RÉSUMÉ DES COURS
DE L'ANNÉE SCOLAIRE 1975-1976

I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, professeur

Le cours a été consacré aux systèmes de représentations l-adiques. Il a complété des cours antérieurs (1965/66, 1967/68, 1970/71), et passé en revue les quelques *résultats* obtenus depuis, et les nombreux *problèmes* qui restent ouverts.

1. *Systèmes de représentations l-adiques*

Soient K un corps de nombres algébriques, $\bar{K}$ une clôture algébrique de K, et G le groupe de Galois de $\bar{K}$ sur K. On s'intéresse aux systèmes de représentations l-adiques (ϱ_l) du type suivant :

a) pour chaque nombre premier l, ϱ_l est un homomorphisme continu de G dans le groupe $\mathrm{Aut}(V_l)$ des automorphismes d'un $\mathbf{Q}_l$-espace vectoriel V_l de dimension finie ;

b) il existe un ensemble fini S de places de K tel que, si $v \notin S$, et si l est distinct de la caractéristique résiduelle p_v de v, alors ϱ_l est non ramifiée en v, et le polynôme caractéristique de l'élément de Frobenius $\varrho_l(\mathrm{Frob}_v)$ est à coefficients dans $\mathbf{Q}$, et ne dépend pas de l.

La condition de compatibilité b) assure que, si l'on connaît ϱ_l pour *un* l, on connaît, sinon tous les ϱ_l, du moins tous leurs semi-simplifiés.

2. *Systèmes fournis par la cohomologie*

Soient X une K-variété projective non singulière, et $\overline{X}$ la $\bar{K}$-variété déduite de X par extension du corps de base à $\bar{K}$. Soit $m \in \mathbf{Z}$. Posons $V_l = H^m(\overline{X} ; \mathbf{Q}_l)$, m-ième groupe de cohomologie l-adique de $\overline{X}$, au sens de Grothendieck-Artin ; c'est un $\mathbf{Q}_l$-espace vectoriel de dimension égale au m-ième nombre de Betti de X. Le groupe G opère par transport de structure sur V_l ; on en déduit une représentation l-adique $\varrho_l : G \to \mathrm{Aut}(V_l)$. D'après un théorème de Deligne (1973), le système (ϱ_l) possède la propriété b) du n° 1 ; on peut prendre pour ensemble exceptionnel S l'ensemble des places de K en lesquelles X a mauvaise réduction.

Lorsque $m = 1$, ce système est dual de celui défini par les modules de Tate de la variété d'Albanese de X ; c'est le cas étudié initialement par Taniyama (1957).

Revenons au cas général, et soit G_l l'image de ϱ_l ; c'est un sous-groupe de Lie du groupe l-adique $\mathrm{Aut}(V_l)$; son algèbre de Lie $\mathfrak{g}_l$ est une sous-algèbre de $\mathrm{End}(V_l)$. On sait très peu de choses sur les $\mathfrak{g}_l$; on ignore même si leur dimension est indépendante de l. Voici quelques résultats élémentaires :

i) Supposons que les $\varrho_l(\mathrm{Frob}_v)$, pour $v \notin S$, $p_v \neq l$, soient semi-simples, ce qui est le cas pour $m = 1$ (on conjecture que c'est vrai pour tout m). Alors $\mathfrak{g}_l$ est scindable, et ses sous-algèbres de Cartan sont commutatives, et formées d'éléments semi-simples (cf. *Bourbaki,* LIE VII).

ii) Si $m \neq 0$, l'enveloppe algébrique $\bar{\mathfrak{g}}_l$ de $\mathfrak{g}_l$ contient les homothéties. (On conjecture que $\bar{\mathfrak{g}}_l = \mathfrak{g}_l$, cf. n° 3.)

Comme Deligne l'a observé, ceci entraîne :

iii) On a $H^i(\mathfrak{g}_l, V_l) = 0$ pour tout $i \neq 0$ (et même pour $i = 0$ si $m \neq 0$).

Le même résultat vaut pour les espaces tensoriels $T^r V_l \otimes T^s V_l^*$, avec $r \neq s$.

Le cas $i = 1$, $m = 1$ a la conséquence suivante (*Izv. Akad. Nauk S.S.S.R.*, 35, 1971) : si A est une variété abélienne sur K, tout sous-groupe d'indice fini de A(K) est un groupe de congruence.

3. *Relations avec les groupes de Hodge : conjectures*

Choisissons un plongement de $\bar{K}$ dans **C**, et soit $X_{\mathbf{C}}$ la variété complexe déduite de X par le changement de base $\bar{K} \to \mathbf{C}$. On peut parler de la cohomologie entière, rationnelle, complexe, ... de $X_{\mathbf{C}}$. Posons :

$$V_0 = H^m(X_{\mathbf{C}}; \mathbf{Q}) \quad \text{et} \quad V_{\mathbf{C}} = \mathbf{C} \otimes V_0 = H^m(X_{\mathbf{C}}; \mathbf{C}).$$

On a :

$$V_l = \mathbf{Q}_l \otimes V_0 \text{ pour tout } l.$$

La bigraduation de $V_{\mathbf{C}}$ fournie par la théorie de Hodge définit une action de $\mathbf{C}^* \times \mathbf{C}^*$ sur $V_{\mathbf{C}}$, d'ou un sous-tore de $\mathbf{GL}(V_{\mathbf{C}})$. Le *groupe de Hodge* $\mathrm{Hdg} = \mathrm{Hdg}_{m,X}$ est le plus petit **Q**-sous-groupe algébrique de $\mathbf{GL}(V_0)$ dont le groupe des **C**-points contienne le tore en question. C'est un groupe réductif connexe. Il a été défini par Mumford-Tate, et étudié en détail dans la thèse de Saavedra (*Lect. Notes*, 265, Springer, 1972). Lorsque m et X varient, les $\mathrm{Hdg}_{m,X}$ forment de manière naturelle un système projectif, dont la limite Hdg_K est un groupe pro-algébrique.

Soit $\mathfrak{h} = \mathfrak{h}_{m,X}$ l'algèbre de Lie de $\mathrm{Hdg}_{m,X}$; on a $\mathfrak{h} \subset \mathrm{End}(V_0)$. On conjecture :

i) *l'algèbre de Lie* $\mathfrak{g}_l$ *du groupe de Galois* G_l *est égale à* $\mathbf{Q}_l \otimes \mathfrak{h}$, ce qui entraîne en particulier que $\mathfrak{g}_l$ est algébrique, réductive dans $\mathrm{End}(V_l)$, et de dimension indépendante de l.

Une formulation équivalente de i) est :

i') les groupes G_l et $\mathrm{Hdg}_{m,X}(\mathbf{Q}_l)$ sont *commensurables* : leur intersection est ouverte dans chacun d'eux.

Ces conjectures sont liées à celles de Hodge et Tate sur les classes de cohomologie « algébriques » :

ii) si la conjecture de Hodge est vraie, on a $\mathfrak{g}_l \subset \mathbf{Q}_l \otimes \mathfrak{h}$;

iii) si la conjecture de Tate est vraie, et si $\mathfrak{g}_l$ est algébrique et réductive dans $\mathrm{End}(V_l)$, on a $\mathfrak{g}_l \supset \mathbf{Q}_l \otimes \mathfrak{h}$.

Variante adélique

Quitte à faire une extension finie de K, il doit être vrai que chacune des ϱ_l applique le groupe de Galois G dans $\mathrm{Hdg}_{m,X}(\mathbf{Q}_l)$. Posons $\mathbf{A}^f = \mathbf{Q} \otimes \hat{\mathbf{Z}}$, anneau des adèles finis de $\mathbf{Q}$. La famille des ϱ_l définit un homomorphisme continu :

$$\varrho : G \to \mathrm{Hdg}_{m,X}(\mathbf{A}^f).$$

Il est naturel de conjecturer *l'équivalence* des propriétés suivantes :

a) $\varrho(G)$ est un sous-groupe *ouvert* de $\mathrm{Hdg}_{m,X}(\mathbf{A}^f)$;

b) pour presque tout l, $\varrho_l(G)$ est un sous-groupe *compact maximal* de $\mathrm{Hdg}_{m,X}(\mathbf{Q}_l)$;

c) le noyau de la projection canonique $\mathrm{Hdg}_K \to \mathrm{Hdg}_{m,X}$ est *connexe.*

4. *Relations avec les groupes de Hodge : résultats*

Ces résultats sont peu nombreux, et concernent presque exclusivement le cas où X est une variété abélienne, l'entier m étant égal à 1. On a alors :

a) (Piatetskii-Šapiro, Deligne) - L'algèbre $\mathfrak{g}_l$ est contenue dans $\mathbf{Q}_l \otimes \mathfrak{h}$.

Du point de vue galoisien, tout se passe donc comme si la conjecture de Hodge était vraie pour les variétés abéliennes.

b) (Shimura, Taniyama, Weil) - On a $\mathfrak{g}_l = \mathbf{Q}_l \otimes \mathfrak{h}$ si X est de type CM (multiplication complexe).

La situation dans ce cas est particulièrement favorable : on connaît la représentation $\varrho = (\varrho_l)$ de G, et l'on connaît aussi le groupe Hdg_K rendu abélien (c'est la limite projective des tores T_m définis dans mon cours à McGill de 1967).

Signalons que, même dans ce cas, il n'est pas toujours vrai que $\varrho(G)$ soit ouvert dans le groupe adélique $\mathrm{Hdg}(\mathbf{A}^f)$: la jacobienne de la courbe $y^2 = 1 - x^{23}$ fournit un contre-exemple.

c) Si X est une courbe elliptique sans multiplication complexe, on a $\mathrm{Hdg} = \mathbf{GL}(V_0)$, $\mathfrak{g}_l = \mathbf{Q}_l \otimes \mathfrak{h} = \mathrm{End}(V_l)$, et $\varrho(G)$ est ouvert dans le groupe adélique $\mathrm{Hdg}(\mathbf{A}^f) \simeq \mathbf{GL}_2(\mathbf{A}^f)$.

La démonstration repose sur une étude détaillée des groupes G_l et $\varrho(G)$, qui avait été exposée dans le cours de 1970/71 et publiée dans *Invent. Math.* 15 (1972) ; on s'est borné à la résumer. Elle comporte deux étapes :

i) montrer que, si les groupes de Galois en question sont « trop petits », ils sont « presque abéliens » (cela provient de ce que $\mathbf{GL}_2$ est de rang-semi-simple 1) ; ii) montrer que, si ces groupes sont « presque abéliens », la courbe a des multiplications complexes (cela peut se faire de diverses façons, par exemple en relevant en caractéristique zéro certaines multiplications complexes de caractéristique p).

d) (« Fausses courbes elliptiques », cf. Ohta et Jacobson) - On suppose que dim.X = 2, et que End(X) est un ordre d'un corps de quaternions D de centre $\mathbf{Q}$. On a alors les mêmes résultats que dans le cas c), le groupe Hdg étant, non plus $\mathbf{GL}_2$, mais le groupe multiplicatif D* de D.

e) On peut également traiter dans certains cas (mais pas dans tous, cf. n° 5) les *produits de courbes elliptiques*, et les variétés abéliennes analogues à ces produits (Ribet, Nakamura).

En dehors de ces cas de dimension 1, il n'y a guère à signaler que celui de la cohomologie des variétés de Fermat

$$X_0^n + \ldots + X_r^n = 0,$$

où le groupe Hdg est commutatif, ce qui permet une analyse des (ϱ_l) analogue à celle de b) (Weil, Deligne).

5. *Courbes elliptiques*

Ce cas pose de nombreux problèmes. Notamment :

a) *Effectivité*

Soit E une courbe elliptique sans multiplication complexe, et soit $\varrho : G \to \prod_l \mathbf{GL}_2(\mathbf{Z}_l)$ la représentation de G donnée par les points d'ordre fini de E. D'après ce qui a été dit plus haut (n° 4 c), $\varrho(G)$ est un sous-groupe ouvert de $\prod \mathbf{GL}_2(\mathbf{Z}_l)$. Peut-on déterminer ce groupe de façon *effective* ? En particulier, peut-on expliciter un entier N_E tel que, pour tout $l > N_E$, l'homomorphisme $\varrho_l : G \to \mathbf{GL}_2(\mathbf{Z}_l)$ soit surjectif ?

Ce problème semble abordable ; l'outil principal devrait être la forme effective du théorème de densité de Čebotarev démontrée récemment par Lagarias-Odlyzko, et qui fera l'objet du cours de 1976/77.

b) *Uniformité*

Avec les notations de a), peut-on choisir l'entier N_E *indépendant de* E (dépendant donc seulement de K) ? Par exemple, pour $K = \mathbf{Q}$, peut-on prendre $N_E = 37$? C'est là une question bien plus optimiste que a). On

peut la reformuler ainsi : notons X_l la courbe modulaire associée au sous-groupe de Borel de $\mathbf{GL}_2(\mathbf{F}_l)$, et Y_l (resp. Z_l) celle qui est associée à un normalisateur de sous-groupe de Cartan déployé (resp. non déployé) de $\mathbf{GL}_2(\mathbf{F}_l)$. Est-il vrai qu'il existe un entier M ne dépendant que de K tel que, pour tout $l > M$, les courbes X_l, Y_l et Z_l n'aient pas d'autres K-points que ceux correspondant aux « pointes » et aux courbes elliptiques à multiplication complexe ? On ne sait presque rien sur ce genre de question, mis à part le cas des X_l pour $K = \mathbf{Q}$, étudié en détail par Ogg, Mazur, Brumer, ...

c) *Isogénies*

Soient E et E′ deux courbes elliptiques dont les systèmes de représentations l-adiques sont isomorphes. Est-il vrai que E et E′ sont *isogènes* ? On ne le sait que lorsque l'invariant modulaire de l'une des deux courbes n'est pas un entier algébrique. Le cas général résulterait de l'assertion de finitude suivante :

(*) Pour tout corps de nombres K, et tout ensemble fini S de places de K, il n'existe qu'un nombre fini de courbes de genre 2 sur K dont les jacobiennes aient bonne réduction en dehors de S.

L'énoncé analogue sur les corps de fonctions a été démontré par Paršin et Zarkin.

d) *Distribution des éléments de Frobenius*

Soit E une courbe sans multiplication complexe sur le corps $K = \mathbf{Q}$; soit S l'ensemble des nombres premiers en lesquels E a mauvaise réduction. Si $p \notin S$, on peut parler de l'endomorphisme de Frobenius π_p de la réduction de E modulo p ; on a $\det(\pi_p) = p$; posons $\mathrm{Tr}(\pi_p) = a_p$. On peut se poser diverses questions sur la variation de a_p avec p, par exemple celle-ci :

Soit F un polynôme non nul en deux variables, sur un corps de caractéristique zéro, et soit P_F l'ensemble des nombres premiers $p \notin S$ tels que $F(p, a_p) = 0$. On montre facilement que P_F est de densité zéro : si $P_F(x)$ désigne le nombre des $p \leqslant x$ qui appartiennent à P_F, on a

$$P_F(x) = o(x/\log x) \qquad \text{pour } x \to \infty.$$

De combien peut-on améliorer cette estimation ? Est-il vrai, par exemple, que $P_F(x) = O(x^{1/2})$? Si l'hypothèse de Riemann généralisée est vraie, on peut déduire du théorème de Lagarias-Odlyzko cité en a) que $P_F(x) = O(x^\alpha)$ pour tout $\alpha > 7/8$. Le cas où F est de la forme $a_p + c$ a été étudié, au point de vue numérique et heuristique, par Lang et Trotter (*Lect. Notes* 504, Springer, 1976) ; on conjecture que $P_F(x)$ est alors de l'ordre de grandeur

de $x^{1/2}/\log x$ (à moins, bien sûr, qu'il n'existe une relation de congruence sur a_p impliquant que $a_p \neq -c$ pour presque tout p, auquel cas $P_F(x)$ est borné).

6. *Problèmes locaux*

Pour étudier une représentation l-adique, il est précieux d'avoir des renseignements sur l'action du groupe d'inertie en une place de caractéristique résiduelle l. Après changement de base (et remplacement de l par p) cela amène à la situation suivante :

le corps K est maintenant un corps complet pour une valuation discrète à corps résiduel algébriquement clos de caractéristique p ; on suppose K de caractéristique zéro. Si $\bar{K}$ est une clôture algébrique de K, on s'intéresse à une représentation p-adique

$$\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(V),$$

où V est un $\mathbf{Q}_p$-espace vectoriel de dimension finie. On peut prendre par exemple pour V un groupe de cohomologie $H^m(\overline{X}\,;\,\mathbf{Q}_p)$, cf. n° 2.

Soit C le complété de $\bar{K}$. Tate a montré en 1966 que, dans certains cas (appelés maintenant « de Hodge-Tate »), le module galoisien $V_C = C \otimes V$ admet une graduation analogue à celle de Hodge dans le cas complexe. Pour un tel module, on peut définir (comme au n° 3) un groupe de Hodge Hdg_V, qui est un sous-groupe algébrique connexe de $\mathbf{GL}(V)$; en outre, d'après un résultat de Sen (*Ann. of Math.* 97, 1973), l'algèbre de Lie du groupe $\mathrm{Im}(\rho)$ est *égale* à celle du groupe Hdg_V ; de ce point de vue, la situation est meilleure que dans le cas global du n° 3. Toutefois :

a) On ignore si les modules galoisiens $H^m(\overline{X}\,;\,\mathbf{Q}_p)$ provenant de la cohomologie d'une variété projective non singulière sont des modules de Hodge-Tate. C'est vrai pour $m = 1$, d'après un théorème de Tate (complété par Raynaud) ; pour $m = 2$, il y a des résultats partiels d'Artin-Mazur (à paraître aux *Ann. Sci. E.N.S.*).

b) On se sait presque rien sur la structure de Hdg_V, même lorsque ce groupe est réductif. On ne sait même pas quels sont les types de groupes simples qui peuvent intervenir : A_n, B_n, ..., E_7, E_8 ? On manque fâcheusement d'exemples.

Séminaire

Pierre Deligne (3 exposés) : *Périodes des motifs de type CM* ;

Barry Mazur (2 exposés) : *Groupe de Brauer formel et décompositions de Hodge p-adiques* ;

Michel Raynaud (2 exposés) : *Travaux de Shankar Sen.*

Missions

Exposés :

— *Lower bounds for discriminants of number fields,* King's College, Londres, novembre 1975 ;

— *Arithmétique et géométrie sur les courbes elliptiques,* Marseille, novembre 1975 ;

— *l-adic representations revisited,* Kyoto, mars 1976 ;

— *Majorations de sommes exponentielles* (*d'après Deligne*), Journées arithmétiques, Caen, mai 1976 ;

— *Représentations linéaires des groupes finis « algébriques »* (*d'après Deligne-Lusztig*), Séminaire Bourbaki, Paris, juin 1976.