I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

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

Le cours a continué celui de l'année précédente, consacré aux représentations ℓ-adiques associées aux variétés abéliennes. Il s'est surtout attaché à la « variation avec ℓ » des groupes de Galois considérés.

1. *Notations*

K est une extension finie de $\mathbf{Q}$, de clôture algébrique $\overline{\mathrm{K}}$; on note $\mathrm{G_K}$ le groupe de Galois $\mathrm{Gal}\,(\overline{\mathrm{K}}/\mathrm{K})$.

A est une variété abélienne sur K, de dimension $n \geqslant 1$.

Pour tout nombre premier ℓ, T_ℓ est le module de Tate de A relativement à ℓ ; c'est un $\mathbf{Z}_\ell$-module libre de rang $2n$. Le groupe $\mathrm{G_K}$ opère sur T_ℓ par une représentation

$$\rho_\ell : \mathrm{G_K} \to \mathrm{Aut}\,(\mathrm{T}_\ell) \simeq \mathbf{GL}_{2n}(\mathbf{Z}_\ell).$$

L'image de cette représentation est notée $\mathrm{G}_{\mathrm{K},\ell}$; le groupe $\mathrm{G}_{\mathrm{K},\ell}$ est le groupe de Galois des « points de ℓ^∞-division » de A.

La famille des ρ_ℓ, pour ℓ premier, définit un homomorphisme

$$\rho : \mathrm{G_K} \to \prod_\ell \mathrm{G}_{\mathrm{K},\ell} \subset \prod_\ell \mathrm{Aut}\,(\mathrm{T}_\ell).$$

Le groupe $\rho(\mathrm{G_K})$ est le groupe de Galois des points de torsion de A.

2. *Résultats*

2.1. *Indépendance des* ρ_ℓ

Disons que les représentations ρ_ℓ sont *indépendantes sur* K si l'homomorphisme $\rho : G_K \to \prod_\ell G_{K,\ell}$ est *surjectif*, i.e. si $\rho(G_K)$ est égal au produit des $G_{K,\ell}$.

THÉORÈME 1 - *Il existe une extension finie* K′ *de* K *telle que les* ρ_ℓ *soient indépendantes sur* K′.

(Bien entendu, K′ dépend de la variété abélienne A considérée.)

Ce résultat peut se reformuler de la manière suivante :

THÉORÈME 1′ - *Si* K *est assez grand,* $\rho(G_K)$ *est un sous-groupe ouvert du produit des* $G_{K,\ell}$.

2.2. *Homothéties*

On sait (BOGOMOLOV) que $G_{K,\ell}$ contient un sous-groupe ouvert du groupe $\mathbf{Z}_\ell^*$ des homothéties. Notons $c(\ell)$ l'indice de $\mathbf{Z}_\ell^* \cap G_{K,\ell}$ dans $\mathbf{Z}_\ell^*$. D'après une conjecture de S. Lang, on devrait avoir $c(\ell) = 1$ pour ℓ assez grand. On peut prouver le résultat plus faible suivant (d'ailleurs suffisant pour les applications que Lang avait en vue) :

THÉORÈME 2 - *Les entiers* $c(\ell)$ *restent bornés quand* ℓ *varie.*

Vu le th. 1, ce résultat équivaut à :

THÉORÈME 2′ - *Il existe un entier* $c \geqslant 1$ *tel que le groupe* $\rho(G_K)$ *contienne toutes les homothéties de* $\hat{\mathbf{Z}}^* = \prod_\ell \mathbf{Z}_\ell^*$ *qui sont des puissances c-ièmes.*

Une autre façon d'énoncer le th. 2′ consiste à dire qu'il existe un entier $c \geqslant 1$ ayant la propriété suivante :

pour tout entier $m \geqslant 1$, *il existe* $s_m \in G_K$ *tel que* $s_m(x) = m^c x$ *pour tout* $x \in A(\overline{K})$ *d'ordre fini premier à m.*

2.3. *Comparaison avec le groupe des similitudes symplectiques*

Choisissons une polarisation e sur A, ce qui munit chacun des T_ℓ d'une forme alternée e_ℓ à discriminant $\neq 0$ (et même à discriminant inversible, si ℓ est assez grand). Le groupe de Galois $G_{K,\ell}$ est contenu dans le groupe $\mathbf{GSp}(T_\ell, e_\ell)$ des similitudes symplectiques de T_ℓ relativement à e_ℓ.

THÉORÈME 3 - *Faisons les hypothèses suivantes* :

(i) *L'anneau* End (A) *des* $\overline{K}$*-endomorphismes de* A *est réduit à* **Z** ;

(ii) *La dimension* n *de* A *est impaire, ou égale à* 2, *ou à* 6.

Alors $G_{K,\ell}$ *est ouvert dans* $\mathbf{GSp}(T_\ell,e_\ell)$ *pour tout* ℓ, *et est égal à* $\mathbf{GSp}(T_\ell,e_\ell)$ *pour tout* ℓ *assez grand.*

En combinant ce résultat avec le th.1, on obtient :

COROLLAIRE - *Si* (i) *et* (ii) *sont satisfaites,* $\rho(G_K)$ *est un sous-groupe ouvert du produit des* $\mathbf{GSp}(T_\ell,e_\ell)$.

Pour $n = 1$, cela revient à dire que $\rho(G_K)$ est ouvert dans le produit des $\mathbf{GL}(T_\ell)$: on retrouve une propriété des courbes elliptiques sans multiplications complexes qui avait fait l'objet du cours de 1970-1971 (voir aussi *Invent. Math.* 15 (1972), 259-331).

2.4. *Orbites des points de torsion de* A

Soit $A(\overline{K})_t$ le sous-groupe de torsion de $A(\overline{K})$. Si $x \in A(\overline{K})_t$, posons :

$N(x)$ = ordre de x ;

$d(x) = |G_K \cdot x|$ = nombre de conjugués de x sur K.

THÉORÈME 4 - *Supposons que* A *ne contienne aucune sous-variété abélienne* $\neq 0$ *de type* CM. *Alors, pour tout* $\epsilon > 0$, *il existe une constante* $C(\epsilon,A,K) > 0$ *telle que* :

$$d(x) \geqslant C(\epsilon,A,K)\cdot N(x)^{2-\epsilon} \quad \textit{pour tout } x \in A(\overline{K})_t.$$

Lorsque A contient une sous-variété abélienne $\neq 0$ de type CM, cet énoncé reste vrai à condition d'y remplacer l'exposant $2 - \epsilon$ par $1 - \epsilon$: cela résulte du th. 2'.

2.5. *Groupes de Galois des points de division par* ℓ

Soit $G_K(\ell)$ l'image de $G_{K,\ell}$ dans $\mathbf{GL}(T_\ell/\ell T_\ell) \simeq \mathbf{GL}_{2n}(\mathbf{F}_\ell)$ par réduction modulo ℓ. L'un des principaux résultats du cours a été de montrer que $G_K(\ell)$ est « presque algébrique ». De façon plus précise, on construit, pour tout ℓ assez grand, un *sous-groupe réductif connexe* H_ℓ de $\mathbf{GL}_{2n}$, défini sur $\mathbf{F}_\ell$, qui jouit des propriétés suivantes :

2.5.1. Quitte à remplacer K par une extension finie, $G_K(\ell)$ est contenu dans $H_\ell(\mathbf{F}_\ell)$, et son indice est borné quand ℓ varie. Pour ℓ assez grand, $G_K(\ell)$ contient le groupe dérivé de $H_\ell(\mathbf{F}_\ell)$.

2.5.2. Le rang de H_ℓ est indépendant de ℓ, et est égal au rang de l'algèbre de Lie du groupe ℓ-adique $G_{K,\ell}$.

2.5.3. La composante neutre du centre de H_ℓ est un tore « indépendant de ℓ » : il s'obtient par réduction (mod ℓ) à partir d'un tore défini sur $\mathbf{Q}$. Ce tore contient le groupe $\mathbf{G}_m$ des homothéties.

2.5.4. La représentation linéaire de degré $2n$ de H_ℓ définie par le plongement $H_\ell \to \mathbf{GL}_{2n}$ est semi-simple ; son commutant est $\mathbf{F}_\ell \otimes \mathrm{End}\,(A)$.

Remarque. Il devrait être possible de préciser (2.5.2) et (2.5.3) en montrant que H_ℓ est la réduction (mod ℓ) de la composante neutre $(G_\ell^{alg})^\circ$ de l'enveloppe algébrique du groupe ℓ-adique $G_{K,\ell}$ (du moins pour ℓ assez grand). Cela n'a pas été fait dans le cours.

3. *Ingrédients des démonstrations*

Il y a d'abord ceux déjà utilisés dans l'étude ℓ-adique, pour ℓ fixé : théorèmes de Faltings, tores de Frobenius, théorie abélienne, et propriétés des groupes d'inertie en les places de K divisant ℓ.

On a également besoin de renseignements sur les sous-groupes de $\mathbf{GL}_N(\mathbf{F}_\ell)$:

3.1. *Sous-groupes d'ordre premier à la caractéristique*

Si k est un corps, *tout sous-groupe fini de* $\mathbf{GL}_N(k)$, *d'ordre premier à la caractéristique de* k, *contient un sous-groupe abélien d'indice* $\leqslant c_1(N)$, où $c_1(N)$ ne dépend que de N. C'est là un théorème classique de C. Jordan (du moins lorsque $k = \mathbf{C}$, cas auquel on se ramène sans difficulté). On a reproduit la démonstration qu'en avait donnée FROBENIUS en 1911 (*Ges. Abh.*, III, n^{os} 87-88). Cette démonstration donne pour $\log c_1(N)$ une majoration de l'ordre de $N^2 \log N$; d'après un résultat récent de B. WEISFEILER (basé sur la classification des groupes finis simples) on peut remplacer $N^2 \log N$ par $N \log N$, ce qui est essentiellement optimal.

3.2. *Sous-groupes de* $\mathbf{GL}_N(\mathbf{F}_\ell)$ *engendrés par leurs éléments d'ordre* ℓ

Supposons $\ell \geqslant N$. Soit G un sous-groupe de $\mathbf{GL}_N(\mathbf{F}_\ell)$, soit G_u l'ensemble des éléments de G d'ordre ℓ, et soit G^+ le sous-groupe de G engendré par G_u (ou, ce qui revient au même, le plus petit sous-groupe normal de G d'indice premier à ℓ). Si $x \in G_u$, on peut écrire x sous la forme $\exp(X)$, avec $X^\ell = 0$; les $\exp(tX)$ forment un sous-groupe algébrique $\mathbf{G}_a(x)$ de $\mathbf{GL}_N$, défini sur $\mathbf{F}_\ell$, et isomorphe au groupe additif $\mathbf{G}_a$. Soit G^{alg} le sous-groupe algébrique de $\mathbf{GL}_N$ engendré par les $\mathbf{G}_a(x)$, pour $x \in G_u$. Le groupe $G^{alg}(\mathbf{F}_\ell)$ des $\mathbf{F}_\ell$-points de G^{alg} contient évidemment G^+ ; *d'après un théorème de V. Nori, on a* :

$$G^+ = G^{alg}(\mathbf{F}_\ell)^+ \quad \textit{si } \ell \geqslant c_2(N)$$

où $c_2(N)$ ne dépend que de N. Ce résultat est particulièrement utile lorsque G agit de façon semi-simple sur $\mathbf{F}_\ell^N$, car le groupe G^{alg} est alors semi-simple, et peut se relever en caractéristique 0 si $c_2(N)$ est bien choisi.

On applique ceci avec $N = 2n$, le groupe G étant le groupe de Galois $G_K(\ell)$. D'après un théorème de Faltings, l'action de ce groupe sur $\mathbf{F}_\ell^N$ est semi-simple si ℓ est assez grand, d'où d'après (3.2) un groupe semi-simple $G_K(\ell)^{alg}$. D'autre part, la théorie abélienne permet de définir un certain sous-tore de $\mathbf{GL}_N$ qui commute à $G_K(\ell)^{alg}$; le groupe réductif connexe H_ℓ engendré par ce tore et par $G_K(\ell)^{alg}$ est celui qui intervient dans (2.5). Une fois le groupe H_ℓ défini, il faut prouver qu'il a les propriétés (2.5.1) à (2.5.4). En fait, c'est (2.5.1) qui est le point essentiel ; on le traite en utilisant les théorèmes de Jordan et de Nori cités ci-dessus, ainsi que le théorème de structure des groupes d'inertie en les places de K divisant ℓ dû à Raynaud. De là, on passe aux théorèmes 1, 2, 3 et 4.

PUBLICATIONS

J.-P. SERRE, *Sur la lacunarité des puissances de* η (*Glasgow Math. J.*, 27, 1985, p. 203-221).

— *Œuvres - Collected Papers* (3 vol., Springer-Verlag, 1986, 2089 p.).

— $\Delta = b^2 - 4ac$ (exposé rédigé par D. FLATH, *Math. Medley*, Singapore Math. Soc. 13, 1985, p. 1-10).

MISSIONS

Cours

— *Curves over Finite Fields*, Harvard, septembre-décembre 1985.

Exposés

— *La fondation Claude-Antoine Peccot*, Colloque de Mathématiques (exposé d'introduction), Collège de France, septembre 1985 ;

— *ℓ-adic representations*, Harvard, décembre 1985 (3 exposés) ; McGill, décembre 1985 (2 exposés) ;

— *Weil + epsilon* $\Longrightarrow$ *Fermat*, McGill, décembre 1985 ;

— *Représentations modulaires de* Gal $(\overline{\mathbf{Q}}/\mathbf{Q})$, séminaire de théorie des nombres, Paris, février 1986 ; Bordeaux, mai 1986 ; Luminy, juin 1986 (3 exposés) ;

— *Le problème de Waring pour les bicarrés, d'après R. Balasubramanian, J.-M. Deshouillers et F. Dress*, Académie des Sciences, mai 1986 ;

— *Extensions de* $\mathbf{Q}$ *à groupe de Galois donné,* Genève, mai 1986 ;

— *Une démonstration topologique du théorème d'induction de Brauer, d'après V. Snaith*, Genève, mai 1986 ;

— *Galois representations, modular forms and Fermat equations*, Cambridge, juin 1986.

Distinction

Prix Balzan, Berne, novembre 1985.