RÉSUMÉ DES COURS
DE L'ANNÉE SCOLAIRE 1974 - 1975

I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, professeur

Le cours a été consacré aux *formes modulaires de poids* 1 et aux *représentations galoisiennes de degré* 2 qui leur correspondent. Il a comporté deux parties. La première a exposé des théorèmes généraux, obtenus en collaboration avec P. Deligne, qui figurent dans un travail paru en 1974 aux Annales Sci. ENS (cité DS dans ce qui suit). La seconde a illustré ces théorèmes par des exemples, dus pour la plupart à J. Tate.

1. *Théorèmes généraux*

Il s'agit de mettre en correspondance les deux types d'objets que voici :

(i) *Systèmes de valeurs propres* (a_p) des opérateurs de Hecke T_p agissant sur les *formes modulaires paraboliques de poids* 1 sur les sous-groupes de congruence de $\mathbf{SL}_2(\mathbf{Z})$.

(ii) *Représentations continues irréductibles* (donc à image finie)

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{C})$$

à déterminant impair, i.e. telles que $\det \rho(c) = -1$, où c est la conjugaison complexe.

On dit que (a_p) et ρ *se correspondent* si, pour presque tout nombre premier p, on a $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p$.

Le principal résultat de DS est :

THÉORÈME 1. — *A tout système* (a_p) *de type* (i) *correspond une représentation* ρ *de type* (ii).

Le théorème de densité de Čebotarev montre qu'une telle représentation ρ est unique, à isomorphisme près. De plus cette représentation jouit des propriétés suivantes (cf. DS) :

(iii) Pour tout caractère continu χ de degré 1 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, la fonction L d'Artin $L(s, \rho \otimes \chi)$ est *holomorphe* dans tout le plan complexe ; en d'autres termes la *conjecture d'Artin* est vraie pour ρ ainsi que pour toutes ses « tordues » $\rho \otimes \chi$.

(iv) Soit N le plus petit entier ≥ 1 tels que (a_p) soit le système de valeurs propres associé à une forme parabolique f sur le sous-groupe $\Gamma_1(N)$ de $\mathbf{SL}_2(\mathbf{Z})$, et soit ε le caractère correspondant de $(\mathbf{Z}/N\mathbf{Z})^*$; identifions comme d'habitude ε à un caractère de degré 1 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On a alors $\det(\rho) = \varepsilon$, et le *conducteur d'Artin* de ρ est égal à N. Si de plus f est normalisée de telle sorte que

$$f = \sum_{n=1}^{\infty} a_n q^n \quad \text{avec} \quad a_1 = 1 \quad (\text{où} \quad q = e^{2\pi i z}),$$

la fonction L d'Artin $L(s, \rho)$ est égale à $\Sigma\, a_n n^{-s}$.

D'après un résultat général de Langlands et Weil, le théorème 1 admet la réciproque suivante :

THÉORÈME 2. — *Toute représentation galoisienne* ρ *qui satisfait à* (ii) *et* (iii) *correspond à un système de valeurs propres* (a_p) *de type* (i).

La *démonstration du théorème* 1 a été exposée en détail. Elle comporte les étapes suivantes :

a) Construction de *représentations « modulaires »* de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ correspondant à un système (a_p) de type (i).

Il s'agit de représentations

$$\varrho_l : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(k_l)$$

où k_l est un corps fini de caractéristique l arbitraire, telles que, pour presque tout $p \neq l$, l'image de a_p dans k_l soit égale à $\mathrm{Tr}(\varrho_l(\mathrm{Frob}_p))$. Si (a_p) était réalisable par une forme parabolique de poids $k \geqslant 2$, l'existence des ϱ_l résulterait directement des théorèmes généraux démontrés par Deligne il y a quelques années (l'hypothèse $k \geqslant 2$ intervenant par le fait que l'on prend la cohomologie de la puissance symétrique $(k - 2)$-ième d'un certain faisceau) ; on se ramène à ce cas en multipliant la forme f de poids 1 considérée par une forme E de poids $k - 1 \geqslant 1$ telle que $E \equiv 1 \pmod{l}$, cf. DS, § 6. (On peut même, comme l'a observé Shimura, prendre pour E une série d'Eisenstein de poids 1 ; on est ainsi ramené au cas $k = 2$, où l'on peut utiliser, à la place des résultats cohomologiques de Deligne, ceux, plus élémentaires, d'Eichler et Shimura, où interviennent simplement les « modules de Tate » des courbes modulaires.)

b) Existence d'une infinité de valeurs de l telles que l'image G_l de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ par ϱ_l soit un *petit* sous-groupe de $\mathbf{GL}_2(\mathbf{Z}/l\mathbf{Z})$, i.e. un sous-groupe dont l'ordre reste borné quand l varie.

C'est le point le plus délicat (cf. DS, §§ 7-8). On utilise d'abord une *majoration en moyenne* des a_p, que l'on obtient par une méthode due à Rankin, cf. DS, § 5. On en déduit que la plus grande partie (en un sens facile à préciser) des traces des éléments de G_l appartiennent à un ensemble qui est petit (i.e. d'ordre borné) ; le fait que G_l lui-même soit petit résulte facilement de là, compte tenu de la liste des sous-groupes de $\mathbf{GL}_2(\mathbf{Z}/l\mathbf{Z})$, cf. DS, § 7.

c) *Relèvement* des ϱ_l en caractéristique zéro.

Les G_l de b) sont d'ordre borné, donc aussi d'ordre premier à l pourvu que l soit assez grand. Les représentations ϱ_l correspondantes se relèvent en caractéristique zéro ; la démonstration du théorème 1 s'achève en montrant que l'on peut prendre comme représentation ϱ l'un de ces relèvements, cf. DS, § 8.

Le théorème 1 a diverses conséquences. Par exemple, si $f = \Sigma a_n q^n$ est une forme modulaire de poids 1, non identiquement nulle, on a

(v) $|a_n| = O(\sigma_0(n))$ pour $n \to \infty$,

(vi) $\limsup \log|a_n|\log\log n/\log n = \log 2$

et en particulier

$$|a_n| = o(n^\delta) \qquad \text{quel que soit } \delta > 0.$$

De plus, si $M(x)$ désigne le nombre des entiers positifs $n \leq x$ tels que $a_n \neq 0$, il existe $\alpha > 0$ tel que

(vii) $M(x) = o(x/\log^\alpha x)$ pour $x \to \infty$,

d'où

(viii) $M(x) = o(x)$ pour $x \to \infty$,

ce qui signifie que « presque tous » les a_n sont nuls.

Ces résultats peuvent d'ailleurs être généralisés ; ainsi (vi) s'applique aux coefficients de la série L d'une représentation quelconque ρ de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, à condition de remplacer log 2 par log deg(ρ) ; quant à (vii) et (viii), ils s'étendent aux coefficients des formes modulaires de poids quelconque, réduits modulo un entier ≥ 1 donné. (Ces résultats, seulement esquissés dans le cours, ont été exposés avec plus de détails dans le séminaire Delange-Pisot-Poitou.)

2. *Exemples*

Posons $\mathbf{PGL}_2(\mathbf{C}) = \mathbf{GL}_2(\mathbf{C})/\mathbf{C}^*$. Si ρ est une représentation irréductible (continue) de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathbf{GL}_2(\mathbf{C})$, notons $\tilde{\rho}$ la représentation correspondante de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathbf{PGL}_2(\mathbf{C})$. La connaissance de $\tilde{\rho}$ est « presque » équivalente à celle de ρ. De façon plus précise, Tate a démontré les résultats suivants :

a) toute représentation $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{PGL}_2(\mathbf{C})$ se relève en une représentation ρ à valeurs dans $\mathbf{GL}_2(\mathbf{C})$; les autres relèvements de $\tilde{\rho}$ sont les $\rho \otimes \chi$ où χ est un caractère de degré 1 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$; pour que ρ satisfasse à la condition (ii) du n° 1 (i.e. pour que $\det(\rho)$ soit impair), il faut et il suffit que $\tilde{\rho}(c) \neq 1$;

b) il existe un relèvement ρ de $\tilde{\rho}$ dont le conducteur N divise les conducteurs de tous les relèvements de ρ ; on dit que N est le *conducteur* de $\tilde{\rho}$; l'exposant d'un nombre premier p dans N ne dépend que de la restriction de $\tilde{\rho}$ au groupe de décomposition en p (c'est un invariant *local* : pour le calculer, on peut passer au corps p-adique $\mathbf{Q}_p$) ;

c) pour qu'un nombre premier p divise N, il faut et il suffit que $\tilde{\varrho}$ soit ramifié en p ; lorsque la ramification de $\tilde{\varrho}$ est modérée, l'exposant de p dans N est 1 ou 2 suivant que l'image par $\tilde{\varrho}$ du groupe de décomposition en p est ou non cyclique.

L'avantage de $\mathbf{PGL}_2(\mathbf{C})$ est que ses sous-groupes finis ont une structure très simple : ils sont cycliques, diédraux, ou isomorphes à l'un des groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$ (groupe du tétraèdre, du cube, de l'icosaèdre). Si ϱ est irréductible, le groupe $\mathrm{Im}(\tilde{\varrho})$ n'est pas cyclique, donc est soit *diédral,* soit *isomorphe à* $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$. Le cas diédral est celui où ϱ est induite par une représentation de degré 1 d'un sous-groupe d'indice 2 ; les formes paraboliques correspondantes sont combinaisons linéaires de *séries thêta* relativement à des formes quadratiques binaires ; elles sont bien connues depuis les travaux de Hecke.

Le cas nouveau est le cas *non diédral,* dont l'étude vient d'être abordée par Tate. Le cours a résumé quelques-uns de ses résultats :

d) lorsque le conducteur N de ϱ est un nombre *premier,* on a $N \not\equiv 1 \pmod 8$. Lorsque $N \equiv 5 \pmod 8$, $\det(\varrho)$ est d'ordre 4, et $\tilde{\varrho}$ est de type $\mathfrak{S}_4$; la plus petite valeur possible de N est $N = 229$, qui correspond à deux représentations non isomorphes. Lorsque $N \equiv 3$ ou $7 \pmod 8$, $\det(\varrho)$ est d'ordre 2 (c'est le caractère de Legendre mod. N), et $\tilde{\varrho}$ est de type $\mathfrak{S}_4$ ou de type $\mathfrak{A}_5$; pour le type $\mathfrak{S}_4$, les plus petites valeurs possibles de N sont $N = 283, 331, 491, 563$; on ignore ce qu'il en est pour le type $\mathfrak{A}_5$.

e) Il existe une représentation $\tilde{\varrho}$ de conducteur $N = 133 = 7.19$ de type $\mathfrak{A}_4$. L'extension K de $\mathbf{Q}$ correspondant au groupe de Galois $\mathrm{Im}(\tilde{\varrho}) \simeq \mathfrak{A}_4$ s'obtient de la manière suivante : si z est une racine primitive 19^e de l'unité, on pose :

$$a = z + z^7 + z^8 + z^{11} + z^{12} + z^{18}$$
$$b = z^2 + z^3 + z^5 + z^{14} + z^{16} + z^{17} = 4 - a^2$$
$$c = z^4 + z^6 + z^9 + z^{10} + z^{13} + z^{15} = 4 - b^2,$$

de sorte que a,b,c sont les trois racines de l'équation $x^3 + x^2 - 6x - 7 = 0$, cf. Gauss, *Disq. Arithm.,* art. 343 et 351 ; le corps $k = \mathbf{Q}(a)$ est une extension cubique cyclique de $\mathbf{Q}$, et K est l'extension biquadratique de k engendrée par $\sqrt{ab}$ *et* $\sqrt{bc}$. De plus — et c'est ce qui fait l'intérêt de cet exemple — la

représentation ϱ ainsi construite *correspond à un système* (a_p) de type (i) : cela a été démontré par Tate (aidé par Atkin ainsi que par des étudiants de Harvard) grâce à la construction explicite de certaines formes paraboliques de poids 1. Il en résulte en particulier que *la conjecture d'Artin est vraie pour* ϱ ainsi que pour les $\varrho \otimes \chi$, cf. (iii).

Séminaire

B. Mazur, *Points rationnels sur les courbes modulaires* $X_0(N)$ (2 exposés).

E. Bombieri, *Le crible analytique* (2 exposés).

Publications

H. Bass, J. Milnor et J.-P. Serre, *On a functorial property of power residue symbols* (*Publ. Math. I.H.E.S.*, n° 44, 1975, p. 241-244).

P. Deligne et J.-P. Serre, *Formes modulaires de poids* 1 (*Ann. Sci. E.N.S.*, 4e série, 7, 1974, p. 507-530).

J.-P. Serre, *Fonctions zêta p-adiques* (*Bull. Soc. Math. France*, Mémoire 37, 1974, p. 157-160).

— *Amalgames et points fixes* (Proc. Int. Conf. Theory of Groups, *Lect. Notes in Math.*, n° 372, Springer, 1974, p. 633-640).

— *Divisibilité des coefficients des formes modulaires de poids entier* (*C.R. Acad. Sci. Paris*, série A, 279, 1974, p. 679-682).

Missions

Cours :

— *Problems on l-adic representations*, Summer Institute on Algebraic Geometry, Arcata, Californie, août 1974 ;

— *Finite groups*, Harvard University, septembre-décembre 1974.

Exposés :

— *Arithmétique et géométrie sur les courbes elliptiques,* conférence du soir du Collège de France, juin 1974 ;

— *Finite subgroups of Chevalley groups over* **Z**, Northeastern University, Boston, octobre 1974 ;

— *Recent results on modular forms,* Yale University, novembre 1974 ; Institute for Advanced Study, Princeton, décembre 1974 ;

— *Modular forms modulo p,* Harvard University, novembre-décembre 1974 ;

— *Cohomology of arithmetic groups,* Harvard University, novembre 1974 ;

— *Trees,* Harvard University, novembre 1974 ;

— *Tits buildings and Steinberg representations,* Harvard University, décembre 1974 ;

— *Divisibilité des coefficients de formes modulaires,* Séminaire Delange-Pisot-Poitou, Paris, avril 1975 ;

— *Séries linéaires et théorème de Riemann-Roch sur les courbes algébriques,* Bordeaux, avril 1975 ;

— *Formes modulaires de poids* 1 *et représentations de groupes de Galois,* Grenoble, mai 1975 ;

— *Modular forms and Galois groups,* London Mathematical Society, mai 1975 ;

— (avec M. MAZUR), *Points rationnels sur les courbes modulaires* $X_0(N)$, Séminaire Bourbaki, Paris, juin 1975 ;

— *Lower bounds for discriminants of number fields,* Arbeitstagung, Bonn, juin 1975.