§1. ENSEMBLES DE NOMBRES PREMIERS

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **22 (1976)**

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

PDF erstellt am: **26.09.2024**

§ 1. ENSEMBLES DE NOMBRES PREMIERS

Soit P un ensemble de nombres premiers. Considérons les propriétés suivantes:

(1.1) $$\sum_{p \in P} 1/p = +\infty ;$$

(1.2) P est de *densité* $\alpha > 0$, i.e. le nombre des $p \in P$ qui sont $\leqslant x$ est égal à $\alpha x/\log x + o(x/\log x)$ quand $x \to \infty$.

(1.3) P est *régulier* de densité $\alpha > 0$, au sens de Delange [3], i.e.

$$\sum_{p \in P} p^{-s} = \alpha \log 1/(s-1) + \theta_P(s),$$

où $\theta_P(s)$ se prolonge en une fonction holomorphe pour $\mathscr{R}(s) \geqslant 1$.

(1.4) P est *frobénien* de densité $\alpha > 0$, i. e. il existe une extension finie galoisienne $K/\mathbf{Q}$, et une partie H du groupe $G = \mathrm{Gal}(K/\mathbf{Q})$ telles que

(a) H est stable par conjugaison,

(b) $|H|/|G| = \alpha$ (on note $|X|$ le nombre d'éléments d'un ensemble fini X),

(c) pour tout p assez grand, on a $p \in P \Leftrightarrow \sigma_p(K/\mathbf{Q}) \in H$, où $\sigma_p(K/\mathbf{Q})$ désigne la substitution de Frobenius [1] de p dans G (définie à conjugaison près lorsque p ne divise pas le discriminant de K).

PROPOSITION 1.5. *On a* (1.4) $\Rightarrow$ (1.3) $\Rightarrow$ (1.2) $\Rightarrow$ (1.1).

L'implication (1.2) $\Rightarrow$ (1.1) est facile. L'implication (1.3) $\Rightarrow$ (1.2) est prouvée dans [3], p. 57, comme conséquence d'un théorème taubérien. D'autre part, sous les hypothèses de (1.4), on a

(1.6) $$\sum_{p \in P} p^{-s} = \frac{1}{|G|} \sum_{\chi} \bar{\chi}(H) \log L(s, \chi)^{1)} + g(s),$$

où:

χ parcourt l'ensemble des caractères irréductibles de G,

$L(s, \chi)$ est la fonction L d'Artin [1] relative à l'extension $K/\mathbf{Q}$ et au caractère χ,

[1]) Ici, comme au §2, la détermination choisie de « log » est celle que l'on obtient par prolongement analytique sur les horizontales à partir de la détermination « évidente » pour $\mathscr{R}(s) > 1$ (i. e. celle fournie par le développement en série — on peut aussi la caractériser par le fait qu'elle tend vers 0 quand $\mathscr{R}(s)$ tend vers $+\infty$).

g est une série de Dirichlet qui converge absolument pour $\mathscr{R}(s) > 1/2$ (donc est holomorphe pour $\mathscr{R}(s) \geqslant 1$),

$$\bar{\chi}(H) = \sum_{h \in H} \bar{\chi}(h).$$

Il résulte alors des propriétés élémentaires des fonctions $L(s, \chi)$ que $\log L(s, \chi) = \delta_\chi \log 1/(s-1) + \theta_\chi(s)$, où $\delta_\chi = 0$ (resp. $\delta_\chi = 1$) si $\chi \neq 1$ (resp. si $\chi = 1$), et $\theta_\chi(s)$ est holomorphe pour $\mathscr{R}(s) \geqslant 1$. La propriété (1.3) en résulte.

Exemples.

(1) Si a et m sont des entiers $\geqslant 1$ tels que $(a, m) = 1$, l'ensemble des nombres premiers p tels que $p \equiv a \pmod{m}$ est frobénien de densité $1/\varphi(m)$.

(2) L'ensemble des nombres premiers qui se décomposent complètement (resp. ont un facteur premier de degré 1) dans une extension finie de $\mathbf{Q}$ est frobénien de densité > 0.

(3) Soit τ la fonction de Ramanujan (cf. [6], [19], [27]). Si m est un entier $\geqslant 1$, l'ensemble des p tels que $\tau(p) \equiv 0 \pmod{m}$ est frobénien de densité $\alpha(m) > 0$; cela résulte de Deligne [4] (voir aussi [19], [27], ainsi que le §4 ci-après). Lorsque m est premier, on peut calculer $\alpha(m)$ grâce à [27]. On trouve:

$$\alpha(m) = \begin{cases} 1, 1/2, 1/4, 1/2, 1/2, 1/690 & \text{si } m = 2, 3, 5, 7, 23, 691 \\ m/(m^2-1) & \text{sinon.} \end{cases}$$

Remarque. Lorsque P est frobénien, on peut préciser un peu le comportement de la fonction $f_P(s) = \sum_{p \in P} p^{-s}$ à gauche de la droite critique $\mathscr{R}(s) = 1$:

PROPOSITION 1.7. *La fonction f_P se prolonge en une fonction holomorphe dans une région de la forme*

$$(1.8) \quad \begin{cases} \mathscr{R}(s) \geqslant 1 - b/\log^A T, & \textit{avec} \quad b, A > 0\,, \quad T = 2 + |\mathscr{I}(s)| \\ \mathscr{I}(s) \neq 0 \quad \textit{ou} \quad s \quad \textit{réel} \quad > 1\,, \end{cases}$$

et y admet une majoration

$$(1.9) \qquad |f_P(s)| = O(\log\log T) \quad \textit{pour} \quad T \to \infty\,.$$

Cela se démontre de la manière suivante: vu (1.6), il suffit de prouver l'énoncé analogue pour $\log L(s, \chi)$; grâce au théorème d'induction de Brauer, on peut en outre supposer que χ est un caractère de degré 1 de

Gal (K/E), où E est un sous-corps de K. On peut alors appliquer à $\log L(s,\chi)$ les méthodes classiques de Hadamard et de La Vallée Poussin, cf. par exemple [10], p. 336-337. [En fait, [10] se borne à prouver l'existence d'une région (1.8) où $L = L(s, \chi)$ est holomorphe $\neq 0$, et où $|L'/L| = O(\log^A T)$. Pour passer de là à la majoration

$$|\log L(s, \chi)| = O(\log\log T),$$

on distingue deux cas, suivant que $\mathscr{R}(s)$ est ou non $\geqslant 1 + 1/\log^A T$. Dans le premier cas, on a:

$$\begin{aligned} |\log L(s, \chi)| \leqslant [E:Q] \log \zeta(\mathscr{R}(s)) &\leqslant [E:Q]\, A \log\log T + O(1) \\ &= O(\log\log T). \end{aligned}$$

Le deuxième cas se ramène au premier: on applique le théorème des accroissements finis au segment horizontal I_s joignant s au point s_0 tel que

$$\mathscr{I}(s_0) = \mathscr{I}(s), \quad \mathscr{R}(s_0) = 1 + 1/\log^A T,$$

et l'on obtient

$$\begin{aligned} |\log L(s, \chi)| &\leqslant |\log L(s_0, \chi)| + |s - s_0| \sup_{\sigma\in I_s} |L'/L(\sigma, \chi)| \\ &= O(\log\log T) + O(1) = O(\log\log T).] \end{aligned}$$

§2. THÉORÈMES DE DENSITÉ

2.1. *Définitions.* Soit E une partie de l'ensemble $\mathbf{N}^*$ des entiers > 0; on note E' le complémentaire $\mathbf{N}^* - E$ de E. Si $x \in \mathbf{N}^*$, on note $E(x)$ le nombre des $n \leqslant x$ qui appartiennent à E; on a $E(x) + E'(x) = x$. Lorsque E est l'ensemble des n satisfaisant à une relation R, on écrit aussi

$$N\{n \leqslant x : R(n)\}$$

à la place de $E(x)$.

On dit que E est de *densité* c si $\lim_{x\to\infty} E(x)/x = c$, autrement dit si

$$E(x) = cx + o(x) \quad \text{pour} \quad x \to \infty.$$

Soit P un ensemble de nombres premiers. Nous dirons que P est *associé* à E si, pour tout $p \in P$ et tout entier $m \geqslant 1$ non divisible par p, on a $pm \in E$.

THÉORÈME 2.2. *Si P est associé à E, et si P jouit de la propriété* (1.1), *à savoir* $\sum_{p\in P} 1/p = +\infty$, *alors E est de densité* 1.