I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a complété celui de l'année précédente, consacré au théorème de densité de Čebotarev, et à ses applications. Il a commencé par exposer, avec démonstrations, un certain nombre de résultats connus :

bornes supérieures dans la méthode du crible (d'après Selberg), et application au théorème de Brun-Titchmarsh ;

régions sans zéros pour les fonctions L (d'après de la Vallée Poussin) ;

zéros exceptionnels (d'après Siegel et Stark) ;

formes effectives du théorème de Čebotarev (d'après Lagarias-Odlyzko).

Les applications ont porté sur les *courbes elliptiques* et sur les *formes modulaires* ; elles sont résumées ci-après. Pour certaines d'entre elles, il a été nécessaire de supposer l'exactitude de l'*Hypothèse de Riemann Généralisée* (GRH).

1. *Courbes elliptiques*

Soient E une courbe elliptique sur $\mathbf{Q}$, et S_E l'ensemble (fini) des nombres premiers p en lesquels E a mauvaise réduction. Si p n'appartient pas à S, soit $E(p)$ le groupe des points de E modulo p.

THÉORÈME 1.1 (sous GRH) - *Supposons que l'un des points d'ordre* 2 *de* E *ne soit pas rationnel sur* $\mathbf{Q}$. *Alors l'ensemble des nombres premiers* $p \notin S_E$ *tels que* $E(p)$ *soit cyclique a une densité* c_E *que est* > 0.

(De plus, cette densité peut se calculer « galoisiennement » : pour tout nombre premier l, soit K_l l'extension de $\mathbf{Q}$ obtenue par adjonction des coordonnées des points d'ordre l de E, et soit K le composé des K_l ; soit $G = \mathrm{Gal}(K/\mathbf{Q})$, soit H_l le noyau de $G \to \mathrm{Gal}(K_l/\mathbf{Q})$, et soit H la réunion des H_l. On a alors

$$c_E = 1 - \mu(H) \quad \text{(sous GRH)}$$

où μ est la mesure de Haar du groupe profini G, normalisée de telle sorte que $\mu(G) = 1$.)

La démonstration suit de près celle donnée par Hooley (*J. Crelle*, 225, 1967) de la « conjecture d'Artin » relative aux nombres premiers p pour lesquels un entier fixé a est racine primitive. Les corps K_l définis ci-dessus remplacent les corps $\mathbf{Q}(\sqrt[l]{1}, \sqrt[l]{a})$. Le fait que K_l contienne $\mathbf{Q}(\sqrt[l]{1})$ joue un rôle essentiel, car il permet d'appliquer le théorème de Brun-Titchmarsh.

Supposons maintenant que E n'admette *pas de multiplication complexe*. Si l'on pose $G_l = \mathrm{Gal}(K_l/\mathbf{Q})$, on sait que $G_l \simeq \mathbf{GL}_2(\mathbf{Z}/l\mathbf{Z})$ pour tout l assez grand (*Invent. Math.* 15, 1972). Le théorème suivant précise ce résultat :

THÉORÈME 1.2 (sous GRH) - *Il existe une constante absolue* C (indépendante de l et de E) *telle que l'on ait* $G_l \simeq \mathbf{GL}_2(\mathbf{Z}/l\mathbf{Z})$ *pour*

$$l \geqslant C.\log N_E\,(\log\log 2N_E)^2, \qquad \text{où } N_E = \prod_{p \in S_E} p$$

On peut également montrer (toujours — hélas — sous GRH), que le nombre des l tels que G_l ne soit pas isomorphe à $\mathbf{GL}_2(\mathbf{Z}/l\mathbf{Z})$ est $o(\log\log 2N_E)$.

Conservons les notations et hypothèses ci-dessus. Si $p \notin S_E$, posons

$$a_p = 1 + p - \mathrm{Card}.E(p) \quad \text{(« trace de Frobenius »)}.$$

Pour tout nombre réel x, désignons par $N\{p \leqslant x : a_p = 0\}$ le nombre des $p \leqslant x$, n'appartenant pas à S_E, pour lesquels $a_p = 0$.

THÉORÈME 1.3 - (i) *Il existe* $\delta > 0$ (par exemple $\delta = 1/10$) *tel que*

$$N\{p \leqslant x : a_p = 0\} = O(x/\log^{1+\delta} x) \quad \textit{pour } x \to \infty$$

(ii) (sous G.R.H.) *On a* $N\{p \leqslant x : a_p = 0\} = O(x^{3/4})$.

L'assertion (ii) avait été démontrée dans le cours 1976/1977 en admettant, non seulement (GRH), mais encore la conjecture d'Artin (AC) sur l'holomorphie des fonctions L. L'utilisation de certains sous-groupes de $\mathbf{PGL}_2(\mathbf{Z}/l^n\mathbf{Z})$ a permis d'éliminer (AC).

2. *Formes modulaires*

Soit $f = \Sigma\, a_n q^n$ une forme modulaire parabolique de type (k, ε) sur $\Gamma_0(N)$, qui est normalisée ($a_0 = 1$), et fonction propre des opérateurs de Hecke T_p, pour $(p, N) = 1$.

THÉORÈME 2.1 - *Supposons* $k \geqslant 2$, *et* f *sans multiplication complexe* (au sens de Ribet, *Lect. Notes* 601, p. 34). *Alors* :

(i) *Il existe* $\delta > 0$ *tel que*

$$N\{p \leqslant x : a_p = 0\} = O(x/\log^{1+\delta} x) \quad \textit{pour } x \to \infty.$$

(ii) (sous GRH). *On a* $N\{p \leqslant x : a_p = 0\} = O(x^{3/4})$.

Ce théorème, ainsi que le théorème 1.3, est un cas particulier d'un résultat applicable à toute représentation l-adique $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{PGL}_2(\mathbf{Q}_l)$ dont l'image est ouverte.

COROLLAIRE 1 - *On a* $\sum_{a_p = 0} \frac{1}{p} < \infty$.

Cela résulte de (i).

COROLLAIRE 2 - *Les entiers* n *tels que* $a_n \neq 0$ *ont une densité* > 0.

Cela se déduit du cor. 1, et du fait que f est fonction propre des T_p.

Exemple - Prenons $N = 11$, $k = 2$, $\varepsilon = 1$, et

$$f = q \prod_{m=1}^{\infty} (1 - q^m)^2 (1 - q^{11m})^2$$

La densité des n tels que $a_n \neq 0$ est égale à $\frac{14}{15} \prod \left(1 - \frac{1}{p+1}\right)$, le produit étant étendu aux nombres premiers p tels que $a_p = 0$ (i.e. $p = 19$, 29, 199, 569, 809, 1 289, ...) ; d'après le cor. 1, ce produit est convergent.

Du cor. 2, on déduit :

THÉORÈME 2.2 - *Soit* $g = \Sigma\, b_n q^n$ *une forme modulaire de type* (k, ε) *sur* $\Gamma_0(N)$, *avec* $k \geqslant 2$. *Les propriétés suivantes sont équivalentes* :

a) $N\{n \leqslant x : b_n \neq 0\} = o(x)$;

b) $N\{n \leqslant x : b_n \neq 0\} = O(x/\log^{1/2} x)$;

c) g *est combinaison linéaire de formes paraboliques à multiplications complexes.*

COROLLAIRE. *Si* $N = 1$, *la propriété* a) *entraîne* $g = 0$.

J.-P. S.

Séminaire

J. Oesterlé : *Forme explicite du théorème de Čebotarev* (1 exposé) ;

J.-M. Deshouillers : *Cribles : bornes supérieures* (3 exposés).

Publications

J.-P. Serre, *Représentations l-adiques* (*Algebraic Number Theory,* ed. by S. Iyanaga, Japan Soc. for the Prom. of Sci., Tokyo, 1977, p. 177-193).

— *Arbres, amalgames,* SL_2 (rédigé avec la collaboration de Hyman Bass, *Astérisque* n° 46, *Soc. Math. France,* 1977, 189 p.).

— *Une « formule de masse » pour les extensions totalement ramifiées de degré donné d'un corps local* (*C.R. Acad. Sci. Paris,* série A, 286, 1978, p. 1031-1036).

J.-P. Serre et H. Stark, *Modular Forms of Weight* 1/2 (*Lect. Notes in Math.,* n° 627, Springer-Verlag, 1977, p. 29-68).

Édition

J.-P. Serre et D. Zagier, *Modular Forms of One Variable* V (*Lect. Notes in Math.,* n° 601, Springer-Verlag, 1977, 294 p.).

— *Modular Forms of One Variable* VI (*Lect. Notes in Math.,* n° 627, Springer-Verlag, 1977, 339 p.).

Missions

Cours :

— *Arithmetic Groups,* Durham, septembre 1977 ;

— *Number Theory Lectures,* Inst. for Adv. Study, Princeton, février-mars 1978.

Exposés :

— *Elliptic Curves and Modular Forms,* Corvallis, juillet 1977 ;

— *Applications of Analytic Number Theory to Elliptic Curves and Modular Forms,* Oberwolfach, novembre 1977 ; Cambridge, juin 1978 ;

— *Points rationnels des courbes modulaires* $X_0(N)$ (d'après Barry MAZUR), séminaire Bourbaki, Paris, novembre 1977 ;

— *Selberg Upper Bound Sieve : an Introduction,* Princeton University, janvier 1978 ;

— *Circuits in Graphs : an elementary Analogue of Selberg's Zeta Function,* Inst. for Adv. Study, Princeton, février 1978 ;

— *Icosahedral Extensions,* Inst. for Adv. Study, Princeton, avril 1978.

DISTINCTION

Doctorat *honoris causa* de l'Université de Cambridge.