

SÉMINAIRE "SOPHUS LIE"

F. BRUHAT

Formes réelles des algèbres semi-simples

Séminaire "Sophus Lie", tome 1 (1954-1955), exp. n° 11 et 12, p. 1-15

http://www.numdam.org/item?id=SSL_1954-1955__1__A15_0

© Séminaire "Sophus Lie"

(Secrétariat mathématique, Paris), 1954-1955, tous droits réservés.

L'accès aux archives de la collection « Séminaire "Sophus Lie" » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Exposés n° 11 et 12

FORMES RÉELLES DES ALGÈBRES SEMI-SIMPLES
(Exposés de F. BRUHAT des 1 et 8.2.55).

Errata aux exposés précédents.

Un certain nombre d'erreurs se sont glissées dans les exposés précédents :

Exposé n°9 : page 9-05 ligne 4 du haut lire $r = - (\sum \dots)$

Exposé n° 10 : page 10-01 ligne 5 du bas lire : V_{Λ} est l'ensemble des vecteurs $v \in V$ tels que $H.v = \Lambda(H)v$

page 10-01 ligne 14 du bas lire : "(avec $a \neq 0$)" et non "avec $a > 0$ ". Le rectificatif 1) de la page 8 est alors sans objet.

page 10-02 lignes 3 à 5 du haut : remplacer le texte par le suivant : "Étudions le cas de V irréductible. Les poids de V étant en nombre fini (ils correspondent aux valeurs propres de H), il existe un poids Λ_0 tel que $\Lambda_0 + \alpha$ ne soit plus un poids. Alors si $e_0 \in V_{\Lambda_0}$ $Xe_0 \in V_{\Lambda_0 + \alpha}$ donc $Xe_0 = 0$." .

page 10-02 ligne 12 du bas lire $Yf_k = (k-m) f_{k+1}$

page 10-03 ligne 10 du haut lire : $\rho(X) \rho(Y)v = -\frac{1}{2}(i+1) j \alpha(H)v$.
ajouter : et $\rho(Y) \rho(X)v = -\frac{1}{2}(j+1) i \alpha(H)v$.

page 10-07 ligne 1 à 3 du haut : remplacer le texte par le suivant
"Le système Π des racines simples détermine le système Σ des racines positives ; en effet toute racine positive est soit simple soit de la forme $\beta = \gamma + \alpha_i$ où γ est une racine positive et α_i est simple. En effet on a $\beta = \sum m_i \alpha_i$ avec $m_i \geq 0$ les α_i étant simples, donc $\langle \beta, \beta \rangle = \sum m_i \langle \beta, \alpha_i \rangle > 0$ si $\beta \neq 0$ donc comme les m_i sont positifs ou nuls, pour un i au moins on a $\langle \beta, \alpha_i \rangle > 0$. Appliquant la proposition 1, on voit que

$$p_{\beta, \alpha_i} + q_{\beta, \alpha_i} = -2 \frac{\langle \beta, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle} < 0$$

donc $p_{\beta, \alpha_i} < 0$ et $\gamma = \beta - \alpha_i$ est une racine. Cette racine est positive sinon on aurait $-\gamma > 0$ et $\alpha_i = \beta - \gamma$ ne serait pas simple.

Cherchons parmi les combinaisons linéaires $\sum m_i \alpha_i$ ($m_i \geq 0$) celles qui sont des racines. Appelons ordre m d'une telle combinaison l'entier positif $\sum m_i$. Les combinaisons d'ordre 1 sont les α_i qui sont des racines. Supposons déterminées les racines d'ordre $\leq m$. Les racines d'ordre $m+1$ sont de la forme $\gamma + \alpha_i$ où γ est une racine d'ordre m . Il faut donc déterminer parmi les $\gamma + \alpha_i$ les combinaisons qui sont des racines. Or la α_i -série contenant γ ne comprend que des racines positives si $\gamma \neq \alpha_i$ car $\gamma = \sum_{j \neq i} m_j \alpha_j + m \alpha_i$
 $\gamma + k \alpha_i = \sum_{j \neq i} m_j \alpha_j + (m+k) \alpha_i$ si l'un des m_j est > 0 ceci implique $m+k \geq 0$ donc $\gamma + k \alpha_i$ positive. Si tous les m_j sont nuls $\gamma = m \alpha_i$ et $m = 1$ donc $\gamma = \alpha_i$. $\gamma + k \alpha_i$ est d'ordre $m+k \leq m$ si $k \leq 0$. Donc la borne inférieure p de la série est connue car on connaît les racines d'ordre $\leq m$. Comme

$p + q = -2 \frac{\langle \gamma, \alpha_i \rangle}{\langle \alpha_i, \alpha_i \rangle}$ d'après la proposition 1, q est connu et on sait suivant que q est plus grand ou plus petit que 1 si $\gamma + \alpha_i$ est racine ou non.

---La première partie de la démonstration de la proposition 5 est incomplète. Il faut remplacer comme suit :

Supposons $\Pi = \Pi' \cup \Pi''$ $E_{\Pi'} \perp E_{\Pi''}$. Soit Σ' l'ensemble des racines positives de la forme $\sum m_i \alpha_i$, $m_i \geq 0$ $\alpha_i \in \Sigma'$ et soit Σ'' défini de manière analogue ; si $\alpha' \in \Sigma'$ $H'_{\alpha'} = \sum m_i H'_{\alpha_i} \in E_{\Pi'}$. Donc si $\alpha' \in \Sigma'$ $\alpha'' \in \Sigma''$ α' et α'' sont perpendiculaires : $\langle \alpha', \alpha'' \rangle = 0$. Or $\alpha' - \alpha''$ n'est pas racine car $\alpha' - \alpha'' = \sum m_i \alpha_i - \sum n_j \beta_j$ ($\alpha_i \in \Sigma'$ $\beta_j \in \Sigma''$ $m_i, n_j \geq 0$) et ceci contredit la définition d'un système fondamental. Mais d'après la proposition 1 $p + q = -2 \frac{\langle \alpha', \alpha'' \rangle}{\langle \alpha'', \alpha'' \rangle} = 0$. Comme $q = 0$ $p = 0$ et $\alpha' + \alpha''$ n'est pas racine.

positive

Or il est clair que toute racine est de la forme α' , α'' ou $\alpha' + \alpha''$ donc $\Sigma = \Sigma' \cup \Sigma''$.

Posons $\mathfrak{g}' = E_{\Pi'} + \sum_{\alpha \in \Sigma'} (\mathfrak{g}^{\alpha} + \mathfrak{g}^{-\alpha})$ $\mathfrak{g}'$ est une sous-algèbre de $\mathfrak{g}$ car si $\alpha, \beta \in \Sigma'$ $\alpha + \beta \in \Sigma'$ et $\alpha - \beta \in \pm \Sigma'$. De plus $[E_{\Pi'}, \mathfrak{g}^{\alpha}] \subset \mathfrak{g}^{\alpha}$ et $[\mathfrak{g}^{\alpha}, \mathfrak{g}^{-\alpha}] = K \cdot H'_{\alpha} \in E_{\Pi'}$. $\mathfrak{g}''$ définie de manière analogue est une sous-algèbre. Or $[\mathfrak{g}', \mathfrak{g}''] = 0$ car $\pm \alpha' \pm \alpha''$ n'est pas une racine donc $[\mathfrak{g}^{\pm \alpha'}, \mathfrak{g}^{\pm \alpha''}] = 0$ et par ailleurs $[H'_{\alpha'}, E_{\Pi''}] = \langle \alpha', \alpha'' \rangle E_{\alpha''} = 0$ etc... Enfin il est clair que $\mathfrak{g}$ est somme directe de $\mathfrak{g}'$ et $\mathfrak{g}''$ donc n'est pas simple.

1.- Normalisation d'une base de Weyl.

Pour ce paragraphe encore, le corps de base est un corps algébriquement clos de caractéristique 0 quelconque - $\mathfrak{g}$ est une algèbre de Lie sémi-simple dont $\mathfrak{h}$ est une sous-algèbre de Cartan. On a choisi $E_\alpha \neq 0$ dans $\mathfrak{g}^\alpha$ de sorte qu'on ait les relations suivantes

- (1) $[H, E_\alpha] = \alpha(H)E_\alpha$
- (2) $[E_\alpha, E_{-\alpha}] = -H'_\alpha$ et $\langle E_\alpha, E_{-\alpha} \rangle = -1$
- (3) $[E_\alpha, E_\beta] = N_{\alpha, \beta} E_{\alpha+\beta}$ si $\alpha+\beta \neq 0$ est une racine
 $= 0$ sinon
- (4) $\langle H, H'_\alpha \rangle = \alpha(H)$

On convient que $N_{\alpha, \beta} = 0$ si $\alpha+\beta \neq 0$ n'est pas une racine. Les formules montrent que la structure de $\mathfrak{g}$ est déterminée par les $N_{\alpha, \beta}$. On va démontrer un certain nombre de relations nécessaires entre les $N_{\alpha, \beta}$, relations qu'on démontre facilement être suffisantes pour que les axiomes des algèbres de Lie soient vérifiés par un crochet donné a priori par les formules (1) à (3). Tout d'abord $N_{\beta, \alpha} = -N_{\alpha, \beta}$ par suite de l'anticommutativité.

Lemme 1.- α, β, γ sont 3 racines non nulles $\alpha+\beta+\gamma=0$. Alors

$$(5) \quad N_{\alpha\beta} = N_{\beta\gamma} = N_{\gamma\alpha}$$

$$\text{On a } [E_\beta, E_\gamma] = N_{\beta, \gamma} E_{\beta+\gamma} = N_{\beta, \gamma} E_{-\alpha}$$

$$[E_\alpha, [E_\beta, E_\gamma]] = N_{\beta, \gamma} [E_\alpha, E_{-\alpha}] = -N_{\beta, \gamma} H'_\alpha$$

Si l'on écrit l'identité de Jacobi relative à $E_\alpha, E_\beta, E_\gamma$ on a

$$(6) \quad [E_\alpha, [E_\beta, E_\gamma]] + [E_\beta, [E_\gamma, E_\alpha]] + [E_\gamma, [E_\alpha, E_\beta]] = 0$$

$$\text{soit} \quad N_{\beta, \gamma} H'_\alpha + N_{\gamma, \alpha} H'_\beta + N_{\alpha, \beta} H'_\gamma = 0$$

$$\text{On a donc} \quad N_{\beta, \gamma} \cdot \alpha + N_{\gamma, \alpha} \cdot \beta + N_{\alpha, \beta} \cdot \gamma = 0$$

Par ailleurs $\alpha+\beta+\gamma=0$. Si ces deux relations linéaires étaient distinctes, les 3 racines seraient proportionnelles à l'une d'elles soit α par exemple, mais alors, on a $\beta = -\alpha$ ou $\gamma = -\alpha$ donc $\gamma=0$ ou $\beta=0$ contrairement aux hypothèses. Ces deux relations linéaires entre α, β, γ n'étant pas distinctes, on a

$$N_{\alpha\beta} = N_{\beta\gamma} = N_{\gamma\alpha}$$

Lemme 2.- Si $\alpha, \beta, \gamma, \delta$ sont 4 racines non nulles, dont les sommes deux à deux ne sont pas nulles et telles que $\alpha + \beta + \gamma + \delta = 0$, on a

$$(7) \quad N_{\alpha\beta} N_{\gamma\delta} + N_{\beta\gamma} N_{\alpha\delta} + N_{\gamma\alpha} N_{\beta\delta} = 0$$

En effet on a $[E_\alpha, [E_\beta, E_\gamma]] = N_{\beta,\gamma} [E_\alpha, E_{\beta+\gamma}] = N_{\beta,\gamma} N_{\alpha, \beta+\gamma} E_{-\delta}$ car $\alpha + \beta + \gamma = -\delta$ et $\beta + \gamma \neq 0$. Mais d'après le lemme 1 $N_{\alpha, \beta+\gamma} = N_{\delta, \alpha} = -N_{\alpha, \delta}$

donc
$$[E_\alpha, [E_\beta, E_\gamma]] = -N_{\beta,\gamma} N_{\alpha,\delta} E_{-\delta}$$

Reportant dans l'identité de Jacobi (6) et tenant compte de $E_{-\delta} \neq 0$, il vient bien l'égalité (9).

Lemme 3.- soient α, β deux racines avec $\alpha + \beta \neq 0$ $\alpha, \beta \neq 0$. Supposons que la α -série qui contient β contienne exactement les $\beta + k\alpha$ avec $p \leq k \leq q$ alors

$$(8) \quad N_{\alpha,\beta} N_{-\alpha,-\beta} = \frac{1}{2} \langle \alpha, \alpha \rangle q(1-p)$$

$\mathfrak{g}^{\beta+k\alpha}$ étant de dimension 1, la représentation de la sous-algèbre $\{E_\alpha, E_{-\alpha}, H'_\alpha\}$ dans $\sum_k \mathfrak{g}^{\beta+k\alpha}$ est irréductible. On peut donc appliquer le 5) du

théorème 1 de l'Exposé n° 10, d'où

$$[E_{-\alpha}, [E_\alpha, E_\beta]] = -\frac{1}{2} \langle \alpha, \alpha \rangle q(1-p) E_\beta$$

mais

$$\begin{aligned} [E_{-\alpha}, [E_\alpha, E_\beta]] &= N_{\alpha,\beta} [E_{-\alpha}, E_{\alpha+\beta}] \\ &= N_{\alpha,\beta} N_{-\alpha, \alpha+\beta} E_\beta \\ &= + N_{\alpha,\beta} N_{-\beta, -\alpha} E_\beta \end{aligned}$$

la dernière égalité résultant du lemme 1 appliqué à $-\alpha$, $\alpha + \beta$, $-\beta$. Si l'on rappelle que $N_{-\alpha, -\beta} = -N_{-\beta, -\alpha}$ le lemme en résulte aussitôt.

Nous allons considérer deux algèbres de Lie semi-simples, $\mathfrak{g}$ et $\mathfrak{g}'$, dont $\mathfrak{h}$ et $\mathfrak{h}'$ sont respectivement des sous-algèbres de Cartan. On suppose donnés des $E_\alpha \in \mathfrak{g}^\alpha$ de sorte que les relations (1) à (4) soient vérifiées avec les constantes de structure $N_{\alpha,\beta}$. Δ (resp. Δ') désigne l'ensemble des racines non nulles de $\mathfrak{g}$ (resp. $\mathfrak{g}'$).

Théorème 1.- Soit φ une application linéaire biunivoque de $\mathfrak{h}_0$ sur $\mathfrak{h}'_0$ telle que t_φ applique Δ' sur Δ . Si l'on pose $\alpha' = t_\varphi \alpha$ on peut trouver des $E'_{\alpha'} \in \mathfrak{g}'^{\alpha'}$ vérifiant les conditions (1) à (4) avec les constantes

de structure $N_{\alpha', \beta'} = N_{\alpha, \beta}$ autrement dit

$$(9) \quad [E'_{\alpha'}, E'_{\beta'}] = N_{\alpha, \beta} E'_{\alpha' + \beta'}$$

Tout d'abord $\Psi = {}^t\varphi$ est une isométrie de $\mathfrak{h}_0^*$ sur $\mathfrak{h}_0^*$. En effet d'après la proposition 1 de l'Exposé précédent on a

$-2 \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} = p + q$ si la α -série qui contient β se compose des $\beta + k\alpha$ pour $p \leq k \leq q$. Puisque Ψ est un isomorphisme linéaire de Δ' sur Δ on a $p = p'$ $q = q'$ donc $-2 \frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} = -2 \frac{\langle \beta', \alpha' \rangle}{\langle \alpha', \alpha' \rangle}$ d'où l'on déduit facilement que

$$(10) \quad \langle \alpha, \beta \rangle = k \langle \alpha', \beta' \rangle$$

où k ne dépend pas de α et de β . Mais on a

$$(11) \quad \langle \alpha, \beta \rangle = \langle H'_{\alpha}, H'_{\beta} \rangle = \sum_{\gamma} \gamma(H'_{\alpha}) \gamma(H'_{\beta}) = \sum_{\gamma} \langle \gamma \alpha \rangle \langle \gamma \beta \rangle$$

et de même $\langle \alpha', \beta' \rangle = \sum_{\gamma'} \langle \gamma' \alpha' \rangle \langle \gamma' \beta' \rangle$. Donc $k = k^2$ et comme

$\langle \alpha, \alpha \rangle \neq 0$ si $\alpha \neq 0$ $k = 1$, ce qui démontre notre assertion.

Munissons maintenant $\mathfrak{h}_0^*$ d'un ordre lexicographique comme dans l'Exposé précédent et appelons Σ_p l'ensemble des racines $\alpha \neq 0$ avec $-\rho < \alpha < \rho$. Supposons choisis des $E'_{\alpha} \in \mathfrak{g}_{\alpha'}$ pour $\alpha \in \Sigma_p$ vérifiant la relation (9) chaque fois que $\alpha, \beta, \alpha + \beta \in \Sigma_p$. On peut de plus choisir E'_{ρ} de sorte que la relation (9) soit vérifiée pour une décomposition $\alpha + \beta = \rho$ car

$[E'_{\alpha}, E'_{\beta}] \neq 0$ et définissons $E'_{-\rho}$ de sorte que $\langle E'_{\rho}, E'_{-\rho} \rangle = -1$. Si σ est le successeur immédiat de ρ $\Sigma_{\sigma} = \Sigma_p \cup \{\rho, -\rho\}$ et E'_{γ} est donc défini pour $\gamma \in \Sigma_{\sigma}$. Posons $[E'_{\gamma}, E'_{\delta}] = N'_{\gamma, \delta} E'_{\gamma + \delta}$ chaque fois que $\gamma, \delta, \gamma + \delta \in \Sigma_{\sigma}$. Il faut donc montrer que $N_{\gamma, \delta} = N'_{\gamma, \delta}$ dans ces conditions. Il faut distinguer plusieurs cas :

a) $\gamma, \delta, \gamma + \delta \in \Sigma_p$ alors $N_{\gamma, \delta} = N'_{\gamma, \delta}$ par hypothèse de récurrence

b) $\gamma + \delta = \rho$ $\gamma, \delta \in \Sigma_p$. On peut supposer cette décomposition distincte de $\alpha + \beta = \rho$. Alors $\alpha + \beta + (-\gamma) + (-\delta) = 0$ et les sommes deux à deux de ces racines sont non nulles et dans Σ_p car on a par exemple $0 < \alpha < \rho$ $0 < \gamma < \rho$ donc $\alpha - \gamma \in \Sigma_p$. On peut donc appliquer le lemme 2 à $\mathfrak{g}$ et $\mathfrak{g}'$ d'où

$$(12) \quad N_{\alpha, \beta} N_{-\gamma, -\delta} = -N_{\beta, -\gamma} N_{\alpha, -\delta} - N_{-\gamma, \alpha} N_{\beta, -\delta}$$

$$(13) \quad N'_{\alpha', \beta'} N'_{-\gamma', -\delta'} = -N'_{\beta', -\gamma'} N'_{\alpha', -\delta'} - N'_{-\gamma', \alpha'} N'_{\beta', -\delta'}$$

Mais les second membres de ces égalités sont égaux car on a $\alpha, \gamma, \alpha - \gamma \in \Sigma_\rho$ par exemple, d'où $N_{-\gamma, \alpha} = N'_{-\gamma, \alpha}$. D'autre part par construction $N_{\alpha, \beta} = N'_{\alpha, \beta}$. Donc comme $N_{\alpha, \beta} \neq 0$ on a $N_{-\gamma, -\delta} = N'_{-\gamma, -\delta}$. Mais on a vu que t_φ est une isométrie donc $\langle \gamma, \gamma \rangle = \langle \gamma', \gamma' \rangle$ et d'après le lemme 3

$$N_{\gamma, \delta} N_{-\gamma, -\delta} = \frac{\langle \gamma, \gamma \rangle}{2} q(1-p) = N'_{\gamma, \delta} N'_{-\gamma, -\delta}$$

donc finalement $N_{\gamma, \delta} = N'_{\gamma, \delta}$.

Donc si $\gamma + \delta = \rho$ on a $N_{\gamma, \delta} = N'_{\gamma, \delta}$ et $N_{-\gamma, -\delta} = N'_{-\gamma, -\delta}$.

c) $\gamma + \delta = -\rho$ $\gamma, \delta \in \Sigma_\rho$ donc $-\gamma, -\delta \in \Sigma_\rho$ $(-\gamma) + (-\delta) = \rho$ par suite $W_{\gamma, \delta} = W'_{\gamma, \delta}$ d'après b).

d) Enfin des 3 racines $\gamma, \delta, -(\gamma + \delta)$ dont la somme est nulle, une au plus peut être égale à $\pm \rho$ si elles sont toutes trois dans Σ_ρ . Mais alors ces cas se ramènent à b) et c) d'après le lemme 1.

Les racines positives étant en nombre fini le théorème est démontré par récurrence.

Corollaire 1 : Soit $L \subset K$ un sous-corps contenant les $N_{\alpha, \beta}$ et $\mathfrak{g}_L$ l'algèbre de Lie formée des combinaisons linéaires à coefficients dans L des E_α et H'_α . Il existe alors une application f L -linéaire de $\mathfrak{g}_L$ dans $\mathfrak{g}'$ prolongeant φ et qui soit un homomorphisme $f([x, y]) = [f(x), f(y)]$ ($x, y \in \mathfrak{g}_L$).

Les relations de structure (1) à (4) montrent tout de suite que $\mathfrak{g}_L$ est stable pour le crochet; $\mathfrak{g}$ étant somme directe des $\mathfrak{g}^\alpha$ et de $\mathfrak{h}$ et $\mathfrak{h}$ ayant même dimension sur K que $\mathfrak{h}_0$ sur $\mathbb{Q}$, f est bien définie par $f(H) = \varphi(H)$ $f(E_\alpha) = E'_\alpha$. Reste à montrer que f est multiplicative $\boxed{(H \in \mathfrak{h}_0)}$

$$(14) \quad f([H, H']) = f(0) = 0 \quad [f(H), f(H')] = 0 \quad \text{car } \mathfrak{h}' \text{ est abélienne}$$

$$(15) \quad f([H, E_\alpha]) = f(\alpha(H) E_\alpha) = \alpha(H) E'_\alpha = \alpha'(\varphi(H)) E'_\alpha = [\varphi(H), E'_\alpha] \\ = [f(H), f(E_\alpha)]$$

$$(16) \quad f([E_\alpha, E_\beta]) = f(N_{\alpha, \beta} E_{\alpha+\beta}) = N_{\alpha, \beta} E'_{\alpha+\beta} = [E'_\alpha, E'_\beta] = [f(E_\alpha), f(E_\beta)]$$

pour $H \in \mathfrak{h}_0$ $\alpha \in \Delta$.

Corollaire 2 : $\mathfrak{g}$ est définie à un isomorphisme près par la donnée de $\mathfrak{h}$ et du système des racines.

En effet si on prend $L = K$ dans le corollaire 1, on définit un isomorphisme de $\mathfrak{g}$ dans $\mathfrak{g}'$ prolongeant φ .

Corollaire 3 : on peut normer les E_α de façon à vérifier les relations (1) à (4) ainsi que (17) $N_{\alpha,\beta} = N_{-\alpha,-\beta}$.

$-\alpha$ est racine en même temps que α , donc la symétrie $H \rightarrow -H$ de $\mathfrak{h}_0$ laisse invariant le système des racines $\alpha' = -\alpha$. D'après le corollaire 1, il existe un automorphisme φ de $\mathfrak{g}$ prolongeant cette symétrie. Choisissons $F_\alpha \in \mathfrak{g}^\alpha$ de sorte que $\langle F_\alpha, F_{-\alpha} \rangle = -1$; φ transforme F_α en $F'_{-\alpha} \in \mathfrak{g}^{-\alpha}$. Donc $F'_{-\alpha} = \rho_\alpha F_{-\alpha}$. Mais d'après le théorème 1, on a

$\langle F'_{-\alpha}, F'_\alpha \rangle = -1$ donc $\rho_\alpha \rho_{-\alpha} = 1$. Posons $E_\alpha = \rho_\alpha^{-\frac{1}{2}} F_\alpha$; alors $f(E_\alpha) = \rho_\alpha^{-\frac{1}{2}} \rho_\alpha F_{-\alpha} = \rho_\alpha^{\frac{1}{2}} F_{-\alpha} = \rho_{-\alpha}^{-\frac{1}{2}} F_{-\alpha} = E_{-\alpha}$. Si l'on exprime maintenant que f est un homomorphisme on trouve de suite $N_{\alpha,\beta} = N_{\alpha',\beta'} = N_{-\alpha,-\beta}$.

Remarquons qu'en vertu du lemme 3 $N_{\alpha,\beta}^2 = \frac{1}{2} \langle \alpha, \alpha \rangle q(1-p) \geq 0$ car $q \geq 0$ $p \leq 0$ donc si K est le corps des complexes $N_{\alpha,\beta}$ est réel.

Définition 1 : une base de $\mathfrak{g}$ formée d'une base $H_1 \dots H_r$ de $\mathfrak{h}_0$ et de $E_\alpha \in \mathfrak{g}^\alpha$ tels que $N_{\alpha,\beta} = N_{-\alpha,-\beta}$ (en plus des relations (1) à (4)) s'appelle une base de Weyl de $\mathfrak{g}$.

2.- Formes réelles des algèbres de Lie.

K sera jusqu'à la fin de cet exposé le corps $\mathbb{C}$ des complexes. R désigne le corps des réels. $\mathfrak{g}$ étant espace vectoriel sur $\mathbb{C}$ est aussi espace vectoriel sur R par restriction des scalaires.

Définition 2.- Une sous-algèbre de Lie réelle $\mathfrak{g}_0$ de $\mathfrak{g}$ (considérée comme algèbre sur R) est dite forme réelle de $\mathfrak{g}$ si l'application canonique de la complexifiée $\mathfrak{g}_0 \otimes_R \mathbb{C}$ de $\mathfrak{g}_0$ dans $\mathfrak{g}$ est un isomorphisme, autrement dit, si $\dim_R \mathfrak{g}_0 = \dim_{\mathbb{C}} \mathfrak{g}$.

Tout élément de $\mathfrak{g}$ est donc de manière unique de la forme $x + iy$ avec $x, y \in \mathfrak{g}_0$. Dans $\mathfrak{g}_0 \otimes \mathbb{C}$ existe une involution σ définie par $\sigma(x \otimes \lambda) = x \otimes \bar{\lambda}$, donc une forme réelle $\mathfrak{g}_0$ de $\mathfrak{g}$ définit une involution σ de $\mathfrak{g}$ (par l'isomorphisme de $\mathfrak{g}_0 \otimes \mathbb{C}$ sur $\mathfrak{g}$) qui a les propriétés suivantes

$$\sigma(\sigma(x)) = x \quad \sigma(x+y) = \sigma(x) + \sigma(y) \quad \sigma(\lambda x) = \bar{\lambda} \sigma(x)$$

$$\sigma([x, y]) = [\sigma(x), \sigma(y)]$$

Réciproquement : soit σ une telle involution sur $\mathfrak{g}$ et $\mathfrak{g}_0$ l'ensemble des points fixes de σ : $x \in \mathfrak{g}_0$ équivaut à $x = \sigma(x)$. Alors si $x, y \in \mathfrak{g}_0$ $\lambda \in R$ il résulte des propriétés de σ que $x+y$, λx , $[x, y] \in \mathfrak{g}_0$. D'autre part tout $x \in \mathfrak{g}_0$ s'écrit d'une manière et d'une seule sous la forme $y + iz$ avec $y, z \in \mathfrak{g}_0$. En effet $x = \frac{1}{2}(x + \sigma(x)) + i(\frac{1}{2i}(x - \sigma(x)))$ et il est immédiat

que $\frac{1}{2}(x + \sigma(x))$ et $\frac{1}{2i}(x - \sigma(x))$ sont dans $\mathfrak{g}_0$. Réciproquement si $x = y + iz$ $\sigma(x) = y - iz$ donc $y = \frac{1}{2}(x + \sigma(x))$ $z = \frac{1}{2i}(x - \sigma(x))$. Donc $\mathfrak{g}_0$ est une forme réelle de $\mathfrak{g}$.

La forme de Killing de $\mathfrak{g}_0$ s'obtient par restriction de celle de $\mathfrak{g}$, car adx ady est un endomorphisme complexe de $\mathfrak{g}$ qui conserve $\mathfrak{g}_0$ donc a même trace considéré comme opérateur de $\mathfrak{g}_0$ ou de $\mathfrak{g}$ (ceci si $x, y \in \mathfrak{g}_0$). Donc B prend des valeurs réelles sur $\mathfrak{g}_0$ et donc $B(x, y) = \overline{B(\sigma(x), \sigma(y))}$ pour $x, y \in \mathfrak{g}_0$. Mais les deux membres de cette égalité sont des formes bilinéaires complexes sur $\mathfrak{g}$ égales sur $\mathfrak{g}_0$ donc sur $\mathfrak{g}$.

Définition 3.- Une algèbre de Lie réelle est dite compacte si la forme quadratique $B(x, x)$ est définie négative. Une forme réelle $\mathfrak{g}_0$ de l'algèbre de Lie complexe $\mathfrak{g}$ s'appelle forme réelle compacte de $\mathfrak{g}$ si $\mathfrak{g}_0$ est une algèbre de Lie réelle compacte.

Pour que $\mathfrak{g}_0$ soit une forme réelle compacte de $\mathfrak{g}$, il faut et il suffit que la forme hermitienne $B(x, \sigma(y))$ sur $\mathfrak{g}$ soit définie négative. En effet si $\mathfrak{g}_0$ est compacte et $x = y + iz \in \mathfrak{g}$ $x \neq 0$ $B(x, \sigma(x)) = B(y + iz, y - iz) = B(y, y) + B(z, z) < 0$. Réciproquement si $B(x, \sigma(y))$ est définie négative et $x \in \mathfrak{g}_0$ $x \neq 0$ on a $x = \sigma(x)$ donc $B(x, x) < 0$.

Etudions maintenant les involutions sur $\mathfrak{g}$.

Lemme 4.- 1) Pour qu'un sous-espace complexe $\mathfrak{v}$ de $\mathfrak{g}$ soit engendré (sur $\mathbb{C}$) par $\mathfrak{v}_0 = \mathfrak{v} \cap \mathfrak{g}_0$, il faut et il suffit que $\sigma(\mathfrak{v}) = \mathfrak{v}$.

2) Si deux involutions σ et τ commutent, $\mathfrak{g}_u$ désignant les points fixes de τ , $\mathfrak{g}_0$ est somme directe de $\mathfrak{g}_u^+$ et $i\mathfrak{g}_u^-$ et $\mathfrak{g}_u$ est somme directe de $\mathfrak{g}_u^+$ et $\mathfrak{g}_u^-$ (où $x \in \mathfrak{g}_u^\pm$ signifie $x \in \mathfrak{g}_u$ et $\sigma(x) = \pm x$).

1) Soit $\mathfrak{v}$ engendré par $\mathfrak{v}_0$ donc si $x \in \mathfrak{v}$ $x = y + iz$ $y, z \in \mathfrak{v}_0$. Alors $\sigma(x) = y - iz \in \mathfrak{v}$ donc $\sigma(\mathfrak{v}) \subset \mathfrak{v}$ et il y a égalité car $\sigma^2 = 1$. Réciproquement si $\sigma(\mathfrak{v}) \subset \mathfrak{v}$ et $x \in \mathfrak{v}$ on a $y = \frac{1}{2}(x + \sigma(x)) \in \mathfrak{v} \cap \mathfrak{g}_0 = \mathfrak{v}_0$ et $z = \frac{1}{2i}(x - \sigma(x)) \in \mathfrak{v} \cap \mathfrak{g}_0 = \mathfrak{v}_0$. Comme $x = y + iz$ $\mathfrak{v}$ est engendré par $\mathfrak{v}_0$.

2) Puisque σ commute à τ , σ conserve $\mathfrak{g}_u$ car si $x \in \mathfrak{g}_u$ $\tau \sigma(x) = \sigma \tau(x) = \sigma(x)$ donc $\sigma(x) \in \mathfrak{g}_u$. σ induit un opérateur $\mathbb{R}$ -linéaire de $\mathfrak{g}_u$ dont le carré est 1. $\mathfrak{g}_u^+ \cap \mathfrak{g}_u^- = 0$ car si $x \in \mathfrak{g}_u^+ \cap \mathfrak{g}_u^-$ $x = \sigma(x) = -x$ donc $x = -x$, $x = 0$. De plus $x = \frac{1}{2}(x + \sigma(x)) + \frac{1}{2}(x - \sigma(x))$ et il est clair que $\frac{1}{2}(x \pm \sigma(x)) \in \mathfrak{g}_u^\pm$ car $\sigma(x) \in \mathfrak{g}_u$; donc $\mathfrak{g}_u = \mathfrak{g}_u^+ + \mathfrak{g}_u^-$.

$\mathfrak{g}$ est somme directe de $\mathfrak{g}_u$ et $i\mathfrak{g}_u$ donc de $\mathfrak{g}_u^+ \mathfrak{g}_u^- i\mathfrak{g}_u^+ i\mathfrak{g}_u^-$. Or σ est l'identité sur $\mathfrak{g}_u^+$ et $i\mathfrak{g}_u^-$ et il vaut -1 sur $\mathfrak{g}_u^-$ et $i\mathfrak{g}_u^+$ donc $\mathfrak{g}_0$ est somme directe de $\mathfrak{g}_u^+$ et $i\mathfrak{g}_u^-$.

Théorème 2.- Soit $\mathfrak{g}_0$ une forme réelle de $\mathfrak{g}$, σ l'involution associée

- 1) il existe une sous-algèbre de Cartan $\mathfrak{h}$ invariante par σ . σ conserve même $\mathfrak{h}_0$ (sous-espace $\mathbb{Q}$ -vectoriel engendré par les H'_α) et ${}^t\sigma$ permute les racines.
- 2) si $\mathfrak{g}_0$ est compacte, alors $\sigma(H) = -H$ pour $H \in \mathfrak{h}_0$ et il existe une base de Weyl E_α de $\mathfrak{g}$ telle que $\sigma(E_\alpha) = E_{-\alpha}$.
- 3) réciroquement étant donnée une base de Weyl de $\mathfrak{g}$, la forme réelle associée à l'involution donnée par $\sigma(H) = -H$ ($H \in \mathfrak{h}_0$) $\sigma(E_\alpha) = E_{-\alpha}$ est une forme réelle compacte.

1) La dimension du sous-espace de $\mathfrak{g}$ annulé par une puissance de adx est égale à la multiplicité de 0 comme racine du polynôme caractéristique $\det(\text{adx} - \lambda.1) = (-\lambda)^n + (-\lambda)^{n-1}\varphi_1(x) + \dots + (-\lambda)^{n-k}\varphi_k(x)$. Pour que x soit régulier, c'est-à-dire que cette dimension soit minima, il faut et il suffit que $\varphi_k(x) \neq 0$.

Comme $\varphi_k(x)$ est une fonction polynôme non nulle sur $\mathfrak{g}$ et donc sur $\mathfrak{g}_0$ il existe un $x \in \mathfrak{g}_0$ qui n'annule pas φ_k , donc $\mathfrak{g}_0$ contient un élément régulier x . D'après l'Exposé n° 9, comme $\mathfrak{g}$ est semi-simple, l'ensemble $\mathfrak{h}$ des éléments qui commutent à x est une sous-algèbre de Cartan. Mais si $H \in \mathfrak{h}$ $[\sigma.H, x] = \sigma([H, \sigma(x)]) = \sigma([H, x]) = 0$ donc $\sigma.H \in \mathfrak{h}$ et $\mathfrak{h}$ est bien invariante par σ . Définissons pour toute racine α suivant $\mathfrak{h}$ une forme linéaire $\bar{\alpha}$ sur $\mathfrak{h}$ par $\bar{\alpha}(H) = \overline{\alpha(\sigma H)}$. On va montrer que $\bar{\alpha}$ est une racine et que $\sigma.\mathfrak{g}_\alpha \subset \mathfrak{g}_{\bar{\alpha}}$. En effet si $y \in \mathfrak{g}_\alpha$ $[H, y] = \alpha(H)y$ donc $[\sigma.H, \sigma(y)] = \overline{\alpha(H)}\sigma(y) = \bar{\alpha}(\sigma H)\sigma(y)$ donc $\sigma(y) \in \mathfrak{g}_{\bar{\alpha}}$ car $\sigma.\mathfrak{h} = \mathfrak{h}$. De plus $\langle \sigma.H'_\alpha, H \rangle = \overline{\langle H'_\alpha, \sigma.H \rangle} = \overline{\alpha(\sigma.H)} = \bar{\alpha}(H) = \langle H'_\alpha, H \rangle$ donc $\sigma.H'_\alpha = H'_{\bar{\alpha}}$. Il en résulte que σ conserve $\mathfrak{h}_0$. Soient choisis des $E_\alpha \in \mathfrak{g}^\alpha$ tels que $\langle E_\alpha, E_{-\alpha} \rangle = -1$ alors comme $\sigma.E_\alpha \in \mathfrak{g}_{\bar{\alpha}}$, il existe des scalaires ρ_α avec $\sigma.E_\alpha = \rho_\alpha E_{\bar{\alpha}}$.

L'involution σ est bien définie par la permutation des racines qu'elle induit et par les ρ_α . Réciproquement supposons nous donné un automorphisme φ (avec $\varphi^2 = 1$) de $\mathfrak{h}_0$ tel que ${}^t\varphi$ permute les racines et des scalaires ρ_α .

A quelles conditions existe-t-il une involution σ qui coïncide avec φ sur $\mathfrak{h}_0$ et telle que $\sigma.E_\alpha = \rho_\alpha E_{-\alpha}$?

a) $\sigma^2.H = \varphi^2.H = H$ pour $H \in \mathfrak{h}_0$

$$\sigma^2 E_\alpha = \sigma(\rho_\alpha E_{-\alpha}) = \overline{\rho_\alpha} \rho_{-\alpha} E_{-\alpha}$$

donc $\sigma^2 = 1$ équivaut à

$$(18) \quad \overline{\rho_\alpha} \rho_{-\alpha} = 1.$$

b) il existe bien une application et une seule semi-linéaire σ telle que $\sigma.H = \varphi.H$ $\sigma E_\alpha = \rho_\alpha E_{-\alpha}$ car $\dim_{\mathbb{C}} \mathfrak{h} = \dim_{\mathbb{R}} \mathfrak{h}_0$ et que $\mathfrak{h}$ et les E_α sont linéairement indépendants. Que σ soit multiplicatif se traduit par $\sigma([E_\alpha, E_{-\alpha}]) = (\sigma E_\alpha, \sigma E_{-\alpha})$ $(\sigma H, \sigma E_\alpha) = \sigma([H, E_\alpha])$ $\sigma([E_\alpha, E_\beta]) = [\sigma E_\alpha, \sigma E_\beta]$, σ étant évidemment un homomorphisme sur l'algèbre abélienne $\mathfrak{h}$. Or ${}^t\sigma$ permutant les racines conserve la métrique (cf. démonstration du théorème 1) soit $\langle {}^t\sigma \bar{\alpha}, {}^t\sigma \beta \rangle = \langle \bar{\alpha}, \beta \rangle$ ou $\sigma.H'_\alpha = H'_{-\alpha}$ donc la 1ère égalité à démontrer équivaut à $-H'_{-\alpha} = [\rho_\alpha E_{-\alpha}, \rho_{-\alpha} E_{-\alpha}]$ soit $-H'_{-\alpha} = -\rho_\alpha \rho_{-\alpha} H'_{-\alpha}$ ou encore à

$$(19) \quad \rho_\alpha \rho_{-\alpha} = 1$$

La 2e s'écrit $\rho_\alpha \bar{\alpha}(\sigma.H)E_{-\alpha} = \overline{\alpha(H)}\sigma.E_\alpha$ et n'est que la traduction de la définition de $\bar{\alpha}$. La 3e s'écrit enfin

$$(20) \quad \overline{N_{\alpha,\beta}} \rho_{\alpha+\beta} E_{-\alpha-\beta} = \rho_\alpha \rho_\beta \overline{N_{-\alpha,-\beta}} E_{-\alpha-\beta} \quad \text{c'est-à-dire}$$

$$\rho_{\alpha+\beta} \overline{N_{\alpha,\beta}} = \rho_\alpha \rho_\beta \overline{N_{-\alpha,-\beta}}$$

2) Supposons $\mathfrak{g}_0$ compacte, c'est-à-dire $B(x, \sigma(x)) < 0$ pour $x \neq 0$. σ induit un opérateur $\mathbb{Q}$ -linéaire dans $\mathfrak{h}_0$ et $\sigma^2 = 1$ donc $\mathfrak{h}_0$ est somme directe de V^+ et V^- avec $\sigma.H = \pm H$ pour $H \in V^\pm$. Mais si $H \in V^+$

$B(H, \sigma.H) = \langle H, H \rangle \geq 0$ ce qui, comme la forme hermitienne est définie négative, implique $H = 0$ donc $V^+ = 0$ $\mathfrak{h}_0 = V^-$. Donc $\bar{\alpha} = -\alpha$; prenons une base de

Weyl E_α , $N_{\alpha,\beta} = \overline{N_{\alpha,\beta}} = \overline{N_{-\alpha,-\beta}}$. Si l'on pose $\sigma.E_\alpha = \rho_\alpha E_{-\alpha}$ on aura donc $\overline{\rho_\alpha} \rho_{-\alpha} = \rho_\alpha \rho_{-\alpha}^{-1}$ $\rho_{\alpha+\beta} = \rho_\alpha \rho_\beta$. De plus $\langle E_\alpha, \sigma.E_\alpha \rangle = \rho_\alpha \langle E_\alpha, E_{-\alpha} \rangle = -\rho_\alpha < 0$ donc $\rho_\alpha > 0$. $\rho_\alpha^{-\frac{1}{2}} = \rho_\alpha$ est donc défini sans ambiguïté et est réel et si l'on pose $E'_\alpha = \rho_\alpha^{-\frac{1}{2}} E_\alpha$, on a $\langle E'_\alpha, E'_{-\alpha} \rangle = -\rho_\alpha^{-\frac{1}{2}} \rho_{-\alpha}^{-\frac{1}{2}} = -1$ et

$\sigma.E'_\alpha = \rho_\alpha^{-\frac{1}{2}} \rho_\alpha E_{-\alpha} = \rho_\alpha^{\frac{1}{2}} E_{-\alpha} = \rho_{-\alpha}^{-\frac{1}{2}} E_{-\alpha} = E'_{-\alpha}$. σ étant un homomorphisme il résulte de là que si $[E'_\alpha, E'_\beta] = N'_{\alpha,\beta} E'_{\alpha+\beta}$ on a $N'_{\alpha,\beta} = \overline{N'_{-\alpha,-\beta}}$ donc que E'_α est une base de Weyl de $\mathfrak{g}$.

3) Réciproquement si l'on pose $\bar{\alpha} = -\alpha$ $\rho_\alpha = 1$ les conditions (18) à (20) sont vérifiées car E_α est une base de Weyl et donc $N_{\alpha, \beta} = N_{-\alpha-\beta}$ est réel. Reste à démontrer $B(x, \sigma(x)) < 0$. Or soit $x = H + \sum_{\alpha} \mu_{\alpha} E_{\alpha}$ $\sigma(x) = \sigma(H) + \sum_{\alpha} \overline{\mu_{\alpha}} E_{-\alpha}$ donc

$$\begin{aligned} B(x, \sigma(x)) &= \langle H, \sigma(H) \rangle + \sum_{\alpha} \mu_{\alpha} \overline{\mu_{\alpha}} \langle E_{\alpha}, E_{-\alpha} \rangle \\ &= \sum_{\alpha} (\alpha(H) \alpha(\sigma(H)) - \mu_{\alpha} \overline{\mu_{\alpha}}) \end{aligned}$$

or

$$\alpha(\sigma(H)) = \bar{\alpha}(H) = -\alpha(H) \quad \text{donc}$$

$$(21) \quad B(x, \sigma(x)) = - \sum_{\alpha} (|\alpha(H)|^2 + |\mu_{\alpha}|^2) < 0 \quad . \quad \text{C.Q.F.D.}$$

Remarques : 1) $\mathfrak{g}_R$ ensemble des combinaisons linéaires à coefficients réels des E_{α} et des H'_{α} est appelée la forme réelle normale associée à la base de Weyl. La forme compacte associée à σ ($\sigma E_{\alpha} = E_{-\alpha}$ $\sigma.H = -H$) est appelée la forme compacte associée à la base de Weyl ; elle a une base sur R formée des iH'_{α_i} , $E_{\alpha} + E_{-\alpha}$ $i(E_{\alpha} - E_{-\alpha})$.

2) on appelle sous-algèbre de Cartan de l'algèbre réelle $\mathfrak{g}_0$ une sous-algèbre $\mathfrak{h}^0 \subset \mathfrak{g}_0$ dont la complexifiée $\mathfrak{h}$ est une sous-algèbre de Cartan de $\mathfrak{g}$. On montre facilement qu'une telle sous-algèbre est caractérisée par les propriétés suivantes :

- $\mathfrak{h}^0$ est une sous-algèbre abélienne maximale de $\mathfrak{g}_0$;
- la représentation adjointe de $\mathfrak{h}^0$ dans $\mathfrak{g}_0$ est complètement réductible.

Maintenant que nous avons déterminé les formes compactes de $\mathfrak{g}$, nous pouvons passer aux autres formes réelles de $\mathfrak{g}$.

Théorème 3. - (E. Cartan, Mostow, Iwasawa). Soit $\mathfrak{g}$ une algèbre de Lie semi-simple complexe, $\mathfrak{g}_0$ une forme réelle de $\mathfrak{g}$ et σ l'involution associée.

- $\mathfrak{g}$ possède une forme réelle compacte $\mathfrak{g}_u$ invariante par σ .
- $\mathcal{P}_0 = \mathfrak{g}_0 \cap \mathfrak{g}_u = \mathfrak{g}_u^+$ est l'ensemble des points fixes d'un automorphisme involutif de $\mathfrak{g}_u$. $\mathfrak{g}_0$ est somme directe de $\mathcal{P}_0$ et de $\mathcal{Y}_0 = i \mathfrak{g}_u^-$ tandis que $\mathfrak{g}_u$ est somme directe de $\mathcal{P}_0$ et $i \mathcal{Y}_0$.
- $\mathfrak{g}_0$ est somme directe de $\mathcal{P}_0$ et d'une sous-algèbre résoluble $\mathfrak{l}_0$.

D'après le lemme 4, il suffira de démontrer qu'il existe une involution τ commutant à σ telle que $B(x, \tau(x)) < 0$ pour $x \neq 0$. $\mathfrak{g}_u$ sera l'ensemble des points fixes de τ . D'après le théorème 2, il existe une sous-algèbre de Cartan $\mathfrak{h}$ invariante par σ et une base de Weyl de $\mathfrak{g}$ avec $\sigma.E_{\alpha} = \rho_{\alpha} E_{\bar{\alpha}}$. Posons $\tau E_{\alpha} = |\rho_{\alpha}| E_{-\alpha}$. Il suffit de vérifier les relations (18) à (20) pour

$\bar{\alpha} = -\alpha$ et $|p_\alpha|$. Les 2 premières sont évidentes et comme $N_{\alpha,\beta} = N_{-\alpha,-\beta}$ la 3e équivaut à $|p_{\alpha+\beta}| = |p_\alpha| |p_\beta|$. Or on sait que $\langle \bar{\alpha}, \bar{\beta} \rangle = \langle \alpha, \beta \rangle = \langle \alpha, \beta \rangle$ et en vertu du lemme 3 $|N_{\alpha,\beta}^2| = \frac{1}{2} \langle \alpha, \alpha \rangle q(1-p) = |N_{\alpha,\beta}^2|$. Prenons le module de la relation (20) on a bien $|p_{\alpha+\beta}| = |p_\alpha| |p_\beta|$. Enfin σ et τ commutent sur $\mathfrak{h}_0$ et

$$\sigma \tau E_\alpha = |p_\alpha| \sigma \cdot E_{-\alpha} = |p_\alpha| p_{-\alpha} E_{-\alpha} = \frac{|p_\alpha|}{p_\alpha} E_{-\alpha}$$

$$\tau \sigma E_\alpha = \tau (p_\alpha E_{-\alpha}) = \overline{p_\alpha} |p_{-\alpha}| E_{-\alpha} = \frac{\overline{p_\alpha}}{|p_\alpha|} E_{-\alpha}$$

donc $\sigma \tau = \tau \sigma$.

Pour démontrer le 3) de ce théorème, il nous faut tout d'abord modifier le choix de la sous-algèbre de Cartan que nous persisterons cependant à appeler $\mathfrak{h}$. On sait que $\mathfrak{g}_u = \mathfrak{g}_u^+ \oplus \mathfrak{g}_u^-$. Soit $\mathfrak{h}_u^-$ une sous-algèbre abélienne maximale contenue dans $\mathfrak{g}_u^-$ et soit $\mathfrak{h}_u$ une sous-algèbre abélienne maximale de $\mathfrak{g}_u$ contenant $\mathfrak{h}_u^-$. $\mathfrak{h}_u$ est une sous-algèbre de Cartan, car les $\text{ad} H$ pour $H \in \mathfrak{h}_u$ sont antisymétriques par rapport à la forme quadratique définie positive $-B(x, x)$ sur $\mathfrak{g}_u$, donc $\text{ad} \mathfrak{h}_u$ est complètement réductible. Tout d'abord montrons que $\mathfrak{h}_u$ est stable pour σ or si $H \in \mathfrak{h}_u$ $H^- \in \mathfrak{h}_u^-$ $[H, H^-] = 0$ donc $[\sigma H, \sigma H^-] = 0$ or $\sigma H^- = -H^-$, donc σH commute à $\mathfrak{h}_u^-$ et il en est de même de $H - \sigma H \in \mathfrak{g}_u^-$. Mais $\mathfrak{h}_u^-$ est abélienne maximale dans $\mathfrak{g}_u^-$ donc $H - \sigma H \in \mathfrak{h}_u^-$ $\sigma H \in \mathfrak{h}_u$. Donc $\mathfrak{h}_u = \mathfrak{h}_u^+ + \mathfrak{h}_u^-$ et si $\mathfrak{h}$ est la complexifiée de $\mathfrak{h}_u$ il résulte du lemme 4 que $\mathfrak{h}^0 = \mathfrak{h} \cap \mathfrak{g}_0 = \mathfrak{h}_u^+ \oplus i \mathfrak{h}_u^-$.

Le sous-espace $\mathfrak{h}_0$ formé des combinaisons linéaires rationnelles des H_α' est stable par σ , donc $\mathfrak{h}_0 = V^+ \oplus V^-$ (cf. plus haut). Prenons une base ordonnée de $\mathfrak{h}_0$ formée d'une base de V^+ soit $H_1 \dots H_m$ précédant une base de V^- soit $K_1 \dots K_n$ et munissons $\mathfrak{h}_0^*$ de l'ordre lexicographique correspondant.

Pour qu'une racine α soit telle que $\bar{\alpha} = -\alpha$, il faut et il suffit que α soit nulle sur V^+ . En effet V^+ est sous-tendu sur $\mathbb{Q}$ par les $H + \sigma H$ ($H \in \mathfrak{h}_0$) et comme $\bar{\alpha}(H) = \alpha(\sigma H) = \alpha(\sigma H)$ (car α prend des valeurs rationnelles sur $\mathfrak{h}_0$), $\bar{\alpha} = -\alpha$ équivaut à $\alpha(H + \sigma H) = 0$ soit à α nulle sur V^+ . Supposons maintenant $\alpha > 0$ et $\bar{\alpha} \neq -\alpha$, α n'est pas nulle sur V^+ donc $\alpha(H_1) = \dots = \alpha(H_i) = 0$ $\alpha(H_{i+1}) \neq 0$ et même $\alpha(H_i) > 0$ puisque $\alpha > 0$. Mais $\bar{\alpha}(H_j) = \alpha(\sigma H_j) = \alpha(H_j)$ (car $H_j \in V^+$) est nul pour $j \leq i$ et $\bar{\alpha}(H_{i+1}) = \alpha(H_{i+1}) > 0$ donc $\bar{\alpha} > 0$. Le système des racines est donc partagé en trois

$$\Delta = \Sigma' \cup \Delta'' \cup (-\Sigma')$$

$$\alpha \in \Sigma' \iff \alpha, \bar{\alpha} > 0$$

$$\alpha \in \Delta'' \iff \alpha \text{ nulle sur } V^+ \text{ ou } \bar{\alpha} = -\alpha.$$

Lemme 5. - Si $\bar{\alpha} = -\alpha$ et $x \in \mathfrak{g}^\alpha$ $\sigma(x) = \tau(x)$ donc $x + \sigma(x) \in \mathfrak{g}_u^+ = \mathcal{P}_0$ en particulier $\sigma.E_\alpha = E_{-\alpha}$.

Comme $\bar{\alpha} = -\alpha$ $\sigma(x) \in \mathfrak{g}^{-\alpha}$ et $y = \sigma(x) - \tau(x) \in \mathfrak{g}^{-\alpha}$. Or y commute à V^+ car si $H \in V^+$ donc $H = \sigma.H$

$$[H, \sigma(x)] = \sigma([H, x]) = \overline{\alpha(H)} \sigma(x) = 0$$

$$[H, \sigma(x)] = -\tau([H, x]) = -\overline{\alpha(H)} \tau(x) = 0$$

car $\tau = -1$ sur $\mathfrak{h}_0$ (cf. théorème 2) et α est nulle sur V^+ . Mais $\mathfrak{h}_u$ est engendrée (sur R) par les iH'_α et $iV^+ \subset \mathfrak{h}_u^-$ $iV^- \subset \mathfrak{h}_u^+$ donc $\mathfrak{h}_u^-$ est engendrée sur R par iV^+ et y commute à $\mathfrak{h}_u^-$. Mais alors $y - \sigma(y) \in \mathfrak{g}_u^-$ commute à $\mathfrak{h}_u^-$ (car $\mathfrak{h}_u^-$ est invariante par σ) donc $y - \sigma(y) \in \mathfrak{h}_u^-$. Or $y \in \mathfrak{g}^{-\alpha}$ $\sigma.y \in \mathfrak{g}^\alpha$ et la somme de $\mathfrak{g}^\alpha$, $\mathfrak{g}^{-\alpha}$, $\mathfrak{h}_u^-$ est directe donc $y = \sigma(y) = 0$ enfin $x + \sigma(x) = x + \tau(x) \in \mathfrak{g}_0 \cap \mathfrak{g}_u = \mathcal{P}_0$.

Pour achever de démontrer le théorème posons $\mathcal{U} = \sum_{\alpha \in \Sigma'} \mathfrak{g}^\alpha$ $\mathcal{U}' = \sum_{\alpha \in \Sigma'} \mathfrak{g}^{-\alpha}$. Si $\alpha \in \Sigma'$ $\bar{\alpha} \in \Sigma'$ car $\bar{\alpha}, \bar{\bar{\alpha}} = \alpha > 0$ donc $\mathcal{U}$ et $\mathcal{U}'$ sont stables pour σ . D'autre part $\tau(\mathcal{U}) \subset \mathcal{U}'$ $\mathcal{U}$ étant stable par σ est engendré sur C par $\mathcal{U}_0 = \mathcal{U} \cap \mathfrak{g}_0$. J'affirme que

$$(22) \quad \mathfrak{g}_0 = \mathcal{P}_0 \oplus i \mathfrak{h}_u^- \oplus \mathcal{U}_0$$

Tout d'abord cette somme est directe car si $k + h + n = 0$ en appliquant τ on trouve $k - h + \tau(n) = 0$ d'où $2h + n - \tau(n) = 0$. Mais $h \in \mathfrak{h}$ $n \in \mathcal{U}$ $\tau(n) \in \mathcal{U}'$ et la somme de $\mathfrak{h}$, $\mathcal{U}$, $\mathcal{U}'$ est directe donc $h = n = 0$ et donc $k = 0$.

De plus $\mathfrak{g}_0$ est engendré sur R par $\mathfrak{h} \cap \mathfrak{g}_0 = \mathfrak{h}_u^+ + i \mathfrak{h}_u^- \subset \mathcal{P}_0 + i \mathfrak{h}_u^-$ et par les $y = x + \sigma(x)$ pour $x \in \mathfrak{g}^\alpha$. Si $\bar{\alpha} = -\alpha$, $x + \sigma(x)$ est dans $\mathcal{P}_0$ d'après le lemme 5. Si $\alpha \in \Sigma'$ $y \in \mathfrak{g}^\alpha + \mathfrak{g}^{\bar{\alpha}} \subset \mathcal{U}$ et comme $y \in \mathfrak{g}_0$ $y \in \mathcal{U}_0$. D'autre part si $-\alpha \in \Sigma'$ on a $\tau(y) \in \mathfrak{g}^{-\alpha} + \mathfrak{g}^{-\bar{\alpha}} \subset \mathcal{U}$ et $y + \tau(y) \in \mathcal{P}_0$ donc y est dans $\mathcal{P}_0 + \mathcal{U}_0$. Donc si $\mathfrak{l}_0 = i \mathfrak{h}_u^- + \mathcal{U}_0$ $\mathfrak{g}_0 = \mathcal{P}_0 \oplus \mathfrak{l}_0$

C.Q.F.D.

APPENDICE

Indiquons sommairement comment on déduit du théorème 3 un théorème de décomposition pour les groupes de Lie. Soient G , G_0 , G_u les groupes adjoints

des algèbres de Lie (réelles) respectives $\mathfrak{g}$, $\mathfrak{g}_0$, $\mathfrak{g}_u$. Comme les automorphismes de $\mathfrak{g}_0$ et $\mathfrak{g}_u$ se prolongent par linéarité (sur $\mathbb{C}$) de manière unique en des automorphismes de $\mathfrak{g}$ et que G conserve la structure complexe de $\mathfrak{g}$, on peut considérer G_0 et G_u comme plongés dans G . On définit une involution σ dans G par $\text{ad } \sigma(g) = \sigma \circ \text{ad } g \circ \sigma^{-1}$ et de même pour τ . On montre alors sans mal que G_0 et G_u sont les points fixes de σ et τ respectivement dans G , donc sont fermés. Mais comme $\mathfrak{g}$ est semi-simple, donc que toute dérivation est intérieure il en résulte que G est la composante connexe du groupe des automorphismes de $\mathfrak{g}$, donc est fermé dans le groupe des opérateurs linéaires de $\mathfrak{g}$. Donc G_0 et G_u sont des groupes linéaires fermés et comme G_u conserve la forme hermitienne définie positive $-B(x, \tau(x))$ G_u est compact de même que $G_0 \cap G_u$. Soit K la composante de l'unité de $G_0 \cap G_u$. C'est un groupe compact dont l'algèbre de Lie est $\mathfrak{p}_0$. De même soit N le sous-groupe résoluble d'algèbre de Lie $\mathfrak{n}_0 + i\mathfrak{h}_u^-$.

Mais par rapport à une base de Weyl $E_{-\rho} \dots E_{-\alpha_1} H_1 \dots H_r E_{\alpha_1} \dots E_{\rho}$, les matrices de $\text{ad } \mathfrak{l}_0$ sont triangulaires et leur diagonale est réelle car $i\mathfrak{h}_u^-$ est engendré sur $\mathbb{R}$ par V^+ et que $\alpha(V^+) \in \mathbb{Q}$ pour toute racine α , et que $\text{ad } \mathfrak{n}_0$ se compose de matrices à diagonale nulle. Mais alors l'exponentielle définit un homéomorphisme de $\mathfrak{l}_0$ sur N qui est donc un groupe résoluble simplement connexe. $K \cap N$ est réduit à l'identité : en effet par rapport à la base de $\mathfrak{g}$ en question les matrices de K sont unitaires comme on le voit en explicitant $B(x, \sigma(x))$ (cf. (21)) et une matrice unitaire ne peut être triangulaire que si elle est diagonale, et une matrice diagonale unitaire ne peut être réelle et positive sans être égale à 1.

On va démontrer que $G = K.N$ c'est-à-dire que tout $g \in G$ s'écrit d'une manière et d'une seule sous la forme $g = k.n$ avec $k \in K$ $n \in N$. En effet, l'espace tangent en e à K s'identifie à $\mathfrak{p}_0$ de même l'espace tangent en e à N s'identifie à $\mathfrak{l}_0$ dans l'espace tangent en $(e, \mathbb{C})$ à $K \times N$ s'identifie à $\mathfrak{p}_0 \oplus \mathfrak{l}_0$. Or on voit facilement que l'application linéaire tangente à $(g, g') \rightarrow gg'$ de $G \times G \rightarrow G$ au point (e, e) est donnée par $(\alpha, \beta) \rightarrow \alpha + \beta$ donc par restriction l'application $(k, n) \rightarrow kn$ induit au point (e, e) l'application $(\alpha, \beta) \rightarrow \alpha + \beta$ de $\mathfrak{p}_0 \times \mathfrak{n}_0$ dans $\mathfrak{g}_0$. Celle-ci étant un isomorphisme, le théorème des fonctions implicites montre qu'il existe un voisinage U de e dans K , un voisinage V de e dans N tels que la restriction à $U \times V$ de l'application de $K \times N$ dans G soit un homéomorphisme. Il existe donc des voisinages $U_1 \subset U$ $V_1 \subset V$ et des fonctions continues k^0 et n^0 telles que

$$(23) \quad n.k = k^0(n,k) n^0(n,k) \quad n \in V_1 \quad k \in U_1$$

Soit $S = \{k_1 \dots k_p\}$ une suite d'éléments de U_1 . On va construire un voisinage $V(S) \subset V_1$ et des fonctions continues n^S et k^S telles que

$$(24) \quad n.k(S).k = k^S(n,k) n^S(n,k) \quad n \in V(S) \quad k \in U_1$$

avec $k(S) = k_1 \dots k_p$. On raisonne pour cela par récurrence sur p , cette formule se réduisant à (23) pour $p = 0$. Puis si $S' = \{k_0\} \cup S$ $k(S') = k_0 k(S)$ et

$$(25) \quad n.k(S').k = n.k_0.k(S).k = k^0(n,k_0) n^0(n,k_0) k(S).k$$

pour $n \in V_1$. Mais $n^0(e, k_0) = e$ d'après l'unicité de la décomposition (23) donc $n^0(n, k_0) \in V(S)$ pour $n \in V(S')$ (voisinage assez petit de e) d'après la continuité de n^0 . Mais alors

$$n.k(S').k = k^0(n, k_0) k^S(n^0(n, k_0), k) n^S(n^0(n, k_0), k)$$

Utilisons maintenant le fait que K est compact. Il existe un nombre fini de suites telles que $K \subset \bigcup_S k(S).U_1$, donc si $n \in \bigcap_S V(S) = V_2$ et $k \in K$ $n.k \in K.N \dots$

Soit maintenant une suite $T = \{n_1 \dots n_q\}$ d'éléments de V_2 et $n(T) = n_1 \dots n_q$. On va montrer que $n(T).k \in K.N$. C'est vrai si $q = 1$ puis si $T' = \{n_0\} \cup T$ $n(T') = n_0 n(T)$.

$n(T').k = n_0 n(T).k \in n_0 K.N$. Mais $n_0 K \subset K.N$ donc $n(T').k \in K.N$. N étant connexe est engendré par le voisinage V_2 de e donc finalement $N.K. = K.N$.

Il n'y a plus de difficulté à démontrer que $NK = KN = H$ est un sous-groupe de G , mais $K.N \supset U_1.V_1$ qui est un voisinage de e donc $H = G$ puisque G est connexe. L'unicité de la décomposition résulte évidemment de ce que $K \cap N = \{e\}$.
