p. 101-127.
- [4] MATHAN (Bernard de). - Approximations diophantiennes dans un corps local,
Bull. Soc. math. France, Mémoire 21, 1970, 93 p. (Thèse Sc. math. Caen,
1968).

- [5] VINOGRADOV (I. M.). - The method of trigonometrical sums in the theory of numbers (Translated from Russian). - London, Interscience Publishers, 1954.

(Texte reçu le 12 octobre 1970)

Georges RHIN
14 rue Leroy
14 - CAEN
