SUR CERTAINS GROUPES SIMPLES

C. CHEVALLEY

(Received February 1, 1955)

Introduction[1]

Presque tous les groupes simples connus sont intimement liés aux groupes continus simples que les méthodes de la théorie des algèbres de Lie permettent de classifier. Pour passer d'un groupe continu G à des groupes simples plus généraux, on procède en général comme suit: on part d'un groupe linéaire Γ localement isomorphe à G; Γ est alors un groupe algébrique, et on cherche à formuler la condition C pour qu'un élément appartienne à Γ en termes qui ne fassent pas intervenir la nature particulière du corps de base dans lequel on opère (celui des nombres réels ou des nombres complexes, suivant les cas); ceci fait, prenant un corps de base K quelconque, les éléments construits au moyen de K et de même nature que ceux dont se compose Γ (que ce soient des matrices ou des automorphismes d'espaces vectoriels) et qui satisfont à la condition C forment un groupe Γ_K. Le groupe Γ_K lui-même, ou plutôt en général un groupe qui s'en déduit facilement, se trouve alors être simple.

Cette méthode a été appliquée avec grand succès d'abord par Dickson ([3], [4]), qui mettait la condition C sous forme de relations algébriques entre éléments des matrices de Γ, et qui se limitait aux corps de base finis, puis par Dieudonné ([5]) qui utilise des définitions géométriques des groupes Γ et qui n'impose aucune limitation au corps K. La portée des méthodes de Dieudonné dépasse d'ailleurs le schéma que nous venons d'esquisser du fait qu'il construit aussi des groupes linéaires liés à des corps K non commutatifs.

Les méthodes de Dickson et de Dieudonné nécessitent une analyse spéciale de chaque type de groupes. Cette analyse a été faite dans le cas des groupes classiques et dans celui du groupe exceptionnel (G_2) ([4]); nous avons nous-même appliqué des méthodes analogues dans un travail encore indédit au cas des groupes exceptionnels $(F_4), (E_6)$ et (E_7). Dans le présent mémoire, nous présentons une méthode uniforme qui consiste à prendre toujours pour Γ le groupe adjoint d'un groupe simple complexe G; cependant, au lieu de définir Γ_K par une condition du genre de la condition C mentionée plus haut, nous le définissons comme engendré par certains sous-groupes que l'on peut indiquer explicitement. L'opération de transfert du corps des nombres complexes à un corps de base quelconque peut se faire simultanément pour tous les types de groupes complexes en s'appuyant sur la théorie des algèbres de Lie semi-simples; elle fournit des groupes simples attachés à

1 Une partie des travaux préliminaires relatifs aux questions traitées dans ce mémoire a été accomplie par l'auteur pendant qu'il était sous contrat avec le "Department of Air Force" de l'armée américaine.

tous les types de groupes continus simples complexes, classiques ou exceptionnels. Par contre, nous n'obtenons pour chaque groupe simple complexe G et chaque corps de base K qu'un seul groupe simple; par exemple, si G est le groupe orthogonal complexe, nous n'obtenons que les groupes simples liés aux formes quadratiques d'indice maximal.

Nous indiquons quelques résultats relatifs à la structure des groupes simples Γ_K que l'on peut obtenir par notre méthode. En particulier, nous généralisons à tous les types de groupes semi-simples et au cas d'un corps de base quelconque les résultats obtenus par F. Bruhat [1] dans le cas des groupes classiques relatifs à la décomposition en classes doubles suivant un sous-groupe résoluble maximal. Ces résultats avaient également été généralisés pour tous les types de groupes, mais en se limitant au cas du corps de base complexe, ou réel, par Harish-Chandra, dont la démonstration, différente de celle ici exposés, n'a pas encore été publiée. Ce résultat nous permet, dans le cas d'un corps de base fini K, d'exprimer l'ordre du groupe Γ_K au moyen d'une formule générale, qui fait intervenir des nombres intimement liés aux exposants primitifs de la cohomologie de l'algèbre de Lie du groupe semi-simple complexe dont nous partons. Nous donnons par ailleurs certains résultats partiels sur les groupes de Sylow des groupes Γ_K.

Terminologie et notations

1. Si f est une application d'un ensemble A dans un ensemble B, nous disons que f est injective si c'est une application biunivoque de A sur une partie de B, surjective si $f(A) = B$ et bijective si elle est à la fois injective et surjective. Si A et B sont des groupes et f un homomorphisme, nous disons que f est un monomorphisme s'il est injectif, un épimorphism s'il est surjectif, un isomorphisme s'il est bijectif.

2. Si A et B sont des parties d'un groupe, nous désignons toujours par AB l'ensemble des produits ab, où $a \in A, b \in B$; et de même pour les produits de plusieurs parties d'un groupe.

3. Nous désignons par $\mathbf{C}$ le corps des nombres complexes, par $\mathbf{Z}$ l'anneau des entiers.

§ I. Preliminaires. Rappel de résultats connus.

Nous désignerons par $\mathfrak{g}$ une algèbre de Lie semi-simple sur le corps des nombres complexes et par $\mathfrak{h}$ une algèbre de Cartan de $\mathfrak{g}$.

I. Si ρ est une représentation de $\mathfrak{g}$, on dit qu'une fonction linéaire w sur $\mathfrak{h}$ est un poids de la représentation ρ s'il existe un élément $x \neq 0$ de l'espace de cette représentation tel que $\rho(H)\cdot x = w(H)x$ pour tout $H \in \mathfrak{h}$. Les poids de toutes les représentations de $\mathfrak{g}$ engendrent un groupe additif de fonctions sur $\mathfrak{h}$; ce groupe est un groupe abélien libre à l générateurs, si l est le rang de $\mathfrak{g}$; nous désignerons ce groupe par P.

Nous appellerons racines ceux des poids de la représentation adjointe de $\mathfrak{g}$ qui sont $\neq 0$. Si r est une racine, il existe donc un élément $X_r \neq 0$ de

$\mathfrak{g}$ tel que $[H, X_r] = r(H)X_r$ pour tout $H \in \mathfrak{h}$. L'élément X_r est déterminé à un facteur scalaire près par cette condition; nous dirons que c'est un *élément radiciel* attaché à r. Si on choisit pour toute racine r un élément radiciel attaché à cette racine, ces éléments forment une base d'un sous-espace vectoriel de $\mathfrak{g}$ supplémentaire à $\mathfrak{h}$. Nous désignerons par P_r le groupe additif engendré par toutes les racines. C'est un sous-groupe d'indice fini de P, et P/P_r est isomorphe au centre d'un groupe compact simplement connexe dont l'algèbre de Lie est une forme réelle de $\mathfrak{g}$. Si r est une racine, il en est de même de $-r$.

Nous appellerons *co-poids* les éléments H de $\mathfrak{h}$ tels que les nombres $w(H)$, $w \in P$, soient tous entiers; ils forment un groupe additif que nous désignerons par $\mathfrak{H}$ (prononcer: ha).

II. Le groupe P_r peut être muni (d'au moins une manière) d'une structure de groupe ordonné; ceci fait, les racines se trouvent réparties en deux ensembles disjoints, celui des racines positives et celui des racines négatives. Si l est le rang de $\mathfrak{g}$, il existe un ensemble bien déterminé de l racines $a_1, \ldots, a_l$ telles que toute racine positive soit combinaison linéaire à coefficients entiers tous $\geqq 0$ de $a_1, \ldots . a_l$ (cf. [9], prop. 3, p. 289). On dit que $\{a_1, \ldots . a_l\}$ est le *système fondamental* défini par notre ordination du groupe P_r, et que les racines de cet ensemble sont les *racines fondamentales*. Si X_i et Y_i sont des éléments radiciels attachés à a_i et $-a_i$ respectivement, les $2l$ éléments X_i, Y_i forment un ensemble de générateurs de $\mathfrak{g}$.

III. Soit Σ un ensemble de racines qui possède les propriétés suivantes: si $r \in \Sigma$, on a aussi $-r \in \Sigma$; si la somme de deux racines de Σ est une racine, cette racine est dans Σ. Soit, pour $r \in \Sigma$, X_r un élément radiciel attaché à r. Les X_r ($r \in \Sigma$) engendrent alors une sous-algèbre semi-simple $\mathfrak{g}_\Sigma$ de $\mathfrak{g}$. L'ensemble $\mathfrak{h} \cap \mathfrak{g}_\Sigma$ est une algèbre de Cartan de $\mathfrak{g}_\Sigma$, et les racines de $\mathfrak{g}_\Sigma$ (relativement à cette algèbre de Cartan) sont les restrictions a $\mathfrak{h} \cap \mathfrak{g}_\Sigma$ des racines $r \in \Sigma$.

Si r est une racine, les seules racines linéairement dépendantes de r sont r et $-r$; si on pose $\Sigma = \{r, -r\}$, l'algèbre $\mathfrak{g}_\Sigma$, que nous désignerons alors par $\mathfrak{g}_r$, est une algèbre simple de dimention 3 et de rang 1. L'algèbre $\mathfrak{g}_r \cap \mathfrak{h}$ admet une base composée d'un élément H_r tel que $r(H_r) = 2$; cette condition détermine entièrement H_r. L'élément H_r est un co-poids, que nous appellerons le *co-poids attaché à* r; les H_r, pour toutes les racines r, engendrent le groupe $\mathfrak{H}$.

Revenant au cas général, nous appellerons *admissibles* les ensembles Σ de racines qui possèdent les propriétés indiquées ci-dessus. Un système admissible est dit simple s'il est non vide et s'il est impossible de le représenter comme réunion de deux systèmes admissibles disjoints non vides. L'ensemble de toutes les racines se décompose d'une manière et d'une seule en la réunion d'un certain nombre de systèmes admissibles simples $\Sigma(j)$, $1 \leqq j \leqq m$. L'algèbre $\mathfrak{g}$ est somme directe des algèbres $\mathfrak{g}_{\Sigma(j)}$, qui sont simples. Tout système fondamental de racines de $\mathfrak{g}$ est la réunion de ses intersections avec les $\Sigma(j)$,

et son intersection avec $\Sigma(j)$ est un système fondamental de racines de $\Sigma(j)$. Si r et s sont des racines qui appartiennent à des systèmes simples $\Sigma(j)$, $\Sigma(j')$ distincts l'un de l'autre, les seules combinaisons linéaires de r, s qui soient des racines sont $\pm r$ et $\pm s$.

IV. Les algèbres simples ont été entièrement classifiées. Les types d'algèbres simples sont les suivants: le type (A_l) $(l \geqq 1)$; le type (B_l) $(l \geqq 2)$; le type (C_l) $(l \geqq 3)$; le type (D_l) $(l \geqq 4)$, le type (E_l) $(l = 6, 7$ ou $8)$; le type (F_4); le type (G_2); dans chaque cas, le nombre qui figure en indice dans la désignation du type indique le rang de l'algèbre correspondante.

Si $\mathfrak{g}$ est simple et de rang 2; on peut choisir un système fondamental de racines $\{a, b\}$ tel que les racines positives de $\mathfrak{g}$ soient:

$a, b, a + b$ si $\mathfrak{g}$ est de type (A_2);

$a, b, a + b, 2a + b$ si $\mathfrak{g}$ est de type (B_2);

$a, b, a + b, 2a + b, 3a + b, 3a + 2b$ si $\mathfrak{g}$ est de type (G_2).

On obtient naturellement toutes les racines en adjoignant aux précédentes celles qu'on en déduit en les multipliant par -1.

Si $\mathfrak{g}$ est une algèbre de Lie quelconque, un système admissible de racines de $\mathfrak{g}$ ne peut être de type (G_2) que si c'est l'un des systèmes simples maximaux en lesquels se décompose l'ensemble de toutes les racines. En particulier, si $\mathfrak{g}$ est simple mais n'est pas de type (G_2), aucun système admissible de racines de $\mathfrak{g}$ ne peut être de type (G_2).

V. Si H, H' sont des éléments de $\mathfrak{h}$, posons

$$\beta(H, H') = \Sigma_r r(H) r(H') = \mathrm{Tr}\,(\mathrm{ad}\, H)(\mathrm{ad}\, H');$$

β est alors une forme bilinéaire symétrique sur $\mathfrak{h} \times \mathfrak{h}$, et la forme quadratique correspondante est définie positive. Pour toute racine r, r est proportionnelle à la forme linéaire $H \to \beta(H, H_r)$ sur $\mathfrak{h}$; le facteur de proportionnalité est le nombre $2(\beta(H_r, H_r))^{-1} > 0$. Dans chacun des systèmes admissibles simples maximaux Σ en lesquels se décompose l'ensemble des racines, nous choisirons une racine r_Σ telle que l'on ait $\beta(H_{r_\Sigma}, H_{r_\Sigma}) \geqq \beta(H_r, H_r)$ pour toute racine $r \in \Sigma$; et, si r est une racine quelconque de Σ, nous poserons

$$\lambda(r) = \beta(H_{r_\Sigma}, H_{r_\Sigma})(\beta(H_r, H_r))^{-1};$$

le nombre $\lambda(r)$ s'appelle alors la *longueur* de la racine r. Si Σ est l'un des systèmes admissibles simples maximaux en lesquels se décompose l'ensemble de toutes les racines, l'ensemble des longueurs des racines de Σ est soit $\{1\}$ (c'est le cas si Σ est de l'un des types (A_l), (D_l) ou (E_l)), soit $\{1, 2\}$ (c'est le cas si Σ est de l'un des types (B_l), (C_l) ou (F_4)), soit $\{1, 3\}$ (c'est le cas si Σ est de type (G_2)).

On dit que des racines r et s sont *orthogonales* si $s(H_r) = 0$, ce qui entraîne $r(H_s) = 0$. Il en est toujours ainsi si r et s appartiennent à des systèmes admissibles simples maximaux distincts, mais la réciproque n'est pas vraie. Les faits suivants résultent de notre définition des longueurs des racines:

si r et s sont des racines quelconques, on a

(1) $$\lambda(s) r(H_s) = \lambda(r) s(H_r);$$

l'application qui à toute racine r fait correspondre l'élément $\lambda(r)H_r$ se prolonge en un homomorphisme de P_r dans $\mathfrak{h}$; en particulier, si $r, s, r+s$ sont des racines, on a

$$\lambda(r+s)H_{r+s} = \lambda(r)H_r + \lambda(s)H_s. \tag{2}$$

Par ailleurs, en écrivant que la forme quadratique associée à β est définie positive, on obtient facilement le résultat suivant:

si r, s sont des racines linéairement indépendantes, on a

$$0 \leqq s(H_r) \cdot r(H_s) \leqq 3. \tag{3}$$

VI. Soit F un système fondamental de racines. On peut associer à F un graphe défini comme suit: ses sommets correspondent biunivoquement aux racines de F; deux sommets sont joints par une arête si et seulement si les racines correspondantes de F ne sont pas orthogonales. Nous entendrons par graphe associé à F l'objet constitué par le graphe tel que nous venons de le définir et par l'application qui à tout sommet du graphe fait correspondre la longueur de la racine associée à ce sommet. La structure de ce graphe ne dépend alors que de l'algèbre $\mathfrak{g}$ (i. e. elle ne dépend ni du choix de l'algèbre de Cartan $\mathfrak{h}$ ni du choix du système fondamental F); nous dirons que c'est le graphe associé à $\mathfrak{g}$. Réciproquement, l'algèbre $\mathfrak{g}$ est déterminée à un isomorphisme près par la connaissance du graphe qui lui est associé. Nous donnons ci-dessous une description des graphes associés aux divers types d'algèbres simples, avec les conventions de notations suivantes: les sommets sont désignés par $S_1, \ldots S_l$; les racines dont les longueurs ne sont pas données sont censéss être de longueur 1; les seules arêtes qui figurent dans le graphe sont celles qui sont explicitement indiquées. Les types de graphes sont alors les suivants:

a) pour le type (A_l): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq l)$;

b) pour le type (B_l): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq l)$, les racines correspondant à $S_1, \cdots, S_{l-1}$ sont de longueur 2;

c) pour le type (C_l): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq l)$, la racine correspondant à S_l est de longueur 2;

(d) pour le type (D_l): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq l-1)$, S_l et S_{l-2} sont joints par une arête;

(e) pour le type (E_l): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq l-1)$, S_l et S_{l-3} sont joints par une arête;

(f) pour le type (F_4): S_{i-1} et S_i sont joints par une arête $(2 \leqq i \leqq 4)$; les racines correspondant à S_3, S_4 sont de longueur 2;

(g) pour le type (G_2): S_1 et S_2 sont joints par une arête; S_2 est de longueur 3.

Les particularités suivantes se dégagent de l'examen de ces graphes:

1) ils sont connexes; cela signifie qu'il est impossible de décomposer l'ensemble des racines d'un systèmes fondamental en deux parties non vides telle que toute racine de l'une soit orthogonale à toute racine de l'autre;

2) ils ne contiennent aucun triangle; cela signifie qu'étant données deux racines non orthogonales r, s d'un système fondamental F, toute racine de

F distincte de r et s est orthogonale à l'une au moins des racines r, s;

3) le graphe formé de ceux des sommets qui correspondent à des racines d'une longueur donnée et des arêtes qui joignent ces sommets entre eux est connexe; cela signifie qu'il est impossible de décomposer l'ensemble des racines de longueur λ d'un système fondamental en deux parties non vides telles que toute racine de l'une soit orthogonale à toute racine de l'autre.

VII. Nous désignerons dans ce no. par r et s des racines linéairement indépendantes de $\mathfrak{g}$.

LEMME 1. *Il existe un système fondamental de racines qui contient r ainsi qu'une racine t telle que s soit combinaison linéaire à coefficients $\geqq 0$ de r et de t.*

Soit $(r_1, \ldots, r_h)$ une base de l'espace vectoriel E composé des combinaisons linéaires à coefficients rationnels des racines telle que $r_1 = r, r_2 = s$. Cette base définit sur E une structure d'espace vectoriel ordonné dans laquelle les éléments > 0 sont les $\sum_{i=1}^{l} \alpha_i r_i$ où les α_i sont des nombres rationnels tels que $\alpha_k > 0$, $\alpha_{k+1} = \ldots = \alpha_l = 0$ pour un certain indice $k \leqq l$. On sait ([9]; voir la remarque qui suit l'énoncé de la prop. 3, p. 289) que les 2 plus petits éléments de l'ensemble des racines relativement à cette relation d'ordre font partie d'un système fondamental de racines. Comme les seules racines linéairement dépendantes de r sont $\pm r$, la plus petite racine positive est r. Soit t la plus petite des racines qui sont $> r$. Comme $t \leqq s$, on a $t = \alpha r + \beta s$ avec $0 < \beta \leqq 1$, d'où $s = \beta^{-1}(t - \alpha r)$. L'expression de s comme combinaison des racines du système fondamental ayant ses coefficients tous de même signe, on a $\alpha \leqq 0$, ce qui démontre le lemme.

L'ensemble des entiers i tels que $s + ir$ soit une racine est un intervalle fermé $[-p, q]$ de l'ensemble des entiers, p et q étant des entiers $\geqq 0$ tels que

$$s(H_r) = p - q.$$

En particulier, si $s(H_r) > 0$ (resp. si $s(H_r) < 0$), alors $s - r$ (resp. $s + r$) est une racine; par ailleurs, si $s(H_r) = 0$, et si l'une des combinaisons $s + r, s - r$ est une racine, il en est de même de l'autre. Si r et s appartiennent à un système fondamental, $s - r$ ne peut être une racine, de sorte que la somme de deux racines orthogonales d'un système fondamental n'est jamais une racine.

Il est clair que $(s - pr)(H_r) = -(p + q)$; faisant usage de la formule (3), on en déduit que $p + q \leqq 3$. De plus, si $p + q > 1$, on a $r(H_{s-pr}) = -1$, et il résulte de (1) que r et $s - pr$ n'ont pas la même longueur. Supposant toujours que $p + q > 1$, r et s appartiennent à un même système admissible simple, et, si $p + q = 3$, il y a dans ce système deux racines dont le rapport des longueurs est 3, ce qui ne peut se produire que si le système admissible en question est de type (G_2). Supposons maintenant que $\mathfrak{g}$ soit simple mais ne soit pas de type (G_2); l'ensemble de celles des racines qui sont des combinaisons linéaires de r et de s est alors un système admissible Σ de rang 2

qui ne peut être que de l'un des types (A_2) ou (G_2). S'il est de type (A_2), Σ ne contient que 6 éléments; s'il est de type (B_2), il contient 8 éléments. On en déduit les résultats suivants :

LEMMA 2. *Supposons que $\mathfrak{g}$ soit simple et ne soit pas de type (G_2). Si r, s sont des racines telles que $s - r$, s, $s + r$ soient racines, les seules combinaisons linéarires de r, s qui soient des racines sont $\pm r, \pm s, \pm (s - r), \pm (s + r)$; si $r + s$, $r + 2s$ sont racines, les seules combinaisons linéaires de r et s qui soient des racines sont $\pm r$, $\pm s$, $\pm(r + s)$, $\pm (r + 2s)$; si $r + s$ est une racine et si aucune des combinaisons $r - s$, $r + 2s$, $2r + s$ n'est racine, les seules racines qui sont des combinaisons linéaires de r et s sont $\pm r, \pm s$ et $\pm (r + s)$.*

LEMME 3. *Supposons que i et j soient des entiers > 0 tels que $ir + js$ soit une racine. Alors l'une au moins des combinaisons $(i - 1)r + js, ir + (j - 1)s$ est une racine; et $r + s$ est une racine.*

On a $(ir + js)(\lambda(ir + js)H_{ir+js}) = 2\lambda(ir + js) > 0$; mais le premier membre est $i\lambda(r)(ir + js)(H_r) + j\lambda(s)(ir + js)(H_s)$ (cf. formule (2)); l'un au moins des nombres $(ir + js)(H_r), (ir + js)(H_s)$ est donc > 0, ce qui démontre la première assertion. La seconde est une conséquence de la première et du fait que $2r$, $2s$ ne sont pas des racines.

VIII. LEMME 4. *Supposons P_r muni d'une structure de groupe ordonné, et soit F le système fondamental de racines correspondant à cette ordination de P_r. Si r est une racine positive, il existe une suite finie $(r_1, \ldots, r_h)$ de racines positives telle que $r_1 \in F$, $r_i - r_{i-1} \in F$ $(2 \leqq i \leqq h)$ et $r_h = r$.*

Toute racine positive étant combinaison linéaire à coefficients entiers $\geqq 0$ des racines $a(1), \ldots, a(l)$ de F, il suffira évidemment d'établir que, si r n'est pas dans F, il y a au moins un i $(1 \leqq i \leqq l)$ tel que $r - a(i)$ soit une racine. Soient λ_i la longueur de $a(i)$ et λ celle de r; on a $2\lambda = r(\lambda H_r) = \sum_{i=1}^{h} c_i \lambda_i r(H_{a(i)})$, si $r = \sum_{i=1}^{l} c_i a(i)$ (cf. formule (2)). Les c_i étant $\geqq 0$, l'un au moins des nombres $r(H_{a(i)})$ est > 0, ce qui démontre le lemme 4.

Les notations étant celles du lemme 4, h est évidemment la somme des coefficients de l'expression de r comme combinaison linéaire des racines $a(i)$ $(1 \leqq i \leqq l)$ de F; on appelle ce nombre la *hauteur* de r (par rapport à F). On peut toujours munir P_r d'une structure de groupe ordonné telle que F soit le système des racines fondamentales pour cette structure d'ordre et que de plus la hauteur soit une fonction croissante sur l'ensemble des racines > 0. En effet, si $u \in P_r$, soient $\rho_i(u)$ les coefficients de l'expression de u comme combinaison linéaire des $a(i)$: posons $\rho'_i(u) = \rho_i(u)$ si $i < l$, $\rho'_l(u) = \rho_1(u) + \ldots + \rho_l(u)$; il suffit alors d'ordonner P_r en prenant comme éléments > 0 les éléments u tels que $\rho'_k(u) > 0, \rho'_{k+1}(u) = \ldots = \rho'_l(u) = 0$ pour au moins un indice $k \leqq l$. Une structure de groupe ordonné sur P_r qui satisfait à la conditions que nous venons d'énoncer sera appelée *régulière*.

IX. Pour toute racine r, soit H_r le co-poids attaché à r. Il y a un automorphisme σ_r du groupe P engendré par les poids qui change tout $u \in$

P en $u - u(H_r)r$; cet automorphisme, qui est d'ordre 2, s'appelle la *symétrie par rapport à* r. Les symétries par rapport à toutes les racines engendrent un groupe fini W, qui s'appelle le *groupe de Weyl*. Les opérations de ce groupe permutent entre elles les racines. Si w est une opération de ce groupe, il y a un automorphisme ω de $\mathfrak{g}$ tel que, pour toute racine r et tout élément radiciel X_r attaché à r, $\omega \cdot X_r$ soit un multiple scalaire de $X_{w(r)}$; ω n'est pas determiné de manière unique par w, mais sa restriction à $\mathfrak{h}$ l'est ; elle transforme le co-poids H_s attaché à une racine s en le co-poids $H_{w(s)}$ attaché à $w(s)$. Il résulte immédiatement de l'existence de ω que, pour toute racine r, $w(r)$ a même longueur que r. Nous ferons la convention de désigner par une même lettre w une opération du groupe de Weyl, la permutation des racines produite par w et l'automorphisme de $\mathfrak{h}$ qui change H_r en $H_{w(r)}$ (pour toute racine r). Si F est un système fondamental de racines, le groupe de Weyl est déjà engendré par les symétries par rapport aux racines de F ([9], cor. 2 to prop. 3, p. 291). Si F' est un autre système fondamental de racines, il y a une opération w et une seule du groupe de Weyl telle que $w(F') = F$ ([8], prop. 4 p. 291). On en conclut facilement que la seule opération w du groupe de Weyl qui permute entre elles les racines positives relativement à la relation d'ordre sur P_r qui définit F est l'identité.

LEMME 5. *Si* $\mathfrak{g}$ *est simple, deux racines de même longueur peuvent toujours être transformées l'une en l'autre par un opération du groupe de Weyl.*

Soient r et s des racines de même longueur λ. Soit R (resp. : S) l'ensemble des transformées de r (resp. : s) par les opérations du groupe de Weyl. Soit F un système fondamental de racines. Chacune des racines r et s appartient à au moins un système fondamental de racines ; comme les systèmes fondamentaux de racines sont permutés transitivement entre eux par les opérations du groupe de Weyl, F rencontre R et S. Or, si r' et s' sont des racines de même longueur appartenant à F et qui ne sont pas orthogonales, r' et s' peuvent être transformées l'une en l'autre par une opération du groupe de Weyl. En effet, il résulte de la formule (1) que les nombres $r'(H_{s'})$, $s'(H_{r'})$, qui sont $\neq 0$, sont égaux entre eux ; ces nombres sont négatifs puisque r' et s' appartiennet à un système fondamental, et leur produit est $\leqq 3$ (formule (3)) ; ils sont donc tous deux égaux à -1. La symétrie par rapport à r' change donc s' en $s' + r'$, et la symétrie par rapport à s' change r' en $r' + s'$, ce qui démontre notre assertion. On en conclut que toute racine de longueur λ de F n'appartenant pas à $F \cap R$ est orthogonale à toutes les racines de $F \cap R$; tenant compte d'une remarque faite plus haut (cf. VI, 3)), on en conclut que $F \cap R$ est l'ensemble de toutes les racines de longueur λ de F, donc rencontre $F \cap S$; puisque $R \cap S \neq \phi$, on a $R = S$.

X. Pour toute racine r, soit X_r un élément radiciel attaché à r et soit H_r le co-poids attaché à r. Alors $[X_r, X_{-r}]$ est un multiple scalaire de H_r. Puisque $H_{-r} = -H_r$, il est possible de choisir les X_r de telle manière que $[X_r, X_{-r}] = H_r$ pour toute racine r. Nous supposerons toujours dans la suite

qu'il en est ainsi. Cette condition ne détermine d'ailleurs pas encore les X_r : on peut les remplacer par les $u_r X_r$, où les u_r sont des nombres complexes tels que $u_r u_{-r} = 1$.

Si r et s sont des racines linéairement indépendantes, et si $r + s$ n'est pas une racine, on a $[X_r, X_s] = 0$; si au contraire $r + s$ est une racine, $[X_r, X_s]$ est de la forme $N_{r,s} X_{r+s}$, $N_{r,s}$ étant un nombre qui jouera un rôle fondamental dans la suite de ce mémoire. Si on remplace les X_r par des $u_r X_r$, avec $u_r u_{-r} = 1$, les $N_{r,s}$ se trouvent remplacés par des nombres $N'_{r,s}$ donnés par la formule

$$N'_{r,s} = u_r u_s u_{r+s}^{-1} N_{r,s} ; \tag{4}$$

il en résulte que $N_{r,s} N_{-r,-s}$ n'est pas changé. Nous allons calculer ce nombre. Soient donc r et s des racines telles que $r + s$ soit racine ; supposons que $[-p, q]$ soit l'intervalle de l'ensemble des entiers composé des i tels que $s + ir$ soit racine. Si $p > 0$, l'identité de Jacobi pour X_r, X_{-r}, X_s donne

$$s(H_r) + N_{-r,s} N_{s-r,r} + N_{s,r} N_{r+s,-r} = 0.$$

Cette formule est d'ailleurs vraie dans tous les cas si nous faisons la convention que $N_{r,s}$ réprésente 0 toutes les fois que ou bien r et s ne sont pas tous deux des racines, ou bien r et s sont des racines, mais non $r + s$. Appliquant cette égalité aux racines $s + ir$ ($-p \leqq i \leqq 0$) et ajoutant les résultats, on obtient la formule

$$N_{r,s} N_{-r,r+s} = q(p + 1). \tag{5}$$

Appliquant maintenant l'identité de Jacobi pour X_{-r}, X_{-s}, X_{r+s}, il vient

$$-N_{-r,-s} H_{r+s} + N_{-s,r+s} H_r + N_{r+s,-r} H_s = 0.$$

Tenant compte de la formule (2) et observant que H_r, H_s sont linéairement indépendants, il vient

$$N_{-r,-s} \lambda(s) + N_{-r,r+s} \lambda(r + s) = 0$$

et par suite

$$N_{r,s} N_{-r,-s} = -q(p + 1) \lambda(r + s) (\lambda(s))^{-1}.$$

Nous allons donner une forme plus simple à ce résultat. Il existe un système fondamental de racines contenant 2 racines a et b telles que r soit soit a soit b et que s soit une combinaison linéaire à coefficients $\geqq 0$ de a et b (Lemme 1). Puisque $r + s$ est une racine, a et b ne sont pas orthogonales ; les racines qui sont des combinaisons linéaires de a et de b forment un système admissible de l'un des type $(A_2), (B_2)$ ou (G_2).

1. Si Σ est de type (A_2), a et b jouent des rôles symétriques, et on peut supposer que $r = a$; $r + s$ étant une racine, on a $s = b$. Puisque ni $2a + b$ ni $a + 2b$ n'est racine, on a $a(H_b) = b(H_a) = -1$, d'où (en vertu de (1)) $\lambda(a) = \lambda(b)$; la symétrie par rapport à a transforme b en $a + b$, d'où $\lambda(a + b) = \lambda(b)$; le nombre $\lambda(r + s) (\lambda(s))^{-1} = 1$ est donc égal à $q^{-1}(p + 1)$, puisqu'ici $p = 0, q = 1$.

2. Si Σ est de type (B_2), nous supposons que $b + 2a$ est racine. On a $b(H_a) = -2$, $a(H_b) = -1$ d'où $\lambda(b) = 2\lambda(a)$. La symétrie par rapport à a

transforme b en $b+2a$, et la symétrie par rapport à b transforme a en $a+b$, d'où $\lambda(b+2a)=\lambda(b), \lambda(a+b)=\lambda(a)$. Si $r=a$, $s=b$, on a $\lambda(r+s)=(1/2)\lambda(s)$, $p=0, q=2$; si $r=a$, $s=a+b$, on a $\lambda(r+s)=2\lambda(s)$, $p=1$, $q=1$; si $r=b, s=a$, on a $\lambda(r+s)=\lambda(s)$, $p=0, q=1$. On a donc dans tous les cas $\lambda(r+s)(\lambda(s))^{-1}=q^{-1}(p+1)$.

3. Si Σ est de type (G_2), nous supposerons que $b+3a$ est une racine. On a $b(H_a)=-3$, $a(H_b)=-1$, d'où $\lambda(b)=3\lambda(a)$. La symétrie par rapport à a transforme b en $b+3a$; la symétrie par rapport à b transforme a en $a+b$. On a $(a+b)(H_a)=-1$, de sorte que la symétrie par rapport à a transforme $b+a$ en $b+2a$. On a $(3a+b)(H_b)=-1$, de sorte que la symétrie par rapport à b transforme $3a+b$ en $3a+2b$. On a donc

$$\lambda(b)=\lambda(3a+b)=\lambda(3a+2b)=3\lambda(a)=3\lambda(a+b)=3\lambda(2a+b). \tag{6}$$

Si $r=a, s=b$, on a $\lambda(r+s)=(1/3)\lambda(s), p=0, q=3$; si $r=a, s=a+b$, on a $\lambda(r+s)=\lambda(s)$, $p=1, q=2$; si $r=a, s=2a+b$, on a $\lambda(r+s)=3\lambda(s)$, $p=2$, $q=1$; si $r=b$, $s=a$, on a $\lambda(r+s)=\lambda(s), p=0, q=1$; si $r=b$, $s=3a+b$, on a $\lambda(r+s)=\lambda(s), p=0, q=1$. On a donc encore $\lambda(r+s)(\lambda(s))^{-1}=q^{-1}(p+1)$.

La formule $\lambda(r+s)(\lambda(s))^{-1}=q^{-1}(p+1)$ est donc vraie dans tous les cas. On en déduit l'expression

$$N_{r,s}N_{-r,-s}=-(p+1)^2$$

du produit $N_{r,s}N_{-r,-s}$.

Nous allons maintenant montrer qu'il est possible de choisir les X_r de telle manière que $N_{r,s}=\pm(p+1)$ pour tout couple (r,s) de racines tel que $r+s$ soit une racine. On sait qu'il existe un automorphisme θ d'orde 2 de $\mathfrak{g}$ qui change tout X_r en un multiple scalaire de X_{-r}: c'est celui qui permet de construire la forme réelle compacte de $\mathfrak{g}$. Soit $\theta \cdot X_r = c_r X_{-r}$; puisque θ est un automorphisme, on voit tout de suite que $\theta \cdot H_r = H_{-r} = -H_r$ pour toute racine r; la formule $[X_r, X_{-r}]=H_r$ donne donc $c_r c_{-r}=1$. On peut donc trouver des nombres u_r tels que $u_r^2=-c_r$, $u_r u_{-r}=1$. On a alors $\theta(u_r^{-1}X_r)=-u_r^{-1}X_{-r}$. Remplaçant les X_r par les $u_r^{-1}X_r$, on voit qu'on peut supposer les X_r choisis de telle manière que $\theta \cdot X_r = -X_{-r}$. Utilisant le fait que θ est un automorphisme, on voit alors tout de suite que $N_{-r,-s}=-N_{r,s}$, d'où

$$N_{r,s}=\pm(p+1).$$

Ni les éléments X_r ni les nombres $N_{r,s}$ ne sont encore déterminés de manière unique par ces conditions. Supposons donné pour chaque racine r un élément radiciel $X'_r=u_r X_r$ attaché à r de telle manière que $[X_r, X_{-r}]=H_r$ pour toute racine r et que $N'_{r,s}=u_r u_s u_{r+s}^{-1} N_{r,s}=\pm(p+1)$ toutes les fois que $r+s$ est une racine. On a alors $u_{r+s}=\pm u_r u_s$. Soit F un système fondamental de racines; c'est une base du groupe P_r engendré par les racines, et il existe par suite un homomorphism f de P_r dans le groupe multiplicatif des nombres complexes $\neq 0$ tel que $f(r)=u_r$ si $r \in S$. Posons $u'_r=u_r(f(r))^{-1}$; on a alors $u'_r=1$ si $r \in F$, $u'_r u'_{-r}=1$. Si $r, s, r+s$ sont des racines, on a $u'_r u'_s (u'_{r+s})^{-1}=u_r u_s (u_{r+s})^{-1}=\pm 1$. Faisant usage du lemme 4, on en déduit tout de suite que $u'_r=\pm 1$ pour toute racine r positive, donc aussi pour toute racine

r, puisque $u'_{-r} = u'^{-1}_r$. Par ailleurs, on a $N'_{r,s} = u'_r u'_s u'^{-1}_{r+s}$. Nous sommes donc arrivés aux résultats suivants;

THÉORÈME 1. *Soit $\mathfrak{g}$ une algèbre de Lie semi-simple sur le corps des nombres complexes, et soit $\mathfrak{h}$ une algèbre de Cartan de $\mathfrak{g}$. Pour toute racine r, soit H_r le co-poids attaché à r. On peut alors attacher à toute racine r un élément radiciel X_r de telle manière que les conditions suivantes soient satisfaites: a) on a $[X_r, X_{-r}] = H_r$ pour toute racine r; b) si $r, s, r+s$ sont des racines, on a $[X_r, X_s] = N_{r,s}X_{r+s}$, avec $N_{r,s} = \pm(p+1)$, p étant le plus grand entier $i \geqq 0$ tel que $s - ir$ soit une racine. Si (X'_r) est un autre système d'éléments radiciels satisfaisant aux mêmes conditions que les X_r, et donnant lieu à des constantes $N'_{r,s}$, on $N'_{r,s} = u_r u_s u^{-1}_{r+s} N_{r,s}$, les u_r étant des nombres tous égaux à ± 1 tels que $u_r u_{-r} = 1$.*

§II. Certains sous-groupes du groupe adjoint.

Nous utiliserons les mêmes notations qu'au §I; nous supposerons qu'on a fait choix d'éléments radiciels X_r (pour toutes les racines) satisfaisant aux conditions du théorème 1, §I.

Soit Γ le groupe adjoint de $\mathfrak{g}$, c'est-à-dire la composante connexe de l'élément unité dans le groupe des automorphismes de $\mathfrak{g}$. C'est un groupe linéaire algébrique complexe dont l'algèbre de Lie est l'image ad $\mathfrak{g}$ de $\mathfrak{g}$ par sa représentation adjointe.

Si r est une racine, et t un nombre complexe, nous poserons

$$x_r(t) = \exp t(\mathrm{ad}X_r).$$

L'opération $\mathrm{ad}X_r$ applique X_{-r} sur H_r et H_r sur $-2X_r$. Par ailleurs, si s est une racine linéairement indépendante de r, ad X_r applique X_s sur $N_{r,s}X_{r+s}$ si $r+s$ est une racine, sur 0 dans le cas contraire. On en conclut que

$$\begin{aligned} &x_r(t)\cdot X_{-r} = X_{-r} + tH_r - t^2X_r; \\ &x_r(t)\cdot H_r = H_r - 2tX_r;\ x_r(t)\cdot X_r = X_r \end{aligned} \tag{1}$$

et

$$x_r(t)\cdot X_s = X_s + \sum_{i=1}^{l} M_{r,s,i}t^i X_{ir+s} \tag{2}$$

si s est une racine linéairement indépendante de r, q étant le plus grand entier tel que $qr + s$ soit racine; on a posé

$$M_{r,s,i} = (i!)^{-1}\prod_{j=0}^{i-1} N_{r,jr+s}. \tag{3}$$

Les nombres $M_{r,s,i}$ sont des entiers. Soit en effet p le plus grand entier tel que $s - pr$ soit une racine: on a alors $N_{r,jr+s} = \pm(p+j)$, et

$$M_{r,s,i} = \pm(i!)^{-1}p(p+1)\ldots(p+i-1),$$

ce qui démontre notre assertion.

Supposons maintenant donnée une structure de groupe ordonné sur le groupe P_r engendré par les racines. L'espace vectoriel $\mathfrak{u}$ engendré par les éléments X_r relatifs aux racines positives r est alors manifestement une sous-algèbre de $\mathfrak{g}$. Son image $\mathrm{ad}_{\mathfrak{g}}\mathfrak{u}$ par la représentation adjointe de $\mathfrak{g}$ est une sous-algèbre de ad $\mathfrak{g}$; c'est l'algèbre de Lie d'un sous-groupe connexe $\mathfrak{U}$ de Γ. Les éléments de $\mathrm{ad}_{\mathfrak{g}}\mathfrak{u}$ sont des endomorphismes nilpotents de l'espace

vectoriel $\mathfrak{g}$. Soit en effet h la plus grande des hauteurs des racines positives de $\mathfrak{g}$. Si $k > 0$, désignons par $\mathfrak{g}_k$ l'espace vectoriel engendrée par les X_r relatifs aux racines $r > 0$ de hauteurs $\geqq k$; posons $\mathfrak{g}_0 = \mathfrak{h} + \mathfrak{g}_1 = \mathfrak{h} + \mathfrak{u}$, et, si $k < 0$, désignons par $\mathfrak{g}_k$ la somme de $\mathfrak{g}_0$ et de l'espace engendré par les X_{-r} où r parcourt les racines > 0 de hauteurs $\leqq -k$. On a alors $\mathfrak{g}_{-h} = \mathfrak{g}$, $\mathfrak{g}_{k+1} \subset \mathfrak{g}_k$, $\mathfrak{g}_{h+1} = \{0\}$, et il est clair que, pour toute racine $r > 0$, $\mathrm{ad}X_r$ applique $\mathfrak{g}_k$ dans $\mathfrak{g}_{k+1}$ pour tout k. Il en résulte que, si X est un élément quelconque de $\mathfrak{u}$, $\mathrm{ad}X$ applique $\mathfrak{g}_k$ dans $\mathfrak{g}_{k+1}$, d'où $(\mathrm{ad}X)^{2h+1} = 0$. Soient par ailleurs $r(1)$, ..., $r(N)$ toutes les racines positives arrangées par ordre de grandeur croissante (relativement à notre ordination de P_r), si $[X_{r(i)}, X_{r(j)}]$ est $\neq 0$, c'est un multiple scalaire de $X_{r(k)}$ où $r(k) = r(i) + r(j)$ d'où il résulte immédiatement que $r(k) > r(i)$, $r(k) > r(j)$ dans notre relation d'ordre. Donc, pour tout i, $(X_{r(i)}, \ldots . X_{r(N)})$ forment une base d'un idéal $\mathfrak{u}_i$ de l'algèbre $\mathfrak{u}$. On sait que, dans ces conditions, tout élément x de $\mathfrak{U}$ se met d'une manière et d'une seule sous la forme

$$x = \prod_{r>0} x_r(t_r),$$

le produit étant étendu à toutes les racines positives arrangées par ordre de grandeur croissante, et les t_r étant des nombres complexes; de plus, si nous posons $t_r = T_r(x)$, toute fonction sur $\mathfrak{U}$ dont la valeur en un point $x \in \mathfrak{U}$ peut s'exprimer comme polynome en les coefficients de la matrice qui représente x par rapport à une base de $\mathfrak{g}$ peut aussi s'exprimer comme polynome en les fonctions T_r; et, réciproquement, les $T_r(x)$ s'expriment comme polynomes en les coefficients de la matrice qui représente x ([2], chap. V, §3, prop. 17, p. 127). Il en résulte immédiatement que les $T_r(xy)$ peuvent s'exprimer comme polynomes en les $T_r(x)$, $T_r(y)$; et, comme les éléments de $\mathfrak{U}$ sont de déterminant 1, les $T_r(x^{-1})$ s'expriment comme polynomes en les $T_r(x)$.

Soient maintenant r et s des racines positives linéairement indépendantes. Désignons par $\mathfrak{a} = \mathfrak{a}(r, s)$ l'espace vectoriel engendré par les X_{ir+js} pour les couples (i, j) d'entiers $\geqq 0$ tels que $ir + js$ soit une racine. Il est clair que $\mathfrak{a}$ est une sous-algèbre de $\mathfrak{u}$. Appliquant à $\mathfrak{a}$ le résultat que nous venons de citer, on voit que l'on a des formules de la forme

$$x_r(t)x_s(u)x_r^{-1}(t) = \Pi_{i,j} x_{ir+js}(W_{ij;r,s}(t, u)),$$

où le produit est étendu aux couples (i, j) d'entiers $\geqq 0$ tels que $ir + js$ soit une racine, ces couples étant arrangés dans un ordre tel que la suite des racines $ir + js$ soit croissante, et où les $W_{ij;r,s}$ sont des polynomes que nous nous proposons déterminer.

Puisque $x_r(t)$ est un automorphisme de $\mathfrak{g}$, on a

$$\begin{aligned} x_r(t)x_s(u)x_r^{-1}(t) &= \exp u(x_r(t)(\mathrm{ad}X_s)x_r^{-1}(t)) \\ &= \exp u(\mathrm{ad}x_r(t)\cdot X_s) = \exp u(\mathrm{ad}X_s + \textstyle\sum_{i=1}^{l} M_{r,s,i}t^i(\mathrm{ad}X_{ir+s})). \end{aligned}$$

Soit $\mathfrak{a}'$ l'espace vectoriel engendré par les X_{ir+js} pour les couples (i, j) tels que $i > 0, j > 1$ et que $ir + js$ soit racine. C'est évidemment un idéal de $\mathfrak{a}$; de

plus, l'espace $\mathfrak{a}_1'$ engendré par $\mathfrak{a}'$, $X_s \ldots, X_{qr+s}$ est une sous-algèbre de $\mathfrak{a}$ et $\mathfrak{a}_1'/\mathfrak{a}'$ est abélien. Soient $\mathfrak{N}$ et $\mathfrak{N}'$ les sous-groupes de Γ dont les algèbres de Lie sont les images $\mathrm{ad}_{\mathfrak{g}}\mathfrak{a}$, $\mathrm{ad}_{\mathfrak{g}}\mathfrak{a}'$ de $\mathfrak{a}$, $\mathfrak{a}'$ par la représentation adjointe de $\mathfrak{g}$; $\mathfrak{N}'$ est donc un sous-groupe distingué de $\mathfrak{N}$. Il est clair que l'on a

$$\exp u(\mathrm{ad}\, X_s + \sum_{i=1}^{q} M_{r,s,i}t^i(\mathrm{ad}X_{ir+s})) = x_s(u)\left(\prod_{i=1}^{q} x_{ir+s}(M_{r,s,i}t^i)\cdot\right)y, \qquad y \in \mathfrak{N}'.$$

L'élément y peut se mettre sous la forme d'un produit $\Pi x_{ir+js}(t_{ij})$, produit étendu aux racines $ir+js$ telles que $i>0, j>1$. Or ces racines, s'il y en a, sont toujours supérieures aux racines $ir+s$. En effet, si l'ensemble Σ des racines qui sont combinaisons linéaires de r et s est un système admissible qui n'est pas de type (G_2), et s'il y a au moins une racine $ir+js$ avec $i>0$, $j>1$, cette racine est $r+2s$, et les seules racines de Σ sont $\pm r$, $\pm s$, $\pm(r+s)$, $\pm(r+2s)$ (lemme 2, §I). Supposons maintenant que Σ soit de type $\pm(G_2)$. Il y a alors un système fondamental de racines de Σ, soit $\{a,b\}$, tel que les racines positives de Σ, relativement à ce système, soient $a, b, a+b$, $2a+b$, $3a+b, 3a+2b$, que r soit l'une des racines a, b et que s soit une combinaison à coefficients $\geqq 0$ de a, b (Lemme 1, §I). Si $r=a$ et s'il y a des entiers $i>0$, $j>1$ tels que $ir+js$ soit racine, cette racine ne peut être que $3r+2s$, et $s=b$; si $r=b$, on a $q=1$, et notre assertion est évidente dans ce cas. On en conclut que

$$W_{0,1;r,s}(t,u)=u\,;\ W_{i,1;r,s}=M_{r,s,i}t^i u \qquad (1\leqq i\leqq q).$$

Pour calculer $W_{ij;r,s}$ quand $j>1$, nous utiliserons la formule

$$\exp(\xi+\eta)=(\exp\xi)(\exp\eta)(\exp -(1/2)[\xi,\eta]), \tag{4}$$

valable quand ξ, η sont des endomorphismes d'un espace vectoriel tels que $[\xi,[\xi,\eta]]=[\eta,[\xi,\eta]]=0$. Si Σ n'est pas de type (G_2) et si $r+2s$ est racine, notre formule donne

$$x_r(t)x_s(u)x_r^{-1}(t)=x_s(u)x_{r+s}(M_{r,s,1}tu)x_{r+2s}(-(1/2)M_{r,s,1}N_{s,r+s}tu^2);$$

on notera que $M_{r,s,1}=N_{r,s}=-N_{s,r}$, d'où $-(1/2)M_{r,s,1}N_{s,r+s}=M_{s,r,2}$.

Supposons maintenant que Σ soit de type (G_2), utilisons les mêmes notations que plus haut. Si $r=a$, $s=b$, on observera que les crochets $[[X,X'],X'']$, où X, X', X'' sont pris parmi $s, r+s, 2r+s, 3r+s$ sont tous nuls. Une première application de la formule (4) donne alors pour $x_r(t)x_s(u)x_r^{-1}(t)$ la valeur

$$(\exp u(\mathrm{ad}X_s+\sum_{i=1}^{2}M_{r,s,i}t^i(\mathrm{ad}\,X_{ir+s}))x_{3r+s}(M_{r,s,3}t^3u)\cdot (\exp -(1/2)M_{r,s,3}N_{s,3r+s}t^3u^2(\mathrm{ad}\,X_{3r+2s})).$$

Par ailleurs, X_s commute avec X_{r+s} et X_{2r+s}; une seconde application de notre formule donne alors la valeur

$$x_s(u)x_{r+s}(M_{r,s,1}tu)x_{2r+s}(M_{r,s,2}t^2u)x_{3r+2s}(-(1/2)\,M_{r,s,1}M_{r,s,2}N_{r+s,2r+s}t^3u^2)\cdot x_{3r+s}(M_{r,s,3}t^3u)x_{3r+2s}\,(-(1/2)M_{r,s,3}N_{s,3r+s}t^3u^2).$$

De plus, $x_{3r+2s}(\tau)$ commute avec $x_{3r+s}(\tau')$, quels que soient τ, τ', et nous

obtenons par suite

$$W_{3,2}(t, u) = -(1/2)(M_{r,s,1}M_{r,s,2}N_{r+s,2r+s} + M_{r,s,3}N_{s,3r+s})t^3u^2.$$

On notera que $M_{r,s,1} = N_{r,s} = \pm 1$, $M_{r,s,2} = (1/2)N_{r,s}N_{r,r+s}$, $= \pm 1$, $N_{r+s,2r+s} = \pm 3$, $M_{r,s,3} = (1/6)N_{r,s}N_{r,r+s}N_{r,2r+s} = \pm 1$ et $N_{s,3r+s} = \pm 1$; $M_{r,s,1}M_{r,s,2}N_{r+s,2r+s} + M_{r,s,3}N_{s,3r+s}$ est donc un nombre pair. Supposons maintenant que $r = b$. S'il y a des entiers $i > 0, j > 1$ tels que $ir + js$ soit racine, on a $s = a$. On a

$$x_a^{-1}(u)x_b(t)x_a(u)$$
$$= x_{a+b}(W_{1,1}(t, u))x_{2a+b}(W_{1,2}(t, n))x_{3a+b}(W_{1,3}(t, u))x_{3a+2b}(W_{2,3}(t, u))x_b(t).$$

Or, $x_b(t)$ commute avec $x_{a+b}(t_1)$, $x_{2a+b}(t_2)$, $x_{3a+2b}(t_3)$ quels soient t_1, t_2, t_3, et on a

$$x_b^{-1}(t)x_{3a+b}(W_{1,3}(t, u))x_b(t)$$
$$= x_{3a+b}(W_{1,3}(t, u))x_{3a+2b}(-tN_{b,3a+b}W_{1,3}(t, u)).$$

Il vient donc

$$x_a^{-1}(u)x_b(t)x_a(u) = x_b(t)x_{a+b}(W_{1,1}(t, u))x_{2a+b}(W_{1,2}(t, u))x_{3a+b}(W_{1,3}(t, u))\cdot$$
$$x_{3a+2b}(W_{2,3}(t, u) - tN_{b,3a+b}W_{1,3}(t, u)).$$

Comparant avec la formule que nous avons déjà obtenue dans le cas où $r = a$, il vient

$$W_{1,1}(t, u) = -M_{a,b,1}tu = -M_{s,r,1}tu$$
$$W_{1,2}(t, u) = M_{s,r,2}tu^2\ W_{1,3}(t, u) = -M_{s,r,s}tu^3$$
$$W_{2,3}(t, u) = Ct^2u^3 - N_{b,3a+b}M_{s,r,3}t^2u^3,$$

où $C = (1/2)(M_{s,r,1}M_{s,r,2}N_{r+s,r+2s} + M_{s,r,3}N_{r,3s+r})$.

En résumé, on a le résultat suivant : on a

$$x_r(t)x_s(u)x_r^{-1}(t) = x_s(u)\prod_{i,j} x_{ir+js}(C_{ij;rs}t^iu^j), \tag{5}$$

où le produit est étendu aux couples d'entiers $i > 0, j > 0$ tels que $ir + js$ soit une racine, ces couples étant rangés dans un ordre tel que les $ir + js$ forment une suite croissante de racines ; les $C_{ij;r,s}$ sont des entiers, et on a

$$C_{i,1;r,s} = M_{r,s,i}\ , \qquad C_{1j;r,s} = (-1)^jM_{s,r,j}.$$

La forme de ce résultat et le fait que les $C_{ij;r,s}$ sont entiers auraient pu être prévus *a priori* sans calculs ; mais nous aurons besoin par la suite de connaître les valeurs de certaines des constantes $C_{ij;r,s}$.

On notera que la structure d'ordre sur P_r n'intervient dans la formule (5) que par l'intermédiaire de l'ordre dans lequel doivent être rangés les facteurs du produit. Etant données deux racines linéairement indépendantes quelconques, il y a toujours une structure de groupe ordonné sur P_r relativement à laquelle ces deux racines sont positives (lemme 1, §I) ; on en conclut que la formule (5) est valable pour tout couple (r, s) de racines linéairement indépendantes pourvu qu'on range les facteurs du produit de telle manière que, dans une relation d'ordre sur P_r relativement à laquelle r, s sont positives, les racines $ir + js$ soient rangées par ordre de grandeur croissante.

Formons une base $(X_1, \ldots, X_\nu)$ de $\mathfrak{g}$ composée d'une base $(H_1, \ldots, H_l)$ du

groupe $\mathfrak{h}$ des co-poids et des éléments X_r pour toutes les racines. Pour toute racine r, il existe alors une matrice $A_r(T)$, dont les coefficients sont des polynomes en une lettre T à coefficients entiers, tels que, pour tout $t \in \mathbf{C}$, la matrice qui représente $x_r(t)$ par rapport à notre base soit $A_r(t)$: cela résulte immédiatement des formules (1), (2) ci-dessous et du fait que le groupe $\mathfrak{h}$ est le groupe engendré par les H_r pour toutes les racines r. Soit $A_r(T) = (A_{r;ij}(T))$; soient par ailleurs c_{ijk} les constantes de structure de $\mathfrak{g}$ relatives à la base $(X_1, \ldots, X_v)$. Les $x_r(t)$ étant des automorphismes de $\mathfrak{g}$, on a

$$\sum_{i',j'} c_{i'j'k'} A_{r;ii'}(T) A_{r;jj'}(T) = \sum_k c_{ijk} A_{r;kk'}(T) \tag{6}$$

quels que soient les indices i, j, k'.

Il est clair que l'on a l'identité

$$A_r(T + T') = A_r(T) A_r(T'), \tag{7}$$

et que, si r, s sont deux racines linéairement indépendantes, on a l'identité

$$A_r(T) A_s(U) A_r^{-1}(T) = A_s(U) \prod_{i,j} A_{ir+js}(C_{ij;r,s} T^i U^j), \tag{8}$$

avec la même convention que plus haut relativement à l'ordre dans lequel doivent être rangés les facteurs du produit.

Soit $(a_1, \ldots, a_l)$ un système fondamental de racines; pour toute racine r, soit $r = \sum_{i=1}^{l} c_i a_i$. Introduisons l indeterminées $Z_1, \ldots, Z_l$, et posons, pour toute racine r, $Z_r = \prod_{i=1}^{l} Z_i^{c_i}$. Soit H la matrice diagonale dans laquelle le coefficient situé dans la i-ième ligne et la i-ième colonne est 1 si X_i est l'un des éléments $H_1, \ldots, H_r$ et Z_r si $X_i = X_r$. On a alors l'identité

$$H A_r(T) H^{-1} = A_r(Z_r T). \tag{9}$$

Soient en effet $z_1, \ldots, z_l$ des nombres complexes $\neq 0$ quelconques; si $r = \sum_{i=1}^{l} c_i a_i$ est une racine, soit $z_r = \prod_{i=1}^{l} z_i^{c_i}$. Soit h l'automorphisme de l'espace vectoriel $\mathfrak{g}$ qui laisse les éléments de $\mathfrak{h}$ fixes et qui transforme X_r en $z_r X_r$ pour toute racine r. Si $r, s, r+s$ sont des racines, on a $z_{r+s} = z_r z_s$, et on a $z_r z_{-r} = 1$ pour toute racine r. Il en résulte immédiatement que h est un automorphisme de l'algèbre de Lie $\mathfrak{g}$. On en conclut que

$$h x_r(t) h^{-1} = \exp ht(\mathrm{ad} X_r) h^{-1} = \exp t(\mathrm{ad} h.\ X_r) = \exp t z_r X_r;$$

la formule (9) résulte immédiatement de là.

Si r est une racine quelconque, désignons maintenant par $\mathfrak{g}_r$ la sous-algèbre de $\mathfrak{g}$ admettant (X_{-r}, H_r, X_r) comme base. Soit Γ_r le sous-groupe analytique de Γ dont l'algèbre de Lie est l'image $\mathrm{ad}_{\mathfrak{g}} \mathfrak{g}_r$ de $\mathfrak{g}_r$ par la représentation adjointe de $\mathfrak{g}$. Soit $\mathfrak{sl}(2; \mathbf{C})$ l'algèbre de Lie du groupe $SL(2; \mathbf{C})$ des matrices de degré 2 et de déterminant 1 à coefficients complexes. Cette algèbre admet une base (N', D, N) composée des matrices

$$N' = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

et on a $[D, N] = 2N, [D, N'] = -2N', [N, N'] = D$. Il y a donc un isomorphisme φ_r de $\mathfrak{sl}(2; \mathbf{C})$ sur $\mathfrak{g}_r$ qui applique N' sur X_{-r}, D sur H_r, N sur X_r. Le groupe $SL(2; \mathbf{C})$ étant simplement connexe, il y a un épimorphisme ϕ_r de ce groupe sur Γ_r dont la différentielle est φ_r. On a

$$\phi_r\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} = x_{-r}(t), \quad \phi_r\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} = x_r(t).$$

Par ailleurs, si z est un nombre complexe $\neq 0$, l'image par ϕ_r de le matrice

$$A(z) = \begin{pmatrix}z & 0\\ 0 & z^{-1}\end{pmatrix}$$

est l'automorphisme de $\mathfrak{g}$ qui laisse fixes les éléments de $\mathfrak{h}$ et qui transforme X_s en $z^{s(H_r)}X_s$ pour toute racine s. Nous nous proposons de montrer qu'il existe une matrice $F_r(Z_{11}, Z_{12}, Z_{21}, Z_{22})$ dont les coefficients sont des polynomes à coefficients entiers en les variables Z_{ij} et qui possède la propriété suivante : si $z_{11}, z_{12}, z_{21}, z_{22}$ sont des nombres complexes tels que $z_{11}z_{22} - z_{12}z_{21} = 1$, $F_r(z_{11}, z_{12}, z_{21}, z_{22})$ est la matrice qui représente l'automorphisme

$$\phi_r\begin{pmatrix}z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix}$$

par rapport à la base $(X_1, \ldots, X_\nu)$ de $\mathfrak{g}$ que nous avons choisie plus haut. Soit s une racine linéairement indépendante de r telle que $s - r$ ne soit pas racine ; désignons par q le plus grand entier tel que $s + qr$ soit une racine et par $\mathfrak{g}_{r;s}$ l'espace vectoriel engendré par $X_s, X_{r+s}, \ldots, X_{qr+s}$. Il est clair que les opérations de Γ_r appliquent $\mathfrak{g}_{r;s}$ dans lui-même ; si $\zeta \in SL(2; \mathbf{C})$, nous désignerons par $\phi_{r;s}(\zeta)$ la restriction de $\phi_r(\zeta)$ à $\mathfrak{g}_{r;s}$. Soit par ailleurs $\mathfrak{g}_0$ l'espace vectoriel engendré par $H_1, \ldots, H_l, H_r, X_r, X_{-r}$, et, soit $\phi_{r;0}(\zeta)$ la restriction de $\phi_r(\zeta)$ à $\mathfrak{g}_0$. L'espace $\mathfrak{g}$ est somme directe de $\mathfrak{g}_0$ et des espaces $\mathfrak{g}_{r;s}$ pour toutes les racines s linéairement indépendantes de r et telles que $s - r$ ne soit pas racine. Il suffira donc d'établir les faits suivants : il existe des matrices $F_{r;s}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$, $F_{r;0}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$ dont les coefficients sont des polynomes à coefficients entiers en les variables Z_{ij} tels que les conditions suivantes soient satisfaites : si

$$\zeta = \begin{pmatrix}z_{11} & z_{12}\\ z_{21} & z_{22}\end{pmatrix}$$

est une matrice quelconque de $SL(2; \mathbf{C})$, alors pour toute racine s satisfaisant aux conditions énoncées plus haut, $F_{r;s}(z_{11}, z_{12}, z_{21}, z_{22})$ est la matrice qui représente $\phi_{r;s}(\zeta)$ relativement à la base $(X_s, X_{r+s}, \ldots, X_{qr+s})$ de $\mathfrak{g}_{r;s}$ et $F_{r;0}(z_{11}, z_{12}, z_{21}, z_{22})$ est la matrice qui représente $\phi_{r;0}(\zeta)$ par rapport à la base $(H_1, \ldots, H_l, X_r, X_{-r})$ de $\mathfrak{g}_0$.

Commençons par établir l'existence de la matrice $F_{r;s}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$. Introduisons deux variables T, U ; q étant le plus grand entier tel que $s + qr$ soit racine, désignons par $\mathfrak{G}_q$ l'espace des formes homogènes de degré q en T, U à coefficients dans $\mathbf{C}$. C'est l'espace d'une représentation $\phi'_{r;s}$ de $SL(2; \mathbf{C})$ qui associe à ζ la restriction à $\mathfrak{G}_q$ de l'automorphisme de l'anneau $\mathbf{C}[T, U]$ des polynomes en T, U qui transforme T en $z_{11}T + z_{12}U$, U en

$z_{21}T + z_{22}U$. Nous allons montrer que $\phi'_{r;s}$ est équivalente à $\phi_{r;s}$. Il suffit de montrer que les différentielles $d\phi_{r;s}$ et $d\phi'_{r,s}$ des représentations $\phi_{r;s}$ et $\phi'_{r;s}$ sont des représentations équivalentes de $\mathfrak{sl}(2; \mathbf{C})$. On a

$$(d\phi_{r;s})(N).X_{ir+s} = N_{r,ir+s}X_{(i+1)r+s} \text{ si } 0 \leqq i < q$$
$$(d\phi_{r;s})(N)\cdot X_{qr+s} = 0$$
$$(d\phi_{r;s})(N')\cdot X_{ir+s} = N_{-r,ir+s}\ X_{(i-1)r+s} \text{ si } 0 < i \leqq q$$
$$(d\phi_{r;s})(N')\cdot X_s = 0.$$

Posons par ailleurs $\tau_i = C_q^i T^{1-i}U^i$ $(0 \leqq i \leqq q)$, les C_q^i étant les coefficients binomiaux. On a alors

$$(d\phi'_{r;s})(N)\cdot\tau_i = (i+1)\ \tau_{i+1} \text{ si } 0 \leqq i < q$$
$$(d\phi'_{r;s})(N)\cdot\tau_q = 0$$
$$(d\phi'_{r,s})(N')\cdot\tau_i = (q-i+1)\ \tau_{i-1} \text{ si } 0 < i \leqq q$$
$$(d\phi'_{r,s})(N')\cdot\tau_0 = 0.$$

Or on sait que $N_{r,ir+s} = \varepsilon_i(i+1)$, ε_i étant un nombre égal à ± 1. Par ailleurs, il résulte de la formule (5), §I que $N_{r,(i-1)r+s}N_{-r,ir+s} = (q-i+1)i$ $(0 < i \leqq q)$, d'où $N_{-r,ir+s} = \varepsilon_{i-1}(q-i+1)$. Comme $\mathfrak{sl}(2; \mathbf{C})$ est engendré par N' et N, on voit que l'isomorphisme de $\mathfrak{g}_s$ sur $\mathfrak{G}_q$ qui applique X_s sur τ_0 et X_{ir+s} sur $\varepsilon_1 \ldots \varepsilon_{i-1}\ \tau_i$ $(0 < i \leqq q)$ est encore un isomorphisme quand on considère $\mathfrak{g}_s$ et $\mathfrak{G}_q$ comme des espaces de représentation de $\mathfrak{sl}(2; \mathbf{C})$, et par suite aussi quand on les considère comme espaces de représentation de $SL(2; \mathbf{C})$. Or on voit facilement que les coefficients de la matrice qui représente $\phi'_{r,s}(\zeta)$ par rapport à la base $(\tau_0, \ldots, \tau_q)$ de $\mathfrak{G}_q$ s'expriment comme polynomes homogènes de degré q à coefficients entiers en z_{11}, z_{12}, z_{21}, z_{22} [On peut par exemple observer que les formes de degré q à coefficients entiers dont toutes les dérivées partielles d'ordre q sont divisibles par $q!$ sont les combinaisons linéaires à coefficients entiers des τ_i]. L'existence de la matrice $F_{r;s}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$ est donc établie; et on voit que l'on peut supposer les coefficients de cette matrice tous homogènes du même degré.

Pour établir l'existence de la matrice $F_{r;0}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$, observons que l'espace $\mathfrak{g}_0$ est somme directe de $\mathfrak{g}_r$ et de l'espace $\mathfrak{h}'$ composé des $H' \in \mathfrak{h}$ tels que $r(H') = 0$ (comme il résulte tout de suite de ce que $r(H_r) = 2 \neq 0$). Désignons par $\phi^*_{r;0}(\zeta)$ la restriction de $\phi_{r;0}(\zeta)$ à $\mathfrak{g}_r$; il est alors clair que l'isomorphisme de $\mathfrak{sl}(2; \mathbf{C})$ sur $\mathfrak{g}_r$ qui applique N' sur X_{-r}, D sur H_r et N sur X_r est un isomorphisme quand on considère $\mathfrak{sl}(2; \mathbf{C})$ comme espace de la représentation adjointe de $SL(2; \mathbf{C})$ et $\mathfrak{g}_r$ comme l'espace de la représentation $\phi^*_{r;0}$. On en déduit les formules

$$\phi_r(\zeta)\cdot X_{-r} = z_{22}^2 X_{-r} + z_{12}z_{22}H_r - z_{12}^2 X_r$$
$$\phi_r(\zeta)\cdot H_r = 2z_{21}z_{22}X_{-r} + (z_{11}z_{22} + z_{12}z_{21})H_r - 2z_{11}z_{12}X_r$$
$$\phi_r(\zeta)\cdot X_r = -z_{21}^2 X_{-r} - z_{11}z_{21}H_r + z_{11}^2 X_r.$$

Ecrivons maintenant $H_i = \rho_i H_r + H_i$, $H_i' \in \mathfrak{h}'$; il vient alors

$$\phi_r(\zeta)\cdot H_i = 2\rho_i z_{21}z_{22}X_{-r} + 2\rho_i z_{12}z_{21}H_r - 2\rho_i z_{11}z_{12}X_r + (z_{11}z_{22} - z_{12}z_{21})H_i$$

(on se souviendra que $z_{11}z_{22} - z_{12}z_{21} = 1$). Or on observera que $2\rho_i$ est entier;

on a en effet $2\rho_i = r(H_i)$, et H_i est un co-poids. Comme H_r est une combinaison linéaire à coefficients entiers de $H_1, \ldots, H_l$, on en conclut que les coefficients de la matrice qui représente $\phi_{r;0}(\zeta)$ par rapport à la base $(H_1, \ldots, H_l, X_r, X_{-r})$ peuvent s'exprimer comme polynomes homogènes de degré 2 à coefficients entiers en les z_{ij}. L'existence de la matrice $F_{r;0}(Z_{11}, Z_{12}, Z_{21}, Z_{22})$ est donc établie, et on voit qu'on peut supposer les coefficients de cette matrice tous homogènes de degré 2.

Nous supposerons les matrices $F_{r;s}, F_{r;0}$ choisies de telle manière que chacune d'elles ait tous ses coefficients homogènes du même degré. Soient $Z'_{11}, Z'_{12}, Z'_{21}, Z'_{22}$ quatre nouvelles variables, et soit $Z''_{ij} = \sum_{k=1}^{2} Z_{ik}Z'_{kj}$. Les coefficients de la matrice

$$F_{r;s}(Z''_{11}, Z''_{12}, Z''_{21}, Z''_{22}) - F_{r;s}(Z_{11}, Z_{12}, Z_{21}, Z_{22})F'_{r;s}(Z'_{11}, Z'_{12}, Z'_{12}, Z'_{22})$$

sont des polynomes dont chacun est séparément homogène par rapport aux deux séries de variables Z_{ij} et Z_{ij}; de plus, ces polynomes s'annulent quand on y donne aux arguments des valeurs z_{ij}, z'_{ij} telles que $z_{11}z_{22} - z_{12}z_{21} = 1$, $z'_{11}z'_{22} - z'_{12}z'_{21} = 1$. Il en résulte tout de suite que ces polynomes sont identiquement nuls. La même remarque s'applique à la matrice $F_{r;0}$. On en conclut que

$$F_r(Z'_{11}, Z''_{12}, Z''_{21}, Z''_{22}) = F_r(Z_{11}, Z_{12}, Z_{21}, Z_{22})\ F_r(Z'_{11}, Z'_{12}, Z'_{21}, Z_{22}). \tag{10}$$

Il est clair que

$$F_r(1, 0, T, 1) = A_r(T)\ , \quad F_r(1, T, 0, 1) = A_{-r}(T). \tag{11}$$

Posons

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \omega_r = \phi_r(\Omega).$$

Si $\mathfrak{h}'$ est l'espace, déjà considéré plus haut, composé des $H' \in \mathfrak{h}$ tels que $r(H') = 0$, ω_r laisse les éléments de $\mathfrak{h}'$ fixes puisque $\omega_r \in \Gamma_r$. Par ailleurs, il résulte des formules écrites plus haut que $\omega_r \cdot H_r = -H_r$; l'automorphisme ω_r de $\mathfrak{g}$ applique donc l'espace $\mathfrak{h}$ dans lui-même. Soit s une racine quelconque; si nous posons $s'(H) = s(\omega_r^{-1} \cdot H)$, on a $[H, \omega_r \cdot X_s] = s'(H)\ \omega_r \cdot X_s$ pour tout $H \in \mathfrak{h}$, on en conclut que la fonction s' est une racine et que $\omega_r \cdot X_s$ est un élément radiciel attaché à cette racine. Par ailleurs, on a $H = H' + (1/2)r(H)H_r$ avec $H' \in \mathfrak{h}'$, et par suite $\omega_r^{-1} \cdot H = H' - (1/2)r(H)H_r = H - r(H)H_r$, d'où $s' = s - s(H_r)r$: c'est l'image de s par la symétrie w_r par rapport à la racine r. La matrice qui représente ω_r par rapport à la base $(X_1, \ldots, X_\nu)$ de $\mathfrak{g}$ est $F_r(0, 1, -1, 0)$, qui est à coefficients entiers; on a donc $\omega_r . X_s = \eta_s X_{w_r(s)}$, où η_s est un entier. Puisque ω_r^4 est l'identité, les entiers η_s sont tous égaux à ± 1. On a $\omega_r x_s(t)\omega_r^{-1} = \exp t(\mathrm{ad}\ \omega_r \cdot X_s) = x_{w_r(s)}(\eta_s t)$, d'où la formule

$$F_r(0, 1, -1, 0)A_s(T)F_r^{-1}(0, 1, -1, 1) = A_{w_r(s)}(\eta_s T). \tag{11}$$

Enfin, si Z est une indeterminée, $F_r(Z, 0, 0, Z^{-1})$ est la matrice diagonale dont le coefficient situé à l'intersectioin de la i-ième ligne et de la i-ième colonne est 1 si X_i est l'un des éléments $H_1, \ldots, H_l$ et est $Z^{s(Hr)}$ si $X_i = X_s$.

§III. Le groupe G.

Soit de nouveau $\mathfrak{g}$ une algèbre de Lie semi-simple sur le corps des nombres complexes. Nous utiliserons au début de ce § les même notations qu'aux §I, II. Nous désignerons par $\mathfrak{g}_{\mathbf{Z}}$ le groupe additif engendré par le groupe $\mathfrak{h}$ des co-poids et par les éléments X_r pour toutes les racines r; nous supposerons choisie une base $(X_1, \ldots, X_p)$ de ce groupe composée d'une base $(H_1, \ldots, H_l)$ de $\mathfrak{h}$ et des X_r. Il est clair que le crochet de deux éléments de $\mathfrak{g}_{\mathbf{Z}}$ est dans $\mathfrak{g}_{\mathbf{Z}}$; $\mathfrak{g}_{\mathbf{Z}}$ peut donc être considéré comme une algèbre de Lie sur l'anneau $\mathbf{Z}$ des entiers rationnels. L'ensemble $\mathfrak{g}_{\mathbf{Z}}$ dépend de $\mathfrak{h}$ et des éléments X_r; mais il résulte tout de suite du théorème 1, §I que la structure d'algèbre de Lie de $\mathfrak{g}_{\mathbf{Z}}$ sur $\mathbf{Z}$ ne dépend que de $\mathfrak{g}$.

Soit maintenant K un corps quelconque, dont nous désignerons quelquefois l'élément unité par 1_K. Le produit tensoriel de groupes additifs $K \otimes \mathfrak{g}_{\mathbf{Z}}$ admet évidemment une structure d'algèbre de Lie sur K; nous poserons

$$\mathfrak{g}_K = K \otimes \mathfrak{g}_{\mathbf{Z}}, \quad \mathfrak{h}_K = K \otimes \mathfrak{h},$$

$$H_r^* = 1_K \otimes H_r, \quad X_r^* = 1_K \otimes X_r, \quad H_i^* = 1_K \otimes H_i, \quad X_i^* = 1_K \otimes X_i.$$

Les éléments $X_1^*, \ldots, X_p^*$ forment une base de $\mathfrak{g}_K$; $\mathfrak{h}_K$ s'identifie canoniquement à un sous-espace de $\mathfrak{g}_K$ et admet une base composée des éléments H_i^*. L'espace $\mathfrak{g}_K$ est somme direct de $\mathfrak{h}_K$ et d'un espace vectoriel admettant une base composée des X_r^* pour toutes les racines r. On a

$$[H_i^*, H_j^*] = 0 \ (1 \leqq i, j \leqq l) \quad [H_i^*, X_r^*] = r(H_i) X_r^*$$

$$[X_r^*, X_s^*] = 0 \text{ si } r + s \text{ n'est pas une racine}$$

$$[X_r^*, X_s^*] = N_{r,s} X_{r+s}^* \text{ si } r + s \text{ est une racine.}$$

Il convient d'observer que l'on peut avoir $[X_r^*, X_s^*] = 0$ même si $r + s$ est une racine: c'est ce qui se produit si $N_{r,s}$ est un multiple de la caractéristique de K; cette circonstance ne peut se présenter que si $s - r$ est une racine.

LEMME 1. *Si r est une racine, H_r fait partie d'au moins une base de $\mathfrak{h}$; on a $H_r^* \neq 0$; $\mathfrak{h}_K$ est sous-tendu par les H_r^* (par toute les racines).*

Pour établir la première assertion, nous observerons que r fait partie d'au moins un système fondamental de racines $\{a_1, \ldots, a_l\}$ de $\mathfrak{g}$ (lemme 1, §I). Or on sait qu'il existe des poids $u_1, \ldots, u_l$ de représentations de $\mathfrak{g}$ tels que l'on ait $u_i(H_{a_j}) = \delta_{ij}$ $(1 \leqq i, j \leqq l)$: ce sont les poids fondamentaux de E. Cartan (Cf. [6], theorem 1, p. 30). Si m est un entier > 0 tel que $m^{-1}H_r \in \mathfrak{h}$, et si $r = a_1$, on a $1 = mu_1(m^{-1}H_r)$, d'où $m = 1$ puisque u_1 ne prend que des valeurs entières sur $\mathfrak{h}$. On sait qu'il en résulte que H_r fait partie d'une base de $\mathfrak{h}$. La seconde assertion du lemme 1 résulte immédiatement de la première. La dernière assertion résulte du fait que $\mathfrak{h}$ est engendré par les H_r.

Cependant, il convient d'observer que, si r, s sont des racines linéairement indépendantes, il peut fort bien se produire que $H_r^* = H_s^*$, bien que H_r, H_s soient linéairement indépendants.

Soit χ un homomorphisme du groupe additif P_r engendré par les racines de $\mathfrak{g}$ dans le groupe multiplicatif K^* des éléments $\neq 0$ de K. Nous désignerons

par $h(\chi)$ l'automorphisme de l'espace vectoriel $\mathfrak{g}_K$ qui laisse fixes les éléments de $\mathfrak{h}_K$ et qui transforme X_r^* en $\chi(r)X_r^*$ pour toute racine r. Il résulte tout de suite des formules écrites plus haut que $h(\chi)$ est un automorphisme de l'algèbre de Lie $\mathfrak{g}_K$. L'application $\chi \to h(\chi)$ est un isomorphisme du groupe des homomorphismes de P_r dans K^* avec un groupe d'automorphismes de $\mathfrak{g}_K$; nous désignerons ce groupe par $\mathfrak{H}$. Pour toute racine r, $A_r(T)$ est une matrice dont les coefficients sont des polynomes à coefficients entiers en la lettre T; si $t \in K$, on peut substituer t à T dans les coefficients de la matrice $A_r(T)$; on obtient ainsi une matrice à coefficients dans K, que nous désignerons par $A_r(t)$. Nous désignerons par $x_r^*(t)$ l'endomorphisme de l'espace vectoriel $\mathfrak{g}_K$ qui est représenté par la matrice $A_r(t)$ relativement à la base $(X_1^*, \ldots, X_\nu^*)$. Il est clair que $A_r(0)$ est la matrice unité; $x_r^*(0)$ est donc l'automorphisme identique de $\mathfrak{g}_K$. Il résulte de la formule (7), §II que l'on a

$$x_r^*(t+t') = x_r^*(t)x_r^*(t') \qquad (t, t' \in K).$$

Par ailleurs, si les c_{ijk} sont les constantes de structure de $\mathfrak{g}$ relativement à la base $(X_1, \ldots, X_\nu)$, les $c_{ijk} \cdot 1_K$ sont celles de $\mathfrak{g}_K$ relativement à la base $(X_1^*, \ldots, X_\nu^*)$; il résulte alors de la formule (6), §II et de la formule que nous venons d'écrire que l'application $t \to x_r^*(t)$ est un homomorphisme du groupe additif de K dans le groupe des automorphismes de l'algèbre de Lie $\mathfrak{g}_K$. Il résulte de la formule (8), §II que l'on a, si r et s sont des racines linéairement indépendantes,

$$x_r^*(t)x_s^*(u)x_r^{*-1}(t) = x_s^*(u) \prod_{i,j} x_{ir+js}^*(C_{ij;r,s}t^i u^j)$$

où le produit est étendu aux couples d'entiers $i > 0, j > 0$ tels que $ir + js$ soit une racine, ces couples étant rangés dans un ordre tel que les $ir + js$ forment une suite croissante de racines quand on munit P_r d'une structure de groupe ordonné telle que r, s soient des racines positives.

Soit χ un homomorphisme de P_r dans K^*. Montrons que l'on a

$$h(\chi)x_r^*(t)(h(\chi))^{-1} = x_r^*(\chi(r)t).$$

Soit en effet H^ϵ la matrice qui se déduit de la matrice H introduite au §II en y substituant aux arguments $Z_1, \ldots, Z_l$ les valeurs $\chi(a_1), \ldots, \chi(a_l)$; si on fait cette substitution dans Z_r, on obtient $\chi(r)$ puisque χ est un homomorphisme. Notre formule résulte alors immédiatement de la formule (9), §II.

Soit maintenant

$$\zeta = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

un élément du groupe $SL(2; K)$ des matrices de degré 2 et de déterminant 1 à coefficients dans K. Nous désignerons par $\phi_r^*(\zeta)$ l'endomorphisme de l'espace vectoriel $\mathfrak{g}_K$ qui est représenté, relativement à la base $(X_1^*, \ldots, X_\nu^*)$, par la matrice $F_r(z_{11}, z_{12}, z_{21}, z_{22})$. Il résulte des formules (11), §II que

$$\phi_r^* \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = x_{-r}^*(t); \quad \phi_r^* \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = x_r^*(t).$$

En particulier, ϕ_r^* applique la matrice unité sur l'automorphisme identique

de $\mathfrak{g}_K$. Il résulte de la formule (10), §II que

$$\phi_r^*(\xi\xi') = \phi_r^*(\xi)\, \phi_r^*(\xi')$$

quels que soient ξ et ξ' dans $SL(2; K)$. Faisant usage de la remarque terminale du §II, on voit que, si z est un élément $\neq 0$ de K, on a

$$\phi_r^* \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} = h(\chi_r)$$

où χ_r est l'homomorphisme de P_r dans K^* tel que $\chi_r(s) = z^{s(Hr)}$ pour toute racine s.

Nous désignerons par Ω^* la matrice

$$\Omega^* = \begin{pmatrix} 0 & 1_K \\ -1_K & 0 \end{pmatrix}$$

de $SL(2; K)$. Nous désignerons par $\mathfrak{N}$ et $\mathfrak{N}'$ les sous-groupes de $SL(2; K)$ formés des matrices

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \qquad (t \in K)$$

respectivement, et par $\mathfrak{D}$ le groupe des matrices diagonales de $SL(2; K)$.

LEMME 2. *Le groupe $SL(2; K)$ est réunion des ensembles disjoints $\mathfrak{D}\mathfrak{N}$ et $\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$; $\mathfrak{D}\mathfrak{N} = \mathfrak{N}\mathfrak{D}$ est un groupe admettant $\mathfrak{N}$ comme sous-groupe distingué. On a $\Omega^*\mathfrak{N}\Omega^{*-1} = \mathfrak{N}'$. Le groupe $SL(2; K)$ est aussi réunion des ensembles disjoints $\mathfrak{N}'\mathfrak{D}\mathfrak{N}$ et $\mathfrak{N}'\Omega^*\mathfrak{D}\mathfrak{N} = \Omega^*\mathfrak{D}\mathfrak{N}$. On a $SL(2;K) = \mathfrak{N}'\mathfrak{D}\mathfrak{N}\mathfrak{N}'$; $\mathfrak{N} \cup \mathfrak{N}'$ est un ensemble de générateurs de $SL(2; K)$.*

On a, si $a \in K^*$, $t \in K$,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & at \\ 0 & a^{-1} \end{pmatrix};$$

il en résulte que $\mathfrak{D}\mathfrak{N}$ est l'ensemble des matrices de $SL(2; K)$ dont les coefficients $(2, 1)$ sont nuls : c'est un groupe. L'application

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \to a$$

est manifestement un homomorphisme de $\mathfrak{D}\mathfrak{N}$ sur le groupe K^*, et le noyau de cet homomorphisme est $\mathfrak{N}$, ce qui montre que $\mathfrak{N}$ est un sous-groupe distingué de $\mathfrak{D}\mathfrak{N}$, d'où $\mathfrak{D}\mathfrak{N} = \mathfrak{N}\mathfrak{D}$. On a

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & t' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -at & -att' + a^{-1} \\ -a & -at' \end{pmatrix},$$

il résulte tout de suite de cette formule que $\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$ n'a aucun élément en commun avec $\mathfrak{D}\mathfrak{N}$ et que, réciproquement, toute matrice de $SL(2; K)$ qui n'est pas dans $\mathfrak{D}\mathfrak{N}$ est dans $\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$. On a

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix},$$

ce qui montre que $\Omega^*\mathfrak{N}\Omega^{*-1} = \mathfrak{N}'$. Le groupe $SL(2;K)$ est la réunion des ensembles disjoints $\Omega^*\mathfrak{D}\mathfrak{N}$ et $\Omega^*\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$. Or on a $\Omega^*\mathfrak{D}\mathfrak{N} = \Omega^*\mathfrak{N}\mathfrak{D}\mathfrak{N} = \mathfrak{N}'\Omega^*\mathfrak{D}\mathfrak{N}$; par ailleurs, on a $\Omega^{*-1} = -\Omega^*$, $-\mathfrak{D} = \mathfrak{D}$, d'où $\Omega^*\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N} = \Omega^*\mathfrak{N}\Omega^{*-1}\,\mathfrak{D}\mathfrak{N} =$

$\mathfrak{N}'\mathfrak{D}\mathfrak{N}$. Si $\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$ était contenu dans $\Omega^*\mathfrak{D}\mathfrak{N}$, $\mathfrak{D}\mathfrak{N}$ contiendrait $\mathfrak{N}'\mathfrak{D}\mathfrak{N}$, et *a fortiori*, $\mathfrak{N}'$, ce qui n'est manifestement pas le cas. Donc $\mathfrak{N}\Omega^*\mathfrak{D}\mathfrak{N}$ rencontre $\mathfrak{N}'\mathfrak{D}\mathfrak{N}$, et Ω^* appartient à $\mathfrak{N}^{-1}\mathfrak{N}'(\mathfrak{D}\mathfrak{N})(\mathfrak{D}\mathfrak{N})^{-1} = \mathfrak{N}\mathfrak{N}'\mathfrak{D}\mathfrak{N}$; il en résulte que $\mathfrak{N}\Omega^*\cdot\mathfrak{D}\mathfrak{N} \subset \mathfrak{N}\mathfrak{N}\mathfrak{N}'\mathfrak{D}\mathfrak{N}\mathfrak{D}\mathfrak{N} = \mathfrak{N}\mathfrak{N}\mathfrak{D}\mathfrak{N} = \mathfrak{N}\mathfrak{D}\mathfrak{N}'\mathfrak{N}$ (car on voit comme plus haut que $\mathfrak{N}'\mathfrak{D} = \mathfrak{D}\mathfrak{N}'$); ce dernier ensemble, contenant aussi $\mathfrak{D}\mathfrak{N}$, est identique à $SL(2; K)$ tout entier. Comme $\Omega^*\mathfrak{N}\Omega^{*-1} = \mathfrak{N}'$, $\Omega^*\mathfrak{N}'\Omega^{*-1} = \mathfrak{N}$, $\Omega^*\mathfrak{D}\Omega^{*-1} = \mathfrak{D}$, on a aussi $SL(2; K) = \mathfrak{N}'\mathfrak{D}\mathfrak{N}\mathfrak{N}'$. Pour montrer que $\mathfrak{N} \cup \mathfrak{N}'$ est un ensemble de générateurs de $SL(2; K)$, il suffit de montrer que $\mathfrak{D}$ est dans le groupe engendré par cet ensemble; c'est ce qui résulte de la formule

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-1}-1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ a^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix}.$$

Ceci dit, il résulte des formules écrites plus haut que les opérations de $\phi_r^*(\mathfrak{N})$, $\phi_r^*(\mathfrak{N}')$ sont des automorphismes de l'algèbre $\mathfrak{g}_K$. On en conclut que ϕ_r^* est un homomorphisme de $SL(2; K)$ dans le groupe des automorphismes de $\mathfrak{g}_K$. Faisant usage des formules établies au §II, on voit que, si

$$\zeta = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

est une matrice quelconpue de $SL(2; K)$, on a

$$\begin{aligned} \phi_r^*(\zeta).\, X_{-r}^* &= z_{22}^2 X_{-r}^* + z_{12}z_{22}H_r^* - z_{12}^2 X_r^* \\ \phi_r^*(\zeta).\, H_r^* &= 2z_{21}z_{22}X_{-r}^* + (z_{11}z_{22} + z_{12}z_{21})H_r^* - 2z_{11}z_{12}X_r^* \\ \phi_r^*(\zeta).\, X_r^* &= -z_{21}^2 X_{-r}^* - z_{11}z_{21}H_r^* + z_{11}^2 X_r^*. \end{aligned}$$

Il résulte de ces formules que le noyau de ϕ_r^* ou bien se compose de la seule matrice unité I ou bien se compose de I et de $-I$.

Nous poserons $\omega_r^* = \phi_r^*(\Omega^*)$. Puisque la matrice Ω est à coefficients entiers, il est clair que ω_r^* est le produit tensoriel de l'application identique de K et de l'automorphisme de $\mathfrak{g}_Z$ induit par ω_r. Or, il résulte immédiatement des définitions que l'opération induite par ω_r sur $\mathfrak{h}$ est la symétrie par rapport à la racine r (cet élément du groupe de Weyl étant considéré comme opérant sur $\mathfrak{h}$); soit w_r cette opération. On a donc $\omega_r(H_s) = H_{w_r(s)}$ pour toute racine s, et par suite $\omega_r^*(H_s^*) = H_{w_r(s)}^*$. Par ailleurs, on sait que ω_r transforme X_s en $\eta_s X_{w_r(s)}$, η_s étant un entier égal à ± 1; il résulte de la formule (12), §II que

$$\omega_r^* x_s^*(t)\omega_r^{*-1} = x_{w_r(s)}^*(\eta_s t) \quad (t \in K).$$

Nous allons maintenant modifier quelque peu les notations que nous venons d'introduire. Les éléments $H_1^*, \ldots, H_l^*, H_r^*, X_r^*$ seront dorénavant désignés par $H_1, \ldots, H_l, H_r, X_r$; nous n'utiliserons donc plus ces dernières notations pour désigner les éléments de l'algèbre de Lie complexe $\mathfrak{g}$ qu'ils désignaient jusqu'ici. Cette règle souffre cependant une exception: si u est un élément du groupe P engendré par les poids, nous désignerons encore par $u(H_r)$ la valeur que u prend en l'élément H_r de $\mathfrak{g}$. Cette notation ne produira pas de confusion, car nous ne considérerons jamais les éléments de P comme des fonctions définies sur $\mathfrak{h}_K$. Les algèbres $\mathfrak{g}_K$ et $\mathfrak{h}_K$ seront désignées par $\mathfrak{g}$ et $\mathfrak{h}$ tandisque l'algèbre de Lie complexe $\mathfrak{g}$ sera désignée par $\mathfrak{g}_c$. Si $t \in K$, l'opération $x_r^*(t)$ sera désignée par $x_r(t)$; le groupe formé des $x_r(t)$ pour

tous les $t \in K$ sera désigné par $\mathfrak{X}_r$. L'homomorphisme ϕ_r^* de $SL(2; K)$ dans le groupe des automorphismes de $\mathfrak{g}$ sera désigné par ϕ_r; l'opération ω_r^* sera désignée par ω_r, la matrice Ω^* sera désignée par Ω.

Nous allons énoncer ci-dessous les propriétés déjà acquises des objets que nous venons d'introduire.

L'algèbre $\mathfrak{g}$ est somme directe de $\mathfrak{h}$ et d'un espace vectoriel qui admet une base composée des X_r pour toutes les racines r; $\mathfrak{h}$ est engendré en tant qu'espace vectoriel par les H_r pour toutes les racines r, et ces éléments sont tous $\neq 0$. Si r, s sont des racines, on a $[H_r, H_s] = 0$, $[H_r, X_s] = s(H_r)X_s$. On a $[X_r, X_{-r}] = H_r$. Si r, s sont des racines linéairement indépendantes, on a $[X_r, X_s] = N_{r,s}X_{r+s}$ si $r + s$ est une racine; et $N_{r,s} = \pm (p + 1)$ si p est le plus grand entier tel que $s - pr$ soit une racine; si $r + s$ n'est pas une racine, on a $[X_r, X_s] = 0$.

Les opérations de $\mathfrak{X}_r$ sont des automorphismes de $\mathfrak{g}$, et $t \to x_r(t)$ est un épimorphisme du groupe additif de K sur $\mathfrak{X}_r$. On a

$$x_r(t)\cdot X_{-r} = X_{-r} + tH_r - t^2X_r\,;\quad x_r(t)\cdot H_r = H_r - 2tX_r\,;\quad x_r(t)\cdot X_r = X_r \tag{1}$$

et, si s est une racine linéairement indépendante de r,

$$x_r(t)\cdot X_s = X_s + \sum_{i=1}^{q} M_{r,s,i}t^iX_{ir+s} \tag{2}$$

où q est le plus grand entier tel que $qr + s$ soit une racine et où les entiers $M_{r,s,i}$ sont définis par les formules

$$M_{r,s,i} = (i!)^{-1}\prod_{j=0}^{i-1} N_{r,jr+s}. \tag{3}$$

Si r et s sont des racines linéairement indépendantes, on a

$$x_r(t)x_s(u)x_r^{-1}(t) = x_s(u)\prod_{i,j} x_{ir+js}(C_{ij;r,s}t^iu^j)\ (t, u \in K) \tag{4}$$

où le produit est étendu aux couples (i, j) d'entiers > 0 tels que $ir + js$ soit une racine, ces couples étant arrangés dans un ordre tel que les racines $ir + js$ forment une suite croissante relativement à une structure de groupe ordonné sur P_r pour laquelle r et s sont positives. Les $C_{ij;r,s}$ sont des entiers et on a

$$C_{i1;r,s} = M_{r,s,i}\quad C_{1j;r,s} = (-1)^jM_{s,r,j}. \tag{5}$$

Si à tout homomorphism χ de P_r dans le groupe K^* des éléments $\neq 0$ de K on fait correspondre l'automorphisme $h(\chi)$ de l'espace $\mathfrak{g}$ qui laisse fixes les éléments de $\mathfrak{h}$ et qui transforme X_r en $\chi(r)X_r$ pour toute racine r, on obtient un isomorphisme du groupe des homomorphismes de P_r dans K^* sur le groupe $\mathfrak{H}$ d'automorphismes de $\mathfrak{g}$. Si r est une racine et $t \in K$, on a

$$h(\chi)x_r(t)h^{-1}(\chi) = x_r(\chi(r)t). \tag{6}$$

L'application ϕ_r est un homomorphisme de $SL(2; K)$ sur un groupe d'automorphismes de $\mathfrak{g}$. On a

$$\phi_r\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} = x_{-r}(t),\ \phi_r\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} = x_r(t).$$

Si $\omega_r = \phi_r(\Omega)$, on a $\omega_r\cdot X_s = \eta_sX_{w_r(s)}$ pour toute racine s, w_r étant la symétrie par rapport à la racine r et η_s un nombre égal à ± 1. On a $\omega_r(H_s) = H_{w_r(s)}$ et $\omega_rX_s\omega_r^{-1} = X_{w_r(s)}$. On a, si z est un élément $\neq 0$ de K,

$$\phi_r\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} = h(\chi_r) \tag{7}$$

où χ_r est l'homomorphisme de P_r dans K^* tel que $\chi_r(u) = z^{u(H_r)}$ pour tout $u \in P_r$.

Nous désignerons par G le groupe engendré par $\mathfrak{H}$ et par tous les groupes $\mathfrak{X}_r$; les opérations de G sont donc des automorphismes de $\mathfrak{g}$. Il résulte immédiatement du lemme 2 que $\phi_r(SL(2; K))$ est contenu dans G, quelle que soit la racine r.

Il est facile de montrer que la structure du groupe G ne dépend que de celle de l'algèbre semi-simple complexe dont nous sommes partis (et, bien entendu, du corps K); nous ne donnerons pas ici la démonstration détaillée de ce fait, pour ne pas alourdir l'exposé.

LEMMA 3. *Soit $\mathfrak{W}$ le groupe engendré par $\mathfrak{H}$ et par les éléments ω_r, pour toutes racines r. Il existe alors un épimorphisme ζ et un seul de $\mathfrak{W}$ sur le groupe de Weyl W qui possède la propriété suivante: si $\omega \in \mathfrak{W}$ et $w = \zeta(\omega)$, on a $\omega \cdot X_r \in KX_{w(r)}$ pour toute racine r. On a alors $\omega\, \mathfrak{X}_r\, \omega^{-1} = \mathfrak{X}_{w(r)}$, et*

$$\omega\, h(\chi)\omega^{-1} = h(\chi')$$

pour tout homomorphisme χ de P_r dans K^*, où χ' est l'homomorphisme de P_r dans K^* défini par $\chi'(r) = \chi(w^{-1}(r))$ pour toute racine r. Le noyau de l'homomorphisme ζ est $\mathfrak{H}$.

Il est clair que tout élément qui est soit l'un des ω_r soit un élément de $\mathfrak{H}$ permute entre eux les sous-espaces KX_r de $\mathfrak{g}$. Il existe donc un homomorphisme ζ de $\mathfrak{W}$ dans le groupe des permutations des racines tel que $\omega \cdot X_r \in KX_{w(r)}$ pour toute racine r, si $\omega \in \mathfrak{W}$ et $\zeta(\omega) = w$. Si $h \in \mathfrak{H}$, on a $h \cdot X_r \in KX_r$ pour toute racine r, ce qui montre que $\mathfrak{H}$ est contenu dans le noyau de ζ. Il est clair que $\zeta(\omega_r)$ est la symétrie par rapport à la racine r; $\zeta(\mathfrak{W})$ est donc le groupe engendré par les symétries par rapport aux racines, c'est-à-dire le groupe de Weyl. Soit ω un élément quelconque de $\mathfrak{W}$ et soit $w = \zeta(\omega)$. Soit s une racine quelconque. Les formules

$$\omega\, \mathfrak{X}_s \omega^{-1} = \mathfrak{X}_{w(s)} \quad \omega \cdot H_s = H_{w(s)}$$

sont vraies si ω est l'un quelconque des éléments ω_r ou est un élément de $\mathfrak{H}$; elles sont donc vraies pour tout élément de $\mathfrak{W}$. Soit χ un homomorphisme de P_r dans K^*; soit $s' = w^{-1}(s)$; on a

$$\omega h(\chi)\omega^{-1} \cdot X_s = \omega h(\chi) c^{-1} X_{s'} = \chi(s') X_s$$

où c est l'élément de K tel que $\omega \cdot X_{s'} = cX_s$. Par ailleurs, il résulte de la formule $\omega \cdot H_s = H_{w(s)}$ que ω permute entre eus lex éléments de $\mathfrak{h}$, donc que $\omega h(\chi)\omega^{-1}$ laisse les éléments de $\mathfrak{h}$ fixes; on a donc bien $\omega\, h(\chi)\omega^{-1} = h(\chi')$, où χ' est défini comme dans l'énoncé. Cette formule prouve que $\mathfrak{H}$ est un sous-groupe distingué de $\mathfrak{W}$. Soit maintenant ω un élément du noyau de ζ. Pour montrer que $\omega \in \mathfrak{H}$, il suffit évidemment de montrer qu'il en est ainsi dans le cas où ω peut s'écrire comme produit d'un certain nombre d'éléments ω_r. Or on a $\omega_r \cdot X_s = \pm X_{w_r(s)}$, si w_r est la symétrie par rapport à la racine r; on a donc $\omega \cdot X_s = c(s)X_s$ pour toute racine s, $c(s)$ étant égal à ± 1. Par ailleurs,

il résulte de la formule $\omega \cdot H_s = H_{w(s)}$ que ω laisse les éléments de $\mathfrak{h}$ fixes. Si K est de caractéristique 2, ω est l'identité, et notre assertion est vraie dans ce cas. Supposons donc que K ne soit pas de caractéristique 2. Pour toute racine r, on a $[X_r, X_{-r}] = H_r$; ω étant un automorphisme de $\mathfrak{g}$, et H_r étant $\neq 0$, il en résulte que $c(r)c(-r) = 1$. Soient maintenant r et s des racines telles que $r + s$ soit une racine. Il résulte de la formule $[X_r, X_s] = N_{r,s}X_{r+s}$ et du fait que ω est un automorphisme de $\mathfrak{g}$ que $c(r)c(s)N_{r,s} = c(r + s)N_{r,s}$, d'où $c(r + s) = c(r)c(s)$ si $N_{r,s}$ n'est pas divisible par la caractéristique de K. Or, $N_{r,s} = \pm(p + 1)$, où p est le plus grand entier tel que $s - pr$ soit racine ; et, $r + s$ étant une racine, on a $p \leqq 2$. Si donc $N_{r,s}$ est divisible par la caractéristique de K, cette dernière est 3, et $s - 2r$ est racine. Il en résulte que $s + 2r = (s + r) - (-r)$ n'est pas racine, donc que $N_{-r,r+s} = \pm 1$ et $c(s + r)c(-r) = c(s)$; comme $c(-r) = (c(r))^{-1}$, la formule $c(r + s) = c(r)c(s)$ est vraie dans tous les cas. Soit maintenant $F = \{a_1, \ldots, a_l\}$ un système fondamental de racines, et soit $r = \sum_{i=1}^{l} e_i a_i$ une racine > 0. Il existe alors une suite finie $(r_1, \ldots, r_h)$ de racines telle que $r_1 \in F$, $r_i - r_{i-1} \in F$ $(2 \leqq i \leqq h)$ et $r_h = r$ (lemme 4, §I). Comme $c(r_i) = c(r_{i-1})c(r_i - r_{i-1})$ $(2 \leqq i \leqq h)$, on en déduit tout de suite que $c(r) = \prod_{i=1}^{l} (c(a_i))^{e_i}$. Soit χ l'homomorphisme de P_r dans K^* tel que $\chi(a_i) = c(a_i)(i = 1, \ldots, l)$ (on se souviendra que les a_i forment une base de P_r) ; on a donc $\chi(r) = c(r)$ pour toute racine $r > 0$, et par suite aussi pour toute racine r, en vertu de la formule $c(r)c(-r) = 1$. Il en résulte que $\omega = h(\chi)$, ce qui achève la démonstration du lemme 3.

Nous supposerons dorénavant choisie une fois pour toutes une structure régulière de groupe ordonné sur P_r. Il correspond à cette structure un système fondamental de racines ; les racines de ce système seront appelées les *racines fondamentales*. Nous désignerons par $\mathfrak{U}$ (resp. : $\mathfrak{V}$) le sous-groupe de G engendré par les groupes $\mathfrak{X}_r$ relatifs aux racines r positives (resp. : négatives).

LEMME 4. *Le groupe G est engendré par le groupe $\mathfrak{H}$ et les groupes $\mathfrak{X}_a$, $\mathfrak{X}_{-a}$ pour les racines fondamentales a.*

Soit G_0 le groupe engendré par $\mathfrak{H}$ et par les $\mathfrak{X}_a, \mathfrak{X}_{-a}$. Il résulte du lemme 2 que, pour toute racine fondamentale a, $\mathfrak{X}_a \cup \mathfrak{X}_{-a}$ est un ensemble de générateurs de $\phi_a(SL(2 ; K))$; on en conclut que $\omega_a \in G_0$. L'image de $G_0 \cap \mathfrak{W}$ par ζ contient donc les symétries par rapport aux racines fondamentales ; or ces dernières engendrent le groupe de Weyl W. On en déduit que $\zeta(G_0 \cap \mathfrak{W}) = W$, et par suite que $\mathfrak{W} \subset G_0$, puisque le noyau $\mathfrak{H}$ de ζ est dans G_0. Soit r une racine quelconque ; puisque r appartient à au moins un système fondamental (lemme 1, §I) et puisque les systèmes fondamentaux sont permutés transitivement entre eux par les opérations du groupe de Weyl, il y a un $w \in W$ et une racine fondamentale a tels que $w(a) = r$. Soit ω un élément de $\mathfrak{W}$ tel que $\zeta(\omega) = w$; on a $\omega \mathfrak{X}_a \omega^{-1} = \mathfrak{X}_r$, d'où $\mathfrak{X}_r \subset G_0$ puisque $\omega \in G_0$; le lemme 4 est donc démontré.

Pour toute entier $m > 0$, nous désignerons par $\mathfrak{U}_m$ le groupe engendré

par les $\mathfrak{X}_r$ pour les racines $r > 0$ de heuteurs $\geqq m$.

LEMME 5. *Le groupe* $\mathfrak{U}_m$ *est un sous-groupe distingué de* $\mathfrak{U}$. *Si* m, m' *sont des entiers* > 0, *le commutateur d'un élément de* $\mathfrak{U}_m$ *et de* $\mathfrak{U}_{m'}$ *est dans* $\mathfrak{U}_{m+m'}$. *En particulier,* $\mathfrak{U}_m/\mathfrak{U}_{m+1}$ *est dans le centre de* $\mathfrak{U}/\mathfrak{U}_{m+1}$.

Soient r une racine de hauteur $\geqq m$ et s une racine de hauteur $\geqq m'$; il résulte immédiatement de la formule (4) et du fait que la hauteur de la somme de deux racines est la somme des hauteurs de ces racines que $x_r(t)$ $x_s(u)x_r^{-1}(t) = x_s(u)z$, avec un $z \in \mathfrak{U}_{m+m'}$. En particulier, on a $x_r(t)x_s(u)x_r^{-1}(t) \in \mathfrak{U}_{m'}$, et il en résulte que $\mathfrak{U}_{m'}$ est un sous-groupe distingué de $\mathfrak{U}$. Par ailleurs, il résulte de notre formule tout d'abord que $xx_s(u)x^{-1} \equiv x_s(u) \pmod{\mathfrak{U}_{m+m'}}$ pour tout $x \in \mathfrak{U}_m$, puisque $xx'x^{-1} \equiv x' \pmod{\mathfrak{U}_{m+m'}}$ pour tout $x \in \mathfrak{U}_m$ et tout $x' \in \mathfrak{U}_{m'}$. La dernière assertion du lemme 5 résulte immédiatement de l'avant dernière.

LEMME 6. *Tout élément* x *de* $\mathfrak{U}$ *se met d'une manière et d'une seule sous la forme* $x = \prod_r x_r(t_r)$, *le produit étant étendu aux racines* $r > 0$ *rangées par ordre de grandeur croissante et les* t_r *étant des éléments de* K; *si* m *est un entier* > 0, *une condition nécessaire et suffisante pour que* $x \in \mathfrak{U}_m$ *est que* $t_r = 0$ *pour toute racine* r *de hauteur* $< m$.

Soit I l'élément unité de G; il est clair que $\mathfrak{U}_m = \{I\}$ pour m assez grand. Nous montrerons par récurrence descendante sur m que tout élément de $\mathfrak{U}_m$ se met d'une manière et d'une seule sous la forme $\prod_r x_r(t_r)$, le produit étant étendu aux racines r de hauteurs $\geqq m$ arrangées par ordre de grandeur croissante et les t_r étant des éléments de K. Notre assertion est vraie pour m assez grand. Supposons la vraie pour $m+1$. Il résulte immédiatement du fait que $\mathfrak{U}_m/\mathfrak{U}_{m+1}$ est un groupe abélien et de ce que les $\mathfrak{X}_r$ sont des groupes que tout élément x de $\mathfrak{U}_m$ se met d'au moins une manière sous la forme voulue. Soit $\mathfrak{u}$ l'espace vectoriel sous-tendu par les X_r pour les racines $r > 0$. Il résulte immédiatement des formules (1), (2) et du fait que $\mathfrak{h}$ est sous-tendu par les éléments H_r que $x'(\mathfrak{u}) \subset \mathfrak{u}$, $x' \cdot H \equiv H \pmod{\mathfrak{u}}$ pour tout $x' \in \mathfrak{U}$ et tout $H \in \mathfrak{h}$. Soit r une racine de hauteur m. Si s est une racine de hauteur $> m$, il résulte de la formule (2) que $x_s(t) \cdot X_{-r} \equiv X_{-r} \pmod{\mathfrak{u}}$ pour tout $t \in K$. Si s est une racine de hauteur m mais $\neq r$, $s - r$ n'est pas une racine; en effet, la somme des coefficients de l'expression de $s - r$ comme combinaison linéaire des racines fondamentales est 0, et ces coefficients ne peuvent par suite être ni tous $\geqq 0$ ni tous $\leqq 0$, ce qui démontre notre assertion. Enfin, on a $x_r(t) \cdot X_{-r} \equiv X_{-r} + tH_r \pmod{\mathfrak{u}}$ (par la formule (1)). Il résulte de là que, si $x = \prod_s x_s(t_s)$ (le produit étant étendu aux racines $s > 0$ de hauteurs $\geqq m$, rangées par ordre de grandeur croissante), on a $x \cdot X_{-r} \equiv X_{-r} + t_r H_r \pmod{\mathfrak{u}}$. La somme $KX_{-r} + KH_r + \mathfrak{u}$ étant directe, et H_r étant $\neq 0$, on voit que t_r est univoquement determiné par la donnée de x. La structure de groupe ordonné que nous avons choisie sur P_r étant supposée régulière, toute racine de hauteur m est inférieure à toute racine de hauteur $> m$; on a donc $x =$

$\prod'_s x_s(t_s) \prod''_s x_s(t_s)$, le produit $\prod'$ étant étendu aux racines de hauteur m, rangées par ordre de grandeur croissante, et le produit $\prod''$ aux racines de hauteurs $> m$, rangées par ordre de grandeur croissante. Appliquant l'hypothèse inductive à l'élément $\left(\prod'_s x_s(t_s)\right)^{-1} x \in \mathfrak{U}_{m+1}$, on voit que les t_s relatifs aux racines s de hauteurs $> m$ sont également déterminés de maniére unique par la donnée de x. Le lemme 6 est donc démontré.

Les notations étant celles du lemme 6, nous poserons

$$T_r(x) = t_r.$$

Les T_r sont donc des fonctions sur $\mathfrak{U}$ à valeurs dans K, et $\mathfrak{U}_m$ se compose des $x \in \mathfrak{U}$ tels que $T_r(x) = 0$ pour toute racine $r > 0$ de hauteur $< m$.

LEMME 7. *Si a est une racine fondamentale, T_a est un épimorphisme de $\mathfrak{U}$ sur le groupe additif de K.*

Cela résulte immédiatement du fait que $\mathfrak{U}/\mathfrak{U}_2$ est abélien. Nous désignerons le noyau de T_a par $\mathfrak{U}_a$.

LEMME 8. *Si r est une racine positive, a une racine fondamentale $\neq r$, i un entier (de signe quelconque) et s un entier > 0 tels que $ia + jr$ soit une racine, cette racine est positive. Si $y \in \mathfrak{X}_{-a}$, on a $y\mathfrak{U}_a y^{-1} = \mathfrak{U}_a$.*

Soient $a = a(1), \ldots . a(l)$ les racines fondamentales, et $r = \sum_{k=1}^{l} c_k a(k)$. Tenant compte de ce que $r \neq a$ et de ce que ca n'est pas une racine si $c \neq \pm 1$, on voit qu'il y a au moins un $k > 1$ tel que $c_k > 0$. Comme le coefficient de $a(k)$ dans l'expression de $ia + jr$ comme combinaison des racines fondamentales est jc_k, il en résulte que $ia + jr > 0$. On a d'ailleurs $ia + jr \neq a$, puisque a et r sont linéairement indépendantes. Il résulte alors de la formule (4) que, si $y \in \mathfrak{X}_{-a}$, $yx_r(t)y^{-1} \in \mathfrak{U}_a$ pour tout $t \in K$; ceci démontre la seconde assertion du lemme 8.

LEMME 9. *L'ensemble $\mathfrak{H}\mathfrak{U} = \mathfrak{U}\mathfrak{H}$ est un groupe contenant $\mathfrak{U}$ comme sous-groupe distingué.*

Cela résulte immédiatement de la formule (6).

LEMME 10. *On a $G = \mathfrak{U}\mathfrak{W}\mathfrak{U}$.*

Faisant usage du lemme 4, on voit qu'il suffit de montrer que $z\mathfrak{U}\mathfrak{W}\mathfrak{U} \subset \mathfrak{U}\mathfrak{W}\mathfrak{U}$ si z est un élément de l'un des groupes $\mathfrak{H}$, $\mathfrak{X}_a$ ou $\mathfrak{X}_{-a}$, a étant une racine fondamentale. Si $z \in \mathfrak{H}$, cela résulte du lemme 9 et de ce que $\mathfrak{H}\mathfrak{W} = \mathfrak{W}$. Si $z \in \mathfrak{X}_a$, c'est évident car $z\mathfrak{U} = \mathfrak{U}$ dans ce cas. Reste à considérer le cas où $z \in \mathfrak{X}_{-a}$. On a $\mathfrak{U} = \mathfrak{U}_a\mathfrak{X}_a$, et par suite $\mathfrak{X}_{-a}\mathfrak{U} = \mathfrak{U}_a\mathfrak{X}_{-a}\mathfrak{X}_a$ (lemme 8). Il suffira donc de montrer que, si $y \in \mathfrak{X}_{-a}$, $x \in \mathfrak{X}_a$, $\omega \in \mathfrak{W}$, $yx\omega$ appartient à $\mathfrak{U}\mathfrak{W}\mathfrak{U}$. Il résulte du lemme 2 et du fait que $\phi_a(\mathfrak{D}) \subset \mathfrak{H}$ que yx appartient à l'un des ensembles $\mathfrak{X}_a\mathfrak{H}$, $\mathfrak{X}_a\omega_a\mathfrak{H}\mathfrak{X}_a = \mathfrak{X}_a\mathfrak{H}\omega_a\mathfrak{X}_a$. Notre assertion est évidente si $yx \in \mathfrak{X}_a\mathfrak{H}$. Sinon, nous distinguerons deux cas suivant que $w^{-1}(a) > 0$ ou $w^{-1}(a) < 0$, w étant $\zeta(\omega)$. Dans le premier cas, on a $\mathfrak{X}_a\omega \subset \omega\mathfrak{U}$, et $yx\omega \in \mathfrak{X}_a\mathfrak{H}\omega_a\omega\mathfrak{U} \subset \mathfrak{U}\mathfrak{W}\mathfrak{U}$.

Dans le second cas, nous écrirons $\omega = \omega_a\omega'$, $\omega' \in \mathfrak{W}$, d'où $w'^{-1}(a) = -w^{-1}(a) > 0$. L'élément $yx\omega_a$ appartient soit à $\mathfrak{X}_a\mathfrak{H}$ soit à $\mathfrak{X}_a\mathfrak{H}\omega_a\mathfrak{X}_a$, et la démonstration s'achève comme dans le cas précédent.

LEMME 11. *Supposons l'ensemble E des racines positives décomposé en deux ensembles disjoints E', E'' tels que, si la somme de deux racines de E' (resp. : E'') est une racine, cette racine soit dans E' (resp:E''). Soit* $\mathfrak{U}'$ *(resp.:* $\mathfrak{U}''$*) l'ensemble des* $x \in \mathfrak{U}$ *tels que* $T_r(x) = 0$ *pour tout* $r \in E''$ *(resp. :* $r \in E'$*):* $\mathfrak{U}'$ *et* $\mathfrak{U}''$ *sont alors des groupes, et on a* $\mathfrak{U} = \mathfrak{U}'\mathfrak{U}''$.

Nous poserons, pour tout $k > 0$, $\mathfrak{U}'_k = \mathfrak{U}_k \cap \mathfrak{U}'$, $\mathfrak{U}''_k = \mathfrak{U}_k \cap \mathfrak{U}''$. Nous allons montrer que $\mathfrak{U}'_k$ et $\mathfrak{U}''_k$ sont des groupes et que $\mathfrak{U}_k = \mathfrak{U}'_k\mathfrak{U}''_k$. Nos assertions sont certainement vraies si k est assez grand. Supposons les vraies pour $k+1$. Soient r une racine de hauteur k appartenant à E' et s une racine de hauteur $k' \geqq k$ appartenant à E'. Montrons que, si i, j sont des entiers $\geqq 0$ tels que $ir + js$ soit une racine, cette racine est dans E'. C'est évident si $i + j = 1$, et cela résulte du lemme 3, §I dans le cas général en procédant par récurrence sur $i + j$. On a donc $x_r(t)x_s(u)x_r^{-1}(t) \equiv x_s(u) \pmod{\mathfrak{U}'_{k+1}}$ quels que soient t et u dans K. On en conclut d'abord que $\mathfrak{X}_r\mathfrak{U}'_{k+1}$ est un groupe, contenant $\mathfrak{U}'_{k+1}$ comme sous-groupe distingué, puis que, si r et s sont toutes deux de hauteur k, $x_r(t)x_s(u) \equiv x_s(u)x_r(t) \pmod{\mathfrak{U}'_{k+1}}$: il en résulte immédiatement que $\mathfrak{U}'_k$ est un groupe. On voit de même que $\mathfrak{U}''_k$ est un groupe. Le groupe $\mathfrak{U}_k/\mathfrak{U}_{k+1}$ étant abélien, il est clair que $\mathfrak{U}_k = \mathfrak{U}'_k\mathfrak{U}''_k\mathfrak{U}_{k+1}$; comme $\mathfrak{U}_{k+1}$ est distingué dans le groupe engendré par $\mathfrak{U}'_k$ et $\mathfrak{U}_{k+1}$, on a $\mathfrak{U}_k = \mathfrak{U}'_k\mathfrak{U}_{k+1}\mathfrak{U}''_k = \mathfrak{U}'_k\mathfrak{U}'_{k+1}\mathfrak{U}''_{k+1}\mathfrak{U}_k' = \mathfrak{U}'_k\mathfrak{U}''_k$. Le lemme 11 résulte immédiatement de là.

On notera que $\mathfrak{U}'$ (resp. : $\mathfrak{U}''$) est le groupe engendré par les $\mathfrak{X}_r$ pour $r \in E'$ (resp. : $r \in E''$).

LEMME 12. *Les notations étant celles du lemme* 11, *supposons de plus donnée une autre représentation de E comme réunion de deux ensembles disjoints* E'_1, E''_1 *tels que si la somme de deux racines de* E'_1 *(resp. :* E''_1*) est une racine, cette racine soit dans* E'_1 *(resp. :* E''_1*). Soit* $\mathfrak{U}'_1$ *le groupe engendré par les* $\mathfrak{X}_r$ *pour* $r \in E'_1$. *Si* $\mathfrak{U}'_1$ *et* $\mathfrak{U}'$ *sont conjugués dans* $\mathfrak{U}$, *ils sont égaux, et* $E'_1 = E'$.

Soit x un élément de $\mathfrak{U}$ tel que $x\mathfrak{U}'x^{-1} = \mathfrak{U}'_1$. Si r est une racine de E', on a $xx_r(1)x^{-1} \in \mathfrak{U}'_1$. Mais cet élément est $\equiv x_r(1) \pmod{\mathfrak{U}_{k+1}}$, si k est la hauteur de r, d'où $T_r(xx_r(1)x^{-1}) = T_r(x_r(1)) = 1$ (car nous supposons que la structure d'ordre sur P_r est régulière) ; cet élément étant $\neq 0$, on a $r \in E'_1$. Puisque $x^{-1}\mathfrak{U}'_1x = \mathfrak{U}'$, on voit de même que $E'_1 \subset E'$, d'où $E'_1 = E'$, $E''_1 = E''$, $\mathfrak{U}'_1 = \mathfrak{U}'$.

Si w est une opération du groupe de Weyl, nous désignerons dans ce qui suit par E'_w (resp. : E''_w) l'ensemble des racines $r > 0$ telles que $w(r) > 0$ (resp. : $w(r) < 0$). Il est clair que E'_w, E''_w sont disjoints, que leur réunion est l'ensemble de toutes les racines > 0 et que si la somme de deux racines de E'_w (resp. : E''_w) est une racine, cette racine est dans E'_w (resp. : E''_w). Nous désignerons par $\mathfrak{U}'_w$ (resp. : $\mathfrak{U}''_w$) le groupe engendré par les $\mathfrak{X}_r$ pour $r \in E'_w$ (resp. : pour $r \in E''_w$). Il résulte alors du lemme 11 que $\mathfrak{U}'_w$ et $\mathfrak{U}''_w$ n'ont que leur élément unité en commun et que

$$\mathfrak{U} = \mathfrak{U}'_w\mathfrak{U}''_w = \mathfrak{U}''_w\mathfrak{U}'_w.$$

De plus, nous choisirons un système de représentants des classes de $\mathfrak{W}$ modulo $\mathfrak{H}$, et nous désignerons par $\omega(w)$ celui de ces représentants pour lequel $\zeta(\omega(w)) = w$, w étant une opération du groupe de Weyl. Il est clair que

$$\omega(w)\mathfrak{U}'_w(\omega(w))^{-1} \subset \mathfrak{U}, \quad \omega(w)\mathfrak{U}''_w(\omega(w))^{-1} \subset \mathfrak{V}.$$

LEMME 13. *Les groupes $\mathfrak{H}\mathfrak{U}$ et $\mathfrak{V}$ n'ont que leur élément unité en commun; il en est de même des groupes $\mathfrak{H}$ et $\mathfrak{U}$.*

Soient h, x, y des éléments de $\mathfrak{H}, \mathfrak{U}, \mathfrak{V}$ tels que $hx = y$. Soit r une racine > 0; désignons par $\mathfrak{x}$ l'espace vectoriel engendré par les X_s pour les racines $s > r$ et par $\mathfrak{y}$ l'espace vectoriel engendré par $\mathfrak{h}$ et par les X_s pour $s < r$. Soit t un élément de K; il est clair que, si s est une racine > 0, $x_s(t)$ applique $\mathfrak{x}$ dans lui-même et applique X_r sur un élément qui lui est congru modulo $\mathfrak{x}$; on a donc $x.X_r \equiv X_r (\mathrm{mod}\ \mathfrak{x})$. Comme $\mathfrak{x}$ est appliqué dans lui-même par les éléments de $\mathfrak{H}$, on a $hx \cdot X_r \equiv h \cdot X_r \ (\mathrm{mod}\ \mathfrak{x})$. Par ailleurs, si s est une racine < 0, on a $x_s(t)(\mathfrak{y}) \subset \mathfrak{y}$ et $x_s(t)$ applique X_r sur un élément qui lui est congru $(\mathrm{mod}\ \mathfrak{y})$; on a donc $y \cdot X_r \equiv X_r \ (\mathrm{mod}\ \mathfrak{y})$. Or, la somme $\mathfrak{y} + KX_r + \mathfrak{x}$ est directe, et $h \cdot X_r$ appartient à KX_r. On en conclut que $x \cdot X_r = y \cdot X_r = h \cdot X_r = X_r$. On voit par un raisonnement entièrement analogue que ces formules sont encore vraies si r est une racine < 0. Comme on a $H_r = [X_r, X_{-r}]$ et que les éléments h, x, y sont des automorphismes de $\mathfrak{g}$, ces opérations sont toutes égales à l'automorphisme identique, ce qui démontre le lemme 13.

THÉORÈME 2. *Le groupe G est la réunion des ensembles $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}''_w$, où w parcourt les éléments du groupe de Weyl. Ces ensembles sont mutuellement disjoints; un élément de $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}''_w$ ne peut se mettre que d'une seule manière sous la forme $xh\omega(w)x''$, avec $x \in \mathfrak{U}$, $h \in \mathfrak{H}$, $x'' \in \mathfrak{U}''_w$.*

Il résulte du lemme 10 que G est la réunion des ensembles $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U} = \mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}'_w\mathfrak{U}'_w$. Or, on a $\omega(w)\mathfrak{U}'_w(\omega(w))^{-1} \subset \mathfrak{U}$, et, en vertu du lemme 9, $\mathfrak{U}\mathfrak{H}\mathfrak{U} = \mathfrak{U}\mathfrak{H}$; G est donc la réunion des ensembles $\mathfrak{U}\mathfrak{H}\omega(w)\mathfrak{U}''_w$. Supposons que $xh\omega(w)x'' = x_1h_1\omega(w_1)x''_1$, où x, x_1 sont dans $\mathfrak{U}$, h, h_1 dans $\mathfrak{H}$, w, w_1 dans le groupe de Weyl et $x'' \in \mathfrak{U}''_w$, $x''_1 \in \mathfrak{U}''_{w_1}$; soit $z = xh\omega(w)x''$. Cherchons les éléments $u \in \mathfrak{U}$ tels que $zuz^{-1} \in \mathfrak{U}$. Pour qu'il en soit ainsi, il faut et suffit que le transformé de $x''ux''^{-1}$ par $\omega(w)$ soit dans $\mathfrak{U}$, puisque $(xh)\mathfrak{U}(xh)^{-1} = \mathfrak{U}$ (lemme 9); or $x''ux''^{-1}$ est dans $\mathfrak{U}$ et peut par suite se mettre sous la forme $u'u''$, $u' \in \mathfrak{U}'_w$, $u'' \in \mathfrak{U}''_w$. Son transformé par $\omega(w)$ est $(\omega(w)u'(\omega(w))^{-1})(\omega(w)u''(\omega(w))^{-1})$, et l'élément $\omega(w)u'(\omega(w))^{-1}$ est dans $\mathfrak{U}$; il est donc nécessaire et suffisant que $\omega(w)u''(\omega(w))^{-1}$ soit dans $\mathfrak{U}$. Mais cet élément est dans $\mathfrak{V}$; tenant compte du lemme 13, on voit que u'' doit être l'élément unité, c'est-à-dire que $x''ux''^{-1}$ doit être dans $\mathfrak{U}'_w$, ou encore que u doit appartenir à $x''^{-1}\mathfrak{U}'_{w}x''$. On a $x''^{-1}\mathfrak{U}'_wx'' = x''^{-1}_1\mathfrak{U}'_{w_1}x''_1$, et les groupes $\mathfrak{U}'_w, \mathfrak{U}'_{w_1}$ sont conjugués dans $\mathfrak{U}$. Il résulte du lemme 12 que cela implique $E'_w = E'_{w_1}$, $E''_w = E''_{w_1}$. Soit r une racine > 0 quelconque. Si $w^{-1}(r) > 0$, on a $w^{-1}(r) \in E'_w = E'_{w_1}$, et par suite $(w_1w^{-1})(r)$

> 0, si $w^{-1}(r) < 0$, on a $-w^{-1}(r) \in E''_w = E''_{w_1}$ et par suite $(w_1 w^{-1})(r) > 0$. Donc l'opération $w_1 w^{-1}$ du groupe de Weyl permute entre elles les racines positives ; on sait qu'il en résulte que $w_1 w^{-1}$ est l'identité (§I, IX), d'où $w_1 = w$. Posons $y = \omega(w)x''(\omega(w))^{-1}$, $y_1 = \omega(w)x_1''(\omega(w))^{-1}$; y et y_1 sont donc dans $\mathfrak{V}$, et on a $xhy = x_1 h_1 y_1$, d'où $(x_1 h_1)^{-1} x h = y_1 y^{-1}$. Le membre de gauche de cette formule est dans $\mathfrak{H}\mathfrak{U}$ (lemme 9), et celui de droite dans $\mathfrak{V}$; les deux membres sont donc égaux à l'élément unité (lemme 13). On a donc $y = y_1$, d'où $x'' = x_1'$. Par ailleurs, on a $x_1 h_1 = xh$, d'où $x^{-1}x_1 = hh_1^{-1}$ et par suite $x = x_1$, $h = h_1$ en vertu du lemme 13. Le théorème 2 est donc démontré.

COROLLAIRE 1. *Le groupe G est la réunion des ensembles $\mathfrak{V}\mathfrak{H}\omega(w)\mathfrak{U}'_w$, où w parcourt les éléments du groupe de Weyl ; ces ensembles sont mutuellement disjoints, et un éléments de $\mathfrak{V}\mathfrak{H}\omega(w)\mathfrak{U}'_w$ ne se met que d'une seule manière sous la forme $yh\omega(w)x'$, $y \in \mathfrak{V}$, $h \in \mathfrak{H}$, $x' \in \mathfrak{U}'_w$.*

Si a décrit l'ensemble des racines fondamentales, il est clair que l'ensemble des $-a$ est encore un système fondamental de racines ; comme deux systèmes fondamentaux peuvent se transformer l'un en l'autre par une opération du groupe de Weyl, on voit qu'il y a un élément w_0 du groupe de Weyl qui change toute racine positive en une racine négative. Si w est une opération quelconque du groupe de Weyl, posons $w = w_0 w^*$, il est alors clair que $E'_{w^*} = E''_w$, $E''_{w^*} = E'_w$. Le groupe $\mathfrak{H}$ étant un sous-groupe distingué de $\mathfrak{V}$, on a $\mathfrak{H}\omega(w) = \omega(w_0)\mathfrak{H}\omega(w^*)$; par ailleurs, il est clair que $(\omega(w_0))^{-1}\mathfrak{U}$ $\omega(w_0)$ est $\mathfrak{V}$. On conclut alors du théorème 2 que G est la réunion des ensembles $\omega(w_0)\mathfrak{V}\mathfrak{H}\omega(w^*)\mathfrak{U}_w{}^*$, où w^* parcourt les éléments du groupe de Weyl ; de plus, ces ensembles sont mutuellement disjoints, et un élément de $\omega(w_0)$ $\mathfrak{V}\mathfrak{H}\omega(w^*)\mathfrak{U}'_w{}^*$ ne se met que d'une seule manière sous la forme $\omega(w_0)yh\omega(w^*)$ x', avec $y \in \mathfrak{V}$, $h \in \mathfrak{H}$, $x' \in \mathfrak{U}'_w{}^*$; ceci démontre le corollaire 1.

COROLLAIRE 2. *Le normalisateur de $\mathfrak{U}$ est $\mathfrak{U}\mathfrak{H}$.*

Nous savons déjà que ce normalisateur contient $\mathfrak{U}\mathfrak{H}$. Soit z un élément du normalisateur de $\mathfrak{U}$; soit $z = xh\omega(w)x''$, $x \in \mathfrak{U}$, $h \in \mathfrak{H}$, $x'' \in \mathfrak{U}''_w$, w étant une opération du groupe de Weyl. Il est alors clair que $\omega(w)$ appartient au normalisateur de $\mathfrak{U}$. Or, $\omega(w)\mathfrak{X}_r(\omega(w))^{-1}$ est $\mathfrak{X}_{w(r)}$; puisque $\mathfrak{U} \cap \mathfrak{V}$ ne contient que l'élément unité, $\mathfrak{X}_{w(r)}$ ne peut être contenu dans $\mathfrak{V}$ si $r > 0$, d'où alors $w(r) > 0$. L'opération w, qui transforme toute racine positive en une racine positive, est l'identité, d'où $\omega(w) \in \mathfrak{H}$, et par suite $z \in \mathfrak{U}\mathfrak{H}$.

Nous appliquerons les résultats précédents au cas où le corps de base K est le corps des nombres complexes. Le groupe G est alors un groupe semi-simple complexe, d'ailleurs isomorphe à son groupe adjoint. Désignons par $G/\mathfrak{H}$ l'espace homogène des classes à droite de G modulo $\mathfrak{H}$, et par π l'application canonique de G sur $G/\mathfrak{H}$. Il résulte alors du théorème 2 que $G/\mathfrak{H}$ est la réunion des ensembles disjoints $\pi(\mathfrak{U}\omega(w)\mathfrak{U}''_w)$, où w parcourt les éléments du groupe de Weyl, et que, pour w donné, l'application $(x, x'') \to \pi(x\omega(w)x'')$ de $\mathfrak{U} \times \mathfrak{U}''_w$ dans $G/\mathfrak{H}$ est injective. Cette application est évidemment continue ; montrons que c'est un homéomorphisme. On peut écrire $x\omega(w)x'$

$= x\omega(w)x''(\omega(w))^{-1}\cdot\omega(w)$, et $\omega(w)x''(\omega(w))^{-1}$ appartient à $\mathfrak{V}$. L'opération de translation à droite par $\omega(w)$ dans $G/\mathfrak{H}$ étant un homéomorphisme, il suffira d'établir que l'application $(x,y)\to\pi(xy)$ de $\mathfrak{U}\times\mathfrak{V}$ dans $G/\mathfrak{H}$ est un homéomorphisme de $\mathfrak{U}\times\mathfrak{V}$ sur une partie de $G/\mathfrak{H}$. Or, tout point (x_0,y_0) de $\mathfrak{U}\times\mathfrak{V}$ possède un voisinage ouvert A dans $\mathfrak{U}\times\mathfrak{V}$ dont l'adhérence $\bar{A}$ est compacte. Par ailleurs, il résulte du lemme 13 que l'application $(x,y)\to\pi(xy)$ est injective; elle induit donc un homéomorphisme de $\bar{A}$, et par suite de A, sur une partie de $G/\mathfrak{H}$. Par ailleurs, $G/\mathfrak{H}$ et $\mathfrak{U}\times\mathfrak{V}$ sont des variétés de même dimension; l'image de A dans $G/\mathfrak{H}$, qui est homéomorphe à un ensemble ouvert, est donc ouverte, ce qui montre que l'application $(x,y)\to\pi(xy)$ transforme tout ensemble ouvert en un ensemble ouvert, et est par suite un homéomorphisme. On sait par ailleurs que G admet un sous-groupe compact maximal G_c qui contient un sous-groupe compact maximal $\mathfrak{H}_c$ de $\mathfrak{H}$ et qui possède la propriété suivante: il existe un sous-groupe $\mathfrak{H}_a$ de $\mathfrak{H}$ (isomorphe au groupe additif d'une espace vectoriel) tel que tout élément z de G se représente d'une manière et d'une seule sous la forme du produit d'un élément de $\mathfrak{U}\mathfrak{H}_a=\mathfrak{H}_a\mathfrak{U}$ par un élément de G_c; de plus, les deux facteurs du produit dépendent continument de z ([8], lemme 3.11, p. 525). Si $x''\in\mathfrak{U}''_w$, nous pouvons donc trouver un $x\in\mathfrak{U}$ et un seul tel que $\pi(x\omega(w)x'')$ appartienne à $\mathfrak{H}G_c/\mathfrak{H}$. L'application $\varphi_w: x''\to\pi(x\omega(w)x'')$ de $\mathfrak{U}''_w$ dans $\mathfrak{H}G_c/\mathfrak{H}$ est un homéomorphisme. De plus, $\mathfrak{H}G_c/\mathfrak{H}$ est la réunion des $\varphi_w(\mathfrak{U}''_w)$ pour tous les w du groupe de Weyl. Or, désignons par N le nombre des racines >0 et par $N(w)$ le nombre des racines de E''_w. L'espace $\mathfrak{U}''_w$ est alors homéomorphe à $\mathbf{R}^{2N(w)}$ (on sait en effet que tout groupe linéaire sur le corps des complexes dont l'algèbre de Lie se compose d'opérations nilpotentes est homéomorphe à un espace euclidien). On en conclut que l'espace homogène $G_c/\mathfrak{H}_c$ des classes à droite de G_c modulo son sous-groupe toroidal maximal $\mathfrak{H}_c$ se trouve décomposé en "cellules" mutuellement disjointes dont chacune est homéomorphe à un espace $\mathbf{R}^{2N(w)}$. Les dimensions de ces cellules étant paires, un raisonnement topologique facile (dans lequel nous n'entrerons pas ici) montre que le polynome de Poincaré de $G_c/\mathfrak{H}_c$ est

$$P(T)=\sum_{w\in W}T^{2N(w)}.$$

Soit par ailleurs $P_G(T)$ le polynome de Poincaré de G_c, et soit l son rang. On sait alors que

$$P(T)=P_G(T)(T-1)^{-l};$$

on obtient donc la formule

$$P_G(T)=(T-1)^l\sum_{w\in W}T^{2N(w)}.$$

Cette formule permet de retrouver (par une méthode assez compliquée que nous n'exposerons pas ici) les nombres de Betti des groupes simples exceptionnels.

Considérons maintenant le cas où K est un corps fini. Nous désignerons sa caractéristique par p et son nombre d'éléments par q. Il est clair que tout élément différent de l'élément unité de l'un quelconque des groupes $\mathfrak{X}_r$ est d'ordre p, et que $\mathfrak{U},\mathfrak{V}$ sont d'ordre q^N (rappelons que nous désignons par

N le nombre des racines > 0); le groupe $\mathfrak{U}''_w$ est d'ordre $q^{N(w)}$. Le groupe $\mathfrak{H}$ est isomorphe au groupe des homomorphismes de P_r dans le groupe multiplicatif des éléments $\neq 0$ de K; ce dernier étant cyclique d'orde $q-1$, et P_r admettant une base de l éléments (l étant le rang de $\mathfrak{g}$), $\mathfrak{H}$ est d'ordre $(q-1)^l$. L'ordre de G est donc

$$(q-1)^l q^N \sum_{w \in W} q^{N(w)}.$$

On notera que $N(w) = 0$ si (et seulement si) w est l'élément unité du groupe de Weyl; on a donc $\sum_{w \in W} q^{N(w)} \equiv 1 \pmod{q}$, et on en conclut que $\mathfrak{U}, \mathfrak{B}$ *sont des groupes de Sylow de* G.

Soit par ailleurs p' un nombre premier qui divise $q-1$, mais qui ne divise pas l'ordre $[W]$ du groupe de Weyl. La formule $\sum_{w \in W} q^{N(w)} \equiv [W] \pmod{q-1}$ montre que p' ne divise pas $\sum_{w \in W} q^{N(w)}$. On en conclut que, si q' est la plus haute puissance de p' qui divise $q-1$, les groupes de Sylow pour p' sont des produits de l groupes cycliques d'ordre q': ils sont abéliens.

Supposons toujours le corps K fini, et soit $\overline{K}$ un sur-corps de K de degré fini sur K; le groupe de Galois de $\overline{K}/K$ est alors engendré par un certain automorphisme σ. Soient $\overline{G}, \overline{\mathfrak{B}}, \overline{\mathfrak{H}}, \overline{\mathfrak{U}}$ les groupes construits au moyen de $\overline{K}$ comme $G, \mathfrak{B}, \mathfrak{H}, \mathfrak{U}$ l'ont été au moyen de K. Ce sont des groupes d'automorphismes de l'algèbre $\mathfrak{g}_{\overline{K}}$ que l'on peut identifier à l'algèbre déduite de $\mathfrak{g}$ par extension à $\overline{K}$ du corps de base. Nous la désignerons par $\overline{\mathfrak{g}}$. On peut faire opérer σ sur $\overline{\mathfrak{g}}$ de telle manière que $\sigma.(X+Y) = \sigma \cdot X + \sigma \cdot Y$ pour $X, Y \in \overline{\mathfrak{g}}$, $\sigma \cdot X = X$ si $X \in \mathfrak{g}$, $\sigma \cdot (aX) = (\sigma \cdot a)(\sigma \cdot X)$ si $a \in \overline{K}$, $X \in \overline{\mathfrak{g}}$. Pour tout endomorphisme E de $\overline{\mathfrak{g}}$ (considéré comme espace vectoriel sur $\overline{K}$), nous désignerons par E^σ l'endomorphisme défini par $E^\sigma \cdot X = \sigma \cdot E(\sigma^{-1} \cdot X)$. Si r est une racine, nous désignerons par $\overline{x}_r(t)$ (où $\overline{t} \in \overline{K}$) l'élément de $\overline{G}$ defini de la même manière que $x_r(t)$ l'a été dans G. Il est alors clair que $\overline{x}_r(\sigma \cdot \overline{t}) = (\overline{x}_r(\overline{t}))^\sigma$; par ailleurs, si $\overline{t} \in K$, $\overline{x}_r(t)$ est l'automorphisme de $\overline{\mathfrak{g}}$ qui prolonge $x_r(\overline{t})$. Soit χ un homomorphisme de P_r dans le groupe multiplicatif des éléments $\neq 0$ de $\overline{K}$, et soit $\overline{h}(\chi)$ l'automorphisme de $\overline{\mathfrak{g}}$ qui applique X_r sur $\chi(r) X_r$ pour toute racine r et laisse invariants les éléments de $\mathfrak{h}$. Si on désigne par χ^σ l'homomorphisme de P_r défini par $\chi^\sigma(r) = \sigma \cdot \chi(r)$ pour toute racine r, il est clair que $\overline{h}(\chi^\sigma) = (\overline{h}(\chi))^\sigma$. Si $\chi(P_r)$ est contenu dans K, $\overline{h}(\chi)$ est le prolongement à $\overline{\mathfrak{g}}$ d'une opération de $\mathfrak{H}$. Il est clair que l'application $E \to E^\sigma$ transforme chacun des groupes $\overline{\mathfrak{U}}, \overline{\mathfrak{H}}, \overline{\mathfrak{B}}$, donc aussi $\overline{G}$, en lui-meme; de plus, les éléments de $\overline{\mathfrak{U}}$ (resp.: $\overline{\mathfrak{H}}, \overline{\mathfrak{B}}$) qui sont laissés fixes par cette application sont ceux qui prolongent des opérations appartenant à $\mathfrak{U}$ (resp.; $\mathfrak{H}, \mathfrak{B}$). Soit réciproquement $\overline{z}$ un élément de $\overline{G}$ tel que $\overline{z}^\sigma = \overline{z}$. Il est alors clair, en vertu du th. 2 qu'il existe un élément x de $\overline{\mathfrak{U}}$, un élément $\overline{h}$ de $\overline{H}$, une opération w du groupe de Weyl et un élément

$\bar{x}''$ du groupe $\bar{\mathfrak{U}}''_w$ défini dans $\bar{G}$ comme $\mathfrak{U}''_w$ là été dans G tels que $\bar{z} = \bar{x}\bar{h}\,\omega(w)\bar{x}''$, $\omega(w)$ désignant ici l'opération de $\bar{G}$ qui prolonge l'opération de G déjà représentée par ce symbole; de plus, ces éléments sont uniquement déterminés. Or, on a $(\omega(w))^\sigma = \omega(w)$, et $(\bar{\mathfrak{U}}''_w)^\sigma = \bar{\mathfrak{U}}''_w$. On en conclut que $\bar{x}^\sigma = \bar{x}$, $\bar{h}^\sigma = \bar{h}$, $\bar{x}''^\sigma = \bar{x}''$, et par suite que $\bar{z}$ prolonge une opération de G. *Le groupe G est donc isomorphe au groupe des opérations de $\bar{G}$ invariantes par l'automorphisme $\bar{z} \to \bar{z}^\sigma$ de ce groupe.*

Soit p' un nombre premier différent de la caractéristique p de K et ne divisant pas l'order du groupe de Weyl. On peut alors choisir $\bar{K}$ de telle manière que son nombre d'éléments $\bar{q}$ soit $\equiv 1 \pmod{p'}$. Un groupe de Sylow de G pour p' étant isomorphe à un sous-groupe d'un groupe de Sylow de $\bar{G}$ pour p', on voit que: *si p' est différent de la caractéristique de K et ne divise pas l'ordre du groupe de Weyl, les groupes de Sylow de G pour p' sont abéliens.*

Soit maintenant p' un nombre premier distinct de la caractéristique de K mais qui peut diviser l'ordre $[W]$ du groupe de Weyl; nous allons déterminer la contribution de p' à l'ordre $[G]$ du groupe G. Il résulte de la formule de Hirsch-Koszul que le polynome $P(T)$ que nous avons introduit plus haut est de la forme $(T^2-1)^{-l}\prod_{i=1}^{l}(T^{2a(i)}-1)$, les $a(i)$ étant les entiers >0 tels que le polynome de Poincaré de G_c soit $\prod_{i=1}^{l}(T^{2a(i)-1}-1)$. On a $P(1) = \prod_{i=1}^{l} a(i)$; l'expression que nous avons donnée plus haut de $P(T)$ conduit donc immédiatement à la formule, d'ailleurs connue, $\prod_{i=1}^{l} a(i) = [W]$. L'ordre de G est $\prod_{i=1}^{l}(q^{\nu(i)}-1)q^N$. Tout revient donc à calculer la contribution de p' à q^a-1 quand a est un entier >0. Soit f l'indice de q pour p'; il est clair que q^a-1 n'est divisible par p' que si $a \equiv 0 \pmod{f}$. Supposons qu'il en soit ainsi, et posons $a = fb$, $q' = q^f$, d'où $q^a - 1 = q'^b - 1$. Soit $b = b'b''$, où b' est une puissance de p' tandisque b'' n'est pas divisible par p'. On a $q'^b - 1 = (q'^{b'}-1)\sum_{k=0}^{b''-1} q'^{kb'}$. Puisque $q' \equiv 1 \pmod{p'}$, le second facteur est $\equiv b'' \pmod{p'}$ et n'est par suite pas divisible par p'. Tout revient donc à considérer le cas où $b = p'^h$ est une puissance de p'. Soit ζ une racine primitive b-ième de l'unité. On a alors, si $h \geqq 1$,

$$q'^{p^h} - 1 = (q'^{p^{h-1}} - 1)N_{Q(\zeta)/Q}(q' - \zeta)$$

où Q est le corps des rationnels. On a $q' - \zeta = (q'-1) - (\zeta - 1)$. Or l'idéal principal $(\zeta - 1)$ est l'idéal premier unique de $Q(\zeta)$ qui divise p'; soit $\mathfrak{p}$ cet idéal. Si $h > 1$ ou si $h = 1$, $p' > 2$, $\mathfrak{p}$ est ramifié par rapport à Q, et, comme $q'-1$ est divisible par p', donc par $\mathfrak{p}^2$, $q' - \zeta$ est divisible par $\mathfrak{p}$ sans l'être par $\mathfrak{p}^2$. Comme $\mathfrak{p}$ est de degré 1, $N_{Q(\zeta)/Q}(q - \zeta)$ est divisible par p' sans l'être par p'^2. Si donc $p' > 2$, et si on désigne par p'^v la contribution de p' à $q^f - 1$ et par $p'^{\nu(a)}$ la contribution de p' à a (que l'on suppose divisible par f), la contribution de p' à $q^a - 1$ est $p'^{v+\nu(a)}$. On vérifie tout de suite qu'il en est

encore ainsi si $p' = 2$ dans le cas où $q \equiv 1 \pmod 4$ (on a alors $f = 1$). Si par contre $q \equiv 3 \pmod 4$, soit $2^{\nu'}$ la contribution de 2 à $q+1$; la contribution de 2 à $q^a - 1$ est alors $2^{\nu(a)+\nu'-1}$. On conclut de là que, *si p' est un nombre premier qui divise $q-1$, et si p'^{ν} est la contribution de p' à [W] l'ordre d'un groupe de Sylow de G pour p' est $p'^{\nu l+\nu}$, où p'^{ν} est la contribution de p' à $q-1$ dans le cas où ou bien $p' > 2$ ou bein $p' = 2$ et $q \equiv 1 \pmod 4$ et est la contribution de 2 à $(1/2)(q+1)$ si $p' = 2, q \equiv -1 \pmod 4$.*

Le quotient $\mathfrak{B}/\mathfrak{H}$ étant isomorphe au groupe de Weyl, on en déduit que, si $p' > 2$ ou si $p' = 2$, $q + 1 \not\equiv 0 \pmod 8$, et si p' divise $q-1$, tout groupe de Sylow de $\mathfrak{B}$ pour p' est aussi un groupe de Sylow de G pour p'.

§IV. Etude d'un sous-groupe distingue de G

Nous aurons fréquemment à nous servir dans ce qui suit des propriétés du groupe $\mathfrak{B}$ parallèles aux propriétés déjà étudiées du groupe $\mathfrak{U}$, dont elles se déduisent en observant que $\mathfrak{B} = \omega(w_0)\mathfrak{U}(\omega(w_0))^{-1}$ si w_0 est une opération du groupe de Weyl qui change toute racine positive en une racine négative. En particulier, tout élément y de $\mathfrak{B}$ se met d'une manière et d'une seule sous la forme $y = \prod_{r<0} x_r(\tau_r)$, les racines $r < 0$ étant arrangées par ordre de grandeur décroissante et les τ_r des éléments de K; nous poserons $\tau_r = T_r(y)$. Si a est une racine fondamentale, T_{-a} est un homomorphisme de $\mathfrak{B}$ dans le groupe additif de K; nous désignerons son noyau par $\mathfrak{B}_{-a}$. On a donc $\mathfrak{B} = \mathfrak{X}_{-a}\mathfrak{B}_{-a} = \mathfrak{B}_{-a}\mathfrak{X}_{-a}$. Si r est une racine < 0 distincte de $-a$, et i, j des entiers > 0 tels que $ia + jr$ soit racine, cette racine est négative et distincte de $-a$; on en conclut que, si $x \in \mathfrak{X}_a$, on a $x\mathfrak{B}_{-a}x^{-1} = \mathfrak{B}_{-a}$, d'où $\mathfrak{X}_a\mathfrak{B}_{-a} = \mathfrak{B}_{-a}\mathfrak{X}_a$. Pour tout $k > 0$, les éléments $y \in \mathfrak{B}$ tels que $T_r(y) = 0$ pour toute racine $r < 0$ telle que $-r$ soit de hauteur $< k$ forment un sousgroupe distingué $\mathfrak{B}_k$ de $\mathfrak{B}$, et le commutateur d'un élément de $\mathfrak{B}_k$ et d'un élément de $\mathfrak{B}_{k'}$ est dans $\mathfrak{B}_{k+k'}$. L'ensemble $\mathfrak{B}\mathfrak{H} = \mathfrak{H}\mathfrak{B}$ est un groupe; c'est le normalisateur de $\mathfrak{B}$ dans G.

Nous désignerons par G' le sous-groupe de G engendré par $\mathfrak{U}$ et $\mathfrak{B}$. Rappelons que les éléments de $\mathfrak{H}$ sont les applications définies par les formules $H_r \to H_r$, $X_r \to \chi(r)X_r$ (pour toute racine r), où χ est un homomorphisme quelconque du groupe P_r des racines dans le groupe multiplicatif K^* des éléments $\neq 0$ de K. Nous désignerons par $\mathfrak{H}'$ le groupe des éléments de $\mathfrak{H}$ qui correspondent à des homomorphismes χ qui peuvent se prolonger en des homomorphismes du groupe P de tous les poids de représentations de $\mathfrak{g}_C$ dans K^*. Le groupe P_r est un sous-groupe d'indice fini de P; si j est cet indice, la puissance j-ième de tout élément de $\mathfrak{H}$ est dans $\mathfrak{H}'$. Si K est algébriquement clos, on a manifestement $\mathfrak{H} = \mathfrak{H}'$.

LEMME 1. *Si $\mathfrak{D}$ est le groupe des matrices diagonales de $SL(2; K)$, et r une racine quelconque, $\phi_r(\mathfrak{D})$ est contenu dans $\mathfrak{H}'$. Le groupe $\phi_r(SL(2; K))$ est contenu dans G'. Toute classe de $\mathfrak{B}$ modulo $\mathfrak{H}$ contient un élément de G'.*

Si z est un élément $\neq 0$ de K, on a

$$\phi_r \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} = h(\chi_r)$$

où χ_r est l'homomorphisme de P_r dans K^* défini par $\chi_r(s) = z^{s(H_r)}$ pour toute racine s. Cet homomorphisme se prolonge en un homomorphisme de P dans K^* qui applique tout $u \in P$ sur $z^{u(H_r)}$; il en résulte que $\phi_r(\mathfrak{D}) \subset \mathfrak{H}'$. Les notations étant celles du lemme 2, §III, on a $\phi_r(\mathfrak{N}) = \mathfrak{X}_r$, $\phi_r(\mathfrak{N}') = \mathfrak{X}_{-r}$; comme $SL(2; K)$ est engendré par $\mathfrak{N}$ et $\mathfrak{N}'$, on a $\phi_r(SL(2; K)) \subset G'$. On sait que $\phi_r(\Omega) = \omega_r$ est un élément de $\mathfrak{W}$ tel que $\zeta(\omega_r)$ soit la symétrie par rapport à la racine r; par ailleurs, cet élément appartient à G' en vertu de ce qu'on vient de démontrer. Comme les symétries par rapport aux racines engendrent le groupe de Weyl, il en résulte que toute classe de $\mathfrak{W}$ modulo $\mathfrak{H}$ est représentée par un élément de G'.

LEMME 2. *Le groupe $\mathfrak{H}'$ est contenu dans G'.*

Soient $a_1, \ldots, a_l$ les racines fondamentales. On sait qu'il y a des poids p_i de représentations de $\mathfrak{g}$ (les poids fondamentaux) tels que $p_i(H_{a_j}) = \delta_{ij}$ ($1 \leqq i, j \leqq l$), et que ces poids forment une base du groupe P des poids (cf. [6], Theorem 1, p. 30). Soit α un élément quelconque de K^*, et soit $\chi_{i,\alpha}$ l'homomorphisme de P dans K^* qui applique p_i sur α et p_j sur 1 si $i \neq j$. Il est clair que les $\chi_{i,\alpha}$ engendrent le groupe des homomorphismes de P dans K^*. Il suffira donc de montrer que l'élément $h_{i,\alpha}$ de $\mathfrak{H}'$ qui correspond à $\chi_{i,\alpha}$ appartient à G'. Or on a, pour toute racine r, $\chi_{i,\alpha}(r) = \alpha^{e_i}$, où $e_i = r(H_{a_i})$; $h_{i,\alpha}$ est donc l'image de la matrice

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

par l'homomorphisme Φ_{a_i}, ce qui démontre le lemme 2.

LEMME 3. *On a $\mathfrak{W}\mathfrak{H}\mathfrak{U}\mathfrak{W} = G$, $\mathfrak{W}\mathfrak{H}'\mathfrak{U}\mathfrak{W} = G'$.*

Montrons d'abord que G' est engendré par les groupes $\mathfrak{X}_a$, $\mathfrak{X}_{-a}$ pour toutes les racines fondamentales a. Soit G'' le groupe engendré par les $\mathfrak{X}_a$ et $\mathfrak{X}_{-a}$. Si a est une racine fondamentale, il résulte du fait que $SL(2; K)$ est engendré par $\mathfrak{N}$ et $\mathfrak{N}'$ (cf. lemme 2, §III) que $\phi_a(SL(2; K))$ est contenu dans G'', donc que $\omega_a = \phi_a(\Omega)$ appartient à G''. Or ω_a est dans $\mathfrak{W}$, et $\zeta(\omega_a)$ est la symétrie par rapport à la racine a. De plus, on sait que le groupe de Weyl est engendré par les symétries par rapport aux racines fondamentales. On en conclut que, pour toute opération w du groupe de Weyl, il y a un élément $\omega \in G'' \cap \mathfrak{W}$ tel que $\zeta(\omega) = w$. Or, soit r une racine quelconque; il y a une opération w du groupe de Weyl et une racine fondamentale a telles que $w(a) = r$ (car r appartient à au moins un système fondamental, et les systèmes fondamentaux sont permutés transitivement par les opérations du groupe de Weyl). Si $\omega \in \mathfrak{W}$ est tel que $\zeta(\omega) = w$, on a $\omega \mathfrak{X}_a \omega^{-1} = \mathfrak{X}_r$; choisissant ω dans G'', on voit que $\mathfrak{X}_r \subset G''$. Les groupes $\mathfrak{U}$ et $\mathfrak{V}$ sont donc contenus dans G'', ce qui prouve que $G'' = G'$.

Comme G est engendré par les groupes $\mathfrak{X}_a, \mathfrak{X}_{-a}$ (pour toutes les racines fondamentales a) et $\mathfrak{H}$, et G' par les groupes $\mathfrak{X}_a, \mathfrak{X}_{-a}$, il suffira pour établir

le lemme 3 de montrer que l'on a

$$\mathfrak{BHU}\mathfrak{X}_a \subset \mathfrak{BHU}, \quad \mathfrak{BHU}\mathfrak{X}_{-a} \subset \mathfrak{BHU}, \quad \mathfrak{BHU}\mathfrak{H} \subset \mathfrak{BHU},$$
$$\mathfrak{BH'U}\mathfrak{X}_a \subset \mathfrak{BH'U}, \quad \mathfrak{BH'U}\mathfrak{X}_{-a} \subset \mathfrak{BH'U}$$

pour toute racine fondamentale a. On a $\mathfrak{BX}_a = \mathfrak{X}_{-a}\mathfrak{B}_{-a}\mathfrak{X}_a = \mathfrak{X}_{-a}\mathfrak{X}_a\mathfrak{B}_{-a}$. Soit $\mathfrak{U}_a$ l'ensemble des $x \in U$ tels que $T_a(x) = 0$; on a $\mathfrak{U} = \mathfrak{X}_a\mathfrak{U}_a = \mathfrak{U}_a\mathfrak{X}_a$ et $\mathfrak{U}_a\mathfrak{X}_{-a} = \mathfrak{X}_{-a}\mathfrak{U}_a$. On a aussi $\mathfrak{U}_a\mathfrak{X}_a = \mathfrak{X}_a\mathfrak{U}_a$, puisque $\mathfrak{U}_a$ est un sous-groupe distingué de $\mathfrak{U}$. On a donc

$$\mathfrak{BHU}\mathfrak{X}_a = \mathfrak{BH}\mathfrak{X}_a\mathfrak{X}_{-a}\mathfrak{X}_a\mathfrak{U}_a\mathfrak{B}_{-a}, \quad \mathfrak{BH'U}\mathfrak{X}_a = \mathfrak{BH'}\mathfrak{X}_a\mathfrak{X}_{-a}\mathfrak{X}_a\mathfrak{U}_a\mathfrak{B}_{-a}.$$

Posons $\mathfrak{H}_a = \phi_a(\mathfrak{D})$, $\mathfrak{D}$ étant le groupe des matrices diagonales de $SL(2 ; K)$. L'ensemble $\mathfrak{X}_a\mathfrak{X}_{-a}\mathfrak{X}_a$ est contenu dans l'image par ϕ_a du groupe $SL(2 ; K) = \mathfrak{N'DNN'}$ (cf. lemme 2, §III) ; il est donc contenu dans $\mathfrak{X}_{-a}\mathfrak{H}_a\mathfrak{X}_a\mathfrak{X}_{-a}$; tenant compte de ce que $\mathfrak{X}_{-a}\mathfrak{U}_a = \mathfrak{U}_a\mathfrak{X}_{-a}$, $\mathfrak{X}_{-a}\mathfrak{B} = \mathfrak{B}$, $\mathfrak{X}_a\mathfrak{U}_a = \mathfrak{U}$, il vient

$$\mathfrak{BHU}\mathfrak{X}_a \subset \mathfrak{BH}\mathfrak{X}_{-a}\mathfrak{H}_a\mathfrak{UB}, \quad \mathfrak{BH'U}\mathfrak{X}_a \subset \mathfrak{BH'}\mathfrak{X}_{-a}\mathfrak{H}_a\mathfrak{UB}.$$

Or on a $\mathfrak{H}\mathfrak{X}_{-a} = \mathfrak{X}_{-a}\mathfrak{H}$, $\mathfrak{H'}\mathfrak{X}_{-a} = \mathfrak{X}_{-a}\mathfrak{H'}$, car, si $h \in \mathfrak{H}$, on a $h\mathfrak{X}_{-a}h^{-1} = \mathfrak{X}_{-a}$. Par ailleurs, on a $\mathfrak{BX}_{-a} = \mathfrak{B}$, $\mathfrak{HH}_a = \mathfrak{H}$; de plus, $\mathfrak{H}_a = \phi_a(\mathfrak{D})$ est contenu dans $\mathfrak{H'}$, d'où $\mathfrak{H'H}_a = \mathfrak{H'}$. On a donc

$$\mathfrak{BHU}\mathfrak{X}_a \subset \mathfrak{BHU}, \quad \mathfrak{BH'U}\mathfrak{X}_a \subset \mathfrak{BH'U}.$$

Comme $\mathfrak{BX}_{-a} = \mathfrak{B}$, on a $\mathfrak{BHU}\mathfrak{X}_{-a} = \mathfrak{BHU}$, $\mathfrak{BH'U}\mathfrak{X}_{-a} = \mathfrak{BH'U}$. On a $\mathfrak{BHU}\mathfrak{H} = \mathfrak{BHUHB} = \mathfrak{BHU}$, car, $\mathfrak{HU}$ étant un groupe, $\mathfrak{HUH} = \mathfrak{HU}$. Le lemme 3 est donc démontré.

LEMME 4. *Le groupe G' est un sous-groupe distingué de G, et G/G' est isomorphe à $\mathfrak{H}/\mathfrak{H'}$. On a $G' \cap \mathfrak{H} = \mathfrak{H'}$. Tout élément de G (resp. : G') peut être transformé en un élément de $\mathfrak{BHU}$ (resp. : $\mathfrak{BH'U}$) par un élément de $\mathfrak{B}$.*

Le normalisateur de G' dans G contient manifestement $\mathfrak{U}$ et $\mathfrak{B}$; il contient aussi $\mathfrak{H}$, car, si $h \in \mathfrak{H}$, $h\mathfrak{U}h^{-1} = \mathfrak{U}$, $h\mathfrak{B}h^{-1} = \mathfrak{B}$; ce normalisateur est donc G tout entier. Comme $\mathfrak{BH} = \mathfrak{HB}$, il résulte du lemme 3 que $G = \mathfrak{HBUB} = \mathfrak{H}G'$, donc que G/G' est isomorphe à $\mathfrak{H}/(\mathfrak{H} \cap G')$. Soit h un élément de $\mathfrak{H}$ appartenant à G' ; on peut alors écrire, en vertu du lemme 3, $h = yh'xy'$, avec y, y' dans $\mathfrak{B}$, h' dans $\mathfrak{H}$ et x dans $\mathfrak{U}$. Si I est l'élément unité de G, on a

$$I = (h^{-1}yh)\,(h^{-1}h')xy'$$

d'où $I = y'(h^{-1}yh)\,(h^{-1}h')x$. Il résulte alors du corollaire 1 au théorème 2, §IV que $y'(h^{-1}yh)$, qui est dans $\mathfrak{B}$, est I, que $h^{-1}h'$, qui est dans $\mathfrak{H}$, est I et que $x = I$; puisque $h = h'$, h est dans $\mathfrak{H'}$. On a donc $G' \cap \mathfrak{H} = \mathfrak{H'}$ et G/G' est isomorphe à $\mathfrak{H}/\mathfrak{H'}$. Si $y \in \mathfrak{B}$, $h \in \mathfrak{H}$, $x \in \mathfrak{U}$, $y' \in \mathfrak{B}$, on a $y'(yhxy')y'^{-1} = (y'y)hx$, ce qui achève de démontrer le lemme 4.

Nous désignerons dans ce qui suit par H un sous-groupe de G tel que $zHz^{-1} = H$ pour tout élément z de G' ; nous supposerons que H contient au moins un élément distinct de l'identité I. De plus, nous supposerons à partir de maintenant que $\mathfrak{g}$ est *simple*. Dans ces conditions, il résulte immédiatement du lemme 4 que H contient un élément $\neq I$ appartenant à l'ensemble $\mathfrak{BHU}$. Nous désignerons par $\mathfrak{M}_0$ l'ensemble des $y \in \mathfrak{B}$ pour lesquels il existe des éléments $h \in \mathfrak{H}$ et $x \in \mathfrak{U}$ tels que $yhx \in H$. Nous nous proposons de montrer

que, sauf dans le cas où $\mathfrak{g}$ est de type (A_1) et K est un corps à 2 ou à 3 éléments, on a $H \cap \mathfrak{N} \neq \{I\}$. La démonstration assez longue de ce fait procèdera par réduction à l'absurde. Dans ce qui suit, nous supposerons donc que $H \cap \mathfrak{N} = \{I\}$, ce qui implique $\mathfrak{M}_0 \neq \{I\}$, et que l'on se trouve pas dans le cas où $\mathfrak{g}$ est de type (A_1) et K a moins de 4 éléments ; nous nous proposons de déduire une contradiction de ces hypothèses.

LEMME 5. *Supposons que* $H \cap \mathfrak{N} = \{I\}$. *Si* $y \in \mathfrak{M}_0$, *il existe des éléments uniquement determinés* h *de* $\mathfrak{H}$ *et* x *de* $\mathfrak{U}$ *tels que* $yhx \in H$; *nous poserons* $\eta(y) = h$, $\xi(y) = x$; $\mathfrak{M}_0$ *est un groupe*; η *est un homomorphisme de* $\mathfrak{M}_0$ *dans* $\mathfrak{H}$, *et on a, pour* $y, y' \in \mathfrak{M}_0$, $\xi(y'^{-1}y) = \eta(y')\xi(y)\,(\xi(y'))^{-1}(\eta(y'))^{-1}$. *Si* $h' \in \mathfrak{H}'$, *on a* $h'yh'^{-1} \in \mathfrak{M}_0$ *et* $\eta(h'yh'^{-1}) = \eta(y)$, $\xi(h'yh'^{-1}) = h'\xi(y)h'^{-1}$.

Soient y, y' des éléments de $\mathfrak{V}$, h, h' des éléments de $\mathfrak{H}$ et x, x' des éléments de $\mathfrak{U}$ tels que yhx et $y'h'x'$ soient dans H. L'élément $yhx(y'h'x')^{-1}$ est alors dans H, et il en est de même de son transformé par y'^{-1}, qui est $(y'^{-1}y)(hh'^{-1})\,(h'(xx'^{-1})h'^{-1})$; on a donc $y'^{-1}y \in \mathfrak{M}_0$, ce qui montre que $\mathfrak{M}_0$ est un groupe. Si $y = y'$, il résulte de ce que $H \cap \mathfrak{N} = \{I\}$ que $h' = h$, $x' = x$, et la première assertion du lemme est démontrée. Comme $\mathfrak{H}$ est commutatif, η est un homomorphisme ; la formule qui donne $\xi(y'^{-1}y)$ résulte immédiatement de la forme que nous avons donnée à $(yhx)\,(y'h'x')^{-1}$. Soit maintenant h' un élément de $\mathfrak{H}'$, donc de G' ; alors $h'(y\eta(y)\xi(y))h'^{-1}$ est dans H; or cet élément s'écrit

$$(h'yh'^{-1})(h'\eta(y)h'^{-1})\,(h'\xi(y)h'^{-1}),$$

ce qui démontre les dernières assertions du lemme.

Nous désignerons par $\mathfrak{M}$ le noyau de l'homomorphisme η de $\mathfrak{M}_0$ dans $\mathfrak{H}$.

LEMME 6. *Si* K *est de caractéristique* $p > 0$, *tout élément de* $\mathfrak{V}$ *est d'ordre fini égal à une puissance de* p.

Si r est une racine et $t \in K$, on a $(x_r(t))^p = x_r(pt) = I$. Pour tout entier $k > 0$, $\mathfrak{V}_k/\mathfrak{V}_{k+1}$ est isomorphe au produit des groupes $\mathfrak{X}_r$ pour les racines $r < 0$ telles que $-r$ soit de hauteur k; tout élément distinct de l'élément unité de ce groupe est donc d'orde p, ce qui démontre le lemme 6.

LEMME 7. *Supposons que* $H \cap \mathfrak{N} = \{I\}$; *on a alors* $\mathfrak{M} \neq \{I\}$.

Si K est de caractéristique $p > 0$, tout élément de $\mathfrak{M}_0/\mathfrak{M}$ est d'ordre fini égal à une puissance de p. Soit par ailleurs χ un homomorphisme de P_r dans le groupe multpilicatif K^* des éléments $\neq 0$ de K. S'il existe un $e \geqq 0$ tel que $(\chi(r))^{p^e} = 1$ pour toute racine r, on a déjà $\chi(r) = 1$; $\mathfrak{H}$ ne contient donc aucun élément $\neq I$ dont l'ordre soit une puissance de p. Comme $\mathfrak{M}_0/\mathfrak{M}$ est isomorphe à un sous-groupe de $\mathfrak{H}$, on a dans ce cas $\mathfrak{M} = \mathfrak{M}_0 \neq \{I\}$.

Considérons maintenant le cas où K est de caractéristique 0. Soit y un élément $\neq I$ de $\mathfrak{M}_0$, et soit r une racine telle que $T_r(y) \neq 0$. Si χ est un homomorphisme du groupe P des poids dans K^*, et h' l'élément correspondant de $\mathfrak{H}'$, on a $T_r(h'yh'^{-1}) = \chi(r)T_r(y)$. Or on peut choisir χ de telle manière que $\chi(r) \neq 1$. On sait en effet par la théorie des diviseurs élémentaires qu'il

existe une base de P contenant un élément w tel que r puisse se mettre sous la forme dw, d étant un entier $\neq 0$. Puisque K est de caractéristique 0, il y a un élément α de K^* tel que $\alpha^d \neq 1$; or, w faisant partie d'une base de P, il y a un homorphisme de P dans K^* tel que $\chi(w) = \alpha$, d'ou $\chi(r) = \alpha^d \neq 1$. Soit donc h' un élément de $\mathfrak{H}'$ tel que $h'yh'^{-1} \neq y$; il résulte alors du lemme 5 que $h'yh'^{-1}y^{-1}$ est un élément $\neq I$ de $\mathfrak{M}$.

LEMME 8. *Supposons que* $H \cap \mathfrak{H}\mathfrak{U} = \{I\}$. *L'application* $y \to (\xi(y))^{-1}$ *induit un monomorphisme de* $\mathfrak{M}$ *dans* $\mathfrak{U}$.

Il résulte immédiatement du lemme 5 que cette application induit un homomorphisme de $\mathfrak{M}$ dans $\mathfrak{U}$. Soit y un élément du noyau de cet homomorphisme; on a donc $y \in H \cap \mathfrak{V}$. Or, il y a une opération du groupe de Weyl qui change toute racine négative en une racine positive. Il résulte donc du lemme 1 qu'il y a un élément $\omega \in G'$ tel que $\omega\mathfrak{V}\omega^{-1} = \mathfrak{U}$, d'ou $\omega y\omega^{-1} \in H \cap \mathfrak{U}$; ceci montre que $y = I$.

LEMME 9. *Soient a une racine fondamentale et t un élément* $\neq 0$ *de K. Si un élément* $x \in \mathfrak{U}$ *commute avec* $x_a(t)$ (*resp.*: *avec* $x_{-a}(t)$), *on a* $T_r(x) = 0$ *pour toute racine* $r > 0$ *telle qu'il y ait un élément de* $\mathfrak{X}_r$ *qui ne commute pas avec tous les éléments de* $\mathfrak{X}_a$ (*resp.*: *de* $\mathfrak{X}_{-a}$).

Nous commencerons par établir que $T_a(x) = 0$ si x commute avec $x_{-a}(t)$. Puisque a est une racine fondamentale, nous avons $x = x_a(T_a(x))x'$, où x' est un élément de $\mathfrak{U}$ tel que $T_a(x') = 0$ (lemme 7, §III), et on sait que $x_{-a}(t)x'x_{-a}^{-1}(t) \in \mathfrak{U}$ (lemme 8, §III). Il suffira donc d'établir le résultat suivant: si τ est un élément de K tel que $x_{-a}(t)x_a(\tau)x_{-a}^{-1}(t) \in \mathfrak{U}$, on a $\tau = 0$. Or, $x_{-a}(t)x_a(\tau)x_{-a}^{-1}(t)$ est l'image par ϕ_a de la matrice

$$\begin{pmatrix} 1 - t\tau & \tau \\ -t^2\tau & 1 + t\tau \end{pmatrix}.$$

Si $t\tau \neq 1$, cette matrice se met sous la forme

$$\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

avec $v = -(1 - t\tau)^{-1}t^2\tau$, $x = 1 - t\tau$, $u = (1 - t\tau)^{-1}\tau$. Or, les images des trois facteurs de cette décomposition sont respectivement dans $\mathfrak{V}$, dans $\mathfrak{H}$ et dans $\mathfrak{U}$. Comme un élément de $\mathfrak{V}\mathfrak{H}\mathfrak{U}$ ne peut se mettre que d'une seule manière sous la forme du produit d'un élément de $\mathfrak{V}$, d'un élément de $\mathfrak{H}$ et d'un élément de $\mathfrak{U}$ (lemme 13, §III), on en conclut que l'image par ϕ_a de la matrice

$$\begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}$$

est l'élément unité, ce qui implique $v = 0$, d'où $\tau = 0$. Si $t\tau = 1$, la matrice en question se met sous la forme

$$\begin{pmatrix} 0 & \tau \\ -\tau^{-1} & 0 \end{pmatrix}\begin{pmatrix} 1 & -2\tau \\ 0 & 1 \end{pmatrix}$$

et l'image du premier facteur par ϕ_a est dans $\mathfrak{U}$. Cette image est le produit d'un élément de $\mathfrak{H}$ par ω_a: ce cas ne peut donc se présenter (théorème 2, §III). Ceci dit, nous diviserons la démonstration du lemme 9 en deux parties, relatives aux cas où $\mathfrak{g}_c$ n'est pas ou est de type (G_2). Supposons d'abord que $\mathfrak{g}_c$ ne soit pas de type (G_2). Il suffira évidemment de montrer que, si, pour un certain $m > 0$, on a $T_r(x) = 0$ pour toute racine $r > 0$ de hauteur $< m$, et si x commute avec $x_a(t)$ (resp.: $x_{-a}(t)$), on a $T_r(x) = 0$ pour toute racine r de hauteur m telle que $\mathfrak{X}_r$ contienne un élément qui ne commute pas avec tous les éléments de $\mathfrak{X}_a$ (resp.: $\mathfrak{X}_{-a}$). Nous poserons $\tau_r = T_r(x)$.

Supposons d'abord que x commute avec $x_a(t)$. On a, pour toute racine r de hauteur $\geqq m$,

$$x_a(t)x_r(\tau_r)x_a^{-1}(t) \equiv x_r(\tau_r)x_{r+a}(N_{a,r}t\tau_r) \qquad (\mathrm{mod}\ \mathfrak{U}_{m+2}),$$

et $x_{r+a}(N_{a,r}t\tau_r) \in \mathfrak{U}_{m+1}$. Comme $\mathfrak{U}_{m+1}/\mathfrak{U}_{m+2}$ est dans le centre de $\mathfrak{U}/\mathfrak{U}_{m+2}$, on a

$$x_a(t)xx_i^{-1}(t) \equiv x \prod\nolimits_r x_{a+r}(N_{a,r}t\tau_r) \qquad (\mathrm{mod}\ \mathfrak{U}_{m+2}).$$

Cet élément étant égal à x, il en résulte que $N_{a,r}\,\tau_r = 0$ pour toute racine r de hauteur m. Si donc $N_{a,r}$ n'est pas divisible par la caractéristique de K, on a $\tau_r = 0$. Si $N_{a,r} = 0$, $a + r$ n'est pas racine, et tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_a$. Si $N_{a,r} \neq 0$ est divisible par la caractéristique de K, $r - a$ est racine (car, sinon, $N_{a,r}$ serait ± 1); comme $\mathfrak{g}_c$ n'est pas de type (G_2), le seul couple d'entiers $i > 0, j > 0$ tel que $ir + ja$ soit racine est $(1, 1)$ (lemme 2, §I), et, quels que soient t', τ' dans K, $x_a(t')x_r(\tau')x_i^{-1}(t') = x_r(\tau')x_{r+a}(N_{a,r}t'\tau') = x_r(\tau')$.

Supposons maintenant que x commute avec $x_{-a}(t)$. Nous savons déjà que τ_a est nul. Si $r \neq a$, on a

$$x_{-a}(t)x_r(\tau_r)x_{-a}^{-1}(t) = x_r(\tau_r) \prod\nolimits_{i,j} x_{-ia+jr}(C_{ij;-a,r}t^i\tau_r^j)$$

où le produit est étendu aux couples (i, j) tels que $i > 0$, $j > 0$ et que $-ia + jr$ soit une racine, arrangés dans un ordre convenable; $-ia + jr$ est alors $\geqq 0$. Soit n le plus petit entier tel qu'il existe une racine r et des entiers $i > 0$, $j > 0$ tels que $-ia + jr$ soit une racine de hauteur n et que $C_{ij;-a,r}\tau_r \neq 0$. On a

$$x_{-a}(t)xx_{-a}^{-1}(t) \equiv x \prod\nolimits_s x_s\left(\sum\nolimits_{-ia+jr=s} C_{ij;-a,r}t^i\tau_r^j\right) \qquad (\mathrm{mod}\ \mathfrak{U}_{n+1})$$

où le produit est étendu aux racines s de hauteur n et la somme aux couples (i, j, r) tels que $s = -ia + jr$, $i > 0$, $j > 0$, r de hauteur $\geqq m$; cela résulte du fait que, si s est de hauteur n et si x' est un élément quelconque de $\mathfrak{U}$, x' commute avec tout élément de $\mathfrak{X}_s$ modulo $\mathfrak{U}_{n+1}$. On a donc $\sum_{-ia+jr=s} C_{ij;-a,r}t^i\tau_r^j = 0$ pour toute racine s de hauteur n. Observons maintenant que, si $n \leqq m$, $s = -ia + jr$, avec $i > 0$, $j > 0$, $\tau_r \neq 0$, r de hauteur $\geqq m$, on a $j = 1$ si s est de hauteur n. En effet, si j était > 1, on aurait $j = 2, i = 1$ puisque $\mathfrak{g}_c$ n'est pas de type (G_2) (lemme 2, §I), d'où $2m - 1 \leqq m$, $m = 1$; mais r serait alors une racine fondamentale, de sorte que $2r - a$ ne serait pas racine (r est $\neq a$ puisque $\tau_r \neq 0$). Comme $i \leqq 2$ (lemme 2, §I), on voit que

$n \geqq m-2$. Le cas $n = m-2$ est impossible, car, s étant une racine de hauteur $n-2$, il n'y a qu'un seul système $(i,j,r), i>0, j>0, r$ de hauteur $\geqq m$ tel que $s = -ia + jr$; on devrait donc avoir $C_{i,j;-a,r}t^i\tau_r^j = 0$, en contradiction avec la définition de n. Si donc r est une racine de hauteur m telle que $r-2a$ soit racine, on a $C_{2,1;-a,r}\tau_r = 0$. Or, $r+a$ n'est alors pas racine (lemme 2, §I) et on a par suite $N_{-a,r} = \pm 1$, $N_{-a,r-a} = \pm 2$, $C_{2,1;-a,r} = \pm 1$ (cf. formule (5), §III) et par suite $\tau_r = 0$. Supposons maintenant que $n = m-1$. Si $s = -ia + r$ est une racine de hauteur $m-1$, avec $i>0$, il n'y a qu'au plus deux couples (i,r) tels que $s = -ia + r$; s'il n'y en a qu'un, on a $i = 1, s = r-a, r$ étant une racine de hauteur m telle que $r+a$ ne soit pas racine ; s'il y en a deux, ce sont $(1,r)$ et $(2, r+a)$, r étant une racine de hauteur r telle que $r-a, r, r+a$ soient racines. Dans le premier cas, on a $C_{1,1;-a,r}\tau_r = N_{-a,r}\tau_r = 0$; mais, $r+a$ n'étant pas racine, $N_{-a,r} = \pm 1$ et $\tau_r = 0$. Dans le second cas, on a

$$C_{1,1;-a,r}t\tau_r + C_{2,1;-a,r}t^2\tau_{a+r} = 0. \tag{1}$$

Nous avons donc $\tau_r = 0$ pour toute racine r de hauteur m telle que $r-a$ soit racine, mais que $r+a$ ne le soit pas. Montrons maintenant que, si $s = r-a, s' = r'-a$, où r' sont des racines de hauteur m, tout élément de $\mathfrak{X}_s$ commute avec tout élément de $\mathfrak{X}_{s'}$ modulo $\mathfrak{U}_{m+1}$. Le commutateur d'un élément de $\mathfrak{X}_s$ et d'un élément de $\mathfrak{X}_{s'}$ est dans $\mathfrak{U}_{2m-2}$; notre assertion est donc vraie si $2m-2 \geqq m+1$, i.e. si $m \geqq 3$. Si $m = 2, s$ et s' sont des racines fondamentales, ainsi que a ; comme $s+a$ et $s'+a$ sont des racines, $s+s'$ ne peut en être une (car le graphe de $\mathfrak{g}_c$ ne comporte aucun triangle), d'où il résulte que tout élément de $\mathfrak{X}_s$ commute alors avec tout élément de $\mathfrak{X}_{s'}$. Par ailleurs, les éléments de $\mathfrak{X}_s$ commutent avec ceux de $\mathfrak{U}_m$ modulo $\mathfrak{U}_{m+1}$. Puisque $\sum_{-ia+jr=s} C_{ij;-a,r}t^i\tau_r^j = 0$ pour toute racine s de hauteur $m-1$, on en conclut que

$$x_{-a}(t)x x_{-a}^{-1}(t) \equiv x \prod_{r'} \left(\sum_{-ia+jr=r'} C_{ij;-a,r}t^i\tau_r^j\right) \pmod{\mathfrak{U}_{m+1}},$$

le produit étant étendu aux racines r' de hauteur m et la somme aux systèmes (i,j,r) tels que $-ia+jr = r', i>0, j>0, r$ de hauteur $\geqq m$. Comme nous l'avons vu plus haut, ceci implique $j = 1$. Or, supposons que r' soit tel que $r'-a$ et $r'+a$ soient racines. Alors $r'+2a$ n'est pas racine, et il n'y a par suite qu'un couple (i,r) tel que $r' = -ia + r$, à savoir $(1, r'+a)$. On a donc alors $C_{1,1;-a,r'+a}\tau_{r'+a} = 0$. Mais $C_{1,1;-a,r'+a} = N_{-a,r'+a} = \pm 1$ puisque $r'+2a$ n'est pas racine (lemme 2, §I). On a donc $\tau_{r'+a} = 0$, et par suite aussi, tenant compte de la relation (1) ci-dessus, appliquée à r', $C_{1,1;-a,r'}\tau_{r'} = 0$. Par ailleurs, $r'-a, r'$ et $r'+a$ étant des racines, le seul couple d'entiers $i>0, j>0$ tels que $-ia+jr'$ soit racine est $(1,1)$ (lemme 2, §I). On a donc, quels que soient t', τ' dans K, $x_{-a}(t')x_{r'}(\tau')x_{-a}^{-1}(t') = x_{r'}(\tau')x_{r'-a}(C_{1,1;-a,r}\, t'\tau') = x_{r'}(\tau')$, et tout élément de $\mathfrak{X}_{-a}$ commute avec tout élément de $\mathfrak{X}_{r'}$. On voit donc que, si $\tau_r \neq 0$ pour une racine r de hauteur m telle que $r-a, r, r+a$ soient racines, tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_{-a}$ (cela ne peut d'ailleurs se produire que si K est de caractéristique 2). Enfin, si $r-a$ n'est pas une racine, tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_{-a}$.

Il reste à envisager le cas où $\mathfrak{g}_c$ est de type (G_2). Soit alors b la racine fondamentale $\neq a$. Il y a à considérer séparément le cas où $b + 3a$ est racine et celui où $a + 3b$ est racine.

Supposons d'abord que $b + 3a$ soit racine, et soit

$$x = x_a(\tau_a)x_b(\tau_b)x_{b+a}(\tau_{b+a})x_{b+2a}(\tau_{b+2a})x_{b+3a}(\tau_{b+3a})x_{2b+3a}(\tau_{2b+3a}).$$

Supposons d'abord que x commute avec $x_a(t)$. On a

$$x_a(t)xx_i^{-1}(t) \equiv xx_{b+a}(C_{1,1;a,b}t\tau_c) \qquad (\text{mod } \mathfrak{U}_3)$$

et $C_{1,1;a,b} = N_{a,b} = \pm 1$, d'où $\tau_b = 0$. On a donc

$$x_a(t)xx_i^{-1}(t) \equiv xx_{b+2a}(C_{1,1;a,b}t\tau_{b+a}) \qquad (\text{mod } \mathfrak{U}_4)$$

et $C_{1,1;a,b+a} = N_{a,b+a} = \pm 2$; on a donc $\tau_{b+a} = 0$ si K n'est pas de caractéristique 2. Si K est de caractéristique 2, on a

$$x_a(t)x_{b+a}(\tau_{b+a})x_i^{-1}(t) = x_{b+a}(\tau_{b+a})x_{b+3a}(C_{2,1;a,b+a}t^2\tau_{b+a})x_{2b+3a}(C_{1,2;a,b+a}t\tau_{b+a}^2)$$
$$x_a(t)x_{b+2a}(\tau_{b+2a})x^{-1}(t) = x_{b+2a}(\tau_{b+2b})x_{b+3a}(C_{1,1;a,b+2a}t\tau_{b+2a})$$

et $x_a(t)$ commute avec $x_{b+3a}(\tau_{b+3a})$, $x_{2b+3a}(\tau_{2b+3a})$. De plus, les éléments de $\mathfrak{X}_{b+2a}$ commutent avec ceux de $\mathfrak{X}_{b+3a}$ et $\mathfrak{X}_{2b+3a}$ est dans le centre de $\mathfrak{U}$. En écrivant que $T_{2b+3a}(x_a(t)xx_i^{-1}(t)) = T_{2b+3a}(x)$, il vient donc $C_{1,2;a,b+a}\tau_{b+a}^2 = 0$. Or on a $C_{1,2;a,b+a} = M_{b+a,a} = (1/2)N_{b+a,a}N_{b+a,b+2a}$. Le plus grand i tel que $a - i(b + a)$ soit racine est 1, et le plus grand i tel que $b + 2a - i(b + a)$ soit racine est 2, d'où $C_{1,2;a,b+a} = \pm 3$; le corps K étant de caractéristique 2, on a $\tau_{b+a} = 0$. Il eù résulte que

$$x_a(t)xx_a^{-1}(t) \equiv x\,x_{b+3a}(C_{1,1;a,b+2a}t\tau_{b+2a}) \qquad (\text{mod } \mathfrak{U}_5),$$

d'où $C_{1,1;a,b+2a}\tau_{b+2a} = 0$. Par ailleurs, on a

$$x_a(t')x_{b+2a}(\tau')x_i^{-1}(t') = x_{b+2a}(\tau')x_{b+3a}(C_{1,1;a,b+2a}t'\tau')$$

quels que soient t', τ'. Il en résulte que, si $\tau_{b+2a} \neq 0$ (ce qui ne peut d'ailleurs se produire que si K est de caractéristique 3), tout élément de $\mathfrak{X}_a$ commute avec tout élément de $\mathfrak{X}_{b+2a}$.

Supposons maintenant que x commute avec $x_{-a}(t)$. Nous savons alors que $\tau_a = 0$. Tout élément de $\mathfrak{X}_{-a}$ commute avec tout élément de $\mathfrak{X}_b$ ou de $\mathfrak{X}_{2b+3a}$. Soit $\mathfrak{Z}$ le groupe engendré par $\mathfrak{X}_b, \mathfrak{X}_{b+a}$, $\mathfrak{X}_{b+2a}$, $\mathfrak{X}_{b+3a}$, $\mathfrak{X}_{2b+3a}$; le groupe des commutateurs de $\mathfrak{Z}$ est contenu dans $\mathfrak{X}_{2b+3a}$, qui est dans le centre de $\mathfrak{U}$. Il résulte immédiatement de là que

$$T_{b+2a}(x_{-a}(t)xx_{-a}^{-1}(t)) = T_{b+2a}(x) + C_{1,1,-a,b+3a}t\,\tau_{b+3a}$$

(car $x_{-a}(t)$ commute avec les éléments de $\mathfrak{X}_{2b+3a}$). On a $C_{1,1;-a,b+3a} = N_{-a,b+3a}$ $= \pm 1$, et par suite $\tau_{b+3a} = 0$. On a donc

$$T_{b+a}(x_{-a}(t)xx_{-a}^{-1}(t)) = T_{b+a}(x) + C_{1,1;-a,b+2a}t\,\tau_{b+2a}.$$

Comme $C_{1,1;-a,b+2a} = \pm 2$, on a $\tau_{b+2a} = 0$ dans le cas où K n'est pas de caractéristique 2. Pour traiter le cas où K est de caractéristique 2, on observe que $T_{2b+3a}(x_{-a}(t)x_{b+a}(\tau_{b+a})x_{-a}^{-1}(t)) = 0$. Comme $\tau_{b+3a} = 0$, on a

$$T_{2b+3a}(x_{-a}^{-1}(t)xx_{-a}^{-1}(t)) = T_{2b+3a}(x) + C_{1,2;-a,b+2a}t\tau_{b+2a}^2,$$

d'où $C_{1,2;-a,b+2a}\tau_{b+2a} = 0$. Or on a $C_{1,2;-a,b+2a} = M_{b+2a,-a,2} = (1/2)N_{b+2a,-a}N_{b+2a,b+a}$ $= (1/2)(\pm 2)(\pm 3) = \pm 3$; K étant de caractéristique 2, on a $\tau_{b+2a} = 0$. On

en déduit que

$$T_b(x_{-a}(t)xx_{-a}^{-1}(t)) = T_b(x) + C_{1,1;\,-a,b+a}t\tau_{b+a};$$

or on a

$$x_{-a}(t')x_{b+a}(\tau')x_{-a}^{-1}(t') = x_{b+a}\,(\tau')x_b(C_{1,1;\,-a,\,b+a}t'\tau')$$

quels que soient t' et τ'; donc, si $\tau_{b+a} \neq 0$ (ce qui ne peut se produire que si K est de caractéristique 3), tout élément de $\mathfrak{X}_{-a}$ commute avec tout élément de $\mathfrak{X}_{b+a}$.

Supposons à partir de maintenant que $3b + a$ soit racine; soit

$$x = x_a(\tau_a)x_b(\tau_b)x_{b+a}(\tau_{b+a})x_{2b+a}(\tau_{2b+a})x_{3b+a}(\tau_{3b+a})x_{3b+2a}(\tau_{3b+2a}).$$

Supposons que x commute avec $x_a(t)$. Les éléments de $\mathfrak{X}_a$ commutent avec ceux de $\mathfrak{X}_a, \mathfrak{X}_{b+a}, \mathfrak{X}_{2b+a}, \mathfrak{X}_{3b+2a}$. On a

$$x_a(t)xx_a^{-1}(t) \equiv xx_{b+a}(C_{1,1;a,b}t\tau_b) \qquad (\mathrm{mod}\ \mathfrak{U}_3)$$

et $C_{1,1;a,b} = \pm 1$, d'où $\tau_b = 0$. On a donc

$$x_a(t)xx_a^{-1}(t) = xx_{3b+2a}(C_{1,1;a,3b+a}t\,\tau_{3b+a})$$

et $C_{1,1;a,3b+a} = \pm 1$, d'où $\tau_{3b+a} = 0$.

Supposons maintenant que x commute avec $x_{-a}(t)$. On a $\tau_a = 0$, et les éléments de $\mathfrak{X}_{-a}$ commutent avec ceux de $\mathfrak{X}_b, \mathfrak{X}_{2b+a}, \mathfrak{X}_{3b+a}$. On a $x_{-a}(t)x_{3b+2a}(\tau_{3b+2a})x_{-a}^{-1}(t) = x_{3b+2a}\,(\tau_{3b+2a})x_{3b+a}(C_{1,1;\,-a,3b+2a}t\tau_{3b+2a})$ et il en résulte que

$$x_{-a}(t)xx_{-a}^{-1}(t) \equiv xx_b\,(C_{1;\,1,\,-a,b+a}t\ \tau_{b+a}) \qquad (\mathrm{mod}\ \mathfrak{U}_2),$$

et $C_{1,1;\,-a,b+a} = \pm 1$, d'où $\tau_{b+a} = 0$. On en conclut alors, au moyen de la relation écrite plus haut, que $C_{1,1;\,-a,3b+2a}\tau_{3b+2a} = 0$. Or on a $C_{1,1;\,-a,3b+2a} = \pm 1$, et par suite $\tau_{3b+2a} = 0$. Le lemme 9 est donc démontré.

LEMME 10. *Soient r et s des racines telles que tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_s$; on a alors $s(H_r) \geqq 0$.*

La conclusion est certainement vraie si $r = s$. Il est par ailleurs impossible que $s = -r$. Supposons en effet pour un moment que tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_{-r}$. Puisque $SL(2\,;\,K)$ est engendré par $\mathfrak{N}$ et $\mathfrak{N}'$ (lemme 2, § III), $\phi_r(SL(2\,;\,K))$ est alors abélien. Mais ce groupe contient l'élément $\omega_r = \phi_r(\Omega)$, et on sait que $\omega_r\mathfrak{X}_r\omega_r^{-1} = \mathfrak{X}_{-r}$, ce qui montre que $\phi_r(SL(2\,;\,K))$ n'est pas abélien. On peut donc supposer r et s linéairement indépendantes. On a alors

$$I = x_r(1)x_s(1)x_r^{-1}(1) = x_s(1)\ \prod_{i,j} x_{ir+js}(C_{i,j;r,s}1_K)$$

où le produit est étendu aux couples (i, j) d'entiers > 0 tel que $ir + js$ soit racine (ces couples étant rangés dans un ordre convenable), et où 1_K est l'élément unité de K; on a donc $C_{ij;r,s}\cdot 1_K = 0$ pour tout couple (i, j) (on peut en effet munir P_r d'une structure de groupe ordonné telle que r et s soient > 0 dans cette ordination de P_r, et les $ir + js$ sont alors tous > 0). En particulier, on a $N_{r,s}\cdot 1_K = 0$, et $s - r$ est par suite racine. Si on avait $s(H_r) < 0$, il en résulterait que $s + 2r$ serait aussi racine, et on aurait $C_{2,1;r,s} = (1/2)N_{r,s}N_{r,r+s}$. Puisque $s + 2r$ serait racine, $s - 2r$ ne serait pas racine, et

on aurait $N_{r,s} = \pm 2$, $N_{r,r+s} = \pm 3$, $C_{2,1;r,s} = \pm 3$. c'est impossible, car $C_{1,1;r,s}.1_K$ et $C_{2,1;r,s}.1_K$ ne seraient pas tous deux nuls.

LEMME 11. *Soit P le groupe des poids. Si r est une racine et u un élément $\neq 0$ de K, il y a un homomorphisme χ de P dans le groupe K^* des éléments $\neq 0$ de K tel que $\chi(r) = u^2$. Supposons que r et s soient des racines linéairement indépendantes et que tout homomorphisme de P dans K^* qui applique r sur 1 applique aussi s sur 1. On est alors dans l'un des cas suivants: a) K est un corps à 2 éléments; b) K est un corps à 3 éléments, et r, s sont des racines orthogonales; c) K est un corps à 3 elements, tout homomorphisme de P dans K^* applique s sur 1 mais il y a un homomorphisme de P dans K^* qui n'applique pas r sur 1; d) K est un corps à 4 elements et $\mathfrak{g}_c$ est de l'un des types (A_2) ou (G_2).*

On peut former un système fondamental de racines $(a_1, \ldots, a_l)$ tel que $r = a_1$, $s = \lambda a_1 + \mu a_2$, λ et μ étant des entiers $\geqq 0$ (lemme 1, §I). Soit d le plus grand entier > 0 tel que $d^{-1}r \in P$; il y a alors une base $(w_1, \ldots, w_l)$ de P telle que $w_1 = d^{-1}r$. Pour tout $u \in K^*$, il y a un homomorphisme χ de P dans K^* tel que $\chi(w_1) = u$, d'où $\chi(r) = u^d$. Par ailleurs, on a $2 = r(H_r) = dw_1(H_r)$; comme $w_1(H_r)$ est entier, d est 1 ou 2, et la première assertion du lemme 11 est démontrée. Posons $s = \sum'_{i=1} n_i w_i$, les n_i étant des entiers. Si $i > 1$, il y a un homomorphisme de P dans K^* qui applique w_i sur u et w_j sur 1 si $i \neq j$; appliquant r sur 1, il applique aussi s sur 1, d'où $u^{n_i} = 1$. Puisque r et s sont linéairement indépendantes, $n_2, \ldots, n_l$ ne sont pas tous nuls; puisque $u^{n_i} = 1$ $(i = 2, \ldots . l)$ pour tout $u \in K^*$, K est un corps fini; soit q le nombre de ses éléments. Les $n_i (i > 1)$ sont divisibles par $q - 1$, d'où $s - d^{-1}n_1 r = (q-1)w$, avec un $w \in P$. Supposons que l'on ne soit pas dans le cas a), d'où $q > 2$. On a

$$s(H_r) = 2n_1 d^{-1} + (q-1)w(H_r), \quad 2 = n_1 d^{-1} r(H_s) + (q-1)w(H_s).$$

Multipliant la première relation par $r(H_s)$ et observant que $w(H_r), w(H_s)$ sont entiers, il vient $s(H_r)r(H_s) \equiv 4 \pmod{q-1}$. Or on sait que $r(H_s)s(H_r)$ est un entier $\geqq 0$. S'il est nul, r et s sont orthogonales, on a $r(H_s) = 0$ et $2 = (q-1)w(H_s)$, d'où $q = 3$. Si $r(H_s)s(H_r) = 1$, on peut supposer sans restriction de généralité que $r(H_s)$ et $s(H_r)$ sont égaux à -1 (s'ils étaient égaux à 1, on changerait s en $-s$). Puisque $q - 1$ divise 3, on a $q = 4$ dans ce cas. Montrons que l'on doit avoir $l = 2$. S'il n'en était pas ainsi, il résulte du fait que $\mathfrak{g}$ est simple que $\{a_1, \ldots, a_l\}$ contiendrait une racine, disons a_3, distincte de a_1, a_2 mais qui ne serait pas orthogonale à a_1 et à a_2. Comme a_1, a_2 ne sont pas orthogonales, a_3 serait d'ailleurs orthogonale à l'une des racines a_1, a_2. Puisque $\mathfrak{g}_c$ ne serait pas de type (G_2), celui des nombres $a_1(H_{a_3})$, $a_2(H_{a_1})$ qui serait $\neq 0$ serait -1 ou -2. On aurait $(s - n_1 d^{-1} r)(H_{a_3}) = 3w(H_{a_3}) \equiv 0 \pmod 3$, et ce nombre serait $(\lambda - n_1 d^{-1})a_1(H_{a_3}) + \mu a_2(H_{a_3})$. Par ailleurs, $\mathfrak{g}$ n'étant pas de type (G_2), μ serait < 3 (lemme 2, §I), et il est clair que $\mu \neq 0$. Il serait donc impossible que $a_1(H_{a_3}) = 0$, d'où $a_2(H_{a_3}) = 0$, $\lambda - n_1 d^{-1} \equiv 0 \pmod 3$. Par ailleurs, la relation $2 - n_1 d^{-1} r(H_s) \equiv 0 \pmod 3$ donnerait $d^{-1}n_1 \equiv 1$

(mod 3), d'où $\lambda \equiv 1 \pmod 3$ et $\lambda = 1$ puisque $\lambda \geqq 0$, $\lambda < 3$ (lemme 2, §I). Il en résulterait que $s - r = \mu a_2$ serait de la forme $3w'$, avec $w' \in P$, d'où $2\mu = 3w'(H_{a_2})$; mais c'est impossible puisque $1 \leqq \mu < 3$. On a donc bien $l = 2$ dans ce cas. De plus, on vérifie tout de suite qu'une algèbre de type (B_2) ne contient aucune couple de racines r, s telles que $r(H_s)s(H_r) = 1$; $\mathfrak{g}_c$ est donc de type (A_2) ou (G_2) si $s(H_r)r(H_s) = 1$. Si $s(H_r)r(H_s) = 2$, la relation $r(H_s)s(H_r) \equiv 4 \pmod{q-1}$ donne $q = 3$. Si on avait $d = 2$, tout homomorphisme de P dans K^* appliquerait $r = 2w_1$ sur un carré, et appliquerait par suite aussi s sur 1. Il en résulte en vertu de la première partie du lemme que $s/2$ serait dans W, donc que n_1 serait pair; $d^{-1}n_1$ serait donc entier, donc $s(H_r)$ serait pair, et on aurait $r(H_s) = \pm 1$; mais ceci est impossible si $d = 2$, puisque $r(H_s) = dw_1(H_s)$. On a donc $d = 1$, et il y a un homomorphisme de P dans K^* qui applique r sur un élément $\neq 1$. La relat on $s(H_r)r(H_s) \equiv 4 \pmod{q-1}$ exclut la possibilité que $r(H_s)s(H_r)$ soit 3. Comme $s(H_r)r(H_s)$ est toujours $\leqq 3$, le lemme 11 est démontré.

Ceci dit, revenons à l'étude du groupe H. On notera que, si $y \in \mathfrak{M}$ et si a est une racine fondamentale telle que $T_{-a}(y) = 0$, on a, pour tout $t \in K$, $x_a(t)yx_i^{-1}(t) \in \mathfrak{M}$ et

$$\xi(x_a(t)yx_i^{-1}(t)) = x_a(t)\xi(y)x_a^{-1}(t);$$

en effet, on sait que $x_a(t)yx_i^{-1}(t) \in \mathfrak{B}$, et l'élément $x_a(t)y\xi(y)x_i^{-1}(t)$ est dans H, tandisque $x_a(t)\xi(y)x_a^{-1}(t)$ est dans $\mathfrak{U}$. On voit de même que, si $y \in \mathfrak{M}$, $T_a(\xi(y)) = 0$, on a $x_{-a}(t)yx_{-a}^{-1}(t) \in \mathfrak{M}$ et

$$\xi(x_{-a}(t)yx_{-a}^{-1}(t)) = x_{-a}(t)\xi(y)x_{-a}^{-1}(t).$$

Ceci dit, soit m le plus grand entier > 0 tel que $\mathfrak{M} \cap \mathfrak{B}_m$ contienne un élément $y \neq I$. Si $y \in \mathfrak{M} \cap \mathfrak{B}_m$, soit $A(y)$ l'ensemble des racines fondamentales a telles que $T_a(\xi(y)) \neq 0$. Parmi tous les $y \in \mathfrak{M} \cap \mathfrak{B}_m$, $y \neq I$, choisissons en un, soit y_0, pour lequel le nombre d'éléments de $A(y)$ soit le plus petit possible; soit A l'ensemble $A(y_0)$. Nous allons montrer que les racines de A (s'il y en a) sont mutuellement orthogonales. Soit a un élément de A. Soit h' un élément de $\mathfrak{H}'$ tel que $h' \cdot X_a = X_a$; h' commute alors avec les éléments de $\mathfrak{X}_a$. L'élément $h'y_0h'^{-1}$ est dans $\mathfrak{B}_m \cap \mathfrak{M}$, et $\xi(h'y_0h'^{-1}) = h'\xi(y_0)h'^{-1}$ (lemme 5). On a $\xi(h'y_0h'^{-1}y_0^{-1}) = (\xi(y_0))^{-1}h'\xi(y_0)h'^{-1}$, et par suite, pour toute racine fondamentale a',

$$T_{a'}(\xi(h'y_0h'^{-1}y_0^{-1})) = T_{a'}(h'\xi(y_0)h'^{-1}) - T_{a'}(\xi(y_0)).$$

Or, si on pose $h' \cdot X_{a'} = \chi(a')X_a$, le second membre est $(\chi(a') - 1)T_a(\xi(y_0))$. Il est nul si a' n'est pas dans $A(y_0)$ et aussi si $a' = a$; donc $A(h'y_0h'^{-1}y_0^{-1})$ est contenu dans $A(y_0)$ mais ne contient pas a. En vertu de notre choix de y_0, ceci entraine $h'y_0h'^{-1}y_0^{-1} = I$ et par suite $\chi(a') = 1$ pour toute racine fondamentale $a' \in A(y_0)$. On en conclut que, si a, a' appartiennent à $A(y_0)$, tout homomorphisme de P dans K^* qui applique l'une des racines a, a' sur 1 applique aussi l'autre sur 1. Faisant alors usage du lemme 11, on voit que, si K n'est pas un corps à 2 ou à 4 éléments, les racines a, a', si elles sont distinctes, sont orthogonales. Supposons maintenant que K soit de caracté-

ristique 2. On sait que tout élément de $\mathfrak{V}_m/\mathfrak{V}_{m+1}$ est alors d'ordre 1 ou 2, d'où $y_0^2 \in \mathfrak{V}_{m+1}$. En vertu de notre choix de m, ceci entraine $y_0^2 = \mathrm{I}$, d'où $(\xi(y_0))^2 = I$, puisque $y \to (\xi(y))^{-1}$ est un homomorphisme. On a $\xi(y_0) \equiv \prod_{\iota \in A} x_a(t_a)$ (mod $\mathfrak{U}_2$), où $t_a = T_a(\xi(y_0)) \neq 0$. Nous allons calculer le carré de cet élément modulo $\mathfrak{U}_3$. On a $x_a^2(t_a) = I$. Si a, a' sont des racines de A telles que $a + a'$ ne soit pas racine, $x_a(t_a)$ commute avec $x_{a'}(t_{a'})$; dans le cas contraire, on a $C_{1,1;r,a'} = \pm 1$ puisque $a - a'$ n'est pas racine, et par suite $x_a(t_a)x_{a'}(t_a)x_i^{-1}(t_a) \equiv x_{a'}(t_{a'})x_{a+a}(t_a t_{a'})$ (mod $\mathfrak{U}_3$). Tenant compte de ce que $\mathfrak{U}_2/\mathfrak{U}_3$ est dans le centre de $\mathfrak{U}/\mathfrak{U}_3$, on voit que $(\xi(y_0))^2$ est congru modulo $\mathfrak{U}_3$ au produit des $x_{a+a'}(t_a t_{a'})$ pour tous les *ensembles* (pas les couples !) de racines a, a' de A telles que $a + a'$ soit racine. Par ailleurs, si $\{a, a'\}$, $\{a_1, a_1'\}$ sont deux distincts de ces ensembles, on a $a + a' \neq a_1 + a_1'$ en vertu de l'indépendence linéaire des racines fondamentales. La relation $(\xi(y_0))^2 = I$ implique donc qu'il n'y a aucun couple de racines a, a' de A telles que $a + a'$ soit racine, donc que les racinss de A sont mutuellement orthogonales.

Soit B l'ensemble des racines fondamentales b n'appartenant pas à A, donc telles que $T_b(\xi(y_0)) = 0$. Si $b \in B, t \in K$, on a $x_{-b}(t)y_0x_{-b}^{-1} \in \mathfrak{M}$ en vertu d'une remarque faite plus haut. Par ailleurs, cet élément est congru à y_0 modulo $\mathfrak{V}_{m+1}$. Comme $\mathfrak{M} \cap \mathfrak{V}_{m+1} = \{I\}$, on a $x_{-b}(t)y_0x_{-b}(t) = y_0$. Nous désignerons par $\mathfrak{M}'$ l'ensemble des $y \in \mathfrak{M}$ tels que, pour tout $b \in B$, y commute avec $x_{-b}(t)$ (pour $t \in K$) et que $T_b(\xi(y)) = 0$; on a donc $y_0 \in \mathfrak{M}'$. Comme l'application $y \to (\xi(y))^{-1}$ est un homomorphisme de $\mathfrak{M}, \mathfrak{M}'$ est un sous-groupe de $\mathfrak{M}$. Il résulte du lemme 8 qu'il y a un plus grand entier $m' > 0$ tel que $\mathfrak{M}'$ contienne un élément, soit y_1, distinct de I et tel que $\xi(y_1) \in \mathfrak{U}_{m'}$. Soit b une racine de B. Si c est une racine fondamentale telle que $T_{-c}(y_1) \neq 0$, il résulte du lemme 9 que tout élément de $\mathfrak{X}_{-b}$ commute avec tout élément de $\mathfrak{X}_{-c}$. Si $c \neq b, c$ est orthogonale à b; car, sinon, $-b-c$ serait une racine, mais non $b - c$, et on aurait $N_{-b-c} = \pm l$, d'où $x_{-b}(1)\, x_{-c}(1)x_{-b}^{-1}(1) \equiv x_{-c}(1)x_{-b-c}(\pm 1)$ (mod $\mathfrak{V}_3$), ce qui n'est pas. Si $c \in A$, c'est orthogonale à toutes les racines de A autres qu'elle-même ; elle est donc alors orthogonale à toutes les racines fondamentales autres qu'elle-même. Mais, $\mathfrak{g}_C$ étant simple, le graphe qui lui est associé est connexe, et cette situation ne peut se produire que si $\mathfrak{g}_C$ est de rang 1, donc de type (A_1).

Supposons maintenant que $\mathfrak{g}_C$ ne soit pas de type (A_1). Il résulte alors de ce que nous venons d'établir que $T_{-a}(y_1) = 0$ pour toute racine $a \in A$. Nous allons voir que, si $a \in A$, $x_a(1)y_1x_i^{-1}(1)$ appartient à $\mathfrak{M}'$. Cet élément est dans $\mathfrak{M}$, puisque $T_{-a}(y_1) = 0$, et

$$\xi(x_a(1)y_1x_i^{-1}(1)) = x_a(1)\xi(y_1)x_i^{-1}(1).$$

Si $b \in B$, b est distincte de a et $a - b$ n'est pas une racine, d'où il résulte que les éléments de $\mathfrak{X}_{-b}$ commutent avec ceux de $\mathfrak{X}_a$; commutant avec y_1, ils commutent aussi avec $x_a(1)y_1x_i^{-1}(1)$. Par ailleurs, on

$$x_a(1)\xi(y_1)x_a^{-1}(1) \equiv \xi(y_1) \qquad \text{(mod } \mathfrak{U}_2),$$

d'où $T_b(\xi(x_a(1)y_1x_i^{-1}(1)) = T_b(\xi(y_1)) = 0$. Ceci établit bien que $x_a(1)y_1x_a^{-1}(1) \in \mathfrak{M}'$.

L'elément $x_a(1)y_1x_i^{-1}(1)y_1^{-1}$ est dans $\mathfrak{M}'$ et son image par ξ est $(\xi(y_1))^{-1}x_a(1)$ $\xi(y_1)x_a^{-1}(1)$; comme $\xi(y_1)$ est dans $\mathfrak{U}_m$, cet élément est dans $\mathfrak{U}_{m'+1}$. En vertu de la définition de m', on a $y_1 = x_a(1)y_1x_i^{-1}(1)$: y_1 et $\xi(y_1)$ commutent donc avec $x_a(1)$. Par ailleurs, si $b \in B$, y_1 commute avec $x_{-b}(1)$, et il en est de même de $\xi(y_1)$, car, $T_b(\xi(y_1))$ etant nul, on a $\xi(y_1) = \xi(x_{-b}(1)y_1x_{-b}^{-1}(1)) = x_{-b}(1)\xi(y_1)x_{-b}^{-1}(1)$. L'élément $z = y_1\xi(y_1)$ est dans H. Soit R l'ensemble des racines r telles que ou bien $r < 0$, $T_r(y_1) \neq 0$ ou bien $r > 0$, $T_r(\xi(y_1)) \neq 0$; z appartient donc au groupe engendré par les $\mathfrak{X}_r$ pour $r \in R$. Par ailleurs, il résulte du lemme 9 que, si $r \in R$, tout élément de $\mathfrak{X}_r$ commute avec tout élément de $\mathfrak{X}_a$ et avec tout élément de $\mathfrak{X}_{-b}$, d'où $r(H_a) \geqq 0$, $r(H_b) \leqq 0$ en vertu du lemme 10.

Soient $a(1), \ldots, a(l)$ les racines fondamentales. Choisissons des nombres réels λ_i $(1 \leqq i \leqq l)$ linéairement indépendants par rapport au corps des rationnels et tels que $\lambda_i > 0$ si $a(i) \in A$, $\lambda_i < 0$ si $a(i) \in B$ (ce qui est evidemment possible). Si u est un élément $\neq 0$ du groupe P_r engendré par les racines, les $u(H_{a(i)})$ sont des entiers non tous nuls, et par suite $\sum_{i=1}^{l} \lambda_i u(H_{a(i)}) = f(u)$ est un nombre réel $\neq 0$. On peut définir sur P_r une structure de groupe ordonné en prenant comme ensemble d'éléments positifs dans P_r l'ensemble des u tels que $f(u) > 0$, il est évident que, relativement à cette relation d'ordre sur P_r, les racines de l'ensemble R sont toutes positives. Notre relation d'ordre détermine un système fondamental F de racines de $\mathfrak{g}$, et il y a une opération w du groupe de Weyl qui transforme F en le systéme $\{a(1), \ldots, a(l)\}$. Il y a une opération ω de $G' \cap \mathfrak{W}$ telle pue $\zeta(\omega) = w$ (lemme 1); puisque $\omega\mathfrak{X}_r\omega^{-1} = \mathfrak{X}_{w(r)}$, les transformés par ω des $\mathfrak{X}_r$, $r \in R$, sont dans $\mathfrak{U}$, d'où $\omega z \omega^{-1} \in \mathfrak{U}$. Mais cet élément est aussi dans H, ce qui nous amène à une contradiction avec l'hypothèse que $H \cap \mathfrak{H}\mathfrak{U} = \{I\}$.

Supposons maintenant que $\mathfrak{g}_\sigma$ soit de type (A_1) mais que K contienne plus de 3 éléments. Il n'y a alors qu'une seule racine positive a, et $G' = \phi_a(SL(2; K))$. Or, le quotient de $SL(2; K)$ par son centre est simple si K contient plus de 3 éléments ([7]). Le noyau de ϕ_a se compose des matrices J et $-J$, J étant la matrice unité: c'est le centre de $SL(2; K)$, et il en résulte que G' est simple. Le groupe $H \cap G'$ est $\neq \{I\}$, car, si $y \in \mathfrak{M}$, $y\xi(y)$ appartient à H et à $\mathfrak{X}_{-a}\mathfrak{X}_a \subset G'$; on a donc $H \cap G' = G'$, en contradiction avec l'hypothèse que $H \cap \mathfrak{H}\mathfrak{U} = \{I\}$. Cette dernière hypothèse est donc fausse.

LEMME 12. *Sauf dans le cas où $\mathfrak{g}_\sigma$ est de type (A_1) et K a au plus 3 elements, H contient un element $\neq I$ du centre de $\mathfrak{U}$.*

Soit hx un élément $\neq I$ de $H \cap \mathfrak{H}\mathfrak{U}$, avec $h \in \mathfrak{H}$, $x \in \mathfrak{U}$. Supposons d'abord que $h \neq I$. Il y a alors au moins une racine r telle que $h \cdot X_r = cX_r$ avec un $c \neq 1$. Comme $h \cdot X_{-r} = c^{-1}X_{-r}$, on peut supposer $r > 0$. On a $h^{-1}x_r(1)h = x_r(c^{-1})$ et par suite $x_r(1)hx_r^{-1}(1) = hx_r(c^{-1} - 1)$. L'élément $x_r(1)hxx_r^{-1}(1)$ appartient à H; il est égal à $hx_r(c^{-1} - 1)(x_r(1)xx_r^{-1}(1))$. Or, si k est la hauteur de r, $\mathfrak{U}_k/\mathfrak{U}_{k+1}$ est dans le centre de $\mathfrak{U}/\mathfrak{U}_{k+1}$, d'où $x_r(1)xx_r^{-1}(1) \equiv x \pmod{\mathfrak{U}_{k+1}}$. Soit $x' = x_r(c^{-1} - 1)x_r(1)xx_r^{-1}(1)$; on a $x' \equiv x_r(c^{-1} - 1)x \pmod{\mathfrak{U}_{k+1}}$, d'où $x' \neq x$ puisque $c^{-1} \neq 1$. L'élément hx' étant dans H, il en est de même de $x^{-1}x'$, ce qui montre

que $H \cap \mathfrak{U} \neq \{I\}$. Soit alors m le plus grand entier > 0 tel que $H \cap \mathfrak{U}_m$ contienne un élément, soit x, distinct de I. Soit s une racine positive quelconque, et soit $t \in K$. Alors l'élément $x^{-1}\, x_s(t) x x_s^{-1}(t)$ est dans H, et aussi dans $\mathfrak{U}_{m+1}$ puisque $\mathfrak{U}_m/\mathfrak{U}_{m+1}$ est dans le centre de $\mathfrak{U}/\mathfrak{U}_{m+1}$. Cet élément est donc I, et x commute avec $x_s(t)$; x est donc dans le centre de $\mathfrak{U}$.

Soit x un élément de H appartenant au centre de $\mathfrak{U}$. Si s est une racine telle que $T_s(x) \neq 0$, et si r est une racine positive quelconque, tout élément de $\mathfrak{X}_s$ commute avec tout élément de $\mathfrak{X}_r$ (lemme 9), d'où $s(H_r) \geqq 0$ (lemme 10). Nous appellerons *dominante* une racine s telle que $s(H_r) \geqq 0$ pour toute racine $r > 0$. Une telle racine est nécessirement positive; le raisonnement qu'on vient de faire (appliqué au cas où $H = G$) montre qu'il y a au moins une racine dominante.

LEMME 13. *Il ne peut exister plus de deux racines dominantes; si $\mathfrak{g}$ est de l'un des types $(A_l), (D_l)\,(l \geqq 4)$ ou $(E_l)\,(l = 6, 7$ ou $8)$, il n'y a qu'une seule racine dominante. Si $\mathfrak{g}_C$ est de type (G_2) et si K n'est pas de caractéristique 3, il n'y a qu'une racine dominate s telle que $\mathfrak{X}_s$ soit dans le centre de $\mathfrak{U}$. S'il y a deux racines dominantes s et s', ces racines ne sont pas orthogonales et ont des longueurs différentes; si $\mathfrak{g}_C$ est de rang > 2, on peut supposer (en rangeant s, s' dans un ordre convenable) qu'il existe une racine c linéairement indépendante de s, s' qui possède les propriétés suivantes: $s + c$ est une racine, mais aucune des combinaisons $s - c, s + 2c\ 2s + c, s' - c, s' + c$ n'est une racine.*

Soient $a(1), \ldots, a(l)$ les racines fondamentales, et soit $s = \sum_{i=1}^{l} c_i a(i)$ une racine dominante, les c_i étant des entiers $\geqq 0$. On a $s(H_{a(j)}) = 2c_j + \sum_{i \neq j} (a(i))(H_{a(j)})$. Or, si i, j sont des indices distincts, $a(i) - a(j)$ n'est pas une racine, d'où $(a(i))(H_{a(j)}) \leqq 0$. De plus, si $l > 1$, il y a au moins un $i \neq j$ tel que $(a(i))(H_{a(j)}) < 0$, car sinon $a(j)$ serait orthogonale à toutes les autres racines fondamentales, ce qui est impossible, $\mathfrak{g}_C$ étant simple. La relation $s(H_{a(j)}) \geqq 0$ montre alors que $c_j > 0$; il en est de même si $l = 1$; les c_i sont donc tous > 0. Supposons qu'il y ait une autre racine dominante s'. On a alors $s(H_{s'}) = \sum_{i=1}^{l} c_i (a(i))(H_{s'})$. Or, les nombres $s'(H_{a(i)})$ sont tous $\geqq 0$ et l'un d'eux au moins est $\neq 0$ (car, sinon, s', étant orthogonale à toutes les racines fondamentales, le serait à toutes les racines, ce qui est absurde). Il en résulte que les $(a(i))(H_{s'})$ sont tous $\geqq 0$ et que l'un de ces nombres est > 0; on a donc $s(H_{s'}) > 0$, et il en résulte que $s - s'$ est une racine. Supposons s et s' telles que $s > s'$, d'où $s - s' > 0$. On a alors $s'(H_{s-s'}) \geqq 0$, d'où $(s - s')(H_{s'}) \geqq 0$ et $s(H_{s'}) \geqq s'(H_{s'}) = 2$. On sait qu'il en résulte que la longueur de s est strictement supérieure à celle de s' (formule (1), §I). Par ailleurs, $\mathfrak{g}_C$ étant simple, l'ensemble des longueurs des racines ne peut contenir plus de deux éléments; il en résulte qu'il ne peut y avoir plus de 2 racines dominantes. Si $\mathfrak{g}_C$ est de l'un des types $(A_l), (D_l)\,(l \geqq 4)$ ou $(E_l)(l = 6, 7$ ou $8)$, toutes les racines ont la même longueur, et il n'y a qu'une seule racine dominantes. Supposons que $\mathfrak{g}_C$ soit de type (G_2), et soient a, b les racines fondamentales, les racines positives étant $a, b, a + b, 2a + b, 3a + b, 3a$

$+ 2b$. Il est clair que les éléments de $\mathfrak{X}_{3a+2b}$ commutent avec ceux de $\mathfrak{X}_r$ pour toute racine $r > 0$, donc que $3a + 2b$ est dominante. On a $a(H_a) = b(H_b) = 2$, $b(H_a) = -3$, $a(H_b) = -1$; il en résulte que $(2a + b)(H_a) = 1$, $(2a + b)(H_b) = 0$, donc que $2a + b$ est dominante. On a $N_{a,2a+b} = \pm 3$, d'où $x_a(1)x_{2a+b}(1)x_i^{-1}(1) = x_{2a+b}(1)x_{3a+b}(\pm 3)$. Il en résulte que, si K n'est pas de caractéristique 3, $\mathfrak{X}_{2a+b}$ n'est pas dans le centre de $\mathfrak{U}$.

Supposons maintenant qu'il y ait 2 racines dominantes distinctes s et s' et que $\mathfrak{g}_C$ soit de rang > 2. Il y a un système fondamental de racines qui contient $-s'$ ainsi qu'une racine s_0 telle que $s = -\lambda s' + \mu s_0$, λ et μ étant des entiers $\geqq 0$ (lemme 1, §I) On a $\mu > 0$. Si r est une racine > 0, on a $\mu s_0(H_r) = s(H_r) + \lambda s'(H_r) \geqq 0$, ce qui montre que s_0 est dominante. Comme $s_0 \neq s'$, on a $s_0 = s$, $\lambda = 0$, $\mu = 1$. Puisque $\mathfrak{g}_C$ est de rang > 2, le système fondamental qui contient $-s'$ et s contient au moins une troisième racine; le graphe associé à $\mathfrak{g}_C$ étant connexe, il y a une racine c de ce système qui n'est pas orthogonale à la fois à s et à s'. Puisque $-s', s, c$ font partie d'un même système fondamental, ni $s' + c$ ni $s - c$ n'est une racine. Le graphe associé à $\mathfrak{g}_C$ ne contenant aucun triangle et s, s' n'étant pas orthogonales, c est orthogonale à l'une des racines s, s'. Supposons que ce soit à s'. Alors $s + c$ est une racine mais $s' - c$ n'en est pas une. Par ailleurs, nous avons vu que s et s' n'ont pas la même longueur; un examen des graphes associés aux divers types d'algèbres simples montre alors que le fait que c ne soit pas orthogonale à s entraîne que c et s ont même longueur. Il résulte alors de la formule (1), §I que $c(H_s) = s(H_c)$; le produit de ces deux nombres étant $\leqq 3$ (formule (3), §I) ils sont tous deux égaux à ± 1; comme $s - c$ n'est pas racine, $c(H_s) = s(H_c) = -1$ et ni $s + 2c$ ni $2s + c$ n'est une racine. Si maintenant c est orthogonale à s, $(-s') + c$ est une racine, mais $(-s') - c$ n'en est pas une, on a $c(H_{s'}) = (-s')(H_c) = -1$, ni $(-s') + 2c$ ni $(-2s') + c$ n'en n'est une racine, et $s + c$ n'est pas une racine. Remplaçant c par $-c$ et échangeant s et s', on obtient une racine ayant les propriétés requises.

LEMMA 14. *Supposons que l'on ne soit pas dans l'un des cas suivants*: 1) $\mathfrak{g}_C$ *est de type* (A_1) *et* K *a au plus* 3 *éléments*; 2) $\mathfrak{g}_C$ *est de type* (B_2) *et* K *n'a que deux éléments. Alors il y a une racine* r *telle que* $H \cap \mathfrak{X}_r \neq \{I\}$.

S'il n'y a qu'une seule racine dominante s telle que $\mathfrak{X}_s$ appartienne au centre de $\mathfrak{U}$, tout élément de H appartenant au centre de $\mathfrak{U}$ est dans $\mathfrak{X}_s$ (lemme 9). Supposons qu'il y en ait deux, soient s et s'; H contient alors un élément de la forme $x_s(t)x_{s'}(t')$ où t, t' ne sont pas tous deux nuls, et il suffit manifestement de considérer le cas où $tt' \neq 0$. Supposons d'abord que K contienne plus de 2 éléments. Il est alors impossible que K soit un corps à 4 éléments et que $\mathfrak{g}$ soit de type (G_2) (lemme 13); on en déduit qu'on peut ranger s et s' dans un ordre tel qu'il existe un homorphisme du groupe P des poids dans le groupe multiplicatif K^* des éléments $\neq 0$ de K qui applique s sur 1 et s' sur un élément $c \neq 1$ (lemme 11; on se souviendra que s, s' ne sont pas orthogonales). Il y a donc un $h' \in H'$ tel que $h' \cdot X_s = X_s$, $h' \cdot X_{s'} = cX_{s'}$. L'élément $h'(x_s(t)x_{s'}(t'))h'^{-1} = x_s(t)x_{s'}(ct')$ est dans H, et il en est de même

de $x_{s'}((c-1)t')$, qui est $\neq I$. Supposons maintenant que K ne contienne que 2 éléments et que $\mathfrak{g}_C$ ne soit pas de type (B_2). Alors, il résulte du lemme 13 que $\mathfrak{g}_C$ ne peut être ni du type (A_2) ni du type (G_2), donc que $\mathfrak{g}_C$ est de rang >2; on peut supposer qu'il y a une racine c telle que $s+c$ soit une racine, mais qu'aucune des combinaisons $s-c, s+2c\ 2s+c, s'-c, s'+c$ ne soit une racine. On a $C_{1,1;c,s} = N_{c,s} = \pm 1$, et $(1,1)$ est le seul couple d'entiers $i>0, j>0$ tel que $ic+js$ soit une racine. On a donc

$$x_c(1)x_s(t)x_c^{-1}(1) = x_s(t)x_{s+c}(\pm t) = x_{s+c}(\pm t)x_s(t)$$

(car $(s+c)+s$ n'est pas racine). Puisque $s'+c$ n'est pas racine, $x_c(1)$ commute avec $x_{s'}(t')$; l'élément

$$x_s(1)\,(x_s(t)x_{s'}(t'))x_c^{-1}(1)\,(x_s(t)x_{s'}(t'))^{-1} = x_{s+c}(\pm t)$$

appartient à H, ce qui démontre le lemme 14.

LEMME 15. *Si r est une racine telle que $H \cap \mathfrak{X}_r \neq \{I\}$, on a $\mathfrak{X}_r \subset H$.*

Soit t un élément $\neq 0$ de K tel que $x_r(t) \in H$. Si K n'a que deux éléments, on a $\mathfrak{X}_r = \{I, x_r(t)\}$; si K n'a que 3 éléments, on a $\mathfrak{X}_r = \{I, x_r(t), x_r^{-1}(t)\}$, et le lemme est vrai dans ces cas. Supposons que K ait plus de 3 éléments. Soit H^* l'ensemble des éléments M de $SL(2; K)$ tels que $\phi_r(M) \in H$; comme $\phi_r(SL(2; K)) \subset G'$ (lemme 1), H^* est un sous-groupe distingué de $SL(2; K)$. Ce groupe contient au moins un élément distinct de la matrice unité appartenant au groupe $\mathfrak{N}$ du lemme 1, §II; il n'est donc pas dans le centre de $SL(2; K)$. Or, le corps K ayant plus de 3 éléments, $SL(2; K)$ est son propre groupe des commutateurs et le quotient de ce groupe par son centre est simple ([7], Hilftssatz 1 and Hauptsatz). Il en résulte que $H^* = SL(2; K)$, ce qui démontre le lemme 15.

Soit R l'ensemble des racines r telles que $\mathfrak{X}_r \subset H$. Si $r \in R$ et si w est une opération du groupe de Weyl, $w(r)$ appartient à R. Il y a en effet un élément $\omega \in G' \cap \mathfrak{W}$ tel que $\zeta(\omega) = w$ (lemme 1), et on a $\mathfrak{X}_{w(r)} = \omega\mathfrak{X}_r\omega^{-1} \subset H$. Si donc λ est la longueur d'une racine de R, R contient toutes les racines de longueur λ (lemme 5, §I). Si toutes les racines, de $\mathfrak{g}_C$ ont même longueur, R est l'ensemble de toutes les racines, d'où $G' \subset H$. Supposons qu'il n'en soit pas ainsi. L'ensemble des racines fondamentales de longueur λ est non vide; il en résulte qu'il y a deux racines fondamentales a et b, de longueurs différentes, non orthogonales, telles que $a \in R$. Supposons d'abord que $\mathfrak{g}_C$ ne soit pas de type (G_2). Ce cas se décompose en deux suivant que $b+2a$ ou $a+2b$ est racine. Si $b+2a$ est racine, on a $\lambda(a) = \lambda(a+b), \lambda(b) = \lambda(b+2a)$ (cf. §I, X). On a, si $t, u \in K$,

$$x_b(t)x_a(u)x_b^{-1}(t) = x_a(u)x_{b+a}(C_{1,1;b,a}tu)x_{b+2a}(C_{1,2;b,a}tu^2).$$

Or on a $C_{1,2;b,a} = M_{a,b,2} = (1/2)\,N_{a,b}N_{a,a+b} = (1/2)\,(\pm 1)\,(\pm 2) = \pm 1$. Comme $\mathfrak{X}_a$ et $\mathfrak{X}_{a+b}$ sont dans H, il en est de même de $\mathfrak{X}_{b+2a}$, et R est l'ensemble de toutes les racines. Supposons maintenant que $a+2b$ soit racine; a et $a+2b$ ont alors même longueur, et il en est de même de b et $a+b$. On a

$$x_b(t)x_a(u)x_b^{-1}(t) = x_{a'}(u)x_{a+b}(C_{1,1;b,a}tu)x_{a+2b}(C_{2,1;b,a}t^2u),$$

et $C_{1,1;b,a} = \pm 1$; comme $\mathfrak{X}_a$ et $\mathfrak{X}_{a+2b}$ sont dans H, il en est de même de $\mathfrak{X}_{a+b}$, et R est l'ensemble de toutes les racines.

Supposons maintenant que $\mathfrak{g}_C$ soit de type (G_2). Nous modifierons alors nos conventions: au lieu de stipuler que $r \in A$, nous supposerons que $3a + b$ ont une racine. Les racines $a, a + b$, $2a + b$ sont alors de même longueur, et il en est de même de $b, 3a + b, 3a + 2b$ (cf. formule (6), §I). On a

$$x_i(t)x_b(u)x_a^{-1}(t) = x_b(u)x_{i+b}(C_{1.1;a,b}tu)x_{2i+b}(C_{2,1;a,b}t^2u)x_{3i+b}(C_{3,1;a,b}t^3u)x_{3i+2b}(C_{3,2;a,b}t^3u^2)$$

et $C_{1,1;a,b} = N_{a,b} = \pm 1$, $C_{2,1;a,b} = (1/2)N_{a,b}N_{a,ab} = \pm 1$, $C_{3,1;a,b} = (1/6)N_{a,b}N_{a,a+b}$ $N_{a,2i+k} = \pm 1$; nous désignerons ces nombres par ε_1, ε_2, et ε_3, et nous poserons $C = C_{3,2;a,b}$. Supposons d'abord que $b \in R$. Alors $x_i(t)x_b(u)x_a^{-1}(t) \in H$, et $\mathfrak{X}_{3i+b} \subset H$, $\mathfrak{X}_{3i+2b} \subset H$. Il en résulte que l'on a $x_{i+b}(\varepsilon_1 tu)x_{2i+b}(\varepsilon_2 t^2u) \in H$. Si K contient plus de deux éléments, soient t, t' des éléments distincts de K tous deux $\neq 0$. Posons $u = t', u' = t$; on a alors $tu = t'u'$, $t^2u \neq t'^2u'$. Il en résulte que $x_{2i+b}(t'^2u' - t^2u) \in H$, d'où $\mathfrak{X}_{2i+b} \subset H$ en vertu du lemme 15, et R est l'ensemble de toutes les racines. Supposons maintenant que $a \in R$. La formule écrite plus haut donne $x_b^{-1}(u)x_i(t)x_b(u) = x_{i+b}(\varepsilon_1 tu)x_{2i+b}(\varepsilon_2 t^2u)x_{3i+b}(\varepsilon_3 t^3u)x_{3i+2b}(Ct^3u^2)x_i(t)$. Elle montre que $x_{3i+b}(\varepsilon_3 t^3u)x_{3i+2b}(Ct^3u^2)$ appartient à H. Or, on a $x_b(u)x_{3i+b}$ $(\varepsilon_3 t^3u)x_b^{-1}(u) = x_{3i+b}(\varepsilon_3 t^3u)x_{3i+2b}(\varepsilon_3\varepsilon_4 t^3u)$, avec $\varepsilon_4 = N_{b,3i+b} = \pm 1$; de plus, $x_b(1)$ commute avec $x_{3i+2b}(Ct^3u^2)$. On en conclut que $x_{3i+2b}(\varepsilon_3\varepsilon_4 t^3u)$ appartient à H, et par suite que R contient toutes les racines.

Si R contient toutes les racines, H contient $\mathfrak{U}$ et $\mathfrak{V}$, donc G'. Nous avons donc démontré le

THÉORÈME 3. *Supposons que l'on ne soit pas dans l'un des cas suivants: a) K est un corps à 2 éléments, et $\mathfrak{g}_C$ est de l'un des types $(A_1), (B_2)$ ou (G_2); b) K est un corps à 3 éléments, et $\mathfrak{g}_C$ est de type (A_1). Alors tout sous-groupe H de G qui contient un élément différent de l'élément unité et qui est tel que $zHz^{-1} = H$ pour tout $z \in G'$ contient G'.*

COROLLAIRE. *Les hypothèses étant celles de théorème 3, G' est le groupe des commutateurs de G et est un groupe simple.*

Il est en effet clair que G' est un groupe simple non abélien, donc identique à son propre groupe des commutateurs, et par suite contenu dans le groupe des commutateurs de G. Par ailleurs, nous avons vu (lemme 4) que G/G' est isomorphe au groupe abélien $\mathfrak{H}/\mathfrak{H}'$, ce que G' contient le groupe des commutateurs de G.

Il est facile de déterminer l'ordre de G' dans le cas où K est un corps fini à q éléments. Rappelons en effet que $\mathfrak{H}'$ est isomorphe au groupe des homomorphismes du groupe P_r engendré par les racines dans K^*(le groupe multiplicatif des éléments $\neq 0$ de K) qui peuvent se prolonger en des homomorphismes de P dans K^*, tandisque $\mathfrak{H}$ est isomorphe au groupe de tous les homomorphismes de P_r dans K^*. Or, P et P_r sont des groupes isomorphes; l'indice de $\mathfrak{H}'$ dans $\mathfrak{H}$ est donc égal à l'ordre u du groupe des homomorphismes de P/P_r dans K^*. Mais le groupe P/P_r est isomorphe au centre du groupe compact simplement connexe correspondant au type de $\mathfrak{g}_C$. Il est cyclique

d'ordre $l+1$ si $\mathfrak{g}_C$ est de type (A_l), cyclique d'ordre 2 si $\mathfrak{g}_C$ est de l'un des types (B_l) ou (C_l) $(l \leqq 2)$, cyclique d'ordre 4 si $\mathfrak{g}_C$ est de type (D_l) avec $l \leqq 4$, l impair, produit direct de 2 groupes cycliques d'ordre 2 si $\mathfrak{g}_C$ est de type (D_l), $l \geqq 4$, l pair; il se réduit à son élément neutre si $\mathfrak{g}_C$ est de l'un des types (G_2), (F_4) ou (E_8); il est cyclique d'ordre 3 si $\mathfrak{g}_C$ est de type (E_6), et cyclique d'ordre 2 si $\mathfrak{g}_C$ est de type (E_7). Le nombre u a donc les valeurs suivantes:

si $\mathfrak{g}_C$ est de type (A_l), u est le p. g. c. d. de $l+1$ et de $q-1$,

si $\mathfrak{g}_C$ est de type (B_l), $l \geqq 2$ ou (C_l) $(l \geqq 3)$ ou (E_7), u est 1 ou 2 suivant que q est pair ou impair;

si $\mathfrak{g}_C$ est de type (D_l), $l \geqq 4$, impair, $u = 1$ si q est pair, $u = 2$ si $q \equiv 3 \pmod 4$, $u = 4$ si $q \equiv 1 \pmod 4$;

si $\mathfrak{g}_C$ est de type (D_l), $l \geqq 4$, pair, $u = 1$ si q est pair, $u = 4$ si q est impair;

si $\mathfrak{g}_C$ est de type (E_6), $u = 1$ si q est congru à 0 ou à $-1 \pmod 3$, $u = 3$ si $q \equiv 1 \pmod 3$;

si $\mathfrak{g}_C$ est de type (E_7), $u = 1$ si q est pair, $u = 2$ si q est impair;

si $\mathfrak{g}_C$ est de l'un des types (G_2), (F_4) ou (E_8), $u = 1$.

Tenant compte de la formule que nous avons donnée pour l'ordre de G, on voit que l'ordre de G' est

$$u^{-1} q^N \prod_{i=1}^{l} (q^{a(i)} - 1)$$

où N est le nombre des racines > 0 tandisque $a(i)$ sont les entiers tels que le polynome de Poincaré d'un groupe compact du type de $\mathfrak{g}_C$ soit

$$\prod_{i=1}^{l} (T^{2a(i)-1} - 1).$$

Rappelons que ces entiers ont les valeurs suivantes:

si $\mathfrak{g}_C$ est de type (A_l), $2, 3, \ldots, l$;

si $\mathfrak{g}_C$ est de l'un des types (B_l) ou (C_l), $2, 4, \ldots, 2l$;

si $\mathfrak{g}_C$ est de type (D_l), $l \geqq 4$, $2, 4, \ldots, 2l-2, l$;

si $\mathfrak{g}_C$ est de type (E_6): $2, 5, 6, 8, 9, 12$;

si $\mathfrak{g}_C$ est de type (E_7): $2, 6, 8, 10, 12, 14, 18$;

si $\mathfrak{g}_C$ est de type (E_8): $2, 8, 12, 14, 18, 20, 24, 30$;

si $\mathfrak{g}_C$ est de type (F_4): $2, 6, 8, 12$;

si $\mathfrak{g}_C$ est de type (G_2): $2, 6$.

§V. Quelques questions non résolues.

Nous indiquons ici quelques questions non résolues qui se posent à propos des résultats que nous avons exposés dans ce mémoire.

1. Il ne fait guère de doute que notre méthode, appliquée aux groupes classiques, conduise aux groupes simples déjà étudiés par Dickson et Dieudonné. D'une manière plus précise, le groupe simple G' que nous avons défini s'identifie presque certainement, dans le cas des groupes classiques, aux groupes suivants:

a) si $\mathfrak{g}_C$ est de type (A_l), au groupe projectif spécial d'un espace projectif de dimension l sur K (l étant > 1 si K n'a que 2 ou 3 éléments):

b) si $\mathfrak{g}_C$ est de type (B_l), au groupe des commutateurs du groupe projectif orthogonal d'une forme quadratique en $2l + 1$ varaibles à coefficients dans K d'indice maximal l ($l \geqq 2$, et $l \geqq 3$ si K n'a que 2 éléments);

c) si $\mathfrak{g}_C$ est de type (C_l), au quotient par son centre du groupe symplectique à $2l$ variables à coefficients dans K ($l \geqq 3$);

d) si $\mathfrak{g}_C$ est de type (D_l), au groupe des commutateurs du groupe projectif orthogonal d'une forme quadratique à $2l$ variables à coefficients dans K d'indice maximal l ($l \geqq 4$).

D'une manière générale, si L est un groupe linéaire complexe quelconque dont l'algèbre de Lie est isomorphe à $\mathfrak{g}_C$, il conviendrait d'étudier dans quel cas on peut associer à L un groupe linéaire L_K défini sur un corps K quelconque et tel que G' soit isomorphe au groupe des commutateurs du quotient de L_K par son centre.

2. Il conviendrait d'établir que les groupes G' relatifs soit à des algèbres de Lie simples $\mathfrak{g}_C$ non isomorphes entre elles soit à des corps de base K différents ne sont pas isomorphes entre eux (sauf en ce qui concerne les groupes des types (B_l) et (C_l) sur des corps de caractéristique 2). Dans le cas des corps de base finis, on peut pour ce faire utiliser le fait que, sauf pour un nombre fini d'exceptions, la caractéristique de K fournit le facteur primaire le plus grand de la décomposition de l'ordre de G' en facteurs premiers; on peut montrer assez facilement ainsi que les groupes exceptionnels fournissent en tous cas une infinité de groupes finis simples véritablement nouveaux. Dans le cas des corps infinis de caractéristique $p > 0$, il est peut être possible de se ramener au cas des corps de base finis au moyen d'une étude systématique des éléments d'ordres finis de G'. Mais il serait en tout état de cause préférable de trouver des méthodes plus intrinsèques, du genre de celles développées par Dieudonné, pour séparer les uns des autres les groupes G' des divers types.

3. Si K est un corps infini, le groupe G que nous avons défini est probablement toujours un groupe algébrique. Il conviendrait d'étudier son algèbre de Lie et notamment de déterminer dans quels cas cette algèbre de Lie est isomorphe à $\mathfrak{g}$, et dans quels cas G est la composante connexe de l'identité dans le groupe des automorphismes de $\mathfrak{g}$.

4. Il conviendrait de déterminer les groupes d'automorphismes des groupes simples G' que nous avons construits.

5. Le problème le plus important, et probablement le plus difficile, serait de généraliser les méthodes que nous avons employées en partant non pas d'une algèbre de Lie simple complexe $\mathfrak{g}_C$ mais d'une forme réelle $\mathfrak{g}_R$ de $\mathfrak{g}_C$. Si on prend pour $\mathfrak{g}_R$ la forme compacte, les résultats de Dieudonné semblent indiquer qu'il n'y a guère d'expoir d'arriver ainsi à des groupes simples; c'est aussi le cas où l'absence complète d'éléments nilpotents semble

opposer une barrière infranchissables à l'emploi de nos méthodes. Mais, dans le cas des autres formes réelles, on peut espérer qu'il y a assez d'éléments nilpotents pour permettre d'étendre le domaine des méthodes que nous avons appliquées ici.

BIBLIOGRAPHIE

[1] F. BRUHAT, Représentations induites des groupes de Lie semi-simples connexes, C. R. Acad. Sci. Paris, 238, p. 437–439, 1954.
[2] C. CHEVALLEY, Théorie des groupes de Lie, III (à paraître prochainement, librairie Hermann, Paris).
[3] L. DICKSON, Linear Groups, Teubner (Leipzig) 1901.
[4] L. DICKSON, Linear groups in an arbitrary field", Trans. Amer. Math. Soc., (1901) p. 363–394, A new system of simple groups, Math. Ann., 60 (1905) p. 137–150.
[5] J. DIEUDONNÉ, Sur les groupes classiques, Hermann, Paris, 1948.
[6] HARISH-CHANDRA, On some applications of the universal enveloping algebra of a semi-simple Lie algebra, Trans. of Amer. Math. Soc., 70(1951), p. 28–96.
[7] K. IWASAWA, Über die Einfacheit der speziellen projektiven Gruppen, Proc. Imp. Acad., Tokyo, 17, p. 57–60, 1941.
[8] K. IWASAWA, On some types of topological groups, Ann. of Math., 50, p. 507–557, 1949.
[9] I. SATAKE, On a theorem of E. Cartan, Journ. of the Math. Soc. of Japan, 2, p. 284–304, 1951.

COLUMBIA UNIVERSITY