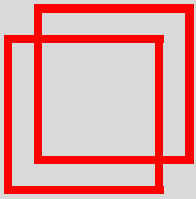
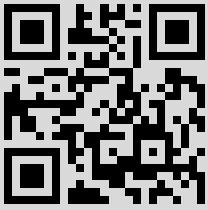

Math-Net.Ru
All Russian mathematical portal

Jean-Pierre Serre, Sur les groupes de congruence des variétés abéliennes, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1964, Volume 28, Issue 1, 3–20

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
http://www.mathnet.ru/eng/agreement

Download details:
IP: 178.193.29.92
November 5, 2020, 20:28:16



ИЗВЕСТИЯ АКАДЕМИИ НАУК СССР
Серия математическая
28 (1964), 3—20

JEAN-PIERRE SERRE

SUR LES GROUPES DE CONGRUENCE DES VARIÉTÉS ABÉLIENNES

Le présent travail apporte un complément aux résultats de Cassels ([2]) et Tate ([10]) sur l'arithmétique des variétés abéliennes. Il s'agit de la question suivante:

Soit A une variété abélienne définie sur un corps de nombres algébriques k, et soit $A(k)$ — le groupe des points rationnels de A. Est-il vrai que tout sous-groupe d'indice fini de $A(k)$ contienne un «groupe de congruence»?

Cette question peut être reformulée en termes de cohomologie des groupes; les groupes qui interviennent sont les groupes de Galois G_p des extensions de k obtenues par adjonction des coordonnées des points de A d'ordre une puissance de p (p premier quelconque). Or il se trouve que G_p est un *groupe de Lie p-adique*, et sa cohomologie est en relations avec celle de son *algèbre de Lie*. Le problème posé se trouve ainsi «linéarisé» et l'on peut le résoudre (affirmativement) dans le cas des courbes elliptiques ainsi que dans le cas des variétés abéliennes ayant suffisamment de multiplications complexes. Le cas général reste ouvert, faute de renseignements assez précis sur les groupes G_p.

Les résultats résumés ci-dessus font l'objet du § 3. Les deux premiers paragraphes sont préliminaires. Le § 1 donne la définition des groupes G_p et quelques-unes de leurs propriétés. Le § 2 contient les résultats de nature cohomologique nécessaires pour la suite.

§ 1. Le groupe de Lie p-adique attaché à une variété abélienne

1.1. Groupes de Lie p-adiques. Soit K un corps valué complet non discret. Une application f d'un ouvert U de K^n dans K est dite *analytique* si elle est développable en série de Taylor au voisinage de tout point de U. Ces fonctions possèdent les propriétés habituelles des fonctions analytiques; on peut les utiliser pour «recoller» des ouverts de K^n et définir ainsi la catégorie des *K-variétés analytiques*. Un groupe dans cette catégorie est appelé un K-groupe analytique, ou encore un *groupe de Lie sur K*. Si G est un tel groupe, on définit comme d'ordinaire son algèbre de Lie $\mathfrak{g}$. Lorsque K est de caractéristique zéro, les théorèmes fondamentaux de Lie s'appliquent à G et $\mathfrak{g}$; en particulier, l'application exponentielle est définie sur un voisinage de 0 dans $\mathfrak{g}$, et donne un isomorphisme de ce voisinage sur un voisinage de l'élément neutre de G; la connaissance de $\mathfrak{g}$ équivaut à celle du *germe* de groupe G [cf. Hooke ([6])].

Dans ce qui suit, nous n'aurons besoin que du cas où le corps de base K est le corps $\mathbf{Q}_p$ des nombres rationnels p-adiques. Un groupe de Lie sur $\mathbf{Q}_p$ est appelé un *groupe de Lie p-adique*; c'est un groupe localement compact totalement discontinu; ses sous-groupes fermés assez petits sont des pro-p-groupes (limites projectives de p-groupes finis).

Proposition 1. (a) *Soient G_1 et G_2 deux groupes de Lie p-adiques. Tout homomorphisme continu $f: G_1 \to G_2$ est analytique.*

(b) *Tout sous-groupe fermé d'un groupe de Lie p-adique est analytique.*

L'énoncé correspondant sur $\mathbf{R}$ est dû à Elie Cartan. Le cas p-adique se traite de façon tout à fait analogue, cf. Hooke ([6]).

Corollaire. *Si un groupe localement compact possède une structure analytique p-adique compatible avec sa structure de groupe topologique, cette structure est unique.*

Cela résulte de l'assertion (a) de la proposition 1.

Proposition 2. *Soit G un groupe de Lie p-adique compact Il existe un sous-ensemble fini X de G qui engendre topologiquement G.* (On dit que X *engendre topologiquement* G lorsque le sous-groupe de G algébriquement engendré par X est dense dans G.)

Soit $\mathfrak{g} = \Sigma \mathfrak{r}_i$ une décomposition de l'algèbre de Lie de G en somme directe de droites. Pour chaque indice i, il existe $x_i \in G$ tel que le sous-groupe topologiquement engendré par x_i ait pour algèbre de Lie $\mathfrak{r}_i$. La famille des x engendre topologiquement un sous-groupe ouvert U de G; comme G est compact, U est d'indice fini dans G. En adjoignant aux x_i des représentants de G/U, on obtient un ensemble fini X qui répond à la question.

1.2. Les groupes G_p. Soit A une variété abélienne de dimension d définie sur un corps k, et soit $\bar{k}$ une clôture algébrique de k. Soit p un nombre premier distinct de la caractéristique de k. Pour tout entier $n \geqslant 1$, les points de A d'ordre divisant p^n sont rationnels sur $\bar{k}$, et forment un $\mathbf{Z}/p^n\mathbf{Z}$ — module libre A_{p^n} de rang $2d$ [cf. Weil ([11]) ou Lang ([7])]. Le *module de Tate* associé au couple (A, p) est défini par la formule:

$$T_p(A) = \varprojlim_n A_{p^n}.$$

C'est un module libre de rang 2d sur l'anneau $\mathbf{Z}_p$ des entiers p-adiques. Le $\mathbf{Q}_p$-espace vectoriel associé sera noté $V_p(A)$. On a donc:

$$V_p(A) = T_p(A) \otimes \mathbf{Q}_p = T_p(A)\left[\frac{1}{p}\right].$$

Dans la suite, on écrira fréquemment T_p et V_p (ou même simplement T et V) à la place de $T_p(A)$ et $V_p(A)$.

Le groupe de Galois $G(\bar{k}/k)$ de l'extension $\bar{k}/k$ opère sur chacun des A_{p^n}, donc aussi sur $T_p(A)$. Cela définit un homomorphisme canonique

$$\pi : G(\bar{k}/k) \to \mathbf{GL}(T_p(A)) = \mathbf{GL}(2d, \mathbf{Z}_p).$$

On vérifie immédiatement que π est *continu*. Son image G_p est donc un sous-groupe fermé du groupe $\mathbf{GL}(T_p) = \mathbf{GL}(2d, \mathbf{Z}_p)$. Mais $\mathbf{GL}(2d, \mathbf{Z}_p)$ est un sous-groupe ouvert du groupe $\mathbf{GL}(2d, \mathbf{Q}_p)$; c'est un groupe de Lie p-adique de dimension $4d^2$. En appliquant la prop. 1, on obtient alors:

Proposition 3. *Le groupe* $G_p = \pi\ (G\ (\bar{k}/k))$ *est un sous-groupe analytique du groupe de Lie p-adique* $\mathbf{GL}\ (T_p)$.

On notera que l'algèbre de Lie de $\mathbf{GL}\ (T_p)$ est la même que celle de $\mathbf{GL}\ (V_p)$: c'est la $\mathbf{Q}_p$-algèbre de Lie $\mathfrak{gl}\ (V_p)$ de tous les endomorphismes de V_p. Il s'ensuit que l'algèbre de Lie $\mathfrak{g}_p$ du groupe G_p s'identifie à une sous-algèbre de $\mathfrak{gl}\ (V_p)$; elle opère donc sur V_p.

Proposition 4. *Lorsqu'on remplace le corps de base k par une extension k' de type fini, le groupe* G_p *est remplacé par un sous-groupe ouvert.*

C'est évident lorsque k' est une extension finie de k. On peut donc se ramener au cas où k' est une extension transcendante pure de k. Les extensions k'/k et $\bar{k}/k$ sont alors linéairement disjointes; on en conclut facilement que le groupe G_p ne change pas.

Corollaire. *L'algèbre de Lie* $\mathfrak{g}_p$ *est invariante par extension de type fini du corps de base.*

C'est clair.

En particulier, soit A une variété abélienne définie sur un corps algébriquement clos quelconque (par exemple $\mathbf{C}$). Choisissons un corps de définition k de A qui soit de type fini sur le corps premier. D'après le corollaire ci-dessus, l'algèbre de Lie $\mathfrak{g}_p$ correspondante ne dépend pas du choix de k. C'est donc un invariant du couple (A, p). On en donnera quelques propriétés au n° suivant. Signalons dès à présent que l'on ne sait à peu près rien de la variation de $\mathfrak{g}_p$ avec p; on ne sait même pas si la dimension de $\mathfrak{g}_p$ dépend de p:

1.3. Propriétés des groupes G_p et des algèbres de Lie $\mathfrak{g}_p$.

(a) Soit R l'anneau d'endomorphismes de la variété abélienne A. Quitte à remplacer k par une extension finie (ce qui ne change pas $\mathfrak{g}_p$) on peut supposer que les éléments de R sont définis sur k; ils commutent alors aux éléments du groupe de Galois $G\ (\bar{k}/k)$. On en conclut que *l'algèbre de Lie* $\mathfrak{g}_p$ *est contenue dans le commutant de* R (dans l'algèbre End (V_p) des $\mathbf{Q}_p$-endomorphismes de V_p).

Supposons en particulier que A admette «suffisamment de multiplications complexes» [cf. Taniyama ([9])], c'est-à-dire que $R \otimes \mathbf{Q}$ soit une algèbre commutative semi-simple de rang $2d$. Le commutant de R dans End (V_p) est alors simplement $R \otimes \mathbf{Q}_p$; d'où l'inclusion:

$$\mathfrak{g}_p \subset R \otimes \mathbf{Q}_p.$$

En particulier, l'algèbre $\mathfrak{g}_p$ est *abélienne.*

b) Soit $\hat{A}$ la variété abélienne duale de A. Soit d'autre part $T_p\ (\mathbf{G}_m)$ le «module de Tate» construit par limite projective à partir des racines p^n-ièmes de l'unité; c'est un $\mathbf{Z}_p$-module libre de rang 1. Soit $V_p\ (\mathbf{G}_m)$ le $\mathbf{Q}_p$-espace vectoriel correspondant; le groupe de Galois $G\ (\bar{k}/k)$ opère en général de façon non triviale sur $V_p\ (\mathbf{G}_m)$. Le symbole (x, y) défini par Weil ([11]) [cf. aussi Lang ([7]), Chap. VII] peut être interprété comme une application bilinéaire:

$$V_p\ (\hat{A}) \times V_p\ (\hat{A}) \to V_p\ (\mathbf{G}_m).$$

Soit X un diviseur ample de A, défini sur k; on lui associe comme on sait une isogénie: $A \to \hat{A}$, d'où un isomorphisme

$$\varphi_X : V_p(A) \to V_p(\hat{A}).$$

En posant $B_X(x, x') = (x, \varphi_X(x'))$, on obtient une forme bilinéaire

$$B_X : V_p(A) \times V_p(A) \to V_p(\mathbf{G}_m).$$

On sait [cf. Lang ([7]), loc. cit.] que B_X est une forme *alternée non dégénérée*. Si $g \in G(\bar{k}/k)$, on a évidemment:

$$B_X(gx, gx') = g \cdot B_X(x, x').$$

On en conclut que le groupe G_p est contenu dans le *groupe des similitudes* de la forme B_X (ce fait m'a été signalé par Grothendieck). Si l'on note $\mathfrak{sp}$ l'algèbre de Lie du groupe symplectique de B_X, et $\mathfrak{c}$ l'algèbre de Lie des homothéties, on a donc:

$$\mathfrak{g}_p \subset \mathfrak{c} \times \mathfrak{sp}.$$

Lorsque k est de type fini sur le corps premier, l'action de $G(\bar{k}/k)$ sur $V_p(\mathbf{G}_m)$ est non triviale, et l'on en conclut que $\mathfrak{g}_p$ *n'est pas contenue dans* $\mathfrak{sp}$.

(c) Supposons que k soit un *corps de nombres algébriques* (autrement dit une extension finie de $\mathbf{Q}$). Si v est une place de k et w une extension de v à $\bar{k}$, le *groupe de décomposition* D_w de w dans G_p est défini; on peut l'interpréter comme le groupe G_p associé au corps local k_v et à sa clôture algébrique $\bar{k}_w$. A conjugaison près, ce groupe (et son algèbre de Lie) ne dépend que de v.

On peut préciser un peu ce qui précède. Soit S un ensemble fini de places de k, contenant les places archimédiennes, et tel que A «se réduise bien» en dehors de S [cf. par exemple Lang — Tate ([8])]. Si $v \notin S$ et si v ne divise pas p, l'extension de k donnée par les points d'ordre une puissance de p est non ramifiée (loc. cit.); le groupe de décomposition D_w correspondant à une telle place s'identifie au groupe G_p de la variété abélienne réduite de A, définie sur le corps résiduel de v; ce groupe est topologiquement engendré par l'élément «de Frobenius» F_w; en particulier son algèbre de Lie est de dimension 1. On sait [cf. par exemple Lang ([7])] que F_w est un endomorphisme semi-simple de V_p, que son polynôme caractéristique a tous ses coefficients entiers (et indépendants de p), et que ses valeurs propres sont de valeur absolue $Nv^{\frac{1}{2}}$ (Nv désignant le nombre d'éléments du corps résiduel de v). En particulier, aucune de ces valeurs propres ne peut être une racine de l'unité. D'après le théorème de Čebotarev, les F_w sont *denses* dans G_p.

Remarque. Comme Grothendieck me l'a fait observer, les résultats de (c) s'étendent en fait à tout corps k qui est de type fini sur le corps premier: on choisit un schéma intègre et normal Y, de type fini sur $\mathbf{Z}$, de corps des fonctions k, tel que A provienne d'un «schéma abélien» sur Y. Les points fermés de Y dont la caractéristique résiduelle n'est pas égale à p donnent alors naissance à des éléments de Frobenius F_w jouissant des mêmes propriétés que ci dessus; on peut montrer que le théorème de Čebotarev est encore valable.

1.4. Courbes elliptiques définies sur un corps de nombres algébriques. On suppose que k est un corps de nom-

bres algébriques, et que la dimension d de A est égale à 1. On a alors

$$\dim V_p = 2;$$

le choix d'une base de V_p permet d'identifier l'algèbre de Lie $\mathfrak{gl}(V_p)$ à l'algèbre $\mathfrak{gl}_2 = \mathfrak{c} \times \mathfrak{sl}_2$ (ici encore, $\mathfrak{c}$ désigne l'algèbre des homothéties). Ainsi, on peut considérer $\mathfrak{g}_p$ comme une sous-algèbre de $\mathfrak{c} \times \mathfrak{sl}_2$; en particulier, sa projection sur le second facteur est une sous-algèbre de Lie de $\mathfrak{sl}_2$. Or les sous-algèbres de Lie de $\mathfrak{sl}_2$ sont faciles à déterminer: à part 0 et $\mathfrak{sl}_2$ il n'y a que des sous-algèbres abéliennes de dimension 1 et des sous-algèbres résolubles de dimension 2 (ces dernières étant conjuguées entre elles). D'autre part, les résultats du n° 1.3 fournissent quelques renseignements sur $\mathfrak{g}_p$; par exemple, $\mathfrak{g}_p$ n'est pas contenue dans $\mathfrak{sl}_2$, et n'annule aucun élément non nul de V_p (sinon l'une des valeurs propres des éléments de Frobenius F_w serait une racine de l'unité). En combinant ces différents renseignements on voit que $\mathfrak{g}_p$ est nécessairement égale à l'une des algèbres suivantes (à un changement de base près dans V_p):

(i) *l'algèbre* $\mathfrak{gl}_2$, de dimension 4;

(ii) *l'algèbre résoluble* $\mathfrak{b}$, de dimension 3, formée des matrices de la forme $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$;

(iii) *la sous-algèbre* $\mathfrak{r}_\lambda$ de $\mathfrak{b}$ formée des matrices de la forme $\begin{pmatrix} a & b \\ 0 & \lambda a \end{pmatrix}$, avec $\lambda \in \mathbf{Q}_p$; c'est une algèbre résoluble de dimension 2;

(iv) *une algèbre abélienne de dimension* 1 *ou* 2.

On pourrait réduire quelque peu cette liste en faisant intervenir les propriétés des *groupes de décomposition* des différentes places de k (et notamment de celles qui divisent p). Cela nous entraînerait trop loin. Nous nous bornerons ici à donner le résultat suivant:

Proposition 5. *Si* $\lambda \in \mathbf{Q}$, *l'algèbre de Lie* $\mathfrak{g}_p$ *ne peut pas être égale à* $\mathfrak{r}_\lambda$.

Supposons que $\mathfrak{g}_p = \mathfrak{r}_\lambda$, avec $\lambda = n/m$, où n et m sont deux entiers premiers entre eux. D'après la théorie de Lie, le groupe G_p contient un sous-groupe ouvert U tel que tout élément $g \in U$ soit de la forme $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ avec $\alpha^n = \gamma^m$. Quitte à remplacer k par l'extension finie correspondant à U, on peut supposer que $G_p = U$. Soit v une place de k de degré 1 (c'est-à-dire telle que $Nv = l$ soit un nombre premier); de telles places sont en nombre infini; on peut donc exiger en outre que $l \neq p$ et que A se réduit bien en v. Soit F un élément de Frobenius correspondant à v, et soient π et $\bar{\pi}$ ses valeurs propres; puisque F est contenu dans G_p, on a $\pi^n = \bar{\pi}^m$ ou $\bar{\pi}^n = \pi^m$. Comme $|\pi| = |\bar{\pi}| = l^{\frac{1}{2}}$, cela donne $n = m$ d'où $\pi = \bar{\pi}$ et π appartient à $\mathbf{Q}$; l'équation

$$l = \pi\bar{\pi} = \pi^2$$

conduit alors à une contradiction, cqfd.

Remarques. 1) Si la courbe elliptique a des *multiplications complexes* (c'est-à-dire si son anneau d'endomorphismes R est distinct de $\mathbf{Z}$), il est facile de voir que $\mathfrak{g}_p$ s'identifie à $R \otimes \mathbf{Q}_p$; c'est une *algèbre abélienne de dimension* 2.

Lorsqu'il n'y a pas de multiplications complexes, je ne connais pas de procédé général permettant de déterminer $\mathfrak{g}_p$; dans tous les cas que j'ai pu traiter, on a $\mathfrak{g}_p = \mathfrak{gl}_2$; peut-être est-ce toujours vrai?

2) Comme on l'a signalé plus haut, l'étude des groupes de décomposition (et d'inertie) de G_p fournit des renseignements supplémentaires sur $\mathfrak{g}_p$. Ainsi, par exemple, si $k = \mathbf{Q}$ et si l'invariant modulaire j n'est pas un entier, on peut montrer que $\mathfrak{g}_p = \mathfrak{gl}_2$.

§ 2. Cohomologie

2.1. Notations. Un groupe topologique G est dit *profini* s'il est limite projective de groupes finis, ou, ce qui revient au même, s'il est compact et totalement discontinu. Soit G un tel groupe et soit A un G-module topologique; nous nous bornerons au cas où A est *séparé* (mais pas nécessairement discret, comme dans Douady ([4])); par définition, le produit $g.a$, $g \in G$, $a \in A$, dépend continûment du couple (g, a). Une n-cochaîne de G à valeurs dans A est une application *continue* f du produit n-uple $G \times \ldots \times G$ dans A. Le cobord df de la cochaîne f est défini par la formule usuelle

$$df(g_1, \ldots, g_{n+1}) = g_1 . f(g_2, \ldots, g_{n+1}) + \\ + \sum_{j=1}^{j=n} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

On obtient ainsi un complexe $C(G, A) = \Sigma C^n(G, A)$ dont les groupes de cohomologie sont notés $H^n(G, A)$. Le groupe $H^0(G, A)$ s'identifie à l'ensemble A^G des éléments de A invariants par G. Un 1-cocycle f est un «homomorphisme croisé» continu de G dans A, autrement dit une application continue vérifiant l'identité

$$f(gh) = f(g) + g \cdot f(h), \quad g, h \in G.$$

C'est un cobord lorsqu'il existe $a \in A$ tel que $f(g) = g \cdot a - a$ pour tout $g \in G$.

Soit $0 \to A \to B \to C \to 0$ une suite exacte de G-modules topologiques; supposons que la topologie de A (resp. de C) soit induite (resp. quotient) de celle de B, et qu'il existe une section continue $C \to B$ (ces conditions sont trivialement vérifiées dans toutes les applications que nous avons en vue). La suite de complexes

$$0 \to C(G, A) \to C(G, B) \to C(G, C) \to 0$$

est alors exacte. On en déduit la suite exacte de cohomologie:

$$\ldots \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \xrightarrow{d} H^{n+1}(G, A) \to \ldots$$

2.2. Le groupe H^1_*. Soit encore G un groupe profini, et soit C un sous-groupe fermé de G. Nous dirons que C est *monogène* s'il peut être engendré topologiquement par un élément; il revient au même de dire que les images de C dans les quotients finis de G sont des groupes cycliques.

Soit A un G-module topologique. Nous définirons $H^1_*(G, A)$ comme le sous-groupe de $H^1(G, A)$ intersection des noyaux des homomorphismes de restriction $H^1(C, A) \to H^1(C, A)$, où C parcourt l'ensemble des sous-groupes monogènes de G. Un élément x de $H^1(G, A)$ appartient donc à $H^1_*(G, A)$ *si et seulement si sa restriction à tout sous-groupe monogène de G est nulle.*

(La définition du foncteur H^1_* est due à Tate, ainsi que l'idée de l'utiliser dans l'étude des groupes de congruence.)

Proposition 6. *Soit U un sous-groupe distingué fermé de G opérant trivialement sur A. L'injection canonique*

$$i : H^1(G/U, A) \to H^1(G, A)$$

définit un isomorphisme de $H^1_*(G/U, A)$ sur $H^1_*(G, A)$.

Montrons d'abord que i applique $H^1_*(G/U, A)$ dans $H^1_*(G, A)$. Soit $x \in H^1_*(G/U, A)$ et soit C un sous-groupe monogène de G. L'image $\overline{C}$ de C dans G/U est un sous-groupe monogène G/U. On a un diagramme commutatif d'applications canoniques:

$$\begin{array}{ccc} H^1(G, A) & \to & H^1(C, A) \\ \uparrow & & \uparrow \\ H^1(G/U, A) & \to & H^1(\overline{C}, A). \end{array}$$

Comme x appartient à $H^1_*(G/U, A)$, son image dans $H^1(\overline{C}, A)$ est nulle. Il en est donc de même de l'image de $i(x)$ dans $H^1(C, A)$, ce qui prouve bien que $i(x)$ appartient à $H^1_*(G, A)$.

Inversement, soit $y \in H^1_*(G, A)$, et soit f un cocycle représentant y. Soit H un sous-groupe monogène de U. Comme la restriction de y à H est nulle, et que H opère trivialement sur A, on voit que f s'annule sur H. Mais U est évidemment réunion de sous-groupes monogènes. On en conclut que f s'annule sur U, i. e. provient d'un 1-cocycle de G/U. On a donc $y = i(x)$, avec $x \in H^1(G/U, A)$. Soit $\overline{C}$ un sous-groupe monogène de G/U. En relevant dans G un générateur topologique de $\overline{C}$, on voit que $\overline{C}$ est image d'un sous-groupe monogène C de G. Le diagramme écrit plus haut montre alors que y induit 0 sur $\overline{C}$, i. e. que y appartient à $H^1_*(G/U, A)$, ce qui achève la démonstration.

La proposition précédente peut notamment s'appliquer en prenant pour U l'ensemble des éléments de G qui opèrent trivialement sur A. Le groupe G/U s'identifie alors à un sous-groupe de Aut (A). En particulier, lorsque A est fini, G/U est fini, et il en est de même de $H^1(G/U, A)$. On obtient donc:

Corollaire. *Si A est fini, $H^1_*(G, A)$ est fini.*

Nous aurons besoin d'une propriété de «passage à la limite» pour les foncteurs H^1 et H^1_*:

Proposition 7. *Si A est limite projective de G-modules compacts A_n, on a*

$$H^1(G, A) = \varprojlim H^1(G, A_n) \text{ et } H^1_*(G, A) = \varprojlim H^1_*(G, A_n).$$

L'assertion relative à H^1 résulte immédiatement de celle relative à H^1 (à condition de l'appliquer aussi aux sous-groupes monogènes C de G). On va donc se borner à H^1.

Montrons d'abord que l'application canonique de $H^1(G, A)$ dans $\varprojlim H^1(G, A_n)$ est injective. Soit x un élément du noyau de cette application, et soit f un 1-cocycle représentant x. Soit f_n le 1-cocycle à valeurs dans A_n obtenu en composant f et $A \to A_n$; par hypothèse, il existe $a \in A_n$ tel que $f_n = da$. Soit F_n l'ensemble des $a \in A_n$ vérifiant cette condition. Les F_n forment un système projectif d'ensembles compacts non vides. D'après un résultat bien connu (cf. Bourbaki, Top. Gén., Chap. I, 3ème éd., § 9, n° 6,

prop. 8), la limite projective des F_n est non vide. Si $a \in A$ appartient à cette limite, on a évidemment $da = f$, d'où $x = 0$.

Soit maintenant (x_n) un élément de $\varprojlim H^1(G, A_n)$. Pour tout n, soit $\mathbf{Z}_n$ l'ensemble des cocycles appartenant à la classe x_n. L'ensemble $\mathbf{Z}_n$ est un espace homogène sur le groupe A_n, le stabilisateur d'un élément étant A_n^G. Cette structure permet de munir $\mathbf{Z}_n$ d'une topologie d'espace compact. Le même argument que ci-dessus montre que $\varprojlim \mathbf{Z}_n$ contient un élément $f = (f_n)$. Il est clair que f est un 1-cocycle à valeurs dans A, et que sa classe x a pour image (x_n), ce qui achève la démonstration.

2.3. Relations avec la cohomologie galoisienne. Soit k un corps de nombres algébriques, soit $\bar{k}$ une clôture algébrique de k, et soit G le groupe de Galois $G(\bar{k}/k)$. Si A est un G-module topologique, on écrira $H^n(k, A)$ à la place de $H^n(G, A)$; c'est la notation usuelle en cohomologie galoisienne, cf. Lang — Tate ([10]). Si v est une place de k, et si w est une extension de v à $\bar{k}$, on note D_w le *groupe de décomposition* correspondant; sa classe (à conjugaison près) ne dépend que de v. En particulier, si un élément x de $H^1(G, A)$ induit 0 sur D_w, il induit aussi 0 sur tous les autres groupes de décomposition correspondant à v; on dit alors que x *s'annule en* v.

Soit S un *ensemble fini de places* de k. On définit $H^1_S(k, A)$ comme le sous-groupe de $H^1(k, A)$ formé des éléments qui s'annulent en toutes les places v n'appartenant pas à S; c'est le noyau de l'application canonique de $H^1(k, A)$ dans le produit des groupes de cohomologie locaux $H^1(k_v, A)$, avec $v \notin S$.

Proposition 8. *Si A est fini, $H^1_S(k, A)$ est contenu dans $H^1_*(G, A)$.*

(Cet énoncé a un sens, car $H^1_S(k, A)$ et $H^1_*(G, A)$ sont tous deux des sous-groupes de $H^1(G, A)$.)

D'après nos conventions générales, A est séparé, donc discret. Soit $x \in H^1_S(k, A)$ et soit f un cocycle représentant x. La continuité de f montre qu'il existe un sous-groupe ouvert U de G sur lequel s'annule. Quitte à restreindre U, on peut supposer que U est distingué dans G, et opère trivialement sur A. Soit C un sous-groupe monogène de G. Son image $C \cdot U/U$ dans G/U est cyclique. D'après le théorème de densité de Frobenius ([5]) il existe une infinité de places ayant un groupe de décomposition (dans G/U) égal à $C \cdot U/U$. On peut donc trouver une place $v \notin S$ et un prolongement w de v tels que $D_w . U = C \cdot U$. Puisque x est nul en v, il existe $a \in A$ tel que

$$f(g) = g \cdot a - a$$

pour tout $g \in D_w$. Tenant compte de ce que f s'annule sur U, et que U opère trivialement sur A, on voit que la même identité vaut pour tout $g \in D_w . U$ et en particulier pour tout $g \in C$. Ainsi la restriction de f à C est un cobord, ce qui prouve bien que x appartient à $H^1_*(G, A)$.

Corollaire. *Si A est fini, $H^1_S(k, A)$ est fini.*

Cela résulte du corollaire à la prop. 6.

2.4. Cohomologie d'un groupe de Lie p-adique. Dans ce n°, ainsi que dans le suivant, on suppose que *G est un groupe de Lie p-adique compact* (cf. n° 1.1.).

LEMME 1. *Si E est un G-module topologique fini, $H^1(G, E)$ est fini.*

D'après la proposition 2 du n° 1.1, il existe un sous-ensemble fini X de G qui engendre topologiquement G. Il est clair que deux homomorphismes croisés f et f' de G dans E qui coïncident sur X coïncident partout. Ces homomorphismes croisés sont donc en nombre fini, ce qui démontre le lemme.

Soit maintenant T un module libre de rang fini N sur l'anneau $\mathbf{Z}_p$ des entiers p-adiques, et soit $V = T \otimes \mathbf{Q}_p$ le $\mathbf{Q}_p$-espace vectoriel associé. On suppose que G *opère continûment* sur T muni de la topologie p-adique (c'est la situation rencontrée au § 1).

Proposition 9. *$H^1(G, T)$ est un $\mathbf{Z}_p$-module de type fini. Son produit tensoriel par $\mathbf{Q}_p$ s'identifie à $H^1(G, V)$.*

Le lemme ci-dessus montre que chacun des $H^1(G, T/p^nT)$ est un p-groupe abélien fini. D'après la prop. 7, le $\mathbf{Z}_p$-module $Y = H^1(G, T)$ s'identifie à $\varprojlim H^1(G, T/p^nT)$; c'est donc un $\mathbf{Z}_p$-module *compact*. De plus, la suite exacte de cohomologie montre que Y/pY, s'identifie à un sous-groupe de $H^1(G, T/pT)$, donc est fini; d'après un résultat classique sur les pro-p-groupes, cela entraîne que Y est topologiquement engendré par un nombre fini d'éléments, ce qui revient à dire que c'est un $\mathbf{Z}_p$-module de type fini. (On aurait pu également raisonner comme dans la démonstration du lemme ci-dessus.) Reste à montrer que $Y \otimes \mathbf{Q}_p$ s'identifie à $H^1(G, V)$. On a en tout cas une application évidente

$$p : Y \otimes \mathbf{Q}_p \to H^1(G, V).$$

Soit $x \in \mathrm{Ker}\,(p)$. Quitte à multiplier x par une constante, on peut supposer que x est de la forme $y \otimes 1$, avec $y \in Y$. Soit f un cocycle représentant y. Par hypothèse, il existe $a \in V$ tel que

$$f(g) = g \cdot a - a$$

pour tout $g \in G$. Si n est assez grand, on a $p^n a \in T$, ce qui montre que $p^n f$ est un cobord, d'où $p^n y = 0$ et $x = 0$. Ainsi p est injective. Sa surjectivité se démontre par un procédé analogue: si v est un élément de $H^1(G, V)$ et si f est un cocycle représentant v, l'image $f(G)$ de G par f est compacte, donc contenue dans un homothétique $p^{-n}T$ de T; le cocycle $p^n f$ prend ses valeurs dans T, et définit un élément $y \in Y$ tel que $p(y \otimes p^{-n}) = v$, cqfd.

Remarque. Il est clair que l'isomorphisme

$$p : H^1(G, T) \otimes \mathbf{Q}_p \to H^1(G, V)$$

transforme $H^1_*(G, T) \otimes \mathbf{Q}_p$ en un sous-espace vectoriel de $H^1_*(G, V)$.

Proposition 10. *Supposons qu'il existe $s \in G$ tel que les relations $s \cdot a = a$, $a \in V$, entraînent $a = 0$. Alors $H^1_*(G, T)$ est un $\mathbf{Z}_p$-module libre de rang $\leqslant \dim H^1_*(G, V)$.*

Vu la proposition précédente et la remarque ci-dessus, il suffit de prouver que $H^1_*(G, T)$ est un $\mathbf{Z}_p$-module *sans torsion*. Soit donc x un élément de $H^1_*(G, T)$ annulé par p. La suite exacte:

$$H^0(G, T) \to H^0(G, T/pT) \xrightarrow{d} H^1(G, T) \xrightarrow{p} H^1(G, T)$$

montre qu'il existe $b \in H^0(G, T/pT)$ tel que $x = db$. Soit C le sous-groupe monogène de G engendré topologiquement par s. On a un diagramme commutatif:

$$\begin{array}{ccc} H^0(C, T/pT) & \xrightarrow{d} & H^1(C, T) \\ i\uparrow & & j\uparrow \\ H^0(G, T/pT) & \xrightarrow{d} & H^1(G, T). \end{array}$$

Comme x appartient à $H^1_*(G, T)$, son image par j est nulle. On a donc $d \circ i(b) = 0$. Mais l'hypothèse faite sur s entraîne que $H^0(C, T)$ est réduit à 0, et l'homomorphisme

$$d : H^0(C, T/pT) \to H^1(C, T)$$

est injectif. D'où $i(b) = 0$, et comme i est trivialement injectif, ceci entraîne $b = 0$ et $x = 0$, cqfd.

Remarque. Les résultats de ce n° restent valables pour tout groupe profini engendré topologiquement par un nombre fini d'éléments.

2.5. Relations avec la cohomologie de l'algèbre de Lie. On conserve les notations et hypothèses du n° précédent.

Il est clair que V et T sont des groupes de Lie p-adiques (abéliens). De plus, la prop. 1 du n° 1.1 montre que l'homomorphisme de G dans le groupe $\mathbf{GL}(T) = \mathbf{GL}(N, \mathbf{Z}_p)$ est analytique; il en résulte que G *opère analytiquement sur* T et sur V.

Proposition 11. *Tout 1-cocycle* $f : G \to V$ *est analytique.*

Les opérations de G sur V permettent de définir le *produit semi-direct* $E = V.G$ de V par G; les éléments de $V.G$ sont les couples (a, g), $a \in V$, $g \in G$, la multiplication étant définie par la formule:

$$(a, g)\cdot(b, h) = (a + g\cdot b, g\cdot h).$$

Si l'on munit E de la structure de variété analytique p-adique produit de celles de V et de G, on obtient un groupe de Lie p-adique. Le cocycle $f : G \to V$ définit une application $\tilde{f} : G \to E$ par la formule:

$$\tilde{f}(g) = (f(g), g).$$

L'identité $f(g\cdot h) = f(g) + g\cdot f(h)$ montre que $\tilde{f}(g\cdot h) = \tilde{f}(g)\cdot\tilde{f}(h)$. Ainsi $\tilde{f}$ est un *homomorphisme*. En appliquant la prop. 1 du n° 1.1, on en déduit que $\tilde{f}$ est analytique, donc aussi f, cqfd.

En fait, l'argument précédent conduit à un résultat plus précis. En effet, l'algèbre de Lie $\mathfrak{e}$ de E s'identifie au *produit semi-direct* $V.\mathfrak{g}$ *de* V *par l'algèbre de Lie* $\mathfrak{g}$ *de* G (V étant muni de sa structure naturelle de $\mathfrak{g}$-module, cf. Bourbaki, Groupes et Alg. de Lie, Chap. I, § 1, n° 8, exemple 2). L'homomorphisme $\tilde{f}$ définit par passage aux algèbres de Lie un homomorphisme

$$\tilde{\varphi} : \mathfrak{g} \to \mathfrak{e} = V\cdot\mathfrak{g}.$$

Si $\varphi : \mathfrak{g} \to V$ est l'application tangente à f en l'élément neutre, on voit facilement que $\tilde{\varphi}(x) = (\varphi(x), x)$ pour tout $x \in \mathfrak{g}$. En écrivant que $\tilde{\varphi}$ est un homomorphisme, on trouve que φ vérifie l'identité:

$$\varphi([x, y]) = x\cdot\varphi(y) - y\cdot\varphi(x), \quad x, y \in \mathfrak{g}$$

[cf. Bourbaki, loc. cit., formule (13)]. Cette identité signifie que φ *est un* 1-cocycle de $\mathfrak{g}$ à valeurs dans V, au sens de la cohomologie des algèbres de Lie [cf. par exemple Cartan — Eilenberg ([1]), Chap. XIII]. S'il existe $a \in V$ tel que $f(g) = g\cdot a - a$ pour tout $g \in G$, on a $\varphi(x) = x\cdot a$ pour tout $x \in \mathfrak{g}$;

ainsi, si f est un cobord (au sens de la cohomologie des groupes), φ est un cobord (au sens de la cohomologie des algèbres de Lie). En faisant correspondre à la classe de cohomologie de f celle de φ on définit une application linéaire canonique

$$\theta : H^1(G, V) \to H^1(\mathfrak{g}, V).$$

Proposition 12. *L'application* θ *est injective.*

Soit $\alpha \in \mathrm{Ker}\ (\theta)$, et soit f un cocycle représentant α. Soit φ l'application tangente à f en l'élément neutre de G. Puisque $\theta(\alpha) = 0$, il existe $a \in V$ tel que $\varphi(x) = x \cdot a$ pour tout $x \in \mathfrak{g}$. Posons $f' = f - da$, et soit φ' l'application tangente à f' en l'élément neutre; on a

$$\varphi'(x) = \varphi(x) - x \cdot a = 0$$

pour tout $x \in \mathfrak{g}$. Soient $\widetilde{f'}$ et σ les homomorphismes de G dans le produit semi-direct $V.G$ définis par les formules:

$$\widetilde{f'}(g) = (f'(g), g), \quad \sigma(g) = (0, g).$$

Du fait que $\varphi' = 0$, $\widetilde{f'}$ et σ induisent *le même homomorphisme* de l'algèbre de Lie de G dans celle de $V.G$; d'après la théorie de Lie, ils coïncident donc sur un voisinage U de l'élément neutre. Quitte à restreindre U, on peut supposer que c'est un sous-groupe ouvert distingué de G. On a $f'(g) = 0$ pourt tout $g \in U$; on en conclut que f' provient d'un 1-cocycle de G/U à valeurs dans V^U; comme V^U est un $\mathbf{Q}_p$-espace vectoriel, on a $H^1(G/U, V^U) = 0$. Donc f' est un cobord et $\alpha = 0$, cqfd.

Remarque. En général l'application θ n'est pas surjective. Toutefois, il est facile de voir qu'il existe un sous-groupe ouvert U de G tel que

$$\theta_U : H^1(U, V) \to H^1(\mathfrak{g}, V)$$

soit surjective (donc bijective).

Dans ce qui suit, nous noterons $H^1_*(\mathfrak{g}, V)$ *le sous-espace de* $H^1(\mathfrak{g}, V)$ *formé des éléments dont la restriction à toute sous-algèbre à une dimension de* $\mathfrak{g}$ *est nulle.* La classe d'un cocycle φ appartient à $H^1_*(\mathfrak{g}, V)$ si $\varphi(x) \in x \cdot V$ pour tout $x \in \mathfrak{g}$.

Proposition 13. *L'image de* $H^1_*(G, V)$ *par* $\theta : H^1(G, V) \to H^1(\mathfrak{g}, V)$ *est contenue dans* $H^1_*(\mathfrak{g}, V)$.

Soit $\mathfrak{h}$ une sous-algèbre à une dimension de $\mathfrak{g}$. D'après la théorie de Lie [cf. Hooke ([6])], il existe une sous-groupe monogène C de G ayant $\mathfrak{h}$ pour algèbre de Lie (on peut même prendre C isomorphe au groupe $\mathbf{Z}_p$). La proposition résulte immédiatement de là.

Remarque. On a en fait

$$H^1_*(G, V) = \theta^{-1}(H^1_*(\mathfrak{g}, V)).$$

On va combiner entre eux les différents résultats obtenus jusqu'ici:

THÉORÈME 1. (i) *Si* $H^1(\mathfrak{g}, V) = 0$, $H^1(G, T)$ *est un p-groupe fini.*

(ii) *Supposons que* $H^1_*(\mathfrak{g}, V) = 0$ *et qu'il existe* $s \in G$ *tel que les relations* $s \cdot a = a$, $a \in V$, *entraînent* $a = 0$. *Alors* $H^1_*(G, T) = 0$.

Si $H^1(\mathfrak{g}, V) = 0$, la prop. 2 montre que $H^1(G, V) = 0$, donc (prop 9) $H^1(G, T)$ est un p-groupe fini.

Si les hypothèses de (ii) sont vérifiées, la prop. 13 montre que $H^1_*(G, V) = 0$, et, en appliquant la prop. 10, on voit que $H^1_*(G, T)$ est réduit à 0.

Remarque. Les résultats relatifs à H^1 démontrés dans ce n° et dans le précédent ont été étendus par Lazard à la cohomologie de dimension quelconque. La méthode de Lazard est d'ailleurs tout à fait différente de celle utilisée ici (qui semble limitée à la dimension 1).

2.6. Un exemple où $H^1_*(\mathfrak{g}, V)$ est non trivial. On prend pour $\mathfrak{g}$ une algèbre commutative de base $\{X, Y\}$, et pour V un espace de dimension 3, de base $\{e_1, e_2, e_3\}$. On fait opérer $\mathfrak{g}$ sur V par les formules

$$Xe_1 = e_2, \quad Xe_2 = e_3, \quad Xe_3 = 0$$
$$Ye_1 = e_3, \quad Ye_2 = 0, \quad Ye_3 = 0.$$

Le calcul de $H^1(\mathfrak{g}, V)$ et de $H^1_*(\mathfrak{g}, V)$ ne présente pas de difficultés. On trouve que $H^1_*(\mathfrak{g}, V)$ est un espace vectoriel de dimension 1, admettant pour base la classe du cocycle φ donné par les formules:

$$\varphi(X) = 0, \quad \varphi(Y) = e_3.$$

§ 3. Groupes de congruence

3.1. Position du problème. Soit A une variété abélienne, définie sur un corps de nombres algébriques k. D'après le théorème de Mordell — Weil, le groupe $A(k)$ des points de A rationnels sur k est un groupe abélien de type fini. En imposant aux éléments de $A(k)$ des conditions «de congruence», on obtient des sous-groupes d'indice fini de $A(k)$. De façon plus précise, donnons-nous un systéme

$$U = \{I, (U_i)_{i \in I}\}$$

où I est un ensemble *fini* de places non archimédiennes de k, et où, pour chaque i, U_i est un *sous-groupe ouvert* du groupe compact $A(k_i)$ des points de A rationnels sur le corps local k_i; les éléments de $A(k)$ qui appartiennent à U_i pour tout $i \in I$ forment un sous-groupe Γ_U de $A(k)$, évidemment d'indice fini dans $A(k)$; nous dirons que Γ_U est un *sous groupe de congruence* de $A(k)$. Il s'agit de savoir si l'on obtient par ce procédé un ensemble cofinal de sous-groupes d'indice fini de $A(k)$. Si S est un ensemble fini de places de k, contenant toutes les places archimédiennes, on peut demander en outre que l'ensemble I soit *disjoint de* S, auquel cas on dira que Γ_U est un *sous-groupe de S-congruence*. On est ainsi amené à formuler la condition suivante:

(C_S) *Pour tout sous-groupe* Γ *d'indice fini de* $A(k)$, *il existe un système* $U = \{I, U_i\}$, *avec* $I \cap S = \emptyset$, *tel que le groupe* Γ_U *correspondant soit contenu dans* Γ.

Cette condition peut aussi s'énoncer en termes topologiques:

(C'_S) *Si l'on plonge* $A(k)$ *dans le groupe compact* $\prod_{v \in S} A(k_v)$, *la topologie induite est celle des sous-groupes d'indice fini.*

C'est sous cette dernière forme que le problème apparaît dans Cassels [2] à cela près que Cassels ne s'intéresse qu'au cas où S est l'ensemble des places archimédiennes de k.

Remarques. 1) Tout sous-groupe Γ d'indice fini de $A(k)$ contient une intersection finie de sous-groupes de la forme $p^n A(k)$, avec p premier

et $n \geqslant 1$. On en conclut que la condition (C_S) équivaut à la conjonction des conditions $(C_S(p))$ suivantes:

$(C_S(p))$: *Pour tout* $n \geqslant 1$, *il existe un groupe de S-congruence* Γ_U *contenu dans* $p^n A(k)$.

2) Des problèmes analogues se posent pour les groupes linéaires, le groupe $A(k)$ étant remplacé par un groupe d'«unités», ou plus généralement de «S-unités». Le cas du groupe multiplicatif $\mathbf{G}_m$ a été résolu affirmativement par Chevalley ([3]); nous reviendrons là-dessus au n° 3.5. Dans le cas semi-simple on n'a que des résultats très partiels; par exemple, pour $k = \mathbf{Q}$ et pour le groupe $\mathbf{SL}_n$, la réponse est négative pour $n = 2$, positive pour $n \geqslant 3$ (ce dernier fait résulte de théorèmes récents de Bass et de Lazard).

3.2. Traduction cohomologique. On va montrer que la propriété $(C_S(p))$ peut se déduire d'une propriété portant sur la cohomologie galoisienne du module $T_p(A)$:

Soit $\bar{k}$ une clôture algébrique de k, et soit A_{p^n} le sous-groupe de $A(\bar{k})$ formé des éléments d'ordre divisant p^n; c'est un module topologique fini sur le groupe de Galois $G(\bar{k}/k)$. On a défini au n° 2.3 le sous-groupe $H^1_S(k, A_{p^n})$ du groupe $H^1(k, A_{p^n})$; lorsque n varie, ces groupes forment un *système projectif*.

THÉORÈME 2. *La propriété* $(C_S(p))$ *est vérifiée si* $\varprojlim H^1_S(k, A_{p^n}) = 0$.

On va utiliser la suite exacte «de Kummer» [cf. Lang — Tate ([8])]; c'est la suite exacte associée à la suite exacte de coefficients:

$$0 \to A_{p^n} \to A \xrightarrow{p^n} A \to 0.$$

Elle définit un opérateur cobord $d_n : A(k) \to H^1(k, A_{p^n})$; le noyau de d_n est égal à $p^n A(k)$.

LEMME 2. *Il existe un sous-groupe de S-congruence* Γ_U *de* $A(k)$, *dont l'image par* d_n *est contenue dans* $H^1_S(k, A_{p^n})$.

Le groupe $d_n(A(k))$ est isomorphe à $A(k)/p^n A(k)$, c'est un groupe fini. Soient $(x_\iota)_{\iota \in I}$ les éléments de $d_n(A(k))$ que n'appartiennent pas à $H^1_S(k, A_{p^n})$. Pour tout $\iota \in I$ il existe une place $v_\iota \notin S$ telle x_ι ait une image non nulle dans $H^1(k_{v_\iota}, A_{p^n})$. Posons d'autre part

$$U_\iota = p^n A(k_{v_\iota});$$

comme l'homomorphisme $p^n : A(k_{v_\iota}) \to A(k_{v_\iota})$ a une application tangente surjective, U_ι est un sous-groupe *ouvert* de $A(k_{v_\iota})$. Soit Γ_U le groupe de S-congruence défini par le système des v_ι et des U_ι. Si $x \in \Gamma_U$, on a $x \in p^n A(k_{v_\iota})$ pour tout ι, et l'image de $d_n(x)$ dans $H^1(k_{v_\iota}, A_{p^n})$ est nulle; ainsi $d_n(x)$ ne peut être égal à aucun des x_ι, et l'on a nécessairement $d_n(x) \in H^1_S(k, A_{p^n})$, ce qui démontre le lemme.

Revenons à la démonstration du théorème 2. Supposons que

$$\varprojlim H^1_S(k, A_{p^n}) = 0.$$

Soit n un entier $\geqslant 1$. Puisque les $H^1_S(k, A_{p^{n+m}})$ sont finis (prop. 8, n° 2.3) et de limite projective réduite à 0, il existe un entier $m \geqslant 0$ tel que l'homomorphisme canonique

$$\alpha : H^1_S(k, A_{p^{n+m}}) \to H^1_S(k, A_{p^n})$$

soit nul. D'après le lemme précédent, il existe un groupe de S-congruence Γ_U, dont l'image par d_{n+m} est contenue dans $H^1_S(k, A_{p^{n+m}})$. Comme d_n s'obti-

ent en composant d_{n+m} et α, on a

$$d_n(\Gamma_U) = 0,$$

d'où $\Gamma_U \subset p^n A(k)$, et la condition $(C_S(p))$ est bien vérifiée.

Remarque. Signalons, d'après Tate ([10]), que la condition $\varprojlim H^1_S(k, A_{p^n}) = 0$ entraîne également la nullité de la composante p-primaire de $H^2(k, A)$ (du moins si $p \neq 2$, ou si k est totalement imaginaire).

Dans l'énoncé suivant, les notations T_p, V_p, G_p, $\mathfrak{g}_p$ sont celles du n° 1.2; les notations cohomologiques sont celles des n^{os} 2.2 et 2.5.

THÉORÈME 3. *On a les implications suivantes*:

$$H^1_*(\mathfrak{g}_p, V_p) = 0 \Rightarrow H^1_*(G_p, T_p) = 0 \Rightarrow \varprojlim H^1_S(k, A_{p^n}) = 0.$$

La première implication résulte du théorème 1 du n° 2.5 (qui est applicable a G_p grâce aux propriétés des éléments de Frobenius signalées au n° 1.3). D'autre part, les propositions 6 et 7 du n° 2.2 montrent que:

$$H^1_*(G_p, T_p) = \varprojlim H^1_*(G_p, A_{p^n}) = \varprojlim H^1_*(G(\bar{k}/k), A_{p^n}),$$

et la prop. 8 du n° 2.3 montre que $H^1_S(k, A_{p^n})$ est un sous-groupe de $H^1_*(G(\bar{k}/k), A_{p^n})$. Il est donc clair que la nullité de $H^1_*(G_p, T_p)$ entraîne celle de $\varprojlim H^1_S(k, A_{p^n})$.

Les deux n^{os} qui suivent contiennent les deux cas particuliers dans lesquels je sais démontrer la nullité de $H^1_*(\mathfrak{g}_p, V_p)$; dans chacun de ces cas, c'est d'ailleurs le groupe $H^1(\mathfrak{g}_p, V_p)$ lui-même qui est nul.

3.3. Variétés abéliennes ayant suffisamment de multiplications complexes.

THÉORÈME 4. *Soit A une variété abélienne ayant suffisamment de multiplications complexes* (cf. n° 1.3). *Pour tout nombre premier p, on a alors $H^1(\mathfrak{g}_p, V_p) = 0$. En particulier*:

(a) *$H^1(G_p, T_p)$ est un p-groupe fini.*

(b) *La condition (C_S) est vérifiée quel que soit l'ensemble fini S.*

Pour démontrer que $H^1(\mathfrak{g}_p, V_p) = 0$ on s'appuie sur le lemme suivant:

LEMME 3. *Soit $\mathfrak{g}$ une algèbre de Lie, soit V un $\mathfrak{g}$-module de dimension finie, et soit $\mathfrak{c}$ un idéal de $\mathfrak{g}$ de dimension 1. Si $H^0(\mathfrak{c}, V) = 0$, on a $H^n(\mathfrak{g}, V) = 0$ pour tout $n \geqslant 0$.*

Soit X un élément non nul de $\mathfrak{c}$. L'hypothèse $H^0(\mathfrak{c}, V) = 0$ signifie que l'endomorphisme de V défini par X est injectif; comme V est de dimension finie, il est aussi surjectif, et $H^1(\mathfrak{c}, V) = 0$. Il est trivial que $H^q(\mathfrak{c}, V) = 0$ pour $q \geqslant 2$. La suite spectrale:

$$H^p(\mathfrak{g}/\mathfrak{c}, H^q(\mathfrak{c}, V)) \Rightarrow H^n(\mathfrak{g}, V)$$

montre alors bien que $H^n(\mathfrak{g}, V) = 0$ pour tout $n \geqslant 0$.

On applique ce lemme à la sous-algèbre $\mathfrak{c}$ de $\mathfrak{g}_p$ tangente au sous-groupe monogène de G engendré topologiquement par un élément de Frobenius F. Comme aucune valeur propre de F n'est une racine de l'unité, on a $H^0(\mathfrak{c}, V) = 0$. D'autre part, on a vu au n° 1. 3 que $\mathfrak{g}_p$ est une algèbre commutative, et $\mathfrak{c}$ est donc bien un idéal de $\mathfrak{g}_p$. Ainsi, on a $H^1(\mathfrak{g}_p, V_p) = 0$. Le théorème 1 du n° 2.5 montre alors que $H^1(G_p, T_p)$ est un p-groupe fini; les théorèmes 2 et 3 du n° 3.3 montrent que la condition $(C_S(p))$ est vérifiée, cqfd.

3.4. Courbes elliptiques. Le résultat est le même qu'au n° précédent:

THÉORÈME 5. *Si A est une courbe elliptique, on a $H^1(\mathfrak{g}_p, V_p) = 0$ pour tout nombre premier p. En particulier:*

(a) *$H^1(G_p, T_p)$ est un p-groupe fini.*

(b) *La condition* (C_S) *est vérifiée quel que soit l'ensemble fini S.*

Ici encore, il suffit de prouver que $H^1(\mathfrak{g}_p, V_p) = 0$. Si $\mathfrak{g}_p$ est abélienne, on applique le lemme 3 du n° 3.3 comme ci-dessus. Si $\mathfrak{g}_p$ est égale à $\mathfrak{gl}_2$ ou à l'algèbre triangulaire $\mathfrak{b}$, on applique le même lemme, en prenant cette fois pour $\mathfrak{c}$ l'algèbre des homothéties (le centre de $\mathfrak{gl}_2$). Reste le cas où $\mathfrak{g}_p$ est égale à une algèbre résoluble $\mathfrak{r}_\lambda$ formée des matrices de la forme $\begin{pmatrix} a & b \\ 0 & \lambda a \end{pmatrix}$. On obtient une base $\{X, Y\}$ de $\mathfrak{r}_\lambda$ en posant:

$$X = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

On a $[X, Y] = (1 - \lambda)\, Y$. Une 1-cochaîne $\varphi : \mathfrak{r}_\lambda \to V$ est déterminée par les deux vecteurs

$$\varphi(X) = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad \varphi(Y) = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

C'est un cocycle si $\varphi([X, Y]) = X \cdot \varphi(Y) - Y \cdot \varphi(X)$, ce qui s'écrit:

$$\begin{cases} (1 - \lambda)\, y_1 = y_1 - x_2, \\ (1 - \lambda)\, y_2 = \lambda y_2. \end{cases}$$

On sait (cf. n° 1.4, prop. 5) que $\lambda \neq \frac{1}{2}$. La deuxième équation donne alors $y_2 = 0$. Soit a le vecteur de composantes x_1 et $\lambda^{-1} x_2$; on vérifie tout de suite que $\varphi(X) = X \cdot a$ et $\varphi(Y) = Y \cdot a$, ce qui montre que φ est un cobord. On a donc bien $H^1(\mathfrak{g}_p, V_p) = 0$ dans tous les cas, cqfd.

Remarques. 1) La finitude de $H^1(G_p, T_p)$ et la validité de la condition (C_S) ont été également démontrées par J. Cassels. La démonstration de Cassels est basée sur une énumération de cas analogue à celle utilisée ici; toutefois elle ne fait aucun usage de la structure analytique de G_p ni *a fortiori* de son algèbre de Lie.

2) Si l'on veut simplement démontrer la nullité de $H^1_*(\mathfrak{g}_p, V_p)$ (ce qui suffit pour le problème des groupes de congruence), on n'a besoin d'*aucune* propriété de $\mathfrak{g}_p$; on peut en effet vérifier que $H^1_*(\mathfrak{g}, V) = 0$ pour toute algèbre de Lie $\mathfrak{g}$ et tout $\mathfrak{g}$-module V de dimension $\leqslant 2$.

3.5. Compléments. Il serait évidemment désirable d'étendre les résultats des deux derniers n^{os} à *toutes* les variétés abéliennes. Il faudrait en savoir davantage sur les algèbres de Lie $\mathfrak{g}_p$; par exemple, V_p est-il toujours un $\mathfrak{g}_p$-module semi-simple? L'algèbre $\mathfrak{g}_p$ contient-elle nécessairement les homothéties? Une réponse affirmative à l'une de ces questions suffirait à entraîner la nullité de $H^1(\mathfrak{g}_p, V_p)$ et *a fortiori* la condition ($C_S(p)$).

Signalons d'autre part que les méthodes utilisées dans ce travail s'appliquent plus généralement aux extensions de variétés abéliennes par des tores; bien entendu, le groupe $A(k)$ doit être remplacé par un groupe d'*unités* (ou de «S-unités»). Le cas d'un tore est particulièrement simple: l'algèbre

de Lie $\mathfrak{g}_p$ est réduite aux homothéties, et sa cohomologie est triviale. Dans le cas du groupe G_m cela redonne le théorème de Chevalley ([3]) cité au n° 3.1.

BIBLIOGRAPHIE

[1] Cartan H. and Eilenberg S., Homological Algebra, Princeton Math. Ser., n° 19, Princeton, 1956.
[2] Cassels J., Arithmetic on an elliptic curve, International Congress, Stockholm, 1962.
[3] Chevalley C., Deux théorèmes d'arithmetique, J. Math. Soc. Japan, 3 (1951), 36—44.
[4] Douady A., Cohomologie des groupes compacts totalement discontinus, Séminaire Bourbaki (1959—60), exposé 189.
[5] Frobenius G., Ueber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sitz. Berlin Akad. (1896), 689—705.
[6] Hooke R., Linear p-adic groups and their Lie algebras, Annals of Math., 43 (1942), 641—655.
[7] Lang S., Abelian varieties, Interscience Tracts, n°7, New York, 1959.
[8] Lang S. and Tate J., Principal homogeneous spaces over abelian varieties, Amer. Journ. of Math., 80 (1958), 659—684.
[9] Taniyama Y., L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, 9 (1957), 330—366.
[10] Tate J., Duality theorems in Galois cohomology over number fields, International Congress, Stockholm, 1962.
[11] Weil A., Variétés abéliennes et courbes algébriques, Act. Sci. Ind., n° 1064, Paris, Hermann, 1948.

О КОНГРУЭНЦПОДГРУППАХ АБЕЛЕВЫХ МНОГООБРАЗИЙ

Ж. П. СЕРР

(РЕЗЮМЕ)

Пусть A — абелево многообразие, определенное над полем алгебраических чисел, k и $A(k)$ — группа его точек, рациональных над k. Подгруппа $\Gamma \subset A(k)$ называется конгруэнцподгруппой, если она задается условием:

$$\gamma \in \Gamma \langle = \rangle \gamma \in U_{\mathfrak{p}}, \quad \mathfrak{p} \in I,$$

где I — конечное множество простых дивизоров поля k, а $U_{\mathfrak{p}}$ для каждого $\mathfrak{p}$ — некоторая открытая подгруппа в группе $A(k_{\mathfrak{p}})$ точек A, рациональных над пополнением k по метрике, соответствующей простому дивизору.

В работе исследуется следующий вопрос, возникший в арифметической теории абелевых многообразий [см. ([2]) и ([10])]. Каково замыкание $\widetilde{A(k)}$ образа группы $A(k)$ при вложении

$$A(k) \to \prod_{\mathfrak{p}} A(k_{\mathfrak{p}}),$$

где $\mathfrak{p}$ пробегает все простые дивизоры поля k? В частности, верно ли, что

$$\widetilde{A(k)} = \varprojlim_{n} A(k)/nA(k)?$$

Последнее утверждение равносильно тому, что любая подгруппа конечного индекса содержит некоторую конгруэнцподгруппу.

Автор рассматривает более общее свойство (C_S):

Для любого конечного множества S простых дивизоров поля k и любой подгруппы конечного индекса Г существует конгруэнцподгруппа, содержащаяся в Г и определенная при помощи множества I, не пересекающегося с S.

Основной результат работы (теоремы 4 и 5):

Свойство (C_S) имеет место, если A является: a) эллиптической кривой, b) абелевым многообразием с достаточным числом комплексных умножений (т. е. алгебра комплексных умножений A коммутативна и ее ранг вдвое больше размерности A).

Доказательство этих утверждений основывается на их последовательной редукции к некоторым другим утверждениям, имеющим самостоятельный интерес. Очевидно, что достаточно доказать свойство (C_S) для подгрупп, индекс которых имеет вид p^n, где p — простое число. Соответствующее утверждение обозначается через ($C_S(p)$). Автор использует известную точную последовательность, связанную с эндоморфизмом умножения на p^n в группе $A(\bar{k})$ ($\bar{k}$ — алгебраическое замыкание поля k) и соответствующую точную последовательность когомологий. Из ее рассмотрения он выводит, что свойство ($C_S(p)$) выполнено, если

$$\varprojlim_n H^1_S(k, A_{p^n}) = 0 \qquad (*)$$

(теорема 2). Здесь $H^1_S(k, A_{p^n})$ — подгруппа группы $H^1(G(\bar{k}/k), A_{p^n})$, состоящая из элементов, ограничение которых на всех подгруппах разложения простых дивизоров, не содержащихся в S, равно нулю; $C(\bar{k}/k)$ — группа Галуа поля $\bar{k}/k$; A_{p^n} — группа элементов порядка, делящего p^n в $A(\bar{k})$.

Пусть G — проконечная группа (т. е. проективный предел конечных групп) и A — топологический G-модуль. Через $H^1_*(G, A)$ автор обозначает подгруппу группы $H^1(G, A)$, состоящую из элементов, которые имеют нулевое ограничение на всех однопараметрических подгруппах группы G (т. е. на замкнутых подгруппах с одной топологической образующей). Пусть $T_p(A) = \varprojlim_n A_{p^n}$ — модуль Тэйта многообразия A, а $V_p(A)$ — расширение этого модуля до векторного пространства над полем p-адических чисел. Вторая редукция заключается в том, что свойство (*) выполнено, если

$$H^1_*(G(\bar{k}/k), T_p(A)) = 0. \qquad (**)$$

Как известно, $T_p(A)$ является свободным модулем над кольцом $\mathbf{Z}_p$ целых p-адических чисел размерности, равной $2d$, где $d = \dim A$. Его группа автоморфизмов совпадает с линейной группой $GL(2d, \mathbf{Z}_p)$. Действие группы $G(\bar{k}/k)$ на этом модуле определяет, следовательно, гомоморфизм $\pi : G(\bar{k}/k) \to GL(2d, \mathbf{Z}_p)$: Группу $GL(2d, \mathbf{Z}_p)$ можно рассматривать как p-адическую группу Ли (точные определения даны в § 1). Группа $\pi G(\bar{k}/k)$ является замкнутой подгруппой этой группы. Это дает возмож-

ность ввести и в группе $\pi G(\bar{k}/k)$ структуру p-адической группы Ли и, в частности, определить ее алгебру Ли $\mathfrak{g}_p$. Представление группы $\pi G(\bar{k}/k)$ в $GL(2d, \mathbf{Z}_p)$ определяет естественным образом представление алгебры Ли $\mathfrak{g}_p$ в $V_p(A)$. Последняя редукция заключается в том, что свойство (**) выполнено, если $H^1_*(\mathfrak{g}_p, V_p(A)) = 0$, где H^1_* определяется для алгебр Ли так же, как для групп (теорема 4). В указанных выше случаях a) и b) автор доказывает более сильное утверждение:

$$H^1(\mathfrak{g}_p, V_p(A)) = 0.$$

В работе указывается на несколько нерешенных вопросов. Приведем некоторые из них.

1. Какова связь алгебр $\mathfrak{g}_p$ для одного и того же абелева многообразия и для разных p? Имеют ли они одинаковую размерность?

2. В случае, когда A — эллиптическая кривая, в рассмотренных автором примерах алгебра $\mathfrak{g}_p$ или абелева размерности 2 (когда A имеет комплексное умножение) или совпадает с алгеброй всех матриц 2-го порядка (когда у A нет комплексных умножений). Верно ли это всегда?

3. Верен ли основной результат работы без ограничений a) и b)?

4. Возможно ли его перенести на другие алгебраические группы? (При рассмотрении линейных групп вместо $A(k)$ естественно рассматривать группу единиц соответствующей группы.) Для мультипликативной группы этот результат был давно получен Шевалле ([3]). Автор сообщает, что для специальной линейной группы размерности $n \geqslant 3$ положительный ответ вытекает из еще неопубликованных результатов Басса и Лазара. С другой стороны, еще со времен Клейна известно, что при $n = 2$ соответствующий вопрос для этой группы решается отрицательно.

Поступило
1. IX. 1963