I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

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

Les résultats récents de G. FALTINGS (*Invent. Math.* 73 (1983), 349-366) permettent de comprendre un peu mieux les propriétés des représentations ℓ-adiques, notamment dans le cas des variétés abéliennes. Le cours en a exploré deux aspects :

1) critère effectif permettant de reconnaître l'isomorphisme de deux représentations ;

2) détermination des enveloppes algébriques des groupes de Galois ℓ-adiques.

Un troisième aspect, celui de la « variation des groupes de Galois avec ℓ » fera l'objet du cours de 1985-1986.

1. *Critère effectif d'isomorphisme. Corps quartiques et isogénies*

1.1. *Le groupe déviation* $\tilde{G}$ (FALTINGS, *loc. cit.*, § 6)

Soient $\rho_1 : G \to \mathbf{GL}(V_1)$ et $\rho_2 : G \to \mathbf{GL}(V_2)$ deux représentations linéaires d'un groupe G dans des $\mathbf{Q}_\ell$-espaces vectoriels V_1 et V_2 de dimension $d < \infty$. Supposons que, pour $i = 1, 2$, ρ_i soit semi-simple et que $\rho_i(G)$ laisse stable un $\mathbf{Z}_\ell$-réseau de V_i. Soit $\mathrm{Tr}\,\rho_i$ le caractère de ρ_i. Les fonctions $\mathrm{Tr}\,\rho_1$ et $\mathrm{Tr}\,\rho_2$ sont

à valeurs dans $\mathbf{Z}_\ell$. Supposons que ces fonctions soient distinctes, i.e. que ρ_1 et ρ_2 ne soient *pas isomorphes*. Soit ℓ^α la plus grande puissance de ℓ telle que :

$$\operatorname{Tr} \rho_2(s) \equiv \operatorname{Tr} \rho_1(s) \pmod{\ell^\alpha} \quad \text{pour tout } s \in G.$$

Notons M la sous-$\mathbf{Z}_\ell$-algèbre de $\operatorname{End}(V_1) \times \operatorname{End}(V_2)$ engendrée par les $(\rho_1(s), \rho_2(s))$ pour $s \in G$. Si $m = (m_1, m_2)$ est un élément de M, posons :

$$\theta(m) = \ell^{-\alpha}(\operatorname{Tr}(m_2) - \operatorname{Tr}(m_1)).$$

La forme linéaire $\theta : M \to \mathbf{Z}_\ell$ est surjective. Par réduction (mod ℓ) elle définit une forme linéaire non nulle :

$$t : M/\ell M \to \mathbf{Z}/\ell\mathbf{Z}.$$

Si s est un élément de G, et $\tilde{s}$ son image dans $M/\ell M$, on a :

$$t(\tilde{s}) \equiv \ell^{-\alpha}(\operatorname{Tr} \rho_2(s) - \operatorname{Tr} \rho_1(s)) \pmod{\ell}.$$

On notera $\tilde{G}$ le sous-groupe de $(M/\ell M)^*$ formé des $\tilde{s}$, pour s parcourant G. C'est un quotient fini de G, d'ordre $< \ell^{2d^2}$. Le couple formé par $\tilde{G}$ et l'application $t : \tilde{G} \to \mathbf{Z}/\ell\mathbf{Z}$ mesure en quelque sorte la « *déviation* » entre ρ_2 et ρ_1. L'intérêt de $(\tilde{G}, t)$ est que c'est un objet « fini » (alors que G lui-même, en pratique, est infini). Cela permet souvent de dresser la liste des $(\tilde{G}, t)$ possibles sans connaître ρ_1 ni ρ_2 (ni α). Supposons par exemple que cette liste soit formée de :

$$(\tilde{G}_1, t_1), \ldots, (\tilde{G}_h, t_h).$$

Pour tout j $(1 \leqslant j \leqslant h)$, on peut alors choisir un élément $s_j \in G$ tel que $t_j(\tilde{s}_j) \neq 0$. L'ensemble $\{s_1, \ldots, s_h\}$ ainsi obtenu jouit de la propriété suivante :

(1) *Si* $\operatorname{Tr} \rho_2(s_j) = \operatorname{Tr} \rho_1(s_j)$ *pour* $j = 1, \ldots, h$, *les représentations* ρ_1 *et* ρ_2 *sont isomorphes* (i.e. l'égalité des caractères de ρ_1 et ρ_2 peut se tester sur $\{s_1, \ldots, s_h\}$.

Sinon, en effet, il existerait un indice j tel que le couple $(\tilde{G}, t)$ associé à (ρ_1, ρ_2) soit isomorphe à $(\tilde{G}_j, t_j)$, ce qui entraînerait :

$$\operatorname{Tr} \rho_2(s_j) \not\equiv \operatorname{Tr} \rho_1(s_j) \pmod{\ell^{\alpha+1}},$$

et contredirait l'hypothèse faite.

1.2. *Le cas* $\ell = d = 2$

Supposons que $\ell = 2$ et $d = 2$, de sorte que l'on puisse réaliser ρ_1 et ρ_2 comme des représentations de G dans $\mathbf{GL}_2(\mathbf{Z}_2)$. Faisons les hypothèses suivantes :

(i) $\det \rho_2 = \det \rho_1$;

(ii) les deux homomorphismes de G dans $\mathbf{GL}_2(\mathbf{Z}/2\mathbf{Z}) = \mathfrak{S}_3$, obtenus en réduisant ρ_1 et ρ_2 modulo 2, sont surjectifs et coïncident.

On peut alors déterminer $(\tilde{G}, t)$. On trouve que $\tilde{G}$ *est isomorphe, soit à* $\mathfrak{S}_4 \times \{\pm 1\}$, *soit à* $\mathfrak{S}_4$, *soit à* $\mathfrak{S}_3 \times \{\pm 1\}$, *et que* $t : \tilde{G} \to \mathbf{Z}/2\mathbf{Z}$ *vaut* 0 *sur les éléments de* $\tilde{G}$ *d'ordre* $\leqslant 3$, *et* 1 *sur les autres.*

1.3. *Courbes elliptiques*

Soient E_1 et E_2 deux courbes elliptiques sur **Q.** Soit S un ensemble fini de nombres premiers tel que $2 \in S$ et que les E_i aient bonne réduction en dehors de S. Soit $G = G_S$ le groupe de Galois de la plus grande extension algébrique de **Q** non ramifiée en dehors de S, et soient ρ_1 et ρ_2 les représentations 2-adiques de G associées à E_1 et E_2. Supposons que les points d'ordre 2 de E_i $(i = 1, 2)$ engendrent une extension K de **Q**, de groupe de Galois $\mathfrak{S}_3$, qui soit indépendante de i.

Toutes les conditions du n° 1.2 sont alors satisfaites. Si ρ_1 et ρ_2 ne sont pas isomorphes (i.e., d'après FALTINGS, si E_1 et E_2 ne sont pas **Q**-isogènes), on en déduit un groupe déviation $\tilde{G}$ de type $\mathfrak{S}_4 \times \{\pm 1\}$, $\mathfrak{S}_4$ ou $\mathfrak{S}_3 \times \{\pm 1\}$, d'où une extension galoisienne $\tilde{K}/\mathbf{Q}$ contenant K et de groupe de Galois $\tilde{G}$. Connaissant S, on peut déterminer explicitement les extensions $\tilde{K}/\mathbf{Q}$ qui sont *a priori* possibles : cela se fait, soit par la théorie du corps de classes, soit par des méthodes de géométrie des nombres. Si $\tilde{K}_1, \ldots, \tilde{K}_h$ désignent les extensions en question, on choisit pour tout $j = 1, \ldots, h$ un nombre premier p_j dont la substitution de Frobenius $\tilde{s}_j$ dans $\tilde{K}_j/\mathbf{Q}$ est d'ordre > 3. On peut alors appliquer le critère (1) du n° 1.1, et l'on en déduit :

(2) *Pour que les courbes* E_1 *et* E_2 *soient isogènes sur* **Q**, *il suffit que les traces des endomorphismes de Frobenius de* E_1 *et* E_2 *soient les mêmes pour les nombres premiers* $p_1, \ldots, p_h$.

(Ou, de façon plus concrète : il suffit que E_1 et E_2 aient le même nombre de points modulo $p_1, \ldots, p_h$.)

1.4. *Exemples d'applications du critère* (2)

(a) *Le cas de* 5077

Ce cas a été traité par J.-F. MESTRE (*C.R. Acad. Sci. Paris,* 300 (1985), 509-512). Les deux courbes E_1 et E_2 dont on veut prouver l'isogénie ont pour conducteur le nombre premier 5077. La première est l'unique « courbe de Weil » de ce conducteur. La seconde est définie par l'équation

$$y^2 + y = x^3 - 7x + 6.$$

Toutes deux ont bonne réduction supersingulière en 2, la trace de l'endomorphisme de Frobenius étant -2. De là, et d'un résultat de HONDA-HILL, on déduit que, si ces courbes ne sont pas isogènes, le groupe $\tilde{G}$ qui leur est associé est de type $\mathfrak{S}_4$ et le corps $\tilde{K}$ correspondant est non ramifié sur K. Or on constate qu'il n'y a que trois corps $\tilde{K}_1, \tilde{K}_2, \tilde{K}_3$ ayant ces propriétés, et que

l'on peut prendre pour p_1, p_2, p_3 les nombres premiers 5, 5 et 11. Comme les traces des endomorphismes de Frobenius de E_1 et E_2 sont les mêmes en 5 et en 11, on en déduit bien que E_1 *et* E_2 *sont isogènes* (donc, en fait, isomorphes).

(b) *Le cas de* 11

Il s'agit de prouver que *toute courbe elliptique sur* **Q** *de conducteur* 11 *est isogène à la courbe* $y^2 - y = x^3 - x^2$, résultat déjà démontré par M. AGRAWAL, J. COATES, D. HUNT et A. van der POORTEN, par des calculs sur machine, utilisant la théorie de BAKER. On applique pour cela le critère (2), en prenant pour E_1 la courbe donnée de conducteur 11, et pour E_2 celle des trois courbes de WEIL de conducteur 11 ou 11^2 qui a même réduction en 2 que E_1. On montre comme ci-dessus que le groupe $\tilde{G}$ associé à E_1 et E_2 (supposées non isogènes) est de type $\mathfrak{S}_4$ et que l'extension $\tilde{K}/K$ correspondante n'est ramifiée qu'au-dessus de 11. Or on vérifie facilement qu'une telle extension n'existe pas (son discriminant contredirait les bornes d'ODLYZKO). D'où l'isogénie de E_1 et E_2, et l'on en déduit aussitôt le résultat cherché.

2. *Représentations l-adiques attachées aux variétés abéliennes*

2.1. *Notations*

K est une extension de type fini de **Q** ;

$\overline{K}$ est une clôture algébrique de K ;

G_K est le groupe de Galois Gal $(\overline{K}/K)$;

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

ℓ est un nombre premier ;

$T_\ell = T_\ell(A)$ est le module de Tate de A relativement à ℓ ; c'est un $\mathbf{Z}_\ell$-module libre de rang $2n$;

$V_\ell = \mathbf{Q} \otimes T_\ell$; c'est un $\mathbf{Q}_\ell$-espace vectoriel de dimension $2n$, sur lequel opère G_K ;

$\rho_\ell : G_K \to \mathrm{Aut}\,(V_\ell)$ est la représentation ℓ-adique correspondante ;

G_ℓ est l'image de ρ_ℓ ; c'est un sous-groupe compact de Aut (V_ℓ) ;

$\mathfrak{g}_\ell$ est l'algèbre de Lie de G_ℓ ; on a $\mathfrak{g}_\ell \subset \mathrm{End}\,(V_\ell)$;

G_ℓ^{alg} est l'adhérence de G_ℓ pour la topologie de Zariski ; c'est un $\mathbf{Q}_\ell$-sous-groupe algébrique du groupe linéaire $\mathbf{GL}_{V_\ell} \simeq \mathbf{GL}_{2n}$.

2.2. *Structure de* G_ℓ^{alg}

2.2.1. (BOGOMOLOV). *Le groupe* G_ℓ *est un sous-groupe ouvert* (pour la topologie ℓ-adique) *du groupe des* $\mathbf{Q}_\ell$*-points de* G_ℓ^{alg}.

Ce résultat peut aussi se formuler en disant que l'algèbre de Lie du groupe G_ℓ^{alg} est égale à $\mathfrak{g}_\ell$, ou encore que $\mathfrak{g}_\ell$ est une sous-algèbre *algébrique* de End (V_ℓ).

2.2.2. (FALTINGS). *Le groupe* G_ℓ^{alg} *est réductif, et son commutant dans* End (V_ℓ) *est égal à* $\mathbf{Q}_\ell \otimes \mathrm{End}_K(A)$. En particulier, $\mathfrak{g}_\ell$ est une algèbre de Lie réductive, de commutant égal à $\mathbf{Q}_\ell \otimes$ End (A).

On conjecture que G_ℓ^{alg} est « indépendant de ℓ » (pour A et K fixés), et plus précisément que sa composante neutre $(G_\ell^{alg})^\circ$ se déduit du « groupe de Mumford-Tate » par extension des scalaires de $\mathbf{Q}$ à $\mathbf{Q}_\ell$. L'un des buts du cours a été de démontrer un certain nombre de résultats partiels dans cette direction :

2.2.3. *Le groupe fini* $G_\ell^{alg}/(G_\ell^{alg})^\circ$ *est indépendant de* ℓ. De façon plus précise, le noyau de l'homomorphisme surjectif

$$G_K \to G_\ell \to G_\ell^{alg}/(G_\ell^{alg})^\circ$$

est indépendant de ℓ.

2.2.4. *Le rang de* G_ℓ^{alg} (dimension d'un sous-tore maximal) *est indépendant de* ℓ.

Ecrivons le groupe réductif connexe $(G_\ell^{alg})^\circ$ sous forme standard :

$$(G_\ell^{alg})^\circ = C_\ell \cdot S_\ell$$

où C_ℓ est un tore central (composante neutre du centre), et S_ℓ un groupe semi-simple (groupe dérivé). On a sur C_ℓ et S_ℓ les renseignements suivants :

2.2.5. (BOGOMOLOV). *Le groupe* C_ℓ *est indépendant de* ℓ, en ce sens qu'il provient par extension des scalaires d'un sous-tore de $\mathbf{GL}_{2n}$ défini sur $\mathbf{Q}$; *il contient le groupe* $\mathbf{G}_m$ *des homothéties.*

2.2.6. (FALTINGS). *On a* $C_\ell = \mathbf{G}_m$ *si* End (A) = $\mathbf{Z}$. *On a* $S_\ell = \{1\}$ *si et seulement si* A *est de type CM.*

Toute polarisation de A munit V_ℓ d'une forme alternée non dégénérée qui est invariante, à un facteur près, par l'action de G_K. On en conclut que G_ℓ^{alg} est contenu dans le groupe $\mathbf{G}_m \cdot \mathbf{Sp}_{2n}$ des *similitudes symplectiques,* et en particulier que l'on a $S_\ell \subset \mathbf{Sp}_{2n}$. On s'intéresse au cas où il y a égalité. Tout d'abord :

2.2.7. *Les propriétés suivantes sont équivalentes* :

(a) $S_\ell = \mathbf{Sp}_{2n}$ *pour un* ℓ ;

(b) $S_\ell = \mathbf{Sp}_{2n}$ *pour tout* ℓ ;

(c) End (A) = $\mathbf{Z}$ *et* rang $(G_\ell^{alg}) = 1 + n$.

[Dans le cours de 1985-1986, on montrera que ces propriétés entraînent la suivante :

(d) *L'image de* $G_K \to \prod_\ell (\mathbf{G}_m \cdot \mathbf{Sp}_{2n})(\mathbf{Q}_\ell)$ *est ouverte pour la topologie adélique.*]

La propriété End (A) = **Z**, à elle seule, n'est pas suffisante pour entraîner (a), (b), (c) : il existe un contre-exemple de MUMFORD pour $n = 4$. On peut toutefois démontrer le résultat suivant :

2.2.8. *Supposons que* End (A) = **Z** *et que n soit impair* (ou $n = 2$, ou $n = 6$). *Alors les propriétés* (a), (b), (c) *ci-dessus sont vraies ; on a*

$$G_\ell^{alg} = \mathbf{G}_m \cdot \mathbf{Sp}_{2n}$$

pour tout ℓ.

(Un énoncé analogue avait déjà été démontré par K. RIBET pour le groupe de MUMFORD-TATE.)

2.3. *Indications sur les démonstrations*

Au moyen du théorème d'irréductibilité de Hilbert, on se ramène au cas où le corps de base K est un corps de nombres algébriques. On dispose alors de trois types de renseignements sur les G_ℓ et les G_ℓ^{alg} :

(i) la théorie générale des représentations ℓ-adiques abéliennes, appliquée à une puissance extérieure convenable de V_ℓ, permet d'étudier le groupe C_ℓ (tout comme dans le cas des variétés abéliennes de type *CM*) ;

(ii) les groupes d'inertie en les places de K divisant ℓ fournissent des sous-tores à 1 paramètre de G_ℓ^{alg} (définis sur une extension convenable de $\mathbf{Q}_\ell$) qui n'ont que deux poids, le poids « 0 » et le poids « 1 », avec multiplicité n chacun ; de tels sous-tores restreignent considérablement la structure du groupe S_ℓ ;

(iii) les places de K ne divisant pas ℓ, et où A a bonne réduction, donnent des « tores de Frobenius » qui sont essentiellement indépendants de ℓ, et ont des propriétés très particulières (dues notamment aux pentes des polygones de Newton, comme l'a remarqué Y. ZARHIN).

En combinant ces informations à 2.2.2. (FALTINGS), on prouve 2.2.1., 2.2.3., 2.2.4. et 2.2.7. La démonstration de 2.2.8. est plus délicate ; elle utilise notamment la classification des représentations « minuscules » des groupes simples.

Signalons également que certains des résultats ci-dessus (par exemple 2.2.2., 2.2.3., 2.2.4., 2.2.5. et 2.2.7.) sont vrais lorsque le corps de base K est une extension de type fini d'un corps fini.

Séminaires

D. Bertrand, *Variétés abéliennes, groupes de Galois et transcendance* (2 exposés).

Publications

J.-P. Serre, *Autour du théorème de Mordell-Weil,* I *et* II, notes de cours rédigées par Michel Waldschmidt, Publ. Math. Univ. Paris VI, 2 vol., 1984, 176 p. + 202 p.

— *L'invariant de Witt de la forme* Tr (x^2), Comm. Math. Helv. 59 (1984), 651-676.

Missions

Exposés

— *ℓ-adic representations,* Düsseldorf, septembre 1984 ;

— *Corps quartiques et isogénies de courbes elliptiques,* Bordeaux, novembre 1984 ;

— *Courbes elliptiques sur* **Q**, Genève, janvier 1985 ;

— **C** *est algébriquement clos,* E.N.S.J.F., Montrouge, janvier 1985 ;

— *Curves over finite fields* (2 exposés), Singapour, février 1985 ;

— *On Faltings' proof of Mordell conjecture,* Singapour, février 1985 ;

— *The Ramanujan function*, Singapour, février 1985 ;

— $\Delta = b^2 - 4ac$, Singapour, février 1985 ;

— *Curves of genus two*, Brighton, février 1985 ;

— *Subgroups of* $\mathbf{GL}_n(\mathbf{F}_p)$, Queen Mary College, Londres, février 1985 ;

— *Nombres de points des courbes algébriques sur les corps finis* (3 exposés), Les Plans-sur-Bex, mars 1985 ;

— « 5077 », Harvard, mai 1985 ;

— *Sur la lacunarité des puissances de êta,* Bordeaux, mai 1985 ;

— *On the quadratic forms of type* Tr (x^2), Oberwolfach, juin 1985 ;

— *Propriétés galoisiennes des points d'ordre fini des variétés abéliennes*, Besançon, juin 1985.