# § 2. DÉMONSTRATION DU THÉORÈME

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **22.09.2024**

$$W_h = \begin{cases} \dfrac{1}{2}, & h = 1 \\ \dfrac{1}{3}, & h = 2 \\ \dfrac{1}{6}, & h = 3 . \end{cases}$$

Un grand nombre des nouveaux calculs par Goldstine et von Neumann [6], Lehmer [15], et Cassels [1] nous ont conduits à douter de la véracité de la conjecture de Kummer; les mêmes calculs semblent aussi indiquer que les angles $\theta_p$ sont équirépartis dans l'intervalle $(0, \pi)$ pour la mesure de Lebesgue. Le but de cette note est de donner une démonstration du résultat suivant.

*Théorème. Soit* $\chi_I$ *la fonction caractérisitique d'un sous-intervalle* $I$ *de* $(0, \pi]$, *alors*

$$\sum_{\substack{p \leq x \\ p \,=\, 1 (mod\ 3)}} \chi_I(3\theta_p) = \frac{|I| x}{2 \log x} + o\Big(\frac{x}{\log x}\Big),$$

*où* $|I|$ *est la mesure de Lebesgue de* $I$.

*Remarque.* Le Théorème a été énoncé comme une loi de distribution des nombres premiers mais on peut dire simplement que les angles de la troisième puissance de $\tau_p$ sont équirépartis dans l'intervalle $(0, \pi]$ pour la mesure de Lebesgue.

## § 2. Démonstration du théorème

L'idée de la démonstration a été déjà considérée par Davenport-Hasse [4] et aussi par Weil [21]. Elle consiste à interpréter les sommes de Gauss comme des traces d'opérateurs de Frobenius.

Soit $E = Q(\rho)$ le corps quadratique imaginaire obtenu en adjoignant $\rho = e^{\frac{2\pi i}{3}}$ à $Q$ et $J_E$ son anneau d'entiers. L'arithmétique de $J_E$ est bien connue et on sait que les nombres premiers dans $J_E$ appartiennent a deux classes selon que la norme est un nombre premier rationnel ou le carré d'un nombre premier rationnel. Dans ce paragraphe, nous décrirons une construction locale des sommes de Gauss. Soit $\mathfrak{q}$ un nombre premier de $J_E$, $F\mathfrak{q}$ son corps résiduel et $N_{E/Q}(\mathfrak{q}) = q$ l'ordre de $F\mathfrak{q}$. Il est très facile de voir que $q \equiv 1 \pmod 3$, ce qui permet de construire un caractère cubique multiplicatif pour le groupe cyclique $F^*\mathfrak{q} = F\mathfrak{q} - (0)$ en prenant la racine de l'unité $\chi\mathfrak{q}$ dans $J_E$ qui satisfait à la congruence

$$\chi\mathfrak{q}(x) \equiv x^{\frac{q-1}{3}} \pmod{\mathfrak{q}}.$$

Pour $x \equiv 0 \pmod{\mathfrak{q}}$ nous posons $\chi\mathfrak{q}(x) = 0$. Soit $\psi(x)$ un caractère additif du groupe $F\mathfrak{q}$ distinct de l'unité. La somme de Gauss attachée au nombre premier $\mathfrak{q}$ est définie par

$$g(\chi\mathfrak{q}, \psi) = \sum_x \chi\mathfrak{q}(x)\psi(x),$$

où $x$ décrit le corps résiduel $F\mathfrak{q}$. Le changement de $x$ en $t\,x$, où $t \varepsilon F^*\mathfrak{q}$, donne

$$g(\chi\mathfrak{q}, \psi) = \chi\mathfrak{q}(t) \sum_x \chi\mathfrak{q}(x)\psi(xt),$$

ce qui prouve que le changement du caractère additif $\psi$ en un autre dans la définition de la somme de Gauss ne fait que multiplier celle-ci par un facteur connu. Il en résulte que $g(\chi\mathfrak{q}, \psi)^3$ ne dépend que du nombre premier $\mathfrak{q}$.

Les propriétés suivantes des sommes de Gauss sont immédiates.

A′) $|g(\chi\mathfrak{q}, \psi)|^2 = N_{E/Q}(\mathfrak{q})$.

C) Si $\mathfrak{g}$ est de degré 1 et $\psi(k) = e^{\frac{2\pi ik}{p}}$, où $p = N_{E/Q}(\mathfrak{g})$ il en résulte que la somme $g(\chi\mathfrak{q}, \psi)$ coincide avec la somme $\tau_p$ definie par (1) pour un choix du générateur $g$ de $(Z/pZ)^*$ bien déterminé.

D) Le symbole local

$$\kappa\mathfrak{q} = g(\chi\mathfrak{q}, \psi)^3$$

ne dépend que de $\mathfrak{q}$.

Pour définir le symbole de Kummer global nous considérons l'ensemble des entiers $I_E(2(1-\rho)^2)$ qui sont premiers avec $2(1-\rho)^2$, et pour chaque $\mathfrak{a} \in I_E(2(1-\rho)^2)$ nous posons

$$\kappa(\mathfrak{a}) = \frac{\prod_{\mathfrak{q} \mid \mathfrak{a}} (-\kappa\mathfrak{q})^{ord\,\mathfrak{q}(\mathfrak{a})}}{N_{E/Q}(\mathfrak{a})^{\frac{3}{2}}}.$$

On a pour le symbole de Kummer $\kappa(\mathfrak{a})$ le résultat suivant.

*Théorème* (Deuring-Shimura-Weil). *Le symbole de Kummer $\kappa(\mathfrak{a})$ est un « Grössencharakter ».*

Pour la démonstration de ce résultat important nous renvoyons aux mémoires de Weil ([20] pp. 489-491), Shimura-Taniyama ([18] pp. 144-148: Main Theorem 4) et Deuring ([5]). Voir aussi notre mémoire ([16] § 3: Generalized Gauss sums as characters) où nous donnons une démonstration valable pour le cas d'une somme de Gauss générale.

Du fait que le symbole $\kappa(\mathfrak{a})$ est un Grössencharakter on peut construire les fonctions

$$L(s, \kappa^v) = \sum{}' \kappa^v(\mathfrak{a}) N(\mathfrak{a})^{-s} = \prod{}' (1 - \kappa^v(\mathfrak{q}) N(\mathfrak{q})^{-s})^{-1},$$

où $\mathfrak{a}$ (resp. $\mathfrak{q}$) sont des entiers (resp. nombres premiers) dans $I_E(2(1-\rho)^2)$ et $v$ un entier rationnel $\geqq 1$. La théorie de Hecke [8] nous donne que

$$L(1 + it, \kappa^v) \neq 0$$

pout tous $-\infty \leqq t \leqq \infty$ et $v \in Z^+$. Alors un raisonnement du type Taubérien nous donne (voir Hecke [8], Serre [17] et Lang [14])

$$\sum_{N(\mathfrak{q}) \leqq x} \kappa_{\mathfrak{q}}^v = o\left(\frac{x}{\log x}\right).$$

Mais nous savons que

$$\sum_{\substack{N\mathfrak{q} \leqq x \\ deg\, \mathfrak{q} = 2}} \kappa_{\mathfrak{q}}^v = o\left(x^{\frac{1}{2}} (\log x)^2\right);$$

il en résulte, selon le critère de Weyl [22], que les angles $\theta\mathfrak{q}$ de $\kappa\mathfrak{q} = e^{i\theta\mathfrak{q}}$ pour les nombres premiers $\mathfrak{q}$ de degré 1 sont équirépartis dans le cercle $R/2\pi Z$ pour la mesure de Lebesgue. Pour vérifier notre Théorème il reste à observer que pour chaque nombre premier $\mathfrak{q}$ in $I_E(2(1-\rho)^2)$ de degré 1 on a par conjugaison un autre nombre premier $\overline{\mathfrak{q}}$ aussi de degré 1 avec la propriété

$$\overline{\kappa\mathfrak{q}} = \kappa\overline{\mathfrak{q}}.$$

Finalement nous faisons usage de l'égalité

$$\kappa\mathfrak{q} = p^{-\frac{3}{2}} \tau_p^{\ 3},$$

où $p = N_{E/Q}(\mathfrak{q})$, ou ce qui est la même chose

$$N_{E|Q}(\mathfrak{q})^{\frac{3}{2}} e^{i\theta\mathfrak{q}} = p^{\frac{3}{2}} e^{i3\theta p}.$$

Cela démontre la proposition.