Algèbre et géométrie

M. Jean-Pierre SERRE, professeur

Soit E une courbe elliptique définie sur un corps de nombres K, et munie d'un point rationnel 0, pris comme origine. Soit $\bar{K}$ une clôture algébrique de K, et soit G le groupe de Galois de $\bar{K}/K$. Soit E_t le sous-groupe de torsion du groupe $E(\bar{K})$ des points de E rationnels sur $\bar{K}$; le groupe E_t est isomorphe à $\mathbf{Q}/\mathbf{Z} \oplus \mathbf{Q}/\mathbf{Z}$ et son groupe d'automorphismes $\mathrm{Aut}(E_t)$ est isomorphe à $\prod_{l \in P} \mathbf{GL}_2(\mathbf{Z}_l)$, où P désigne l'ensemble des nombres premiers, et où $\mathbf{Z}_l$ est l'anneau des entiers l-adiques. Le groupe G opère sur E_t, ce qui définit un homomorphisme continu $\varphi : G \to \mathrm{Aut}(E_t)$.

Le but principal du cours a été la démonstration du résultat suivant :

THÉORÈME 1. *Supposons que la courbe elliptique* E *n'ait pas de multiplication complexe. Alors* $\varphi(G)$ *est un sous-groupe* ouvert (*donc d'indice fini*) *du groupe compact* $\mathrm{Aut}(E_t) \simeq \prod_{l \in P} \mathbf{GL}_2(\mathbf{Z}_l)$.

Notons $\varphi_l : G \to \mathbf{GL}_2(\mathbf{Z}_l)$ la l-ième composante de φ ; elle indique comment G opère sur la composante l-primaire de E_t. Posons $G_l = \varphi_l(G)$; c'est un sous-groupe fermé de $\mathbf{GL}_2(\mathbf{Z}_l)$. Le théorème 1 équivaut à la conjonction des deux assertions suivantes :

(1) *Pour tout* l, G_l *est un sous-groupe ouvert de* $\mathbf{GL}_2(\mathbf{Z}_l)$.

(2) *Pour presque tout* l (i.e. tout l sauf un nombre fini), *le groupe* $\varphi(G)$ *contient le* l*-ième facteur* $\mathbf{GL}_2(\mathbf{Z}_l)$ *de* $\mathrm{Aut}(E_t)$.

L'assertion (1) avait déjà été démontrée dans le cours de 1965/1966, et sa démonstration se trouve dans « *Abelian l-adic representations and elliptic curves* » (notes rédigées avec la collaboration de W. KUYK et J. LABUTE, publiées par W. A. Benjamin, New York, 1968). Le résultat nouveau est (2), qui entraîne :

(3) *Pour presque tout* l, *on a* $G_l = \mathbf{GL}_2(\mathbf{Z}_l)$.

En particulier, si $\tilde{G}_l$ désigne l'image de G_l dans $\mathbf{GL}_2(\mathbf{F}_l)$ par réduction modulo l, on a :

(4) *Pour presque tout l, le groupe $\tilde{G}_l$ est égal à* $\mathbf{GL}_2(\mathbf{F}_l)$.

(Noter que $\tilde{G}_l$ est le groupe de Galois de l'extension K_l de K obtenue en adjoignant à K les coordonnées des points d'ordre l de la courbe elliptique E ; l'assertion (4) équivaut donc à dire que $[K_l:K] = l(l-1)(l^2-1)$ pour presque tout l.)

En fait, il n'est pas difficile de montrer que (2), (3) et (4) sont *équivalents*. Tout revient donc à prouver (4), c'est-à-dire à montrer que $\tilde{G}_l$ est « aussi gros » que possible.

Les *groupes d'inertie* en l fournissent un premier renseignement sur $\tilde{G}_l$. Plus précisément, soit v une place de K dont la caractéristique résiduelle p_v est égale à l ; supposons que v soit non ramifiée sur $\mathbf{Q}$, et que la courbe E ait bonne réduction (ou mauvaise réduction de type multiplicatif) en v. Soit I_v le groupe d'inertie de G relativement à une place de $\bar{K}$ prolongeant v. Une étude locale montre que l'image de I_v dans $\tilde{G}_l$ contient un groupe de l'un des types suivants :

(i) (« demi-sous-groupe de Cartan déployé ») Un groupe cyclique d'ordre $l-1$, représentable matriciellement sous la forme $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$.

(ii) (« sous-groupe de Cartan non déployé ») Un groupe cyclique d'ordre l^2-1.

Le cas (i) est celui où E a bonne réduction de hauteur 1 en v (ou mauvaise réduction de type multiplicatif, à la Tate) ; le cas (ii) est celui où E a bonne réduction de hauteur 2. De plus, les *caractères* de I_v définis par $I_v \to \tilde{G}_l \subset \mathbf{GL}_2(\mathbf{F}_l)$ sont, dans le cas (i), le caractère unité et le caractère fondamental $I_v \to \mathbf{F}_l^*$ de hauteur 1, et dans le cas (ii), les deux caractères fondamentaux $I_v \to \mathbf{F}_{l^2}^*$ de hauteur 2.

On peut faire la liste des sous-groupes de $\mathbf{GL}_2(\mathbf{F}_l)$ contenant un sous-groupe de type (i) ou de type (ii). On en déduit en particulier que, si (4) est en défaut, on peut trouver un ensemble infini L de nombres premiers tel que, pour tout $l \in L$, on ait l'une des situations suivantes :

(a) $\tilde{G}_l$ est contenu dans un sous-groupe de Cartan, ou dans un sous-groupe de Borel ;

(b) $\tilde{G}_l$ est contenu dans le normalisateur N d'un sous-groupe de Cartan H, mais n'est pas contenu dans H.

Dans le cas (b), le groupe $H \cap \tilde{G}_l$ est d'indice 2 dans $\tilde{G}_l$, donc définit une extension quadratique K'_l de K, contenue dans K_l. On peut montrer que les extensions K'_l/K ainsi obtenues sont *non ramifiées* en dehors d'un ensemble fini de places de K, qui ne dépend pas de l. Ces extensions

sont donc en nombre fini, et leur composé K′ est de degré fini sur K. En remplaçant K par K′, *on est ainsi ramené au cas* (a). Soit alors

$$\tilde{\varphi}_l : G \to \mathbf{GL}_2(\mathbf{F}_l),\ l \in L,$$

la représentation de degré 2 de G déduite par « semi-simplification » de la représentation $G \to \tilde{G}_l \subset \mathbf{GL}_2(\mathbf{F}_l)$. Les $(\tilde{\varphi}_l)_{l\in L}$ sont *abéliennes*, et ont les deux propriétés suivantes :

— (« *Rationalité des éléments de Frobenius* ») Pour presque toute place v de K, il existe un polynôme $P_v \in \mathbf{Z}[T]$ tel que, si $l \in L$ est distinct de p_v, $\tilde{\varphi}_l$ est non ramifiée en v, et l'élément de Frobenius correspondant de $\tilde{\varphi}_l(G)$ a pour polynôme caractéristique la réduction modulo l de P_v.

— (« *Caractères bornés* ») Il existe un entier N tel que, pour tout $l \in L$ et toute place v de K telle que $p_v = l$, la représentation du groupe d'inertie I_v fournie par $\tilde{\varphi}_l$ ne fasse intervenir que des produits des caractères fondamentaux $I_v \to \mathbf{F}_{l^m}^*$ affectés d'exposants au plus égaux à N en valeur absolue.

Vu la théorie du corps de classes, on peut interpréter les $\tilde{\varphi}_l$ comme des représentations du groupe des *classes d'idèles* de K. Cela permet de montrer que le système $(\tilde{\varphi}_l)_{l\in L}$ provient par réduction modulo l du système de représentations l-adiques $(\varrho_l)_{l\in P}$ associé à une représentation $\varrho : S_{\mathfrak{m}} \to \mathbf{GL}_2$ d'un certain groupe agébrique $S_{\mathfrak{m}}$ (défini dans le cours de 1965/1966, cf. « *Abelian l-adic representations...* », chap. II). On en déduit alors que, pour tout $l \in P$, la semi-simplifiée de $\varphi_l : G \to \mathbf{GL}_2(\mathbf{Q}_l)$ est isomorphe à ϱ_l, donc abélienne ; vu les résultats rappelés au début, cela montre que E a de la multiplication complexe, d'où le théorème 1.

Exemples numériques

(Dans ces exemples, on a $K = \mathbf{Q}$; on définit la courbe E comme cubique non singulière du plan projectif, et l'on donne son équation ; on note N le *conducteur* de E, au sens de WEIL.)

$y^2 - y = x^3 - x^2$ (N = 11) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour $l \neq 5$;

$y^2 + xy + y = x^3 - x$ (N = 14) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour $l \neq 2,3$;

$y^2 + xy + y = x^3 - x^2 - 3x + 3$ (N = 26) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour $l \neq 7$;

$y^2 + y = x^3 - x$ (N = 37) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour tout l ;

$y^2 + xy + y = x^3 - x^2$ (N = 53) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour tout l ;

$y^2 = x^3 - 2x^2 - x$ (N = 2^7) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour $l \neq 2$;

$y^2 + xy = x^3 + x^2 - 2x - 7$ (N = 11^2) : $\tilde{G}_l = \mathbf{GL}_2(\mathbf{F}_l)$ pour $l \neq 11$.

Compléments

L'assertion (2) peut être précisée de la manière suivante :

THÉORÈME 2. *Pour toute place ultramétrique v de* K, *notons* J_v *le sous-groupe distingué fermé de* G *engendré par les sous-groupes d'inertie des places de* $\bar{K}$ *prolongeant v. Pour presque tout v, l'image de* J_v *par* $\varphi : G \to \mathrm{Aut}(E_t)$ *est égale au l-ième facteur* $\mathbf{GL}_2(\mathbf{Z}_l)$ *de* $\mathrm{Aut}(E_t)$, *avec* $l = p_v$.

On peut d'autre part comparer les groupes de Galois associés à *deux courbes elliptiques* E *et* E′ sur K (sans multiplication complexe). Notons A le sous-groupe de $\mathrm{Aut}(E_t) \times \mathrm{Aut}(E'_t)$ formé des couples d'éléments ayant même déterminant. L'image de G par $(\varphi,\varphi') : G \to \mathrm{Aut}(E_t) \times \mathrm{Aut}(E'_t)$ est contenue dans A. De plus :

THÉORÈME 3. *Soit* $l \in P$. *Supposons que les représentations l-adiques*

$$\varphi_l : G \to \mathbf{GL}_2(\mathbf{Q}_l) \qquad \text{et} \qquad \varphi'_l : G \to \mathbf{GL}_2(\mathbf{Q}_l)$$

associées à E *et* E′ *ne soient isomorphes sur aucune extension finie de* K. *L'image de* G *par* (φ,φ') *est alors un sous-groupe ouvert du groupe* A *défini ci-dessus.*

(L'hypothèse faite sur φ_l et φ'_l est en réalité indépendante du choix de l. Il est probable qu'elle équivaut simplement à « E et E′ ne sont pas isogènes sur $\bar{K}$ », mais ce n'est démontré que lorsque l'invariant modulaire de E n'est pas un entier algébrique.)

On peut enfin se demander si des résultats analogues au théorème 1 valent pour d'autres systèmes de représentations l-adiques, par exemple pour le système $(\varphi_l^{\triangle})$ associé à la fonction τ de Ramanujan. Malheureusement, on n'a pas suffisamment de renseignements sur l'action des groupes d'inertie, et l'on ne sait pas prouver la propriété « caractères bornés » utilisée de façon essentielle ci-dessus. Pour cette raison, on n'obtient que des résultats partiels, par exemple le suivant :

THÉORÈME 4. *Soit* H_l *le sous-groupe de* $\mathbf{GL}_2(\mathbf{Z}_l)$ *formé des éléments dont le déterminant est une puissance* 11*-ième. On a* $\varphi_l^{\triangle}(G) \subset H_l$ *pour tout* l, *et l'ensemble* S *des* l *tels que* $\varphi_l^{\triangle}(G) \neq H_l$ *a une densité nulle.*

En fait, il est probable que $S = \{2,3,5,7,23,691\}$.

SÉMINAIRE

Michel RAYNAUD a fait deux exposés sur la structure des schémas en groupes de type $(p,...,p)$. Ses résultats généralisent ceux de OORT-TATE sur les groupes d'ordre p ; comme eux, il utilise de façon essentielle les « sommes de Jacobi ». L'une des conséquences de sa théorie est la détermination des caractères qui interviennent dans l'action du groupe de Galois (l'anneau de base étant un anneau de valuation discrète de caractéristique résiduelle p) ; il prouve que ces caractères s'expriment en fonction des caractères fondamentaux avec des exposants compris entre 0 et l'indice de ramification absolu de l'anneau de base ; cela démontre une conjecture faite dans le cours.

Jacques VÉLU a fait deux exposés sur les courbes elliptiques sur $\mathbf{Q}$ de conducteur 11. Deux telles courbes étaient connues :

$y^2 - y = x^3 - x^2$, qui correspond au groupe modulaire $\Gamma_0^0(11)$,
$y^2 - y = x^3 - x^2 - 10x - 20$, qui correspond à $\Gamma_0(11)$.

Il en obtient une troisième :

$$y^2 - y = x^3 - x^2 - 7820x - 263580.$$

Ces courbes sont liées par des isogénies de degré 5, que l'on peut expliciter. Il est probable (mais non démontré) que ce sont les seules courbes de conducteur 11, à isomorphisme près.

La situation est analogue pour le conducteur 11^2 : on a une liste de telles courbes, qui est probablement complète. Celles de ces courbes d'invariants modulaires $j = -2^{15}, -11^2, -11.131^3$ ont un sous-groupe d'ordre 11 rationnel sur $\mathbf{Q}$; ces trois valeurs de j sont d'ailleurs les seules à avoir cette propriété.

Gérard LIGOZAT a fait un exposé sur les courbes modulaires associées aux groupes $\Gamma_0(N)$, et leurs rapports avec les courbes elliptiques sur $\mathbf{Q}$ de conducteur N (conjectures de WEIL). Il a donné un certain nombre de propriétés (modèle de NÉRON, détermination des points rationnels) de celles de ces courbes qui sont de genre 1, ce qui se produit pour N = 11,14,15,17, 19,20,21,24,27,32,36 et 49.

PUBLICATIONS

A. BOREL et J.-P. SERRE, *Adjonction de coins aux espaces symétriques ; applications à la cohomologie des groupes arithmétiques* (*C. R. Acad. Sci. Paris,* 271, 1970, p. 1156-1158).

— *Cohomologie à supports compacts des immeubles de Bruhat-Tits ; applications à la cohomologie des groupes* S*-arithmétiques* (*C. R. Acad. Sci. Paris,* 272, 1971, p. 110-113).

J.-P. SERRE, *Sur une question d'Olga Taussky* (*J. of Number Theory,* 2, 1970, p. 235-236).

— *Le problème des groupes de congruence pour* $\mathbf{SL}_2$ (*Ann. of Math.,* 92, 1970, p. 489-527).

MISSIONS

Conférences à l'Institute for Advanced Study de Princeton (octobre-décembre 1970), à l'Université de Harvard (décembre 1970), au Colloque de Nancy (janvier 1971) et aux Journées arithmétiques de Marseille (mai 1971).