HIDEYA MATSUMOTO

Sur les sous-groupes arithmétiques des groupes semi-simples déployés

Annales scientifiques de l'É.N.S. 4e série, tome 2, nº 1 (1969), p. 1-62
<http://www.numdam.org/item?id=ASENS_1969_4_2_1_1_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 2, 1969, p. 1 à 62.

SUR LES SOUS-GROUPES ARITHMÉTIQUES DES GROUPES SEMI-SIMPLES DÉPLOYÉS

PAR HIDEYA MATSUMOTO.

INTRODUCTION.

Soient k un corps de nombres algébriques et $\mathfrak{o}$ l'anneau des entiers de k. Soient G un groupe algébrique linéaire connexe défini sur k et G_k le groupe des points rationnels de G. Si l'on note $G_{\mathfrak{o}}$ le groupe des points entiers de G relativement à un plongement donné de G dans un groupe linéaire GL_n, un sous-groupe Γ' de G_k est appelé sous-groupe arithmétique si $\Gamma' \cap G_{\mathfrak{o}}$ est d'indice fini dans Γ' et dans $G_{\mathfrak{o}}$. Pour tout idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$, le sous-groupe $\Gamma_{\mathfrak{q}}$ de $G_{\mathfrak{o}}$ formé des éléments g tels que $g \equiv 1$ modulo $\mathfrak{q}$ est un tel sous-groupe de G_k. Un sous-groupe arithmétique Γ' de G_k est appelé sous-groupe de congruence si Γ' contient le sous-groupe $\Gamma_{\mathfrak{q}}$ de $G_{\mathfrak{o}}$ pour un idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$. Ces définitions de sous-groupes arithmétique et de congruence ne dépendent pas du choix du plongement de G dans un groupe linéaire.

Le problème des groupes de congruence pour G_k consiste à savoir si tout sous-groupe arithmétique de G_k est un sous-groupe de congruence, autrement dit si tout sous-groupe d'indice fini dans $G_{\mathfrak{o}}$ contient $\Gamma_{\mathfrak{q}}$ pour un idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$. Le but principal du présent Mémoire est de résoudre ce problème pour les groupes simples simplement connexes G déployés sur k et de rang ≥ 2. Nous traitons également un problème analogue pour les groupes $G_{\mathfrak{o}}$ où $\mathfrak{o}$ est un anneau de Dedekind dit de type arithmétique.

Au chapitre I, nous étudions les propriétés d'une suite exacte de groupes localement compacts liée au problème des groupes de congruence. Soit G un groupe simple simplement connexe déployé sur k. Mettons une topologie T_a [resp. T_c] sur G_k en prenant comme base de voisinages de l'élément neutre les sous-groupes arithmétiques [resp. de congruence] de G_k, et notons $\hat{G}_k$ [resp. $\overline{G}_k$] le complété de G_k pour T_a [resp. T_c]; ces complétés sont des groupes localement compacts totalement discontinus. Comme T_a est plus fine que T_c, on a un morphisme canonique π de $\hat{G}_k$ dans $\overline{G}_k$; le morphisme π est surjectif et propre. Le problème des groupes de congruence revient à savoir si le noyau $C(G_k)$ de π se réduit à l'élément neutre. On sait, d'après le théorème de l'approximation forte, que $\overline{G}_k$ s'identifie au groupe adélifié $G_{A_k^f}$, où A_k^f désigne l'anneau des adèles finis de k, c'est-à-dire le produit restreint des complétés k_v de k relatif aux anneaux $\mathfrak{o}_v$ des entiers dans k_v, v parcourant l'ensemble des places finies de k. D'autre part, l'extension $\hat{G}_k$ de $G_{A_k^f}$ est triviale au-dessus du groupe G_k, regardé comme groupe discret, contenu dans $G_{A_k^f}$.

Nous démontrons pour les groupes $G_{\mathfrak{o}}$ un théorème de réduction sur le rang de G, analogue à un théorème de stabilité de H. Bass [2] pour les groupes $SL_n(\mathfrak{o})$, et nous en déduisons que, si G est de rang $\geqq 2$, le noyau $C(G_k)$ de π est central dans $\hat{G}_k$. En outre, l'extension $\hat{G}_k$ de $G_{A_k^f}$ possède une propriété universelle qui la caractérise entre toutes les extensions centrales de $G_{A_k^f}$.

Les schémas en groupes sur **Z** associés par C. Chevalley [15] aux groupes semi-simples joueront un rôle fondamental dans le premier chapitre comme dans le deuxième, et d'ailleurs ils nous permettront de soumettre les groupes de divers types à un traitement unifié, ne serait-ce que pour éviter des calculs de matrices.

Le chapitre II est consacré à l'étude des extensions centrales de G_{k_t} où G est un groupe simple simplement connexe déployé sur un corps topologique k_t infini; le groupe G_{k_t} est muni de la topologie définie à partir de celle de k_t. Si A est un groupe abélien topologique, les classes d'extensions centrales de G_{k_t} par A forment, avec la multiplication de Baer, le groupe de cohomologie $H^2(G_{k_t}, A)$. Nous ramenons la détermination des extensions centrales de G_{k_t} par A à celle de certains cocycles sur $k_t^\times$ à valeurs dans A, en suivant la méthode de R. Steinberg [30] et de C. Moore [26]; c'est donc la décomposition de Bruhat de G_{k_t} qui y joue un rôle primordial.

On appellera *cocycle de Steinberg* toute application c de $k_t^\times \times k_t^\times$ dans A satisfaisant aux équations et aux conditions suivantes :

(S 1) $c(x, y)\, c(xy, z) = c(x, yz)\, c(y, z)$;

(S 2) $c(1,1) = 1$; $c(x, y) = c(x^{-1}, y^{-1})$;

(S 3) $c(x, y) = c(x, (1-x)y)$ *si* $x \neq 1$;

(S 0) *La fonction* $c(x, y)$ *est continue dans* $k_t^\times \times k_t^\times$, *et, quand on convient que* $c(0,1) = 1$, *la fonction* $c(x, 1-xy)$ *de* (x, y), *définie sur un voisinage de* $(0, 0)$ *dans* $k_t \times k_t$, *est continue en* $(0, 0)$.

Soient alors $S(k_t^\times, A)$ le groupe des cocycles de Steinberg sur $k_t^\times$ à valeurs dans A, et $S^0(k_t^\times, A)$ son sous-groupe formé des éléments c qui sont bilinéaires comme applications de $k_t^\times \times k_t^\times$ dans A. Le théorème principal du chapitre II affirme que le groupe $H^2(G_{k_t}, A)$ est isomorphe à $S(k_t^\times, A)$ ou à $S^0(k_t^\times, A)$ suivant que G est isomorphe ou non à un groupe symplectique. Pour $G = SL_2$, ce résultat a été essentiellement obtenu par C. Moore [26].

Soient k_v un corps localement compact non discret, et μ_v le groupe des racines de l'unité contenues dans k_v. Si $k_v \neq \mathbf{C}$, le symbole de restes normiques $(x, y)_{m, k_v}$, m étant l'ordre de μ_v, est un cocycle de Steinberg bilinéaire c^0 sur $k_v^\times$ à valeurs dans μ_v. Par ailleurs, comme $\mathbf{R}$ est un corps ordonné, on définit comme suit un cocycle de Steinberg c_0, non bilinéaire, sur $\mathbf{R}^\times$ à valeurs dans $\mathbf{Z}$: $c_0(x, y) = 1$ si $x < 0$, $y < 0$; $c_0(x, y) = 0$ sinon.

Au chapitre III, nous rappelons d'abord des généralités sur les extensions centrales des groupes localement compacts; notamment les notions, dues à C. Moore [26], de revêtement universel, de groupe fondamental et de groupe fondamental relatif. Puis nous combinons les théorèmes des chapitres précédents avec deux résultats arithmétiques de C. Moore [26] sur la détermination des cocycles de Steinberg pour un corps local et sur l'unicité des formules de réciprocité dans un corps global.

En utilisant le premier de ces résultats, nous voyons que, si k_v est un corps local ultramétrique [resp. le corps $\mathbf{R}$], l'extension de G_{k_v} correspondant au cocycle de Steinberg canonique c^0 [resp. c_0 ou c^0 suivant que G est isomorphe ou non à un groupe symplectique] est un revêtement universel de G_{k_v}; pour $k_v = \mathbf{C}$, il est bien connu que $G_{\mathbf{C}}$ est lui-même simplement connexe au sens topologique.

Soient k un corps global et A_k l'anneau des adèles de k. Le théorème de C. Moore sur les formules de réciprocité entraîne que le groupe fondamental relatif du groupe adélifié G_{A_k} par rapport à son sous-groupe G_k est isomorphe au groupe μ_k des racines de l'unité contenues dans k; ce qui signifie essentiellement qu'il existe une extension centrale $\tilde{G}_{A_k}$ de G_{A_k} par μ_k qui est triviale au-dessus de G_k, et que toute extension centrale de G_{A_k} par un groupe abélien localement compact B, triviale au-dessus de G_k, se déduit de $\tilde{G}_{A_k}$ par un morphisme de μ_k dans B uniquement déterminé.

De tels revêtements de G_{k_v} et de G_{A_k} ont été remarqués et construits pour les groupes SL_n et Sp_{2n} par A. Weil [32], T. Kubota [19], C. Moore [26] et H. Bass, J. Milnor et J.-P. Serre [4]. Le cas du corps $\mathbf{R}$ remonte, bien entendu, à É. Cartan [11], qui avait d'ailleurs déterminé le groupe fondamental $\pi_1(G_{\mathbf{R}})$ pour tout groupe simple simplement connexe G sur $\mathbf{R}$, déployé ou non.

Nous tirons de ces théorèmes une solution au problème des groupes de congruence pour les groupes simples simplement connexes G de rang $\geqq 2$ et déployés sur un corps de nombres algébriques k : le noyau $C(G_k)$ du morphisme π de $\hat{G}_k$ sur $\overline{G}_k$ est isomorphe à μ_k si k est totalement imaginaire; sinon, $C(G_k)$ se réduit à l'élément neutre. En particulier, si k possède au moins un conjugué réel, tout sous-groupe arithmétique de G_k est un sous-groupe de congruence. On voit aussi que, si G est de rang $\geqq 2$, tout sous-groupe arithmétique de G_k contient un sous-groupe d'indice fini engendré par des éléments unipotents.

Cette solution au problème des groupes de congruence avait été obtenue, pour les groupes SL_n $(n \geqq 3)$ et Sp_{2n} $(n \geqq 2)$ sur $\mathbf{Q}$, indépendamment par J. Mennicke ([22], [23]) et par H. Bass, M. Lazard et J.-P. Serre [3], et ensuite pour ces mêmes groupes sur un corps de nombres arbitraire par Bass, J. Milnor et Serre [4]. Le cas de SL_2 a récemment été résolu par Serre (*voir* [29]).

Cette thèse a été réalisée sous la direction de M. F. Bruhat, qui m'avait suggéré l'idée d'entreprendre cette étude. Je lui en exprime toute ma gratitude. Je tiens à remercier vivement M. J.-P. Serre pour les conseils qu'il n'a cessé de me prodiguer tant au cours de l'élaboration de mon travail que pendant sa rédaction définitive. Je remercie également M. P. Samuel, qui a bien voulu me proposer un second sujet de thèse.

CHAPITRE I.

Sous-groupes arithmétiques d'un groupe simple déployé.

1. Nous allons dans ce numéro formuler le problème des groupes de congruence, que nous étudierons ensuite pour les groupes simples simplement connexes déployés.

Soit k une extension de $\mathbf{Q}$ de degré fini ou un corps de fonctions algébriques de dimension 1 sur un corps fini. Un sous-anneau $\mathfrak{o}$ de k sera appelé *anneau de Dedekind de type arithmétique*, s'il existe un ensemble fini non vide S de places de k contenant les places archimédiennes et tel que $\mathfrak{o}$ soit l'ensemble des éléments x de k tels que $v(x) \leqq 1$ pour toute place $v \notin S$; où l'on a noté la valuation v multiplicativement. S'il en est ainsi, k est le corps des fractions de $\mathfrak{o}$ et S est uniquement déterminé par $\mathfrak{o}$. Les idéaux premiers de $\mathfrak{o}$ correspondent canoniquement avec les places $v \notin S$ de k.

Soient G un groupe algébrique linéaire connexe défini sur k et G_k le groupe des points rationnels de G. On choisit un plongement de G dans un groupe linéaire GL_m et l'on considère le groupe $G_{\mathfrak{o}}$ des points de G à valeurs dans $\mathfrak{o}$, où $\mathfrak{o} = \mathfrak{o}(S)$ est l'anneau de Dedekind de type arithmétique défini à partir d'un ensemble S de places de k. Un sous-groupe Γ' de G_k est appelé *sous-groupe* S-*arithmétique* si $\Gamma' \cap G_{\mathfrak{o}}$ est d'indice fini dans Γ' et dans $G_{\mathfrak{o}}$. Un sous-groupe S-arithmétique Γ' de G_k est appelé *sous-groupe de* S-*congruence* si Γ' contient, pour un idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$, le sous-groupe $\Gamma_{\mathfrak{q}}$ de $G_{\mathfrak{o}}$ formé des éléments g tels que $g \equiv 1$ modulo $\mathfrak{q}$.

On voit aisément que ces définitions ne dépendent pas du choix du plongement de G dans un groupe linéaire GL_m. Par suite, on peut définir sur G_k une topologie de groupe $T_a(S)$ [resp. $T_c(S)$] en prenant comme base de voisinages de e les sous-groupes S-arithmétiques [resp. de S-congruence] de G_k. Soit donc $\widehat{G_k(S)}$ [resp. $\overline{G_k(S)}$] le complété de G_k par rapport à $T_a(S)$ [resp. à $T_c(S)$]; les groupes $\widehat{G_k(S)}$ et $\overline{G_k(S)}$ sont localement compacts et totalement discontinus. Puisque $T_a(S)$ est plus fine que $T_c(S)$, on a un morphisme canonique π de $\widehat{G_k(S)}$ dans $\overline{G_k(S)}$.

Le complété $\hat{G}_{\mathfrak{o}}$ [resp. $\overline{G}_{\mathfrak{o}}$] de $G_{\mathfrak{o}}$ par rapport à $T_a(S)$ [resp. à $T_c(S)$] est un sous-groupe ouvert compact de $\widehat{G_k(S)}$ [resp. de $\overline{G_k(S)}$]. Le groupe $\hat{G}_{\mathfrak{o}}$ n'est autre que le complété de $G_{\mathfrak{o}}$ par rapport à la topologie des sous-groupes d'indice fini. On voit aisément que la restriction de π à $\hat{G}_{\mathfrak{o}}$ a pour image $\overline{G}_{\mathfrak{o}}$ et pour noyau un groupe profini $C(G_{\mathfrak{o}})$. Par conséquent, le morphisme π applique $\widehat{G_k(S)}$ sur $\overline{G_k(S)}$, et le noyau $C^S(G_k)$ de π, qui s'identifie canoniquement avec $C(G_{\mathfrak{o}})$, est un groupe profini.

On a ainsi une suite exacte de groupes localement compacts :

$$1 \to C^S(G_k) \to \widehat{G_k(S)} \xrightarrow{\pi} \overline{G_k(S)} \to 1. \tag{1.1}$$

Le problème des groupes de congruence pour G_k relatif à S consiste à savoir si $C^S(G_k)$ se réduit à l'élément neutre, c'est-à-dire si tout sous-groupe d'indice fini dans $G_{\mathfrak{o}}$ contient $\Gamma_{\mathfrak{q}}$ pour un idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$.

Le cas habituel est celui où S est l'ensemble S_∞ des places archimédiennes de k, ce qui équivaut à dire que $\mathfrak{o}$ est l'anneau des entiers d'un corps de nombres k. On vérifie aisément que $C^{S_\infty}(G_k)$ se réduit à $\{e\}$ si G est un groupe unipotent. D'après C. Chevalley [12], c'est encore le cas si G est un tore. D'autre part, $C^{S_\infty}(G_k)$ est généralement infini si G est un groupe semi-simple non simplement connexe (J.-P. Serre [28]). On sait d'ailleurs, depuis F. Klein, que $C^{S_\infty}(G_k)$ est infini pour $G = SL_2$ et $k = \mathbf{Q}$.

Nous supposerons dans le reste de ce numéro que G est un groupe semi-simple simplement connexe.

Soit $A_k(S)$ l'anneau des S-adèles de k, c'est-à-dire le produit restreint des complétés de k pour les places $v \notin S$ de k. Le groupe $G_{A_k(S)}$ des points de G à valeurs dans $A_k(S)$, muni de la topologie définie à partir de celle de $A_k(S)$, est un groupe localement compact. On voit que la topologie de $G_{A_k(S)}$ induit sur G_k exactement la topologie $T_c(S)$, et donc que $\overline{G_k(S)}$ s'identifie à l'adhérence de G_k dans $G_{A_k(S)}$. Par suite, si k est de caractéristique o et si G satisfait à l'approximation forte relativement à S, $\overline{G_k(S)}$ s'identifie au groupe adélifié $G_{A_k(S)}$ (*cf.* M. Kneser [18]).

D'autre part, la suite exacte (1.1) est triviale au-dessus du groupe G_k, regardé comme groupe discret, contenu dans $\overline{G_k(S)}$.

Lorsque $C^S(G_k)$ est fini et que le quotient de G_k par son centre Z_k n'a pas de quotient fini non trivial, on voit immédiatement que $C^S(G_k)$ est central dans $\widehat{G_k(S)}$. En général, notons $C^S_*(G_k)$ l'adhérence du sous-groupe de $C^S(G_k)$ engendré par les commutateurs $xyx^{-1}y^{-1}$ pour $x \in C^S(G_k)$ et $y \in \widehat{G_k(S)}$. On a alors, par passage au quotient, une extension centrale $\widetilde{G_k(S)}$ de $\overline{G_k(S)}$:

$$1 \to C^S_0(G_k) \to \widetilde{G_k(S)} \xrightarrow{\tilde{\pi}} \overline{G_k(S)} \to 1;$$

où

$$\widetilde{G_k(S)} = \widehat{G_k(S)}/C^S_*(G_k) \qquad \text{et} \qquad C^S_0(G_k) = C^S(G_k)/C^S_*(G_k).$$

Cela étant, le théorème suivant exprime un caractère universel de l'extension $\widehat{G_k(S)}$ de $\overline{G_k(S)}$ (Bass-Milnor-Serre [4]) :

THÉORÈME 1.1. — *Avec les notations ci-dessus, soit donnée une extension* E *de* $\overline{G_k(S)}$ *par un groupe profini* F *telle que sa restriction au groupe* G_k, *regardé comme discret, soit triviale.*

(*a*) *Il existe alors un morphisme* φ *de* $\widehat{G_k(S)}$ *dans* E *tel que* $p \circ \varphi = \pi$, *où* p *désigne la projection de* E *sur* $\overline{G_k(S)}$.

(*b*) *Supposons que* G_k *ne possède pas de quotient fini abélien non trivial. Alors, si de plus* F *est central dans* E, *il existe un morphisme* $\tilde{\varphi}$ *et un seul de* $\widetilde{G_k(S)}$ *dans* E *tel que* $p \circ \tilde{\varphi} = \tilde{\pi}$.

Pour l'énoncé (*a*), nous reproduisons la démonstration de [4]. Il existe, par hypothèse, un morphisme σ de G_k dans E tel que $p \circ \sigma(g) = g$ pour tout $g \in G_k$. L'application $\varphi = \sigma \circ \pi$ est donc un morphisme défini sur le groupe G_k contenu dans $\widehat{G_k(S)}$. Or, l'image de $G_\mathfrak{o}$ par φ est contenu dans le sous-groupe profini $p^{-1}(\overline{G}_\mathfrak{o})$ de E. Par suite, compte tenu de la définition de $\hat{G}_\mathfrak{o}$, $\varphi \mid G_\mathfrak{o}$ se prolonge en un morphisme continu de $\hat{G}_\mathfrak{o}$ dans $p^{-1}(\overline{G}_\mathfrak{o})$. Le morphisme φ se prolonge donc en un morphisme continu φ de $\widehat{G_k(S)}$ dans E. Il est clair que $p \circ \varphi = \pi$. Quant à l'énoncé (*b*), on déduit de (*a*), par passage au quotient, qu'il existe un morphisme $\tilde{\varphi}$ de $\widetilde{G_k(S)}$ dans E tel que $p\circ\tilde{\varphi}=\tilde{\pi}$. Si $\tilde{\psi}$ un morphisme de $\widetilde{G_k(S)}$ dans E ayant la même propriété, l'application δ, définie par $\delta(x)=\tilde{\psi}(x)\,\tilde{\varphi}(x)^{-1}$, est un morphisme de $\widetilde{G_k(S)}$ dans F; comme F est un groupe profini abélien, notre hypothèse sur G_k entraîne que δ est trivial dans G_k et donc, par continuité, dans $\widetilde{G_k(S)}$ tout entier. Ceci achève de démontrer le théorème.

2. Dans ce numéro, nous rappellerons la construction de certains schémas en groupes déployés sur $\mathbf{Z}$ et quelques-unes de leurs propriétés fondamentales (*cf.* C. Chevalley [15] et M. Demazure [16]).

Soient G un groupe algébrique connexe semi-simple sur $\mathbf{C}$ et H un tore maximal de G. On désignera par $\mathfrak{g}$ et $\mathfrak{h}$ les algèbres de Lie de G et de H respectivement. Soit Φ le système de racines de G relatif à H. On choisit un réseau de Chevalley $\mathfrak{g}_{\mathbf{Z}}$ de $\mathfrak{g}$ adaptée à $\mathfrak{h}$:

$$\mathfrak{g}_{\mathbf{Z}}=\mathfrak{h}_{\mathbf{Z}}+\sum_{\alpha}\mathbf{Z}\mathbf{e}_\alpha$$

avec un réseau $\mathfrak{h}_{\mathbf{Z}}$ de $\mathfrak{h}$ et un système d'éléments radiciels $\mathbf{e}_\alpha$. Pour chaque $\alpha\in\Phi$, l'élément $\mathbf{h}_\alpha=[\mathbf{e}_\alpha,\mathbf{e}_{-\alpha}]$ appartient à $\mathfrak{h}_{\mathbf{Z}}$ et l'on a $\alpha(\mathbf{h}_\alpha)=2$, la racine α étant identifiée à sa différentielle; $\alpha(\mathbf{h})$ est dans $\mathbf{Z}$ quel que soit $\mathbf{h}\in\mathfrak{h}_{\mathbf{Z}}$; si α, β et $\alpha+\beta$ sont des racines, on a $[\mathbf{e}_\alpha,\mathbf{e}_\beta]=N_{\alpha,\beta}\mathbf{e}_{\alpha+\beta}$ avec un entier non nul $N_{\alpha,\beta}$; on a $N_{\alpha,\beta}=-N_{-\alpha,-\beta}$. Notons que, si $\{\varepsilon_\alpha\}$, $\alpha\in\Phi$, est un ensemble d'entiers ± 1 tel que $\varepsilon_\alpha=\varepsilon_{-\alpha}$ pour tout α, alors les éléments $\varepsilon_\alpha\mathbf{e}_\alpha$ forment eux aussi un système d'éléments radiciels pour le réseau de Chevalley $\mathfrak{g}_{\mathbf{Z}}$.

Pour $\alpha,\beta\in\Phi$, l'entier $\alpha(\mathbf{h}_\beta)$ sera appelé l'entier de Cartan relatif à α et β, et sera noté $\alpha\beta^*$.

Soit ρ une représentation de G dans un espace vectoriel V; on a $V=\sum_\lambda V^\lambda$, où λ parcourt l'ensemble $\Lambda(\rho)$ des poids de ρ relatifs à H et où V^λ est le sous-espace de V appartenant à λ. Rappelons qu'un réseau $V_{\mathbf{Z}}$ de V est dit *admissible* par rapport à $\mathfrak{g}_{\mathbf{Z}}$ si $V_{\mathbf{Z}}$ satisfait aux conditions suivantes :

(i) $V_{\mathbf{Z}}=\sum_\lambda V_{\mathbf{Z}}^\lambda$, où $V_{\mathbf{Z}}^\lambda=V_{\mathbf{Z}}\cap V_\lambda$;

(ii) Pour tout $\alpha\in\Phi$ et tout entier $k\geq 0$, $\rho(\mathbf{e}_\alpha)^k/k!$ laisse $V_{\mathbf{Z}}$ stable.

Considérons une représentation fidèle ρ de G dans un espace vectoriel V et un réseau admissible $V_{\mathbf{Z}}$ de V par rapport à $\mathfrak{g}_{\mathbf{Z}}$. Toute base $\{v_1,\ldots,v_m\}$ de $V_{\mathbf{Z}}$ détermine les coordonnées $t_{i,j}$ $(1\leq i,j\leq m)$ sur GL(V), et les restrictions de celles-ci à G engendrent un sous-anneau $\mathbf{Z}[G]$ de l'algèbre affine $\mathbf{C}[G]$ de G. L'anneau $\mathbf{Z}[G]$, muni de la co-multication $\tilde{\pi}$ induite de celle de $\mathbf{C}[G]$, définit un schéma $\mathfrak{G}$ en groupes sur $\mathbf{Z}$, que nous appellerons le schéma de Chevalley-Demazure associé à G. On sait que le schéma en groupes $\mathfrak{G}$ ne dépend, à un isomorphisme près, pas du choix de H, de $\mathfrak{g}_{\mathbf{Z}}$, de ρ ou de $V_{\mathbf{Z}}$.

L'algèbre $\mathbf{Q}[G] = \mathbf{Z}[G] \otimes_{\mathbf{Z}} \mathbf{Q}$ fait de G un groupe algébrique défini sur $\mathbf{Q}$. Si X est un sous-groupe de G défini sur $\mathbf{Q}$, le plongement canonique ι de X dans G induit un morphisme $\tilde{\iota}$ de $\mathbf{C}[G]$ sur $\mathbf{C}[X]$; on notera $\mathbf{Z}[X]$ le sous-anneau $\tilde{\iota}(\mathbf{Z}[G])$ de $\mathbf{C}[X]$.

Introduisons quelques sous-groupes de G. Soit N le normalisateur de H dans G; le quotient N/H est le groupe de Weyl W de G relatif à H et l'on a $N = HN_{\mathbf{Z}}$. Lorsque G est simplement connexe, le groupe $N_{\mathbf{Z}}$ est appelé le groupe de Weyl étendu associé à G. Pour chaque racine α, U^{α} désignera le sous-groupe radiciel $\exp(\mathbf{C}\mathbf{e}_{\alpha})$, et G^{α} le sous-groupe simple de G engendré par U^{α} et $U^{-\alpha}$. On définit l'isomorphisme x_{α} du groupe additif sur U^{α} par $x_{\alpha}(t) = \exp(t\mathbf{e}_{\alpha})$ pour $t \in \mathbf{C}$; il existe alors un morphisme φ_{α} du groupe SL_2 sur G^{α} tel que $\varphi_{\alpha}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_{\alpha}(t)$ et que $\varphi_{-\alpha}\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-\alpha}(t)$ pour tout $t \in \mathbf{C}$.

Soient Δ un système de racines simples de Φ, et Φ^{+} l'ensemble des racines positives. Le sous-groupe U^{+} [resp. U^{-}] de G engendré par les U^{α} [resp. les $U^{-\alpha}$], $\alpha \in \Phi^{+}$, est un sous-groupe unipotent maximal de G.

Soit Δ' une partie de Δ et posons $\Delta'' = \Delta - \Delta'$. Notons $G(\Delta')$ [resp. $G(\Delta'')$] le sous-groupe de G engendré par les G^{α}, $\alpha \in \Delta'$ [resp. $\alpha \in \Delta''$]. Soit encore $U^{+}(\Delta')$ [resp. $U^{-}(\Delta')$] le sous-groupe engendré par les U^{α} [resp. les $U^{-\alpha}$], $\alpha \in \Phi^{+} - \Phi'^{+}$, où Φ'^{+} est l'ensemble des racines positives de $G(\Delta')$ relatif à $H(\Delta') = G(\Delta') \cap H$. Si $H(\Delta'')$ désigne $G(\Delta'') \cap H$, on a $H = H(\Delta')H(\Delta'')$; on sait que $H(\Delta') \cap H(\Delta'')$ se réduit à $\{e\}$ si G est simplement connexe. Le groupe réductif $S(\Delta') = G(\Delta')H(\Delta'')$ normalise $U^{+}(\Delta')$, et $U^{+}(\Delta')S(\Delta')$ est un sous-groupe parabolique de G. Ces sous-groupes de G sont tous définis sur $\mathbf{Q}$.

Rappelons le résultat suivant sur les algèbres affines de ces groupes :

a. Quand les éléments α de Φ^{+} sont convenablement rangés, l'application ε d'un espace affine $\mathbf{C}^{p}$ ($p = \dim U^{+}$) sur U^{+}, définie par

$$\varepsilon(t_1, \ldots, t_p) = \prod_i \exp(t_i \mathbf{e}_{\alpha_i}),$$

est un isomorphisme de variétés algébriques. De plus, $\mathbf{Z}[U^{+}]$ est l'algèbre des polynômes sur $\mathbf{Z}$ en les p variables $t_i \circ \varepsilon^{-1}$. On a un résultat analogue pour les groupes U^{-}, $U^{+}(\Delta')$ et $U^{-}(\Delta')$.

b. L'algèbre $\mathbf{Z}[H]$ est engendrée sur $\mathbf{Z}$ par $\chi_1, \chi_1^{-1}, \ldots, \chi_r, \chi_r^{-1}$, si $\{\chi_1, \ldots, \chi_r\}$ est un ensemble générateur du groupe des caractères de H. On a un résultat analogue pour $H(\Delta')$ et $H(\Delta'')$.

c. Soit $\mathfrak{g}'$ l'algèbre de Lie de $G' = G(\Delta')$. Alors $\mathfrak{g}'_{\mathbf{Z}} = \mathfrak{g}' \cap \mathfrak{g}_{\mathbf{Z}}$ s'écrit sous la forme $\mathfrak{h}_{\mathbf{Z}} \cap \mathfrak{g}' + \sum_{\alpha} \mathbf{Z}\mathbf{e}_{\alpha}$, où α parcourt l'ensemble des racines de G' relatives à $H(\Delta')$; donc $\mathfrak{g}'_{\mathbf{Z}}$ constitue un réseau de Chevalley de $\mathfrak{g}'$ adaptée à $\mathfrak{g}' \cap \mathfrak{h}$. Pour la restriction de ρ à G', $V_{\mathbf{Z}}$ est un réseau admissible de V par rapport à $\mathfrak{g}'_{\mathbf{Z}}$. Par conséquent, l'algèbre $\mathbf{Z}[G']$ que nous avons définie pour le sous-groupe G' de G est identique à celle qu'on peut définir, de même que pour G, pour le groupe semi-simple G'.

On va maintenant rappeler un théorème de décomposition. Soit μ un caractère de H, dominant par rapport au système de racines simples Δ, tel que μ s'annule sur $H(\Delta')$ et ne s'annule sur $H \cap G^{\alpha}$ pour aucun $\alpha \in \Delta''$. On choisit une représentation irréductible ρ de G dans un espace vectoriel V, de plus haut poids μ; on a $V = \sum_{\lambda} V^{\lambda}$, où λ parcourt l'ensemble des poids de ρ relatifs à H et où V^{λ} est le sous-espace de V appartenant au poids λ. Alors, le sous-groupe $U^{+}(\Delta')\,S(\Delta')$ est le stabilisateur dans G de V^{μ}, et la fonction t_{μ} sur G, définie par $\rho(g)\,v^{\mu} \equiv t_{\mu}(g)\,v^{\mu}$ modulo $\sum_{\lambda \neq \mu} V^{\lambda}$ avec un vecteur non nul v^{μ} de V^{μ}, appartient à $\mathbf{Z}[G]$. L'application $\pi \otimes \pi$ de $U^{-}(\Delta') \times S(\Delta') \times U^{+}(\Delta')$ dans G définie par $\pi \otimes \pi\,(u', s, u) = u'su$ est un isomorphisme de variétés algébriques de $U^{-}(\Delta') \times S(\Delta') \times U^{+}(\Delta')$ sur un ouvert affine Ω_{μ} de G, dont l'algèbre affine est justement $\mathbf{C}[G]\,(t_{\mu}^{-1})$. Il en est évidemment de même de l'application, définie de façon analogue, de $U^{-}(\Delta') \times U^{+}(\Delta') \times S(\Delta')$ sur Ω_{μ}. Si $H(\Delta'') \cap G(\Delta') = \{e\}$, l'application π de $H(\Delta'') \times G(\Delta')$ sur $S(\Delta')$ est également un isomorphisme de variétés algébriques.

Plus précisément, d'après [15], on a ainsi des isomorphismes d'algèbres :

$$\tilde{\pi} \otimes \tilde{\pi} : \quad \mathbf{Z}[G]\,(t_{\mu}^{-1}) \to \mathbf{Z}[U^{-}(\Delta')] \otimes \mathbf{Z}[S(\Delta')] \otimes \mathbf{Z}[U^{+}(\Delta')],$$
$$\tilde{\pi} \otimes \tilde{\pi} : \quad \mathbf{Z}[G]\,(t_{\mu}^{-1}) \to \mathbf{Z}[U^{-}(\Delta')] \otimes \mathbf{Z}[U^{+}(\Delta')] \otimes \mathbf{Z}[S(\Delta')]$$

et, si $H(\Delta'') \cap G(\Delta') = \{e\}$,

$$\tilde{\pi} : \quad \mathbf{Z}[S(\Delta')] \to \mathbf{Z}[H(\Delta'')] \otimes \mathbf{Z}[G(\Delta')];$$

où l'on a respectivement

$$\tilde{\pi} \otimes \tilde{\pi}\,(t_{\mu}) = 1 \otimes (t_{\mu} \,|\, S(\Delta')) \otimes 1,$$
$$\tilde{\pi} \otimes \tilde{\pi}\,(t_{\mu}) = 1 \otimes 1 \otimes (t_{\mu} \,|\, S(\Delta'))$$

et

$$\tilde{\pi}\,(t_{\mu} \,|\, S(\Delta')) = (\mu \,|\, H(\Delta'')) \otimes 1.$$

En particulier, pour $\Delta' = \emptyset$, cela donne un morphisme de $U^{-} \times H \times U^{+}$ sur un ouvert affine Ω_{μ_0} de G, et un isomorphisme d'algèbres

$$\tilde{\pi} \otimes \tilde{\pi} : \quad \mathbf{Z}[G]\,(t_{\mu_0}^{-1}) \to \mathbf{Z}[U^{-}] \otimes \mathbf{Z}[H] \otimes \mathbf{Z}[U^{+}].$$

Nous allons ensuite étudier les réseaux admissibles de certaines représentations de G.

Soit ρ une représentation de G dans un espace vectoriel V. Si $V_{\mathbf{Z}}$ est un réseau admissible de V par rapport à $\mathfrak{g}_{\mathbf{Z}}$, les coefficients de ρ relatifs à une base de $V_{\mathbf{Z}}$ appartiennent à $\mathbf{Z}[G]$; l'action de G sur V induit donc un morphisme d'algèbre $\tilde{\rho}$ de $\mathbf{Z}[V]$ dans $\mathbf{Z}[G]\otimes\mathbf{Z}[V]$, où $\mathbf{Z}[V]$ désigne le sous-anneau de l'algèbre affine $\mathbf{C}[V]$ de V engendré par les coordonnées de V relatives à une base de $V_{\mathbf{Z}}$.

Pour éviter une complication inutile, on supposera dans le reste de ce numéro que G est simple.

On voit aisément que pour une représentation irréductible ρ de G les conditions suivantes sont équivalentes :

(C) Tous les poids non nuls de ρ sont transformés les uns en les autres par le groupe de Weyl W de G;

(C′) Si λ et μ sont des poids non nuls de ρ dont la différence est une racine α, alors λ est le transformé de μ par la réflexion $\sigma_\alpha\in W$ associée à α.

On appellera *représentation basique* toute représentation irréductible non triviale de G vérifiant ces conditions.

On a d'abord le lemme suivant ([14], exposé 20) :

Lemme 2.1. — *Soit ρ une représentation basique de* G.

(*a*) *Tout poids non nul de ρ est alors de multiplicité* 1 *et la multiplicité du poids zéro est le nombre des racines simples figurant parmi les poids non nuls de ρ.*

(*b*) *Soient $\Delta(\rho)$ l'ensemble de ces dernières racines simples, et pour chaque $\alpha\in\Delta(\rho)$, v^α un vecteur non nul de V^α. Alors, V^0 possède une base constituée par des éléments v^0_β, $\beta\in\Delta(\rho)$, de sorte que $\rho(\mathbf{e}_\alpha)v^0_\beta=\delta_{\alpha,\beta}v^\alpha$, où $\delta_{\alpha,\beta}=1$ si $\alpha=\beta$ et $\delta_{\alpha,\beta}=0$ si $\alpha\neq\beta$.*

En effet, la première assertion de (*a*) est bien connue. Considérons ensuite la sous-algèbre $\mathfrak{m}$ de $\mathfrak{g}$ engendrée par les $\mathbf{e}_\alpha$ et $\mathbf{e}_{-\alpha}$, $\alpha\in\Delta(\rho)$, et la représentation de $\mathfrak{m}$ dans le plus petit sous-espace V' de V contenant V^0 et stable par $\mathfrak{m}$. D'après (C′), on a $V'=V^0+\sum_\lambda V^\lambda$, où λ parcourt l'ensemble des transformés des $\alpha\in\Delta(\rho)$ par le groupe de Weyl de $\mathfrak{m}$ relatif à $\mathfrak{m}\cap\mathfrak{h}$. La représentation de $\mathfrak{m}$ dans V' est donc équivalente à la représentation adjointe de $\mathfrak{m}$. D'où les assertions de notre lemme.

Rappelons que G est simple. On dit qu'une racine α de G est longue [resp. courte], si aucune racine de G n'a une longueur supérieure [resp. inférieure] à celle de α.

On sait qu'il existe une représentation basique de G dont les poids non nuls sont les racines courtes de G; elle est d'ailleurs, à une équivalence près, la seule représentation basique de G à avoir effectivement le poids zéro. D'autre part, toute représentation basique de G est une représentation fondamentale, à l'exception de la représentation adjointe d'un groupe de type A_n. Si G est simplement connexe, il existe au moins c représentations basiques de G non équivalentes où c est l'ordre du centre de G ([14], *loc. cit.*). Notons aussi que pour les groupes classiques, leurs réalisations habituelles (SL, Sp, SO et Spin) vérifient la condition (C).

Nous signalons le lemme suivant :

LEMME 2.2. — *Si* G *est simplement connexe et de rang* $\geqq 2$, G *admet une représentation fondamentale vérifiant* (C) *et la condition suivante :*

(D) *Elle est de degré* $\geqq 3$ *et son plus haut poids n'est pas somme de deux racines simples.*

En effet, si G est de rang $\geqq 3$, toute représentation irréductible non triviale de G satisfait à cette dernière condition, car tout poids dominant $\neq 0$ est combinaison linéaire de toutes les racines simples avec des coefficients strictement positifs. Si G est de type A_2 [resp. C_2], G possède une représentation fondamentale de degré 3 [resp. 4] vérifiant (C) et n'ayant pas zéro pour poids. Pour le groupe de type G_2, la représentation fondamentale de degré 7 satisfait à nos conditions.

Soit maintenant ρ une représentation basique de G dans un espace vectoriel V. On va choisir un réseau admissible de V uniquement déterminé à une homothétie près. Désignons par $\Lambda(\rho)$ l'ensemble des poids de ρ, par $\Lambda(\rho)^\star$ celui des poids non nuls et par $\Delta(\rho)$ celui des racines simples figurant dans $\Lambda(\rho)$. On prend un réseau admissible $V_{\mathbf{Z}}$ de V par rapport à $\mathfrak{g}_{\mathbf{Z}}$: on a $V_{\mathbf{Z}} = \sum_\lambda V^\lambda_{\mathbf{Z}}$, où $V_{\mathbf{Z}} = V_{\mathbf{Z}} \cap V^\lambda$ pour $\lambda \in \Lambda(\rho)$. On choisit ensuite, pour chaque $\lambda \in \Lambda(\rho)^\star$, un vecteur primitif v^λ de $V^\lambda_{\mathbf{Z}}$. Il existe alors, d'après le lemme 2.1, une base $\{v^0_\alpha\}$ de V^0 indexée par $\Delta(\rho)$ et telle que $\rho(\mathbf{e}_\alpha) v^0_\beta = \delta_{\alpha,\beta} v^\beta$, pour tout α, $\beta \in \Delta(\rho)$. Ceci implique aussi que

$$\rho(\mathbf{e}_{-\alpha}) v^0_\beta = \pm \delta_{\alpha,\beta} v^{-\alpha}$$

pour α, $\beta \in \Delta(\rho)$. On déduit de là que le $\mathbf{Z}$-module engendré par les éléments de $V_{\mathbf{Z}}$ et les v^0_α est un réseau admissible de V par rapport à $\mathfrak{g}_{\mathbf{Z}}$.

Supposons que le réseau $V_{\mathbf{Z}}$ soit ainsi normalisé; $V_{\mathbf{Z}}$ possède une base constituée par les v^λ, $\lambda \in \Lambda(\rho)^\star$, et les v^0_α, $\alpha \in \Delta(\rho)$. Cette base nous permet de voir explicitement comment les groupes radiciels U^α opèrent sur V.

LEMME 2.3. — *L'action des sous-groupes radiciels* $U^\alpha (\alpha \in \Phi)$ *sur* V *s'écrit, en termes de la base normalisée, par les formules suivantes* [*où l'on convient d'écrire* $x_\alpha(t)$ *au lieu de* $\rho(x_\alpha(t))$ *et où* ± 1 *signifie une constante* ± 1 *ne dépendant pas de la variable* t] :

(*a*) *Si* $\lambda \in \Lambda(\rho)^\star$ *et* $\lambda + \alpha \notin \Lambda(\rho)$; $x_\alpha(t) v^\lambda = v^\lambda$;

(*b*) *Si* λ, $\lambda+\alpha\in\Lambda(\rho)^\star$; $x_\alpha(t)v^\lambda = v^\lambda \pm t v^{\lambda+\alpha}$;

(*c*) *Si* $\alpha\notin\Lambda(\rho)$; $x_\alpha(t)v^0 = v^0$ *pour tout* $v^0\in V^0$;

(*d*) *Si* $\alpha\in\Lambda(\rho)$; $x_\alpha(t)v^0 = v^0 + t\,\alpha_*(v^0)v^\alpha$ *pour tout* $v^0\in V^0$,

$$\text{et}\quad x_\alpha(t)v^{-\alpha} = v^{-\alpha} + t v^0(\alpha) \pm t^2 v^\alpha,$$

où α_* *est un élément non nul du dual* $(V^0)^\star$ *de* V^0 *et* $v^0(\alpha)$ *un élément non nul de* $V^0_{\mathbf{Z}}$;

(*e*) *Pour tout* $\alpha\in\Delta(\rho)$, $v^0(\alpha) = \pm v^0(-\alpha)$ *et* $\alpha_* = \pm(-\alpha)_*$. *Les* α_*, $\alpha\in\Delta(\rho)$, *constituent dans* $(V^0)^\star$ *une base du réseau* $(V^0_{\mathbf{Z}})_*$ *dual à* $V^0_{\mathbf{Z}}$.

Cela résulte tout de suite de ce qui précède le lemme et d'un résultat élémentaire sur les représentations d'un groupe simple de rang 1.

3. Nous étudierons dans ce numéro le problème des groupes de congruence pour les groupes simples simplement connexes déployés.

Soit G un groupe simple simplement connexe sur $\mathbf{C}$. On associe à G le schéma $\mathfrak{G}$ en groupes sur $\mathbf{Z}$, en choisissant un tore maximal H de G et un réseau de Chevalley $\mathfrak{g}_{\mathbf{Z}}$ avec un système d'éléments radiciels $\mathbf{e}_\alpha$ (*voir* n° 2); Φ désignera le système de racines de G relatif à H et Δ un système de racines simples dans Φ.

Soit $\mathfrak{o}$ un anneau commutatif à unité. On déduit de $\mathfrak{G}$, par extension des scalaires de $\mathbf{Z}$ à $\mathfrak{o}$, un schéma ${}_{\mathfrak{o}}G$ en groupes affines sur $\mathfrak{o}$; le groupe $G_{\mathfrak{o}}$ des points de ${}_{\mathfrak{o}}G$ à valeurs dans $\mathfrak{o}$ est l'ensemble des morphismes de l'algèbre $\mathbf{Z}[G]\otimes_{\mathbf{Z}}\mathfrak{o}$ dans $\mathfrak{o}$. Si $\mathfrak{o}$ est un corps k, ${}_kG$ définit un groupe simple simplement connexe du même type que G. Tout groupe simple simplement connexe déployé sur k est isomorphe sur k à un groupe défini de cette manière ([16], [6]).

Le groupe $G_{\mathfrak{o}}$ possède les sous-groupes correspondant aux divers sous-schémas en groupes de $\mathfrak{G}$ définis au n° 2 : en particulier, le tore $H_{\mathfrak{o}}$, les groupes unipotents $U^+_{\mathfrak{o}}$ et $U^-_{\mathfrak{o}}$, les sous-groupes radiciels $U^\alpha_{\mathfrak{o}}$ ($\alpha\in\Phi$). Pour chaque $\alpha\in\Phi$, x_α désignera l'isomorphisme du groupe additif sur U^α, déterminé par le choix de l'élément radiciel $\mathbf{e}_\alpha$ (*voir* n° 2).

Soit $\mathfrak{o}^\times$ le groupe multiplicatif des éléments inversibles de $\mathfrak{o}$. Pour tout $\alpha\in\Phi$ et $t\in\mathfrak{o}^\times$, posons $w_\alpha(t) = x_\alpha(t)\,x_{-\alpha}(-t^{-1})\,x_\alpha(t)$; cet élément appartient au normalisateur algébrique $N_{\mathfrak{o}}$ de $H_{\mathfrak{o}}$. L'application h_α, définie par $h_\alpha(t) = w_\alpha(t)\,w_\alpha(1)^{-1}$, est un isomorphisme de $\mathfrak{o}^\times$ sur un sous-groupe $H^\alpha_{\mathfrak{o}}$ de $H_{\mathfrak{o}}$. De plus, $H_{\mathfrak{o}}$ est le produit direct des sous-groupes $H^\alpha_{\mathfrak{o}}$, α parcourant le système de racines simples Δ. D'autre part, les éléments $w_\alpha(1)$, $\alpha\in\Phi$, engendrent un sous-groupe fini $\mathfrak{N}_{\mathfrak{o}}$ de $N_{\mathfrak{o}}$, et l'on a $N_{\mathfrak{o}} = H_{\mathfrak{o}}\mathfrak{N}_{\mathfrak{o}}$.

Dans le cas d'un corps k, le groupe G_k est engendré par les sous-groupes radiciels U^α_k, et l'on a $G_k = U^+_k N_k U^-_k = U^+_k N_k U^+_k$. Lorsque k est un corps infini, on sait que G_k est égal à son groupe des commutateurs et que le quotient de G_k par son centre Z_k est simple en tant que groupe abstrait [13].

Pour simplifier l'exposé ultérieur, on convient de dire, si G est isomorphe à l'un des groupes symplectiques, que le groupe simple simplement connexe G ou son diagramme de Dynkin Δ est *de type symplectique*; sinon, on dira que G ou Δ est *de type non symplectique*.

Nous venons maintenant au problème des groupes de congruence pour G_k, où k est le corps des fractions d'un anneau de Dedekind $\mathfrak{o}$ de type arithmétique; l'anneau $\mathfrak{o}$ est déffni dans k à partir d'un ensemble S de places de k.

Considérons la suite exacte (1.1) :

$$1 \to C^S(G_k) \to \widehat{G_k(S)} \xrightarrow{\pi} \overline{G_k(S)} \to 1.$$

D'une part, d'après ce qui précède, le groupe des commutateurs de $\widehat{G_k(S)}$ [resp. de $\overline{G_k(S)}$] est dense dans $\widehat{G_k(S)}$ [resp. $\overline{G_k(S)}$]. D'autre part, on voit que G_k est dense dans le groupe adélifié $G_{A_k(S)}$, d'après le théorème de l'approximation forte ou d'après le fait que $G_{k'}$ est engendré par ses sous-groupes radiciels $U^\alpha_{k'}$ pour chaque complété k' de k.

En vue d'étudier la suite exacte restreinte à $\hat{G}_\mathfrak{o}$, nous définirons quelques sous-groupes de $G_\mathfrak{o}$ où $\mathfrak{o}$ est un anneau commutatif à unité. Quand on a fixé l'anneau $\mathfrak{o}$, Γ désignera $G_\mathfrak{o}$, et le sous-groupe de $G_\mathfrak{o}$ engendré par les sous-groupes radiciels $U^\alpha_\mathfrak{o}$ sera noté $E_\mathfrak{o}$. Si $\mathfrak{q}$ est un idéal de $\mathfrak{o}$, on notera $\Gamma_\mathfrak{q}$ le noyau du morphisme de réduction de $G_\mathfrak{o}$ dans $G_{\mathfrak{o}/\mathfrak{q}}$, et $E_\mathfrak{q}$ le plus petit sous-groupe distingué de $E_\mathfrak{o}$ contenant les $\Gamma_\mathfrak{q} \cap U^\alpha_\mathfrak{o} (\alpha \in \Phi)$. On a vu plus haut que $E_\mathfrak{o}$ contient $N_\mathfrak{o}$.

LEMME 3.1. — *Supposons que* G *soit de rang* $\geqq 2$ *et que* $\mathfrak{o}$ *soit un anneau intègre infini. Alors, tout sous-groupe d'indice fini dans* $G_\mathfrak{o}$ *contient le groupe* $E_\mathfrak{q}$ *pour un idéal* $\mathfrak{q}$ *non nul de* $\mathfrak{o}$.

Soit Γ' un sous-groupe d'indice fini dans $G_\mathfrak{o}$: pour démontrer le lemme, on peut supposer que Γ' est distingué dans $G_\mathfrak{o}$. Notons d'abord que, si $\mathfrak{o}$ est de caractéristique 0, notre assertion est triviale et valable aussi pour SL_2; en effet, si $G_\mathfrak{o}/\Gamma'$ est d'ordre n, Γ' contient tous les éléments de la forme $x_\alpha(nt)$ $(\alpha \in \Phi,\ t \in \mathfrak{o})$, et donc le groupe $E_\mathfrak{q}$ pour $\mathfrak{q} = n\mathfrak{o}$. Même en caractéristique arbitraire, il suffit d'envisager les cas de rang 2, puisque E contient $\mathfrak{N}_\mathfrak{o}$ et que tout sous-groupe radiciel $U^\alpha_\mathfrak{o}$ est transformé par un élément de $\mathfrak{N}_\mathfrak{o}$ en $U^\beta_\mathfrak{o}$ pour une racine simple β. Nous distinguons les trois cas de rang 2.

Dans le cas du type A_2, notons α, β et $\alpha+\beta$ les racines positives. On a la relation de commutation ([13], [16]) :

$$x_\alpha(u)\, x_\beta(v)\, x_\alpha(u)^{-1}\, x_\beta(v)^{-1} = x_{\alpha+\beta}(\pm uv)\,;$$

la constante ± 1 dépend évidemment du choix des isomorphismes x_γ, et l'on peut supposer qu'elle soit égale à 1, quitte à remplacer $x_\gamma(u)$

par $x_\gamma(\varepsilon_\gamma u)$ $(\gamma \in \Phi)$, où $\{\varepsilon_\gamma\}$ est un ensemble d'entiers ± 1 tel que $\varepsilon_\gamma = \varepsilon_{-\gamma}$ pour tout γ; on appliquera cette dernière remarque également aux types C_2 et G_2. D'abord, puisque $\mathfrak{o}$ est un groupe additif infini, Γ' contient $x_\alpha(s)$ pour un élément $s \neq 0$ de $\mathfrak{o}$. Alors, la relation de commutation montre que Γ' contient $x_{\alpha+\beta}(\mathfrak{q})$ pour $\mathfrak{q} = s\mathfrak{o}$. Le groupe Γ' contient $x_\gamma(\mathfrak{q})$ pour tout $\gamma \in \Phi$, et donc $E_\mathfrak{q}$.

Pour le type C_2, soient α et β les racines simples avec $\alpha\beta^\star = -1$ et $\beta\alpha^\star = -2$; les racines positives sont α, β, $\alpha+\beta$ et $2\alpha+\beta$. On peut supposer que la relation de commutation pour U^α et U^β soit donnée par

$$x_\alpha(u)\, x_\beta(v)\, x_\alpha(u)^{-1}\, x_\beta(v)^{-1} = x_{\alpha+\beta}(uv)\, x_{2\alpha+\beta}(u^2 v).$$

Prenons un élément $x_\alpha(s)$ de Γ' tel que $s(s-1) \neq 0$. Alors, d'après la relation de commutation, Γ' contient, pour tout $t \in \mathfrak{o}$,

$$g_1 = x_{\alpha+\beta}(st)\, x_{2\alpha+\beta}(s^2 t)$$

ainsi que son transformé g_2 par $w_\alpha(1)$; on a

$$g_2 = x_{\alpha+\beta}(-st)\, x_\beta(\pm s^2 t) = g_1^{-1} g_3, \qquad \text{où} \quad g_3 = x_{2\alpha+\beta}(s^2 t)\, x_\beta(\pm s^2 t).$$

L'élément

$$g_4 = x_\alpha(1) g_3 x_\alpha(1)^{-1} g_3^{-1} = x_{\alpha+\beta}(\pm s^2 t)\, x_{2\alpha+\beta}(\pm s^2 t)$$

appartient à Γ'. Par suite, Γ' contient

$$g_1 g_4^{\pm 1} = x_{\alpha+\beta}(s(1-s)\,t).$$

Pour $\mathfrak{q}' = s(1-s)\mathfrak{o}$, Γ' contient donc $x_{\alpha+\beta}(\mathfrak{q}')$ et aussi $x_\alpha(\mathfrak{q}')$. La relation de commutation montre alors que $x_{2\alpha+\beta}(\mathfrak{q})$ est contenu dans Γ' pour $\mathfrak{q} = \mathfrak{q}'^2$. Par conséquent, Γ' contient $E_\mathfrak{q}$.

Pour le type G_2, soient α et β les racines simples avec $\alpha\beta^\star = -1$ et $\beta\alpha^\star = -3$; les racines positives sont α, β, $\alpha+\beta$, $2\alpha+\beta$, $3\alpha+\beta$ et $3\alpha+2\beta$. La relation de commutation pour U^α et U^β peut s'écrire par

$$x_\alpha(u)\, x_\beta(v)\, x_\alpha(u)^{-1}\, x_\beta(v)^{-1} = x_{\alpha+\beta}(uv)\, x_{2\alpha+\beta}(u^2 v)\, x_{3\alpha+\beta}(u^3 v)\, x_{3\alpha+2\beta}(u^3 v^2).$$

On voit d'abord, comme les racines longues $\pm\beta$, $\pm(3\alpha+\beta)$ et $\pm(3\alpha+2\beta)$ forment un système de racines de type A_2, que Γ' contient $x_\gamma(\mathfrak{q}')$ pour toute racine longue γ, où $\mathfrak{q}'$ est un idéal non nul de $\mathfrak{o}$. Prenons un élément $x_\alpha(s)$ de Γ' tel que $s \in \mathfrak{q}'$ et que $s(1-s) \neq 0$. En calculant

$$x_\alpha(s)\, x_\beta(t)\, x_\alpha(s)^{-1}\, x_\beta(t)^{-1} \qquad \text{et} \qquad x_\alpha(1)\, x_\beta(s^2 t)\, x_\alpha(1)^{-1}\, x_\beta(s^2 t)^{-1},$$

on voit que Γ' contient

$$x_{\alpha+\beta}(st)\, x_{2\alpha+\beta}(s^2 t) \qquad \text{et} \qquad x_{\alpha+\beta}(s^2 t)\, x_{2\alpha+\beta}(s^2 t)$$

pour tout $t \in \mathfrak{o}$; Γ' contient donc $x_{\alpha+\beta}(\mathfrak{q})$ pour $\mathfrak{q} = s(1-s)\mathfrak{o}$. On en conclut que Γ' contient $E_\mathfrak{q}$. Cela achève de prouver le lemme 3.1.

Le lemme suivant sera démontré dans le n° 4 :

LEMME 3.2. — *Supposons que* G *soit de rang* $\geqq 2$ *et que le quotient* $\mathfrak{o}/\mathfrak{q}$ *soit semi-local pour tout idéal* $\mathfrak{q}$ *non nul de* $\mathfrak{o}$. *Alors :*

(*a*) $E_\mathfrak{q}$ *est un sous-groupe distingué de* $G_\mathfrak{o}$ *pour tout idéal* $\mathfrak{q}$ *de* $\mathfrak{o}$;

(*b*) *Si* $\mathfrak{q}$ *et* $\mathfrak{q}'$ *sont des idéaux non nuls de* $\mathfrak{o}$ *tels que* $\mathfrak{q}$ *contienne* $\mathfrak{q}'$, *on a* $\Gamma_\mathfrak{q} = E_\mathfrak{q}\Gamma_{\mathfrak{q}'}$;

(*c*) *Si* $\mathfrak{q}$ *est un idéal de* $\mathfrak{o}$, *le commutateur* $xyx^{-1}y^{-1}$ *appartient à* $E_\mathfrak{q}$ *pour tout* $x \in E_\mathfrak{o}$ *et* $y \in \Gamma_\mathfrak{q}$.

Nous allons appliquer ces lemmes au problème des groupes de congruence. Supposons que G soit de rang $\geqq 2$ et que $\mathfrak{o}$ soit un anneau de Dedekind de type arithmétique.

Soit $\mathfrak{q}$ un idéal non nul de $\mathfrak{o}$. D'après le lemme 3.2, (*a*), $E_\mathfrak{q}$ est un sous-groupe distingué de Γ; on a donc une suite exacte :

$$1 \to C_\mathfrak{q} \to \Gamma/E_\mathfrak{q} \to \Gamma/\Gamma_\mathfrak{q} \to 1,$$

où $C_\mathfrak{q} = \Gamma_\mathfrak{q}/E_\mathfrak{q}$. Munissons $\Gamma/E_\mathfrak{q}$ et donc $C_\mathfrak{q}$ de la topologie des sous-groupes d'indice fini; en notant $\widehat{\Gamma/E_\mathfrak{q}}$ et $\hat{C}_\mathfrak{q}$ les complétés-séparés de $\Gamma/E_\mathfrak{q}$ et de $C_\mathfrak{q}$, on a une suite exacte de groupes profinis :

$$1 \to \hat{C}_\mathfrak{q} \to \widehat{\Gamma/E_\mathfrak{q}} \to \Gamma/\Gamma_\mathfrak{q} \to 1.$$

Si $\mathfrak{q}'$ est un idéal non nul de $\mathfrak{o}$ contenu dans $\mathfrak{q}$, on a un diagramme commutatif :

$$\begin{tikzcd} 1 \arrow[r] & C_{\mathfrak{q}'} \arrow[r] \arrow[d] & \Gamma/E_{\mathfrak{q}'} \arrow[r] \arrow[d] & \Gamma/\Gamma_{\mathfrak{q}'} \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & C_\mathfrak{q} \arrow[r] & \Gamma/E_\mathfrak{q} \arrow[r] & \Gamma/\Gamma_\mathfrak{q} \arrow[r] & 1. \end{tikzcd}$$

Le morphisme de $C_{\mathfrak{q}'}$ dans $C_\mathfrak{q}$ est surjectif, d'après le lemme 3.2, (*b*). On déduit de là un diagramme analogue pour les complétés-séparés où le morphisme de $\hat{C}_{\mathfrak{q}'}$ dans $\hat{C}_\mathfrak{q}$ est surjectif.

Passons à la limite projective sur l'ensemble des idéaux non nuls de $\mathfrak{o}$. La limite des $\Gamma/\Gamma_\mathfrak{q}$ s'identifie au groupe $\overline{G}_\mathfrak{o}$ et, d'après le lemme 3.1, la limite des $\widehat{\Gamma/E_\mathfrak{q}}$ s'identifie à $\hat{G}_\mathfrak{o}$. De plus, le morphisme limite de $\hat{G}_\mathfrak{o}$ sur $\overline{G}_\mathfrak{o}$ n'est autre que celui qu'on a noté π au n° 1. On a donc la suite exacte :

$$1 \to \varprojlim \hat{C}_\mathfrak{q} \to \hat{G}_\mathfrak{o} \xrightarrow{\pi} \overline{G}_\mathfrak{o} \to 1,$$

où $\varprojlim \hat{C}_\mathfrak{q}$ s'identifie canoniquement à $C(G_\mathfrak{o})$.

Rappelons que $\hat{G}_{\mathfrak{o}}$ est le complété de $G_{\mathfrak{o}}$ pour la topologie des sous-groupes d'indice fini. Le lemme 3.2, (*c*) affirme que tout élément de $E_{\mathfrak{o}}$ commute avec les éléments de $\varprojlim \hat{C}_{\mathfrak{q}}$. Revenons-en à la suite exacte (1.1) :

$$1 \rightarrow C^S(G_k) \rightarrow \widehat{G_k(S)} \xrightarrow{\pi} \overline{G_k(S)} \rightarrow 1.$$

On rappelle que $\widehat{G_k(S)}$ est le complété de G_k pour la topologie $T_a(S)$. Le centraliseur de $C^S(G_k)$ dans G_k est un sous-groupe distingué de G_k, et l'on vient de voir qu'il contient $E_{\mathfrak{o}}$. Comme le quotient de G_k par son centre est simple en tant que groupe abstrait, cela entraîne que tout élément de G_k commute avec les éléments de $C^S(G_k)$. Puisque G_k est dense dans $\widehat{G_k(S)}$, on en conclut que $C^S(G_k)$ est central dans $\widehat{G_k(S)}$.

En combinant ce résultat avec le théorème 1.1, nous avons le théorème suivant :

Théorème 3.3. — *Soit k le corps des fractions d'un anneau de Dedekind $\mathfrak{o}(S)$ de type arithmétique. Soit G un groupe simple simplement connexe déployé sur k de rang ≥ 2. La suite exacte* (1.1)

$$1 \rightarrow C^S(G_k) \rightarrow \widehat{G_k(S)} \xrightarrow{\pi} G_{A_k(S)} \rightarrow 1,$$

associée à G_k relativement à $\mathfrak{o}(S)$, jouit des propriétés suivantes :

(*a*) *Le noyau $C^S(G_k)$ est central dans $\widehat{G_k(S)}$ et est un groupe profini;*

(*b*) *La suite exacte est triviale au-dessus du groupe discret G_k contenu dans $G_{A_k(S)}$;*

(*c*) *Le groupe des commutateurs de $\widehat{G_k(S)}$ est dense dans $\widehat{G_k(S)}$;*

(*d*) *Si E est une extension centrale de $G_{A_k(S)}$ par un groupe abélien profini, qui est triviale au-dessus de G_k, alors il existe un morphisme φ de $\widehat{G_k(S)}$ dans E tel que $p \circ \varphi = \pi$, où p désigne la projection de E sur $G_{A_k(S)}$.*

Notons que ces propriétés caractérisent $\widehat{G_k(S)}$ entre toutes les extensions de $G_{A_k(S)}$, c'est-à-dire, si une extension de $G_{A_k(S)}$ par un groupe localement compact B possède ces propriétés, elle est isomorphe à $\widehat{G_k(S)}$ comme extension de $G_{A_k(S)}$, B étant isomorphe à $C^S(G_k)$. On pourrait déduire de là tout de suite que, si S' contient S, le groupe $C^{S'}(G_k)$ est isomorphe à un quotient de $C^S(G_k)$.

4. Dans ce numéro, nous étudierons les sous-groupes $\Gamma_{\mathfrak{q}}$ et $E_{\mathfrak{q}}$ de $G_{\mathfrak{o}}$ introduits au n° 3 et donnerons une démonstration du lemme 3.2.

Nous reprenons les notations du n° 3. En outre, on supposera toujours que *$\mathfrak{o}$ est un anneau commutatif à unité tel que $\mathfrak{o}/\mathfrak{q}$ soit semi-local pour tout idéal $\mathfrak{q}$ non nul de $\mathfrak{o}$.*

Nous aurons besoin du lemme suivant :

LEMME 4.1. — *Soit* $\mathfrak{q}$ *un idéal de* $\mathfrak{o}$ *et soient* a_0, a_1 *et* a_2 *des éléments de* $\mathfrak{o}$ *tels que* $a_0\mathfrak{o} + \mathfrak{q} = \mathfrak{o}$ *et que* $\mathfrak{o}/a_0\mathfrak{o}$ *soit semi-local. Alors :*

(*a*) *Si* $\mathfrak{m}$ *est un idéal maximal de* $\mathfrak{o}$ *contenant* a_0, *il existe un élément* t *de* $\mathfrak{q}$ *tel que* $t \notin \mathfrak{m}$ *et que* $\mathfrak{o}/(a_0 + a_1 t)\mathfrak{o}$ *soit semi-local;*

(*b*) *Si* $\mathfrak{m}$ *est un idéal maximal de* $\mathfrak{o}$ *contenant* a_0 *et* a_1, *il existe un élément* t *de* $\mathfrak{q}$ *tel que* $t \notin \mathfrak{m}$ *et que tout idéal maximal de* $\mathfrak{o}$ *contenant* a_0 *et* $(a_1 + a_2 t)$ *contienne aussi* a_1.

Démontrons d'abord (*a*). Puisqu'on a $\mathfrak{m} + \mathfrak{q} = \mathfrak{o}$, il existe un élément t de $\mathfrak{q}$ tel que $t \notin \mathfrak{m}$. Si $\mathfrak{q} \neq \mathfrak{o}$, alors $a'_0 = a_0 + a_1 t$ est différent de o et, par notre hypothèse sur $\mathfrak{o}$, $\mathfrak{o}/a'_0\mathfrak{o}$ est semi-local. Si $\mathfrak{o}$ est lui-même semi-local, $\mathfrak{o}/a'_0\mathfrak{o}$ l'est évidemment. Supposons donc que $\mathfrak{q} = \mathfrak{o}$ et qu'il existe une infinité d'idéaux maximaux de $\mathfrak{o}$. Soit alors $\mathfrak{m}'$ un idéal maximal de $\mathfrak{o}$ tel que $a_0 \notin \mathfrak{m}'$. On a $\mathfrak{m} + \mathfrak{m}' = \mathfrak{o}$, et il existe un élément t de $\mathfrak{m}'$ tel que $t \notin \mathfrak{m}$; alors, $a'_0 = a_0 + a_1 t$ est différent de o et $\mathfrak{o}/a'_0\mathfrak{o}$ est semi-local.

Quant à l'énoncé (*b*), considérons les idéaux maximaux de $\mathfrak{o}$ contenant a_0 et non a_1. Ces idéaux $\mathfrak{m}_i$ $(1 \leq i \leq k)$ ainsi que $\mathfrak{m}$ et $\mathfrak{q}$ forment un système fini d'idéaux distincts deux à deux étrangers. Il existe donc un élément t de $\mathfrak{q}$ tel que $t \notin \mathfrak{m}$ et que $t \in \mathfrak{m}_i$ pour tout i. Alors, $a_1 + a_2 t$ n'est dans $\mathfrak{m}_i$ pour aucun i et, par suite, tout idéal maximal de $\mathfrak{o}$ contenant a_0 et $a_1 + a_2 t$ contient nécessairement a_1. Cela achève de démontrer le lemme.

On va considérer certaines représentations de $G_\mathfrak{o}$ dans des $\mathfrak{o}$-modules. Soient ρ une représentation de G dans un espace vectoriel V et $V_\mathbf{Z}$ un réseau admissible de V par rapport à $\mathfrak{g}_\mathbf{Z}$ (*voir* n° 2). Le morphisme d'algèbres de $\mathbf{Z}[V]$ dans $\mathbf{Z}[G] \otimes \mathbf{Z}[V]$ définit une action ρ de $G_\mathfrak{o}$ sur $V_\mathfrak{o}$, où $V_\mathfrak{o} = V_\mathbf{Z} \otimes_\mathbf{Z} \mathfrak{o} = \mathrm{Hom}\,(\mathbf{Z}[V], \mathfrak{o})$.

Supposons G de rang ≥ 2 et prenons une représentation fondamentale ρ de G vérifiant les conditions (C) et (D) du n° 2. On a alors un réseau admissible normalisé $V_\mathbf{Z}$ de V dont une base est constituée par les v^λ $(\lambda \in \Lambda(\rho)^\star)$ et les v^0_α $(\alpha \in \Delta(\rho))$. Ces éléments forment donc une base de $V_\mathfrak{o}$ sur $\mathfrak{o}$.

Cela dit, le lemme 2.3 va nous permettre de prouver le

LEMME 4.2. — *Soient* $\mathfrak{q}$ *un idéal de* $\mathfrak{o}$ *et* v_0 *un élément unimodulaire de* $V_\mathfrak{o}$ *tel que* $v_0 \equiv uv^\lambda \bmod \mathfrak{q}V_\mathfrak{o}$ *avec un poids non nul* λ *et un élément inversible* u *de* $\mathfrak{o}$. *Il existe alors un élément* g *de* $E_\mathfrak{q}$ *tel que* $\rho(g)v_0 \equiv uv^\lambda \bmod \sum_\nu \mathfrak{q}V^\nu_0$, *où* ν *parcourt l'ensemble des poids de* ρ *différents de* λ.

Notre démonstration de ce lemme est directement inspirée de celle que [2] et [3] donnent dans le cas de la représentation naturelle de SL_n

dans $\mathfrak{o}^n (n \geqq 3)$. On écrira ci-dessous gv au lieu de $\rho(g)v$ pour $g \in G_\mathfrak{o}$ et $v \in V_\mathfrak{o}$.

On note d'abord que $N_\mathfrak{o}$ contient un élément n tel que $n(uv^\lambda) = v^\mu$, μ étant le plus haut poids de ρ. Or $N_\mathfrak{o}$ normalise $E_\mathfrak{q}$ et tout élément de $N_\mathfrak{o}$ permute entre eux les sous-modules V_0^ν de $V_\mathfrak{o}(\nu \in \Lambda(\rho))$. Par conséquent, il suffit de démontrer le lemme dans le cas où $\lambda = \mu$ et $u = 1$.

Supposons donc que $v_0 \equiv v^\mu \mod \mathfrak{q}V_\mathfrak{o}$. On dira qu'un poids λ est de hauteur $-\sum_i m_i$ si $\mu - \lambda = \sum_i m_i \alpha_i$ par rapport aux racines simples α_i; μ est le seul de hauteur 0, il y a un poids μ_1 et un seul de hauteur -1, et, d'après la condition (D), il y a au moins un poids de hauteur -2 et zéro ne figure pas parmi ces poids-là. D'autre part, tout élément v de $V_\mathfrak{o}$ se décompose en λ-composantes $(\lambda \in \Lambda(\rho))$ et l'on pose

$$v = \sum_\lambda a_\lambda(v)\, v^\lambda + \sum_\alpha b^\alpha(v)\, v_\alpha^0$$

par rapport à la base normalisée de $V_\mathfrak{o}$. On établira en cette étape de la démonstration qu'il existe un élément g de $E_\mathfrak{q}$ tel que

$$a_\mu(gv_0)\,\mathfrak{o} + a_{\mu_1}(gv_0)\,\mathfrak{o} = \mathfrak{o}.$$

Notons d'abord qu'on peut supposer que $a_\mu(v_0) \neq 0$; c'est évident si $\mathfrak{q} \neq \mathfrak{o}$. Dans le cas où $\mathfrak{q} = \mathfrak{o}$, si l'on a $a_\lambda(v_0) \neq 0$ pour un $\lambda \in \Lambda(\rho)^*$, il existe un élément g de $N_\mathfrak{o}$ tel que $a_\mu(gv_0) = a_\lambda(v_0)$; si $a_\lambda(v_0) = 0$ pour tout $\lambda \in \Lambda(\rho)^*$, on trouve un élément $g = x_\alpha(\pm 1)$, $\alpha \in \Delta(\rho)$, tel que $a_\alpha(gv_0) = b^\alpha(v_0) \neq 0$, ce qui nous ramène au cas précédent. Supposons donc que $\mathfrak{o}/a_\mu(v_0)\mathfrak{o}$ soit semi-local. Pour prouver notre assertion ci-dessus, il suffit maintenant de vérifier l'énoncé suivant, en désignant par $\mathfrak{J}(v)$, $v \in V_\mathfrak{o}$, l'ensemble des idéaux maximaux de $\mathfrak{o}$ contenant $a_\mu(v)$ et $a_{\mu_1}(v)$:

Soient $\mathfrak{m}$ *un élément de* $\mathfrak{J}(v_0)$ *et* λ *un poids de* ρ *ayant la hauteur la plus élevée parmi les poids* ν *tels que la* ν*-composante de* v_0 *ne soit pas nulle* $\mathrm{mod}\, \mathfrak{m}V_\mathfrak{o}$. *Alors il existe un élément* g *de* $E_\mathfrak{q}$ *tel que* $\mathfrak{o}/a_\mu(gv_0)\mathfrak{o}$ *soit semi-local, que* $\mathfrak{J}(v_0)$ *contienne* $\mathfrak{J}(gv_0)$ *et que* gv_0 *ait une* λ'*-composante non nulle* $\mathrm{mod}\, \mathfrak{m}V_\mathfrak{o}$ *pour un poids* λ' *d'une hauteur strictement plus élevée que celle de* λ.

En effet, ceci permet d'éliminer l'un après l'autre les éléments de $\mathfrak{J}(v_0)$ en remplaçant v_0 par gv_0 avec un élément g de $E_\mathfrak{q}$. Démontrons l'énoncé ci-dessus; nous traitons deux cas séparément, suivant que λ est égal ou non à 0.

Dans le cas où $\lambda \neq 0$, soit α une racine simple telle que $\lambda + \alpha$ soit un poids de ρ. Si $\alpha = \mu_1 - \mu_2$ pour un poids μ_2 de hauteur -2, on prend un élément t de $\mathfrak{q}$ qui satisfait au lemme 4.1, (b) pour

$$(a_0, a_1, a_2) = (a_\mu(v_0), a_{\mu_1}(v_0), a_{\mu_2}(v_0));$$

sinon, on prend un élément t de $\mathfrak{q}$ qui satisfait au lemme 4.1, (a) pour

$$(a_0, a_1) = (a_\mu(v_0), a_{\mu_1}(v_0)).$$

En posant $g = x_\alpha(\pm t)$, on vérifie alors, d'après les lemmes 2.3 et 4.1, que $\mathfrak{o}/a_\mu(gv_0)\mathfrak{o}$ est semi-local, que $\mathfrak{J}(gv_0)$ est contenu dans $\mathfrak{J}(v_0)$ et que la λ'-composante de gv_0 n'est pas nulle mod $\mathfrak{m}V_\mathfrak{o}$ pour $\lambda' = \lambda + \alpha$ ou $\lambda + 2\alpha$, suivant que $\lambda + \alpha$ est égal ou non à o.

Dans le cas où $\lambda = 0$, soit α une racine simple telle que $b^\alpha(v_0)$ ne soit pas dans $\mathfrak{m}$. On trouve d'abord, d'après le lemme 2.3, un élément $g' = x_{-\alpha}(s)$, $s \in \mathfrak{q}$, tel que $a_{-\alpha}(g'v_0)$ soit dans $\mathfrak{m}$. On choisit ensuite un élément t de $\mathfrak{q}$ pour α et $g'v_0$, comme on l'a fait pour α et v_0 dans le cas précédent. En posant $g = x_\alpha(\pm t)g'$, on voit par les lemmes 2.3 et 4.1 que $\mathfrak{o}/a_\mu(gv_0)\mathfrak{o}$ est semi-local, que $\mathfrak{J}(gv_0)$ est contenu dans $\mathfrak{J}(v_0)$ et que la α-composante de gv_0 n'est pas nulle mod $\mathfrak{m}V_\mathfrak{o}$. Cela achève de démontrer notre énoncé et établit qu'il existe un élément g de $E_\mathfrak{q}$ tel que

$$a_\mu(gv_0)\,\mathfrak{o} + a_{\mu_1}(gv_0)\,\mathfrak{o} = \mathfrak{o}.$$

Supposons donc que $v_0 \equiv v^\mu \bmod \mathfrak{q}V_\mathfrak{o}$ et que $a_0 = a_\mu(v_0)$ et $a_1 = a_{\mu_1}(v_0)$ soient étrangers entre eux. Soit μ_2 un poids de ρ de hauteur -2; on a $\mu_1 = \mu - \alpha_1$ et $\mu_2 = \mu_1 - \alpha_2 \neq 0$, où α_1 et α_2 sont deux racines simples et $\beta = \alpha_1 + \alpha_2$ une racine. Soient s et s' deux éléments de $\mathfrak{o}$ tels que $sa_0 + s'a_1 = 1$. Alors, posant

$$g_1 = x_{-\alpha_2}(\pm s't)\, x_{-\beta}(\pm st), \qquad \text{où} \quad t = (a_0 - 1) - a_{\mu_2}(v_0),$$

on a, pour $v_1 = g_1 v_0$, $a_\mu(v_1) = a_0$ et $a_{\mu_2}(v_1) = a_0 - 1$, en vertu du lemme 2.3. On a donc

$$a_\mu(v_2) = 1 \quad \text{et} \quad a_{\mu_2}(v_2) = a_0 - 1 \qquad \text{pour} \quad v_2 = g_2 v_1,$$

avec $g_2 = x_\beta(\pm 1)$; puis

$$a_\mu(v_3) = 1 \quad \text{et} \quad a_{\mu_2}(v_3) = 0 \qquad \text{pour} \quad v_3 = g_3 v_2,$$

avec $g_3 = x_{-\beta}(\pm(a_0 - 1))$. Par suite, on a encore $a_\mu(v_4) = 1$ pour $v_4 = g_2^{-1} v_3$. On a donc $a_\mu(gv_0) = 1$ pour $g = g_2^{-1} g_3 g_2 g_1$, et g appartient à $E_\mathfrak{q}$ puisque g_1 et g_3 sont dans $E_\mathfrak{q}$.

Cela achève finalement la démonstration du lemme 4.2.

On va maintenant procéder à un théorème de réduction qui aura pour corollaire le lemme 3.2. Puisque ρ est une représentation fondamentale, il existe une seule racine simple α_1 telle que $\mu - \alpha_1$ soit un poids de ρ En posant $\Delta'' = \{\alpha_1\}$ et $\Delta' = \Delta - \Delta''$, nous définissons, comme dans le n° 2, des sous-groupes de G; $G' = G(\Delta')$, $H'' = H(\Delta'')$, $U^+(\Delta')$ et $U^-(\Delta')$. On rappelle que G' est un groupe semi-simple simplement connexe, H'' un tore,

$U^+(\Delta')$ et $U^-(\Delta')$ des groupes unipotents. On a, dans $G_{\mathfrak{o}}$, les sous-groupes correspondants : $G'_{\mathfrak{o}}$, $H''_{\mathfrak{o}}$, $U^+_{\mathfrak{o}}(\Delta')$ et $U^-_{\mathfrak{o}}(\Delta')$.

Théorème 4.3. — *On conserve les hypothèses et notations ci-dessus : en particulier,* G *est de rang* ≥ 2. *On a* $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G'_{\mathfrak{o}})$ *pour tout idéal* $\mathfrak{q}$ *de* $\mathfrak{o}$.

En vue de démontrer ce théorème, rappelons d'abord le théorème de décomposition énoncé dans le nº 2. L'algèbre $\mathbf{Z}[G]$ possède un élément t_μ tel que le morphisme d'algèbres, dual de la multiplication dans G, de $\mathbf{Z}[G](t_\mu^{-1})$ dans $\mathbf{Z}[U^-(\Delta')] \otimes \mathbf{Z}[U^+(\Delta')] \otimes \mathbf{Z}[H''] \otimes \mathbf{Z}[G']$, soit un isomorphisme entre ces deux algèbres. L'image de t_μ est $1 \otimes 1 \otimes \mu'' \otimes 1$, où μ'' est la restriction à H'' de t_μ ou du poids μ. Par suite, l'application π de $U^-_{\mathfrak{o}}(\Delta') \times U^+_{\mathfrak{o}}(\Delta') \times H''_{\mathfrak{o}} \times G'_{\mathfrak{o}}$ dans $G_{\mathfrak{o}}$, définie par

$$\pi(u^-, u^+, h'', g') = u^- u^+ h'' g',$$

est injective et a pour image le sous-ensemble de $G_{\mathfrak{o}}$ formé des éléments g tels que $t_\mu(g)$ soit inversible dans $\mathfrak{o}$. On sait aussi que $\mathbf{Z}[H'']$ est engendrée sur $\mathbf{Z}$ par μ'' et $(\mu'')^{-1}$.

Pour démontrer notre théorème, soit g un élément de $\Gamma_{\mathfrak{q}}$. Considérons la représentation ρ de $G_{\mathfrak{o}}$ dans $V_{\mathfrak{o}}$. On voit aisément que

$$\rho(g)\, v^\mu \equiv v^\mu \bmod \mathfrak{q} V_{\mathfrak{o}}.$$

Par suite, d'après le lemme 4.2, il existe un élément g de $E_{\mathfrak{q}}$ tel que

$$\rho(g_1 g)\, v^\mu \equiv v^\mu \bmod \sum_{\nu \neq \mu} \mathfrak{q} V^\nu_{\mathfrak{o}},$$

ce qui signifie que $t_\mu(g_1 g) = 1$. Par le théorème de décomposition, $g_1 g$ peut donc s'écrire sous la forme $u^- u^+ h'' g'$, où $u^- \in U^-_{\mathfrak{o}}(\Delta')$, $u^+ \in U^+_{\mathfrak{o}}(\Delta')$, $h'' \in H''_{\mathfrak{o}}$ et $g' \in G'_{\mathfrak{o}}$. On a $\mu(h'') = t_\mu(g_1 g) = 1$; d'où $h'' = e$. On voit aussi que u^-, u^+ et g' sont dans $\Gamma_{\mathfrak{q}}$, en vertu de l'unicité de la décomposition analogue dans $G_{\mathfrak{o}}/\mathfrak{q}$. Or on vérifie aisément, d'après la remarque du nº 2 sur les algèbres $\mathbf{Z}[U^-(\Delta')]$ et $\mathbf{Z}[U^+(\Delta')]$, que $U^-_{\mathfrak{o}}(\Delta') \cap \Gamma_{\mathfrak{q}}$ et $U^+_{\mathfrak{o}}(\Delta') \cap \Gamma_{\mathfrak{q}}$ sont contenus dans $E_{\mathfrak{q}}$. Par conséquent, g appartient à $E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G'_{\mathfrak{o}})$. Le théorème est ainsi démontré.

Le corollaire suivant contient le lemme 3.2 :

Corollaire 4.4. — (*a*) *Pour tout* $x \in E_{\mathfrak{o}}$ *et tout* $y \in \Gamma_{\mathfrak{q}}$, *le commutateur* $xyx^{-1}y^{-1}$ *appartient à* $E_{\mathfrak{q}}$.

(*b*) *Si* $\mathfrak{o}$ *est un anneau semi-local,* $\Gamma_{\mathfrak{q}}$ *est égal à* $E_{\mathfrak{q}}$ *même pour* G *de rang* 1.

(*c*) $E_{\mathfrak{q}}$ *est un sous-groupe distingué de* $G_{\mathfrak{o}}$.

(*d*) *Si* $\mathfrak{q}'$ *est un idéal non nul de* $\mathfrak{o}$ *contenu dans* $\mathfrak{q}$, $\Gamma_{\mathfrak{q}}$ *est égal à* $E_{\mathfrak{q}}\Gamma_{\mathfrak{q}'}$.

Rappelons d'abord que $G'_{\mathfrak{o}}$ est le groupe des points à valeurs dans $\mathfrak{o}$ du schéma en groupes sur $\mathfrak{o}$ déduit du schéma en groupes sur $\mathbf{Z}$ associé au groupe semi-simple simplement connexe G' et que les sous-groupes radiciels de $G'_{\mathfrak{o}}$ sont également des sous-groupes radiciels de $G_{\mathfrak{o}}$; ce qui nous permettra parfois de raisonner par récurrence sur le rang de G. Démontrons l'énoncé (a). Soit x un élément de $U^+_{\mathfrak{o}}(\Delta')$; si y est un élément de $\Gamma_{\mathfrak{q}} \cap G'_{\mathfrak{o}}$, le commutateur $xyx^{-1}y^{-1}$ est dans $U^+_{\mathfrak{o}}(\Delta') \cap \Gamma_{\mathfrak{q}}$, donc dans $E_{\mathfrak{q}}$; on en déduit, compte tenu du théorème 4.3, que $xyx^{-1}y^{-1}$ est dans $E_{\mathfrak{q}}$ pour tout $y \in \Gamma_{\mathfrak{q}}$. Par suite, comme chaque sous-groupe radiciel $U^{\alpha}_{\mathfrak{o}}$ de $G_{\mathfrak{o}}$ a dans $U^+_{\mathfrak{o}}(\Delta')$ un conjugué par un élément de $\mathfrak{N}_{\mathfrak{o}}$, l'énoncé (a) est vérifié pour tout élément x de $U^{\alpha}_{\mathfrak{o}}$. Puisque $E_{\mathfrak{o}}$ est engendré par les groupes radiciels, cela entraîne aussitôt notre assertion pour tout élément x de $E_{\mathfrak{o}}$. Quant à l'énoncé (b), on voit aisément qu'il est vrai pour le groupe de rang 1, i. e. pour SL_2. Par suite, on conclut du théorème 4.3, par récurrence sur le rang de G, qu'il est vrai pour G. Pour prouver l'énoncé (c), supposons que $\mathfrak{q}$ soit un idéal non nul (si $\mathfrak{q} = \{0\}$, il est trivial). Alors le groupe $G_{\mathfrak{o}}/\mathfrak{q}$ est engendré par des sous-groupes radiciels; d'où $G_{\mathfrak{o}} = \Gamma_{\mathfrak{q}} E_{\mathfrak{o}}$. Par suite, $E_{\mathfrak{q}}$ est un sous-groupe distingué de $G_{\mathfrak{o}}$, car, d'après (a), $\Gamma_{\mathfrak{q}}$ normalise $E_{\mathfrak{q}}$. L'énoncé (d) est une conséquence immédiate de (b).

COROLLAIRE 4.5. — *Soient* α *une racine longue dans* Δ *et* G^{α} *le sous-groupe simple de* G *engendré par* U^{α} *et* $U^{-\alpha}$. *Si* $G^{\alpha}_{\mathfrak{o}}$ *désigne le sous-groupe de* $G_{\mathfrak{o}}$ *correspondant à* G^{α}, *on a* $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G^{\alpha}_{\mathfrak{o}})$ *pour tout idéal* $\mathfrak{q}$ *de* $\mathfrak{o}$.

En effet, d'après le théorème 4.3, on a $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G'_{\mathfrak{o}})$ pour un sous-groupe semi-simple G' de rang $r - 1$, où r est le rang de G. En raisonnant par récurrence sur le rang de G, on a donc $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}} \prod_{\beta} (\Gamma_{\mathfrak{q}} \cap G^{\beta}_{\mathfrak{o}})$, les éléments β de Δ étant convenablement rangés. Or Δ possède un ou deux éléments β et γ tels que tout élément de Δ puisse se transformer en β ou γ par un élément du groupe de Weyl W et que β et γ ne soient pas orthogonaux. Soit alors $G^{\beta\gamma}$ le sous-groupe de G engendré par G^{β} et G^{γ}. Pour chaque δ de Δ, il existe un élément n de $\mathfrak{N}_{\mathfrak{o}}$ tel que $n G^{\delta}_{\mathfrak{o}} n^{-1} \subset G^{\beta\gamma}_{\mathfrak{o}}$; on a donc $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G^{\beta\gamma}_{\mathfrak{o}})$ d'après le corollaire 4.4. En appliquant le théorème 4.3 au groupe $G^{\beta\gamma}$, on déduit de là que $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G^{\delta}_{\mathfrak{o}})$, δ étant l'une des racines β et γ; d'après la démonstration du lemme 2.2, δ doit être une racine longue dans les cas de rang 2. Cela entraîne aussitôt notre corollaire.

On observera aussi les remarques suivantes sur les groupes de divers types.

a. Si G est simple de rang $\geqq 2$, on peut choisir la représentation ρ vérifiant les conditions (C) et (D) de telle sorte que G' soit, lui aussi, simple.

b. Si G est de type non symplectique de rang $\geqq 3$, Δ contient deux racines longues α, β non orthogonales; d'après le corollaire 4.5, on a $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G_{\mathfrak{o}}^{\alpha\beta})$, où $G^{\alpha\beta}$ est un groupe simple de type A_2. Par contre, si G est de type symplectique, deux racines longues non opposées sont toujours orthogonales. Pour le groupe de type G_2, les sous-groupes radiciels U^{α} correspondant aux racines longues engendrent un groupe simple $G^{\alpha\beta}$ simplement connexe de type A_2; on a donc $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}(\Gamma_{\mathfrak{q}} \cap G_{\mathfrak{o}}^{\alpha\beta})$.

c. Si G est de rang $\geqq 2$, le commutateur $xyx^{-1}y^{-1}$ appartient à $E_{\mathfrak{q}}$ pour tout $x \in G_{\mathfrak{o}}$ et $y \in \Gamma_{\mathfrak{q}}$; autrement dit, $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ *est central dans* $G_{\mathfrak{o}}/E$. Compte tenu du corollaire 4.4, cela équivaut à dire que $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ est abélien. Pour les groupes de rang $\geqq 3$ et le groupe de type C_2, ceci résulte facilement des corollaires 4.4 et 4.5, parce que le système de racines Φ possède, dans ces cas-là, deux racines longues orthogonales entre elles. Pour les groupes de types A_2 et G_2, notre assertion résulte, compte tenu de la remarque précédente, d'un théorème de Mennicke, qui entraîne en particulier que $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ est abélien pour $G = SL_3$ (*voir* [4], théor. 5.4, lemme 2.9).

La question d'évaluer les groupes $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ est ainsi ramenée, dans une certaine mesure, aux cas des groupes SL_2, SL_3 et Sp_4 :

Corollaire 4.6. — *Le groupe* $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ *pour* G *de rang* $\geqq 2$ *est isomorphe à un quotient du groupe correspondant soit pour* SL_3, *soit pour* Sp_4. *En particulier, on a* $G_{\mathfrak{o}} = E_{\mathfrak{o}}$ *pour* G *de rang* $\geqq 2$ *si cela est vrai, soit pour* SL_2, *soit pour* SL_3 *et* Sp_4.

CHAPITRE II.

Extensions centrales d'un groupe simple déployé.

5. Nous étudierons dans ce chapitre, suivant la méthode de R. Steinberg [30] et de C. Moore [26], les extensions centrales du groupe G_k, où G est un groupe simple simplement connexe déployé sur un corps k.

Nous reprenons les notations du n° 3; k est un corps et G_k est le groupe des points rationnels du groupe simple simplement connexe déployé sur k défini à partir d'un schéma $\mathfrak{G}$ en groupes déployés sur $\mathbf{Z}$.

On sait ([13], [16]) que le groupe G_k est engendré par les sous-groupes radiciels U_k^{α} ($\alpha \in \Phi$) et que ces générateurs satisfont aux relations suivantes (R 1), (R 2) et (R 3), x_α désignant l'isomorphisme choisi de k sur U_k^{α} :

(R 1) $x_\alpha(u)\, x_\alpha(v) = x_\alpha(u+v)$ pour tout $\alpha \in \Phi$ et $u, v \in k$;

(R 2) (i) $x_\alpha(u)\, x_\beta(v)\, x_\alpha(u)^{-1}\, x_\beta(v)^{-1} \prod\limits_{i,j \in \mathbf{N}^*} x_{i\alpha+j\beta}\,(N_{\alpha,\beta:i,j}\; u^i\, v^j)$ pour tout α,

$\beta \in \Phi$ tels que $\alpha + \beta \neq 0$ et pour tout u, $v \in k$; où les $N_{\alpha, \beta : i, j}$ sont certains entiers rationnels;

(ii) $w_\alpha(u)\, x_\alpha(v)\, w_\alpha(u)^{-1} = x_{-\alpha}(-u^{-2} v)$ pour tout $\alpha \in \Phi$, $u \in k^\times$ et $v \in k$, avec $w_\alpha(u) = x_\alpha(u)\, x_{-\alpha}(-u^{-1})\, x_\alpha(u)$;

(R 3) $h_\alpha(u)\, h_\alpha(v) = h_\alpha(uv)$ pour tout $\alpha \in \Phi$ et u, $v \in k^\times$, avec $h_\alpha(u) = w_\alpha(u)\, w_\alpha(1)^{-1}$.

R. Steinberg [30] a démontré les résultats suivants :

a. (R 1), (R 2) et (R 3) forment une famille exhaustive de relations pour les générateurs $x_\alpha(u)$ du groupe abstrait G_k.

b. Soit $E(G_k)$ le groupe engendré par les mêmes générateurs soumis aux seules relations (R 1) et (R 2). Alors, le noyau $\pi_1(G_k)$ du morphisme naturel p de $E(G_k)$ sur G_k est central dans $E(G_k)$. Si k est un corps fini, $\pi_1(G_k)$ se réduit à $\{e\}$.

c. $E(G_k)$ est égal à son groupe des commutateurs sauf si $k = \mathbf{F}_2$, $G = SL_2$, Sp_4, G_2 ou si $k = \mathbf{F}_3$, $G = SL_2$.

d. Si k possède au moins 11 éléments, toute extension centrale de $E(G_k)$ est triviale.

Ces résultats affirment, en langage homologique, que si A est un G_k-module trivial, le groupe de cohomologie $H^2(G_k, A)$ est isomorphe au groupe $\mathrm{Hom}(\pi_1(G_k), A)$ des morphismes de $\pi_1(G_k)$ dans A, lorsque k a assez d'éléments.

Dans ce numéro et les suivants, on supposera sauf mention du contraire que k est un corps infini, et l'on écrira simplement X au lieu de X_k pour un sous-groupe X de G.

Commençons par examiner de plus près le résultat de Steinberg.

Soit A un groupe abélien et soit E une extension centrale de G_k par A :

$$1 \to A \to E \xrightarrow{\pi} G_k \to 1.$$

D'après [30], il existe des relèvements $r(U^\alpha)$ dans E des groupes radiciels U^α de telle sorte que les éléments $\tilde{x}_\alpha(u) = r(x_\alpha(u))$ satisfassent aux relations (R 1) et (R 2). Posons alors, pour tout $\alpha \in \Phi$ et $t \in k^\times$,

$$\tilde{w}_\alpha(t) = \tilde{x}_\alpha(t)\, \tilde{x}_{-\alpha}(-t^{-1})\, \tilde{x}_\alpha(t) \qquad \text{et} \qquad \tilde{h}_\alpha(t) = \tilde{w}_\alpha(t)\, \tilde{w}_\alpha(1)^{-1}.$$

On a d'abord le lemme suivant ([30], [16]) :

LEMME 5.1. — (*a*) *Pour tout* $\alpha \in \Phi$, x_α *définit un isomorphisme de* k *sur* $\tilde{U}^\alpha$. *Soit* $\tilde{U}^+$ [*resp.* $\tilde{U}^-$] *le sous-groupe de* E *engendré par les* $\tilde{U}^\beta$ [*resp. les* $\tilde{U}^{-\beta}$], $\beta \in \Phi^+$. *Alors* π *induit un isomorphisme de* $\tilde{U}^+$ [*resp. de* $\tilde{U}^-$] *sur* U^+ [*resp.* U^-].

(*b*) *Soient* α *et* β *des éléments de* Φ. *On a*

$$\tilde{w}_\alpha(t)\,\tilde{x}_\beta(u)\,\tilde{w}_\alpha(t)^{-1} = \tilde{x}_{\sigma_\alpha\beta}(\eta t^{-c}u)$$

pour tout $t \in k^\times$ *et* $u \in k$; *où* $\sigma_\alpha \in \mathrm{W}$ *est la réflexion associée à* α, c *l'entier de Cartan* $\beta\alpha^\star$ *relatif à* β *et* α, *et* η *une constante* $\eta(\alpha, \beta)$ *égale à* ± 1.

(*c*) *On a*

$$\eta(\alpha, \beta) = \eta(\alpha, -\beta); \qquad \eta(\alpha, \alpha) = \eta(\alpha, -\alpha) = -1;$$
$$\eta(\alpha, \beta) = 1 \quad \text{si} \quad \alpha \pm \beta \neq 0, \quad \alpha \pm \beta \notin \Phi;$$
$$\eta(\alpha, \beta)\,\eta(\beta, \alpha) = -1 \quad si \quad \alpha\beta^\star = \beta\alpha^\star = -1;$$
$$\eta(\alpha, \beta) = -1 \quad si \quad \alpha\beta^\star = 0, \quad \alpha \pm \beta \in \Phi.$$

Ce lemme permet de déduire diverses relations entre les éléments $\tilde{x}_\alpha(u)$ Nous en recueillons quelques-unes [30] :

Lemme 5.2. — *On a les relations suivantes :*

(*a*) $$\tilde{w}_\alpha(t)\,\tilde{w}_\beta(u)\,\tilde{w}_\alpha(t)^{-1} = \tilde{w}_{\sigma_\alpha\beta}(\eta\, t^{-c}u);$$

(*b*) $$\tilde{w}_\alpha(t)\,\tilde{h}_\beta(u)\,\tilde{w}_\alpha(t)^{-1} = \tilde{h}_{\sigma_\alpha\beta}(\eta t^{-c}u)\,\tilde{h}_{\sigma_\alpha\beta}(\eta t^{-c})^{-1};$$

(*c*) $$\tilde{h}_\alpha(t)\,\tilde{x}_\beta(u)\,\tilde{h}_\alpha(t)^{-1} = \tilde{x}_\beta(t^c u),$$
$$\tilde{h}_\alpha(t)\,\tilde{x}_\alpha(u)\,\tilde{h}_\alpha(t)^{-1}\tilde{x}_\alpha(u)^{-1} = \tilde{x}_\alpha(u(t^2-1));$$

(*d*) $$\tilde{h}_\alpha(t)\tilde{w}_\beta(u)\,\tilde{h}_\alpha(t)^{-1} = \tilde{w}_\beta(t^c u);$$

(*e*) $$\tilde{h}_\alpha(t)\,\tilde{h}_\beta(u)\,\tilde{h}_\alpha(t)^{-1} = \tilde{h}_\beta(t^c u)\,\tilde{h}_\beta(t^c)^{-1}, \qquad c = \beta\alpha^\star;$$

(*f*) $$\tilde{w}_\alpha(1)\,\tilde{h}_\beta(t)\,\tilde{w}_\alpha(1)^{-1} = \tilde{h}_\beta(t)\,\tilde{h}_\alpha(t^{-d}), \qquad d = \alpha\beta^\star;$$

(*g*) $$\tilde{w}_\alpha(t) = \tilde{w}_{-\alpha}(-t^{-1}), \qquad \tilde{h}_\alpha(t) = \tilde{h}_{-\alpha}(t)^{-1},$$
$$\tilde{w}_\alpha(1)\,\tilde{h}_\alpha(t)\,\tilde{w}_\alpha(1)^{-1} = \tilde{h}_\alpha(t^{-1});$$

(*h*) $$\tilde{w}_\alpha(1)^{-1}\tilde{x}_\alpha(t)\,\tilde{w}_\alpha(1) = \tilde{x}_{-\alpha}(-t) = \tilde{x}_\alpha(-t^{-1})\,\tilde{w}_\alpha(t^{-1})\,\tilde{x}_\alpha(-t^{-1}), \qquad t \neq 0.$$

Posons $\tilde{\mathrm{H}} = \pi^{-1}(\mathrm{H})$, $\tilde{\mathrm{N}} = \pi^{-1}(\mathrm{N})$, et rappelons la décomposition de Bruhat de $\mathrm{G}_k : \mathrm{G}_k = \mathrm{U}^+\mathrm{N}\mathrm{U}^- = \mathrm{U}^+\mathrm{N}\mathrm{U}^+$. En la relevant dans E, on a $\mathrm{E} = \tilde{\mathrm{U}}^+\tilde{\mathrm{N}}\,\tilde{\mathrm{U}}^- = \tilde{\mathrm{U}}^+\tilde{\mathrm{N}}\,\tilde{\mathrm{U}}^+$. Le lemme suivant précise cette décomposition de E :

Lemme 5.3. — (*a*) *Pour tout élément* $\tilde{n}$ *de* $\tilde{\mathrm{N}}$, $\tilde{\mathrm{U}}^+\tilde{n}\tilde{\mathrm{U}}^+ \cap \tilde{\mathrm{N}}$ *se réduit à* $\{\tilde{n}\}$.

(*b*) *On définit comme suit des applications* ν *et* $\tilde{\nu}$:

$$\nu : \ \mathrm{G}_k \to \mathrm{N}, \quad \nu(unu') = n \quad pour \quad u, u' \in \mathrm{U}^+ \quad et \quad n \in \mathrm{N};$$
$$\tilde{\nu} : \ \mathrm{E} \to \tilde{\mathrm{N}}, \quad \tilde{\nu}(\tilde{u}\,\tilde{n}\,\tilde{u}') = \tilde{n} \quad pour \quad \tilde{u}, \tilde{u}' \in \tilde{\mathrm{U}}^+ \quad et \quad \tilde{n} \in \tilde{\mathrm{N}}.$$

Alors on a $\nu \circ \pi = \pi \circ \tilde{\nu}$.

(*c*) $\tilde{\nu}(\tilde{u}\,\tilde{g}) = \tilde{\nu}(\tilde{g})$ *pour tout* $\tilde{u} \in \mathrm{U}^+$ *et* $\tilde{g} \in \mathrm{E}$;
$\tilde{\nu}(\tilde{h}\,\tilde{g}) = \tilde{h}\,\tilde{\nu}(\tilde{g})$ *pour tout* $\tilde{h} \in \tilde{\mathrm{H}}$ *et* $\tilde{g} \in \mathrm{E}$.

(*d*) *Soit* α *une racine simple. Alors, pour un élément* $\tilde{g}$ *de* E, $\tilde{\nu}(\tilde{w}_\alpha(-1)\tilde{g})$ *est égal ou bien à* $\tilde{w}_\alpha(-1)\tilde{\nu}(\tilde{g})$ *ou bien à* $\tilde{h}_\alpha(t^{-1})\tilde{\ }(\tilde{g})$ *avec un élément* t *de* $k^\times$.

Démontrons d'abord l'énoncé (*a*), qui justifie la définition de $\tilde{\nu}$. L'énoncé analogue pour G_k est bien connu, et si n est un élément de N, $U_n^+ = U^+ \cap nU^+n^{-1}$ est engendré par des groupes radiciels U^β. Supposons que $\tilde{n}' = \tilde{u}\,\tilde{n}\,\tilde{u}'$, avec $\tilde{n}$, $\tilde{n}'$ dans $\tilde{N}$ et $\tilde{u}$, $\tilde{u}'$ dans $\tilde{U}^+$. En descendant à G_k, on voit d'abord que $\tilde{n}' = \tilde{n}a$ avec un élément a de A. On a donc $a = (\tilde{n}^{-1}\tilde{u}\,\tilde{n})\tilde{u}'$. Ceci montre que $\pi(\tilde{u}) \in U_n^+$ pour $n = \pi(\tilde{n})$, et donc que $\tilde{u}$ appartient au relèvement $\tilde{U}_n^+$ de U_n^+ dans $\tilde{U}^+$. Or, comme $\tilde{U}_n^+$ est engendré par des sous-groupes radiciels $\tilde{U}^\beta$, on a $\tilde{n}^{-1}\tilde{U}_n^+\tilde{n} \subset \tilde{U}^+$, en vertu du lemme 5.1, (*b*), qui entraîne que tout élément de $\tilde{N}$ permute entre eux les groupes radiciels $\tilde{U}^\gamma$. Il en résulte que $a \in \tilde{U}^+$; d'où $a = e$. Cela prouve l'énoncé (*a*). Les assertions (*b*) et (*c*) sont maintenant évidentes. Examinons (*d*). Notons d'abord que $\tilde{U}_\alpha^+ = \tilde{U}^+ \cap \tilde{w}_\alpha(1)\tilde{U}^+\tilde{w}_\alpha(1)^{-1}$ est le sous-groupe de $\tilde{U}^+$ engendré par les groupes radiciels $\tilde{U}^\beta$ pour $\beta \in \Phi^+$, $\beta \neq \alpha$, et qu'on a

$$\tilde{U}^+ = \tilde{U}_\alpha^+\tilde{U}^\alpha, \qquad \tilde{U}_\alpha^+ \cap \tilde{U}^\alpha = \{e\}.$$

Posons $\tilde{g} = \tilde{u}\,\tilde{n}\,\tilde{u}'$, avec $\tilde{n} = \nu(\tilde{g})$ et $\tilde{u}$, $\tilde{u}'$ dans $\tilde{U}^+$, et puis $\tilde{u} = \tilde{u}_1\tilde{x}_\alpha(t)$, avec $\tilde{u}_1 \in \tilde{U}_\alpha^+$ et $t \in k$. On a $\tilde{n}^{-1}\tilde{U}^\alpha\tilde{n} = \tilde{U}^{\sigma^{-1}\alpha}$, avec $\sigma = \omega(\pi(\tilde{n}))$, où ω est le morphisme canonique de N sur W. Nous distinguons maintenant deux cas :

(i) Si $\tilde{n}^{-1}\tilde{x}_\alpha(t)\tilde{n}$ est dans $\tilde{U}^+$, autrement dit si $\sigma^{-1}\alpha > 0$ ou si $t = 0$, alors on a

$$\tilde{w}_\alpha(-1)\,\tilde{g} = \tilde{w}_\alpha(-1)\,\tilde{u}_1\tilde{w}_\alpha(1)\,.\,\tilde{w}_\alpha(-1)\,\tilde{n}\,.\,\tilde{n}^{-1}\tilde{x}_\alpha(t)\,\tilde{n}\,.\,\tilde{u}' = \tilde{u}_2\,\tilde{w}_\alpha(-1)\,\tilde{n}\,\tilde{u}'_2,$$
$$\text{avec}\quad \tilde{u}_2 \in \tilde{U}_\alpha^+ \quad\text{et}\quad \tilde{u}'_2 \in \tilde{U}^+.$$

D'où

$$\tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}) = \tilde{w}_\alpha(-1)\,\tilde{\nu}(\tilde{g}).$$

(ii) Si $\sigma^{-1}\alpha < 0$ et $t \neq 0$, alors on a

$$\begin{aligned}\tilde{w}_\alpha(-1)\,\tilde{g} &= \tilde{w}_\alpha(-1)\,\tilde{u}_1\tilde{w}_\alpha(1)\,.\,\tilde{w}_\alpha(-1)\,\tilde{x}_\alpha(t)\,\tilde{w}_\alpha(1)\,.\,\tilde{w}_\alpha(-1)\,\tilde{n}\,\tilde{u}'\\ &= \tilde{u}_2\tilde{x}_\alpha(-t^{-1})\,\tilde{w}_\alpha(t^{-1})\,\tilde{x}^\alpha(-t^{-1})\,.\,\tilde{w}_\alpha(-1)\,\tilde{n}\,\tilde{u}', \qquad \text{avec}\quad \tilde{u}_2 \in \tilde{U}_\alpha^+\\ &= \tilde{u}_2\,x_\alpha(-t^{-1})\,\tilde{w}_\alpha(t^{-1})\,\tilde{w}_\alpha(-1)\,\tilde{n}\,\tilde{u}'_2, \qquad \text{avec}\quad \tilde{u}'_2 \in \tilde{U}^+.\end{aligned}$$

D'où

$$\tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}) = \tilde{w}_\alpha(t^{-1})\,\tilde{w}_\alpha(-1)\,\tilde{n} = \tilde{h}_\alpha(t^{-1})\,\tilde{n}.$$

L'assertion (*d*) est donc démontrée.

Nous nous intéresserons désormais à certains cocycles sur $k^\times$ à valeurs dans A.

Pour chaque $\alpha \in \Phi$, on définit une application c_α de $k^\times \times k^\times$ dans A par

$$c_\alpha(s,t) = \tilde{h}_\alpha(s)\,\tilde{h}_\alpha(t)\,\tilde{h}_\alpha(st)^{-1};$$

c'est un cocycle normalisé sur $k^{\times}$ à valeurs dans A. Le cocycle c_α sera appelé le *cocycle de Steinberg en* α de E relatif aux isomorphismes x_α. Rappelons qu'on a choisi une fois pour toutes les isomorphismes x_α du groupe additif sur les sous-groupes radiciels U^α de G_k; nous verrons à la fin de ce numéro qu'en général l'application $\tilde{h}_\alpha$ et le cocycle c_α dépendent du choix de x_α et $x_{-\alpha}$, tandis que le monomorphisme h_α du groupe multiplicatif dans H n'en dépend pas. Néanmoins, quand on a choisi les isomorphismes x_α, le cocycle c_α est uniquement déterminé par E ou même par la classe d'extensions de E, car les isomorphismes relevés $\tilde{x}_\alpha$ sont, d'après le lemme 5.2, (*c*), uniquement déterminés par E.

On va étudier les propriétés des cocycles c_α.

Lemme 5.4. — (*a*) $c_\alpha(s, t) = c_{-\alpha}(t, s)^{-1}$ *pour tout* $\alpha \in \Phi$.

(*b*) *S'il existe un élément* σ *du groupe de Weyl* W *tel que* $\beta = \sigma\alpha$, *alors* c_β *est identique à* c_α *ou à* $c_{-\alpha}$.

(*c*) *Pour tout* $\alpha, \beta \in \Phi$, *on a*

$$\tilde{h}_\alpha(s)\,\tilde{h}_\beta(t)\,\tilde{h}_\alpha(s)^{-1}\,\tilde{h}_\beta(t)^{-1} = c_\alpha(s, t^d) = c_\beta(t, s^c)^{-1},$$

où $c = \beta\alpha^\star$ *et* $d = \alpha\beta^\star$.

(*d*) *Les cocycles* c_α *sont des applications bilinéaires de* $k^\times \times k^\times$ *dans* A *sauf éventuellement pour les racines longues* α *d'un groupe symplectique* G.

L'énoncé (*a*) est une conséquence immédiate du lemme 5.2, (*g*). L'assertion (*b*) résulte du lemme 5.2, (*b*), car celui-ci affirme que, si $\beta = \sigma_\alpha\gamma$, on a ou bien

$$\tilde{w}_\alpha(1)\,\tilde{h}_\gamma(u)\,\tilde{w}_\alpha(1)^{-1} = \tilde{h}_\beta(u)$$

ou bien

$$\tilde{w}_\beta(1)\,\tilde{w}_\alpha(1)\,\tilde{h}_\gamma(u)\,\tilde{w}_\alpha(1)^{-1}\,\tilde{w}_\beta(1)^{-1} = \tilde{h}_{-\beta}(u).$$

L'énoncé (*c*) se déduit facilement du lemme 5.2, (*e*), et il implique que $c_\alpha(s, t^d)$, où $d = \alpha\beta^\star$, est une fonction bilinéaire de (s, t). D'où résulte la dernière assertion, compte tenu du fait que pour une racine α il en existe une autre β telle que $\alpha\beta^\star = 1$, sauf si α est une racine longue dans le système de racines de type symplectique.

On a ensuite la proposition suivante, en considérant le cas du groupe G de rang 1 :

Proposition 5.5. — *Les cocycles* c_α *satisfont aux équations suivantes :*

(S 1) $$c(x, y)\,c(xy, z) = c(x, yz)\,c(y, z);$$

(S 2) $$c(1, 1) = 1; \qquad c(x, y) = c(x^{-1}, y^{-1});$$

(S 3) $$c(x, y) = c(x, (1 - x)\,y) \qquad si \quad x \neq 1.$$

En effet, (S 1) n'est autre que l'identité de cocycle, et (S 2) est entraîné immédiatement par le lemme 5.2, (*g*). Reste à vérifier l'identité (S 3). Nous voyons d'abord que $c_\alpha(t, -t^{-1}) = 1$ pour tout $t \in k^\times$; en effet, d'après le lemme 5.2, (*a*), (*g*),

$$\begin{aligned} c_\alpha(t, -t^{-1}) &= \tilde{h}_\alpha(t)\,\tilde{h}_\alpha(-t^{-1})\,\tilde{h}_\alpha(-1)^{-1} \\ &= \tilde{w}_\alpha(t)\,\tilde{w}_\alpha(-1)\,\tilde{w}_\alpha(-t^{-1})\,\tilde{w}_\alpha(-1)\,\tilde{w}_\alpha(-1)^{-2} \\ &= \tilde{w}_\alpha(t)\,\tilde{w}_{-\alpha}(t^{-1}) = \tilde{w}_\alpha(t)\,\tilde{w}_\alpha(-t) = 1. \end{aligned}$$

Cette identité, combinée avec (S 1), entraîne que

$$c_\alpha(s, t) = c_\alpha(s, t)\,c_\alpha(st, -s^{-1}t^{-1}) = c_\alpha(s, -s^{-1})\,c_\alpha(t, -s^{-1}t^{-1}) = c_\alpha(t, -s^{-1}t^{-1});$$

ce qui, en se répétant, donne l'identité

$$c_\alpha(s, t) = c_\alpha(-s^{-1}t^{-1}, s).$$

Calculons maintenant

$$\tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1)) \qquad \text{pour} \quad \tilde{g} = \tilde{x}_\alpha(u)\,\tilde{w}_\alpha(1)\,\tilde{x}_\alpha(v) \qquad \text{avec} \quad uv(1-uv) \neq 0.$$

D'une part, d'après le lemme 5.2, (*g*),

$$\begin{aligned} \tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1) &= \tilde{w}_\alpha(-1)\,\tilde{x}_\alpha(u)\,\tilde{w}_\alpha(1)\,\tilde{x}_\alpha(v)\,\tilde{w}_\alpha(-1) \\ &= \tilde{w}_\alpha(-1)\,\tilde{x}_\alpha(u - v^{-1})\,\tilde{w}_\alpha(v^{-1})\,\tilde{x}_\alpha(-v^{-1}); \end{aligned}$$

d'où, d'après le lemme 5.3, (*d*),

$$\begin{aligned} \tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1)) &= \tilde{h}_\alpha((u - v^{-1})^{-1})\,\tilde{w}_\alpha(v^{-1}) \\ &= \tilde{h}_\alpha((u - v^{-1})^{-1})\,\tilde{h}_\alpha(v^{-1})\,\tilde{w}_\alpha(1). \end{aligned}$$

D'autre part,

$$\begin{aligned} \tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1) &= \tilde{x}_\alpha(-u^{-1})\,\tilde{h}_\alpha(u^{-1})\,\tilde{w}_\alpha(1)\,\tilde{x}_\alpha(v - u^{-1})\,\tilde{w}_\alpha(-1) \\ &= \tilde{x}_\alpha(-u^{-1})\,\tilde{h}_\alpha(u^{-1})\,\tilde{x}_\alpha(-(v-u^{-1})^{-1})\,\tilde{w}_\alpha((v-u^{-1})^{-1})\,\tilde{x}_\alpha(-(v-u^{-1})^{-1}); \end{aligned}$$

d'où

$$\begin{aligned} \tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1)) &= \tilde{h}_\alpha(u^{-1})\,\tilde{w}_\alpha((v - u^{-1})^{-1}) \\ &= \tilde{h}_\alpha(u^{-1})\,\tilde{h}_\alpha((v - u^{-1})^{-1})\,\tilde{w}_\alpha(1). \end{aligned}$$

Mettant en comparaison ces deux expressions de $\tilde{\nu}(\tilde{w}_\alpha(-1)\,\tilde{g}\,\tilde{w}_\alpha(-1))$, on a

$$c_\alpha(u^{-1}, (v - u^{-1})^{-1}) = c_\alpha((u - v^{-1})^{-1}, v^{-1});$$

donc, d'après (S 2),

$$c_\alpha(u, v - u^{-1}) = c_\alpha(u - v^{-1}, v).$$

D'où, en appliquant aux deux membres l'identité

$$c_\alpha(s, t) = c_\alpha(-s^{-1}t^{-1}, s),$$

on déduit que

$$c_\alpha((1-uv)^{-1}, u) = c_\alpha((1-uv)^{-1}, u - v^{-1}).$$

En substituant t à $(1 - uv)^{-1}$, on en conclut que

$$c_\alpha(t, u) = c_\alpha(t, u(1-t)^{-1}).$$

D'où l'identité (S 3). Notre proposition est ainsi démontrée.

Le lemme suivant est facile à prouver :

LEMME 5.6. — *Les équations* (S 1), (S 1) *et* (S 3) *sont vérifiées par toute application c de $k^\times \times k^\times$ dans* A *satisfaisant aux suivantes :*

(S⁰ 1) $$c(x, yz) = c(x, y)\, c(x, z)\,;$$

(S⁰ 2) $$c(xy, z) = c(x, z)\, c(y, z)\,;$$

(S⁰ 3) $$c(x, 1-x) = 1 \quad si \quad x \neq 1.$$

On appellera *cocycle de Steinberg* sur $k^\times$ à valeurs dans A toute application c de $k^\times \times k^\times$ dans A vérifiant les équations (S 1), (S 2) et (S 3). Un tel cocycle c sera dit *bilinéaire* si c satisfait aux équations (S⁰ 1), (S⁰ 2) et (S⁰ 3). On sait [30] que, si k est un corps fini, toute application de $k^\times \times k^\times$ dans A vérifiant (S 1), (S 2) et (S 3) est triviale quel que soit A.

Notons $S(k^\times, A)$ le groupe multiplicatif des cocycles de Steinberg et $S^0(k^\times, A)$ le sous-groupe des cocycles de Steinberg bilinéaires sur $k^\times$ à valeurs dans A.

La proposition suivante donne des propriétés fondamentales d'un cocycle de Steinberg :

PROPOSITION 5.7. — *Soit c un cocycle de Steinberg sur $k^\times$ à valeurs dans* A. *Alors :*

(*a*) *On a*

$$c(x, y) = c(x, -xy) = c(-xy, y) = c(y^{-1}, x)$$

et

$$c(x^2, y) = c(x, y^2)$$

pour tout $x, y \in k^\times$.

(*b*) *L'application $c^\natural$ définie par $c^\natural(x, y) = c(x, y^2)$ est un cocycle de Steinberg bilinéaire. On a $c^\natural(x, -1) = 1$ pour tout $x \in k^\times$.*

(*c*) *L'application $\check{c}$ définie par $\check{c}(x, y) = c(y, x)^{-1}$ est un cocycle de Steinberg. On a $c^\natural = (\check{c})^\natural = c\check{c}$. Si c est bilinéaire, on a $\check{c} = c$ et $c^\natural = c^2$.*

(*d*) *L'extension centrale de $k^\times$ par* A *définie par le cocycle c est un groupe abélien si et seulement si $c^\natural$ est trivial.*

Notons tout d'abord que c est un cocycle normalisé. D'après les conditions (S 2) et (S 3), on a

$$\begin{aligned} c(x, y) &= c(x^{-1}, y^{-1}) = c(x^{-1}, (1 - x^{-1})\, y^{-1}) \\ &= c(x, (1 - x^{-1})^{-1} y) = c(x, -(1-x)^{-1} xy) = c(x, -xy)\,; \end{aligned}$$

ce qui donne une partie de (a) et entraîne que

$$c(x, -x^{-1}) = c(x, 1) = 1$$

pour tout $x \in k^{\times}$. Par suite, on a

$$c(y, -1) = c(y, -1)\, c(x, -x^{-1}) = c(y, x)\, c(yx, -x^{-1});$$

d'où

$$c(y, y)^{-1}\, c(xy, y) = c(y, -1)^{-1}\, c(xy, -x^{-1}) = c(y, x)^{-1}.$$

On voit donc que

$$c(x, y^2) = c(x, y)\, c(xy, y)\, c(y, y)^{-1} = c(x, y)\, c(y, x)^{-1};$$

ce qui signifie $c^{\natural} = c\check{c}$ dans nos notations.

Considérons l'extension $\mathfrak{e}$ de $k^{\times}$ définie à partir du cocycle c. L'identité $c^{\natural} = c\check{c}$ montre qu'on a

$$c^{\natural}(x, y) = \mathfrak{s}(x)\, \mathfrak{s}(y)\, \mathfrak{s}(x)^{-1}\, \mathfrak{s}(y)^{-1}$$

pour une section $\mathfrak{s}$ de $\mathfrak{e}$; cela prouve l'énoncé (d), et entraîne que $c^{\natural}$ est une application bilinéaire de $k^{\times} \times k^{\times}$ dans A. Puisque la condition (S^0 3) pour $c^{\natural}$ est une conséquence immédiate de (S 3) pour c, on en conclut que $c^{\natural}$ est un cocycle de Steinberg bilinéaire. Alors, $\check{c} = c^{\natural} c^{-1}$ est aussi un cocycle de Steinberg, et les autres assertions de (c) sont évidentes.

Reste à prouver l'énoncé (a). On a déjà vu que $c(x, y) = c(x, -xy)$, et, comme $\check{c}$ est lui aussi un cocycle de Steinberg, on vérifie également que $c(x, y) = c(-xy, y)$. Cela entraîne que

$$c(x, y) = c(-xy^{-1}, y) = c(-xy^{-1}, x) = c(y^{-1}, x).$$

On a enfin

$$c(x^2, y)^{-1} = \check{c}^{\natural}(y, x) = c^{\natural}(y, x) = c^{\natural}(x, y)^{-1} = c(x, y^2)^{-1}.$$

Nous avons ainsi démontré toutes les assertions de la proposition.

Revenons-en à l'extension E de G_k. D'après le lemme 5.4 et la proposition 5.7, si G est de type non symplectique, les cocycles de Steinberg c_α sont identiques pour toutes les racines α d'une même longueur. Si G est de type symplectique, le système de racines simples Δ ne possède qu'une seule racine longue.

Nous donnons donc la définition suivante : si α est une racine longue dans Δ, le cocycle de Steinberg c_α en α sera appelé le *cocycle de Steinberg de* E relatif à Δ et aux isomorphismes x_α.

Le lemme suivant est une conséquence du lemme 5.4 :

LEMME 5.8. — *Soit c le cocycle de Steinberg de l'extension* E.

(a) *Pour chaque $\alpha \in \Phi$, le cocycle de Steinberg c_α en α de* E *est égal à l'un des suivants : c, $\check{c}$, $c^{\natural}$, c^3.*

(*b*) *Le sous-groupe* $\tilde{\mathrm{H}}$ *de* E *est abélien si et seulement si l'une des conditions suivantes est vérifiée :* (i) c *est trivial;* (ii) G *est de type symplectique et* $c^\natural$ *est trivial.*

En effet, si α est une racine longue dans Φ, d'après le lemme 5.4, (*b*), on a $c_\alpha = c$ ou $\check{c}$. Si β est une racine non longue dans Φ, il en existe une autre α telle que $\beta\alpha^\star = -1$ et que $\alpha\beta^\star = -3$ ou -2, suivant que G est de type G_2 ou non; on a donc $c_\beta = c_\alpha^{⁝}$ ou $c_\alpha^\natural$, en vertu du lemme 5.4, (*c*). Cela prouve l'énoncé (*a*). L'assertion (*b*) résulte facilement du lemme 5.4, (*c*).

Nous aurons plus tard besoin du lemme suivant :

Lemme 5.9. — *Soit* α *un élément de* Φ. *Si* u *et* v *sont des éléments de* $k^\times$ *tel que* $1 + uv \neq 0$, *l'élément* $\tilde{x}_{-\alpha}(u)\,\tilde{x}_\alpha(v)$ *peut s'écrire sous la forme*

$$\tilde{x}_\alpha(v(1+uv)^{-1})\,\tilde{h}_\alpha((1+uv)^{-1})\,c_\alpha(-u, 1+uv)\,c_\alpha(1+uv, -1)^{-1}\tilde{x}_{-\alpha}(u(1+uv)^{-1}).$$

En effet, si l'on considère le cas de rang 1, il s'agit de mettre $\tilde{x}_{-\alpha}(u)\,\tilde{x}_\alpha(v)$ dans la « grosse cellule » $\tilde{\mathrm{U}}^\alpha\tilde{\mathrm{H}}\,\tilde{\mathrm{U}}^{-\alpha}$ de $\mathrm{E} = \tilde{\mathrm{U}}^\alpha\tilde{\mathrm{N}}\,\tilde{\mathrm{U}}^{-\alpha}$. Cela se fait par un calcul facile, en utilisant notamment le lemme 5.2, (*h*).

Rappelons que les classes d'extensions centrales de G_k par A forment, avec la multiplication de Baer, le groupe de cohomologie $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$. On sait déjà que le cocycle de Steinberg c_E de E relatif à Δ et aux isomorphismes x_α ne dépend que de la classe d'extensions de E. D'après le théorème de Steinberg sur G_k, l'extension E est triviale si et seulement si c_E l'est. On voit d'ailleurs aisément que, si c_E et $c_{\mathrm{E}'}$ sont ainsi associés à des extensions E et E′, le produit $c_\mathrm{E}c_{\mathrm{E}'}$ est le cocycle de Steinberg du produit de Baer de E et de E′.

Nous pouvons maintenant énoncer l'un des théorèmes principaux de ce chapitre; rappelons que k est un corps infini.

Théorème 5.10. — *Lorsqu'on fait correspondre à une extension centrale* E *de* G_k *par* A *son cocycle de Steinberg relatif à* Δ *et aux isomorphismes* x_α, *on obtient un isomorphisme du groupe* $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$ *des classes d'extensions centrales de* G_k *par* A *sur le groupe* $\mathrm{S}(k^\times, \mathrm{A})$ [*resp.* $\mathrm{S}^0(k^\times, \mathrm{A})$] *des cocycles de Steinberg* [*resp. de Steinberg bilinéaires*] *sur* $k^\times$ *à valeurs dans* A, *si* G *est de type symplectique* [*resp. non symplectique*].

Pour démontrer ce théorème, il nous reste à voir que l'application $\mathrm{E} \mapsto c_\mathrm{E}$ a pour image $\mathrm{S}(k^\times, \mathrm{A})$ ou $\mathrm{S}^0(k^\times, \mathrm{A})$ tout entier. Nous le vérifierons aux deux numéros suivants.

Ce théorème permet de représenter par générateurs et relations le noyau $\pi_1(\mathrm{G}_k)$ du revêtement $\mathrm{E}(\mathrm{G}_k)$ de G_k considéré par Steinberg [30] et repris au début de ce numéro.

Corollaire 5.11. — *Si* G *est de type symplectique* [*resp. non symplectique*], $\pi_1(\mathrm{G}_k)$ *est isomorphe au groupe abélien* $\mathrm{S}(k)$ [*resp.* $\mathrm{S}^0(k)$] *engendré* *par les symboles* $c(x, y)$ $(x, y \in k^\times)$ *soumis aux relations* (S 1), (S 2) *et* (S 3) [*resp.* (S° 1), (S° 2) *et* (S° 3)].

Pour $G = SL_2$, le théorème 5.10 et son corollaire ont été obtenus par C. Moore [26].

Dans le cas de SL_2, on peut aussi donner une jolie formule qui exprime en termes de c_E un cocycle sur G_k déterminant E.

Définissons comme suit une application χ de G_k dans $k^\times$:

$$\chi(g) = \chi(\nu(g)) \quad \text{pour tout } g \in G_k;$$
$$\chi(h_\alpha(t)) = t, \qquad \chi(w_\alpha(t)) = -t \qquad \text{pour} \quad t \in k^\times, \quad \alpha \in \Delta.$$

D'autre part, on choisit comme suit une section $\mathfrak{s}$ de E :

$$\tilde{\nu}(\mathfrak{s}(g)) = \mathfrak{s}(\nu(g)) \quad \text{pour tout } g \in G_k;$$
$$\mathfrak{s}(h_\alpha(t)) = c_\alpha(t, t)^{-1}\,\tilde{h}_\alpha(t), \qquad \mathfrak{s}(w_\alpha(t)) = \tilde{w}_\alpha(t) \qquad \text{pour} \quad t \in k^\times, \quad \alpha \in \Delta.$$

Alors, le cocycle z_E sur G_k par rapport à $\mathfrak{s}$ est donné par

$$z_E(g, g') = c_E(\chi(g), \chi(g'))^{-1}\, c_E(\chi(gg'), -\chi(g)^{-1}\chi(g')).$$

Le corollaire suivant est donc une conséquence du théorème 5.10 :

Corollaire 5.12. — *Posons* $G = SL_2$. *Soit* χ *l'application de* G_k *dans* $k^\times$ *définie comme suit :*

$$\chi\begin{pmatrix} s & t \\ u & v \end{pmatrix} = v \quad \textit{ou} \quad u, \quad \textit{suivant que } u = 0 \textit{ ou non.}$$

Alors :

(*a*) *Si c est un cocycle de Steinberg sur* $k^\times$ *à valeurs dans* A, *la formule*

$$z_c(g, g') = c(\chi(g), \chi(g'))^{-1}\, c(\chi(gg'), -\chi(g)^{-1}\chi(g'))$$

donne un cocycle sur G_k *à valeurs dans* A.

(*b*) *L'application* $c \mapsto z_c$ *établit un isomorphisme de* $S(k^\times, A)$ *sur* $H^2(G_k, A)$.

T. Kubota [19] avait prouvé directement le corollaire 5.12, (*a*) dans le cas particulier où k est un corps local et c le symbole de restes normiques de k (*cf.* n° 9).

Revenons-en au cas général et examinons comment les automorphismes algébriques de G_k agissent sur $H^2(G_k, A)$.

Rappelons que G_k est le groupe des points rationnels du schéma ${}_kG$ en groupes sur k déduit d'un schéma $\mathfrak{G}$ en groupes déployés sur **Z**. On notera $\mathrm{Aut}\,({}_kG)_k$ le groupe des automorphismes de ${}_kG$ définis sur k.

Nous avons choisi un tore maximal déployé ${}_kH$ de ${}_kG$ et, pour chaque racine α de ${}_kG$ relative à ${}_kH$, un isomorphisme x_α du groupe additif sur le sous-groupe radiciel ${}_kU^\alpha$; x_α et $x_{-\alpha}$ sont liés de telle sorte que

$x_\alpha(t)\, x_{-\alpha}(-t^{-1})\, x_\alpha(t)$ soit dans le normalisateur ${}_k\mathrm{N}$ de ${}_k\mathrm{H}$ pour tout $t \neq 0$. Si x'_α et $x'_{-\alpha}$ sont d'autres isomorphismes du groupe additif sur ${}_k\mathrm{U}^\alpha$ et ${}_k\mathrm{U}^{-\alpha}$ définis sur k et possédant cette dernière propriété, il existe un élément r de $k^\times$ tel que $x'_\alpha(u) = x_\alpha(ru)$ et $x'_{-\alpha}(u) = x_{-\alpha}(r^{-1}u)$ pour tout u.

D'autre part, $\mathrm{Aut}\,({}_k\mathrm{G})_k$ contient le groupe $\mathrm{Ad}(\mathrm{G}_k)$ des automorphismes de ${}_k\mathrm{G}$ définis par des éléments de G_k. En vertu du théorème de conjugaison des tores déployés maximaux [6], si α est une racine de ${}_k\mathrm{G}$ relative à ${}_k\mathrm{H}$ et si σ est un élément de $\mathrm{Aut}({}_k\mathrm{G})_k$, il existe un élément τ de $\mathrm{Ad}(\mathrm{G}_k)$ tel que $\sigma\tau$ laisse stables ${}_k\mathrm{H}$, ${}_k\mathrm{U}^\alpha$ et ${}_k\mathrm{U}^{-\alpha}$. Si $\{r_\alpha\}$ $(\alpha \in \Delta)$ est un ensemble d'éléments de $k^\times$, il existe un élément σ de $\mathrm{Aut}({}_k\mathrm{G})_k$ tel que σ laisse fixes les éléments de ${}_k\mathrm{H}$ et que $x_\alpha(u)^\sigma = x_\alpha(r_\alpha u)$ pour tout $\alpha \in \Delta$.

Un élément σ de $\mathrm{Aut}({}_k\mathrm{G})_k$ agit sur les cocycles z sur G_k à valeurs dans A, par $z^\sigma(g_1, g_2) = z(g_1^\sigma, g_2^\sigma)$; σ définit donc un automorphisme de $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$. Le groupe $\mathrm{Aut}({}_k\mathrm{G})_k$ opère ainsi sur $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$, et il est évident que $\mathrm{Ad}(\mathrm{G}_k)$ y agit trivialement.

Supposons qu'un élément σ de $\mathrm{Aut}({}_k\mathrm{G})_k$ laisse stables ${}_k\mathrm{H}$, ${}_k\mathrm{U}^\alpha$ et ${}_k\mathrm{U}^{-\alpha}$ pour un élément α de Φ; on a

$$x'_\alpha(u) = x_\alpha(u)^\sigma = x_\alpha(ru) \qquad \text{et} \qquad x'_{-\alpha}(u) = x_{-\alpha}(u)^\sigma = x_{-\alpha}(r^{-1}u)$$

avec un élément r de $k^\times$. Soit E une extension centrale de G_k par A, et calculons en termes de c_α le cocycle de Steinberg c'_α en α de E^σ. Posons dans E

$$\tilde{x}'_\alpha(u) = \tilde{x}_\alpha(ru) \qquad \text{et} \qquad \tilde{x}'_{-\alpha}(u) = \tilde{x}_{-\alpha}(r^{-1}u)\,;$$

alors

$$\tilde{w}'_\alpha(t) = \tilde{x}'_\alpha(t)\, \tilde{x}'_{-\alpha}(-t^{-1})\, \tilde{x}'_\alpha(t) = \tilde{w}_\alpha(rt)\,;$$

$$\tilde{h}'_\alpha(t) = \tilde{w}'_\alpha(t)\, \tilde{w}'_\alpha(-1) = \tilde{h}_\alpha(rt)\, \tilde{h}_\alpha(r)^{-1} = c_\alpha(t, r)^{-1}\, \tilde{h}_\alpha(t)\,;$$

d'où

$$c'_\alpha(s, t) = c_\alpha(s, t)\, c_\alpha(st, r)\, c_\alpha(s, r)^{-1}\, c_\alpha(t, r)^{-1}.$$

Nous sommes ainsi amenés au résultat suivant :

Proposition 5.13. — (*a*) *Le groupe* $k^\times$ *opère sur* $\mathrm{S}(k^\times, \mathrm{A})$ *par la formule suivante :*

$$(\delta(t)\, c)\,(x, y) = c(x, y)\, c(xy, t)\, c(x, t)^{-1}\, c(y, t)^{-1}.$$

Les éléments de $(k^\times)^2$ *y agissent trivialement, et* $\delta(-1)\,c = \check{c}$ *pour tout* $c \in \mathrm{S}(k^\times, \mathrm{A})$.

(*b*) $\mathrm{Aut}({}_k\mathrm{G})_k$ *opère sur* $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$ *et donc sur* $\mathrm{S}(k^\times, \mathrm{A})$ [*resp.* $\mathrm{S}^0(k^\times, \mathrm{A})$] *d'après l'isomorphisme du théorème* 5.10. *L'action d'un élément de* $\mathrm{Aut}({}_k\mathrm{G})_k$ *est identique à* $\delta(t)$ *pour un élément* t *de* $k^\times$.

(*c*) *Les invariants de* $\mathrm{Aut}({}_k\mathrm{G})_k$ *dans* $\mathrm{H}^2(\mathrm{G}_k, \mathrm{A})$ *sont les éléments qui correspondent à ceux de* $\mathrm{S}^0(k^\times, \mathrm{A})$.

(*d*) *L'isomorphisme restreint de* $S^0(k^\times, A)$ *sur* $H^2(G_k, A)^0$ *ne dépend ni du choix des isomorphismes* x_α *ni du choix du système de racines simples* Δ *ni du choix du tore maximal* ${}_kH$ *déployé sur* k.

On pourrait donc dire que l'isomorphisme de $S(k^\times, A)$ [resp. de $S^0(k^\times, A)$] sur $H^2(G_k, A)$ est canonique après restriction à $S^0(k^\times, A)$.

6. Ce numéro et le suivant sont consacrés à la démonstration du théorème 5.10.

Nous étudierons d'abord une extension centrale du groupe de Weyl étendu $\mathcal{N} = N_{\mathbf{Z}}$ associé au groupe simple simplement connexe G. Le groupe $\mathcal{N}$ est une extension du groupe de Weyl W par le groupe abélien $\mathcal{H} = H_{\mathbf{Z}}$ d'ordre 2^r, où r est le rang de G. Rappelons que Φ désigne le système de racines de G relatif au tore maximal H et qu'on a choisi un système de racines simples Δ de Φ.

On a le lemme suivant (Demazure [16], Tits [31]) :

LEMME 6.1. — *Le groupe* $\mathcal{N}$ *est engendré par les éléments* $w_\alpha = w_\alpha(-1)$ *pour* $\alpha \in \Delta$ *et défini par les relations suivantes* (W 1), (W 2) et (W 3) :

$$\text{(W 1)} \quad h_\alpha w_\beta h_\alpha^{-1} = w_\beta^{c'} \ \textit{avec} \ h_\alpha = w_\alpha^2 \ \textit{et} \ c' = (-1)^{\beta\alpha^*}, \ \textit{pour tout} \ \alpha, \beta \in \Delta;$$

$$\text{(W 2)} \quad \left\{ \begin{array}{lll} w_\alpha w_\beta = w_\beta w_\alpha & si & \beta\alpha^* = 0; \\ w_\alpha w_\beta w_\alpha^{-1} = w_\beta w_\alpha^{-1} w_\beta^{-1} & si & \alpha\beta^* = \beta\alpha^* = -1; \\ w_\beta w_\alpha w_\beta w_\alpha^{-1} = w_\alpha w_\beta w_\alpha^{-1} w_\beta & si & \beta\alpha^* = -2; \\ w_\beta w_\gamma w_\beta^{-1} = w_\gamma w_\beta^{-1} w_\gamma^{-1} \ \textit{avec} \ w_\gamma = w_\alpha w_\beta w_\alpha^{-1}, & si & \beta\alpha^* = -3; \end{array} \right.$$

$$\text{(W 3)} \quad h_\alpha^2 = e \ \textit{pour tout} \ \alpha \in \Delta.$$

En effet, appliquant à G les lemmes 5.1 et 5.2, on voit aisément que les générateurs w_α satisfont à ces relations. Soit $\mathcal{N}'$ le groupe engendré par les symboles w_α soumis aux relations (W 1), (W 2) et (W 3); c'est naturellement une extension de $\mathcal{N}$. D'après (W 1), on a

$$w_\beta h_\alpha w_\beta^{-1} = h_\alpha h_\beta^{c''} \quad \text{et} \quad h_\beta h_\alpha h_\beta^{-1} = h_\alpha h_\beta^{2c''} \quad \text{avec} \quad 2c'' = (-1)^{\beta\alpha^*} - 1;$$

les éléments h_α engendrent donc un sous-groupe distingué $\mathcal{H}'$ de $\mathcal{N}'$, et, d'après (W 3), $\mathcal{H}'$ est abélien d'ordre 2^r. Le groupe quotient $\mathcal{N}'/\mathcal{H}'$ est engendré par les éléments involutifs $\overline{w}_\alpha$ vérifiant les relations (W 2), qui forment une famille exhaustive de relations pour les générateurs σ_α du groupe de Weyl W (*voir* N. Bourbaki [8]). Par conséquent, $\mathcal{N}'$ est isomorphe à $\mathcal{N}$.

On va rappeler à cette occasion d'autres propriétés du groupe de Weyl W. On sait que W est engendré par les réflexions σ_α pour $\alpha \in \Delta$ et défini par les relations (W 2) avec les w_α remplacés par les σ_α. On définit comme suit la fonction longueur l sur W par rapport à Δ : pour $\sigma \in W$, $l(\sigma)$ désigne le plus petit entier non négatif m tel que σ puisse s'écrire comme produit $\prod_{i=1}^{m} \sigma_{\alpha_i}$ avec $\alpha_i \in \Delta$. On notera également l la fonction sur N définie par $l(n) = l(\omega(n))$, où ω désigne le morphisme canonique de N sur W.

On connaît alors les résultats suivants sur le groupe de Weyl W, son action sur Φ et l'application ν du lemme 5.3, (*b*) (*cf.* [8], [20], [31]).

LEMME 6.2. — (*a*) *Soient* Δ' *une partie de* Δ *et* W' *le sous-groupe de* W *engendré par les éléments* σ_α *pour* $\alpha \in \Delta'$. *Alors, chaque classe* $W'\sigma$ *de* W *modulo* W' *possède un élément* σ_0 *tel que* $l(\sigma'\sigma_0) = l(\sigma') + l(\sigma_0)$ *pour tout* $\sigma' \in W'$.

(*b*) *Soit* β *une racine positive, et soient* σ, σ' *des éléments de* W *tels que*

$$l(\sigma'\sigma) = l(\sigma') + l(\sigma).$$

Alors, si $\sigma'\sigma\beta$ *est positive, il en est de même de* $\sigma\beta$.

(*c*) *Si* g *et* g' *sont des éléments de* G_k *tels que*

$$l(\nu(g)\,\nu(g')) = l(\nu(g)) + l(\nu(g')),$$

alors $\nu(gg') = \nu(g)\,\nu(g')$.

(*d*) *Supposons que des éléments* d_α, *indexés par* Δ, *d'un monoïde à unité* D *satisfassent aux relations suivantes :*

$$\text{(W 2')} \quad \begin{cases} d_\alpha d_\beta = d_\beta d_\alpha & si \quad \beta\alpha^* = 0\,; \\ d_\alpha d_\beta d_\alpha = d_\beta d_\alpha d_\beta & si \quad \alpha\beta^* = \beta\alpha^* = -1\,; \\ (d_\alpha d_\beta)^2 = d_\beta d_\alpha)^2 & si \quad \beta\alpha^* = -2\,; \\ (d_\alpha d_\beta)^3 = (d_\beta d_\alpha)^3 & si \quad \beta\alpha^* = -3. \end{cases}$$

Si un élément σ *de* W *s'exprime en deux mots minimaux* $\prod_{i=1}^{m} \sigma_{\alpha_i}$ *et* $\prod_{j=1}^{m} \sigma_{\alpha'_j}$, *où* $m = l(\sigma)$ *et* $\alpha_i, \alpha'_j \in \Delta$, *alors on a, dans* D,

$$\prod_{i=1}^{m} d_{\alpha_i} = \prod_{j=1}^{m} d_{\alpha'_j}.$$

Rappelons d'abord que $l(\sigma_\alpha\sigma) = l(\sigma) + 1$ pour $\sigma \in W$ et $\alpha \in \Delta$ si et seulement si $\sigma^{-1}\alpha$ est positive. On déduit de là aisément les énoncés (*b*) et (*c*), par récurrence sur $l(\sigma')$ ou $l(\nu(g))$. Pour les assertions (*a*) et (*d*), une démonstration se trouve dans [8].

Le théorème suivant jouera un rôle important dans la démonstration du théorème 5.10.

THÉORÈME 6.3. — *Soient* $\tilde{\mathfrak{N}}$ *le groupe engendré par les symboles* w_α ($\alpha \in \Delta$) *soumis aux seules relations* (W 1) *et* (W 2), *et* π *le morphisme naturel de* $\tilde{\mathfrak{N}}$ *sur* $\mathfrak{N}$. *Alors :*

(*a*) *Le noyau* $\mathfrak{Z}$ *de* π *est central dans* $\tilde{\mathfrak{N}}$ *et engendré par* w_α^4, *où* α *est une racine longue dans* Δ. *Le groupe* $\mathfrak{Z}$ *est cyclique d'ordre infini* [*resp. d'ordre* 2] *si* Δ *est de type symplectique* [*resp. non symplectique*].

(*b*) ***Le groupe $\tilde{\mathfrak{N}}$ peut être défini par les relations suivantes :***

(W 1′) $w_\beta^{-1} h_\alpha w_\beta = h_\alpha w_\beta^{c''}$ *avec* $h_\alpha = w_\alpha^2$ *et* $c'' = 1 - (-1)^{\beta\alpha^*}$, *pour tout* $\alpha, \beta \in \Delta$;

(W 2′)
$$\begin{cases} w_\alpha w_\beta = w_\beta w_\alpha & si \quad \beta\alpha^* = 0; \\ w_\alpha w_\beta w_\alpha = w_\beta w_\alpha w_\beta & si \quad \alpha\beta^* = \beta\alpha^* = -1; \\ (w_\alpha w_\beta)^2 = (w_\beta w_\alpha)^2 & si \quad \beta\alpha^* = -2; \\ (w_\alpha w_\beta)^3 = (w_\beta w_\alpha)^3 & si \quad \beta\alpha^* = -3. \end{cases}$$

(*c*) ***Le sous-groupe $\tilde{\mathfrak{H}}$ de $\tilde{\mathfrak{N}}$ engendré par les éléments h_α ($\alpha \in \Delta$) est défini par les relations suivantes :***

$$h_\beta^{-1} h_\alpha h_\beta = h_\alpha h_\beta^{c''} \quad avec \ c'' = 1 - (-1)^{\beta\alpha^*}, \quad pour\ tout\ \alpha, \beta \in \Delta.$$

D'abord, les relations (W 1) impliquent que les éléments $z_\alpha = w_\alpha^4$ engendrent dans $\tilde{\mathfrak{N}}$ un sous-groupe central, qui, par le lemme 6.1, est égal au noyau $\mathfrak{Z}$ de π. On voit d'ailleurs aisément que les familles de relations (W 1) et (W 1′) sont équivalentes et que, sous l'hypothèse de celles-ci, il en est de même pour les relations (W 2) et (W 2′). D'autre part, les relations (W 1′) entraînent immédiatement celles de l'énoncé (*c*); autrement dit,

$$h_\alpha^{-1} h_\beta^{-1} h_\alpha h_\beta = h_\beta^{c''} = h_\alpha^{-d''}, \qquad \text{avec} \quad c'' = 1 - (-1)^{\beta\alpha^*}, \quad d'' = 1 - (-1)^{\alpha\beta^*}.$$

On déduit de là que $z_\beta^2 = e$ si $\beta\alpha^*$ est impair pour un élément α de Δ, que $z_\beta = e$ si $\alpha\beta^* = -2$, et que $z_\alpha = z_\beta$ si $\alpha\beta^*$ et $\beta\alpha^*$ sont impairs. Or, les racines de Δ ont, au plus, deux longueurs différentes, et celles qui sont longues forment un sous-système irréductible. On en conclut que $\mathfrak{Z}$ est engendré par z_α, où α est une racine longue quelconque dans Δ, et que $\mathfrak{Z}$ est d'ordre 1 ou 2 si Δ est de type non symplectique.

Il nous reste donc à déterminer l'ordre de $\mathfrak{Z}$. D'abord, des relations (W 1′) et (W 2′), on obtient une présentation du groupe quotient de $\tilde{\mathfrak{N}}$ par son groupe des commutateurs; si Δ est de type symplectique, on y voit aussitôt que l'élément $\bar{w}_\alpha$ est d'ordre infini dans ce groupe abélien, α étant la racine longue dans Δ. Par suite, $\mathfrak{Z}$ est un groupe infini dans le cas symplectique. Pour déterminer l'ordre de $\mathfrak{Z}$ dans le cas non symplectique, nous allons construire une extension de $\mathfrak{N}$ par un groupe d'ordre 2, qui sera isomorphe à $\tilde{\mathfrak{N}}$ dans le cas non symplectique. Cette construction est valable pour tous les types, mais il suffit, pour achever la démonstration du théorème, de traiter les cas où Δ consiste en racines d'une même longueur. En effet, les cas des types $B_n (n \geq 3)$, F_4 et G_2 peuvent facilement être conclus en faisant agir sur les groupes $\mathfrak{N}$ de types D_{n+1}, E_6 et D_4 un automorphisme « extérieur » d'ordre 2 ou 3 (*cf.* lemme 6.4).

Soit $\tilde{\mathcal{H}}'$ le groupe engendré par les symboles $t_\alpha\,(\alpha \in \Delta)$ soumis aux relations suivantes :

$$t_\alpha^4 = e, \qquad t_\beta^{-1}\, t_\alpha t_\beta = t_\alpha t_\beta^{c''} \ \text{avec}\ c'' = 1 - (-1)^{\beta\alpha^\star}, \quad \text{pour tout } \alpha,\, \beta \in \Delta.$$

Comme on l'a vu plus haut, $\tilde{\mathcal{H}}'$ est une extension centrale de $\mathcal{H}$ par le noyau d'ordre 2. Puis on définit un groupe d'automorphismes de $\tilde{\mathcal{H}}'$; pour chaque $\alpha \in \Delta$, l'application $t_\beta \mapsto t_\beta t_\alpha^{d'}$ $(\beta \in \Delta,\ 2d' = 1 - (-1)^{\alpha\beta^\star})$ se prolonge en un automorphisme θ_α^{-1} de $\tilde{\mathcal{H}}'$. Ces automorphismes $\theta_\alpha\,(\alpha \in \Delta)$ satisfont aux relations (W 1), (W 2) et (W 3) avec les w_α remplacés par les θ_α; on note également que $\theta_\alpha^2 = \mathrm{Ad}(t_\alpha)$ pour tout $\alpha \in \Delta$.

On définit ensuite, pour chaque $\alpha \in \Delta$, une transformation λ_α de l'ensemble produit $\tilde{\mathcal{H}} \times \mathrm{W}$:

$$\lambda_\alpha(t, \sigma) = (\theta_\alpha(t), \sigma_\alpha\sigma) \qquad \text{si} \quad l(\sigma_\alpha\sigma) > l(\sigma);$$
$$\lambda_\alpha(t, \sigma) = (\theta_\alpha(tt_\alpha), \sigma_\alpha\sigma) \qquad \text{si} \quad l(\sigma_\alpha\sigma) < l(\sigma).$$

Soit Λ le groupe de transformations de $\tilde{\mathcal{H}}' \times \mathrm{W}$ engendré par les λ_α. On voit aisément que $\lambda_\alpha^2(t, \sigma) = (t_\alpha t, \sigma)$ pour tout α, et que $\lambda_\alpha^2 \lambda_\beta \lambda_\alpha^{-2} = \lambda_\beta^{c'}$ avec $c' = (-1)^{\beta\alpha^\star}$ pour tout $\alpha, \beta \in \Delta$; autrement dit, les générateurs λ_α satisfont aux relations (W 1′) et les éléments λ_α^2 engendrent un sous-groupe distingué de Λ qui est isomorphe à $\tilde{\mathcal{H}}'$. Par conséquent, lorsqu'on aura vérifié pour Λ les relations (W 2′), on en conclura, dans le cas non symplectique, que Λ est isomorphe à $\tilde{\mathcal{N}}$ et que $\mathcal{Z}$ est d'ordre 2.

Soient α, β deux éléments de Δ, et W′ le sous-groupe de W engendré par σ_α et σ_β. Rappelons que θ_α et θ_β satisfont aux relations (W 1′) et (W 2′). Alors, en vertu du lemme 6.2, (*a*) et de la définition de λ_α et λ_β, on voit que la relation (W 2′) pour λ_α et λ_β est vérifiée si elle l'est sur le sous-ensemble $\{e\} \times \mathrm{W}'$ de $\tilde{\mathcal{H}}' \times \mathrm{W}$. Nous sommes ainsi ramenés aux cas de rang 2. Le cas où $\alpha\beta^\star = 0$ est trivial. Dans le cas du type A_2, un calcul direct montre que la relation (W 2′) pour λ_α et λ_β est vraie sur les éléments de $\{e\} \times \mathrm{W}'$. Le théorème 6.3 est ainsi démontré.

On remarquera que la construction de Λ est motivée par le lemme 6.2, (*d*) et que nos arguments ressemblent beaucoup à ceux de Tits [31] qui permettent d'établir, à partir de W, l'existence d'un groupe isomorphe à $\mathcal{N}$.

On sait d'ailleurs que le revêtement universel $\tilde{G}_{\mathbf{R}}$ du groupe de Lie connexe $G_{\mathbf{R}}$ possède un sous-groupe isomorphe à $\tilde{\mathcal{N}}$; il suffit de prendre $\pi^{-1}(N_{\mathbf{Z}})$, où π désigne la projection de $\tilde{G}_{\mathbf{R}}$ sur $G_{\mathbf{R}}$ (*cf.* n° 9). Cela fournit une autre preuve de la non-trivialité de $\mathcal{Z}$.

Nous allons maintenant entamer la démonstration du théorème 5.10. Soit donné un cocycle de Steinberg c (bilinéaire si G est de type non symplectique) sur $k^\times$ à valeurs dans A. Il s'agit alors de montrer l'existence d'une extension centrale de G_k par A dont le cocycle de Steinberg en α soit égal à c pour une racine longue α dans Δ.

Notons d'abord le lemme suivant, qui nous permettra par la suite de nous borner aux cas de certains types.

LEMME 6.4. — *Il existe un plongement du groupe* G' *de type* B_n $(n \geqq 3)$ [*resp.* F_4 *ou* G_2] *dans le groupe* G *de type* D_{n+1} [*resp.* E_6 *ou* D_4] *de sorte que la conclusion du théorème* 5.10 *pour* G' *se déduit par restriction de celle pour* G.

En effet, les diagrammes Δ de types A_{2n-1} $(n \geqq 2)$, D_{n+1} $(n \geqq 3)$ et E_6 [resp. de type D_4] admettent un automorphisme ρ d'ordre 2 [resp. 3] qui laisse fixe au moins un sommet. Cet automorphisme ρ se relève en un automorphisme ρ de G tel que $\rho \circ x_\alpha = x_{\rho\alpha}$ et $\rho \circ x_{-\alpha} = x_{-\rho\alpha}$ pour tout $\alpha \in \Delta$. Les points fixes de ρ dans G forment un groupe simple simplement connexe G' de type $C_n (n \geqq 2)$, $B_n (n \geqq 3)$, F_4 ou G_2. Le groupe $H' = G' \cap H$ est un tore maximal de G', les racines de G' relatives à H' sont les restrictions à H' des racines α de G, et les racines longues de G' sont ainsi identifiées avec les racines de G qui sont fixes par ρ. L'automorphisme ρ de G se transporte en un automorphisme du schéma $\mathfrak{G}$ en groupes sur $\mathbf{Z}$ et puis en un automorphisme de G_k, qu'on note encore ρ. Le groupe G'_k des points fixes de ρ dans G_k est l'ensemble des points rationnels d'un groupe simple simplement connexe déployé sur k et du même type que G'. Si E est une extension centrale de G_k par A, on en déduit par restriction une extension centrale E' de G'_k par A. Alors, une racine longue α de G' étant identifiée à une racine de G, on voit tout de suite que les cocycles de Steinberg en α de E et de E' sont identiques. Par conséquent, si G' est de type non symplectique, la conclusion du théorème 5.10 pour G' résulte de celle pour G.

Nous ne traiterons désormais que, d'une part, le cas où G est de type symplectique et, d'autre part, le cas où les racines de G ont même longueur et où le cocycle de Steinberg c donné est bilinéaire. Nous nous servirons librement des propriétés des cocycles de Steinberg énoncées dans la proposition 5.7.

La première étape de la démonstration consiste à définir une extension centrale de H par A. Posons $c^0 = c^\natural$ dans le cas symplectique et $c^0 = c$ dans le cas non symplectique; c^0 est un cocycle de Steinberg bilinéaire. On définit comme suit les cocycles $c_\alpha (\alpha \in \Delta)$ et $c_{\alpha\beta} (\alpha, \beta \in \Delta, \alpha \neq \beta)$: $c_\alpha = c$ pour les racines longues α et $c_\beta = c^0$ pour les racines courtes β dans le cas symplectique; $c_{\alpha\beta} = 1$ si $\beta\alpha^* = 0$ et $c_{\alpha\beta} = (c^0)^{-1}$ si $\beta\alpha^* \neq 0$. Posons alors

$$\mathfrak{f}\Big(\prod_\alpha h_\alpha(u_\alpha),\ \prod_\beta h_\beta(v_\beta)\Big) = \prod_\alpha c_\alpha(u_\alpha, v_\alpha) \prod_{\beta<\alpha} c_{\alpha\beta}(u_\alpha, v_\beta),$$

Δ étant muni d'un ordre total quelconque; $\mathfrak{c}$ est un cocycle sur H à valeurs dans A. Soit $\tilde{H}$ l'extension centrale de H par A définie à partir de $\mathfrak{c}$:

$$1 \to A \to \tilde{H} \xrightarrow{\varphi} H \to 1.$$

On peut relever dans $\tilde{H}$ les éléments $h_\alpha(t)$ ($\alpha \in \Delta$, $t \in k^\times$) de telle sorte que les éléments relevés $\tilde{h}_\alpha(t)$ satisfassent aux relations suivantes :

$$\tilde{h}_\beta(u)\,\tilde{h}_\beta(v) = c_\beta(u, v)\,\tilde{h}_\beta(uv)$$

et

$$\tilde{h}_\beta(u)\,\tilde{h}_\gamma(v)\,\tilde{h}_\beta(u)^{-1}\,\tilde{h}_\gamma(v)^{-1} = c_\beta(u, v^{\beta\gamma^\star}) = c_\gamma(u^{\gamma\beta^\star}, v)$$

pour tout $\beta, \gamma \in \Delta$.

Puis nous allons définir un groupe d'automorphismes de $\tilde{H}$.

Lemme 6.5. — (*a*) *Pour chaque* $\alpha \in \Delta$, *il existe un automorphisme* θ_α *de* $\tilde{H}$ *tel que* $\theta_\alpha^{-1}(a) = a$ *pour* $a \in A$ *et que* $\theta_\alpha^{-1}(\tilde{h}_\beta(t)) = \tilde{h}_\beta(t)\,\tilde{h}_\alpha(t^{-\alpha\beta^\star})$ *pour tout* $\beta \in \Delta$.

(*b*) θ_α *induit, par passage au quotient, l'automorphisme de* H *défini par l'élément* $w_\alpha(-1)$ *de* N.

(*c*) $\theta_\alpha^2 = \theta_\alpha^{-2} = \mathrm{Ad}(\tilde{h}_\alpha(-1))$ *pour tout* $\alpha \in \Delta$. *Les automorphismes* θ_α *satisfont aux relations* (W 1), (W 2) *et* (W 3).

Notons d'abord que $c_\alpha(u, v^{\alpha\beta^\star})$ est bilinéaire en (u, v) quels que soient $\alpha, \beta \in \Delta$. Pour vérifier (*a*), il suffit de montrer que les éléments $\theta_\alpha^{-1}(\tilde{h}_\beta(t))$ satisfont aux mêmes relations que les $\tilde{h}_\beta(t)$. On a

$$\begin{aligned}
&\theta_\alpha^{-1}(\tilde{h}_\beta(u))\,\theta_\alpha^{-1}(\tilde{h}_\beta(v))\\
&\quad= \tilde{h}_\beta(u)\,\tilde{h}_\alpha(u^{-\alpha\beta^\star})\,\tilde{h}_\beta(v)\,\tilde{h}_\alpha(v^{-\alpha\beta^\star})\\
&\quad= \tilde{h}_\beta(u)\,\tilde{h}_\beta(v)\,\tilde{h}_\alpha((uv)^{-\alpha\beta^\star})\,c_\alpha(u^{-\alpha\beta^\star}, v^{\alpha\beta^\star})\,c_\alpha(u^{-\alpha\beta^\star}, v^{-\alpha\beta^\star})\\
&\quad= c_\beta(u, v)\,\tilde{h}_\beta(uv)\,\tilde{h}_\alpha((uv)^{-\alpha\beta^\star})\\
&\quad= c_\beta(u, v)\,\theta_\alpha^{-1}(\tilde{h}_\beta(uv));\\
&\theta_\alpha^{-1}(\tilde{h}_\beta(u))\,\theta_\alpha^{-1}(\tilde{h}_\gamma(v))\,(\theta_\alpha^{-1}(\tilde{h}_\beta(u)))^{-1}\,(\theta_\alpha^{-1}(\tilde{h}_\gamma(v)))^{-1}\\
&\quad= c_\alpha(u, v^{\beta\gamma^\star})\,c_\alpha(u^{-\alpha\beta^\star}, v^{\alpha\gamma^\star})\,c_\alpha(u^{\alpha\beta^\star}, v^{-\alpha\gamma^\star})\,c_\alpha(u^{-\alpha\beta^\star}, v^{-\alpha\gamma^\star})^2\\
&\quad= c_\beta(u, v^{\beta\gamma^\star}).
\end{aligned}$$

L'énoncé (*a*) est ainsi démontré. L'assertion (*b*) résulte immédiatement du lemme 5.2, (*f*) appliqué à G_k. Vérifions (*c*). On a d'abord

$$\begin{aligned}
\theta_\alpha^{-1}(\tilde{h}_\alpha(t)) &= \tilde{h}_\alpha(t)\,\tilde{h}_\alpha(t^{-2}) = \tilde{h}_\alpha(t^{-1});\\
\theta_\alpha^{-2}(\tilde{h}_\beta(u)) &= \tilde{h}_\beta(u)\,\tilde{h}_\alpha(u^{-\alpha\beta^\star})\,\tilde{h}_\alpha(u^{\alpha\beta^\star})\\
&= \tilde{h}_\beta(u)\,c_\alpha(u^{-\alpha\beta^\star}, u^{\alpha\beta^\star}) = \tilde{h}_\beta(u)\,c_\alpha(u^{-\alpha\beta^\star}, -1)\\
&= \tilde{h}_\alpha(-1)\,\tilde{h}_\beta(u)\,\tilde{h}_\alpha(-1)^{-1}.
\end{aligned}$$

Ceci prouve que $\theta_\alpha^{-2} = \theta_\alpha^2 = \mathrm{Ad}\,(\tilde{h}_\alpha(-1))$ et entraîne facilement que les automorphismes θ_α vérifient les relations (W 1) et (W 3). La relations (W 2') pour θ_α et θ_β est évidente si $\beta\alpha^\star = 0$. Si $\alpha\beta^\star = \beta\alpha^\star = -1$, on a

$$\begin{aligned}
(\theta_\alpha\theta_\beta\theta_\alpha)^{-1}(\tilde{h}_\gamma(t)) &= (\theta_\beta\theta_\alpha)^{-1}(\tilde{h}_\gamma(t)\,\tilde{h}_\alpha(t^{-\alpha\gamma^\star}))\\
&= \theta_\alpha^{-1}(\tilde{h}_\gamma(t)\,\tilde{h}_\beta(t^{-\beta\gamma^\star})\,\tilde{h}_\alpha(t^{-\alpha\gamma^\star})\,\tilde{h}_\beta(t^{-\alpha\gamma^\star}))\\
&= \tilde{h}_\gamma(t)\,\tilde{h}_\alpha(t^{-\alpha\gamma^\star})\,\tilde{h}_\beta(t^{-\beta\gamma^\star})\,\tilde{h}_\alpha(t^{-\beta\gamma^\star})\,\tilde{h}_\alpha(t^{\alpha\gamma^\star})\,\tilde{h}_\beta(t^{-\alpha\gamma^\star})\,\tilde{h}_\alpha(t^{-\gamma\alpha^\star})\\
&= \tilde{h}_\gamma(t)\,\tilde{h}_\alpha(t^{-\alpha\gamma^\star-\beta\gamma^\star})\,\tilde{h}_\beta(t^{-\alpha\gamma^\star-\beta\gamma^\star})\,c_\beta(-1,\,t^{\beta\gamma^\star}),\\
&= \tilde{h}_\gamma(t)\,\tilde{h}_\beta(t^{-\alpha\gamma^\star-\beta\gamma^\star})\,\tilde{h}_\alpha(t^{-\alpha\gamma^\star-\beta\gamma^\star})\,c_\alpha(-1,\,t^{\alpha\gamma^\star})\\
&= (\theta_\beta\theta_\alpha\theta_\beta)^{-1}(\tilde{h}_\gamma(t));
\end{aligned}$$

d'où la relation (W 2') pour θ_α et θ_β. Traitons finalement le cas où $\beta\alpha^\star = -2$. On va comparer $(\theta_\alpha\theta_\beta)^2(\tilde{h}_\gamma(t))$ et $(\theta_\beta\theta_\alpha)^2(\tilde{h}_\gamma(t))$. Notons d'abord que les éléments de la forme $\tilde{h}_\alpha(t^i)\tilde{h}_\beta(t^{2j})$ $(i, j \in \mathbf{Z})$ forment un sous-groupe abélien $\tilde{\mathrm{H}}'(t)$ de $\tilde{\mathrm{H}}$. Les automorphismes θ_α et θ_β laissent stables $\tilde{\mathrm{H}}'(t)$ et $\tilde{h}_\gamma(t)\,\tilde{\mathrm{H}}'(t)$. Nous avons donc

$$(\theta_\alpha\theta_\beta)^2(\tilde{h}_\gamma(t)) = \tilde{h}_\gamma(t)\,\tilde{h}'_1 \qquad \text{et} \qquad (\theta_\beta\theta_\alpha)^2(\tilde{h}_\gamma(t)) = \tilde{h}_\gamma(t)\,\tilde{h}'_2,$$

avec $\tilde{h}'_1, \tilde{h}'_2 \in \tilde{\mathrm{H}}'(t)$. On en déduit, par l'énoncé (b) et le lemme 6.1, que $\varphi(\tilde{h}'_1) = \varphi(\tilde{h}'_2)$. D'où $\tilde{h}'_1 = \tilde{h}'_2$, puisque la restriction de φ à $\tilde{\mathrm{H}}'(t)$ est injective. Cela achève la démonstration de (c).

Soient $\tilde{\mathfrak{N}}$ le groupe engendré par les symboles $\tilde{w}_\alpha$ $(\alpha \in \Delta)$ soumis aux relations (W 1) et (W 2), et $\tilde{\mathcal{H}}$ son sous-groupe engendré par les éléments $\tilde{h}_\alpha = \tilde{w}_\alpha^2$. D'après le lemme 6.5, (c), on peut alors former un groupe $\mathrm{N}^\star$ produit semi-direct de $\tilde{\mathrm{H}}$ par $\tilde{\mathfrak{N}}$, où $\tilde{\mathfrak{N}}$ opère sur $\tilde{\mathrm{H}}$ de sorte que $\tilde{w}_\alpha\tilde{h}\,\tilde{w}_\alpha^{-1} = \theta_\alpha(\tilde{h})$ pour $\alpha \in \Delta$ et $\tilde{h} \in \tilde{\mathrm{H}}$. On a alors le lemme suivant :

LEMME 6.6. — *(a) Il existe un morphisme j de $\tilde{\mathcal{H}}$ dans $\tilde{\mathrm{H}}$ tel que $j(\tilde{h}_\alpha) = \tilde{h}_\alpha(-1)$ pour tout $\alpha \in \Delta$. Les éléments de la forme $\tilde{h}\,j(\tilde{h})^{-1}$ $(\tilde{h} \in \tilde{\mathcal{H}})$ constituent un sous-groupe distingué* J *de* $\mathrm{N}^\star$.

(b) Soit $\tilde{\mathrm{N}}$ le groupe quotient de $\mathrm{N}^\star$ par J. *Alors $\tilde{\mathrm{H}}$ s'identifie à un sous-groupe distingué de $\tilde{\mathrm{N}}$. Le groupe $\tilde{\mathrm{N}}$ est une extension centrale de* N *par* A :

$$1 \to \mathrm{A} \to \tilde{\mathrm{N}} \xrightarrow{\varphi} \mathrm{N} \to 1;$$

où $\varphi(\tilde{h}_\alpha(t)) = h_\alpha(t)$ et $\varphi(p^\star(\tilde{w}_\alpha)) = w_\alpha(-1)$ pour $\alpha \in \Delta$, $p^\star$ désignant le morphisme naturel de $\mathrm{N}^\star$ sur $\tilde{\mathrm{N}}$. Posons

$$\tilde{w}_\alpha(t) = \tilde{h}_\alpha(t)\,p^\star(\tilde{w}_\alpha)^{-1} \quad \textit{pour tout } \alpha \in \Delta \quad \textit{et} \quad t \in k^\times;$$

alors

$$p^\star(\tilde{w}_\alpha) = \tilde{w}_\alpha(-1) \qquad \text{et} \qquad \tilde{w}_\alpha(t)^{-1} = \tilde{w}_\alpha(-t).$$

L'existence du morphisme j résulte du théorème 6.3, (c) et du fait que $c^0(-1, -1)^2 = c^\natural(-1, -1) = 1$. Le lemme 6.5, (c) entraîne que les éléments $\tilde{h}j(\tilde{h})^{-1}$ forment un sous-groupe distingué de $N^\star$. L'énoncé (b) est alors facile à vérifier.

Nous allons maintenant définir une extension E de G_k. Soit S le sous-ensemble de $G_k \times \tilde{N}$ formé des couples $[g, \tilde{n}]$ tels que $\nu(g) = \varphi(\tilde{n})$, où ν est l'application de G_k dans N définie dans le lemme 5.3, (b). On a un diagramme commutatif :

$$\begin{array}{ccc} S & \xrightarrow{\nu} & \tilde{N} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \varphi} \\ G_k & \xrightarrow{\nu} & N \end{array}$$

où $p([g, \tilde{n}]) = g$ et $\tilde{\nu}([g, \tilde{n}]) = \tilde{n}$. Définissons comme suit des transformations de S, $\lambda(\tilde{h})$, $\lambda(u)$ et λ_α $(\tilde{h} \in \tilde{H}, u \in U^+, \alpha \in \Delta)$:

(i) *Pour tout* $\tilde{h} \in \tilde{H}$, $\lambda(\tilde{h})[g, \tilde{n}] = [\varphi(\tilde{h})g, \tilde{h}\,\tilde{n}]$;

(ii) *Pour tout* $u \in U^+$, $\lambda(u)[g, \tilde{n}] = [ug, \tilde{n}]$;

(iii) *Pour tout* $\alpha \in \Delta$, $\lambda_\alpha[g, \tilde{n}]$ *est égal à*

$$[w_\alpha(-1)g, \tilde{w}_\alpha(-1)\tilde{n}] \quad \textit{ou à} \quad [w_\alpha(-1)g, \tilde{h}_\alpha(t^{-1})\tilde{n}],$$

suivant que $\nu(w_\alpha(-1)g)$ *est égal à* $w_\alpha(-1)\nu(g)$ *ou à* $h_\alpha(t^{-1})\nu(g)$.

Soit E le groupe de transformations de S engendré par $\lambda(\tilde{H})$, $\lambda(U^+)$ et les $\lambda_\alpha(\alpha \in \Delta)$. L'application λ donne un isomorphisme de $\tilde{H}$ [resp. de U^+] sur $\lambda(\tilde{H})$ [resp. $\lambda(U^+)$], et $\lambda(A)$ est un sous-groupe central de E. Par suite, E opère sur l'ensemble des orbites de $\lambda(A)$, lequel s'identifie à G_k par p. Les éléments de E agissent ainsi sur G_k comme des translations à gauche; d'où un morphisme canonique π de E sur G_k. Notre tâche consistera dorénavant à établir que le noyau de π se réduit bien à $\lambda(A)$.

Nous allons voir les relations existant entre divers éléments du groupe E.

LEMME 6.7. — (a) $\lambda(\tilde{h})\lambda(u)\lambda(\tilde{h})^{-1} = \lambda(\varphi(\tilde{h})u\varphi(\tilde{h})^{-1})$ *pour tout* $\tilde{h} \in \tilde{H}$ *et* $u \in U^+$.

(b) *Posons*

$$U_\alpha^+ = U^+ \cap w_\alpha(1)U^+w_\alpha(1)^{-1} \quad \textit{pour} \quad \alpha \in \Delta.$$

On a alors

$$U_\alpha^+ = w_\alpha(1)U_\alpha^+w_\alpha(1)^{-1} \quad \textit{et} \quad \lambda_\alpha^{-1}\lambda(u)\lambda_\alpha = \lambda(w_\alpha(1)uw_\alpha(1)^{-1})$$

pour tout $u \in U_\alpha^+$.

(c) $\lambda_\alpha^2 = \lambda(\tilde{h}_\alpha(-1))$ *pour tout* $\alpha \in \Delta$.

(d) $\lambda_\alpha^{-1}\lambda(\tilde{h})\lambda_\alpha = \lambda(\tilde{w}_\alpha(1)\tilde{h}\tilde{w}_\alpha(1)^{-1})$ *pour tout* $\alpha \in \Delta$ *et* $\tilde{h} \in \tilde{H}$.

Les deux premières assertions sont immédiates. Vérifions (c).

Si $\nu(w_\alpha(-1)g) = w_\alpha(-1)\nu(g)$, alors

$$\nu(w_\alpha(-1)^2 g) = w_\alpha(-1)\nu(w_\alpha(-1)g);$$

par suite,

$$\lambda_\alpha^2[g, \tilde{n}] = \lambda_\alpha[\tilde{w}_\alpha(-1)g, \tilde{w}_\alpha(-1)\tilde{n}] = [h_\alpha(-1)g, \tilde{w}_\alpha(-1)^2\tilde{n}].$$

Si $\nu(w_\alpha(-1)g) = h_\alpha(t^{-1})\nu(g)$, alors

$$\nu(w_\alpha(-1)^2 g) = h_\alpha(-t)\nu(w_\alpha(-1)g);$$

par suite,

$$\lambda_\alpha^2[g, \tilde{n}] = \lambda_\alpha[w_\alpha(-1)g, \tilde{h}_\alpha(t^{-1})\tilde{n}] = [h_\alpha(-1)g, \tilde{h}_\alpha(-t)\tilde{h}_\alpha(t^{-1})\tilde{n}].$$

On a donc, dans les deux cas, $\lambda_\alpha^2[g, \tilde{n}] = [h_\alpha(-1)g, \tilde{h}_\alpha(-1)\tilde{n}]$. Ajoutons que l'énoncé (c) permet d'écrire λ_α^{-1} : $\lambda_\alpha^{-1}[g, \tilde{n}]$ est égal à $[w_\alpha(1)g, \tilde{w}_\alpha(1)\tilde{n}]$ ou à $[w_\alpha(1)g, \tilde{h}_\alpha(-t)^{-1}\tilde{n}]$, suivant que $\nu(w_\alpha(1)g)$ est égal à $w_\alpha(1)\nu(g)$ ou à $h_\alpha(-t)^{-1}\nu(g)$.

Quant à la dernière assertion, on peut supposer que $\tilde{h}$ soit de la forme $\tilde{h}_\beta(s)$ ($\beta \in \Delta$, $s \in k^\times$).

Si $\nu(w_\alpha(-1)g) = w_\alpha(-1)\nu(g)$, alors on a

$$\lambda_\alpha^{-1}\lambda(\tilde{h})\lambda_\alpha[g, \tilde{n}] = [w_\alpha(1)h_\beta(s)w_\alpha(-1)g, \tilde{w}_\alpha(1)\tilde{h}_\beta(s)\tilde{w}_\alpha(-1)\tilde{n}].$$

Si $\nu(w_\alpha(-1)g) = \tilde{h}_\alpha(t^{-1})\nu(g)$, alors on a

$$\nu(w_\alpha(1)h_\beta(s)w_\alpha(-1)g) = h_\alpha(t^{-1}s^{\alpha\beta^\star})^{-1}\nu(h_\beta(s)w_\alpha(-1)g);$$

par suite,

$$\lambda_\alpha^{-1}\lambda(h)\lambda_\alpha[g, \tilde{n}] = [w_\alpha(1)h_\beta(s)w_\alpha(-1)g, \tilde{h}_\alpha(t^{-1}s^{\alpha\beta^\star})^{-1}\tilde{h}_\beta(s)\tilde{h}_\alpha(t^{-1})\tilde{n}].$$

Or, on a dans $\tilde{\mathrm{H}}$

$$\begin{aligned}
&\tilde{h}_\alpha(t^{-1}s^{\alpha\beta^\star})^{-1}\tilde{h}_\beta(s)\tilde{h}_\alpha(t^{-1}) \\
&\quad = \tilde{h}_\beta(s)\tilde{h}_\alpha(s^{-\alpha\beta^\star})c_\alpha(ts^{-\alpha\beta^\star}, s^{\alpha\beta^\star})c_\alpha(t^{-1}s^{\alpha\beta^\star}, s^{\alpha\beta^\star}) \\
&\quad = \tilde{h}_\beta(s)\tilde{h}_\alpha(s^{-\alpha\beta^\star}) = \tilde{w}(1)\tilde{h}_\beta(s)\tilde{w}_\alpha(1)^{-1}.
\end{aligned}$$

On en conclut donc que

$$\lambda_\alpha^{-1}\lambda(\tilde{h}_\beta(s))\lambda_\alpha = \lambda(\tilde{w}_\alpha(1)\tilde{h}_\beta(s)\tilde{w}_\alpha(1)^{-1}).$$

Nous avons ensuite le lemme suivant :

Lemme 6.8. — (a) *Si* G *est de rang* 1, E *est une extension centrale de* G_k *par* $\lambda(\mathrm{A})$. *Le cocycle de Steinberg* c_E *de* E *est égal à* $\lambda \circ c$, *où* c *est le cocycle de Steinberg initialement donné.*

(b) *Si* G *est de rang* 2, *les deux éléments* λ_α *et* λ_β *satisfont aux relations* (W 1) *et* (W 2) *du lemme* 6.1.

Ce lemme sera démontré au numéro suivant. Notons toutefois ici que c'est au cours de cette démonstration qu'intervient vraiment la condition non multiplicative (S 3) des cocycles de Steinberg.

Soient maintenant Δ' une partie de Δ et G'_k le sous-groupe de G_k engendré par les groupes radiciels U^β et $U^{-\beta}$ ($\beta \in \Delta'$). Posons

$$U'^{+} = G'_k \cap U^{+}, \qquad H' = G'_k \cap H, \qquad N' = G'_k \cap N \quad \text{et} \quad \tilde{H}' = \varphi^{-1}(H'),$$
$$\tilde{N}' = \varphi^{-1}(N'), \qquad S' = p^{-1}(G'_k).$$

On a alors le lemme suivant :

Lemme 6.9. — *Soit* E' *le sous-groupe de* E *engendré par* $\lambda(\tilde{H}')$, $\lambda(U'^{+})$ *et les éléments* λ_β ($\beta \in \Delta'$). *Alors* E' *laisse* S' *stable, et, si un élément de* E' *agit trivialement sur* S', *il est l'élément neutre.*

Il est clair que E' laisse S' stable. Considérons une classe arbitraire $G'_k g$ de G_k modulo G'_k. D'après le lemme 6.2, (*a*) et (*c*), il existe dans $G'_k g$ un élément g_1 tel que $\nu(g' g_1) = \nu(g')\,\nu(g_1)$ pour tout $g' \in G'_k$. On choisit alors un élément $\tilde{n}_1$ de $\tilde{N}$ tel que $\varphi(\tilde{n}_1) = \nu(g_1)$ et définit une application $\tau = \tau(g_1, \tilde{n}_1)$ de S' dans S par $\tau([g', \tilde{n}']) = [g' g_1, \tilde{n}'\tilde{n}_1]$; l'image de τ, qui est l'orbite de E' passant par $[g_1, \tilde{n}_1]$, est stable par E'. On voit alors de la définition même des générateurs initiaux de E, que $\varepsilon \circ \tau = \tau \circ \varepsilon$ sur S' pour les générateurs ε de E', à savoir $\lambda(\tilde{H}')$, $\lambda(U'^{+})$ et les λ_β ($\beta \in \Delta'$). L'égalité $\varepsilon \circ \tau = \tau \circ \varepsilon$ vaut donc pour tout élément ε de E'. Par conséquent, si un élément de E' agit sur S' trivialement, il agit trivialement aussi sur $\tau(S')$. Puisque $\tau(S')$ est une orbite arbitraire de E' dans S, cela prouve notre assertion.

Le lemme suivant est une conséquence des deux précédents :

Lemme 6.10. — (*a*) *Si l'on prend pour* Δ' *un élément* α *de* Δ, *le sous-groupe* E' *de* E *est une extension centrale de* G'_k *par* $\lambda(A)$ *et* $\lambda \circ c_\alpha$ *est le cocycle de Steinberg en* α *de* E'.

(*b*) *Les éléments* λ_α ($\alpha \in \Delta$) *de* E *satisfont aux relations* (W 1) *et* (W 2).

En effet, si l'on prend pour Δ' un ou deux éléments de Δ, l'action du groupe E' sur S' peut être regardée, soit comme l'un des cas de rang $\leqq 2$, soit comme composé direct de deux cas de rang 1, cas que nous avons étudiés dans le lemme 6.8. Nos assertions résultent donc des lemmes 6.8 et 6.9.

On en arrive finalement au résultat suivant :

Lemme 6.11. — (*a*) *L'isomorphisme* λ *de* $\tilde{H}$ *sur* $\lambda(\tilde{H})$ *se prolonge en un monomorphisme* λ *de* $\tilde{N}$ *dans* E *de sorte que* $\lambda(\tilde{w}_\alpha(-1)) = \lambda_\alpha$ *pour tout* $\alpha \in \Delta$ *Le quotient de* $\lambda(\tilde{N})$ *par* $\lambda(\tilde{H})$ *est isomorphe à* W.

(*b*) *Soit* λ_σ *un représentant dans* $\lambda(\tilde{\mathrm{N}})$ *d'un élément* σ *de* W. *Alors, si* α *et* σ_α *sont des racines positives, on a dans* E

$$\lambda_\sigma \lambda(\mathrm{U}^\alpha)\lambda_\sigma^{-1} = \lambda(\mathrm{U}^{\sigma\alpha}).$$

(*c*) *Le groupe* E *est la réunion des sous-ensembles* $\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_\sigma\lambda(\mathrm{U}^+)$, *où* $\{\lambda_\sigma\}$ *est un système de représentants de* W *dans* $\lambda(\tilde{\mathrm{N}})$.

(*d*) *Le noyau du morphisme canonique* π *de* E *sur* G_k *se réduit à* $\lambda(\mathrm{A})$. *Pour chaque* $\alpha \in \Delta$, *le cocycle de Steinberg en* α *de l'extension centrale* E *est égal à* $\lambda \circ c_\alpha$.

Notons Λ le sous-groupe de E engendré par les éléments λ_α pour $\alpha \in \Delta$. Le quotient de Λ par $\Lambda \cap \lambda(\tilde{\mathrm{H}})$ est isomorphe à W, en vertu du théorème 6.3 et du lemme 6.10, (*b*). Notre premier énoncé résulte alors du lemme 6.7, (*d*) Quant à l'énoncé (*b*), si $l(\sigma) = 1$, il découle immédiatement du lemme 6.7,(*a*) et (*b*). Le cas général résulte de là, d'après le lemme 6.2, (*b*), par récurrence sur $l(\sigma)$. On peut maintenant vérifier l'assertion (*c*) par un procédé habituel. En effet, il suffit de montrer que cette réunion de sous-ensembles de E est stable par multiplication à gauche des générateurs initiaux de E. Ceci est évident pour $\lambda(\tilde{h})$ et $\lambda(u)$ $(\tilde{h} \in \tilde{\mathrm{H}},\ u \in \mathrm{U}^+)$. Soient α un élément de Δ et σ un élément de W. D'abord, l'ensemble $\lambda_\alpha\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_\sigma\lambda(\mathrm{U}^+)$ est identique à $\lambda(\mathrm{U}_\alpha^+)\lambda(\tilde{\mathrm{H}})\lambda_\alpha\lambda(\mathrm{U}^\alpha)\lambda_\sigma\lambda(\mathrm{U}^+)$. Puis, si $\sigma^{-1}\alpha$ est positive, l'énoncé (*b*) entraîne que

$$\lambda(\mathrm{U}^\alpha)\lambda_\sigma = \lambda_\sigma\lambda(\mathrm{U}^\beta), \qquad \text{où} \quad \beta = \sigma^{-1}\alpha;$$

$\lambda_\alpha\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_\sigma\lambda(\mathrm{U}^+)$ est alors contenu dans $\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_{\sigma'}\lambda(\mathrm{U}^+)$ pour $\sigma' = \sigma_\alpha\sigma$. Si β n'est pas positive, alors $\sigma'^{-1}\alpha$ est positive; d'autre part, $\lambda_\alpha\lambda(\mathrm{U}^\alpha)\lambda_\alpha^{-1}$ est contenu dans la réunion de $\lambda(\mathrm{U}^\alpha)\lambda(\tilde{\mathrm{H}}^\alpha)$ et $\lambda(\mathrm{U}^\alpha)\lambda(\tilde{\mathrm{H}}^\alpha)\lambda_\alpha\lambda(\mathrm{U}^\alpha)$, en vertu du lemme 6.10, (*a*); il en résulte que $\lambda_\alpha\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_\sigma\lambda(\mathrm{U}^\alpha)$ est contenu dans la réunion de $\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_\sigma\lambda(\mathrm{U}^+)$ et $\lambda(\mathrm{U}^+)\lambda(\tilde{\mathrm{H}})\lambda_{\sigma'}\lambda(\mathrm{U}^+)$. L'énoncé (*c*) est ainsi démontré. On déduit de celui-ci immédiatement que le noyau de π est contenu dans $\lambda(\tilde{\mathrm{H}})$ et donc qu'il se réduit à $\lambda(\mathrm{A})$. Le lemme 6.10, (*a*) entraîne la dernière assertion de (*d*).

On conclut ainsi, en identifiant par λ le noyau $\lambda(\mathrm{A})$ avec A, que E est une extension centrale de G_k par A et que le cocycle de Steinberg c_E de E est le cocycle c initialement donné.

Nous avons ainsi achevé la démonstration du théorème 5.10.

7. Nous donnerons dans ce numéro une démonstration du lemme 6.8.

Nous allons d'abord introduire un autre groupe de transformations de S. Soit ι la transformation de S d'ordre 2 définie comme suit :

$$\iota[g, \tilde{n}] = [g^{-1}, \tilde{n}^{-1}] \quad \text{pour tout } [g, \tilde{n}] \in \mathrm{S}.$$

Notons E^* le transformé de E par ι; $E^* = \iota E \iota$. Le groupe E^* opère, comme E, transitivement sur S.

Nous nous proposons de montrer que les éléments de E commutent avec ceux de E^* dans le groupe des transformations de S. Posons

$$\rho(\tilde{h}) = \iota\lambda(\tilde{h})\iota, \qquad \rho(u) = \iota\lambda(u)\iota, \qquad \rho_\alpha = \iota\lambda_\alpha\iota \qquad \text{pour } \tilde{h} \in \tilde{H}, \quad u \in U^+, \quad \alpha \in \Delta.$$

Le lemme suivant allégera notre travail.

LEMME 7.1. — (*a*) *Les éléments de* $\lambda(\tilde{H})$ *ou de* $\lambda(U^+)$ [*resp. de* $\rho(\tilde{H})$ *ou de* $\rho(U^+)$] *commutent avec tous les éléments de* E^* [*resp. de* E].

(*b*) *Soient* α, β *des éléments de* Δ. *Si* λ_α *commute avec* ρ_β, *alors* ρ_α *commute avec* λ_β.

(*c*) *On a* $(\lambda_\alpha^{-1}\rho_\beta\lambda_\alpha\rho_\beta^{-1})\varepsilon = \varepsilon(\lambda_\alpha^{-1}\rho_\beta\lambda_\alpha\rho_\beta^{-1})$ *pour tout élément* ε *de* $\lambda(\tilde{H})$, $\lambda(U_\alpha^+)$, $\rho(\tilde{H})$ *ou* $\rho(U_\beta^+)$.

(*d*) *Si* $\lambda_\alpha^{-1}\rho_\beta\lambda_\alpha\rho_\beta^{-1}$ *laisse fixe un élément* $\mathbf{s}$ *de* S, *il en est de même pour* $\lambda_\alpha\mathbf{s}$ *et* $\rho_\beta^{-1}\mathbf{s}$.

On voit d'abord aisément que les éléments de $\rho(\tilde{H})$ ou de $\rho(U^+)$ commutent avec les générateurs initiaux de E. L'énoncé (*b*) est évident. Quant à l'énoncé (*c*), si ε est un élément de $\lambda(\tilde{H})$ ou de $\lambda(U_\alpha^+)$, alors

$$(\lambda_\alpha\rho_\beta^{-1})\,\varepsilon\,(\lambda_\alpha\rho_\beta^{-1})^{-1} = \lambda_\alpha\varepsilon\lambda_\alpha^{-1} = (\rho_\beta^{-1}\lambda_\alpha)\,\varepsilon\,(\rho_\beta^{-1}\lambda_\alpha)^{-1},$$

compte tenu de l'énoncé (*a*). Enfin, si $\lambda_\alpha\rho_\beta^{-1}\mathbf{s} = \rho_\beta^{-1}\lambda_\alpha\mathbf{s}$, alors

$$\lambda_\alpha\rho_\beta^{-1}(\lambda_\alpha\mathbf{s}) = \lambda_\alpha(\rho_\beta^{-1}\lambda_\alpha\mathbf{s}) = \lambda_\alpha^2\rho_\beta^{-1}\mathbf{s} = \rho_\beta^{-1}\lambda_\alpha^2\mathbf{s},$$

d'après les lemmes 6.7, (*c*) et 7.1, (*a*). Il en va de même pour $\rho_\beta^{-1}\mathbf{s}$. Le lemme est ainsi démontré.

Pour voir que $\lambda_\alpha\rho_\beta^{-1} = \rho_\beta^{-1}\lambda_\alpha$, il suffit, d'après le lemme 7.1, (*c*), de vérifier que $\lambda_\alpha\rho_\beta^{-1}\mathbf{s} = \rho_\beta^{-1}\lambda_\alpha\mathbf{s}$ pour tout élément $\mathbf{s}$ de S_1, si S_1 est une partie de S qui rencontre toutes les orbites du groupe $\lambda(U_\alpha^+)\lambda(\tilde{H})\rho(\tilde{H})\rho(U_\beta^+)$. Utilisant la décomposition de Bruhat de G_k, on peut aisément déterminer les orbites dans S de ce dernier groupe.

On sait, d'après les lemmes 6.1 et 6.6, que les éléments $w_\alpha(1)$ [resp. $\tilde{w}_\alpha(1)$] ($\alpha \in \Delta$) satisfont aux relations (W 1) et (W 2). Définissons alors un système de représentants $\{w(\sigma)\}$ [resp. $\{\tilde{w}(\sigma)\}$] de W dans N [resp. $\tilde{N}$] si σ s'écrit comme mot minimal $\prod_{i=1}^{m}\sigma_{\alpha_i}$, où $m = l(\sigma)$ et $\alpha_i \in \Delta$, alors

$$w(\sigma) = \prod_{i=1}^{m} w_{\alpha_i}(1) \left[\text{resp. } \tilde{w}(\sigma) = \prod_{i=1}^{m} \tilde{w}_{\alpha_i}(1)\right].$$

Cette définition est justifiée par le lemme 6.2, (*d*).

Alors, on voit aisément que toute orbite dans S du groupe $\lambda(U_\alpha^+)\lambda(\tilde{H})\rho(\tilde{H})\rho(U_\beta^+)$ contient un élément **s** de la forme

$$[x_\alpha(u)\, w(\sigma)\, x_\beta(v),\ \tilde{w}(\sigma)], \qquad \text{où} \quad \sigma\in W \quad \text{et} \quad u, v\in k.$$

Rappelons que nous ne discutons que les cas du type A_1, A_2 ou C_2.

LEMME 7.2. — (*a*) *Si* $\sigma\beta \neq \pm\alpha$, *alors*

$$l(\sigma_\alpha\sigma) - l(\sigma) = l(\sigma_\alpha\sigma\sigma_\beta) - l(\sigma\sigma_\beta) \qquad et \qquad l(\sigma\sigma_\beta) - l(\sigma) = l(\sigma_\alpha\sigma\sigma_\beta) - l(\sigma_\alpha\sigma).$$

(*b*) *Si* $\sigma\beta = \alpha$, *alors*

$$\sigma\sigma_\beta = \sigma_\alpha\sigma, \qquad w(\sigma)\, x_\beta(v)\, w(\sigma)^{-1} = x_\alpha(v) \qquad et \qquad \tilde{w}(\sigma)\, \tilde{h}_\beta(t)\, \tilde{w}(\sigma)^{-1} = \tilde{h}_\alpha(t)$$

pour tout $v\in k$, $t\in k^\times$.

(*c*) *Si* $\sigma\beta = -\alpha$, *alors*

$$\sigma\sigma_\beta = \sigma_\alpha\sigma \qquad et \qquad l(\sigma\sigma_\beta) = l(\sigma) - 1.$$

(*d*) *Si c est un cocycle de Steinberg sur* $k^\times$ *à valeurs dans* A, *alors*

$$c(u^{-1}, (v-u^{-1})^{-1}) = c((u-v^{-1})^{-1}, v^{-1})$$

pour tout $u, v\in k^\times$ *tels que* $1 - uv \neq 0$.

Le lemme 6.2 entraîne facilement les énoncés (*a*) et (*c*), qui sont valables quel que soit le type de Δ. On vérifie l'assertion (*d*) par le même raisonnement que celui de la proposition 5.5. Quant à l'énoncé (*b*), il est évident que $\sigma\sigma_\beta = \sigma_\alpha\sigma$. Pour voir les autres assertions de (*b*), nous distinguons plusieurs cas; le premier cas où $\alpha = \beta$ et $\sigma = e$, le deuxième où Δ est de type C_2, $\alpha = \beta$ et $\sigma = \sigma_\gamma\sigma_\alpha\sigma_\gamma$ avec l'autre élément γ de Δ, et le troisième où Δ est de type A_2, $\alpha \neq \beta$ et $\sigma = \sigma_\beta\sigma_\alpha$. Dans le premier cas, nos assertions sont triviales. Dans les autres cas, on déduit aisément, en appliquant à G_k le lemme 5.1, que $w(\sigma)\, x_\beta(v)\, w(\sigma)^{-1} = x_\alpha(v)$. Puis, dans le deuxième cas, on a

$$\begin{aligned}
\tilde{w}(\sigma)\, \tilde{h}_\alpha(t)\, \tilde{w}(\sigma)^{-1} &= (\tilde{w}_\gamma(1)\, \tilde{w}_\alpha(1))\, \tilde{h}_\alpha(t)\, \tilde{h}_\gamma(t^{-\gamma\alpha^*})\, (\tilde{w}_\gamma(1)\, \tilde{w}_\alpha(1))^{-1} \\
&= \tilde{w}_\gamma(1)\, \tilde{h}_\alpha(t^{-1})\, \tilde{h}_\gamma(t^{-\gamma\alpha^*})\, \tilde{h}_\alpha(t^2)\, \tilde{w}_\gamma(1)^{-1} \\
&= \tilde{w}_\gamma(1)\, \tilde{h}_\alpha(t)\, \tilde{h}_\gamma(t^{-\gamma\alpha^*})\, \tilde{w}_\gamma(1)^{-1} \\
&= \tilde{h}_\alpha(t)\, \tilde{h}_\gamma(t^{-\gamma\alpha^*})\, \tilde{h}_\gamma(t^{\gamma\alpha^*}) \\
&= \tilde{h}_\alpha(t).
\end{aligned}$$

Enfin, dans le troisième cas, on a

$$\begin{aligned}
\tilde{w}(\sigma)\, \tilde{h}_\beta(t)\, \tilde{w}(\sigma)^{-1} &= \tilde{w}_\beta(1)\, \tilde{h}_\beta(t)\, \tilde{h}_\alpha(t)\, \tilde{w}_\beta(1)^{-1} \\
&= \tilde{h}_\beta(t^{-1})\, \tilde{h}_\alpha(t)\, \tilde{h}_\beta(t) = c_\beta(t, t)\, c_\beta(t^{-1}, t)\, \tilde{h}_\alpha(t) \\
&= \tilde{h}_\alpha(t).
\end{aligned}$$

Les assertions de l'énoncé (*b*) sont ainsi démontrées.

Nous allons maintenant vérifier que $\lambda_\alpha \rho_\beta^{-1} \mathbf{s} = \rho_\beta^{-1} \lambda_\alpha \mathbf{s}$ pour tout élément $\mathbf{s}$ de la forme $[x_\alpha(u)\, w(\sigma)\, x_\beta(v), \tilde{w}(\sigma)]$ où $\sigma \in \mathrm{W}$ et $u, v \in k$.

Si $\sigma\beta \neq \pm \alpha$, alors on vérifie, d'après le lemme 7.2, (a), que

$$\nu(g)^{-1} \nu(g w_\beta(-1)) = \nu(w_\alpha(-1) g)^{-1} \nu(w_\alpha(-1) g\, w_\beta(-1))$$

et

$$\nu(w_\alpha(-1) g)\, \nu(g)^{-1} = \nu(w_\alpha(-1) g w_\beta(-1))\, \nu(g w_\beta(-1))^{-1}$$

pour $g = x_\alpha(u)\, w(\sigma)\, x_\beta(v)$; ce qui entraîne, vu la définition de λ_α et ρ_β^{-1}, que $\lambda_\alpha \rho_\beta^{-1} \mathbf{s} = \rho_\beta^{-1} \lambda_\alpha \mathbf{s}$.

Si $\sigma\beta = \alpha$, on peut supposer $v = 0$, d'après le lemme 7.2, (b). Alors, pour $g = x_\alpha(u)\, w(\sigma)$ avec $u \neq 0$, on a

$$\nu(g w_\beta(-1)) = \nu(g)\, w_\beta(-1) \qquad \text{et} \qquad \nu(w_\alpha(-1) g w_\beta(-1)) = h_\alpha(u^{-1})\, \nu(g w_\beta(-1))\,;$$

d'où

$$\begin{aligned}\tilde{\nu}(\lambda_\alpha \rho_\beta^{-1}[g, \tilde{w}(\sigma)]) &= \tilde{h}_\alpha(u^{-1})\, \tilde{w}(\sigma)\, \tilde{w}_\beta(-1) = \tilde{h}_\alpha(u^{-1})\, \tilde{w}(\sigma)\, \tilde{h}_\beta(-1)\, \tilde{w}_\beta(1)\\ &= \tilde{h}_\alpha(u^{-1})\, \tilde{h}_\alpha(-1)\, \tilde{w}(\sigma\sigma_\beta)\,;\end{aligned}$$

d'autre part, on a de façon analogue,

$$\begin{aligned}\tilde{\nu}(\rho_\beta^{-1} \lambda_\alpha[g, \tilde{w}(\sigma)]) &= \tilde{w}_\alpha(-1)\, \tilde{w}(\sigma)\, \tilde{h}_\beta(u) = \tilde{h}_\alpha(-1)\, \tilde{w}_\alpha(1)\, \tilde{h}_\alpha(u)\, \tilde{w}(\sigma)\\ &= \tilde{h}_\alpha(-1)\, \tilde{h}_\alpha(u^{-1})\, \tilde{w}(\sigma_\alpha \sigma).\end{aligned}$$

Le lemme 7.2, (b) montre ainsi que $\lambda_\alpha \rho_\beta^{-1} \mathbf{s} = \rho_\beta^{-1} \lambda_\alpha \mathbf{s}$.

Supposons enfin que $\sigma\beta = -\alpha$. Si $uv(1 - uv) = 0$, on se ramène au cas précédent par le lemme 7.1, (d). Si $uv(1 - uv) \neq 0$, alors, pour $g = x_\alpha(u)\, w(\sigma)\, x_\beta(v)$, on a

$$\begin{aligned}g w_\beta(-1) &= x_\alpha(u)\, w(\sigma\sigma_\beta)\, x_\beta(-v^{-1})\, w_\beta(1)\, h_\beta(v)\, x_\beta(-v^{-1})\\ &= x_\alpha(u - v^{-1})\, w(\sigma)\, h_\beta(v)\, x_\beta(-v^{-1})\,;\end{aligned}$$

d'où

$$\begin{aligned}\tilde{\nu}(\lambda_\alpha \rho_\beta^{-1}[g, \tilde{w}(\sigma)]) &= \tilde{h}_\alpha((u - v^{-1})^{-1})\, \tilde{w}(\sigma)\, \tilde{h}_\beta(v)\\ &= \tilde{h}_\alpha((u - v^{-1})^{-1})\, \tilde{h}_\alpha(v^{-1})\, \tilde{w}(\sigma)\,;\end{aligned}$$

d'autre part, on a de façon analogue,

$$\begin{aligned}\tilde{\nu}(\rho_\beta^{-1} \lambda_\alpha[g, \tilde{w}(\sigma)]) &= \tilde{h}_\alpha(u^{-1})\, \tilde{w}(\sigma)\, \tilde{h}_\beta(v - u^{-1})\\ &= \tilde{h}_\alpha(u^{-1})\, \tilde{h}_\alpha((v - u^{-1})^{-1})\, \tilde{w}(\sigma).\end{aligned}$$

Le lemme 7.2 entraîne ainsi que $\lambda_\alpha \rho_\beta^{-1} \mathbf{s} = \rho_\beta^{-1} \lambda_\alpha \mathbf{s}$.

Nous savons donc que les éléments λ_α de E commutent avec les éléments ρ_β de $\mathrm{E}^\star$. Il en résulte, compte tenu du lemme 7.1, (a), que tout élément de E commute avec les éléments de $\mathrm{E}^\star$. Puisque E et $\mathrm{E}^\star$ sont transitifs sur S, on en conclut que E est simplement transitif sur S.

Alors, comme les éléments $\tilde{w}_\alpha(-1)$ $(\alpha \in \Delta)$ satisfont aux relations (W 1) et (W 2), on voit aussitôt qu'il en va de même pour les éléments λ_α de E.

Dans le cas de rang 1, puisque E est simplement transitif sur S, la décomposition de Bruhat de G_k indique que E est la réunion de $\lambda(U^+)\lambda(\tilde{H})$ et de $\lambda(U^+)\lambda(\tilde{H})\lambda_\alpha\lambda(U^+)$. On en conclut aussitôt que le noyau du morphisme canonique π de E sur G_k se réduit à $\lambda(A)$. Le groupe E est donc une extension centrale de G_k par $\lambda(A)$. En posant

$$\xi_\alpha(u) = \lambda(x_\alpha(u)) \qquad \text{et} \qquad \xi_{-\alpha}(u) = \lambda_\alpha \xi_\alpha(-u)\lambda_\alpha^{-1},$$

on vérifie aisément que

$$\omega_\alpha(t) = \xi_\alpha(t)\,\xi_{-\alpha}(-t^{-1})\,\xi_\alpha(t) = \lambda(\tilde{h}_\alpha(t))\,\lambda_\alpha^{-1}$$

pour tout $t \in k^\times$. Or, d'après les lemmes 6.7, (*a*), 5.2, (*c*) et 5.1, ξ_α et $\xi_{-\alpha}$ donnent les isomorphismes de k dans $\pi^{-1}(U^\alpha)$ et $\pi^{-1}(U^{-\alpha})$ qui servent à définir le cocycle de Steinberg c_E en α de E relatif aux isomorphismes x_α et $x_{-\alpha}$. On en conclut que $c_E = \lambda \circ c_\alpha = \lambda \circ c$, où c est le cocycle de Steinberg initialement donné.

Nous avons ainsi achevé la démonstration du lemme 6.8.

Ajoutons que le lemme 7.2, (*b*) est en fait valable, avec les notations du n° 5, quel que soit le type de G et quelle que soit l'extension centrale E de G_k.

8. Nous étudierons dans ce numéro les conditions supplémentaires à imposer dans le cas topologique aux cocycles de Steinberg.

Soient k un corps topologique infini et A un groupe abélien topologique, qu'on suppose, bien entendu, séparés. Le cas qui nous intéresse particulièrement est celui où k et A sont localement compacts.

Le groupe G_k est alors muni d'une structure naturelle de groupe topologique. Les sous-groupes H_k, N_k, U_k^+, U_k^-, U_k^α $(\alpha \in \Phi)$ sont tous fermés dans G_k. L'application $(u, h, u') \mapsto uhu'$ de $U_k^+ \times H_k \times U_k^-$ dans G_k induit un homéomorphisme de l'espace produit sur un ouvert Ω_k de G_k.

Soit E une extension centrale de G_k par A. On entend par là la donnée d'une suite exacte: $1 \to A \xrightarrow{i} E \xrightarrow{\pi} G_k \to 1$, où est i un isomorphisme de A sur un sous-groupe central fermé de E et où π induit un isomorphisme de $E/i(A)$ sur G_k.

On va considérer, comme au n° 5, les relèvements $\tilde{U}^\alpha$ des groupes radiciels U_k^α $(\alpha \in \Phi)$, les applications $\tilde{x}_\alpha$, $\tilde{w}_\alpha$, $\tilde{h}_\alpha$ et les sous-groupes $\tilde{U}^+$, $\tilde{U}^-$, $\tilde{H}$ et $\tilde{N}$ de E.

On a le lemme suivant :

Lemme 8.1. — (*a*) *Pour tout* $\alpha \in \Phi$, $\tilde{x}_\alpha$ *est un isomorphisme de* k *sur le sous-groupe fermé* $\tilde{U}^\alpha$ *de* E. *Le groupe* $\tilde{U}^+$ [*resp.* $\tilde{U}^-$] *est un sous-groupe fermé de* E, *duquel* π *induit un isomorphisme sur* U_k^+ [*resp.* U_k^-].

(*b*) *Pour tout* $\alpha \in \Phi$, $\tilde{h}_\alpha$ *est un homéomorphisme de* $k^\times$ *sur un sous-ensemble fermé de* E.

(*c*) *Pour tout* $\alpha \in \Phi$, *le cocycle de Steinberg* c_α *en* α *est une application continue de* $k^\times \times k^\times$ *dans* A.

(*d*) *L'application* $(u, h, u') \mapsto uhu'$ *définit un homéomorphisme de* $\tilde{\mathrm{U}}^+ \times \tilde{\mathrm{H}} \times \tilde{\mathrm{U}}^-$ *sur un ouvert* Ω_{E} *de* E.

(*e*) *Quand on convient que* $c_\alpha(0, 1) = c_\alpha(1, 0) = 1$, *la fonction* $c_\alpha(u, 1 - uv)$ *de* (u, v), *définie sur un voisinage de* $(0, 0)$ *dans* $k \times k$, *est continue en* $(0, 0)$.

Vérifions d'abord l'énoncé (*a*). D'après le lemme 5.2, (*c*), on a

$$\tilde{x}_\alpha(u(t^2 - 1)) = \tilde{h}_\alpha(t)\, \mathfrak{s}(x_\alpha(u))\, \tilde{h}_\alpha(t)^{-1} \mathfrak{s}(x_\alpha(u))^{-1},$$

où t est un élément fixe de $k^\times$ tel que $t^2 \neq 1$ et où $\mathfrak{s}$ est un relèvement quelconque de U_k^α dans E. Soit $\mathfrak{V}$ un voisinage de e dans E. Il existe alors un voisinage ouvert $\mathfrak{V}'$ de e dans E tel que

$$\tilde{h}_\alpha(t)\, \tilde{g}\, \tilde{h}_\alpha(t)^{-1} \tilde{g}^{-1} \in \mathfrak{V} \quad \text{pour tout } \tilde{g} \in \mathfrak{V}'.$$

L'image $\pi(\mathfrak{V}')$, étant un ouvert de G_k, contient $x_\alpha(\mathfrak{V}^0)$ pour un voisinage $\mathfrak{V}^0$ de 0 dans k. Par suite, si u est dans $\mathfrak{V}^0$, l'élément $\tilde{x}_\alpha(u(t^2 - 1))$ appartient à $\mathfrak{V}$. Ceci montre que l'isomorphisme $\tilde{x}_\alpha$ est continu en 0, et donc dans k tout entier. Compte tenu de l'épimorphisme π, alors $\tilde{x}_\alpha$ induit un isomorphisme de k sur un sous-groupe fermé de E. De là résultent facilement l'assertion sur $\tilde{\mathrm{U}}^+$ et $\tilde{\mathrm{U}}^-$ et les énoncés (*b*), (*c*) et (*d*). On a une application continue $(u, v) \mapsto \tilde{x}_{-\alpha}(u)\tilde{x}_\alpha(v)$ de $k \times k$ dans E. L'élément $\tilde{x}_{-\alpha}(u)\tilde{x}_\alpha(v)$ est dans $\tilde{\mathrm{U}}^+\tilde{\mathrm{H}}\tilde{\mathrm{U}}^-$ si $1 + uv \neq 0$, et d'après le lemme 5.9, on a

$$\begin{aligned}\tilde{x}_{-\alpha}(u)\, \tilde{x}_\alpha(v) = \tilde{x}_\alpha(v(1 + uv)^{-1})\, \tilde{h}_\alpha((1 + uv)^{-1})& \\ \times [c_\alpha(-u, 1 + uv)\, c_\alpha(1 + uv, -1)^{-1}]\, \tilde{x}_{-\alpha}(u(1 + uv)^{-1});&\end{aligned}$$

avec notre convention, cette formule est valable dès que $1 + uv \neq 0$. La continuité entraîne alors que $c_\alpha(-u, 1 + uv)$ tend vers 1 lorsque (u, v) tend vers $(0, 0)$. D'où l'assertion (*e*).

Nous disons à ce numéro qu'un cocycle de Steinberg c sur $k^\times$ à valeurs dans A est *topologique*, s'il vérifie la condition suivante :

(S 0) *La fonction* $c(x, y)$ *est continue dans* $k^\times \times k^\times$, *et, quand on convient que* $c(1, 0) = c(0, 1) = 1$, *la fonction* $c(x, 1 - xy)$ *de* (x, y), *définie sur un voisinage de* $(0, 0)$ *dans* $k \times k$, *est continue en* $(0, 0)$.

Notons, provisoirement, $\mathrm{St}(k^\times, \mathrm{A})$ le groupe des cocycles de Steinberg topologiques sur $k^\times$ à valeurs dans A. Puisqu'un cocycle de Steinberg c vérifie l'identité $c(1 - uv, u) = c(v, 1 - uv)$, si c appartient à $\mathrm{St}(k^\times, \mathrm{A})$, il en est de même de $\check{c}$ et de $c^\natural$, avec les notations de la proposition 5.7.

Nous allons démontrer la version topologique du théorème 5.10.

THÉORÈME 8.2. — *Soient k un corps topologique infini, A un groupe abélien topologique et G_k le groupe topologique des points rationnels d'un groupe simple simplement connexe G déployé sur k. Alors, les classes d'extensions centrales de G_k par A sont en correspondance biunivoque avec les cocycles de Steinberg topologiques (et bilinéaires si G est de type non symplectique) sur $k^\times$ à valeurs dans A. Le groupe multiplicatif de ces derniers est isomorphe au groupe $H^2(G_k, A)$ que forment les premières avec la multiplication de Baer.*

En effet, d'après le théorème 5.10 et le lemme 8.1, on obtient un homomorphisme de $H^2(G_k, A)$ dans $\mathrm{St}(k^\times, A)$, en associant à une extension centrale E de G_k par A le cocycle de Steinberg c_E appartenant à E. D'abord, cet homomorphisme est injectif. En effet, d'après le lemme 8.1, si c_E est trivial, les groupes radiciels $\tilde{U}^\alpha$ engendrent un sous-groupe fermé de E qui est isomorphe à G_k par π.

Compte tenu du théorème 5.10, il nous reste à montrer, étant donnée une extension centrale E de G_k par A au sens abstrait, que si c_E vérifie la condition (S 0), E peut être munie d'une topologie qui en fasse une extension de G_k par A au sens topologique.

On note tout d'abord que, d'après le lemme 5.8 et la remarque précédant notre théorème, les cocycles de Steinberg c_α en α ($\alpha \in \Phi$) vérifient tous la condition (S 0). Munissons $\tilde{H}$ d'une topologie en disant que l'application

$$\left(\prod_{\alpha\in\Delta} h_\alpha(t_\alpha),\ a\right) \mapsto \left(\prod_{\alpha\in\Delta} \tilde{h}_\alpha(t_\alpha)\right) a$$

est un homéomorphisme de $H_k \times A$ sur $\tilde{H}$. Cette topologie fait de $\tilde{H}$ une extension topologique de H_k, puisque les cocycles c_α sont continus dans $k^\times \times k^\times$. On transporte, d'autre part, sur $\tilde{U}^+$ [resp. $\tilde{U}^-$] la topologie de U_k^+ [resp. de U_k^-] au moyen du morphisme π de E sur G_k.

Considérons ensuite le sous-ensemble $\Omega_E = \tilde{U}^+ \tilde{H} \tilde{U}^-$ de E, qu'on munit, par cette décomposition, de la topologie produit. On définit alors les voisinages de l'élément neutre e dans E comme les sous-ensembles de E rencontrant Ω_E suivant un voisinage de e dans Ω_E. On va montrer que ces données à l'origine font de E un groupe topologique, en vérifiant que l'application $(x, y) \mapsto x^{-1}y$ est continue en (e, e) et que $\mathrm{Ad}(z)$ et $\mathrm{Ad}(z^{-1})$ sont continus en (e, e) pour tout élément z d'un ensemble générateur de E. Dans le cas de rang 1, on le vérifie tout de suite, en tenant compte du lemme 5.9 et en prenant pour générateurs A, $\tilde{U}^\alpha$ et $\tilde{w}_\alpha(1)$. Dans le cas général, on voit immédiatement que $(x, y) \mapsto x^{-1}y$ est continu en (e, e)

pour $x \in \tilde{U}^+ \tilde{H}$ et $y \in E$. D'autre part, en se ramenant au cas de rang 1, on vérifie que $\mathrm{Ad}(z)$ est continu en e pour $z \in \tilde{U}^{\alpha}$ ou $z \in \tilde{U}^{-\alpha}$, α étant un élément de Δ; par suite, $\mathrm{Ad}(z)$ est continu en e pour tout élément z de E. Soit β un élément de Φ; il existe alors un élément n de $\tilde{N}$ tel que $\tilde{U}^{\beta} = n \tilde{U}^{\alpha} n^{-1}$ avec une racine positive α; l'identité $(nxn^{-1})^{-1} y = n(x^{-1}(n^{-1}yn))n^{-1}$ montre que $(x, y) \mapsto x^{-1}y$ est continu en (e, e) pour $x \in \tilde{U}^{\beta}$ et $y \in E$. Compte tenu de la décomposition de Ω_E, cela entraîne aussitôt que $(x, y) \mapsto x^{-1}y$ est continu en (e, e). Ainsi E est un groupe topologique. Il est maintenant clair que A est un sous-groupe fermé de E et que π induit un isomorphisme de E/A sur G_k.

Ceci achève de démontrer le théorème 8.2.

9. Nous donnerons dans ce numéro des exemples de cocycles de Steinberg.

Dans ce qui suit, k est un corps topologique et A un groupe abélien topologique, et l'on entendra par cocycle de Steinberg un cocycle de Steinberg topologique. On notera $S(k^{\times}, A)$ le groupe des cocycles de Steinberg sur $k^{\times}$ à valeurs dans A.

Remarquons d'abord des propriétés fonctorielles évidentes des groupes $S(k^{\times}, A)$.

a. Si j est un plongement continu d'un corps topologique k_1 dans k, on a un homomorphisme j^* de $S(k^{\times}, A)$ dans $S(k_1^{\times}, A)$, défini par

$$j^*(c)\,(x, y) = c(j(x), j(y)) \qquad \text{pour} \quad c \in S(k^{\times}, A) \quad \text{et} \quad x, y \in k_1^{\times}.$$

b. Soient B un groupe abélien topologique et $\mathrm{Hom}(A, B)$ le groupe des morphismes continus de A dans B. Pour $c \in S(k^{\times}, A)$ et $\lambda \in \mathrm{Hom}(A, B)$, la composée $\lambda \circ c$ est un cocycle de Steinberg sur $k^{\times}$ à valeurs dans B. Si l'on regarde $S(k^{\times}, A)$, $S(k^{\times}, B)$ et $\mathrm{Hom}(A, B)$ comme des $\mathbf{Z}$-modules, on obtient ainsi un homomorphisme du produit tensoriel $S(k^{\times}, A) \otimes_{\mathbf{Z}} \mathrm{Hom}(A, B)$ dans $S(k^{\times}, B)$.

La théorie des algèbres simples, combinée avec la théorie des corps kummériens, fournit un exemple de cocycle de Steinberg bilinéaire. Supposons que k possède n racines $n^{\text{ièmes}}$ de l'unité distinctes, et notons $B(k)$ le groupe de Brauer de k et $B(k)_n$ son sous-groupe formé des éléments d'ordre divisant n. Alors, en choisissant une racine primitive $n^{\text{ième}}$ de 1 dans k, on définit le symbole de Hilbert $\{x, y\}_n$ (*cf.* A. Weil [33], p. 185); c'est une application bilinéaire de $k^{\times} \times k^{\times}$ dans $B(k)_n$, qui vérifie $\{x, 1-x\}_n = 1$ pour $x \in k^{\times}$, $x \neq 1$. Le symbole $\{x, y\}_n$ satisfait donc aux équations d'un cocycle de Steinberg bilinéaire. Pour que $\{x, y\}_n$ vérifie la condition topologique (S 0), $B(k)_n$ étant un groupe discret, il suffit, par exemple, que l'ensemble $(k^{\times})^n$ formé des x^n $(x \in k^{\times})$ soit un ouvert de $k^{\times}$.

Un autre exemple de cocycle de Steinberg, non bilinéaire celui-là, vient de la théorie des corps ordonnés (*cf.* N. Bourbaki [7]). Soit k un corps ordonné, archimédien ou non. Définissons comme suit une application c de $k^\times \times k^\times$ dans $\mathbf{Z}$: $c(x, y) = 1$ si $x < 0$, $y < 0$; $c(x, y) = 0$ sinon. On voit que c est un cocycle de Steinberg sur $k^\times$ pour la topologie de k définie à partir de l'ordre total sur k. On en déduit, par passage au quotient, un cocycle de Steinberg bilinéaire c^0 sur $k^\times$ à valeurs dans $\mathbf{Z}/2\mathbf{Z}$. En fait, c^0 provient d'un symbole de Hilbert. Soient, en effet, $\bar{k}$ une clôture algébrique de k et k_1 un sur-corps ordonné de k maximal contenu dans $\bar{k}$; on a alors $\bar{k} = k_1(\sqrt{-1})$, et le groupe de Brauer $B(k_1)$ de k_1 est d'ordre 2. De plus, k_1 possède exactement deux racines de 1, et l'on a un symbole de Hilbert $\{x, y\}_{k_1}$ sur $k_1^\times$ à valeurs dans $B(k_1)$. Le cocycle c^0 n'est autre que la restriction de $\{x, y\}_{k_1}$ à $k^\times \times k^\times$, $B(k_1)$ étant identifié avec $\mathbf{Z}/2\mathbf{Z}$.

On va expliciter ce que donnent ces exemples dans le cas d'un corps localement compact non discret.

Si $k = \mathbf{R}$, le groupe G_k est un groupe de Lie connexe. Puisque k est un corps ordonné, G_k possède une extension centrale E par $\mathbf{Z}$ [resp. $\mathbf{Z}/2\mathbf{Z}$] si G est de type symplectique [resp. non symplectique]. Le groupe E est localement isomorphe à G_k et est engendré par des sous-groupes à un paramètre. Par suite, E est un groupe de Lie connexe. On sait que E est le revêtement universel du groupe de Lie connexe G_k (É. Cartan [11]).

Soit k un corps local ultramétrique. Les racines de 1 dans k forment un groupe cyclique fini μ_k, disons, d'ordre m; l'ensemble $(k^\times)^m$ est alors un ouvert de $k^\times$. D'après la théorie locale du corps de classes ([1], [27], [33]), le groupe $B(k)_m$ est cyclique d'ordre m, et l'on peut remplacer le symbole de Hilbert $\{x, y\}_m$ par le symbole de restes normiques $(x, y)_{m,k}$, qui est une application bilinéaire de $k^\times \times k^\times$ dans μ_k canoniquement définie (*voir* n° 11). On sait également que $(x, y)_{m,k}$ a pour image μ_k tout entier. Nous avons donc le cocycle canonique $(x, y)_{m,k}$ sur $k^\times$ à valeurs dans μ_k, et, par le théorème 8.2, une extension centrale E_0 de G_k par μ_k. Le groupe E_0 est localement isomorphe à G_k, et est égal à son propre groupe des commutateurs; on pourrait donc dire que E_0 est un revêtement de G_k à m feuillets. Soient n un diviseur de m et $\mu_{k,n}$ le sous-groupe de μ_k formé des éléments d'ordre divisant n. Alors, on a, par passage à la puissance, le cocycle $(x, y)_{n,k} = (x, y)_{m,k}^{m/n}$ sur $k^\times$ à valeurs dans $\mu_{k,n}$, et donc une extension centrale de G_k par $\mu_{k,n}$.

A. Weil [32] a remarqué l'existence de tels revêtements pour les groupes symplectiques et $n = 2$. L'existence du revêtement E_0 a été prouvée, pour $G = SL_2$, indépendamment par T. Kubota [19] et C. Moore [26], et ce dernier l'a conjecturée dans le cas général. H. Bass, J. Milnor et J.-P. Serre [4] ont démontré cette conjecture pour les groupes SL_n et Sp_{2n} en caractéristique 0.

CHAPITRE III.

Rappel de résultats de C. Moore et conclusion.

10. Dans ce numéro, nous exposons, suivant C. Moore ([25], [26]), des généralités sur les extensions centrales des groupes localement compacts. Tous les énoncés de ce numéro sont essentiellement démontrés dans les deux mémoires.

Dans ce qui suit, nous supposerons que les groupes localement compacts qui interviennent sont tous *séparables*, c'est-à-dire qu'ils ont une base dénombrable d'ouverts.

Soient G un groupe localement compact et A un G-module localement compact. C. Moore [25] a défini les groupes de cohomologie $H^n(G, A)$ ($n \geq 0$) au sens topologique, qui ont une interprétation habituelle en basses dimensions. Nous nous intéressons exclusivement au cas où G opère sur A trivialement. Dans ce cas-là, $H^1(G, A)$ est le groupe des morphismes de G dans A, et $H^2(G, A)$ est le groupe que forment avec la multiplication de Baer les classes d'extensions centrales de G par A. On entend par extension centrale de G par A la donnée d'une suite exacte de groupes localement compacts

$$1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1,$$

où i est un isomorphisme de A sur un sous-groupe central de E et où p induit un isomorphisme de $E/i(A)$ sur G.

On dit qu'un groupe localement compact G est *simplement connexe* si G vérifie la condition suivante : pour toute extension centrale E de G à noyau localement compact, il existe un morphisme φ et un seul de G dans E tel que $p \circ \varphi = \mathrm{id}_G$, où p est la projection de E sur G et id_G l'application identique de G.

On a alors le critère suivant (*cf.* [26]) :

Lemme 10.1. — *Un groupe localement compact* G *est simplement connexe si et seulement si l'on a* $H^1(G, \mathbf{T}) = H^2(G, \mathbf{T}) = \{0\}$, *où* $\mathbf{T}$ *est le groupe multiplicatif des nombres complexes de module* 1.

Supposons que le groupe $[G, G]$ des commutateurs de G soit dense dans G, autrement dit que $H^1(G, \mathbf{T}) = \{0\}$. On dira qu'une extension centrale E de G est un revêtement de G, si le groupe des commutateurs de E est dense dans E. Un revêtement E de G sera dit *universel* si le groupe E est simplement connexe. Le groupe G possède, à un isomorphisme d'extensions près, au plus un revêtement universel. Le noyau d'un revêtement universel de G sera appelé le *groupe fondamental* de G et sera noté $\pi_1(G)$.

Le lemme suivant donne une propriété fondamentale du revêtement universel [26] :

LEMME 10.2. — *Supposons que* G *possède un revêtement universel* E_0 :

$$1 \to \pi_1(G) \to E_0 \xrightarrow{\pi} G \to 1.$$

Alors :

(*a*) *Pour toute extension centrale* E *de* G, *il existe un morphisme* φ *et un seul de* E_0 *dans* E *tel que* $\pi = p \circ \varphi$, *où* p *est la projection de* E *sur* G.

(*b*) *Si* A *est un groupe abélien localement compact*, $H^2(G, A)$ *est isomorphe au groupe* $\mathrm{Hom}(\pi_1(G), A)$ *des morphismes de* $\pi_1(G)$ *dans* A.

En particulier, si G possède un revêtement universel, le groupe $H^2(G, \mathbf{T})$ peut être muni d'une topologie de sorte qu'il soit le dual de $\pi_1(G)$.

Soit j un morphisme d'un groupe localement compact H dans un autre G. Alors, à toute extension centrale E de G par A, on associe, suivant j, une extension centrale $j^*(E)$ de H par A; on obtient ainsi un morphisme j^* de $H^2(G, A)$ dans $H^2(H, A)$. L'extension $j^*(E)$ de H est triviale si et seulement s'il existe un morphisme φ^* de H dans E tel que $j = p \circ \varphi^*$, où p est la projection de E sur G.

Rappelons quelques résultats sur l'existence de revêtements universels pour certains groupes localement compacts [26].

Si G est un groupe discret tel que $G = [G, G]$, il existe un revêtement universel de G, qui est lui-même un groupe discret.

Pour qu'un groupe de Lie connexe G soit simplement connexe à notre sens, il faut et il suffit que G soit simplement connexe en tant que variété différentiable et que les groupes de cohomologie $H^1(\mathfrak{g}, \mathbf{R})$ et $H^2(\mathfrak{g}, \mathbf{R})$ s'annulent, où $\mathfrak{g}$ est l'algèbre de Lie de G et $\mathbf{R}$ le $\mathfrak{g}$-module trivial. Un groupe de Lie connexe G possède un revêtement universel E si et seulement si G est égal à son groupe des commutateurs, c'est-à-dire que $\mathfrak{g}$ est égale à son algèbre dérivée. S'il en est ainsi, E est lui-même un groupe de Lie connexe et $\pi_1(G)$ est la somme directe du groupe fondamental de la variété sous-jacente à G et du dual de $H^2(\mathfrak{g}, \mathbf{R})$.

Soit K un groupe compact. D'abord, si K est un groupe de Lie, $H^2(K, \mathbf{T})$ est un groupe fini. Si K est une limite projective de groupes de Lie compacts K_α, α décrivant un ensemble filtrant dénombrable, alors $H^2(K, \mathbf{T})$ est isomorphe à la limite inductive des groupes $H^2(K_\alpha, \mathbf{T})$. Supposons que $[K, K]$ soit dense dans K. Alors, K possède un revêtement universel, qui est lui-même compact; $\pi_1(K)$ est un groupe profini, étant le dual de $H^2(K, \mathbf{T})$.

Soit maintenant j un morphisme injectif d'un groupe localement compact H dans un autre G, et supposons que $[G, G]$ soit dense dans G. Une extension centrale E de G est dite triviale au-dessus de H, si $j^*(E)$

est triviale. Un revêtement E_0 de G sera appelé *revêtement universel relatif* de G par rapport à H, si E_0 satisfait à la condition suivante : l'extension E_0 est triviale au-dessus de H et, pour toute extension centrale E triviale au-dessus de H, il existe un morphisme φ de E_0 dans E tel que $p \circ \varphi = \pi$, où π [resp. p] est la projection de E_0 [resp. de E] sur G. Il existe, à un isomorphisme d'extensions près, au plus un tel revêtement de G. Le noyau de l'extension E_0 sera appelé le *groupe fondamental relatif* de G par rapport à H et sera noté $\pi_1(G, H)$. Alors, si A est un groupe abélien localement compact, le noyau du morphisme de restriction j^* de $H^2(G, A)$ dans $H^2(H, A)$ est isomorphe à Hom $(\pi_1(G, H), A)$.

Soit j un morphisme injectif de H dans G, et supposons que G et H possèdent des revêtements universels E et F respectivement. Il existe alors un morphisme j_* de F dans E tel que $\pi \circ j_* = j \circ \pi'$, où π [resp. π'] est la projection de E [resp. de F] sur G [resp. H]. Le morphisme j_* applique $\pi_1(H)$ dans $\pi_1(G)$; c'est le dual du morphisme j^* de $H^2(G, \mathbf{T})$ dans $H^2(H, \mathbf{T})$. Soit $\overline{j_*(\pi_2(H))}$ l'adhérence de $j_*(\pi_1(H))$ dans $\pi_1(G)$; on obtient, par passage au quotient, une extension $E/\overline{j_*(\pi_1(H))}$ de G par $\pi_1(G)/\overline{j_*(\pi_1(H))}$. Cette extension est un revêtement universel relatif de G par rapport à H [26]. On a ainsi le lemme suivant :

LEMME 10.3. — *Soit j un morphisme injectif de* H *dans* G, *et supposons que* G *et* H *possèdent des revêtements universels. Alors, il existe un revêtement universel relatif de* G *par rapport à* H, *et* $\pi_1(G, H)$ *est isomorphe au quotient de* $\pi_1(G)$ *par* $\overline{j_*(\pi_1(H))}$.

Ajoutons que $\pi_1(G, H)$ est un groupe discret si H est en outre un sous-groupe ouvert compact de G.

Traitons finalement le passage au produit restreint. Soit $\{G_\alpha\}$ une famille de groupes localement compacts, α parcourant un ensemble dénombrable d'indices; soit K_α un sous-groupe ouvert compact de G_α défini pour presque tout α. Notons G le produit restreint des groupes G_α relatif aux K_α.

Supposons que G_α possède un revêtement universel E_α pour tout α et que $[K_\alpha, K_\alpha]$ soit dense dans K_α pour presque tout α. Lorsque cette dernière hypothèse a lieu pour α, soient L_α un revêtement universel de K_α, et j_*^α le morphisme de L_α dans E_α relevé du plongement j^α de K_α dans G_α. L'image par j_*^α de L_α [resp. de $\pi_1(K_\alpha)$] est ouverte et compacte dans E_α [resp. $\pi_1(G_\alpha)$], et $j_*^\alpha(L_\alpha)$ est égal à l'adhérence de $[p_\alpha^{-1}(K_\alpha), p_\alpha^{-1}(K_\alpha)]$ dans E_α, p_α étant la projection de E_α sur G_α. On a alors le résultat suivant [26] :

LEMME 10.4. — *Le produit restreint des groupes* E_α *relatif aux* $j_*^\alpha(L_\alpha)$ *est un revêtement universel de* G. *Le groupe fondamental* $\pi_1(G)$ *de* G *est le produit restreint des groupes* $\pi_1(G_\alpha)$ *relatif aux* $j_*^\alpha(\pi_1(K_\alpha))$.

11. On rappellera dans ce numéro les résultats arithmétiques de C. Moore [26] sur la détermination des cocycles de Steinberg pour un corps local et sur l'unicité des formules de réciprocité dans un corps global.

Soit k un corps localement compact non discret. On va tout d'abord rappeler la définition du symbole de restes normiques (Artin-Tate [1], Serre [27], Weil [33]). Soient $\bar{k}$ une clôture algébrique de k, k_{ab} l'extension abélienne maximale de k contenue dans $\bar{k}$ et $\mathfrak{A}$ le groupe de Galois de l'extension k_{ab} de k. Soit α_k le morphisme canonique de $k^\times$ dans $\mathfrak{A}$. Alors, si k contient n racines $n^{\text{ièmes}}$ de l'unité distinctes, le symbole de Hilbert $(x, y)_{n,k}$ est défini comme suit :

$$\text{pour tout } x, y \in k^\times, \quad (x, y)_{n,k} = \xi^{-1}\xi^{\alpha_k(y)}$$

où ξ est une racine $n^{\text{ième}}$ de x. C'est une application bilinéaire de $k^\times \times k^\times$ dans le groupe μ_k des racines de 1 contenues dans k, et l'on a $(x, 1-x)_{n,k} = 1$ pour tout $x \in k^\times$, $x \neq 1$.

Puisque $(k^\times)^n$ est ouvert dans $k^\times$, le symbole de Hilbert $(x, y)_{n,k}$ est une application localement constante et est un cocycle de Steinberg sur $k^\times$ à valeurs dans μ_k. Notons $S(k^\times, \mu_k)$ le groupe des cocycles de Steinberg sur $k^\times$ à valeurs dans μ_k, et $H(k^\times, \mu_k)$ son sous-groupe engendré par les symboles de Hilbert. Si $k = \mathbf{C}$, $H(k^\times, \mu_k)$ est trivial. Si k est le corps $\mathbf{R}$ ou un corps ultramétrique, μ_k est cyclique d'ordre fini m; le groupe $H(k^\times, \mu_k)$ est lui aussi d'ordre m et est engendré par le symbole $(x, y)_{m,k}$.

Posons, dans ce dernier cas, $c^0(x, y) = (x, y)_{m,k}$. Pour $k = \mathbf{R}$, définissons comme suit un cocycle de Steinberg c_0 sur $k^\times$ à valeurs dans $\mathbf{Z}$: $c_0(x, y) = 1$ si $x < 0$, $y < 0$; $c_0(x, y) = 0$ sinon.

Ceci étant, le théorème suivant, dû à C. Moore [26], permet de déterminer les cocycles de Steinberg sur $k^\times$ à valeurs dans un groupe abélien localement compact, séparable ou non.

THÉORÈME 11.1. — *Soient k un corps local et* A *un groupe abélien localement compact. Notons* $S(k^\times, A)$ [*resp.* $S^0(k^\times, A)$] *le groupe des cocycles de Steinberg* [*resp. de Steinberg bilinéaires*] *sur $k^\times$ à valeurs dans* A.

(*a*) *Si* $k = \mathbf{C}$, $S(k^\times, A) = \{1\}$.

(*b*) *Si* $k = \mathbf{R}$, *l'application* $\lambda \mapsto \lambda \circ c_0$ [*resp.* $\lambda \mapsto \lambda \circ c^0$] *est un isomorphisme de* $\mathrm{Hom}(\mathbf{Z}, A)$ [*resp. de* $\mathrm{Hom}(\mu_k, A)$] *sur* $S(k^\times, A)$ [*resp.* $S^0(k^\times, A)$].

(*c*) *Si k est ultramétrique, l'application* $\lambda \mapsto \lambda \circ c^0$ *est un isomorphisme de* $\mathrm{Hom}(\mu_k, A)$ *sur* $S(k^\times, A)$. *Tout élément de* $S(k^\times, A)$ *est bilinéaire.*

En fait, Moore montre, sans supposer la continuité de $c(x, 1-xy)$ en $(x, y) = (0, 0)$, que l'on obtient ainsi toutes les applications continues de $k^\times \times k^\times$ dans A satisfaisant aux équations (S 1), (S 2) et (S 3) du n° 5.

En ce qui concerne la démonstration, bornons-nous aux indications suivantes. Le résultat général se déduit facilement du cas particulier où $A = \mathbf{T}$. Considérons alors deux applications $c \mapsto h(c)$ et $c \mapsto c^{\natural}$ de $S(k^{\times}, \mathbf{T})$ respectivement dans $H^2(k^{\times}, \mathbf{T})$ et $S^0(k^{\times}, \mathbf{T})$: $h(c)$ est la classe de cohomologie de c et $c^{\natural}$ est défini par $c^{\natural}(x, y) = c(x, y^2)$. Ces deux homomorphismes ont pour noyau commun le sous-groupe $S_0(k^{\times}, \mathbf{T})$ formé des éléments c tels que $c(x, y^2) = 1$ pour tout $x, y \in k^{\times}$. Le groupe $H^2(k^{\times}, \mathbf{T})$ est trivial pour $k = \mathbf{C}$ ou $\mathbf{R}$, et est un groupe de torsion pour k ultramétrique. Cela entraîne aussitôt le théorème pour $\mathbf{C}$ et $\mathbf{R}$. Dans le cas ultramétrique, on voit de là que $S(k^{\times}, \mathbf{T})/S_0(k^{\times}, \mathbf{T})$ est un groupe de torsion. On doit alors déterminer $S_0(k^{\times}, \mathbf{T})$, $S^0(k^{\times}, \mathbf{T})$ et l'image du morphisme $c \mapsto c^{\natural}$. Ceci se fait à l'aide de résultats essentiels de la théorie locale du corps de classes (*voir* C. Moore [26]).

Rappelons aussi le cas des corps finis, dû à R. Steinberg [30] :

LEMME 11.2. — *Soit $\mathbf{F}_q$ un corps fini à q éléments. Si q est impair, $\mathbf{F}_q$ possède un élément x tel que ni x ni $1 - x$ ne soit carré dans $\mathbf{F}_q^{\times}$. Tout cocycle de Steinberg sur $\mathbf{F}_q^{\times}$ est trivial.*

On va maintenant envisager le cas adélique. Soit k une extension de $\mathbf{Q}$ de degré fini ou un corps de fonctions algébriques de dimension 1 sur un corps fini. On notera μ_k le groupe des racines de l'unité contenues dans k. Pour chaque place v de k, on note k_v le complété de k pour v, et μ_v le groupe des racines de 1 contenues dans k_v. Si v est non archimédienne, $\mathfrak{o}_v$ désigne le sous-anneau compact maximal de k_v et $\mathfrak{o}_v^{\times}$ le groupe multiplicatif des éléments inversibles de $\mathfrak{o}_v$.

Soit $A_k^{\times}$ le groupe des idèles de k, c'est-à-dire le produit restreint des groupes $k_v^{\times}$ relatif aux $\mathfrak{o}_v^{\times}$, v parcourant l'ensemble des places de k. Le groupe $k^{\times}$ est canoniquement un sous-groupe discret de $A_k^{\times}$. Il est bien connu (et d'ailleurs résulte tout de suite du lemme 11.2) qu'un symbole de Hilbert $(x, y)_{n_v, k_v}$ d'un corps ultramétrique k_v est trivial sur $\mathfrak{o}_v^{\times} \times \mathfrak{o}_v^{\times}$ si n_v est premier avec la caractéristique résiduelle p_v de k_v. On sait aussi que l'ordre de μ_v est premier avec p_v pour presque toute place v. Par suite, si k contient n racines $n^{\text{ièmes}}$ de 1 distinctes, on peut définir sur $A_k^{\times} \times A_k^{\times}$ le produit $(x, y)_n$ des symboles locaux $(x_v, y_v)_{n, k_v}$: $(x, y)_n = \prod_v (x_v, y_v)_{n, k_v}$ pour $x = (x_v)$, $y = (y_v)$ dans $A_k^{\times}$. C'est un cocycle, localement constant, sur $A_k^{\times}$ à valeurs dans μ_k. La loi de réciprocité affirme alors que $(x, y)_n = 1$ pour tout x, y dans $k^{\times}$.

Désignons par $S(A_k^{\times}, \mathbf{T})$ [resp. $S^0(A_k^{\times}, \mathbf{T})$] le produit des groupes $S(k_v^{\times}, \mathbf{T})$ [resp. $S^0(k_v^{\times}, \mathbf{T})$]. Chaque élément $c = (c_v)$ de $S(A_k^{\times}, \mathbf{T})$ définit un cocycle, localement constant, sur $A_k^{\times}$ à valeurs dans $\mathbf{T}$. On identifie donc $S(A_k^{\times}, \mathbf{T})$ au groupe de cocycles sur $A_k^{\times}$. Au plongement canonique j de $k^{\times}$ dans $A_k^{\times}$, on associe un morphisme de restriction $j^\star$ de $S(A_k^\times, \mathbf{T})$ dans $S(k^\times, \mathbf{T})$, où k est regardé, bien entendu, comme un corps discret. En vertu de la formule de réciprocité $(x, y)_m = 1$ $(x, y \in k^\times)$, où m est l'ordre de μ_k, on voit que le noyau de $j^\star$ contient un sous-groupe d'ordre m, dual de μ_k.

Réciproquement, C. Moore [26] a démontré le résultat suivant :

Théorème 11.3. — *Le noyau du morphisme de restriction* $j^\star$ *de* $S(A_k^\times, \mathbf{T})$ *dans* $S(k^\times, \mathbf{T})$ *est isomorphe au dual du groupe* μ_k *des racines de l'unité contenues dans* k.

Ceci constitue, dans la théorie du corps de classes, un théorème d'unicité pour les formules de réciprocité dans k.

Soient maintenant S un ensemble fini de places de k, et $A_k^\times(S)$ le groupe des S-idèles de k, c'est-à-dire le produit restreint des groupes $k_v^\times$ pour les places $v \notin S$. Notons $S(A_k^\times(S), \mathbf{T})$ le produit des groupes $S(k_v^\times, \mathbf{T})$ pour les places $v \notin S$. Le morphisme de restriction de $S(A_k^\times(S), \mathbf{T})$ dans $S(k_k^\times, \mathbf{T})$, associé au plongement canonique de $k^\times$ dans $A_k^\times(S)$, n'est autre que la restriction à $S(A_k^\times(S), \mathbf{T})$ du morphisme $j^\star$ de $S(A_k^\times, \mathbf{T})$ dans $S(k^\times, \mathbf{T})$. On a donc le corollaire suivant :

Corollaire 11.4. — *Le noyau du morphisme de restriction de* $S(A_k^\times(S), \mathbf{T})$ *dans* $S(k^\times, \mathbf{T})$ *est isomorphe au dual de* μ_k *si* S *consiste entièrement en places imaginaires. Sinon, il se réduit à l'élément neutre.*

12. Ce numéro est consacré à nos théorèmes principaux pour les groupes simples G simplement connexes déployés. Il s'agit de réunir les résultats des numéros précédents, pour en arriver à une solution au problème des groupes de congruence pour G de rang $\geqq 2$.

Nous reprenons les notations des chapitres I et II, relatives au schéma de Chevalley-Demazure $\mathfrak{G}$ associé à un groupe simple simplement connexe G; en particulier, le tore H, le système de racines Φ, les sous-groupes radiciels U^α, le système de racines simples Δ.

Les théorèmes 8.2 et 11.1 entraînent le résultat suivant sur les revêtements universels des groupes G_k sur un corps local k :

Théorème 12.1. — *Soient* k *un corps local et* G_k *le groupe des points rationnels d'un groupe simple simplement connexe déployé sur* k. *Le groupe localement compact* G_k *possède un revêtement universel* E_0.

(*a*) *Si* $k = \mathbf{C}$, *le groupe* G_k *est lui-même simplement connexe.*

(*b*) *Si* $k = \mathbf{R}$, *le groupe fondamental* $\pi_1(G_k)$ *de* G_k *est isomorphe à* $\mathbf{Z}$ [*resp. à* $\{\pm 1\}$] *lorsque* G *est de type symplectique* [*resp. non symplectique*].

(*c*) *Si* k *est ultramétrique,* $\pi_1(G_k)$ *est isomorphe au groupe* μ_k *des racines de l'unité contenues dans* k.

En effet, le cas de $\mathbf{C}$ est conséquence immédiate des théorèmes 8.2 et 11.1. Démontrons l'énoncé du cas ultramétrique; le cas de $\mathbf{R}$ est analogue et d'ailleurs bien connu. Prenons le symbole de restes normiques $(x, y)_{m,k}$, m étant l'ordre de μ_k; c'est le cocycle de Steinberg canonique c^0 utilisé dans le théorème 11.1. Soit E_0 l'extension centrale de G_k par μ_k correspondant à c^0 par le théorème 8.2 : $1 \to \mu_k \to E_0 \xrightarrow{\pi} G_k \to 1$. Le groupe E_0 est égal à son groupe des commutateurs. Soit E une extension centrale de E_0 par un groupe localement compact A : $1 \to A \to E \xrightarrow{p} E_0 \to 1$. Il s'agit alors de vérifier que cette extension est triviale. Regardons E comme extension de G_k par $B = p^{-1}(\mu_k)$; on voit aisément que B est central dans E. Soit donc c_E le cocycle de Steinberg appartenant à l'extension E de G_k. D'une part, on a évidemment $c^0 = p \circ c_E$; d'autre part, d'après le théorème 11.1, il existe un morphisme λ de μ_k dans B tel que $c_E = \lambda \circ c^0$. On a donc $p \circ \lambda = \mathrm{id}_{\mu_k}$, et B est le produit de $\lambda(\mu_k)$ par A. Par suite, d'après le n° 8, les éléments $\tilde{x}_\alpha(u)$ de E engendrent un sous-groupe E′ tel que $E' \cap B = \lambda(\mu_k)$, et p induit un isomorphisme de E′ sur E_0. L'extension E de E_0 est donc triviale. Le théorème est ainsi démontré.

Examinons encore le cas ultramétrique. Soit $\mathfrak{o}$ le sous-anneau compact maximal du corps ultramétrique k. Alors $G_{\mathfrak{o}}$ est un sous-groupe ouvert compact de G_k, et est engendré par les sous-groupes radiciels $U_{\mathfrak{o}}^{\alpha}$: par le lemme 5.2, (*c*), $G_{\mathfrak{o}}$ est donc son propre groupe des commutateurs si le corps résiduel de k possède au moins quatre éléments. Considérons dans le revêtement universel E_0 de G_k le sous-groupe F_0 engendré par les éléments $\tilde{x}_\alpha(u)$ $(\alpha \in \Phi,\ u \in \mathfrak{o})$. En utilisant la décomposition de Bruhat de $G_{\mathfrak{o}}$ ([17], [10]) et le lemme 5.9, on voit sans difficulté que F_0 est un sous-groupe ouvert compact de E_0, qui est une extension centrale de $G_{\mathfrak{o}}$ par le p-groupe de Sylow de μ_k, où p est la caractéristique résiduelle de k. En particulier, l'extension E_0 est triviale au-dessus de $G_{\mathfrak{o}}$ si l'ordre de μ_k est premier avec p.

Soient maintenant k un corps global et A_k l'anneau des adèles de k. Le groupe adélifié G_{A_k} est le produit restreint des groupes G_{k_v} relatif aux $G_{\mathfrak{o}_v}$, où $G_{\mathfrak{o}_v}$ est défini pour toute place non archimédienne. Pour chaque v, soit E_v le revêtement universel de G_{k_v} défini à partir du cocycle canonique c^0 ou c_0 de k_v. Si v est non archimédienne, F_v désigne le sous-groupe de E_v engendré par les éléments $\tilde{x}_\alpha(u)$ $(\alpha \in \Phi,\ u \in \mathfrak{o}_v)$. D'après ce qui précède, pour presque tout v, $G_{\mathfrak{o}_v}$ est égal à son groupe des commutateurs et F_v est isomorphe à $G_{\mathfrak{o}_v}$.

Le théorème suivant est donc conséquence du lemme 10.4 :

THÉORÈME 12.2. — *Le groupe adélifié* G_{A_k} *possède un revêtement universel. Le groupe fondamental* $\pi_1(G_{A_k})$ *de* G_{A_k} *est isomorphe à la somme directe des groupes* $\pi_1(G_{k_v})$.

On voit maintenant que le groupe compact $S(A_k^\times, \mathbf{T})$ ou $S^0(A_k^\times, \mathbf{T})$, défini dans le numéro précédent, est justement le dual de $\pi_1(G_{A_k})$.

On va ensuite considérer le plongement j de G_k dans G_{A_k}. Soit E_k [resp. E_{A_k}] le revêtement universel de G_k [resp. de G_{A_k}], et notons j_* le morphisme, relevé de j, de E_k dans E_{A_k}. D'après le lemme 10.3, il existe un revêtement universel relatif de G_{A_k} par rapport à G_k, et $\pi_1(G_{A_k}, G_k)$ est isomorphe à $\pi_1(G_{A_k})/j_*(\pi_1(G_k))$. Or, on vérifie aisément que le morphisme j_* de $\pi_1(G_k)$ dans $\pi_1(G_{A_k})$ a pour dual le morphisme j^*, défini au n° 11, de $S(A_k^\times, \mathbf{T})$ [resp. de $S^0(A_k^\times, \mathbf{T})$] dans $S(k^\times, \mathbf{T})$ [resp. $S^0(k^\times, \mathbf{T})$]. Le théorème 11.3 affirme alors que $\pi_1(G_{A_k}, G_k)$ est isomorphe à μ_k. On a ainsi le théorème suivant :

THÉORÈME 12.3. — *Il existe un revêtement universel relatif $\tilde{G}_{A_k}$ de G_{A_k} par rapport à G_k. Le groupe fondamental relatif $\pi_1(G_{A_k}, G_k)$ est isomorphe au groupe μ_k des racines de l'unité contenues dans k.*

On peut, par ailleurs, construire $\tilde{G}_{A_k}$ directement à partir du cocycle canonique $c = (c_v)$, sur $A_k^\times$ à valeurs dans μ_k, donné par $c_v(x, y) = (x, y)_{m, k_v}$ pour tout v, où m est l'ordre de μ_k.

Soient maintenant S un ensemble fini de places de k, et $A_k(S)$ l'anneau des S-adèles de k. Pour le groupe adélifié $G_{A_k(S)}$ et le plongement canonique de G_k dans $G_{A_k(S)}$, on a un résultat analogue aux deux théorèmes précédents. Notamment, le corollaire 11.4 entraîne le théorème suivant :

THÉORÈME 12.4. — *Il existe un revêtement universel relatif $\tilde{G}_{A_k(S)}$ de $G_{A_k(S)}$ par rapport à G_k. Le groupe fondamental relatif $\pi_1(G_{A_k(S)}, G_k)$ est isomorphe à μ_k si S consiste entièrement en places imaginaires; sinon, il se réduit à l'élément neutre.*

Nous sommes à présent en état de répondre au problème des groupes de congruence pour G de rang $\geqq 2$.

Soient S un ensemble fini non vide de places de k contenant toutes les places archimédiennes, et $\mathfrak{o}$ l'anneau de Dedekind de type arithmétique défini à partir de S. Rappelons la suite exacte étudiée dans le n° 3 :

$$1 \to C^S(G_k) \to \widehat{G_k(S)} \xrightarrow{\pi} G_{A_k(S)} \to 1.$$

Le théorème précédent et le théorème 3.3 permettent de déterminer le noyau $C^S(G_k)$.

THÉORÈME 12.5. — *Supposons que G soit de rang $\geqq 2$. Alors, le groupe $\widehat{G_k(S)}$ constitue un revêtement universel relatif de $G_{A_k(S)}$ par rapport à G_k. Le noyau $C^S(G_k)$ est isomorphe au groupe μ_k des racines de l'unité contenues dans k si S consiste entièrement en places imaginaires. Sinon, $C^S(G_k)$ se réduit à l'élément neutre.*

En effet, d'après les deux théorèmes cités, il existe un morphisme φ de $\widehat{G_k(S)}$ dans $\tilde{G}_{A_k(S)}$ et un autre ψ de $\tilde{G}_{A_k(S)}$ dans $\widehat{G_k(S)}$ tels que $\pi = \pi' \circ \varphi$ et $\pi' = \pi \circ \psi$, où π' est la projection de $\tilde{G}_{A_k(S)}$ sur $G_{A_k(S)}$. On en déduit que ψ est l'inverse de φ et donc que les deux revêtements de $G_{A_k(S)}$ sont isomorphes.

Corollaire 12.6. — *Supposons que* G *soit de rang* $\geqq 2$. *Si* S *contient au moins une place non imaginaire de* k, *tout sous-groupe* S-*arithmétique de* G_k *est un sous-groupe de* S-*congruence.*

Dans le n° 3, nous avons utilisé les sous-groupes $\Gamma_{\mathfrak{q}}$ et $E_{\mathfrak{q}}$ de $G_{\mathfrak{o}}$ définis pour tout idéal $\mathfrak{q}$ de $\mathfrak{o}$. On rappelle que $C^S(G_k)$ est la limite projective, sur les idéaux $\mathfrak{q}$ non nuls, des complétés-séparés $\hat{C}_{\mathfrak{q}}$ des groupes $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$. Le théorème 12.5 entraîne donc que les $\hat{C}_{\mathfrak{q}}$ sont des groupes cycliques finis. En fait, pour $G = SL_3$ ou Sp_4, Bass, Milnor et Serre [4] ont montré que les $\Gamma_{\mathfrak{q}}/E_{\mathfrak{q}}$ sont eux-mêmes des groupes finis et notamment que $G_{\mathfrak{o}}$ est égal à $E_{\mathfrak{o}}$. Par le corollaire 4.6, il en est alors de même généralement pour G de rang $\geqq 2$. On a ainsi le théorème suivant :

Théorème 12.7. — *Supposons que* G *soit de rang* $\geqq 2$. *Alors, le groupe* $G_{\mathfrak{o}}$ *est engendré par les sous-groupes radiciels* $U_{\mathfrak{o}}^{\alpha}$, *et tout sous-groupe* S-*arithmétique de* G_k *possède un sous-groupe d'indice fini engendré par des éléments unipotents.*

Pour $G = SL_2$ et un anneau de Dedekind $\mathfrak{o}$ de type arithmétique, J.-P. Serre [29] a montré que la conclusion du théorème 12.5 reste valable si S consiste en au moins deux places de k (*voir* aussi J. Mennicke [24]). En revanche, $C^S(SL_2(k))$ est un groupe infini si $\mathfrak{o}$ est l'anneau des entiers de $\mathbf{Q}$ ou d'un corps quadratique imaginaire; le premier cas est dû à F. Klein, et le second à Serre [29].

13. Il serait d'intérêt de généraliser des résultats de ce mémoire aux groupes semi-simples G simplement connexes non déployés. Il s'agit essentiellement d'un problème local relatif à $\pi_1(G_{k_v})$, d'un problème adélique relatif à $\pi_1(G_{A_k}, G_k)$ et du problème des groupes de congruence pour G_k, où k_v est un corps local et k un corps global.

Le seul résultat systématique que nous connaissions dans cette direction est celui d'É. Cartan sur les revêtements universels des groupes semi-simples réels.

Soit G un groupe semi-simple simplement connexe défini sur $\mathbf{R}$ et $\mathbf{R}$-simple. Les théorèmes suivants sont dus à É. Cartan [11] :

a. Le groupe $G_{\mathbf{R}}$ *est topologiquement connexe;*

b. Le groupe fondamental $\pi_1(G_{\mathbf{R}})$ *de* $G_{\mathbf{R}}$ *est isomorphe à* $\{0\}$, $\mathbf{Z}/2\mathbf{Z}$ *ou* $\mathbf{Z}$.

On connaît de ces théorèmes plusieurs démonstrations d'un point de vue « compact ». En fait, la méthode de ce mémoire, appuyée sur la théorie relative des groupes algébriques [6], permet de retrouver ces résultats d'un point de vue « anticompact » et sans faire de vérification cas par cas. On y trouve aussi le critère suivant pour l'ordre de $\pi_1(G_{\mathbf{R}})$:

c. Soient H^d *un tore de* G *déployé sur* $\mathbf{R}$ *maximal et* H^c *un tore de* G *compact sur* $\mathbf{R}$ *tels que* $H = H^d H^c$ *soit un tore maximal de* G. *Alors,* $\pi_1(G_{\mathbf{R}})$ *est trivial si et seulement si aucune racine longue de* G *relative à* H *ne s'annule sur* H^c. *Supposons que certaines racines longues de* G *s'annulent sur* H^c. *Alors, pour que* $\pi_1(G_{\mathbf{R}})$ *soit infini, il faut et il suffit que deux telles racines, non opposées, soient nécessairement orthogonales, autrement dit que* G *soit sur* $\mathbf{R}$ *de type* C_n *ou* $BC_n (n \geqq 1)$.

Le problème local est ainsi complètement résolu dans le cas réel.

Dans le cas d'un corps local ultramétrique k, il est naturel de conjecturer que, si G est un groupe simple simplement connexe de rang relatif $\geqq 1$ sur k, le groupe G_k possède un revêtement universel avec le groupe fondamental $\pi_1(G_k)$ fini.

BIBLIOGRAPHIE.

[1] E. Artin et J. Tate, *Class field theory*, Benjamin, New-York, 1968.

[2] H. Bass, *K-theory and stable algebra* (*Publ. Math. I. H. E. S.*, nº 22, 1964, p. 5-60).

[3] H. Bass, M. Lazard et J.-P. Serre, *Sous-groupes d'indice fini dans* SL $(n, \mathbf{Z})$ (*Bull. Amer. Math. Soc.*, t. 70, 1964, p. 385-392).

[4] H. Bass, J. Milnor et J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geqq 3)$ *and* Sp_{2n} $(n \geqq 2)$ (*Publ. Math. I. H. E. S.*, nº 33, 1968, p. 59-137).

[5] A. Borel et Harish-Chandra, *Arithmetic subgroups of algebraic groups* (*Ann. Math.*, t. 75, 1962, p. 485-535).

[6] A. Borel et J. Tits, *Groupes réductifs* (*Publ. Math. I. H. E. S.*, nº 27, 1965, p. 55-151).

[7] N. Bourbaki, *Algèbre*, chap. 6, Hermann, Paris, 1952.

[8] N. Bourbaki, *Groupes et algèbres de Lie*, chap. 4 à 6, Hermann, Paris, 1969.

[9] F. Bruhat, *Sur une classe de sous-groupes compacts maximaux des groupes de Chevalley sur un corps p-adique* (*Publ. Math. I. H. E. S.*, nº 23, 1964, p. 45-74).

[10] F. Bruhat et J. Tits, *Groupes simples résiduellement déployés sur un corps local* (*C. R. Acad. Sc.*, t. 263, 1966, p. 766-768).

[11] É. Cartan, *Sur certaines formes riemanniennes remarquables des géométries à groupe fondamental simple* (*Ann. scient. Éc. Norm. Sup.*, t. 44, 1927, p. 345-467).

[12] C. Chevalley, *Deux théorèmes d'arithmétique* (*J. Math. Soc. Japan*, t. 3, 1951, p. 36-44).

[13] C. Chevalley, *Sur certains groupes simples* (*Tôhoku Math. J.*, t. 7, 1955, p. 14-62).

[14] C. Chevalley, *Séminaire sur la classification des groupes de Lie algébriques*, E. N. S., 1956-1958 (notes multigraphiées).

[15] C. Chevalley, *Certains schémas de groupes semi-simples* (*Sém. Bourbaki*, exp. 219, 1960-1961).

[16] M. Demazure et A. Grothendieck, *Séminaire de géométrie algébrique, Schémas en groupes*, I. H. E. S., 1963-1964 (notes multigraphiées).

[17] N. Iwahori et H. Matsumoto, *On some Bruhat decomposition of p-adic Chevalley groups* (*Publ. Math. I. H. E. S.*, nº 25, 1965, p. 5-48).

[18] M. Kneser, *Strong approximation* (*Proc. Symp. Pure Math.*, t. 9, 1966, p. 187-196).

[19] T. KUBOTA, *Topological covering of* SL_2 *over a local field* (*J. Math. Soc. Japan*, t. 19, 1967, p. 114-121).
[20] H. MATSUMOTO, *Générateurs et relations des groupes de Weyl généralisés* (*C. R. Acad. Sc.*, t. 258, 1964, p. 3419-3422).
[21] H. MATSUMOTO, *Subgroups of finite index in certain arithmetic groups* (*Proc. Symp. Pure Math.*, t. 9, 1966, p. 99-103).
[22] J. MENNICKE, *Finite factor groups of the unimodular group* (*Ann. Math.*, t. 81, 1965, p. 31-37).
[23] J. MENNICKE, *Zur Theorie der Siegelschen Modulgruppe* (*Math. Ann.*, t. 159, 1965, p. 115-129).
[24] J. MENNICKE, *On Ihara's modular group* (*Invent. Math.*, t. 4, 1967, p. 202-228).
[25] C. MOORE, *Extensions and low-dimensional cohomology theory of locally compact groups* (*Trans. Amer. Math. Soc.*, t. 113, 1964, p. 40-86).
[26] C. MOORE, *Group extensions of p-adic and adelic linear groups* (*Publ. Math. I. H. E. S.*, n° 35, 1969, p.5-74).
[27] J.-P. SERRE, *Corps locaux*, Hermann, Paris, 1962.
[28] J.-P. SERRE, *Groupes de congruence* (*Sém. Bourbaki*, exp. 330, 1966-1967).
[29] J.-P. SERRE, *Le problème des groupes de congruence pour* SL_2 (en préparation)
[30] R. STEINBERG, *Générateurs, relations et revêtements de groupes algébriques* (*Colloque sur la théorie des groupes algébriques*, Bruxelles, 1962, p. 113-127).
[31] J. TITS, *Normalisateurs de tores* (*J. Alg.*, t. 4, 1966, p. 96-116).
[32] A. WEIL, *Sur certains groupes d'opérateurs unitaires* (*Acta Math.*, t. 111, 1964, p. 143-211).
[33] A. WEIL, *Basic number theory*, Springer-Verlag, Berlin, 1967.

(Manuscrit reçu le 2 juillet 1968.)