THÉORIE DES GROUPES. — *Extensions centrales non résiduellement finies de groupes arithmétiques.* Note (*) de M. **Pierre Deligne,** Membre de l'Académie.

Une variante des méthodes connues pour traiter le problème des sous-groupes de congruence fournit des résultats comme le suivant : pour $n \geqq 2$, le groupe $\mathrm{Sp}(2n, \mathbf{Z})^{\sim}$ image inverse de $\mathrm{Sp}(2n, \mathbf{Z})$ dans le revêtement universel de $\mathrm{Sp}(2n, \mathbf{R})$ (une extension centrale de $\mathrm{Sp}(2n, \mathbf{Z})$ par $\pi_1 \mathrm{Sp}(2n, \mathbf{R}) = \mathbf{Z}$) n'est pas séparé pour la topologie des sous-groupes d'indice fini. Plus précisément, tout sous-groupe d'indice fini de $\mathrm{Sp}(2n, \mathbf{Z})^{\sim}$ contient $2\pi_1 \mathrm{Sp}(2n, \mathbf{R})$.

A variant of known methods to handle the congruence subgroup problem yields results like the following. Let $\mathrm{Sp}(2n, \mathbf{Z})^{\sim}$ *be the inverse image of* $\mathrm{Sp}(2n, \mathbf{Z})$ *in the universal covering of* $\mathrm{Sp}(2n, \mathbf{R})$*; it is a central extension of* $\mathrm{Sp}(2n, \mathbf{Z})$ *by* $\pi_1 \mathrm{Sp}(2n, \mathbf{R}) \simeq \mathbf{Z}$. If $n \geqq 2$, the group $\mathrm{Sp}(2n, \mathbf{Z})^{\sim}$ *is not residually finite : any subgroup of finite index contains* $2\pi_1 \mathrm{Sp}(2n, \mathbf{R})$.

1. GROUPES S-ARITHMÉTIQUES. — Soit G un groupe presque simple simplement connexe isotrope sur un corps global F. Pour simplifier les énoncés, nous supposerons aussi que G(F) est parfait (i. e. égal à son groupe des commutateurs); c'est le cas, sauf peut-être si G est une forme trialitaire de D_4. Soit par ailleurs S un ensemble fini de places de F, contenant toutes les places à l'infini, et supposons que

(i) $$\sum_{v \in S} \mathrm{rang}(G/F_v) \geqq 2.$$

Pour chaque place v de F, posons $G_v = G(F_v)$. Pour chaque ensemble fini T de places, posons de même $G_T = \prod_{v \in T} G_v$ et $G_{T'} = \prod_{v \notin T} G_v$ (produit restreint) : pour **A** l'anneau des adèles de F, on a $G(\mathbf{A}) = G_T \times G_{T'}$.

Un sous-groupe de G(F) est dit de S-congruence s'il est l'image inverse d'un sous-groupe compact ouvert de $G_{S'}$. Il est dit S-arithmétique s'il est commensurable à un sous-groupe de S-congruence, i.e. s'il contient, avec un indice fini, un sous-groupe d'indice fini dans un groupe de S-congruence. Les sous-groupes de S-congruence (resp. S-arithmétiques) forment un système fondamental de voisinages de l'origine pour une topologie (de groupe topologique) $\mathcal{T}(c)$ [resp. $\mathcal{T}(a)$] sur G(F). Pour Γ un sous-groupe de S-congruence fixe, on obtient encore un système fondamental de voisinages en ne considérant que les sous-groupes de S-congruence distingués dans Γ (resp. que les sous-groupes distingués d'indice fini de Γ). Ceci assure l'existence du complété $G(F)(c)$ [resp. $G(F)(a)$] de G(F) pour $\mathcal{T}(c)$ [resp. $\mathcal{T}(a)$]. La topologie $\mathcal{T}(c)$ est la topologie induite de celle de $G_{S'}$. Puisque G(F) est dense dans $G_{S'}$ (théorème d'approximation forte), on a $G(F)(c) = G_{S'}$. Le complété $G(F)(a)$ de G(F) est une extension de $G(F)(c) = G_{S'}$ par le groupe profini $C(S, G) = \lim\,\mathrm{proj}\,\Gamma/\Delta$ (limite projective sur les couples $\Delta \subset \Gamma$, avec Δ distingué d'indice fini dans Γ et Γ de S-congruence).

Pour G de rang $\geqq 2$, Raghunathan ([1]) a montré que :

(ii) $G(F)(a)$ *est une extension centrale de* $G(F)(c) = G_{S'}$,

et il achève de vérifier que la même conclusion vaut sous la seule hypothèse (i).

Soient $G_S^{\sim}$ une extension centrale topologique de G_S par un groupe discret A, et $G(F)^{\sim}$ l'image inverse de G(F) dans $G_S^{\sim}$. Un sous-groupe de $G(F)^{\sim}$ sera dit de S-congruence s'il est image inverse d'un sous-groupe de S-congruence de G(F), et S-arithmétique s'il est commensurable à un sous-groupe de S-congruence. On note encore $\mathcal{T}(c)$ et $\mathcal{T}(a)$ les topologies correspondantes, et $G(F)^{\sim}(c)$, $G(F)^{\sim}(a)$ les complétés séparés pour ces topologies. On a encore $G(F)^{\sim}(c) = G_{S'}$, tandis que $G(F)^{\sim}(a)$ est extension de $G_{S'}$ par un groupe profini $C^{\sim}(S, G)$, lui-même extension de $C(S, G)$ par

$$A^{\wedge} = \text{lim proj } A/A \cap \Gamma \ (\Gamma \text{ S-arithmétique}).$$

PROPOSITION 1. — *Si la condition* (ii) *est vérifiée*, $G(F)^{\sim}(a)$ *est une extension centrale de* $G(F)^{\sim}(c) = G_{S'}$.

Rappelons que, si un groupe $\tilde{H}$ est une extension centrale d'un groupe H, l'application commutateur $\tilde{H} \times \tilde{H} \to \tilde{H}$ se factorise par une application, encore notée $(\ ,\ ) : H \times H \to \tilde{H}$. En particulier, le groupe $G(F)^{\sim}(a)$ étant une extension centrale de $G(F)(a)$ par $\hat{A}$, l'application commutateur : $C^{\sim}(S, G) \times G(F)^{\sim}(a) \to G(F)^{\sim}(a)$ se factorise par $C(S, G) \times G(F)(a)$. D'après (ii), elle se factorise par une application bimultiplicative

$$C(S, G) \times G(F)(a) \to \hat{A};$$

puisque $G(F)$ est parfait, et dense dans $G(F)(a)$, celle-ci est triviale.

En termes plus concrets, la proposition signifie que pour tout sous-groupe S-arithmétique Δ, on a :

(1 *a*) Pour tout conjugué Δ^g de $\Delta\,(g \in G(F)^{\sim})$, il existe un groupe de S-congruence Γ tel que $\Gamma \cap \Delta = \Gamma \cap \Delta^g$.

(1 *b*) $G(F)^{\sim}$ agit trivialement sur le groupe fini $C_\Delta = \text{lim proj } \Gamma/\Gamma \cap \Delta$.

Ces conditions équivalent encore à

(1 *c*) Pour tout $g \in G(F)$, il existe Γ de S-congruence tel que $(g, \Gamma) \subset \Delta$.

On a $C^{\sim}(S, G) = \text{lim proj } C_\Delta$.

2. EXTENSIONS CENTRALES DE GROUPES ADÉLIQUES. — Nous supposerons dorénavant que : (iii) le groupe $G_S^{\sim}$ est parfait.

Le cas le plus intéressant serait celui où $G_S^{\sim}$ est l'extension centrale universelle de G_S par un groupe discret (le « revêtement universel » de G_S), mais nous ne tenons pas à supposer l'existence d'une telle extension universelle.

Une extension centrale topologique E de G(A) par un groupe discret X est déterminée par les extensions E_S et $E_{S'}$ de G_S et $G_{S'}$ par X images inverses de G_S et $G_{S'}$ dans E : parce que G_S est parfait, on a $E \xleftarrow{\sim} (E_S \times E_{S'})/\{(x, -x) \mid x \in X\}$. Si l'extension E_S est dominée par G_S, i. e. se déduit de G_S en poussant par $f : A \to X$, l'application f est unique, et la donnée de E revient à celle de l'extension $E_{S'}$, et de f (équivalence de catégorie); on a $E \xleftarrow{\sim} G_S^{\sim} \times E_{S'}/\{(a, -f(a)) \mid a \in A\}$.

Soit $\mathscr{L}$ la catégorie des extensions centrales topologiques de G(A) par un groupe fini, scindées au-dessus de G(F), et avec E_S dominé par $G_S^{\sim}$:

$$\begin{tikzcd} 1 \arrow[r] & X \arrow[r] & E \arrow[r] & G(A) \arrow[r] & 1 \\ & & & G(F) \arrow[ul, "s"] \arrow[u, hook] & \end{tikzcd}$$

Il reviendrait au même d'exiger « scindable au-dessus de G(F) » : puisque G(F) est parfait, le scindage, s'il existe, est unique. La catégorie $\mathscr{L}$ est filtrante à gauche. Pour (E, *s*) dans $\mathscr{L}$, l'adhérence dans E de (image de $G_S^{\sim}$) . *s* G(F) s'envoie sur G(A) : elle s'envoie sur un fermé, car X est fini, et contient G_S . G(F) qui est dense (approximation forte). La sous-catégorie L de $\mathscr{L}$ formée des (E, *s*) avec (image de $G_S^{\sim}$) . *s* G(F) dense dans E est donc cofinale; puisqu'il y a au plus une flèche entre deux objets de L, elle se réduit à un ensemble ordonné filtrant.

PROPOSITION 2. — *Sous les hypothèses (ii) et (iii), nous construisons un isomorphisme naturel entre* $C^{\sim}(S, G)$ *et la limite projective sur* $\mathscr{L}$, *ou* L, lim proj X. *Via cet isomorphisme, l'application naturelle de* A *dans* $C^{\sim}(S, G)$ *est la limite des* $-f : A \to X$, f *étant tel que* E_S *se déduise de* $G_S^{\sim}$ *par* f.

Soit E une extension centrale topologique de G(A) par un groupe discret X. Se donner un scindage s de E au-dessus de G(F) revient à se donner un isomorphisme entre l'extension de G(F) par X déduite de E_S, et l'opposée de celle déduite de $E_{S'}$. Pour E_S dominé par $G_S^{\sim}$, et f comme ci-dessus, cela revient à se donner un diagramme commutatif

$$\begin{tikzcd} 1 \arrow[r] & X \arrow[r] & E_{S'} \arrow[r] & G_{S'} \arrow[r] & 1 \\ 1 \arrow[r] & A \arrow[r] \arrow[u, "-f"] & G(F)^{\sim} \arrow[r] \arrow[u, "\iota"'] & G(F) \arrow[r] \arrow[u] & 1. \end{tikzcd}$$

De là une équivalence entre la catégorie $\mathscr{L}$ et celle, $\mathscr{L}'$, des diagrammes commutatifs

$$\begin{tikzcd} 1 \arrow[r] & X \arrow[r] & E_{S'} \arrow[r, "q"] & G_{S'} \arrow[r] & 1 \\ & & G(F)^{\sim} \arrow[r] \arrow[u, "t"'] & G(F) \arrow[u, hook] & \end{tikzcd} \tag{1}$$

($E_{S'}$ extension centrale topologique de $G_{S'}$ par un groupe fini) : on reconstruit E comme étant $G_S^{\sim} \times E_{S'}/\{(a, ta) \mid a \in A\}$, et le scindage sur G(F) par $s(g) = (\tilde{g}, t\tilde{g})$ mod les (a, ta) pour $\tilde{g} \in G(F)^{\sim} \subset G_S^{\sim}$ d'image g dans G(F). La sous-catégorie L de $\mathscr{L}$ correspond à celle, L', des diagrammes (1) avec t d'image dense.

Soient $(E_{S'}, t)$ dans L', et $\mathscr{T}$ la topologie sur $G(F)^{\sim}$ induite par celle de $E_{S'}$. Si K est un sous-groupe compact ouvert de $E_{S'}$, disjoint de X, les intersections de $\Delta = t^{-1} K$ avec les sous-groupes de S-congruence forment un système fondamental de voisinages pour $\mathscr{T}$. Pour Γ un sous-groupe de S-congruence défini par un sous-groupe compact ouvert $K_1 \subset q K$, on a de plus

$$X \xrightarrow{\sim} XK/K \xleftarrow{\sim} q^{-1} K_1/(K \cap q^{-1} K_1) \xleftarrow{\sim} \Gamma/\Delta \cap \Gamma \xleftarrow{\sim} C_{\Delta}. \tag{2}$$

Puisque X est fini, Δ est S-arithmétique. Réciproquement, la proposition 1 assure qu'un système fondamental de groupes S-arithmétiques est ainsi obtenu : l'ensemble ordonné filtrant L' s'identifie à celui des germes (pour la topologie de S-congruence) de groupes S-arithmétiques, et l'isomorphisme de la proposition 2 est défini comme la limite projective des isomorphismes (2).

3. GROUPES QUASI DÉPLOYÉS. — Soit μ le groupe des racines de l'unité de F et, pour chaque place non complexe v de F, soit μ_v le groupe des racines de l'unité de F_v. Pour v complexe, on pose $\mu_v = \{1\}$. Deodhar a montré que, pour G quasi-déployé, il existe une extension topologique centrale universelle $G_v^{\sim}$ de G_v par un groupe discret (le « revêtement universel »), et que pour v non réelle, son noyau $\pi_1(G_1)$ est canoniquement un quotient de μ_v. J'ai complété ce résultat en montrant qu'en fait $\pi_1(G_v) = \mu_v$. Pour v réelle, on a $\pi_1(G_v) = \mathbf{Z}$, ou $\mathbf{Z}/2$. Dans tous les cas, μ_v apparaît comme un quotient de $\pi_1(G_v)$.

Pour presque tout v, l'extension G_v se scinde au-dessus du sous-groupe compact maximal naturel de G_v. Ceci permet de définir le produit restreint des G_v, une extension de G(A) par la somme des $\pi_1(G_v)$. Poussons-la par

$$R : \oplus \pi_1(G_v) \to \oplus \mu_v \xrightarrow{\sigma} \mu : \sigma((x_v)) = \prod_v x_v^{[\mu_v : \mu]}.$$

On obtient une extension centrale de $G(A)$ par μ, et il résulte de Deodhar [2] et C. Moore [3] que c'est l'extension centrale topologique universelle de $G(A)$ par un groupe discret, qui se scinde au-dessus de $G(F)$:

$$\begin{tikzcd} 1 \arrow[r] & \mu \arrow[r] & G(A)^{\sim} \arrow[r] & G(A) \arrow[r] & 1 \\ & & & G(F) \arrow[ul] \arrow[u] & \end{tikzcd} \tag{3}$$

Prenons pour $G_S^{\sim}$ le revêtement universel de G_S, et notons R_S la restriction de R à $\pi_1 G_S = \prod_{v \in S} \pi_1 G_v$. La proposition 2 identifie le complété $G(F)^{\sim}(a)$ de $G(F)^{\sim}$ à l'image inverse $G(A)_{S'}^{\sim}$ de $G_{S'} = G(F)^{\sim}(c)$ dans (3), et fournit un diagramme commutatif exact

$$\begin{tikzcd} 1 \arrow[r] & \mu \arrow[r] & G(A)_{S'}^{\sim} \arrow[r] & G_{S'} \arrow[r] & 1 \\ & \prod_{v \in S} \pi_1(G_v) \arrow[u, "-R_S"] \arrow[r] & G(F)^{\sim}(a) \arrow[u, "\iota"] \arrow[r] & G(F)(a) \arrow[u] \arrow[r] & 1 \end{tikzcd} \tag{4}$$

En particulier

Théorème. — *Soient G/F quasi déployé, et $G(F)^{\sim}$ l'image inverse de $G(F)$ dans le revêtement universel de G_S. Si $\sum_{v \in S} \operatorname{rang}(G_v) \geqq 2$, l'intersection des sous-groupes S-arithmétiques de $G(F)^{\sim}$ est le noyau de $R_S : \prod_{v \in S} \pi_1(G_v) \to \mu$.*

Pour $Sp(2n, \mathbf{Q})$, et $S = \infty$, c'est le résultat annoncé dans l'introduction. Pour $SL(n, K)$, avec K quadratique réel, et $S = \infty$, le résultat obtenu généralise celui de J. Millson [4].

Problème. — Tout sous-groupe discret de covolume fini du revêtement universel de $Sp(2n, \mathbf{R})$ $(n \geqq 2)$ contient-il $2\pi_1 Sp(2n, \mathbf{R})$? [5].

4. Le système de facteurs des fonctions θ. — Lorsque la condition (i) n'est pas vérifiée, on ne dispose plus de la proposition 1; il reste néanmoins possible d'étudier les sous-groupes S-arithmétiques vérifiant une condition de type (1 *a*).

Soient donc S un ensemble fini non vide de places, contenant toutes les places à l'infini, et $T \supset S$ tel que (G, T) vérifie la condition (ii). Le cas intéressant est celui où S est réduit à une place, en laquelle G est de rang 1. Soient encore $G_S^{\sim}$ une extension centrale topologique de G_S par un groupe discret, et $G(F)^{\sim}$ l'image inverse de $G(F)$ dans $G_S^{\sim}$. Pour Δ un sous-groupe S-arithmétique de $G(F)^{\sim}$, considérons la condition :

$(\star)$ il existe un sous-groupe T-arithmétique U de $G(F)^{\sim}$, tel que, pour tout conjugué Δ^g de Δ $(g \in U)$, il existe un groupe de S-congruence Γ tel que $\Gamma \cap \Delta = \Gamma \cap \Delta^g$ (U-invariance du germe de Δ).

Proposition 3. — *Le complété $G(F)^{\sim}(a^*)$ de $G(F)^{\sim}$ pour la topologie des sous-groupes S-arithmétiques vérifiant $(\star)$ est une extension centrale de $G(F)^{\sim}(c) = G_{S'}$.*

En termes plus concrets, il nous faut vérifier que si (U, Δ) vérifie $(\star)$, alors Δ vérifie (1 *c*). Pour le prouver, il est loisible de rapetisser au préalable U et Δ. En particulier, on peut supposer que $\Delta \subset U$ (remplacer Δ par $\Delta \cap U$). Le groupe U agit alors par conjugaison sur le groupe fini $C^{U}_{\Delta} = \lim \operatorname{proj} \Gamma \cap U / \Gamma \cap \Delta$ (Γ de S-congruence); remplaçant U par le noyau de cette action, et Δ par un $\Delta \cap \Gamma$, on peut supposer de plus que U agit trivialement sur C^{U}_{Δ}.

Puisque U est T-arithmétique, son complété $U(c) \subset G_{S'}$ est d'indice fini dans un sous-groupe $G_{T-S} \times L$, avec $L \subset G_{T'}$ compact ouvert; le groupe G_{T-S} n'ayant pas de sous-groupe ouvert d'indice fini, $U(c)$ lui-même est de la forme $G_{T-S} \times L$. La condition ($\star$) assure que les $\Delta \cap \Gamma$ (Γ de S-congruence) forment un système fondamental de voisinages de l'origine pour une topologie (de groupe topologique) sur U. Le complété $U(\Delta)$ correspondant est extension de $U(c)$ par C^{U}_{Δ} — donc une extension centrale de $G_{T-S} \times L$. Remplaçons L par un sous-groupe ouvert L_1 au-dessus duquel cette extension soit triviale, et U et Δ par les images inverses de L_1. Puisque G_{T-S} est parfait, une extension centrale de $G_{T-S} \times L$ est déterminée par ses restrictions aux deux facteurs, et ceci nous ramène au cas où l'extension centrale $U(\Delta)$ de $G_{T-S} \times L$ est l'image inverse d'une extension centrale $G^{\sim}_{T-S}$ de G_{T-S} par C^{U}_{Δ}. Par construction, U se relève dans $G^{\sim}_{T-S}$ et Δ est l'image inverse d'un sous-groupe compact ouvert K de $G^{\sim}_{T-S} \times L$:

$$\begin{tikzcd} K \arrow[r, hook] & G^{\sim}_{T-S} \times L \\ \Delta \arrow[u] \arrow[r] & U \arrow[u] \end{tikzcd} \tag{5}$$

Soient $G(F)^{\sim}_{T}$ l'extension centrale de $G(F)$ image inverse de $G(F)$ dans $G^{\sim}_{T} = G^{\sim}_{S} \times G^{\sim}_{T-S}$, et $\tilde{U}$ le relèvement (5) de U dans $G(F)^{\sim}_{T}$. Pour $g \in G(F)$, la proposition 1 assure $(g, \Gamma_T) \subset \tilde{U}$ pour Γ_T de T-congruence défini par $L' \subset L$ assez petit. Si le sous-groupe de S-congruence Γ défini par $K' \subset G_{T-S} \times L'$, d'image inverse K'' dans $G^{\sim}_{T-S} \times L'$, est assez petit pour que $(g, K') \subset K$, on a $(g, \Gamma) \subset \Delta$, ce qui vérifie (1 *c*).

Le noyau $C^{\sim *}(S, G) = \operatorname{Ker}(G(F)^{\sim}(a^*) \to G(F)(c))$ est encore décrit par la proposition 2 (avec la même démonstration), et le calcul peut être mené à terme dans le cas quasi déployé (*cf.* le n° 3). Voici une application, avec $G = SL(2, \mathbf{Q})$, $S = \{\infty\}$, et $T = \{\infty, p\}$. On pose $SL(2, \mathbf{R})^{\sim}$ = le revêtement double de $SL(2, \mathbf{R})$. On peut interpréter les systèmes de facteurs des fonctions θ, restreints à des sous-groupes de congruence arbitrairement petits de $SL(2, \mathbf{Z})$, comme définissant un germe τ (pour la topologie des sous-groupes de congruence) de relèvements de $SL(2, \mathbf{Z})$ dans $SL(2, \mathbf{R})^{\sim}$. Ce germe est invariant par $GL(2, \mathbf{Q})$. Si on définit une forme modulaire de poids demi-entier $k/2$ comme étant une fonction sur le demi-plan de Poincaré qui, sous l'action d'un sous-groupe de congruence de $SL(2, \mathbf{Z})$, se transforme comme la fonction θ d'une forme quadratique à k variables, cela revient à dire que, si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbf{Q})$ est de déterminant positif, et que f est modulaire de poids $k/2$, alors $f(-z^{-})^{-}$ et $(cz+d)^{k/2} f[(az+b)/(cz+d)]$ le sont également. Réciproquement, on a :

PROPOSITION 4. — *Quel que soit p premier, le germe τ est l'unique germe de relèvement de* $SL(2, \mathbf{Z})$ *dans* $SL(2, \mathbf{R})^{\sim}$ *qui soit invariant par un sous-groupe d'indice fini de* $SL(2, \mathbf{Z}[1/p])$.

Les arguments qui mènent au théorème du n° 3 montrent que tout sous-groupe arithmétique de $SL(2, \mathbf{Z})$, de germe invariant par un sous-groupe d'indice fini de $SL(2, \mathbf{Z}[1/p])$, est de congruence.

Soient $\Gamma \subset SL(2, \mathbf{Z})$ de congruence, et $\tau_1 = \tau_2$ deux relèvements de Γ dans $SL(2, \mathbf{R})^{\sim}$.

Soit Δ le sous-groupe de Γ où $\tau_1 = \tau_2$. Si les germes de τ_1 et τ_2 sont distincts, et invariants par un groupe $\{p\}$-arithmétique, Δ vérifie ($\star$), et n'est pas de congruence.

(*) Séance du 3 juillet 1978.

(1) M. S. RAGHUNATHAN, *Publ. Math. I.H.E.S.*, 46, 1976, p. 107-162.

(2) V. V. DEODHAR, *On central extensions of rational points of algebraic groups* (à paraître).

(3) C. C. MOORE, *Publ. Math. I.H.E.S.*, 35, 1968, p. 5-70.

(4) J. MILLSON, *Real Vector Bundles with Discrete Structure Groups* (à paraître).

(5) J'apprends de Mostow qu'un tel sous-groupe Γ contient en tout cas un sous-groupe d'indice fini de $\pi_1 \operatorname{Sp}(2n, \mathbf{R})$: on vérifie que la projection de Γ dans $\operatorname{Sp}(2n, \mathbf{R})$ est discrète, sans quoi l'algèbre de Lie de son adhérence serait centrale non triviale.

Institut des Hautes Études scientifiques, 91440 *Bures-sur-Yvette*