PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

JACQUES TITS

Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples

Publications mathématiques de l'I.H.É.S., tome 31 (1966), p. 21-58
<http://www.numdam.org/item?id=PMIHES_1966__31__21_0>

SUR LES CONSTANTES DE STRUCTURE ET LE THÉORÈME D'EXISTENCE DES ALGÈBRES DE LIE SEMI-SIMPLES

par J. TITS

INTRODUCTION

Cet article a pour objet l'étude des constantes de structure des algèbres semi-simples complexes et l'exposé d'une nouvelle démonstration élémentaire du fait qu'à tout système de racines correspond une telle algèbre (théorème d'existence). (En fait, les algèbres semi-simples considérées seront définies sur un corps de caractéristique o quelconque, mais comme nous les supposerons toujours déployées, il n'y a pas là un gain de généralité essentiel par rapport au cas complexe, auquel nous nous restreignons dans cette introduction.)

Soient $\mathfrak{G}$ une algèbre de Lie semi-simple complexe, $\mathfrak{T}$ une sous-algèbre de Cartan, Σ le système des racines de $\mathfrak{G}$ relatives à $\mathfrak{T}$, et, pour toute racine $a \in \Sigma$, $\mathfrak{e}_a$ un vecteur propre associé à a. Les relations de structure de $\mathfrak{G}$ ont alors la forme suivante, où $a, b \in \Sigma$ et $\mathfrak{t} \in \mathfrak{T}$:

$$[\mathfrak{T}, \mathfrak{T}] = \{0\}$$

$$[\mathfrak{t}, \mathfrak{e}_a] = a(\mathfrak{t}) \cdot \mathfrak{e}_a$$

$$[\mathfrak{e}_a, \mathfrak{e}_b] = \begin{cases} \mathfrak{t}_a \in \mathfrak{T} & \text{si } a+b=0 \\ N_{a,b} \cdot \mathfrak{e}_{a+b} & \text{si } a+b \in \Sigma \\ 0 & \text{si } a+b \notin \Sigma \cup \{0\}. \end{cases}$$

Pour chaque paire a, $-a$ de racines opposées, on peut évidemment choisir $\mathfrak{e}_a$, $\mathfrak{e}_{-a}$ de telle sorte que $\mathfrak{t}_a = -a^*$, où a^* est défini par la relation bien connue

$$b(a^*) = 2(a, b)/(a, a) \qquad \text{pour tout } b \in \Sigma,$$

(,) désignant la forme de Killing (on s'arrange généralement pour que $t_a = a^*$, mais nous verrons que $\mathfrak{t}_a = -a^*$ est un choix plus « naturel »); alors se trouve automatiquement vérifiée la relation de H. Weyl [10] $N_{a,b} = N_{-a,-b}$. C. Chevalley a montré [3] qu'on peut en outre choisir les $\mathfrak{e}_a$ de telle façon que la valeur absolue de $N_{a,b}$ soit le plus petit entier positif f tel que $b-f.a$ ne soit pas une racine; on dit alors que les $\mathfrak{e}_a$ forment, avec une base de $\mathfrak{T}$, une *base de Chevalley* de $\mathfrak{G}$. Pour obtenir des relations de structure tout à fait explicites pour $\mathfrak{G}$ il reste à étudier la *question des signes des* $N_{a,b}$.

Dans la première partie de cet article, nous reprenons l'étude des constantes $N_{a,b}$ du point de vue suivant. Supposons qu'au lieu de fixer $\mathfrak{e}_a$ nous le laissions parcourir l'ensemble $\mathfrak{E}^*_a$ de tous les vecteurs propres non nuls associés à a; alors $N_{a,b}$ devient une fonction sur $\mathfrak{E}^*_a \times \mathfrak{E}^*_b \times \mathfrak{E}^*_{a+b}$ à valeur dans $\mathbf{C}^*$. Au n° 2.3, nous ramenons l'étude des fonctions $N_{a,b}$ en question à celle d'une fonction δ définie sur une partie de $\Sigma \times \Sigma \times \Sigma \times N \times N \times N$, où N désigne le normalisateur de $\mathfrak{T}$ dans le groupe simplement connexe G ayant $\mathfrak{G}$ pour algèbre de Lie (le double emploi malencontreux de la lettre N sera évité dans le corps du texte par le fait que nous n'utiliserons plus guère la notation $N_{a,b}$), et nous montrons au n° 2.6 que cette fonction δ peut être caractérisée par des relations simples, faisant seulement intervenir le système de racines Σ et le groupe « abstrait » N (et aussi certaines structures additionnelles dans N, structures susceptibles toutefois d'une description « directe » : cf. à ce sujet le n° 2.4 et la remarque *a)* de 2.6). Le passage des fonctions $N_{a,b}$ à la fonction δ est basée sur une propriété élémentaire du groupe SL_2, qui fait l'objet de la proposition 1 (n° 1.1).

On sait que le groupe N est une extension d'un groupe fini W, le *groupe de Weyl*, par un tore maximal T, et que N contient un sous-groupe fini $N_{\mathbf{Z}}$, le *groupe de Weyl étendu*, extension de W par le 2-groupe abélien élémentaire des éléments d'ordre 2 de T (ce groupe $N_{\mathbf{Z}}$, qui n'est défini qu'à conjugaison près, est aussi le groupe des points entiers de N pour une **Z**-structure convenable dans G; cf. par ex. [5], [9]). Au n° 2.9, nous examinons ce qui se passe lorsqu'on restreint le domaine de variation des trois derniers arguments de δ à $N_{\mathbf{Z}}$; il s'avère que ceci revient à restreindre le domaine de variation des $\mathfrak{e}_a$ à une « double base de Chevalley », c'est-à-dire à la réunion d'une base de Chevalley et de son opposée. De plus, nous observons que, dans ce cas, les trois premiers arguments de δ deviennent superflus, et que δ peut être remplacée par une fonction ε sur une partie de $N_{\mathbf{Z}} \times N_{\mathbf{Z}} \times N_{\mathbf{Z}}$, à valeurs dans l'ensemble $\{+1, -1\}$; c'est en somme la *fonction décrivant les signes des* $N_{a,b}$.

Le fait qu'on puisse donner des relations de structure explicites pour les algèbres semi-simples complexes suggère la possibilité de démontrer leur existence par simple vérification de la relation de Jacobi; une démonstration d'existence selon ce principe fait l'objet de la deuxième partie. Cette démonstration est sans doute plus longue et certainement moins « conceptuelle » que celle de Harish-Chandra-Jacobson [6], cependant elle peut présenter un certain intérêt propre : elle est à certains égards plus élémentaire, et surtout elle met en évidence, de façon « concrète », les propriétés particulières des systèmes de racines qui « font marcher » la relation de Jacobi.

Cette deuxième partie relève uniquement de la théorie des *algèbres* de Lie; à cet égard, elle est plus élémentaire que la première (où la théorie globale intervient aussi, par l'intermédiaire du groupe G), *dont elle est entièrement indépendante*, au moins du point de vue logique; nous y retrouvons d'ailleurs en fait l'essentiel des résultats de la première partie, mais sous une forme moins « naturelle » et de façon quelque peu détournée. Avertissons ici le lecteur d'une différence essentielle qu'il pourra observer entre les conceptions des deux parties. Dans la première, où il s'agit d'exposer des résultats en principe nouveaux, nous n'avons imposé aucune restriction aux moyens utilisés, pour autant qu'ils aident à atteindre le but plus rapidement, ou à mieux mettre en évidence la raison des propriétés établies ou la signification des notions introduites. Par contre, dans la deuxième partie, consacrée à une démonstration élémentaire d'un résultat bien connu, nous avons cherché à réduire les « prerequisites » à un minimum : en fait, outre les éléments de l'algèbre linéaire, nous y utilisons seulement un petit nombre de propriétés simples bien connues des systèmes de racines, propriétés rappelées au n° 3.2; la question des simplifications qui peuvent être apportées à la démonstration moyennant l'admission de tel ou tel préalable supplémentaire est brièvement discutée au n° 4.3.2. Par ailleurs, comme nous cherchons à donner une démonstration d'existence aussi courte que possible, les notations et définitions sont introduites dans la deuxième partie sans aucune « motivation »; celle-ci peut généralement être trouvée dans la première partie, qui fait ainsi en quelque sorte office d'introduction. Ceci explique qu'en dépit de la logique, nous ayons choisi de mettre en première place la partie la moins élémentaire de l'exposé, ce qui conduit d'ailleurs à quelques redites, heureusement peu importantes (n° 2.5).

L'article se termine par un appendice; l'objet des deux paragraphes qui le constituent est expliqué dans les premières lignes de ceux-ci et il n'y a rien d'autre à en dire ici.

Signalons enfin que certains des résultats de la première partie ont déjà été exposés dans [8].

CONSTANTES DE STRUCTURE

1. LE GROUPE SL_2

1.1. Une « trijection » canonique.

Dans tout l'article K *désigne un corps commutatif de caractéristique* 0.

Nous commençons par établir quelques propriétés élémentaires du groupe $SL_2(K)$ et de son algèbre de Lie $\mathfrak{SL}_2(K)$, notés ici simplement SL_2 et $\mathfrak{SL}_2$.

Posons

$$T=\left\{\begin{pmatrix} k & 0 \\ 0 & k^{-1}\end{pmatrix}\middle| k\in K^*\right\}, \qquad \mathfrak{T}=\left\{\begin{pmatrix} k & 0 \\ 0 & -k\end{pmatrix}\middle| k\in K\right\},$$

$$M=\left\{\begin{pmatrix} 0 & -k \\ k^{-1} & 0\end{pmatrix}\middle| k\in K^*\right\},$$

$$\mathfrak{h}_+=\begin{pmatrix} 1 & 0 \\ 0 & -1\end{pmatrix}, \qquad \mathfrak{h}_-=\begin{pmatrix} -1 & 0 \\ 0 & 1\end{pmatrix}, \qquad h=\begin{pmatrix} -1 & 0 \\ 0 & -1\end{pmatrix},$$

$$\mathfrak{E}_+=\left\{\begin{pmatrix} 0 & k \\ 0 & 0\end{pmatrix}\middle| k\in K\right\}, \qquad \mathfrak{E}_-=\left\{\begin{pmatrix} 0 & 0 \\ k & 0\end{pmatrix}\middle| k\in K\right\},$$

$$\mathfrak{E}_\pm^*=\mathfrak{E}_\pm-\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0\end{pmatrix}\right\}.$$

On notera que T est un tore maximal de SL_2, que $\mathfrak{T}$ est l'algèbre de Lie de T, que M est l'unique classe latérale (ne contenant pas l'élément neutre) de T dans son normalisateur, que $\mathfrak{E}_+$ et $\mathfrak{E}_-$ sont les espaces propres correspondant aux racines de $\mathfrak{SL}_2$ relatives à $\mathfrak{T}$, et enfin que $\mathfrak{h}_+$ et $\mathfrak{h}_-$ sont les éléments de $\mathfrak{T}$ caractérisés par la relation

$$[\mathfrak{h}_\pm, \mathfrak{x}]=2\mathfrak{x} \qquad \text{pour tout } \mathfrak{x}\in\mathfrak{E}_\pm. \tag{1}$$

Nous aurons aussi à faire usage du fait que, *dans l'algèbre des matrices d'ordre* 2,

$$\mathfrak{x}^2=0 \qquad \text{pour tout } \mathfrak{x}\in\mathfrak{E}_+\cup\mathfrak{E}_-. \tag{2}$$

Proposition 1. — *Soient* $\mathfrak{e}_+ \in \mathfrak{E}^*_+$, $\mathfrak{e}_- \in \mathfrak{E}^*_-$, $m \in \mathrm{M}$. *Alors, les relations suivantes sont équivalentes :*

$$\exp \mathfrak{e}_+ . \exp \mathfrak{e}_- . \exp \mathfrak{e}_+ = m; \tag{3}$$

$$\exp \mathfrak{e}_- . \exp \mathfrak{e}_+ . \exp \mathfrak{e}_- = m. \tag{4}$$

Elles définissent trois bijections

$$\begin{array}{ccc} \mathfrak{E}^*_+ & \longleftrightarrow & \mathfrak{E}^*_- \\ & \nwarrow\!\!\searrow \quad \swarrow\!\!\nearrow & \\ & \mathrm{M} & \end{array} \tag{5}$$

c'est-à-dire qu'étant donné arbitrairement l'un des trois éléments $\mathfrak{e}_+$, $\mathfrak{e}_-$ *et* m, *il en existe deux autres, bien déterminés, tels que* (3) *et* (4) *soient vérifiées. L'élément* $\mathfrak{e}_-$ *associé à un élément* $\mathfrak{e}_+$ *donné est aussi caractérisé par la relation*

$$[\mathfrak{e}_+, \mathfrak{e}_-] = -\mathfrak{h}_+, \tag{6}$$

et l'élément m *défini par* (3) *est tel que*

$$(\mathrm{Ad}\, m)(\mathfrak{e}_+) = \mathfrak{e}_-. \tag{7}$$

Enfin, si $\mathfrak{e}_+$, $\mathfrak{e}_-$ *et* m *vérifient* (3), *il en est de même de* $k.\mathfrak{e}_+$, $k^{-1}.\mathfrak{e}_-$ *et*

$$\begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix} . m$$

quel que soit $k \in \mathrm{K}^* = \mathrm{K} - \{0\}$.

La preuve est un simple calcul. Les triples d'éléments vérifiant (3) et (4) ont pour expression générale

$$\mathfrak{e}_+ = \begin{pmatrix} 0 & k \\ 0 & 0 \end{pmatrix}, \qquad \mathfrak{e}_- = \begin{pmatrix} 0 & 0 \\ -k^{-1} & 0 \end{pmatrix}, \qquad m = \begin{pmatrix} 0 & k \\ -k^{-1} & 0 \end{pmatrix} \quad (k \in \mathrm{K}^*).$$

On observera que ces matrices satisfont aussi à la relation

$$m = \mathfrak{e}_+ + \mathfrak{e}_-. \tag{8}$$

Il convient cependant, à ce propos, de faire une

Remarque importante. — Par suite de la notation utilisée, qui identifie SL_2 et $\mathfrak{SL}_2$ à des parties de l'algèbre des matrices d'ordre 2, l'ensemble M (donc l'élément m) est contenu « accidentellement » à la fois dans SL_2 et dans $\mathfrak{SL}_2$. Comme il ressort du contexte, c'est en tant que partie de SL_2 qu'il est envisagé ici; en particulier, (3), (4), (6) et (7) *expriment des relations intrinsèques entre l'élément* m *du groupe algébrique* SL_2 *et les éléments* $\mathfrak{e}_+$ *et* $\mathfrak{e}_-$ *de son algèbre de Lie.*

Il n'en est pas de même de (8), qui fait intervenir la notation matricielle, et qui exprime donc une propriété particulière de la « représentation linéaire naturelle » (de dimension 2) de SL_2.

1.2. Représentations linéaires.

Proposition 2. — Soient $\mathfrak{e}_+ \in \mathfrak{E}_+^*$, $\mathfrak{e}_- \in \mathfrak{E}_-^*$ *et* $m \in \mathrm{M}$ *vérifiant* (3) *et* (4), *et soit* $\mathfrak{V}$ *un module de représentation irréductible de* $\mathfrak{S}\mathfrak{L}_2$ *sur* K, *de dimension* $d+1$. *Alors,* $\mathfrak{V}$ *possède une base* $\{\mathfrak{v}_i\}$ $(i=-d, \ -d+2, \ldots, d-2, d)$ *telle que*

(9) $$\mathfrak{h}_+(\mathfrak{v}_i) = i \cdot \mathfrak{v}_i;$$

(10) $$\mathfrak{e}_\pm(\mathfrak{v}_i) = \begin{cases} 0 & si \quad i = \pm d \\ \frac{1}{2}(-i \pm d) \cdot \mathfrak{v}_{i\pm 2} & si \quad i \neq \pm d \end{cases}$$

(dans cette dernière égalité, il faut prendre simultanément tous les signes supérieurs ou tous les signes inférieurs). La représentation donnée de $\mathfrak{S}\mathfrak{L}_2$ *« s'intègre » de façon unique en une représentation de* SL_2 *telle que*

(11) $$(\exp \mathfrak{x})(\mathfrak{v}) = \sum_{i=0}^{\infty} (i!)^{-1} \mathfrak{x}^i(\mathfrak{v})$$

pour tout $\mathfrak{x} \in \mathfrak{E}_+ \cup \mathfrak{E}_-$ *et tout* $\mathfrak{v} \in \mathfrak{V}$ *(la puissance* $\mathfrak{x}^i$ *est prise ici dans l'algèbre enveloppante universelle de* $\mathfrak{S}\mathfrak{L}_2$*; le second membre de* (11) *n'a qu'un nombre fini de termes non nuls en vertu de* (10)). *Pour cette représentation de* SL_2 *et pour toute base* $\{\mathfrak{v}_i\}$ *vérifiant* (10), *on a les relations*

(12) $$h(\mathfrak{v}_i) = (-1)^d \cdot \mathfrak{v}_i,$$

(13) $$m(\mathfrak{v}_i) = (-1)^{\frac{d+i}{2}} \cdot \mathfrak{v}_{-i}.$$

Identifions SL_2 et $\mathfrak{S}\mathfrak{L}_2$ respectivement avec le groupe endomorphismes de déterminant 1 et avec l'algèbre de Lie des endomorphismes de trace 0 d'un espace vectoriel $\mathfrak{U}$ de dimension 2. On sait que $\mathfrak{S}\mathfrak{L}_2$ possède, à équivalence près, une seule représentation irréductible de dimension $d+1$, à savoir, la représentation induite dans la d-ième puissance symétrique de $\mathfrak{U}$ par la représentation « naturelle » de $\mathfrak{S}\mathfrak{L}_2$ dans $\mathfrak{U}$ (cf. par ex. [6]). Nous pouvons donc, sans nuire à la généralité, supposer que $\mathfrak{V}$ est la d-ième puissance symétrique de $\mathfrak{U}$. La représentation de SL_2 dans $\mathfrak{V}$ induite par la représentation « naturelle » dans $\mathfrak{U}$ satisfait évidemment à la relation (11), et celle-ci la caractérise puisque SL_2 est engendré par $\exp(\mathfrak{E}_+ \cup \mathfrak{E}_-)$.

Choisissons dans $\mathfrak{U}$ une base $\{\mathfrak{u}, \mathfrak{u}'\}$ telle que

$$\mathfrak{e}_+(\mathfrak{u}) = \mathfrak{u}' \quad \text{et} \quad \mathfrak{e}_-(\mathfrak{u}') = -\mathfrak{u},$$

de sorte que, vu (2), (6) et (8),

$$\begin{aligned} \mathfrak{e}_+(\mathfrak{u}') &= \mathfrak{e}_-(\mathfrak{u}) = 0, \\ \mathfrak{h}_+(\mathfrak{u}) &= m(\mathfrak{u}') = -\mathfrak{u}, \\ \mathfrak{h}_+(\mathfrak{u}') &= m(\mathfrak{u}) = \mathfrak{u}'. \end{aligned}$$

Les monômes

$$\mathfrak{v}_i = \mathfrak{u}^{\frac{d-i}{2}} \cdot \mathfrak{u}'^{\frac{d+i}{2}} \qquad (i=-d, \ -d+2, \ldots, d-2, d)$$

forment une base de $\mathfrak{V}$ et il résulte de calculs immédiats qu'elle satisfait aux relations (9), (10), (12) et (13). En outre, si $\{\mathfrak{v}'_i\}$ est une base quelconque vérifiant (10), la transformation linéaire de $\mathfrak{V}$ qui applique $\mathfrak{v}_i$ sur $\mathfrak{v}'_i$ pour tout i commute avec les éléments de $\mathfrak{E}_+$ et $\mathfrak{E}_-$ (considérés comme endomorphismes de $\mathfrak{V}$) donc aussi, vu (11), avec les éléments de SL_2, et la base $\{\mathfrak{v}'_i\}$ satisfait aussi aux relations (12) et (13), ce qui achève la démonstration.

1.3. *Corollaire. — Notons a la racine de $\mathfrak{S}\mathfrak{L}_2$ à laquelle appartient $\mathfrak{e}_+$, et soient r l'unique élément non neutre du groupe de Weyl, b un poids et $\mathfrak{v}$ un vecteur de poids b dans un module de représentation irréductible de dimension $d+1$. Alors,*

(14) *si* $b=-a/2$ (i.e. $r(b)=b+a$), *on a*

$$e_+(\mathfrak{v})=(-1)^{\left(\frac{d-1}{2}\right)}\cdot\binom{\frac{d+1}{2}}{}\cdot m(\mathfrak{v}),$$

et

(15) *si* $b=0$ (i.e. $r(b)=b$), *on a* $m(\mathfrak{v})=(-1)^{d/2}\cdot\mathfrak{v}$.

2. LES CONSTANTES DE STRUCTURE D'UNE ALGÈBRE SEMI-SIMPLE DÉPLOYÉE

2.1. Notations.

Tous les groupes algébriques dont il sera question sont définis sur K. Un groupe et l'ensemble de ses points rationnels sur K seront toujours désignés par le même symbole. Le gain en généralité résultant du fait qu'au lieu du corps des complexes, on considère un corps K de caractéristique 0 quelconque, est assez inessentiel; il n'y aura donc pas grand inconvénient, pour le lecteur qui préfère la théorie des groupes de Lie à celle des groupes algébriques, à supposer que $K=\mathbf{C}$, et à traduire les expressions « groupe algébrique semi-simple déployé sur K » et « tore maximal », par « groupe analytique complexe semi-simple » et « sous-groupe de Cartan ».

Les notations suivantes seront utilisées tout au long du § 2 :

G est un groupe algébrique semi-simple déployé simplement connexe, $\mathfrak{G}$ son algèbre de Lie, T un tore maximal de G, $\mathfrak{T}$ l'algèbre de Lie de T, N le normalisateur de T dans G, $\mathfrak{T}'$ le dual de $\mathfrak{T}$, $\Sigma(\subset\mathfrak{T}')$ l'ensemble des racines de $\mathfrak{G}$ relatives à $\mathfrak{T}$, $W=N/T$ le groupe de Weyl (identifié éventuellement, de la façon habituelle, à un groupe de transformations linéaires de $\mathfrak{T}$ ou de $\mathfrak{T}'$) et $\pi: N\to W$ la projection canonique;

dans $\mathfrak{T}'$, nous choisissons une fois pour toutes un produit scalaire (,) non dégénéré invariant par W, et tel que pour toute racine a, (a, a) soit un nombre rationnel positif, noté $\lambda(a)$;

pour toute racine $a\in\Sigma$, nous notons $r_a(\in W)$ la réflexion de $\mathfrak{T}'$ par rapport à l'hyperplan orthogonal à a, a^* l'élément de $\mathfrak{T}$ défini par la relation

$$\mathfrak{t}'(a^*)=2\cdot(a,\mathfrak{t}')/(a,a) \qquad \text{pour tout } \mathfrak{t}'\in\mathfrak{T}',$$

$\mathfrak{E}_a = \{\mathfrak{g} \in \mathfrak{G} \mid [\mathfrak{t}, \mathfrak{g}] = a(\mathfrak{t}) . \mathfrak{g}$ pour tout $\mathfrak{t} \in \mathfrak{T}\}$ la sous-algèbre à une dimension de $\mathfrak{G}$ correspondant à a, $\mathfrak{G}_a (\cong \mathfrak{S}\mathfrak{L}_2)$ la sous-algèbre engendrée par $\mathfrak{E}_a$ et $\mathfrak{E}_{-a}$, $G_a (\cong SL_2)$ le sous-groupe connexe de G « engendré par $\mathfrak{G}_a$ », nous posons $\mathfrak{E}_a^* = \mathfrak{E}_a - \{0\}$, $\mathfrak{T}_a = \mathfrak{T} \cap \mathfrak{G}_a$, $T_a = T \cap G_a$ (tore maximal de G_a « engendré par $\mathfrak{T}_a$ »), $N_a = N \cap G_a$ (normalisateur de T_a dans G_a), $M_a = N_a - T_a$ (classe latérale de T_a dans N_a), et, pour tout $k \in K^*$, nous désignons par k_a l'image de la matrice $\begin{pmatrix} k & 0 \\ 0 & k^{-1} \end{pmatrix}$ par un homomorphisme $SL_2 \to G_a$ quelconque dont la dérivée à l'élément neutre applique les ensembles $\mathfrak{E}_+$ et $\mathfrak{E}_-$ du n° 1.1 respectivement sur $\mathfrak{E}_a$ et $\mathfrak{E}_{-a}$; en particulier $(-1)_a$ est l'élément non neutre du centre de G_a;

on a les relations

$$r_{-a} = r_a, \qquad G_{-a} = G_a, \qquad T_{-a} = T_a, \qquad N_{-a} = N_a, \qquad M_{-a} = M_a,$$

$$T_a = \{k_a \mid k \in K^*\},$$

(1) $$k_{-a} = k_a^{-1},$$

(2) $$m^2 = (-1)_a \qquad \text{pour tout } m \in M_a;$$

étant données deux racines $a, b \in \Sigma$, le plus petit entier positif f tel que $b - f.a$ n'est pas une racine est noté $f(a, b)$;

si $g \in G$ et $\mathfrak{g} \in \mathfrak{G}$, nous posons $g(\mathfrak{g}) = (\mathrm{Ad}\, g)(\mathfrak{g})$; enfin la notation

(3) $$x(y) = x . y . x^{-1}$$

se rapportant à deux éléments x, y d'un groupe quelconque, sera utilisée dans tout l'article.

L'isomorphisme $G_a \cong SL_2$, qui jouera un rôle décisif dans ce paragraphe, est un cas particulier du fait bien connu que, si $\Sigma' \subset \Sigma$ est fermé dans Σ pour les combinaisons linéaires à coefficients rationnels, le sous-groupe connexe de G « engendré » par les $\mathfrak{E}_a (a \in \Sigma')$ est simplement connexe. (Cf. à ce sujet le § 5.)

2.2. Les $\mathfrak{e}_{a,m}$.

La « trijection canonique » de la proposition 1 fait correspondre à tout élément $m \in M_a$ un élément de $\mathfrak{E}_a^*$ et un élément de $\mathfrak{E}_{-a}^*$; ceux-ci seront notés $\mathfrak{e}_{a,m}$ et $\mathfrak{e}_{-a,m}$. Il résulte immédiatement du caractère intrinsèque de la trijection en question que pour tout $n \in N$,

(4) $$n(\mathfrak{e}_{a,m}) = \mathfrak{e}_{(\pi(n))(a),\, n(m)};$$

en particulier,

$$m(\mathfrak{e}_{a,m}) = \mathfrak{e}_{-a,m}$$

ce qui résulte d'ailleurs aussi de 1.1 (7). En vertu de la dernière assertion de la proposition 1, on a, pour tout $k \in K^*$,

(5) $$k . \mathfrak{e}_{a,m} = \mathfrak{e}_{a,k_a.m};$$

en particulier, vu (2),

(6) $$-\mathfrak{e}_{a,m} = \mathfrak{e}_{a,m^{-1}}.$$

2.3. Relations de commutation dans $\mathfrak{G}$: position du problème. Les fonctions δ et $\varkappa_{a,b}$.

Les relations suivantes, où $a, b \in \Sigma$, $m \in M_a$, $n \in N_b$ et $\mathfrak{t} \in \mathfrak{T}$, sont des conséquences immédiates des définitions et de 1.1 (6) :

(7) $$[\mathfrak{T}, \mathfrak{T}] = \{0\},$$

(8) $$[\mathfrak{t}, \mathfrak{e}_{a,m}] = a(\mathfrak{t}) . \mathfrak{e}_{a,m},$$

(9) $$[\mathfrak{e}_{a,m}, \mathfrak{e}_{-a,m}] = -a^*,$$

(10) $$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = 0 \quad \text{si} \quad a+b \notin \Sigma \cup \{0\}.$$

Pour compléter l'énoncé des relations de commutation dans $\mathfrak{G}$, il reste à déterminer le commutateur $[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}]$ lorsque $a+b$ est une racine, soit $-c$ (la raison du choix de cette notation apparaîtra plus loin). Nous pouvons exprimer ce commutateur de deux façons, soit comme un multiple d'un élément $\mathfrak{e}_{-c,p} \in \mathfrak{E}^*_{-c}$ quelconque, soit directement sous la forme $\mathfrak{e}_{-c,p}$ pour un $p \in M_c$ particulier, ce qui se traduit par les formules suivantes, où p désigne un élément quelconque de M_c :

$$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \delta'(a, b, c;\ m, n, p) . \mathfrak{e}_{-c,p}$$
$$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \mathfrak{e}_{-c, \varkappa'_{a,b}(m,n)}.$$

La première de ces relations définit une fonction $\delta' : \Omega \to K^*$ sur l'ensemble $\Omega \subset \Sigma \times \Sigma \times \Sigma \times N \times N \times N$ des sextuples $(a, b, c;\ m, n, p)$ tels que $a+b+c=0$, $m \in M_a$, $n \in M_b$, $p \in M_c$, et la seconde, une fonction $\varkappa'_{a,b} : M_a \times M_b \to M_{a+b}$ pour chaque paire de racines a, b telles que $a+b \in \Sigma$. En fait, au lieu des fonctions δ' et $\varkappa'_{a,b}$, nous nous intéresserons plutôt aux fonctions δ et $\varkappa_{a,b}$ définies par

$$\delta'(a, b, c;\ m, n, p) = f(a, b) . \delta(a, b, c;\ m, n, p),$$
$$\varkappa'_{a,b} = f(a, b) . \varkappa_{a,b}.$$

L'introduction de ce facteur $f(a, b)$ s'expliquera *a posteriori* par la forme des identités qui seront établies aux n^{os} 2.6 et 2.7; elle est d'ailleurs suggérée par la propriété caractéristique des bases de Chevalley ($|N_{a,b}| = f(a, b)$) rappelée dans l'introduction (cf. aussi le n^o 2.9).

Pour faciliter les références, réécrivons les dernières relations de structure de $\mathfrak{G}$ dans les nouvelles notations : si $a, b, c = -a-b \in \Sigma$, on a, pour tous $m \in M_a$, $n \in M_b$, $p \in M_c$,

(11) $$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \delta(a, b, c;\ m, n, p) . f(a, b) . \mathfrak{e}_{-c,p} = f(a, b) . \mathfrak{e}_{-c, \varkappa_{a,b}(m,n)}.$$

On peut à présent concevoir comme suit le *problème de la détermination des constantes de structures de* $\mathfrak{G}$: il s'agit tout d'abord de *donner une description « directe » (indépendante de la théorie des groupes algébriques) du système* $\{N, M_a\ (a \in \Sigma)\}$ *formé du groupe* N *et des parties* M_a *de* N, et ensuite *déterminer la fonction* δ *ou, ce qui revient au même, les fonctions* $\varkappa_{a,b}$. Ces questions font l'objet des n^{os} 2.4, 2.6 et 2.7.

2.4. Une description du système $\{N, M_a(a \in \Sigma)\}$.

Notons $\widetilde{X}$ le groupe des poids de $\mathfrak{G}$, c'est-à-dire l'ensemble des points $x \in \mathfrak{X}'$ tels que $x(a^*) \in \mathbf{Z}$ pour tout $a \in \Sigma$, Σ^0 l'ensemble des racines simples pour un ordre donné dans $\widetilde{X}$, et l_{ab} (pour $a, b \in \Sigma^0$) l'ordre du produit $r_a r_b$ dans le groupe de Weyl W.

Le groupe des poids $\widetilde{X}$ est aussi, à un isomorphisme canonique près, le groupe des caractères de T, de sorte que T peut être canoniquement identifié au groupe $\mathrm{Hom}(\widetilde{X}, K^*)$; moyennant cette identification, k_a (pour $k \in K^*$) est l'homomorphisme $\widetilde{X} \to K^*$ donné par

(12) $$x \mapsto k^{x(a^*)},$$

de sorte que T_a est l'ensemble des homomorphismes (12) avec $k \in K^*$, et l'action « naturelle » de W sur T (par l'intermédiaire des automorphismes intérieurs de N) est contragrédiente de son action sur $\widetilde{X}$ (comme « groupe engendré par les réflexions sur r_a ») (cf. [4], [7]). Compte tenu de ces diverses propriétés, de la relation rappelée plus haut entre le groupe des poids $\widetilde{X}$ et le système de racines Σ, et du fait que toute racine est transformée d'une racine simple par un élément de W, la proposition suivante donne une construction du système $\{N, M_a\ (a \in \Sigma)\}$ à partir de Σ.

Proposition 3. — Pour tout $a \in \Sigma^0$, *choisissons dans* M_a *un élément quelconque* q_a. *Alors les relations suivantes sont vérifiées quels que soient* $a, b \in \Sigma^0$ *et* $t \in T$:

(13) $$q_a^2 = (-1)_a$$

(14) $$\underbrace{q_a q_b q_a \ldots}_{l_{ab}\ \textit{facteurs}} = \underbrace{q_b q_a q_b \ldots}_{l_{ab}\ \textit{facteurs}},$$

(15) $$q_a t q_a^{-1} = r_a(t).$$

Le groupe N *est engendré par* $T \cup \{q_a | a \in \Sigma^0\}$ *et est « défini par les relations* (13), (14), (15), *ajoutées au fait que* T *est un sous-groupe de* N », *c'est-à-dire que toute relation entre éléments de* N *est conséquence de* (13), (14), (15) *et de relations entre éléments de* T. *L'homomorphisme* $\pi : N \to W$ *est défini par*

(16) $$\pi(q_a) = r_a$$

et $\pi(T) = \{1\}$. *Si* $n \in N$, $w = \pi(n)$ *et* $a \in \Sigma^0$, *on a*

(17) $$M_{w(a)} = n . q_a . T_a . n^{-1};$$

en particulier, $M_a = q_a . T_a$.

Cette proposition est un cas particulier de résultats de [9]; pour la commodité du lecteur, nous la redémontrons.

La relation (13) est un cas particulier de (2). Les relations (pratiquement équivalentes) (15) et (16) sont bien connues (cf. [3], [4]).

Établissons (15). Pour cela, nous aurons à utiliser le fait que, pour toute racine $c \in \Sigma$ et tout $n \in N$

(18) $$M_{(\pi(n))(c)} = n . M_c . n^{-1},$$

ce qui résulte immédiatement des définitions. Notons respectivement q et q' les deux membres de (15), et soit b' la racine égale à b ou à a selon que l_{ab} est pair ou impair. On a

$$q' = q_b \cdot q \cdot q_{b'}^{-1}. \tag{19}$$

D'autre part, il résulte de la définition de l_{ab} et de (16) que $\pi(q) = \pi(q')$, de sorte que, vu (19), $(\pi(q))(r_{b'}) = r_b$, ce qui signifie que $(\pi(q))(b') = \pm b$. On a donc, compte tenu de (18),

$$q' . q^{-1} = q_b . q . q_{b'}^{-1} . q^{-1} \in q_b . q . \mathrm{M}_{b'} . q^{-1} = q_b . \mathrm{M}_{(\pi(q))(b')} = q_b . \mathrm{M}_b = \mathrm{T}_b.$$

En permutant a et b, on montre de même que $q . q'^{-1} \in \mathrm{T}_a$, d'où il résulte finalement que $q' . q^{-1} \in \mathrm{T}_a \cap \mathrm{T}_b$. Or cette intersection est réduite à l'élément neutre lorsque $a \neq b$; en effet, si nous identifions comme plus haut T à $\mathrm{Hom}(\widetilde{\mathrm{X}}, \mathrm{K}^*)$, un élément de $\mathrm{T}_a \cap \mathrm{T}_b$ est un homomorphisme de la forme

$$x \mapsto k^{x(a^*)} = k'^{x(b^*)} \qquad (k, k' \in \mathrm{K}^*),$$

et en prenant pour x un élément tel que $x(a^*) = 1$ et $x(b^*) = 0$ (par exemple le poids fondamental dominant associé à a), on déduit de la dernière égalité que $k = 1$. Ainsi, $q' . q^{-1} = 1$, ce qui établit (15).

Soit N' le « groupe engendré par $\mathrm{T} \cup \{q_a | a \in \Sigma^0\}$ et défini par (13), (14), (15) et par les relations définissant le groupe T » (cet abus de langage, qui implique l'identification de $\mathrm{T} \cup \{q_a\}$ avec une partie de N', est légitimé par le fait que, les relations en question étant vérifiées dans N, l'application canonique $\mathrm{T} \cup \{q_a | a \in \Sigma^0\} \to \mathrm{N}'$ est effectivement injective). De (15), il résulte que T est un sous-groupe distingué de N'. Soit r'_a $(a \in \Sigma^0)$ l'image canonique de q_a dans N'/T. De (13) et (14), il résulte que, pour tous $a, b \in \Sigma^0$,

$$r'^2_a = (r'_a . r'_b)^{l_{ab}} = 1, \tag{20}$$

c'est-à-dire que les r'_a vérifient les relations de définition bien connues du groupe de Weyl ([4], [7]). Mais alors, l'homomorphisme $\mathrm{N}' \to \mathrm{N}$ qui prolonge l'application identique de $\mathrm{T} \cup \{q_a | a \in \Sigma^0\}$ induit un isomorphisme $\mathrm{N}'/\mathrm{T} \to \mathrm{N}/\mathrm{T} = \mathrm{W}$, et est donc lui-même un isomorphisme.

Les autres assertions de l'énoncé sont des conséquences immédiates des définitions.

Remarque. — La proposition précédente donne une définition de N par générateurs et relations, c'est-à-dire caractérise N comme un quotient du groupe libre engendré par $\mathrm{T} \cup \{q_a | a \in \Sigma^0\}$. De la définition initiale de T, de N et des M_a comme parties de G, il résulte que l'application canonique $\mathrm{T} \cup \{q_a | a \in \Sigma^0\} \to \mathrm{N}$ est injective (ce qui a d'ailleurs été utilisé dans la démonstration). Pour la même raison, nous savons *a priori* que les relations (17) sont cohérentes, c'est-à-dire que si $n, n' \in \mathrm{N}$ et $a, a' \in \Sigma^0$ sont tels que $(\pi(n))(a) = (\pi(n'))(a')$, on a aussi $n . q_a . \mathrm{M}_a . n^{-1} = n' . q_{a'} . \mathrm{M}_{a'} . n'^{-1}$. Cependant, il peut être intéressant de donner de ces propriétés une démonstration directe, indépendante des théorèmes d'existence des groupes semi-simples. Une telle démonstration peut être trouvée dans [9]; les principaux éléments en sont d'ailleurs repris, dans un contexte un peu différent au nº 3.6 ci-dessous.

2.5. Trois propriétés des triples de racines de somme nulle.

Lemme 1. — *Soient* $a, b, c \in \Sigma$ *trois racines telles que* $a+b+c=0$. *Alors*

$$f(a, b)=f(b, a); \tag{21}$$

$$f(b, c).a^* + f(c, a).b^* + f(a, b).c^* = 0; \tag{22}$$

(23) *les quatre propriétés suivantes sont équivalentes :*

(i) $r_a(b)=-c$;

(ii) $b(a^*)=-1$;

(iii) $\lambda(a) \geqslant \lambda(b)$ *et* $\lambda(a) \geqslant \lambda(c)$;

(iv) $f(a, b)=f(a, c)=1$, *ou bien* a, b, c *sont trois racines « courtes » d'un facteur direct de type* G_2 *de* G (*auquel cas* $f(a, b)=f(a, c)=2$).

Il s'agit en fait de propriétés des systèmes de racines de rang 2, et comme telles susceptibles de vérification immédiate « cas par cas ». Le détail de cette vérification sera omis. Pour une démonstration un peu plus « conceptuelle » de (21), (22) et de l'implication (iii) ⇒ (i), nous renvoyons le lecteur aux n^{os} 3.3 et 3.4. Notons encore ici que l'équivalence de (i) et (ii) résulte de l'identité

$$r_a(\mathfrak{t}')=\mathfrak{t}'-\mathfrak{t}'(a^*).a \quad (\mathfrak{t}' \in \mathfrak{T}'),$$

et que l'implication (i) ⇒ (iii) est conséquence immédiate du fait bien connu que si les racines de G n'ont pas toutes la même longueur, la somme de deux racines « longues » ne peut être une racine « courte ».

2.6. Détermination de la fonction δ.

Dans ce numéro, a, b, c désignent toujours trois racines telles que $a+b+c=0$, et $m \in M_a$, $n \in M_b$, $p \in M_c$.

Le premier membre de (11) étant indépendant de p, il doit en être de même du second, qui ne change donc pas lorsqu'on y remplace p par $k_c.p$ $(k \in K^*)$, ce qui peut s'écrire, vu (1) et (5),

$$\delta(a, b, c;\ m, n, k_c.p)=k.\delta(a, b, c;\ m, n, p). \tag{24}$$

En vertu de (9) et (11), la relation de Jacobi pour les trois éléments $\mathfrak{e}_{a,m}$, $\mathfrak{e}_{b,n}$, $\mathfrak{e}_{c,p}$ peut s'écrire

$$\Sigma\,\delta(a, b, c;\ m, n, p).f(a, b).c^*=0, \tag{25}$$

où la sommation est étendue à une permutation circulaire simultanée de a, b, c, et de m, n, p. Des relations (22) et (25), et de l'indépendance linéaire de a^* et b^* (conséquence de l'indépendance linéaire de a et b), il résulte que

$$\delta(a, b, c;\ m, n, p)=\delta(b, c, a;\ n, p, m). \tag{26}$$

Soit $\mathfrak{V}$ le sous-espace linéaire de $\mathfrak{G}$ engendré par les $\mathfrak{E}_d$ avec $d=a+zb\in\Sigma$ ($z\in\mathbf{Z}$). En appliquant 1.3 (14) à la représentation de $\mathfrak{G}_a$ dans $\mathfrak{V}$ obtenue par restriction à partir de la représentation adjointe de $\mathfrak{G}$, on voit, compte tenu de (11) et du lemme 1, que

$$\text{si } \lambda(a)\geqslant\lambda(b), \lambda(c) \text{ on a } \delta(a, b, c;\ m, n, m(n))=(-1)^{f(a,b)+1}; \tag{27}$$

autrement dit, $\delta(a, b, c; m, n, m(n))=1$ sauf si a, b, c sont trois racines courtes d'un facteur direct de type G_2 de $\mathfrak{G}$, auquel cas $\delta(a, b, c;\ m, n, m(n))=-1$.

Proposition 4. — La fonction δ est caractérisée par les relations (24), (26), (27).

En effet, soit à déterminer la valeur de δ en un point $(a, b, c; m, n, p)$ donné. Quitte à permuter cycliquement a, b, c, ce qui est loisible grâce à (26), nous pouvons, sans nuire à la généralité, supposer que $\lambda(a)\geqslant\lambda(b), \lambda(c)$. Mais alors, $\delta(a, b, c; m, n, p)$ est donné par (24) et (27).

Corollaire 2. — On a

$$\delta(-a, -b, -c;\ m, n, p)=\delta(a, b, c;\ m, n, p)^{-1}. \tag{28}$$

Il suffit de remarquer que, compte tenu de (1), les relations (24), (26), (27), sont invariantes par la substitution $(a, b, c, \delta)\mapsto(-a, -b, -c, \delta^{-1})$.

Remarques. — a) La caractérisation de la fonction δ fournie par la proposition 4 fait intervenir non seulement le groupe N et les ensembles M_a, mais encore les homomorphismes $k\mapsto k_a$ de K^* dans T. Ceci ne présente pas d'inconvénient du point de vue des problèmes posés à la fin du nº 2.3, grâce au fait que — d'ailleurs pour cette raison — nous avons inclu une « description directe » de ces homomorphismes aux considérations préliminaires du nº 2.4. Notons que les k_a ne joueront par contre aucun rôle dans la caractérisation des fonctions $\varkappa_{a,b}$ (proposition 5).

b) Lorsque $k=-1$, la relation (24) devient, vu (2),

$$\delta(a, b, c;\ m, n, p^{-1})=-\delta(a, b, c;\ m, n, p). \tag{29}$$

c) De (11) et de l'anticommutativité du commutateur, il résulte que

$$\delta(a, b, c;\ m, n, p)=-\delta(b, a, c;\ n, m, p). \tag{30}$$

L'ensemble des relations (26) et (30) signifie que *la fonction δ est antisymétrique en les paires (a, m), (b, n) et (c, p).*

d) La proposition 4 établit l'unicité de la fonction $\delta:\Omega\to K^*$ vérifiant (24), (26), (27). Le problème d'existence ne se pose pas ici, vu la définition de δ donnée au nº 2.3. Cependant, dans l'esprit de la remarque terminant le nº 2.4, on peut se proposer de démontrer l'existence de la fonction δ indépendamment de l'existence de $\mathfrak{G}$, en partant de la caractérisation du système $\{N, M_a\}$ donnée en 2.4. Il est effectivement facile de donner une telle démonstration; nous ne le ferons pas ici, mais nous aurons au nº 3.8 à résoudre un problème analogue pour une autre fonction ε, essentiellement la restriction de δ à une certaine partie de Ω, et la démonstration qui sera donnée là se transpose aisément au cas présent.

2.7. Détermination de la fonction $\varkappa_{a,b}$.

Il résulte de (11) que $\varkappa_{a,b}(m, n)$ est l'unique élément x de M_c tel que $\delta(a, b, c; m, n, x) = 1$. Cela étant, la proposition suivante est une conséquence immédiate de (26), (27), (29) et (30).

Proposition 5. — Soient $a, b, c = -a-b \in \Sigma$. *Posons* $\varkappa_{a,b}(m, n) = p$, *sauf si* a, b, c *sont trois racines « courtes » d'un facteur direct de type* G_2 *de* $\mathfrak{G}$, *auquel cas nous posons* $\varkappa_{a,b}(m, n) = p^{-1}$. *Alors*

(31) $$\text{si } \lambda(a) \geqslant \lambda(b), \lambda(c), \text{ on a } p = m(n);$$

(32) $$\text{si } \lambda(b) \geqslant \lambda(c), \lambda(a), \text{ on a } p = n(m)^{-1};$$

(33) *si* $\lambda(c) \geqslant \lambda(a), \lambda(b)$, p *est le seul élément de* M_c *tel que* $p(m) = n$ *et aussi le seul élément de* M_c *tel que* $p(n) = m^{-1}$.

Corollaire 3. — On a les relations

(34) $$\varkappa_{a,b} = \varkappa_{-a,-b},$$

(35) $$\varkappa_{a,b}(m, n) = \varkappa_{a,b}(n, m)^{-1}.$$

La relation (35) est aussi une conséquence immédiate de (1), (21) et de l'anticommutativité du commutateur.

Remarques. — a) Lorsque les racines de $\mathfrak{G}$ ont toutes la même longueur, (31) est applicable quelles que soient les racines a, b telles que $a+b \in \Sigma$, et les relations de commutation (11) prennent la forme particulièrement simple

(36) $$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \mathfrak{e}_{a+b, m(n)}.$$

b) L'existence de l'identité (34) fait qu'il n'est généralement pas gênant d'omettre les indices a, b du symbole $\varkappa_{a,b}$; en effet, lorsqu'on sait (par exemple par le contexte) que les arguments m, n appartiennent respectivement à M_a et M_b, et que $\varkappa(m, n) \in M_c$, les indices affectant $\varkappa$ ne peuvent être que a, b ou $-a$, $-b$.

2.8. Le groupe $N_{\mathbf{Z}}$ et les ensembles $M_{a,\mathbf{Z}}$.

Pour toute racine simple $d \in \Sigma^0$, choisissons dans M_d un point q_d. Nous noterons $N_{\mathbf{Z}}$ le groupe engendré par les q_d $(d \in \Sigma^0)$ et, pour toute racine $a \in \Sigma$, nous poserons $M_{a,\mathbf{Z}} = M_a \cap N_{\mathbf{Z}}$. Le choix de ces notations s'explique par le fait que $N_{\mathbf{Z}}$ est effectivement le groupe des points de N rationnels sur **Z** pour une « **Z**-structure déployée » convenable (d'ailleurs unique) de G (en termes plus précis : il existe un **Z**-schéma en groupes déployé ${}_{\mathbf{Z}}G$, un tore ${}_{\mathbf{Z}}T$ faisant partie d'une donnée de déploiement de ${}_{\mathbf{Z}}G$ et, désignant par ${}_{K}G$ et ${}_{K}T$ les groupes algébriques déduits de ${}_{\mathbf{Z}}G$ et ${}_{\mathbf{Z}}T$ par changement de base de **Z** à K, un isomorphisme $\varphi : {}_{K}G \to G$ tel que $\varphi({}_{K}T) = T$ et tel que $N_{\mathbf{Z}}$ soit l' « image par φ » du groupe des points sur **Z** du normalisateur de ${}_{\mathbf{Z}}T$) ([5], [9]). Nous ne ferons cependant pas usage de cette interprétation schématique de $N_{\mathbf{Z}}$ et nous établirons, indépendamment d'elle, la

Proposition 6. — *Le groupe* $T_{\mathbf{Z}}=T\cap N_{\mathbf{Z}}$ *est un 2-groupe abélien élémentaire d'ordre* 2^l, *où* l *désigne le rang de* G; *il se compose de l'élément neutre et de tous les éléments d'ordre* 2 *de* T. *Le groupe* $N_{\mathbf{Z}}$ *est une extension du groupe de Weyl* W *par* $T_{\mathbf{Z}}$. *Pour toute racine* $a\in\Sigma$, *l'ensemble* $M_{a,\mathbf{Z}}$ *se compose de deux éléments, inverses l'un de l'autre.*

Soit $T'_{\mathbf{Z}}$ le groupe engendré par les $(-1)_d$ $(d\in\Sigma^0)$. Il est contenu dans $N_{\mathbf{Z}}$ en vertu de (13). Il résulte de la description de T et des k_a donnée au début du n° 2.4, et du fait que les d^* (avec $d\in\Sigma^0$) forment une base du dual du réseau des poids, que $T'_{\mathbf{Z}}$ est abélien élémentaire d'ordre 2^l et se compose de l'élément neutre et de tous les éléments d'ordre 2 de T. En particulier, $T'_{\mathbf{Z}}$ est distingué dans $N_{\mathbf{Z}}$. De (13) et (14), il résulte que les images canoniques des q_d dans le quotient $N_{\mathbf{Z}}/T'_{\mathbf{Z}}$ satisfont aux relations (20), de sorte que l'homomorphisme $N_{\mathbf{Z}}/T'_{\mathbf{Z}}\to N/T$ induit par l'injection canonique $N_{\mathbf{Z}}\to N$ est un isomorphisme. Ceci établit les deux premières assertions de l'énoncé.

Toujours d'après le début du n° 2.4, $(-1)_a$ est le seul élément d'ordre 2 de T_a de sorte que $T_{a,\mathbf{Z}}=T_a\cap T_{\mathbf{Z}}=\{1,(-1)_a\}$. Il s'ensuit, vu (17), que $M_{a,\mathbf{Z}}$ est vide ou se compose de deux éléments, inverses l'un de l'autre. Mais il existe un élément $w\in W$ et une racine simple $d\in\Sigma^0$ tels que $w(d)=a$, et si $n\in N_{\mathbf{Z}}$ appartient à l'image réciproque de w par l'épimorphisme canonique $N_{\mathbf{Z}}\to W$, on a $n(q_d)\in M_{a,\mathbf{Z}}$, de sorte que $M_{a,\mathbf{Z}}$ ne peut être vide, ce qui achève la démonstration.

Remarque. — Nous verrons au numéro suivant que le système formé par le groupe $N_{\mathbf{Z}}$ et les ensembles $M_{a,\mathbf{Z}}$ est un instrument essentiel pour l'étude des « signes des constantes de structures » de $\mathfrak{G}$. Il est donc utile d'en donner aussi une description « directe », indépendante de $\mathfrak{G}$. En principe, nous disposons déjà d'une telle description, puisque $N_{\mathbf{Z}}$ a été défini de façon purement « abstraite » à partir de N et des M_a, mais on peut aussi éviter de passer par l'intermédiaire de N en remarquant que *tout ce qui a été dit au n° 2.4 reste valable si on y remplace* K^*, T, N, T_a, M_a *respectivement par le groupe* $\mathbf{Z}^*=\{+1,-1\}$, $T_{\mathbf{Z}}$, $N_{\mathbf{Z}}$, $M_{a,\mathbf{Z}}$, $T_{a,\mathbf{Z}}$ (on notera toutefois cette différence qu'ici, l'ensemble $\{q_a\}$ engendre $N_{\mathbf{Z}}$ à lui seul). (Pour un développement de cette remarque, cf. [9].)

2.9. Double base de Chevalley. Signes des constantes de structure.

Conservons les notations de 2.8 et désignons par Ψ l'intersection de $N_{\mathbf{Z}}\times N_{\mathbf{Z}}\times N_{\mathbf{Z}}$ avec la projection dans $N\times N\times N$ de l'ensemble Ω du n° 2.3, c'est-à-dire l'ensemble des triples (m,n,p) tels qu'il existe trois racines a,b,c de somme nulle pour lesquelles $m\in M_{a,\mathbf{Z}}$, $n\in M_{b,\mathbf{Z}}$, $p\in M_{c,\mathbf{Z}}$.

En vertu de (6), l'ensemble des $\mathfrak{e}_{a,m}$, avec $a\in\Sigma$, $m\in M_{a,\mathbf{Z}}$, est une « double base », c'est-à-dire est la réunion d'une base et de son opposée, dans l'espace somme des $\mathfrak{E}_a$.

Soient a,b,c trois racines telles que $a+b+c=0$ et soient $m\in M_{a,\mathbf{Z}}$, $n\in M_{b,\mathbf{Z}}$, $p\in M_{c,\mathbf{Z}}$. Alors $\delta(a,b,c;m,n,p)=\pm 1$: cela résulte de (27), (29) et de la proposition 6 lorsque $\lambda(a)\geqslant\lambda(b),\lambda(c)$, et ensuite de (26) dans le cas général. D'après (28), la valeur de $\delta(a,b,c;m,n,p)$ est alors entièrement déterminée par les arguments m,n,p, ce qui nous permet de définir une fonction $\varepsilon:\Psi\to\{+1,-1\}$ en posant

$$\delta(a,b,c;m,n,p)=\varepsilon(m,n,p). \tag{37}$$

La relation de commutation (11) peut s'écrire à présent

$$(38) \qquad [\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \varepsilon(m, n, p) . f(a, b) . \mathfrak{e}_{-c,p}$$

(toujours sous l'hypothèse que $m, n, p \in \mathrm{M}_{\mathbf{Z}}$), de sorte que *la fonction* ε *décrit les signes des « constantes de structure » de* G. D'après la proposition 4, *cette fonction satisfait aux trois relations suivantes, qui la caractérisent complètement :*

$$(39) \qquad \varepsilon(m, n, p^{-1}) = -\varepsilon(m, n, p);$$

$$(40) \qquad \varepsilon(m, n, p) = \varepsilon(p, m, n);$$

(41) *si* $\lambda(a) \geqslant \lambda(b), \lambda(c)$, *on a* $\varepsilon(m, n, m(n)) = (-1)^{f(a,b)+1}$;

autrement dit, $\varepsilon(m, n, m(n)) = 1$ *sauf si a, b, c sont trois racines « courtes » d'un facteur direct de type* G_2 *de* $\mathfrak{G}$, *auquel cas* $\varepsilon(m, n, m(n)) = -1$.

Pour toute paire de racines opposées $(a, -a)$, choisissons l'un des deux éléments de $\mathrm{M}_{a,\mathbf{Z}} = \mathrm{M}_{-a,\mathbf{Z}}$, notons le $q_a = q_{-a}$, et pour toute racine a posons $\mathfrak{e}_a = \mathfrak{e}_{a,q_a}$. Alors la relation de commutation (11) devient

$$(42) \qquad [\mathfrak{e}_a, \mathfrak{e}_b] = \varepsilon_{a,b} . f(a, b) . \mathfrak{e}_{a+b}$$

où le « signe » $\varepsilon_{a,b}$ est donné par

$$\varepsilon_{a,b} = \varepsilon(q_a, q_b, q_{a+b}).$$

En particulier, on voit que le coefficient $\mathrm{N}_{a,b}$ de $\mathfrak{e}_{a+b}$ dans (42) satisfait à la « relation de Weyl » $\mathrm{N}_{a,b} = \mathrm{N}_{-a,-b}$ et à la « règle de Chevalley » $|\mathrm{N}_{a,b}| = f(a, b)$, rappelées dans l'introduction, de sorte que les $\mathfrak{e}_a$ $(a \in \Sigma)$ forment avec une base de $\mathfrak{T}$ une *base de Chevalley* de $\mathfrak{G}$.

DEUXIÈME PARTIE

THÉORÈME D'EXISTENCE

Rappelons que cette deuxième partie, dont le but est la démonstration du théorème d'existence énoncé au nº 4.1, est entièrement indépendante de la première partie.

3. SYSTÈMES DE RACINES

3.1. Définitions.

Soient $\mathfrak{X}$ un espace vectoriel sur K et $\mathfrak{X}'$ son dual. Une partie finie Σ de $\mathfrak{X}'$ est un *système de racines* (dans $\mathfrak{X}'$) si

(1) $$\Sigma \text{ engendre } \mathfrak{X}'\text{[1]},$$

(2) $$\text{les relations } a, ka \in \Sigma \text{ et } k \in \mathbf{Z} \text{ impliquent } k = \pm 1,$$

et s'il existe une application $^* : \Sigma \to \mathfrak{X}$ satisfaisant aux trois conditions suivantes, où on pose $^*(a) = a^*$:

(3) $$a(a^*) = 2 \quad \text{pour tout} \quad a \in \Sigma;$$

(4) $$b(a^*) \in \mathbf{Z} \quad \text{pour tous} \quad a, b \in \Sigma;$$

(5) $$\text{si} \quad a, b \in \Sigma, \quad \text{alors} \quad b - b(a^*).a \in \Sigma.$$

Les éléments de Σ sont les *racines*. La dimension de $\mathfrak{X}$ est le *rang* du système Σ. L'application * est univoquement déterminée par les propriétés (3) à (5); en effet, il résulte immédiatement de celles-ci et de (1) que a^* est l'unique élément de $\mathfrak{X}$ tel que $a(a^*) = 2$ et tel que, pour tout $b \in \Sigma$, la somme $\sum_{b'} b'(a^*)$ étendue à toutes les racines b' de la forme $b - ka$ $(k \in \mathbf{Z})$ soit nulle.

Nous noterons $r_a : \mathfrak{X}' \to \mathfrak{X}'$ $(a \in \Sigma)$ la *réflexion par rapport à a*, définie par

(6) $$r_a(x') = x' - x'(a^*).a \qquad (x' \in \mathfrak{X}')$$

et aussi sa contragrédiente $\mathfrak{X} \to \mathfrak{X}$; celle-ci laissant fixe chaque point du noyau de a et permutant a^* et $-a^*$ (vu (3) et (6)), elle est donnée par

(7) $$r_a(x) = x - a(x).a^* \qquad (x \in \mathfrak{X}).$$

Le groupe W engendré par les $r_a (a \in \Sigma)$ est le *groupe de Weyl*, que nous ferons aussi opérer tantôt sur $\mathfrak{X}'$, tantôt sur $\mathfrak{X}$. Vu (4), W laisse invariant Σ, et est donc un groupe fini, en vertu de (1). Il résulte alors de l'unicité de l'application * que

(8) $$w(a)^* = w(a^*) \qquad \text{pour tous} \quad a \in \Sigma, w \in \mathrm{W};$$

---

[1] Nous nous écartons en ceci de la terminologie adoptée par exemple dans [1] et [9].

en particulier, pour $w = r_a$,

(9) $$(-a)^* = -a^*.$$

Dans la suite de cette deuxième partie, nous nous donnons une fois pour toutes les espaces $\mathfrak{T}$ et $\mathfrak{T}'$ et un système de racines Σ. Sauf mention explicite du contraire, les lettres a, b, c, d désigneront toujours des éléments de Σ.

3.2. Rappels.

Dans ce numéro nous rassemblons quelques propriétés bien connues des systèmes de racines. Nous donnons cependant des indications de démonstration qui doivent normalement permettre au lecteur non informé de reconstruire des démonstrations complètes (celles-ci peuvent, par ailleurs, être trouvées dans [2], [3], [6]). Notre but est de souligner ainsi le caractère tout à fait élémentaire des moyens employés dans la démonstration d'existence du § 4; on notera en particulier que la classification des systèmes de racines de rang >2 n'intervient pas ici.

3.2.1. La fonction λ.

Vu (7), tout point de $\mathfrak{T}$ fixe par W appartient au noyau de toute racine, et est donc nul d'après (1). Pour tout $x' \in \mathfrak{T}'$ et tout $x \in \mathfrak{T}$, on a donc $\sum_{w \in W} (w(x'))(x) = x'(\sum_{w \in W} w(x)) = 0$, d'où $\sum_{w \in W} w(x') = 0$. Si x' est invariant par W, on en déduit que x' est nul; autrement dit

(10) si $x' \in \mathfrak{T}'$ et si $x'(a^*) = 0$ pour toute racine a, on a $x' = 0$.

Nous noterons $\lambda : \mathfrak{T}' \to K$ la forme quadratique somme des carrés des formes linéaires $x' \mapsto x'(a^*)$ $(a \in \Sigma)$, et $\beta : \mathfrak{T}' \times \mathfrak{T}' \to K$ la forme bilinéaire symétrique associée. Les deux assertions suivantes résultent de (4), (10) et de l'invariance de λ par W :

(11) si X est le groupe engendré par Σ, on a $\lambda(X - \{0\}) \in \mathbf{N}^*$ (ensemble des nombres entiers strictement positifs);

(12) $$\lambda(a) . b(a^*) = \lambda(b) . a(b^*) = 2\beta(a, b).$$

En particulier, les relations $a(b^*) = 0$ et $b(a^*) = 0$ sont équivalentes; lorsqu'elles sont vérifiées, a et b sont dites *orthogonales*. De (11) et (12) on déduit que

(13) la forme 2β est non dégénérée, et est donc associée à une transformation linéaire bijective $\mathfrak{T}' \to \mathfrak{T}$, laquelle applique toute racine a sur $\lambda(a) . a^*$,

et que

(14) $$b(a^*) . a(b^*) < 4 \quad \text{sauf si} \quad a = \pm b,$$

donc, aussi vu (4), que

(15) $$\text{si} \quad a \neq \pm b,\ b(a^*) \neq 0 \quad \text{et} \quad \lambda(a) \geqslant \lambda(b),$$
$$\text{on a} \quad |b(a^*)| = 1 \quad \text{et} \quad |a(b^*)| = \lambda(a)/\lambda(b) = 1,\ 2 \text{ ou } 3.$$

Nous aurons encore à utiliser la propriété suivante :

(16) soient a_i $(i=0, \ldots, n)$ des racines telles que $a_i(a^*_{i-1}) \neq 0$ pour tout $i \geqslant 1$; alors, le nombre $\lambda(a_i)$ prend au plus deux valeurs distinctes; si de plus $a_0 \neq a_1$ et $a_{n-1} \neq a_n$, alors on ne peut avoir $1 \neq |a_1(a^*_0)| \neq |a_n(a^*_{n-1})| \neq 1$.

La deuxième assertion est conséquence immédiate de (15) et de la première assertion. Celle-ci est établie par induction sur n. Quitte à remplacer au besoin a_n par $r_{a_{n-1}}(a_n)$, on peut supposer que $a_n(a^*_{n-2}) \neq 0$. Alors, si $n=2$, l'assertion résulte de (15); si $n>2$ elle est conséquence de l'hypothèse d'induction appliquée aux trois suites $(a_0, \ldots, a_{n-1})$, $(a_0, \ldots, a_{n-2}, a_n)$ et (a_{n-2}, a_{n-1}, a_n).

3.2.2. Système de racines simples.

Munissons le groupe X engendré par Σ d'une structure d'ordre compatible avec la loi de groupe. Les racines positives qui ne sont pas combinaisons linéaires à coefficients rationnels positifs d'autres racines positives sont dites *simples* (pour l'ordre en question). L'ensemble des racines simples sera noté Σ^0.

(17) Soit A un ensemble de racines positives non linéairement indépendantes. Alors, il existe $a, b \in \mathrm{A}$ telles que $a \neq b$ et $a(b^*)>0$.

En effet, soit $x=y$ avec $x=\sum_i k_i a_i$, $y=\sum_j l_j b_j$, $a_i, b_j \in \mathrm{A}$, $a_i \neq b_j$, $k_i, l_j \in \mathbf{N}^*$, les indices i, j parcourant des ensembles finis $\mathrm{I} \neq \varnothing$ et J (l'existence d'une telle relation résulte de l'hypothèse faite sur A et de (4), (10)). Puisque les a_i sont positives, on a $x \neq 0$, d'où $\beta(x,y)=\beta(x,x)>0$, et il existe donc $i \in \mathrm{I}$ et $j \in \mathrm{J}$ tels que $\beta(a_i, b_j)>0$.

(18) Soient $a \in \Sigma^0$ et $b>0$ telles que $b(a^*)>0$; alors $b \notin \Sigma^0$ et $b>r_a(b)>0$.

C'est une conséquence immédiate des définitions et de (6). De (17) et (18), on déduit successivement que

(19) Σ^0 est une base de $\mathfrak{X}'$;

(20) toute racine est transformée d'une racine simple par un produit de r_a, avec $a \in \Sigma^0$;

(21) W est engendré par les r_a $(a \in \Sigma^0)$;

(22) tout élément de Σ (resp. Σ^*) est combinaison linéaire à coefficients entiers d'éléments de Σ^0 (resp. Σ^{0*}) (cette dernière assertion résulte de (20), vu (6), (7) et (4)).

(23) Étant données deux racines a, b, il existe dans X un ordre tel que l'ensemble Σ^0 des racines simples contienne a et une racine de la forme $ka+lb$ $(l \neq 0)$;

supposant a et b non proportionnelles, il suffit de prendre l'ordre lexicographique des coordonnées pour une base ordonnée formée de a, de b, et d'une suite quelconque d'éléments de X.

(24) Soit $a_1, a_2, \ldots, a_k$ une suite de racines simples (éventuellement avec répétitions) telle que $\prod_{i=1}^{k} r_{a_i}=1$, et, pour tout i $(1 \leqslant i \leqslant k)$, posons

$$a'_i=\Big(\prod_{j=1}^{i} r_{a_j}\Big)(a_i);$$

alors, pour tout $b \in \Sigma$, les racines b et $-b$ interviennent un même nombre de fois dans la suite $a'_1, a'_2, \ldots, a'_k$.

En effet, posons $b'_0 = b$ et $b'_i = (\prod_{j=i}^{1} r_{a_j})(b)$ pour $1 \leqslant i \leqslant k$; on vérifie immédiatement que $a'_i = b$ si et seulement si $b'_{i-1} > 0 > b'_i$ et que $a'_i = -b$ si et seulement si $b'_{i-1} < 0 < b'_i$, et l'assertion résulte alors du fait que b'_0 et b'_k « ont même signe » (ils sont même égaux).

3.2.3. Systèmes de rang 2.

L'assertion suivante est une conséquence immédiate de la définition du n° 3.1, et de (13), (22), (23).

(25) Soient a, b deux racines et $\mathfrak{S}'$ (resp. $\mathfrak{S}$) le sous-espace vectoriel de $\mathfrak{T}'$ (resp. $\mathfrak{T}$) engendré par a et b (resp. a^* et b^*). Alors, les espaces $\mathfrak{S}$ et $\mathfrak{S}'$ sont mis en dualité par la restriction à $\mathfrak{S} \times \mathfrak{S}'$ du produit scalaire $\mathfrak{T} \times \mathfrak{T}' \to \mathrm{K}$; l'intersection $\Sigma \cap \mathfrak{S}'$ est un système de racines dans $\mathfrak{S}'$, on a $(\Sigma \cap \mathfrak{S}')^* = \Sigma^* \cap \mathfrak{S}$ et la restriction de * à $\Sigma \cap \mathfrak{S}'$ est l'application * du système de racines $\Sigma \cap \mathfrak{S}'$; enfin l'intersection de $\mathfrak{S}'$ (resp. $\mathfrak{S}$) avec le groupe engendré par Σ (resp. Σ^*) est le groupe engendré par $\Sigma \cap \mathfrak{S}'$ (resp. $\Sigma^* \cap \mathfrak{S}$).

La proposition suivante ne fait aucune hypothèse sur le rang de Σ, mais il suffit de l'établir pour le rang 2, en vertu de (25). Pour démontrer (26) et (27), on peut par exemple les vérifier directement après avoir déterminé explicitement tous les systèmes de rang 2, ce qui ne présente aucune difficulté.

(26) Si a, b sont orthogonales, l'un des ensembles de conditions suivants est rempli :

(i) les seules racines combinaisons linéaires de a et b sont $\pm a$ et $\pm b$;

(ii) $\lambda(a) = \lambda(b)$, $a + b \in \Sigma$, $a - b \in \Sigma$;

(iii) $\lambda(a) = \lambda(b)$, $\frac{1}{2}(a+b) \in \Sigma$, $\frac{1}{2}(a-b) \in \Sigma$, $\left(\frac{1}{2}(a \pm b)\right)^* = a^* \pm b^*$;

(iv) $\lambda(a) \neq \lambda(b)$, $a + b \notin \Sigma$, $a - b \notin \Sigma$, et il existe deux racines a', a'' telles que $r_b(a') = a''$ et $r_{a'}(a'') = r_{a''}(a') = a' + a'' = a$.

(27) Soit Σ de rang 2. Alors, si $\lambda(a) = \lambda(b)$, il existe une transformation linéaire de $\mathfrak{T}$ conservant Σ et permutant a et b.

3.3. La fonction f.

Soient a, b deux racines, et h le plus grand nombre réel tel que $b - ha \in \Sigma$; il résulte de (22) et (23) que h est un entier. Nous noterons f la fonction $\Sigma \times \Sigma \to \mathbf{Z}$ définie par $f(a, b) = h + 1$, qu'il sera commode d'étendre à $\mathfrak{T}' \times \mathfrak{T}'$ en posant $f(x, y) = 0$ lorsque $(x, y) \notin \Sigma \times \Sigma$. On a alors, pour tous $a, b \in \Sigma$,

(28) $$f(a, b - a) = f(a, b) - 1.$$

La fonction f est évidemment invariante par W, c'est-à-dire que

(29) $$f(w(a), w(b)) = f(a, b) \quad \text{pour tout } w \in \mathrm{W}.$$

Soit $h' = f(-a, b) - 1$ le plus grand nombre réel tel que $b + h'a \in \Sigma$. Il est clair que les racines $b - ha$ et $b + h'a$ sont permutées par r_a, ce qui peut s'écrire, compte tenu de (3) et (7),

$$b(a^*) = h - h',$$

c'est-à-dire

(30) $$b(a^*) = f(a, b) - f(-a, b).$$

La relation suivante, conséquence immédiate de (28) et (30), sera utilisée plus loin :

(31) $$b(a^*) = f(-a, b) . f(a, b - a) - f(a, b) . f(-a, b + a).$$

Si $a - b$ est une racine, il en est de même de $b - a$, donc

(32) les relations $f(a, b) = 1$ et $f(b, a) = 1$ sont équivalentes.

Montrons que

(33) si $a + b \in \Sigma$ et si $f(a, b) \neq 1$, on a $\lambda(a) = \lambda(b)$.

Vu (32), nous pouvons, sans nuire à la généralité, supposer que $\lambda(b) \geqslant \lambda(a)$. L'un des deux nombres $|(a \pm b)(b^*)| = |a(b^*) \pm 2|$ est $\geqslant 2$; vu (17), il s'ensuit que $\lambda(a + b) > \lambda(b)$ ou $\lambda(a - b) > \lambda(b)$, ce qui implique notre assertion, en vertu de (16). De (32), (33), (25) et (27), il résulte que

(34) si $a + b \in \Sigma$, on a $f(a, b) = f(b, a)$.

Soient $a, b, c \in \Sigma$ telles que $a + b + c = 0$. On a, en vertu de (33) et (34), appliqué aux racines $-a$ et b,

$$\lambda(a) . (f(-a, b) - 1) = \lambda(b) . (f(b, -a) - 1)$$

qui peut encore s'écrire, eu égard à (28) et au fait que $f(-x, -y) = f(x, y)$,

$$\lambda(a) . f(a, c) = \lambda(b) . f(b, c),$$

d'où

(35) $$f(a, c) . \lambda(b)^{-1} - f(b, c) . \lambda(a)^{-1} = 0.$$

Permutant b et c, on trouve de même,

(36) $$f(a, b) . \lambda(c)^{-1} - f(b, c) . \lambda(a)^{-1} = 0.$$

Multiplions respectivement (35) et (36) par b et c et ajoutons membres à membres; il vient

$$f(a, c) . \lambda(b)^{-1} . b + f(a, b) . \lambda(c)^{-1} . c + f(b, c) . \lambda(a)^{-1} . a = 0.$$

Eu égard à (13), nous avons ainsi établi que

(37) si $a + b + c = 0$, on a $f(a, b) . c^* + f(b, c) . a^* + f(c, a) . b^* = 0$.

3.4. Les relations $\lrcorner$ et $\perp\!\!\!\perp$. Trois lemmes.

Nous noterons $\lrcorner$ et $\perp\!\!\!\perp$ les relations entre paires de racines a, b, définies comme suit :

(38) $$a \lrcorner b \Leftrightarrow f(a, b) = 1 \text{ et } b(a^*) = -1;$$

(39) $$a \perp\!\!\!\perp b \Leftrightarrow f(a, b) = 1 \text{ et } b(a^*) = 0.$$

La relation $a \perp\!\!\!\perp b$ signifie donc aussi que a et b sont orthogonales et que $a+b$ n'est pas racine.

Lemme 2. — *Soient a, b, c trois racines telles que $a+b+c=0$. Alors, si $\lambda(a) \geqslant \lambda(b)$ et $\lambda(a) \geqslant \lambda(c)$, on a $r_a(b) = -c$.*

En effet, $$b(a^*) + c(a^*) = -a(a^*) = -2,$$
ce qui implique, vu (15), que
$$b(a^*) = c(a^*) = -1.$$

Lemme 3. — *Soient a, b, c, d quatre racines telles que $a+b+c+d=0$ et telles que $b(a^*) = c(a^*) = -1$. Alors $a \rfloor b$ et $a \rfloor c$. En outre $a \perp\!\!\!\perp d$ sauf peut-être si $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(d)$.*

Des hypothèses et de (3), il résulte que $d(a^*) = 0$.

Supposons que $b-a$ soit une racine. En vertu de (12) et (15), on a $|(b-a)(b^*)| = |2-a(b^*)| \leqslant 3$ et $a(b^*) < 0$; par suite $a(b^*) = -1$ et $2b+a = r_b(a-b) \in \Sigma$. Or $(2b+a)(b^*) = 3$ et $(2b+a)(d^*) = 2b(d^*)$. Vu (16), ceci implique que $b(d^*) = 0$. Mais alors, $c(d^*) = -(d+a+b)(d^*) = -2$, ce qui contredit (16) puisque $(2b+a)(b^*) = 3$. Ainsi, $b-a$ n'est pas une racine et $a \rfloor b$. De même, $a \rfloor c$.

Supposons qu'on n'ait pas $a \perp\!\!\!\perp d$. Alors $a+d \in \Sigma$, et comme $(a+d)(a^*) = a(a^*) = 2$, on a $\lambda(a+d) > \lambda(a)$, d'où $\lambda(a) = \lambda(b) = \lambda(c)$, en vertu de (15) et (16). Quant à l'égalité $\lambda(a) = \lambda(d)$, elle résulte de (26).

Lemme 4. — *Soient $a, b, c, d \in \Sigma$ quatre racines deux à deux non opposées, dont la somme est nulle. Alors, après permutation éventuelle des trois racines a, b, c, l'un des ensembles de conditions suivants est réalisé, où on a posé $a' = b+c$, $b' = c+a$, $c' = a+b$:*

(i) $a \rfloor b$, $a \rfloor c$, $a \perp\!\!\!\perp d$;

(ii) $a' \in \Sigma$, $a \rfloor b$, $a \perp\!\!\!\perp c$, $a \rfloor a'$;

(iii) $a' \in \Sigma$, $b' \in \Sigma$, $c' \in \Sigma$, $a(b^*) = a(c^*) = -1$, $a \rfloor b$, $a \rfloor c$, $a' \rfloor a$, $-a' \rfloor b$, $-a' \rfloor c$, $f(b, c) = 2$, $a' \perp\!\!\!\perp b'$, $a' \perp\!\!\!\perp c'$.

Faisons tout d'abord deux remarques préliminaires.

(40) Si quatre racines a_i $(i = 1, 2, 3, 4)$, deux à deux non opposées, ont une somme nulle et si $\lambda(a_1) \geqslant \lambda(a_i)$ pour tout i tel que $a_i(a_1^*) \neq 0$, alors les trois nombres $a_j(a_1^*)$ $(j = 2, 3, 4)$ sont, à l'ordre près, égaux à $-1, -1, 0$.

Cela résulte de (15) et du fait que $\sum_{j=2}^{4} a_j(a_1^*) = -a_1(a_1^*) = -2$.

(41) Un ensemble de quatre racines deux à deux non opposées, de somme nulle, ne peut être décomposé en deux sous-ensembles mutuellement orthogonaux,

Supposons en effet qu'une telle décomposition existe et soient b_1, b_1' deux racines réalisant le maximum de λ respectivement dans les deux sous-ensembles en question; on arrive alors à une contradiction en appliquant (40) successivement pour $a_1 = b_1$ et pour $a_1 = b_1'$.

Considérons à présent quatre racines a, b, c, d vérifiant les hypothèses de l'énoncé. Quitte à permuter a, b, c, nous pouvons, sans nuire à la généralité, supposer que

(42) $$\lambda(a) \geqslant \lambda(b), \qquad \lambda(a) \geqslant \lambda(c).$$

Examinons en premier lieu le cas où

(43) $$a(d^*) = d(a^*) = 0.$$

Vu (40), cette relation implique que $b(a^*) = c(a^*) = -1$ et, en vertu du lemme 3, $a \lrcorner b$ et $a \lrcorner c$. Si $a' \notin \Sigma$, les conditions (i) de l'énoncé sont remplies. Supposons donc que $a' \in \Sigma$, et montrons qu'on a alors les relations (iii). Tout d'abord, il résulte du lemme 3 que $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(d)$. De plus, $b' = r_a(c)$, $c' = r_a(b)$, de sorte que $b', c' \in \Sigma$ et $\lambda(b') = \lambda(c') = \lambda(a)$. Tenant compte de (12), (15), (40), on a à présent successivement : $a(b^*) = a(c^*) = b(d^*) = c(d^*) = d(c^*) = d(b^*) = -1$, $c(b^*) = b(c^*) = 0$, $-a'(a^*) = a'(b^*) = a'(c^*) = 2$, $-a(a'^*) = b(a'^*) = c(a'^*) = 1$ et $b'(a'^*) = c'(a'^*) = 0$. Des relations $(-a'-b)(b^*) = (-a'-c)(c^*) = (a'-a)(a^*) = (c-2b)(b^*) = -4$, il résulte que $-a'-b$, $-a'-c$, $a'-a$ et $c-2b$ ne sont pas racines. Par contre, $c-b = r_b(a') \in \Sigma$. Enfin $a' \perp\!\!\perp b'$ et $a' \perp\!\!\perp c'$ en vertu de (26) et du fait que $\lambda(a') = 2\lambda(a) > \lambda(b') = \lambda(c')$. Ceci achève la démonstration dans le cas (43).

Si

(44) $$\lambda(d) \geqslant \lambda(a) = \lambda(b) = \lambda(c),$$

l'une des racines a, b, c est orthogonale à d, vu (40), de sorte qu'on peut se ramener à l'hypothèse (43) par une permutation éventuelle de a, b, c. Nous supposerons donc dorénavant que *ni* (43) *ni* (44) *n'est vérifiée*. Vu (42), ceci implique que $\lambda(a)$ est strictement plus grand que l'un au moins des nombres $\lambda(b)$, $\lambda(c)$, $\lambda(d)$, puis, compte tenu de (16) et (41), que

(45) $$\lambda(a) \geqslant \lambda(e) \quad \text{pour toute racine } e \text{ non orthogonale à } a.$$

Appliquant (40), on voit alors que, après permutation éventuelle de b et c, on a $d(a^*) = b(a^*) = -1$, $c(a^*) = 0$. En vertu du lemme 3 et de l'hypothèse d'après laquelle (44) n'est pas vérifiée, ceci implique que $a \lrcorner b$ et $a \perp\!\!\perp c$. En outre, $a' = -r_a(d) \in \Sigma$, $a'(a^*) = -1$, et il résulte de (15) et (45) que $a'-a \notin \Sigma$, car $(a'-a)(a^*) = -3$, de sorte que $a \lrcorner a'$. Les conditions (ii) de l'énoncé sont donc remplies, et la démonstration achevée.

3.5. Le système $\{N, M_a, \pi\}$: axiomatique.

Soient $X^*(\subset T)$ le groupe engendré par les $a^*(a \in \Sigma)$, H le 2-groupe quotient $X^*/2X^*$, noté multiplicativement, et h_a l'image de a^* par la projection canonique $X^* \to H$; cette image n'est jamais nulle en vertu de (22) et (23).

Toute la suite de cette deuxième partie est basée sur la considération d'un système $\{N, M_a\ (a \in \Sigma), \pi\}$ jouissant des propriétés suivantes : N est un groupe contenant H;

$\pi : N \to W$ est un homomorphisme surjectif de noyau H; pour tout $n \in N$ et tout $h \in H$, on a

$$(46) \qquad n.h.n^{-1} = (\pi(n))(h),$$

où l'opération de W sur H est induite par son action naturelle sur X^*; enfin, pour tout $a \in \Sigma$, M_a est une partie de N formée de deux éléments, inverses l'un de l'autre, et

$$(47) \qquad M_a = M_{-a},$$

$$(48) \qquad m \in M_a \Rightarrow m^2 = h_a,$$

$$(49) \qquad \pi(M_a) = \{r_a\},$$

$$(50) \qquad n.M_a.n^{-1} = M_{(\pi(n))(a)} \quad \text{pour tout } n \in N.$$

On peut montrer [9] qu'il existe, à isomorphisme près, un et un seul système $\{N, M_a, \pi\}$ possédant ces propriétés. Seule l'existence nous importera ici; la démonstration que nous en donnons au n° 4.2 est essentiellement celle de [9], que nous reproduisons pour la commodité du lecteur. Pour faire le lien avec le § 2, signalons que les N, M_a présents correspondent aux N_Z, $M_{a,Z}$ du n° 2.8.

3.6. Existence du système $\{N, M_a, \pi\}$.

Soient $R = \{r_a \mid a \in \Sigma\}$ l'ensemble des réflexions par rapport aux racines et R^* une copie de R. La réplique d'un élément $r \in R$ dans R^* sera notée r^*. Soient L le groupe abélien libre engendré par R^*, et $\overline{H}$ le groupe des carrés dans L, qui est librement engendré par l'ensemble $\{r^{*2} \mid r \in R\}$. Les relations

$$w(r^*) = (w.r.w^{-1})^*$$

définissent une action de W sur L; le produit semi-direct de W et L relatif à cette action sera simplement noté W.L et W et L seront identifiés à des sous-groupes de ce produit. Soient $\overline{N}$ le sous-groupe de W.L engendré par les $r_a.r_a^*$ avec $a \in \Sigma^0$ (système de racines simples), et $\overline{\pi} : \overline{N} \to W$ la restriction à $\overline{N}$ de la projection canonique $W.L \to W (= W.L/L)$; l'homomorphisme $\overline{\pi}$ est surjectif, en vertu de (21).

Montrons que

$$(51) \qquad \overline{N} \cap L = \overline{H}.$$

L'intersection $\overline{N} \cap L$ contient $(r_a.r_a^*)^2 = r_a^{*2}$ pour tout $a \in \Sigma^0$, donc aussi

$$n.r_a^{*2}.n^{-1} = (r_{(\overline{\pi}(n))(a)})^{*2}$$

pour tout $n \in \overline{N}$; vu (20), cela signifie que $\overline{N} \cap L \supset \{r^{*2} \mid r \in R\}$, donc que $\overline{N} \cap L \supset \overline{H}$. Les générateurs $r_a.r_a^*$ $(a \in \Sigma^0)$ de $\overline{N}$ étant congrus à leurs inverses mod $\overline{H}$, tout élément de $\overline{N}$ est congru mod $\overline{H}$ à un élément de la forme $n = \prod_i (r_{a_i}.r_{a_i}^*)$, avec $a_i \in \Sigma^0$, lequel peut encore s'écrire, par un calcul évident,

$$(52) \qquad n = \prod_i r_{a'_i}^* . \prod_i r_{a_i}$$

où on a posé
$$a'_i = \Big(\prod_{j=1}^{i} r_{a_j}\Big)(a_i).$$

Si $n \in \mathrm{L}$, on doit avoir $\overline{\pi}(n) = \Pi r_{a_i} = 1$, et, vu (24) et (52), n appartient à $\overline{\mathrm{H}}$, ce qui établit (51).

Soit $\overline{\mathrm{H}}^0$ le noyau de l'homomorphisme $\overline{\mathrm{H}} \to \mathrm{H}$ qui envoie r_a^{*2} sur h_a pour tout $a \in \Sigma$, identifions H avec le quotient $\overline{\mathrm{H}}/\overline{\mathrm{H}}^0$, posons $\mathrm{N} = \overline{\mathrm{N}}/\overline{\mathrm{H}}^0$, et soit $\pi : \mathrm{N} \to \mathrm{W}$ l'homomorphisme induit par $\overline{\pi}$. Pour toute racine $a \in \Sigma$, soient $\overline{\mathrm{M}}_a$ l'ensemble des éléments de $\overline{\pi}^{-1}(r_a)$ dont le carré est égal à $r_a^{*\pm 2}$, et M_a l'image de $\overline{\mathrm{M}}_a$ par la projection canonique $\overline{\mathrm{N}} \to \mathrm{N}$. Il est clair que les M_a satisfont aux relations (47), (48), (50) et que (49) est vérifié si M_a n'est pas vide. Reste donc à montrer que M_a se compose de deux éléments, inverses l'un de l'autre. Vu (20) et (50), nous pouvons, sans nuire à la généralité, supposer que $a \in \Sigma^0$. Alors $\overline{\pi}^{-1}(r_a)$ est l'ensemble des éléments de la forme $r_a . r_a^* . \overline{h}$, avec $\overline{h} \in \overline{\mathrm{H}}$. Le carré de $r_a . r_a^* . \overline{h}$ est égal à r_a^{*2} si et seulement si $r_a(\overline{h}) = \overline{h}^{-1}$; comme $\overline{\mathrm{H}}$ possède un système générateur libre invariant par r_a, cette condition signifie qu'il existe un $\overline{h}'$ tel que $\overline{h} = r_a(\overline{h}') . \overline{h}'^{-1}$, mais alors l'image canonique de $\overline{h}$ dans H est de la forme $r_a(h) . h^{-1}$, donc est égal à une puissance de h_a (par (7)), c'est-à-dire à 1 ou à h_a. Il s'ensuit que M_a se compose de l'image canonique de $r_a . r_a^*$ dans N et de son inverse.

L'existence d'un système $\{\mathrm{N}, \mathrm{M}_a, \pi\}$ est ainsi démontrée.

3.7. Trois identités.

Proposition 7. — Soient $a, b \in \Sigma$, $m \in \mathrm{M}_a$ et $n \in \mathrm{M}_b$. Alors

$$\text{si } b(a^*) = -1, \text{ on a } h_a . n . h_a . n = 1; \tag{53}$$

$$\text{si } a(b^*) = b(a^*) = -1, \text{ on a } m . n . m = n . m . n; \tag{54}$$

$$\text{si } a \perp\!\!\!\perp b, \text{ on a } m . n = n . m. \tag{55}$$

Il résulte de (7) que

$$\text{si } b(a^*) = -1, \text{ on a } r_b(h_a) = h_a . h_b, \tag{56}$$

de sorte que (53) est une conséquence immédiate de (46) et (48).

Soit $a(b^*) = b(a^*) = -1$. On a alors $r_a(r_b(a)) = b$, donc, vu (50),

$$m . n . \mathrm{M}_a . n^{-1} . m^{-1} = \mathrm{M}_b,$$

de sorte que $m . n . m . n^{-1} . m^{-1} . n^{-1} \in \mathrm{M}_b . n^{-1} = \{1, h_b\}$. Permutant a et b, on voit de même que $m . n . m . n^{-1} . m^{-1} . n^{-1} \in \{1, h_a\}$. Ceci établit (54) car en vertu de (13) et des hypothèses faites sur a, b, on a $h_a . h_b = h_{a+b} \neq 1$.

Soit à présent $a \perp\!\!\!\perp b$. Alors, $r_a(b) = b$, donc $m . \mathrm{M}_b . m^{-1} = \mathrm{M}_b$ et

$$m . n . m^{-1} . n^{-1} \in \{1, h_b\}.$$

De même, $m . n . m^{-1} . n^{-1} \in \{1, h_a\}$. Si on se trouve dans le cas (i) ou le cas (iii) de (26), on a $h_a \neq h_b$ (dans le cas (i), cela résulte de (25), et dans le cas (iii), de ce que $h_a . h_b = h_{a+b}$), et l'assertion (55) s'ensuit. Plaçons-nous au contraire dans le cas (iv) de (26), dont nous reprenons les notations, et soient $m' \in M_{a'}$, et $m'' = n.m'.n^{-1} \in M_{a''}$. On a alors $n.m''.n^{-1} = h_b.m'.h_b = m'^{-1}$ (vu (53)), donc

$$n.m''.m'.m''^{-1}.n^{-1} = m'^{-1}.m''.m' = m''.m'.m''^{-1}$$

(vu (54)). Ceci établit (55) puisque m est égal à $m''.m'.m''^{-1}$ ou à son inverse.

3.8. La fonction ε.

Soit Ψ la partie de $N \times N \times N$ formée des triples (m, n, p) tels qu'il existe trois racines $a, b, c \in \Sigma$ de somme $a + b + c = 0$, pour lesquelles $m \in M_a$, $n \in M_b$ et $p \in M_c$.

Proposition 8. — *Il existe une fonction* $\varepsilon : \Psi \to \{+1, -1\}$ *et une seule possédant les propriétés suivantes :*

(57) $$\varepsilon(m, n, p) = \varepsilon(n, p, m)$$

(58) *si* $a, b \in \Sigma$, $r_a(b) = a + b$, $m \in M_a$, $n \in M_b$ *et* $p \in M_{a+b}$, *on a* $p = m(n)^{\varepsilon(m,n,p)}$.

(Pour la notation $m(n)$, cf. 2.1 (3); à propos de (58) et du lien avec la fonction ε du n° 2.9, voir le n° 4.3.3).

Soit Ψ_1 (resp. Ψ_2, Ψ_3) la réunion des ensembles $M_a \times M_b \times M_c$ avec $a + b + c = 0$ et $r_a(b) = -c$ (resp. $r_b(c) = -a$; $r_c(a) = -b$) et soient $\varepsilon_i : \Psi_i \to \{+1, -1\}$ $(i = 1, 2, 3)$ les fonctions définies comme suit :

$$\varepsilon_1(m, n, p) = \varepsilon_2(p, m, n) = \varepsilon_3(n, p, m) = +1 \text{ ou } -1$$

selon que $$p = m(n) \text{ ou } m(n)^{-1}.$$

Montrons que les fonctions ε_i et ε_j $(i \neq j)$ ont même restriction à l'intersection $\Psi_i \cap \Psi_j$. La question étant invariante par permutation cyclique simultanée des trois arguments des indices 1, 2, 3, nous pouvons supposer que $i = 1$ et $j = 2$. Soit donc $(m, n, p) \in \Psi_1 \cap \Psi_2$; ceci signifie que $m \in M_a$, $n \in M_b$ et $p \in M_{a+b}$ avec $b(a^*) = a(b^*) = -1$. Il s'agit d'établir les implications $p = m(n) \Rightarrow n = p(m)$ et $p = m(n)^{-1} \Rightarrow n = p(m)^{-1}$. La seconde se ramène à la première par la substitution $n \to n^{-1}$; quant à la première, elle s'exprime par la relation $(m(n))(m) = n$, qui n'est autre que (54), comme le montre un calcul immédiat.

En vertu du lemme 2, la réunion des Ψ_i $(i = 1, 2, 3)$ est l'ensemble Ψ tout entier. Par conséquent, il existe une fonction $\varepsilon : \Psi \to \{+1, -1\}$ et une seule dont la restriction à Ψ_i soit ε_i pour tout $i = 1, 2, 3$; cette fonction satisfait manifestement aux conditions de l'énoncé. Réciproquement, (58) signifie que la restriction de ε à Ψ_1 est ε_1, et si ε satisfait en outre à (57), ses restrictions à Ψ_2 et Ψ_3 doivent être respectivement ε_2 et ε_3, ce qui démontre la proposition.

Proposition 9. — *La fonction* ε *est invariante par* N, *c'est-à-dire que*

(59) $$\varepsilon(x(m), x(n), x(p)) = \varepsilon(m, n, p)$$

pour tous $x \in N$ *et* $(m, n, p) \in \Psi$. *Elle satisfait aux identités*

(60) $$\varepsilon(m^{-1}, n, p) = \varepsilon(m, n^{-1}, p) = \varepsilon(m, n, p^{-1}) = -\varepsilon(m, n, p).$$

Enfin elle est alternée en m, n, p :

(61) $$\varepsilon(n, m, p) = \varepsilon(m, p, n) = -\varepsilon(m, n, p).$$

La première assertion est une conséquence immédiate de l'unicité de ε.

Montrons (60). En vertu du lemme 2, nous pouvons supposer, quitte à permuter cycliquement m, n, p, que $m \in \mathrm{M}_a$, $n \in \mathrm{M}_b$, $p \in \mathrm{M}_{a+b}$ avec $r_a(b) = a + b$. Dans ce cas, les deux dernières égalités (60) sont conséquences immédiates de (58), et l'égalité $\varepsilon(m^{-1}, n, p) = -\varepsilon(m, n, p)$, qui peut s'écrire $m^{-1}(n) = m(n)^{-1}$, n'est rien d'autre que l'identité (53). Tenant compte de l'identité (60) ainsi établie, on voit que les conditions (57), (58) sont remplacées par des conditions équivalentes lorsqu'on y remplace ε par la fonction $\varepsilon' : \Psi \to \{+1, -1\}$ définie par $\varepsilon'(m, n, p) = -\varepsilon(m, p, n)$; vu l'unicité de ε, on a donc $\varepsilon' = \varepsilon$, ce qui est la deuxième égalité (61) ; la première reproduit (57).

4. LE THÉORÈME D'EXISTENCE

4.1. Énoncé du théorème.

Théorème 1. — Soient $\mathfrak{T}$ *un espace vectoriel sur* K, Σ *un système de racines dans le dual de* $\mathfrak{T}$, $\mathfrak{E}_a$ $(a \in \Sigma)$ *des espaces vectoriels à une dimension et* $\mathfrak{G}$ *l'espace somme directe de* $\mathfrak{T}$ *et des* $\mathfrak{E}_a$. *Soient* $a^* \in \mathfrak{T}$ $(a \in \Sigma)$, f, N, $\mathrm{M}_a \subset \mathrm{N}$ $(a \in \Sigma)$ *et* ε *définis comme aux nos* 3.1, 3.3, 3.5 *et* 3.8. *Pour toute racine* $a \in \Sigma$ *désignons par* $\mathfrak{e}_{a,m}$ $(m \in \mathrm{M}_a)$ *deux éléments quelconques de* $\mathfrak{E}_a$, *non nuls et opposés* $(\mathfrak{e}_{a,m^{-1}} = -\mathfrak{e}_{a,m})$. *Alors, les relations suivantes, où* $\mathfrak{t} \in \mathfrak{T}$, $a, b \in \Sigma$, $m \in \mathrm{M}_a$, $n \in \mathrm{M}_b$, *et* $p \in \mathrm{M}_{a+b}$ *lorsque* $a + b \in \Sigma$, *définissent une structure d'algèbre de Lie dans* $\mathfrak{G}$:

(1) $$[\mathfrak{T}, \mathfrak{T}] = 0,$$

(2) $$[\mathfrak{t}, \mathfrak{e}_{a,m}] = -[\mathfrak{e}_{a,m}, \mathfrak{t}] = a(\mathfrak{t}) \cdot \mathfrak{e}_{a,m},$$

(3) $$[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = \begin{cases} \varepsilon(m, n, p) \cdot f(a, b) \cdot \mathfrak{e}_{a+b,p} & \text{si } a + b \in \Sigma \\ -a^* \quad \text{si} \quad a + b = 0 & \text{et} \quad m = n \\ 0 \quad \text{si} \quad a + b \notin \Sigma \cup \{0\}. \end{cases}$$

(N.B. — Pour le rapport entre ces $\mathfrak{e}_{a,n}$-ci et ceux du no 2.2, cf. le no 4.3.3).

4.2. Démonstration : identité de Jacobi.

4.2.1. Il résulte de 3.8 (60) que les relations (1), (2) et (3) sont cohérentes et définissent une application bilinéaire $[\ ,\ ] : \mathfrak{G} \times \mathfrak{G} \to \mathfrak{G}$. Celle-ci est anticommutative en vertu de 3.3 (34) et 3.8 (61). Il reste donc à vérifier l'identité de Jacobi.

4.2.2. Définissons une *représentation linéaire du groupe* N *dans* $\mathfrak{G}$ par les formules

$$n(\mathfrak{t}) = (\pi(n))(\mathfrak{t}) \qquad (n \in \mathrm{N},\ \mathfrak{t} \in \mathfrak{T})$$

$$n(\mathfrak{e}_{a,m}) = \mathfrak{e}_{(\pi(n))(a),\, n(m)} \qquad (n \in \mathrm{N},\ a \in \Sigma,\ m \in \mathrm{M}_a).$$

Les transformations linéaires de $\mathfrak{G}$, images des éléments de N, sont des automorphismes de l'algèbre $(\mathfrak{G}, [\ ,\ ])$, c'est-à-dire que, pour tout $n \in \mathrm{N}$ et tous $\mathfrak{g}, \mathfrak{g}' \in \mathfrak{G}$,

$$n([\mathfrak{g}, \mathfrak{g}']) = [n(\mathfrak{g}), n(\mathfrak{g}')]; \tag{4}$$

cela résulte immédiatement de 3.8 (59), et de l'invariance par W des fonctions * et f. Les assertions suivantes, où $a, b \in \Sigma$, $m \in \mathrm{M}_a$ et $n \in \mathrm{M}_b$, sont conséquences de 3.8 (58) et de 3.7 (55) respectivement :

(5) si $a \rfloor b$, on a $[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = m(\mathfrak{e}_{b,n})$;

(6) si $a \perp\!\!\!\perp b$, on a $m(\mathfrak{e}_{b,n}) = \mathfrak{e}_{b,n}$ (c'est-à-dire que M_a centralise $\mathfrak{E}_b$).

4.2.3. *La relation de Jacobi pour trois éléments de* $(\bigcup_{a\in\Sigma} \mathfrak{E}_a) \cup \mathfrak{T}$ *dont un au moins appartient à* $\mathfrak{T}$ est évidente.

4.2.4. *La relation de Jacobi pour un triple* $(\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}, \mathfrak{e}_{c,p})$ *avec* $a+b+c=0$ s'écrit

$$\Sigma[[\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}], \mathfrak{e}_{c,p}] = \Sigma\varepsilon(m, n, p) . f(a, b) . [\mathfrak{e}_{-c,p}, \mathfrak{e}_{c,p}] = 0$$

ou encore

$$\Sigma\varepsilon(m, n, p) . f(a, b) . c^* = 0,$$

où les sommes sont étendues aux permutations cycliques simultanées de a, b, c et m, n, p. Elle est donc vérifiée en vertu de 3.3 (37) et 3.8 (57).

4.2.5. *Vérification de la relation de Jacobi pour un triple* $(\mathfrak{e}_{a,m}, \mathfrak{e}_{-a,m}, \mathfrak{e}_{b,n})$. On a

$$[[\mathfrak{e}_{a,m}, \mathfrak{e}_{-a,m}], \mathfrak{e}_{b,n}] = -b(a^*) . \mathfrak{e}_{b,n}. \tag{7}$$

Supposons que $c = -a - b \in \Sigma$, et soit $p \in \mathrm{M}_c$. On a alors

$$[[\mathfrak{e}_{b,n}, \mathfrak{e}_{a,m}], \mathfrak{e}_{-a,m}] = \varepsilon(n, m, p) . f(a, b) . [\mathfrak{e}_{-c,p}, \mathfrak{e}_{-a,m}] =$$
$$= \varepsilon(n, m, p) . \varepsilon(p, m, n) . f(a, b) . f(a+b, -a) . \mathfrak{e}_{b,n},$$

d'où, vu 3.8 (61),

$$[[\mathfrak{e}_{b,n}, \mathfrak{e}_{a,m}], \mathfrak{e}_{-a,m}] = -f(a, b) . f(a+b, -a) . \mathfrak{e}_{b,n}, \tag{8}$$

et cette relation reste évidemment valable si $a+b \notin \Sigma$. Remplaçons-y a par $-a$ et multiplions les deux membres par -1; il vient

$$[[\mathfrak{e}_{-a,m}, \mathfrak{e}_{b,n}], \mathfrak{e}_{a,m}] = f(-a, b) . f(b-a, a) . \mathfrak{e}_{b,n}. \tag{9}$$

La relation cherchée s'obtient à présent en ajoutant (7), (8) et (9) membres à membres, et en faisant usage de 3.3 (31).

4.2.6. *Vérification de la relation de Jacobi pour un triple* $(\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}, \mathfrak{e}_{c,p})$, *où les racines* a, b, c *sont distinctes et deux à deux non opposées.*

Le cas où $a+b+c \notin \Sigma$ est trivial. Supposons donc que $d = -a-b-c \in \Sigma$. On est alors dans la situation du lemme 4, et on peut supposer, sans nuire à la généralité, que l'un des trois ensembles de conditions (i) à (iii) de l'énoncé de ce lemme est rempli. Nous examinerons les trois cas à tour de rôle.

Cas (i). — Puisque $a \perp\!\!\!\perp d$, il résulte de (6) que m centralise $\mathfrak{E}_{-d}$. On a donc, vu (5) et 3.7 (53),

$$[[\mathrm{e}_{a,m}, \mathrm{e}_{b,n}], \mathrm{e}_{c,p}] = [m(\mathrm{e}_{b,n}), \mathrm{e}_{c,p}] = m([m(\mathrm{e}_{b,n}), \mathrm{e}_{c,p}]) = [h_a(\mathrm{e}_{b,n}), m(\mathrm{e}_{c,p})] = [-\mathrm{e}_{b,n}, [\mathrm{e}_{a,m}, \mathrm{e}_{c,p}]],$$

et ceci est la relation à établir puisque $b+c = -a-d \notin \Sigma$.

Cas (ii). — Vu (5) et 3.7 (55), on a

$$[\mathrm{e}_{a,m}, [\mathrm{e}_{b,n}, \mathrm{e}_{c,p}]] = m([\mathrm{e}_{b,n}, \mathrm{e}_{c,p}]) = [m(\mathrm{e}_{b,m}), \mathrm{e}_{c,m(p)}] = [[\mathrm{e}_{a,m}, \mathrm{e}_{b,n}], \mathrm{e}_{c,p}]$$

ce qui est la relation cherchée, puisque $a+c \notin \Sigma$.

Cas (iii). — Posons $a' = b+c$, $c' = a+b$, et soit u l'élément de $\mathrm{M}_{a'}$ défini par $\varepsilon(n, p, u) = 1$. On a

$$[\mathrm{e}_{b,n}, \mathrm{e}_{c,p}] = 2\mathrm{e}_{a',u}. \tag{10}$$

Des relations $a' \lrcorner\, a$ et $a' \lrcorner\, (-b)$, il résulte, vu (5), que

$$u(\mathrm{e}_{a,m}) = [\mathrm{e}_{a',u}, \mathrm{e}_{a,m}], \tag{11}$$

et

$$u(\mathrm{e}_{-b,n}) = [\mathrm{e}_{a',u}, \mathrm{e}_{-b,n}] = \mathrm{e}_{c,p}. \tag{12}$$

En vertu de la relation $a' \perp\!\!\!\perp c'$ et de (6), u centralise $\mathfrak{E}_{c'}$; en particulier, on a

$$u([\mathrm{e}_{a,m}, \mathrm{e}_{b,n}]) = [\mathrm{e}_{a,m}, \mathrm{e}_{b,n}]. \tag{13}$$

Puisque $a-b \notin \Sigma$, on a, compte tenu de 4.2.5,

$$[[\mathrm{e}_{a,m}, \mathrm{e}_{b,n}], \mathrm{e}_{-b,n}] = [\mathrm{e}_{a,m}, [\mathrm{e}_{b,n}, \mathrm{e}_{-b,n}]] = a(b^*) \,.\, \mathrm{e}_{a,m} = -\mathrm{e}_{a,m}.$$

Transformons les deux membres extrêmes de cette relation par u; il vient, tous calculs faits et compte tenu des relations (10) à (13),

$$[[\mathrm{e}_{a,m}, \mathrm{e}_{b,n}], \mathrm{e}_{c,p}] = -\frac{1}{2}[[\mathrm{e}_{b,n}, \mathrm{e}_{c,p}], \mathrm{e}_{a,m}].$$

En soustrayant membres à membres cette dernière relation et celle qu'on en déduit en interchangeant b et c, on obtient la relation de Jacobi cherchée.

Le théorème est ainsi démontré.

4.3. Remarques.

4.3.1. Le théorème d'unicité.

Soient $\mathfrak{T}$, Σ, $\mathfrak{E}_a$ et $\mathfrak{G}$ comme dans l'énoncé du nº 4.1. Le théorème d'unicité de l'algèbre ayant un système de racines donné peut alors s'énoncer comme suit :

Soit données dans $\mathfrak{G}$ *deux structures d'algèbres de Lie vérifiant toutes deux les relations* (1),

$$[\mathrm{t}, \mathrm{e}] = a(t) \,.\, \mathrm{e} \quad \textit{pour tous} \quad \mathrm{t} \in \mathfrak{T}, \ \mathrm{e} \in \mathfrak{E}_a, \tag{14}$$

et

$$[\mathfrak{E}_a, \mathfrak{E}_b] \begin{cases} = \mathfrak{E}_{a+b} & \textit{si} \quad a+b \in \Sigma, \\ \subset \mathfrak{T} & \textit{si} \quad a+b = 0, \\ = \{0\} & \textit{si} \quad a+b \notin \Sigma \cup \{0\}. \end{cases} \tag{15}$$

Alors il existe une transformation linéaire de $\mathfrak{G}$, *conservant* $\mathfrak{T}$ *et chacun des* $\mathfrak{E}_a$, *induisant sur* $\mathfrak{T}$ *la transformation identique, et transformant l'une des deux structures en l'autre.*

Ce théorème, dont la démonstration, élémentaire et bien connue (cf. par ex. [6]), ne sera pas reprise ici, peut être précisé comme suit, en vertu du théorème 1 :

Théorème 2. — Soit donnée sur $\mathfrak{G}$ *une structure d'algèbre de Lie vérifiant les relations* (1), (14) *et* (15). *Alors, il existe un système d'applications* $\mathfrak{e}_a : \mathrm{M}_a \to \mathfrak{E}_a - \{0\}$ $(a \in \Sigma)$ *telles que* $\mathfrak{e}_a(m^{-1}) = -\mathfrak{e}_a(m)$, *et que la structure d'algèbre de Lie en question soit définie par les relations* (1), (2), (3), *où on pose* $\mathfrak{e}_{a,m} = \mathfrak{e}_a(m)$.

On peut se proposer de démontrer le théorème d'unicité directement sous cette forme, sans passer par l'intermédiaire de la forme usuelle ni du théorème d'existence. C'est en somme ce que nous avons fait au § 2, utilisant toutefois la théorie globale. On trouvera au § 5 des indications sur une démonstration plus élémentaire, relevant exclusivement de la théorie des algèbres de Lie.

4.3.2. Variantes de la démonstration d'existence.

a) Soit Σ' un sous-système du système de racines Σ, fermé dans Σ pour les combinaisons linéaires à coefficients rationnels, et soient N', M'_a, ε' définis à partir de Σ' comme N, M_a, ε à partir de Σ. Alors, il existe un monomorphisme $\varphi : \mathrm{N}' \to \mathrm{N}$ tel que $\varphi(\mathrm{M}'_a) = \mathrm{M}_a$ et qu'on ait (avec un abus de notation évident) $\varepsilon' = \varepsilon\varphi$. Nous traduirons ce fait en disant que la fonction ε est *héréditaire.*

Il résulte de cette propriété, et du fait que l'identité de Jacobi est conséquence de relations entre triples $\mathfrak{e}_{a,m}$, $\mathfrak{e}_{b,n}$, $\mathfrak{e}_{c,p}$, que pour établir le théorème 1, il suffit de considérer le cas où Σ est de rang $\leqslant 3$. Si on suppose connu le théorème 2, on peut alors remplacer la vérification de l'identité de Jacobi effectuée au n° 4.2 par une démonstration quelconque d'existence d'une algèbre de Lie vérifiant (1), (2), (3), pour un système de racines de rang $\leqslant 3$. Lorsqu'on procède ainsi, le § 3 peut être considérablement raccourci; en particulier, on n'a plus besoin du n° 3.4. Si on s'intéresse seulement à l'existence de l'algèbre ayant un système de racines donné, et non aux relations de structure, il suffit de montrer l'existence d'une fonction ε héréditaire telle que le théorème 2 soit vrai, sans qu'on ait à la déterminer explicitement. Au lieu de la fonction ε, on peut d'ailleurs faire usage de la fonction δ, dont l'existence est établie par les considérations du n° 2.2. Celles-ci ramènent donc en fait la démonstration du théorème d'existence à la simple vérification de l'existence des algèbres A_1, A_2, C_2, G_2, A_3, B_3 et C_3 (le § 3 devient ici tout à fait inutile, puisqu'on n'a plus besoin d'une description explicite d'ε). Notons encore que si on admet la théorie classique des algèbres de Lie complexes semi-simples (théorème d'existence exclu) et la classification des systèmes de racines, il suffit, pour établir l'existence de ces sept algèbres, d'exhiber sept algèbres simples de dimensions 3, 8, 10, 14, 15, 21 et 21, les deux dernières étant non isomorphes.

Comme il a déjà été remarqué, le fait de recourir aux considérations du n° 2.2 fait sortir la démonstration du cadre de la théorie des algèbres de Lie. Remarquons toutefois que les faits de la théorie globale qu'on utilise relèvent de la partie la plus élémentaire de cette théorie, exception faite peut-être pour l'isomorphisme $G_a \cong SL_2$ (cf. à ce sujet le § 5).

b) R. Steinberg a imaginé un procédé de « démultiplication des racines courtes », permettant de ramener très simplement la démonstration d'existence (et d'unicité) au cas particulier où toutes les racines du système Σ ont la même longueur. Lorsqu'on se borne à ce cas, notre démonstration se simplifie considérablement. Par exemple : si $a, b, a+b \in \Sigma$, on a toujours $r_a(b) = a+b$ et $f(a, b) = 1$, ce qui simplifie la forme de la plupart des relations et rend évidentes les identités (34) et (37) du nº 3.3; en examinant la démonstration du lemme 4, on constate qu'une bonne partie de celle-ci devient inutile et que dans l'énoncé de ce lemme, on peut ne conserver que la condition (i), ce qui réduit à peu de chose le nº 4.2.6; etc.

4.3.3. La fonction ε et les $\mathfrak{e}_{a,m}$.

Il existe un isomorphisme du groupe $N_{\mathbf{Z}}$ du nº 2.8 sur le groupe N du nº 3.5 qui applique les $M_{a,\mathbf{Z}}$ sur les M_a; pour la facilité de l'exposé, identifions les deux groupes par un tel isomorphisme.

En comparant les relations (39), (40), (41) du nº 2.9 et les relations (57), (58) du nº 3.8, on voit que les deux fonctions ε coïncident sauf si l'argument (m, n, p) appartient à $M_a \times M_b \times M_c$ où a, b, c sont trois racines courtes d'un facteur direct de type G_2 de $\mathfrak{G}$. Cela signifie aussi que, dans l'énoncé du théorème 1, $\mathfrak{e}_{a,m}$ est l'élément de $\mathfrak{E}_a - \{0\}$ correspondant à m par la trijection canonique du nº 1.1, sauf si a est une racine courte d'un facteur direct de type G_2, auquel cas il en est l'opposé.

Dans la démonstration du nº 5.2, nous aurions pu, sans inconvénient, utiliser la fonction ε du nº 2.9 au lieu de celle du nº 3.8; comme il s'agit ici essentiellement d'un auxiliaire de démonstration, nous avons cependant préféré une définition plus simple à une définition plus « naturelle ».

APPENDICE

5. UNE DÉFINITION DU SYSTÈME $\{N, M_a\}$ NE FAISANT PAS INTERVENIR LE GROUPE SIMPLEMENT CONNEXE G

Dans ce paragraphe nous indiquons succinctement une façon d'établir les résultats du § 2 (donc aussi le théorème d'unicité du nº 4.3.1) sans faire usage du groupe simplement connexe G, c'est-à-dire sans utiliser le fait qu'étant donnée une algèbre de Lie semi-simple déployée $\mathfrak{G}$, il existe un groupe G ayant $\mathfrak{G}$ pour algèbre de Lie et tel que, pour toute racine a, le sous-groupe de $\mathfrak{G}$ « engendré par l'algèbre $\mathfrak{G}_a$ » (avec la notation du nº 2.1) soit isomorphe à SL_2. Ce fait peut d'ailleurs être démontré à son tour très simplement à partir de la proposition 10 du nº 5.3, en faisant usage de la décomposition de Bruhat; nous y reviendrons dans une publication ultérieure. Notons encore que la signification donnée ici aux notations M_a, N est à nouveau celle du § 2 (au mode de définition près), et non celle de la deuxième partie.

5.1. Les ensembles M_a.

Soient $\mathfrak{G}$, $\mathfrak{T}$, Σ, $\mathfrak{E}_a$ $(a\in\Sigma)$, $\mathfrak{E}_a^*$, $\mathfrak{G}_a$, a^*, W, r_a, f définis comme au nº 2.1.

Pour toute racine a, nous notons $M_a(=M_{-a})$ l'ensemble des paires $\{\mathfrak{e}, \mathfrak{e}'\}$ telles que $\mathfrak{e}\in\mathfrak{E}_a^*$, $\mathfrak{e}'\in\mathfrak{E}_{-a}^*$ et $[\mathfrak{e}, \mathfrak{e}']=-a^*$; les deux éléments $\mathfrak{e}$, $\mathfrak{e}'$ formant une paire $m\in M_a$ sont désignés par $\mathfrak{e}_{a,m}$ et $\mathfrak{e}_{-a,m}$. Nous posons $M=\bigcup_{a\in\Sigma} M_a$ et $T=\operatorname{Hom}(\widetilde{X}, K^*)$, où $\widetilde{X}$ est le groupe des poids de $\mathfrak{G}$ (nº 2.4). Pour tout $k\in K^*$, l'homomorphisme $x\mapsto k^{x(a^*)}$ de $\widetilde{X}$ dans K^* est noté k_a; l'ensemble $\{k_a \mid k\in K^*\}$ est un sous-groupe de T désigné par T_a.

Pour tous $m=\{\mathfrak{e}, \mathfrak{e}'\}\in M_a$, $n\in M_b$, $t\in T$ et $k\in K^*$, posons

(1) $$m^2=(-1)_a, \qquad k_a . m = m . k_a^{-1}=\{k.\mathfrak{e}, k^{-1}.\mathfrak{e}'\};$$

(2) $$t(m)=t(a)_a . m;$$

(3) $$m(n)=(\exp \operatorname{ad} \mathfrak{e} . \exp \operatorname{ad} \mathfrak{e}' . \exp \operatorname{ad} \mathfrak{e})(n)=(\exp \operatorname{ad} \mathfrak{e}' . \exp \operatorname{ad} \mathfrak{e} . \exp \operatorname{ad} \mathfrak{e}')(n)\in M_{r_a(b)}.$$

L'égalité des deuxième et troisième membres de (3) résulte de la proposition 1; l'appartenance de $m(n)$ à $M_{r_a(b)}$ se déduit du fait que $(\exp \operatorname{ad} \mathfrak{e} . \exp \operatorname{ad} \mathfrak{e}' . \exp \operatorname{ad} \mathfrak{e})$ centralise le noyau de a dans $\mathfrak{T}$ et permute a^* et $-a^*$, donc induit sur $\mathfrak{T}$ la réflexion r_a. Les relations (1) définissent une loi de groupe dans $T_a \cup M_a$; pour cette loi,

(4) $$m^{-1}=(-1)_a . m=\{-\mathfrak{e}, -\mathfrak{e}'\}.$$

Les relations (2) et (3) définissent des opérations de T et de M sur M.

On définit comme au nº 2.3 la fonction δ qui détermine les constantes de structure de $\mathfrak{G}$. La proposition 4 du n° 2.6, à la démonstration de laquelle il n'y a rien à changer ici, caractérise δ à partir des diverses structures définies dans M par (1), (2), (3). Reste à déterminer à isomorphisme près l'ensemble M muni de ces structures. C'est là l'objet de la proposition 10.

5.2. Identités.

Lemme 5. — Soient $a, b \in \Sigma$, $m \in \mathrm{M}_a$, $n \in \mathrm{M}_b$, $p \in \mathrm{M}$.

$$(m(n))(p) = m(n(m^{-1}(p))); \tag{5}$$

$$m(m(n)) = ((-1)_a)(n); \qquad m^{-1}(n) = ((-1)_a)(m(n)); \tag{6}$$

$$si \quad r_a(b) = b, \quad on\ a \quad m(n) = n^{(-1)^{f(a,b)+1}}; \tag{7}$$

$$si \quad r_a(b) = a+b, \quad on\ a \quad [\mathfrak{e}_{a,m}, \mathfrak{e}_{b,n}] = f(a, b) \cdot \mathfrak{e}_{a+b,q}, \quad avec \quad q = m(n)^{(-1)^{f(a+b)+1}}; \tag{8}$$

$$si \quad r_a(b) = r_b(a) = a+b, \quad on\ a \quad m(n) = n(m^{-1}). \tag{9}$$

(5) est immédiate. Les identités (6) à (8) résultent de la proposition 2 (n° 1.2) et de son corollaire (n° 1.3), appliqués à la représentation de $\mathfrak{G}_a$ dans l'espace $\mathfrak{B}$ du n° 2.6, déduite par restriction de la représentation adjointe de $\mathfrak{G}$. Enfin, (9) est une conséquence directe de (8).

5.3. Le groupe N.

Proposition 10. — Il est possible d'inclure l'ensemble $\mathrm{M} \cup \mathrm{T}$ *dans un groupe* N *de telle façon que* $\mathrm{M} \cup \mathrm{T}$ *engendre* N, *que le groupe* T *et les groupes* $\mathrm{T}_a \cup \mathrm{M}_a$ *définis par* (1) *soient des sous-groupes de* N, *et que les opérations de* T *et* M *sur* M *définies par* (2), (3) *soient les opérations par automorphisme intérieur au sein de* N. *Ces conditions caractérisent* N *et l'injection* $\mathrm{M} \cup \mathrm{T} \rightarrow \mathrm{N}$ *à isomorphisme canonique près. Si* Σ^0 *est un système de racines simples et si, pour tout* $a \in \Sigma^0$, q_a *désigne un élément quelconque de* M_a, *l'ensemble* $\mathrm{T} \cup \{q_a \mid a \in \Sigma^0\}$ *engendre* N *et les relations* (13), (14), (15) *de* 2.4 *forment avec les relations définissant la loi de groupe de* T *un système complet de relations pour* N.

Nous ne ferons qu'indiquer les grandes lignes de la démonstration.

Soient T′ une copie du groupe T et $\{q'_a \mid a \in \Sigma^0\}$ une copie de l'ensemble $\{q_a \mid a \in \Sigma^0\}$. Un élément de T′ sera représenté par la même lettre que l'élément de T qu'il reproduit, affectée d'un accent. Soit N′ un groupe contenant $\mathrm{T}' \cup \{q'_a \mid a \in \Sigma^0\}$, engendré par cet ensemble, et tel que les relations en question dans l'énoncé précédent, transposées à $\mathrm{T}' \cup \{q'_a \mid a \in \Sigma^0\}$, forment un système complet de relations pour N′. L'existence d'un tel groupe N′ a été établie dans [9]; elle se déduit aussi aisément de 3.6. La projection canonique $\mathrm{N}' \rightarrow \mathrm{W} \cong \mathrm{N}'/\mathrm{T}'$ sera notée π'.

Pour tous $t \in \mathrm{T}$, $m \in \mathrm{M}$, $a \in \Sigma^0$, posons

$$t'(m) = t(m) \tag{10}$$

et

$$q'_a(m) = q_a(m). \tag{11}$$

Ainsi est définie une opération de l'ensemble $T' \cup \{q'_a | a \in \Sigma^0\}$ sur M, et la première étape de la démonstration consiste à montrer que cette opération s'étend en une opération du *groupe* N' sur M. Pour cela, il faut établir les relations suivantes, où $m \in M$, t, $t_1 \in T$, $a, b \in \Sigma^0$, et l_{ab} est défini comme au nº 2.4 :

(12) $$(t.t_1)(m) = t(t_1(m));$$

(13) $$q_a(q_a(m)) = (-1)_a(m);$$

(14) $$q_a(t(q_a^{-1}(m))) = (r_a(t))(m);$$

(15) $$\underbrace{q_a(q_b(q_a(\ldots}_{l_{ab}\text{ termes}}(m)\ldots))) = \underbrace{q_b(q_a(q_b(\ldots}_{l_{ab}\text{ termes}}(m)\ldots))).$$

Les trois premières résultent immédiatement de (2) et (6). Examinons (15) de plus près. Si $l_{ab} = 2$, il suit de (7) que

(16) $$q_a(q_b) = q_b.$$

Si $l_{ab} = 3$, il résulte de (9) que

(17) $$q_a(q_b) = q_b(q_a^{-1}).$$

Si $l_{ab} = 4$, et si a est la « plus longue » des deux racines a, b, on a $r_b(a) \perp\!\!\!\perp a$, de sorte que, vu (7),

(18) $$(q_b(q_a))(q_a) = q_a.$$

Enfin, si $l_{ab} = 6$, on a $r_a(r_b(a)) \perp\!\!\!\perp b$, et

(19) $$(q_a(q_b(q_a)))(q_b) = q_b.$$

Faisant opérer sur m les deux membres de chacune des relations (16) à (19), on obtient (15) par des transformations faciles, utilisant (5) et (6).

Ces calculs montrent non seulement que les relations (10), (11) définissent une action de N' sur M, mais aussi que s'il existe un groupe N possédant les propriétés de l'énoncé, l'application canonique $T' \cup \{q'_a | a \in \Sigma^0\} \to T \cup \{q_a | a \in \Sigma^0\}$ s'étend en un homomorphisme $N' \to N$. Celui-ci est en fait un isomorphisme parce que $T' \to T$ est bijectif et que le groupe de Weyl $W = N'/T'$ opère effectivement sur $T \cong T'$. Ceci établit l'unicité de N et la dernière assertion de l'énoncé.

L'étape suivante est la démonstration du fait que, si $n \in N'$, $a, b \in \Sigma^0$ et $t \in T_b$, alors

(20) $$n(q_a) = t.q_b \Leftrightarrow n(q'_a) = n.q'_a.n^{-1} = t'.q'_b.$$

Posons $\pi'(n) = w$. Les deux relations (20) impliquent que $w(a) = \pm b$. Quitte à remplacer éventuellement n par $n.q'_a$, nous pouvons supposer que $w(a) = b$. Utilisant la proposition 1.5 de [9], on se ramène par des raisonnements faciles à la considération du seul cas où w appartient au groupe engendré par r_a et r_c avec $c \in \Sigma^0$ (si $b \neq a$, on a nécessairement $c=b$). Par l'examen des systèmes de racines de rang 2, on voit alors que l'une des conditions suivantes est remplie :

(i) $w=1$, $b=a$;

(ii) $l_{ac}=2$, $w=r_c$, $b=a$;

(iii) $l_{ac}=3$, $w=r_a.r_c$, $b=c$;

(iv) $l_{ac}=4$, $w=r_c.r_a.r_c$, $b=a$;

(v) $l_{ac}=6$, $w=r_c.r_a.r_c.r_a.r_c$, $b=a$.

Dans le cas (i), (20) est une conséquence immédiate de (2). Plus généralement, on montre sans peine que si (20) est vraie pour un $n\in N'$, elle l'est pour tout élément de $n.T'$. Il suffit donc, dans chacun des cas (ii) à (v), d'établir (20) pour un élément $n\in\pi'^{-1}(w)$ particulier. Nous choisissons cet élément comme suit :

$$\text{(21)}\qquad \begin{cases} \text{(ii)} \quad n=q'_c; & \text{(iii)} \quad n=q_a'^{-1}.q'_c; \\ \text{(iv)} \quad n=q'_c(q'_a); & \text{(v)} \quad n=(q'_c(q'_a(q'_c))). \end{cases}$$

Il résulte alors de (7) et (9) que l'élément $t\in T_b$ défini par la première relation (20) est donné, suivant le cas, par

$$\text{(22)}\qquad \begin{cases} \text{(ii) et (v)} & t=1; \\ \text{(iii)} & t=(-1)_b; \\ \text{(iv)} & t=1 \text{ ou } (-1)_b \text{ selon que la racine } a \text{ est} \\ & \quad \text{« plus longue » ou « plus courte » que } c. \end{cases}$$

Développant à présent les relations obtenues en remplaçant n et t par les diverses valeurs (21) et (22) dans la deuxième relation (20), on constate que celle-ci se ramène chaque fois à la relation 2.4 (14) (où les q sont remplacés par des q').

En vertu de l'équivalence (20), ainsi établie, les relations

$$\varphi(n(q_a))=n(q'_a) \quad (n\in N',\ a\in\Sigma^0)$$

définissent une injection $\varphi: M\to N'$. Soient N un ensemble contenant $M\cup T$ et $\psi: N\to N'$ une bijection dont les restrictions à T et M soient respectivement l'isomorphisme canonique $T\to T'$ et l'injection φ. Transportons la structure de groupe de N' sur N par ψ^{-1}. Il est à présent immédiat que le groupe N possède les propriétés de l'énoncé.

6. QUATERNES DE RACINES DE SOMME NULLE

Le lemme 4 du n° 3.4 est un lemme *ad hoc* rassemblant les propriétés des quaternes de racines deux à deux non opposées, de somme nulle, utilisées dans la démonstration du n° 4.2. En fait, on peut aisément décrire toutes les configurations possibles d'un tel quaterne. C'est ce que nous nous proposons de faire ici.

Soient $a_i\ (i=1, \ldots, 4)$ quatre racines, deux à deux non opposées, telles que $\sum_i a_i=0$. Les a_i appartiennent à un même facteur direct simple de Σ, sinon la somme $\sum_i a_i$

pourrait être décomposée en deux sommes partielles nulles, dont l'une au moins n'aurait pas plus de deux termes. Posons $\lambda_i = \lambda(a_i)$ et $a_j(a_i^*) = \alpha_{ij}$. D'après les relations (3), (11), (12), (15) et (16) du § 3, ces nombres possèdent les propriétés suivantes :

les λ_i sont entiers >0, et prennent au plus deux valeurs;

si $\lambda_i = \lambda_j$ on a $\alpha_{ij} = 0, \pm 1$ ou 2; si $\lambda_i > \lambda_j$, $\lambda_i/\lambda_j = 2$ ou 3 et $\alpha_{ij} = 0$ ou ± 1;

$$\alpha_{ii} = 2;$$

$$\sum_j \alpha_{ij} = 0 \quad \text{pour tout } i;$$

$$\alpha_{ij}\alpha_{ji}^{-1} = \lambda_j \lambda_i^{-1}.$$

Il est facile de déterminer toutes les solutions de ce système de relations; on trouve qu'à une permutation des indices 1 à 4 près, elles sont toutes données par l'un des ensembles de relation (I) à (VI) ci-après, où α désigne la matrice des α_{ij} et $\therefore$ symbolise la proportionnalité :

(I) $\quad (\lambda_i) \therefore (1, 1, 1, 1)$ et $\alpha = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

(II) $\quad (\lambda_i) \therefore (1, 1, 1, 2)$ et $\alpha = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 1 & -2 \\ -1 & 1 & 2 & -2 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

(III) $\quad (\lambda_i) \therefore (1, 1, 1, 3)$ et $\alpha = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 2 & -3 \\ -1 & 2 & 2 & -3 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

(IV) $\quad (\lambda_i) \therefore (1, 1, 2, 2)$ et $\alpha = \begin{pmatrix} 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

(V) $\quad (\lambda_i) \therefore (1, 1, 2, 2)$ et $\alpha = \begin{pmatrix} 2 & 2 & -2 & -2 \\ 2 & 2 & -2 & -2 \\ -1 & -1 & 2 & 0 \\ -1 & -1 & 0 & 2 \end{pmatrix}$

(VI) $\quad (\lambda_i) \therefore (1, 1, 3, 3)$ et $\alpha = \begin{pmatrix} 2 & 1 & -3 & 0 \\ 1 & 2 & 0 & -3 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$

La matrice α détermine, à similitude près, la configuration « euclidienne » du quaterne (a_i). Il reste à voir, dans chacun des cas (I) à (VI) si le quaterne correspondant peut être inclus dans un système de racines. Nous nous proposons de donner ici, sans entrer dans le détail des démonstrations, d'ailleurs élémentaires, la solution d'un problème plus précis, à savoir, la classification, par rapport au groupe des automorphismes d'un système de racines donné Σ, de tous les quaternes de racines deux à deux non opposées, de somme nulle.

Supposant à nouveau que les $\{a_i\}$ fassent partie d'un système de racines Σ, nous noterons Σ' le sous-système de Σ formé par toutes les racines qui sont combinaisons linéaires à coefficients rationnels des a_i. Nous dirons que deux quaternes sont *de même type* si leurs matrices α sont les mêmes (après permutation éventuelle de l'un des quaternes) et si les systèmes Σ' qu'ils engendrent sont isomorphes. La raison de cette terminologie apparaîtra dans l'énoncé qui termine ce paragraphe. Le tableau ci-après donne l'énumération de tous les types de quaternes possibles. Le chiffre romain de la première colonne se rapporte à la numérotation des matrices α introduite plus haut; les deux autres colonnes donnent le type auquel appartient le système Σ' (avec la notation classique d'E. Cartan), et un ensemble de racines simples de ce système. Les notations relatives au cas I s'expliquent ainsi : les cas I′ et I″ se distinguent par le fait que dans le type I″, a_1+a_4 est une racine, et non dans les types I′. On remarquera que dans tous les cas, à l'exception de I'_2, les éléments de Σ' sont combinaisons linéaires à coefficients *entiers* des a_i; dans le cas I'_2, les racines qui sont combinaisons linéaires à coefficients entiers des a_i forment un sous-système de type A_3.

Types de quaternes

α	Σ'	Racines simples
I'_1	A_3	a_1, a_2, a_4
I'_2	B_3	$\frac{1}{2}(a_4-a_1), a_1, a_2$
I''	C_3	a_4-a_1, a_1, a_2
II	C_3	a_1, a_2, a_4
III	G_2	$a_1=a_3, a_4$
IV	B_3	a_1, a_3, a_4
V	B_2	$a_1=a_2, a_3$
VI	G_2	$a_1, a_3=a_2-2a_1$

Enfin, la solution au problème posé plus haut est à présent contenue dans l'énoncé suivant.

Pour qu'un système de racines Σ contienne un quaterne de type donné, il faut et il suffit que le diagramme de Dynkin de Σ possède un sous-diagramme isomorphe au diagramme de Dynkin du système Σ' du type en question. Si Σ est simple, deux quaternes de même type sont équivalents pour le groupe des automorphismes de Σ. Plus précisément, si les deux quaternes $\{a_i\}$ et $\{a'_i\}$ sont ordonnés de telle façon que $a_j(a_i^*) = a'_j(a'_i)$ pour tous i, j, alors il existe un automorphisme de Σ qui transforme a_i en a'_i pour tout i.

BIBLIOGRAPHIE

[1] Borel (A.) et Tits (J.), Groupes réductifs, *Publ. Math.* I.H.E.S., 27 (1965), 55-151.
[2] Bourbaki (N.), *Groupes et algèbres de Lie*, chap. V : « Systèmes de racines » (à paraître).
[3] Chevalley (C.), Sur certains groupes simples, *Tôhoku Math. Jour.* (1), 7 (1955), 14-66.
[4] Chevalley (C.), *Séminaire sur la classification des groupes de Lie algébriques*, 2 vol., Paris, 1958 (notes polycopiées).
[5] Demazure (M.) et Grothendieck (A.), *Schémas en groupes*, I.H.E.S., 1964 (notes polycopiées).
[6] Jacobson (N.), *Lie algebras*, Inters. tracts in pure math., 10, Interscience publ., New York, 1962.
[7] *Séminaire Sophus Lie*, I, Théorie des algèbres de Lie, 1954-55, Paris, Secrétariat Mathématique.
[8] *Séminaire sur les algèbres de Lie*, VI, Bases de Chevalley (exposés de J. Tits, rédigés par P. Deligne), Bruxelles, 1964, notes polycopiées.
[9] Tits (J.), Normalisateurs de tores, I, Groupes de Coxeter étendus, *Journal of Algebra*, 3 (1966).
[10] Weyl (H.), Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformation, III, *Math. Zeitschrift*, 24 (1926), 328-376 (= *Selecta*, Birkhäuser Verlag, 1956, p. 325).

---

(1) Nous nous écartons en ceci de la terminologie adoptée par exemple dans [1] et [9].

Manuscrit reçu le 1er mars 1966.