Jean-Pierre Serre, Sur les groupes de congruence des variétés abéliennes. II, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1971, Volume 35, Issue 4, 731–737

ИЗВЕСТИЯ АКАДЕМИИ НАУК СССР

Серия математическая

35 (1971), 731—737

УДК 519.44

JEAN-PIERRE SERRE

SUR LES GROUPES DE CONGRUENCE DES VARIÉTÉS ABÉLIENNES. II

Introduction. Soit A une variété abélienne définie sur un corps de nombres algébriques k, et soit $A(k)$ le groupe des points de A rationnels sur k. Nous nous proposons de montrer que *tout sous-groupe d'indice fini de* $A(k)$ *est un groupe de congruence.*

D'après ([6]), il suffit pour cela de prouver la nullité des groupes de cohomologie de certaines *algèbres de Lie p-adiques* attachées à A. Cette nullité a été démontrée (*loc. cit.*) lorsque $\dim(A) = 1$, ou lorsque A a suffisamment de multiplications complexes; nous verrons qu'elle est vraie dans le cas général.

1. Un critère de nullité pour la cohomologie d'une algèbre de Lie. Soit V un espace vectoriel de dimension finie sur un corps commutatif K, et soit $\mathfrak{g}$ une sous-algèbre de Lie de l'algèbre de Lie $\mathfrak{gl}(V)$ des K-endomorphismes de V. Soit $x \in \mathfrak{g}$, et soit L l'ensemble des valeurs propres de x (dans une clôture algébrique $\overline{K}$ de K). Si N est un entier $\geqslant 0$, considérons la propriété suivante de L:

(P_N) *Pour toute famille* $(\lambda_1, \ldots, \lambda_{N+1}, \mu_1, \ldots, \mu_N)$ *formée de* $2N+1$ *éléments de* L, *on a*

$$\lambda_1 + \ldots + \lambda_{N+1} \neq \mu_1 + \ldots + \mu_N.$$

(Noter que l'on ne suppose pas que les λ_i et μ_j soient distincts.)

Ainsi, (P_0) signifie que 0 n'appartient pas à L; (P_1) signifie que $\lambda, \mu \in L$ entraîne $\lambda + \mu \notin L$. On a $(P_N) \Rightarrow (P_n)$ si $n \leqslant N$.

THÉORÈME 1. *Soit* N *un entier* $\geqslant 0$, *et soit* $\mathfrak{g}$ *une sous-algèbre de Lie de* $\mathfrak{gl}(V)$. *Supposons que* $\mathfrak{g}$ *contienne un élément* x *dont le spectre* L *jouisse de la propriété* (P_N) *ci-dessus. On a alors* $H^n(\mathfrak{g}, V) = 0$ *pour tout* $n \leqslant N$.

(Pour la définition des groupes de cohomologie $H^n(\mathfrak{g}, V)$, voir par exemple Cartan—Eilenberg ([2]), chap. XIII.)

Soit C le complexe des cochaînes de $\mathfrak{g}$ à valeurs dans V. C'est un complexe gradué; notons d son opérateur cobord, et C^n sa composante homogène de degré n; on a $d(C^n) \subset C^{n+1}$. Un élément de C^n est une application n-linéaire alternée de $\mathfrak{g}^n$ dans V.

Soit $x \in \mathfrak{g}$. L'élément x définit deux endomorphismes i_x et θ_x de l'espace vectoriel C:

a) i_x est le *produit intérieur* par x; il transforme $f \in C^n$ en l'élément $i_x f$ de C^{n-1} défini par la formule

$$(i_x f)(y_1, \ldots, y_{n-1}) = f(x, y_1, \ldots, y_{n-1}) \text{ pour } y_i \in \mathfrak{g}.$$

On a $i_x i_x = 0$.

b) θ_x est la *dérivée de Lie* par rapport à x (pour l'action naturelle de $\mathfrak{g}$ sur C); si $f \in C^n$, on a $\theta_x f \in C^n$ et:

$$(\theta_x f)(y_1, \ldots, y_n) = x \cdot f(y_1, \ldots, y_n) - \sum_{i=1}^{i=n} f(y_1, \ldots, [x, y_i], \ldots, y_n).$$

Les endomorphismes d, i_x et θ_x sont liés par la classique *formule d'homotopie*:

$$di_x + i_x d = \theta_x.$$

Comme d et i_x sont de carré nul, cette formule montre que

$$d\theta_x = di_x d = \theta_x d \text{ et } i_x \theta_x = i_x d i_x = \theta_x i_x.$$

Supposons maintenant que le spectre L de x vérifie la propriété (P_N). On va en déduire:

LEMME 1. *Si n est un entier $\leqslant N$, la restriction de θ_x à C^n est un automorphisme de C^n.*

L'espace vectoriel C^1 est canoniquement isomorphe à un sous-espace de $T^n(\mathfrak{g}') \otimes V$, où $T^n(\mathfrak{g}')$ dèsigne la puissance tensorielle n-ème du dual $\mathfrak{g}'$ de $\mathfrak{g}$. D'autre part $\mathfrak{g}'$ est isomorphe à un quotient de $V \otimes V'$, où V' désigne le dual de V. Ces isomorphismes identifient donc C^n à un sous-espace d'un quotient de l'espace tensoriel $T^{n+1}(V) \otimes T^1(V')$, et cette identification est compatible avec l'action de $\mathfrak{g}$, et en particulier avec celle de x. On en conclut que les valeurs propres de θ_x sur C^n sont de la forme

$$(\lambda_1 + \ldots + \lambda_{n+1}) - (\mu_1 + \ldots + \mu_n), \text{ avec } \lambda_i, \mu_j \in L.$$

Comme L vérifie (P_N), donc aussi (P_n), aucune de ces valeurs propres n'est nulle, ce qui signifie bien que la restriction de θ_x à C^n est un automorphisme.

La nullité de $H^n(\mathfrak{g}, V) = H^n(C)$ pour $n \leqslant N$ est maintenant immédiate. En effet, soit $f \in C^n$ tel que $df = 0$. D'après le lemme 1, il existe $u \in C^n$ tel que $\theta_x u = f$, d'où

$$di_x u + i_x du = \theta_x u = f.$$

Mais, puisque θ_x commute à i_x et d, on a

$$\theta_x i_x du = i_x d\theta_x u = i_x df = 0,$$

d'où $i_x du = 0$ en appliquant le lemme 1. La formule écrite plus haut se réduit alors à $di_x u = f$, ce qui montre bien que f est un cobord, et achève la démonstration.

Remarques. 1) Le cas important pour la suite est celui où $n=1$; il est facile à traiter directement.

2) On peut déduire le théorème 1 de la suite spectrale

$$H^*(\mathfrak{h}, C(\mathfrak{g}/\mathfrak{h}, V)) \Rightarrow H^*(\mathfrak{g}, V),$$

où $\mathfrak{h}$ désigne la sous-algèbre de $\mathfrak{g}$ engendrée par x (cf. Hochschild — Serre ([3]), § 2).

2. Cohomologie à valeurs dans les modules de Tate. Soient k un corps de nombres algébriques, $\bar{k}$ une clôture algébrique de k, et A une variété abélienne sur k, de dimension d. Soit p un nombre premier. Si n est un entier $\geqslant 0$, notons A_{p^n} le noyau de la multiplication par p^n dans le groupe $A(\bar{k})$ des points de A à valeurs dans $\bar{k}$. Le *module de Tate* T_p de la variété A est défini comme la limite projective des A_{p^n}, pour $n \to \infty$; c'est un module libre de rang $2d$ sur l'anneau $\mathbf{Z}_p$ des entiers p-adiques; on pose $V_p = T_p \otimes \mathbf{Q}_p$, de sorte que V_p est un $\mathbf{Q}_p$-espace vectoriel de dimension $2d$.

Le groupe de Galois $\mathrm{Gal}(\bar{k}/k)$ opère continûment sur T_p et V_p; son image dans le groupe $\mathbf{GL}(T_p)$ des automorphismes de T_p est un sous-groupe compact G_p de $\mathbf{GL}(T_p)$. On sait [cf. ([1]), chap. III, § 8, n° 2, th. 2, ainsi que ([6]), prop. 3] que G_p est un sous-groupe de Lie du groupe de Lie p-adique $\mathbf{GL}(T_p)$; son algèbre de Lie $\mathfrak{g}_p$ est une sous-algèbre de l'algèbre de Lie $\mathfrak{gl}(V_p)$.

THÉORÈME 2. *On a* $H^n(\mathfrak{g}_p, V_p) = 0$ *pour tout* $n \geqslant 0$.

Choisissons une place ultramétrique v de k qui ne divise pas p et qui soit telle que A ait bonne réduction en v. On sait que la représentation $\mathrm{Gal}(\bar{k}/k) \to \mathbf{GL}(T_p)$ définie ci-dessus est alors non ramifiée en v. Si w est une place de $\bar{k}$ prolongeant v, on peut donc parler de *l'élément de Frobenius* F_w de G_p attaché à w; la classe de conjugaison de F_w ne dépend que de v.

LEMME 2. *Soit P l'ensemble des valeurs propres de F_w (dans une clôture algébrique de $\mathbf{Q}_p$). Si $a_1, \ldots, a_n, b_1, \ldots, b_m$ appartiennent à P, et si $m \neq n$, l'élément $a_1 \ldots a_n b_1^{-1} \ldots b_m^{-1}$ n'est pas une racine de l'unité.*

En effet, d'après un résultat classique de Weil ([8]), les a_i et les b_j sont des nombres algébriques dont toutes les valeurs absolues (complexes) sont égales à $Nv^{1/2}$, où Nv désigne le nombre d'éléments du corps résiduel de v. Il en résulte que $a_1 \ldots a_n b_1^{-1} \ldots b_m^{-1}$ est un nombre algébrique dont toutes les valeurs absolues sont égales à $Nv^{(n-m)/2}$; ce n'est donc pas une racine de l'unité.

Passons maintenant à l'algèbre de Lie $\mathfrak{g}_p$ de G_p. Puisque G_p est compact, le *logarithme p-adique*

$$\log : G_p \to \mathfrak{g}_p$$

est défini sur G_p tout entier (cf. Bourbaki ([1]), Chap. III, § 7, n°6).

LEMME 3. *Soit L l'ensemble des valeurs propres de l'élément* $\log(F_w)$ *de* $\mathfrak{g}_p$. *Si* $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m$ *appartiennent à* L, *et si* $m \neq n$, *on a*

$$\lambda_1 + \ldots + \lambda_n \neq \mu_1 + \ldots + \mu_m.$$

Après extension finie du corps des scalaires $\mathbf{Q}_p$, on peut mettre F_w sous forme triangulaire (et même sous forme diagonale, car F_w est semi-simple). On en déduit facilement que L n'est autre que l'ensemble des logarithmes des éléments du spectre P de F_w. Si l'on avait

$$\lambda_1 + \ldots + \lambda_n = \mu_1 + \ldots + \mu_m \quad (n \neq m),$$

avec $\lambda_i, \mu_j \in L$, il existerait donc $a_1, \ldots, a_n, b_1, \ldots, b_m \in P$ tels que

$$\log(a_1 \ldots a_n) = \log(b_1 \ldots b_m),$$

et l'élément $a_1 \ldots a_n b_1^{-1} \ldots b_m^{-1}$ serait une racine de l'unité (Bourbaki, *loc. cit.*, prop. 13), ce qui contredirait le lemme 2.

Il résulte du lemme 3 que l'élément $\log(F_w)$ possède la propriété (P_N) du n°1 pour tout entier $N \geqslant 0$. Le théorème 2 résulte donc du théorème 1, appliqué à l'algèbre de Lie $\mathfrak{g}_p$ et à l'élément $\log(F_w)$.

Corollaire. *Pour tout* $n \geqslant 0$, *on a* $H^n(G_p, V_p) = 0$, *et* $H^1(G_p, T_p)$ *est un p-groupe fini.*

(Il s'agit de cohomologie calculée au moyen de cochaînes *continues* — ou *analytiques*, cela revient au même d'après Lazard ([4]), chap. V. th. 2.3.10.)

D'après Lazard, *loc. cit.*, V.2.4.10, $H^n(G_p, V_p)$ s'identifie à un sous-espace vectoriel de $H^n(\mathfrak{g}_p, V_p)$; vu le th. 2, on a donc bien $H^n(G_p, V_p) = 0$. D'autre part, d'après V.3.2.7, le groupe $H^n(G_p, T_p)$ est un $\mathbf{Z}_p$-module de type fini, et son produit tensoriel avec $\mathbf{Q}_p$ est isomorphe à $H^n(G_p, V_p)$; vu la nullité de ce dernier groupe, $H^n(G_p, T_p)$ est un $\mathbf{Z}_p$-module de longueur finie, donc un p-groupe fini.

Remarques. 1) Soit V_p' le dual de V_p, et soit W un sous-$\mathfrak{g}_p$-module d'un espace tensoriel $T^i(V_p) \otimes T^j(V_p')$. Si $i \neq j$, les valeurs propres de $\log(F_W)$ dans W vérifient encore les propriétés (P_N), et l'on en conclut que les groupes $H^n(\mathfrak{g}_p, W)$ sont tous nuls.

2) Le théorème 2 et son corollaire restent valables lorsque l'on suppose seulement que *le corps de base k est de type fini sur le corps premier*, p étant distinct de la caractéristique de k; en effet, cette hypothèse suffit à assurer l'existence d'un «élément de Frobenius» dans G_p, cf. ([6]), fin du n° 1.3.

3) On ne sait pas grand chose sur les algèbres de Lie $\mathfrak{g}_p$, à part le cas $\dim(A) = 1$, traité dans ([7]), chap. IV, § 2. Une conjecture naturelle est que $\mathfrak{g}_p$ coincide avec l'algèbre de Lie du «groupe de Hodge» de A, augmentée des homothéties (cf. Mumford ([5]), n° 4). Signalons à ce sujet une propriété des $\mathfrak{g}_p$: leurs sous-algèbres de Cartan sont abéliennes, et formées d'éléments semi-

simples dans $\mathfrak{gl}(V_p)$ (cela se déduit facilement du fait que les éléments $\log(F_W)$ sont denses dans $\mathfrak{g}_p$, et semi-simples).

3. Le problème des groupes de congruence. Conservons les notations et hypothèses du n° précédent. Si v est une place de k, notons k_v le complété de k pour v; le groupe $A(k_v)$ des points de A à valeurs dans k_v a une structure naturelle de groupe k_v-analytique compact; si v est ultramétrique, c'est un groupe compact totalement discontinu.

Soit $A(k)$ le groupe des points de A à valeurs dans k. D'aprés le théorème de Mordell — Weil, c'est un groupe abélien de type fini. Soit S un ensemble fini de places de k contenant les places archimédiennes. Un sous-groupe Γ de $A(k)$ est appelé un *sous-groupe de S-congruence* s'il existe un ensemble fini I de places de k, disjoint de S, et un sous-groupe ouvert U de $\prod_{v\in I} A(k_v)$ tel que Γ contienne $A(k)\cap U$. Un tel sous-groupe est d'indice fini dans $A(k)$. Réciproquement:

THÈOREME 3. *Tout sous-groupe d'indice fini de $A(k)$ est un groupe de S-congruence.*

On a défini dans ([6]) un certain sous-groupe $H^1_*(\mathfrak{g}_p, V_p)$ de $H^1(\mathfrak{g}_p, V_p)$ et montré que la nullité de ces sous-groupes (pour tout p premier) entraîne le théorème 3 (loc. cit., n° 3.2, th. 2 et 3). Or, d'après le théorème 2, on a $H^1(\mathfrak{g}_p, V_p) = 0$, d'où a fortiori $H^1_*(\mathfrak{g}_p, V_p) = 0$, cqfd.

Remarque. On peut reformuler le théorème 3 en disant que la topologie induite sur $A(k)$ par la topologie produit de $\prod_{v\notin S} A(k_v)$ est la topologie des sous-groupes d'indice fini.

BIBLIOGRAPHIE

[1] Bourbaki N., Groupes et Algèbres de Lie, chap. II—III, Act. Sci Ind., n° 1349, Paris, Hermann, 1971.

[2] Cartan H. and Eilenberg S., Homological Algebra, Princeton Math. Ser., n° 19, Princeton, 1956.

[3] Hochschild G. et Serre J.-P., Cohomology of Lie algebras, Ann. Math., 57 (1953), 591—603.

[4] Lazard M., Groupes analytiques p-adiques, Publ. Math. I. H. E. S., 26 (1965), 1—219.

[5] Mumford D., Families of Abelian Varieties, Proc. Symp. pure math., IX (Boulder), Amer. Math. Soc. (1966), 347—351.

[6] Serre J-P., Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk SSSR. Ser. mat., 28 (1964), 3—20.

[7] Serre J-P., Abelian l-adic representations and elliptic curves, New York, Benjamin, 1968.

[8] Weil A., Variétés abéliennes et courbes algébriques, Act. Sci. Ind., n° 1064, Paris, Hermann, 1948.

О КОНГРУЭНЦПОДГРУППАХ АБЕЛЕВЫХ МНОГООБРАЗИЙ. II

Ж.-П. СЕРР

(РЕЗЮМЕ)

Работа посвящена положительному решению конгруэнцпроблемы для абелевых многообразий, определенных над полем алгебраических чисел k. Иными словами, доказывается, что любая подгруппа конечного индекса в группе k-рациональных точек абелева многообразия содержит подгруппу точек, сравнимых (в естественном смысле) с нулевой точкой по модулю некоторого дивизора поля k.

В работе ([6]) автор редуцировал это утверждение к соотношениям (для любого простого числа p)

$$H^1(\mathfrak{g}, V_p) = 0, \qquad (*)$$

где $V_p = T_p \otimes \mathbf{Q}_p$, T_p — модуль Тэйта абелева многообразия, $\mathbf{Q}_p$ — поле p-адических чисел, а $\mathfrak{g}$ — алгебра Ли той замкнутой подгруппы в группе $GL(V_p)$, которая задается действием группы Галуа алгебраического замыкания поля k в пространстве V_p. В ([6]) эти соотношения были доказаны для эллиптических кривых и абелевых многообразий CM-типа. Теперь они доказываются для произвольного абелева многообразия.

Вот идея доказательства. Рассмотрим произвольный простой дивизор поля k, который не делит p и по модулю которого абелево многообразие имеет хорошую редукцию. Обозначим через F автоморфизм Фробениуса, соответствующий этому простому дивизору. Можно считать, что $F \in GL(T_p)$, и тогда логарифмирование определяет соответствующий элемент $x = \log F \in \mathfrak{g}$.

Из доказанного А. Вейлем аналога гипотезы Римана для абелевых многообразий сразу же следует, что собственные значения эндоморфизма x обладают следующими свойствами: 0 не является собственным значением; сумма и разность собственных значений не является собственным значением. Из первого свойства вытекает, что x является обратимым эндоморфизмом в V_p. Поэтому любой одномерный коцикл $f : \mathfrak{g} \to V_p$ можно так изменить в его классе когомологий, что $f(x) = 0$. При этом условии определение коцикла дает:

$$f([x, y]) = x \cdot f(y) \qquad (**)$$

для всех $y \in \mathfrak{g}$. Иначе говоря, линейное преобразование $f : \mathfrak{g} \to V_p$ коммутирует с x, который действует на V_p естественным образом, а на $\mathfrak{g}$ при помощи присоединенного представления. Легко вычислить, каковы собственные значения x, действующего таким образом в $\mathfrak{g}$. Так как $\mathfrak{g} \subset \mathrm{End}\, V_p = V_p \otimes V_p^*$ (V_p^* — дуальное пространство), то все они должны иметь вид $\lambda - \mu$, где λ и μ — собственные значения x при его естественном действии в V_p. Ввиду указанного выше свойства собственных значений эндоморфизма x ни одно из этих чисел не совпадает с собственным значением x в V_p. Поэтому соотношение (**) показывает, что $f = 0$.

В работе доказывается более общее соотношение, чем (*):

$$H^n(\mathfrak{g}, V_p) = 0$$

для всех $n \geqslant 0$. Приведенное выше рассуждение заменяется при этом следующим утверждением.

Пусть $\mathfrak{g}$ — алгебра Ли, $\mathfrak{g} \subset \hat{\mathrm{E}}\mathrm{nd}\, V$, V — конечномерное векторное пространство $x \in \mathfrak{g}$ и множество L собственных значений эндоморфизма x обладает свойством: если $\lambda_1, \ldots, \lambda_{N+1}, \mu_1, \ldots, \mu_N \in L$, то $\lambda_1 + \ldots + \lambda_{N+1} \neq \mu_1 + \ldots + \mu_N$. Тогда $H^n(\mathfrak{g}, V) = 0$ для всех $n \leqslant N$.

Доказывается, что собственные значения эндоморфизма $x = \log F \in \hat{\mathrm{E}}\mathrm{nd}\, V_p$ обладают этими свойствами для всех $N \geqslant 0$.

Collège de France

Поступило
5.III.1970