

SÉMINAIRE "SOPHUS LIE"

F. BRUHAT

Automorphismes des algèbres de Lie semi-simples

Séminaire "Sophus Lie", tome 1 (1954-1955), exp. n° 16, p. 1-8

http://www.numdam.org/item?id=SSL_1954-1955__1__A19_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/>

Exposé n° 16

AUTOMORPHISMES DES ALGÈBRES DE LIE SEMI-SIMPLES

(Exposé de F. BRUHAT, le 22.3.1955)

Le corps de base est le corps des complexes.

Par automorphisme d'une algèbre de Lie $\mathfrak{g}$, il faut entendre un automorphisme A de la structure d'espace vectoriel de $\mathfrak{g}$ tel que $A[x,y] = [Ax,Ay]$ pour tous $x, y \in \mathfrak{g}$.

Supposons $\mathfrak{g}$ de dimension n ; l'ensemble des automorphismes de $\mathfrak{g}$, que nous noterons $\text{Aut } \mathfrak{g}$, est un sous-groupe de $\text{GL}(n, \mathbb{C})$, fermé, non nécessairement connexe.

C'est un groupe de Lie pour la structure induite.

L'algèbre de Lie de $\text{Aut } \mathfrak{g}$ est l'algèbre de Lie des dérivations de $\mathfrak{g}$ (cf. Chevalley, p. 137). A l'idéal $\text{ad } \mathfrak{g}$ des dérivations intérieures correspond un sous-groupe invariant $\text{Int } \mathfrak{g}$ de $\text{Aut } \mathfrak{g}$, le groupe des automorphismes intérieurs. Si $\mathfrak{g}$ est l'algèbre d'un groupe G connexe $\text{Int } \mathfrak{g} \approx G/Z$ (Z est le centre de G). En général $\text{Int } \mathfrak{g}$ n'est pas fermé dans $\text{Aut } \mathfrak{g}$, mais si $\mathfrak{g}$ est semi-simple, toute dérivation est intérieure et $\text{Int } \mathfrak{g}$ est la composante connexe de l'unité dans $\text{Aut } \mathfrak{g}$, donc est fermé dans $\text{Aut } \mathfrak{g}$.

Soient $\mathfrak{h}, \mathfrak{h}'$ deux sous-algèbres de Cartan de $\mathfrak{g}$. On a vu (Exposé n° 15) qu'il existe un automorphisme intérieur u de $\mathfrak{g}$ qui applique $\mathfrak{h}$ sur $\mathfrak{h}'$. Soit alors $A \in \text{Aut } \mathfrak{g}$; $A\mathfrak{h}$ est une algèbre de Cartan, donc il existe $u \in \text{Int } \mathfrak{g}$, tel que $u^{-1} A\mathfrak{h} = \mathfrak{h}$. Donnons-nous une fois pour toutes l'algèbre de Cartan $\mathfrak{h}$ et désignons maintenant par A un automorphisme de $\mathfrak{g}$ qui conserve $\mathfrak{h}$. (Nous venons de voir que toute classe de $\text{Aut } \mathfrak{g}$ modulo $\text{Int } \mathfrak{g}$ contient un tel automorphisme).

A conserve la forme de Killing, i.e. $\langle Ax, Ay \rangle = \langle x, y \rangle$, puisque A conserve le crochet.

A permute entre elles les racines. Soit α une racine, et prenons $E_\alpha \in \mathfrak{g}^\alpha$. On a :

$$A[H, E_\alpha] = \alpha(H)AE_\alpha = [AH, AE_\alpha] \text{ et d'autre part :}$$

$$\alpha(H) = \langle H, H'_\alpha \rangle = \langle AH, AH'_\alpha \rangle = \alpha^*(AH), \text{ d'où :}$$

$$[AH, AE_\alpha] = \alpha^*(AH) AE_\alpha$$

et puisque A conserve $\mathfrak{h}$, $\alpha^*(H)$ définit bien une forme linéaire sur $\mathfrak{h}$. Nous dirons que α^* est l'image de α par A ; AE_α est un vecteur de $\mathfrak{g}^{\alpha^*}$ et donc $AE_\alpha = \nu_\alpha E_{\alpha^*}$.

Supposons que les E_α définissent une base de Weyl canonique. Puisque A est un automorphisme, $[E_\alpha, E_{-\alpha}] = -H'_\alpha$ entraîne $A[E_\alpha, E_{-\alpha}] = [\nu_\alpha E_{\alpha^*}, \nu_{-\alpha} E_{-\alpha^*}] = -H'_{\alpha^*}$ (évidemment $AH'_\alpha = H'_{A\alpha} = H'_{\alpha^*}$). Comme par ailleurs on avait $[E_{\alpha^*}, E_{-\alpha^*}] = -H'_{\alpha^*}$, on en déduit :

$$(1) \quad \nu_\alpha \nu_{-\alpha} = 1.$$

Ensuite, de $[E_\alpha, E_\beta] = N_{\alpha, \beta} E_{\alpha+\beta}$, on tire :

$$[\nu_\alpha E_{\alpha^*}, \nu_\beta E_{\beta^*}] = N_{\alpha, \beta} \nu_{\alpha+\beta} E_{\alpha^*+\beta^*}$$

et par conséquent :

$$(2) \quad \nu_\alpha \nu_\beta = \frac{N_{\alpha, \beta}}{N_{\alpha^*, \beta^*}} \nu_{\alpha+\beta}.$$

Mais nous avons vu (Exposé n° 11) que :

$$N_{\alpha, \beta}^2 = \frac{1}{2} \langle \alpha, \alpha \rangle q(1-p) \quad (q \geq 0, p \leq 0);$$

$q \leq k \leq p$ entraîne que $\beta + k\alpha$ est une racine, tandis que $\beta + (p-1)\alpha$ et $\beta + (q+1)\alpha$ ne sont pas des racines. Or $(\beta + k\alpha)^* = \beta^* + k\alpha^*$, donc les nombres p et q sont les mêmes pour (α, β) et (α^*, β^*) . De plus $\langle \alpha, \alpha \rangle = \langle \alpha^*, \alpha^* \rangle$, d'où : $N_{\alpha, \beta}^2 = N_{\alpha^*, \beta^*}^2$ ou encore $N_{\alpha, \beta} = \pm N_{\alpha^*, \beta^*}$. Ainsi la formule (2) devient :

$$(3) \quad \nu_\alpha \nu_\beta = \pm \nu_{\alpha+\beta}.$$

Soit alors $\tilde{H} \in \mathfrak{h}$. L'automorphisme $B = e^{\text{ad} \tilde{H}} = \sum \frac{1}{n!} \text{ad}^n \tilde{H}$ est l'identité sur $\mathfrak{h}$ (qui est abélienne) et, pour chaque racine α

$$\begin{aligned} B E_\alpha &= \sum \frac{1}{n!} [\underbrace{\tilde{H}, [\tilde{H}, \dots, [\tilde{H}, E_\alpha], \dots,]}_n] = \sum \frac{1}{n!} [\alpha(\tilde{H})]^n E_\alpha = \\ &= e^{\alpha(\tilde{H})} E_\alpha. \end{aligned}$$

Le composé AB conserve évidemment $\mathfrak{h}$; on a :

$$AB E_\alpha = \nu'_\alpha E_{\alpha^*}, \text{ avec } \nu'_\alpha = e^{\alpha(\tilde{H})} \nu_\alpha.$$

Prenons alors un système $\alpha_1, \dots, \alpha_r$ de racines simples et choisissons $\tilde{H} \in \mathfrak{h}$ tel que $\alpha_i(\tilde{H}) = -\log \nu_{\alpha_i}$. Ceci est toujours possible ; $\nu_{\alpha_i} \neq 0$ car A est un automorphisme de $\mathfrak{g}$. Soit une racine $\alpha = \sum_{i=1}^r a_i \alpha_i$, où les a_i sont tous des entiers de même signe. On a :

$$\nu'_\alpha = (\prod \nu_{\alpha_i}^{-a_i}) \nu_\alpha.$$

Or en utilisant la formule (3) et le fait que si α n'est pas simple et $\alpha \succ 0$ on a $\alpha = \beta + \gamma$ avec $\beta, \gamma \succ 0$, on démontre par récurrence que :

$$(4) \quad \nu_\alpha = \pm \prod \nu_{\alpha_i}^{a_i}$$

d'où l'on déduit que $\nu'_\alpha = \pm 1$. Remarquons que AB appartient à la classe modulo $\text{Int } \mathfrak{g}$ de A , puisque $B \in \text{Int } \mathfrak{g}$. En conclusion, nous pouvons énoncer :

Dans chaque classe modulo $\text{Int } \mathfrak{g}$ de $\text{Aut } \mathfrak{g}$, on peut trouver un automorphisme A de $\mathfrak{g}$ qui conserve une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$, tel de plus que

$$A E_\alpha = \pm E_{\alpha^*} \quad (\alpha^* = \check{A}\alpha)$$

pour toute racine α .

Remarquons que A conserve la forme compacte $\mathfrak{g}_u$ de $\mathfrak{g}$ (engendrée par les iH'_α , les $(E_\alpha + E_{-\alpha})$ et les $(E_\alpha - E_{-\alpha})$).

Proposition 1.- Pour qu'un automorphisme A de $\mathfrak{g}$ coïncide avec l'identité sur $\mathfrak{h}$, il faut et il suffit qu'il existe $H' \in \mathfrak{h}$ tel que $A = e^{\text{ad } H'}$.

Que la condition soit suffisante est évident. Pour voir qu'elle est nécessaire, partons du fait que $AH = H$ pour tout $H \in \mathfrak{h}$ implique $\alpha^* = \alpha$ pour toute racine α . De la formule (2), on déduit $\nu_{\alpha+\beta} = \nu_\alpha \nu_\beta$. La formule (4) devient alors $\nu_\alpha = \prod \nu_{\alpha_i}^{a_i}$ et conduit à $\nu'_\alpha = +1$, B étant défini comme il a été dit. Mais alors AB est l'identité sur $\mathfrak{h}$, et pour chaque racine α , $AB E_\alpha = E_\alpha$. Autrement dit, AB est l'identité sur $\mathfrak{g}$ tout entier. Ceci prouve que A est l'inverse de B et, par conséquent, démontre la proposition 1, car $A = e^{-\text{ad } \tilde{H}} \quad (\tilde{H} \in \mathfrak{h})$.

Nous noterons $\text{Exp ad } \mathfrak{h}$ le groupe des automorphismes de $\mathfrak{g}$ qui induisent l'identité sur $\mathfrak{h}$; c'est un sous-groupe abélien maximal dans $\text{Aut } \mathfrak{g}$ (et non pas seulement maximal dans l'ensemble des sous-groupes abéliens connexes de $\text{Aut } \mathfrak{g}$).

On désigne par $\mathcal{O}$ le groupe des transformations orthogonales (i.e. qui

conservent la forme de Killing) de $\mathfrak{h}$ et qui permutent les racines entre elles. C'est fini car les racines sont en nombre fini et si une transformation linéaire de $\mathfrak{h}$ conserve chaque racine, c'est l'identité sur $\mathfrak{h}$ (les racines sont linéairement indépendantes). Tout élément de $\mathcal{C}$ se prolonge en un automorphisme de $\mathfrak{g}$ d'après le théorème 1 de l'Exposé n° 11.

Nous noterons $\mathcal{J}$ le sous-groupe de $\mathcal{C}$ correspondant à $\text{Int } \mathfrak{g}$. Il est alors clair que $\text{Aut } \mathfrak{g} / \text{Int } \mathfrak{g} \approx \mathcal{C} / \mathcal{J}$ est un groupe, non seulement discret, mais aussi fini.

Soit alors λ une forme linéaire sur $\mathfrak{h}$; P_λ sera l'hyperplan d'équation $\lambda(H) = 0$ dans $\mathfrak{h}$ et P_λ^* l'hyperplan d'équation $\langle \lambda, \mu \rangle = 0$ dans $\mathfrak{h}^*$; S_λ désignera la symétrie par rapport à P_λ dans $\mathfrak{h}$ et aussi la symétrie par rapport à P_λ^* dans $\mathfrak{h}^*$. On a donc

$$S_\lambda(H) = H - 2 \frac{\langle \lambda, H \rangle}{\langle \lambda, \lambda \rangle} H_\lambda \quad H \in \mathfrak{h}$$

$$S_\lambda(\mu) = \mu - 2 \frac{\langle \lambda, \mu \rangle}{\langle \lambda, \lambda \rangle} \lambda \quad \mu \in \mathfrak{h}^*$$

En particulier, prenons pour λ une racine α et appliquons S_α à une autre racine β : $S_\alpha(\beta) = \beta - 2 \frac{\langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle} \alpha$.

Or d'une part, $p+q = -2 \frac{\langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle}$ (Exposé n° 10) ($p < 0$, $q > 0$), de l'autre, $\beta + k\alpha$ est une racine pour tout k compris entre p et q ; donc $S_\alpha(\beta) = \beta + (p+q)\alpha$ est une racine. On appelle groupe de Weyl de $\mathfrak{g}$ le groupe $\mathcal{G}$ engendré par les symétries S_α , où α parcourt le système Δ des racines de $\mathfrak{g}$ sur $\mathfrak{h}$. Nous allons montrer, plus loin, que $\mathcal{G} = \mathcal{J}$.

Notons toujours P_α ($\alpha \in \Delta$) l'hyperplan de $\mathfrak{h}$ défini par $\alpha(H) = 0$. Soit $K = \mathfrak{h} - \bigcup_{\alpha \in \Delta} P_\alpha$; on appelle Chambre de Weyl dans $\mathfrak{h}$ tout convexe maximal de K . Soient r racines simples $\alpha_1, \dots, \alpha_r$ (qui engendrent $\mathfrak{h}$). L'ensemble C_0 des $H \in \mathfrak{h}$ tels que $\langle \alpha_i, H \rangle > 0$ pour tout $1 \leq i \leq r$ est une chambre de Weyl. On ne peut avoir $\langle \alpha, H \rangle = 0$ pour aucune racine α car $\alpha = \sum k_i \alpha_i$, où les k_i sont des entiers tous de même signe.

Soit alors $\mathcal{G}'$ le sous-groupe de $\mathcal{G}$ engendré par les $S_{\alpha_i} = S_i$ ($1 \leq i \leq r$). $\mathcal{G}'$ est transitif sur les chambres de Weyl; i.e. si C_1 est une chambre de Weyl arbitraire, il existe $s \in \mathcal{G}'$ tel que $C_0 = s C_1$. Il suffit de montrer que, w étant quelconque dans C_1 , il existe $s \in \mathcal{G}'$ tel que $s w \in C_0$ (car alors on aura $s w' \in C_0$ pour tout $w' \in C_1$). On considère tous les transformés σw de w lorsque σ parcourt $\mathcal{G}'$. Etant donné un point quelconque w_0 de

C_0 , on prend celui des σw le plus proche de w_0 . Il appartient nécessairement à C_0 , sinon il existerait une symétrie S_i ($1 \leq i \leq r$) telle que $S_i \sigma w$ soit plus proche de w_0 que σw (se vérifie immédiatement sur un dessin).

$\mathcal{G}'$ est transitif sur les faces des chambres de Weyl, c'est-à-dire sur les plans P_α (car $S \in \mathcal{G}'$ transforme un plan P_α en un autre plan P_α). Soit donc une racine α ; α et $-\alpha$ sont les seules racines orthogonales à P_α . Donnons nous une racine simple α_i ($1 \leq i \leq r$) quelconque; il existe $s \in \mathcal{G}'$ telle que $s P_{\alpha_i} = P_\alpha$. En particulier, $s \alpha_i = \pm \alpha$. Si $s \alpha_i = -\alpha$, considérons $s(S_{\alpha_i} \alpha_i) = s(-\alpha_i) = \alpha$. Il existe donc $s \in \mathcal{G}'$ telle que $s \alpha_i = \alpha$ et l'on voit que $S_\alpha = s S_i s^{-1}$. Comme $s, S_i \in \mathcal{G}'$, ceci signifie que $S_\alpha \in \mathcal{G}'$, donc que $\mathcal{G} = \mathcal{G}'$. Nous avons donc démontré :

Théorème 1.- Si $\{\alpha_i\}$ ($1 \leq i \leq r$) est un système de racines simples de $\mathfrak{g}$, les symétries S_{α_i} engendrent le groupe de Weyl $\mathcal{G}$ de $\mathfrak{g}$. De plus, $\mathcal{G}$ est transitif sur les chambres de Weyl et toute racine α est l'image d'une racine α_i par une transformation $s \in \mathcal{G}$.

Une conséquence de ce théorème est que le système des racines simples détermine celui de toutes les racines, résultat déjà obtenu différemment (Exposé n° 10).

Nous allons maintenant établir que $\mathcal{G}$ n'est pas autre chose que le sous-groupe $\mathcal{J}$ de $\mathcal{G}$ correspondant à $\text{Int } \mathfrak{g}$ (cf. p.16-04).

1.- $\mathcal{G} \subset \mathcal{J}$.

Il suffit de montrer que $S_\alpha (\alpha \in \Delta)$ est induite sur $\mathfrak{h}$ par un automorphisme de la forme $U = e^{\text{ad } X}$. Il n'y a qu'à prendre $X = \frac{\pi}{\sqrt{2} \langle \alpha, \alpha \rangle} (E_\alpha + E_{-\alpha})$.

Comme $\text{ad } X$ est nulle sur P_α , U est l'identité sur P_α . Pour $H \in \mathfrak{h}$ quelconque U est la symétrie désirée. On le voit en écrivant :

$$U.H = H + \sum_{p=0}^{\infty} \frac{1}{(2p+1)!} \text{ad}^{2p+1} X.H + \sum_{p=0}^{\infty} \frac{1}{(2p+2)!} \text{ad}^{2p+2} X.H$$

La somme de la 1ère série est le produit d'un certain facteur par $\sin \pi$, donc est nulle. La deuxième est égale à $\frac{\cos \pi - 1}{\langle \alpha, \alpha \rangle} \alpha(H) H'_\alpha$, ce qu'on voulait. Dans le cas particulier où $H = H'_\alpha$, on trouve $U.H = -H'_\alpha$. De même, on verrait que $U.E_\alpha = E_{-\alpha}$ et $U.E_{-\alpha} = E_\alpha$. Dans l'algèbre à trois dimensions engendrée par H'_α , E_α et $E_{-\alpha}$, la matrice de U s'écrit :

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

D'autre part, on remarque que $X \in \mathfrak{O}_{\mathfrak{u}}$ (forme compacte de $\mathfrak{O}$). Ceci entraîne que $\mathfrak{O}$ et $\mathfrak{O}_{\mathfrak{u}}$ ont même groupe de Weyl.

2.- $\mathcal{T} = \mathcal{G}$.

Il suffira de montrer que $\mathcal{T}$ est simplement transitif sur les chambres de Weyl. $\mathcal{G}$, qui est un sous-groupe de $\mathcal{T}$ d'après 1., devra être identique à $\mathcal{T}$. En particulier, on aura établi que le groupe de Weyl est simplement transitif sur les chambres de Weyl.

Soit alors $A \in \mathcal{T}$. On a $A\mathfrak{h} = \mathfrak{h}$. Supposons qu'une chambre de Weyl soit stable pour A ; ou encore supposons que $\check{A}$ conserve le système $\sum$ des racines > 0 . Nous allons prouver que $A \in \exp \operatorname{ad} \mathfrak{h}$, ce qui établira que A induit l'identité sur $\mathfrak{h}$.

$\check{A}$ est une permutation du système Δ de toutes les racines; soient $\sigma_1, \dots, \sigma_p$ les différents cycles de Δ pour cette permutation. On peut écrire :

$$\mathfrak{O} = \mathfrak{h} + \sum_{i=1}^p \mathfrak{O}^{\sigma_i},$$

chacun des $\mathfrak{O}^{\sigma_i}$ étant stable pour A . Une base de $\mathfrak{O}^{\sigma}$ est constituée par E_{α} , $E_{A\alpha}$, ..., $E_{A^{q-1}\alpha}$, où $\alpha \in \sigma$. Et :

$$A \cdot E_{A^m \alpha} = \nu_m E_{A^{m+1} \alpha}$$

Dans $\mathfrak{O}^{\sigma}$, la matrice qui représente A est de la forme

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & \nu_q \\ \nu_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \nu_2 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \dots & \nu_{q-1} & 0 \end{pmatrix}$$

et, par suite, $\det(A - \lambda I) = 0$ n'est autre que l'équation :

$$(5) \quad \lambda^q - \nu_1, \dots, \nu_q = 0$$

Au lieu de A , considérons maintenant AB , avec $B = e^{\text{ad } H}$, $H \in \mathfrak{h}$.
 $AB \in \text{Int } \mathfrak{O}$ évidemment et définit la même permutation des racines que A . Ce
 que nous venons de dire reste donc valable pour AB ; l'équation (5) est dans ce
 cas :

$$(6) \quad \lambda^q - (\nu'_1 \dots \nu'_q) = 0.$$

Mais comme $\nu'_m = e^{\sum_{m=0}^q A^m \alpha(H)} \nu_m$, elle peut encore s'écrire

$$\lambda^q - e^{\sum_{m=0}^q A^m \alpha(H)} \nu_1 \dots \nu_q = 0.$$

Du fait que A conserve le système $\sum$ des racines positives, découle que

$$\sum_{m=0}^q A^m \alpha(H) \neq 0, \text{ puisque les } A^m \alpha(H) \text{ (} 0 \leq m \leq q \text{) ont toutes le même signe.}$$

Choisissons alors $H \in \mathfrak{h}$ tel que

$$e^{\sum_{m=0}^q A^m \alpha(H)} \nu_1 \dots \nu_q \neq 1.$$

Dans ces conditions, (6) ne peut admettre la racine 1. Choisissons H (ce qui
 est manifestement possible) de telle sorte que cette situation se retrouve dans
 tous les sous-espaces $\mathfrak{O}^\sigma$ à la fois. Alors

$$\mathfrak{O}(AB, 1) \cap \left(\sum_{i=1}^p \mathfrak{O}^{\sigma_i} \right) = (0)$$

et donc $\mathfrak{O}(AB, 1) \subset \mathfrak{h}$. Rappelons que $\mathfrak{O}(U, \lambda)$ est le sous-espace propre
 de l'endomorphisme U de $\mathfrak{O}$ correspondant à la valeur propre λ .

Nous allons maintenant utiliser le lemme suivant :

Lemme. - Si $A \in \text{Int } \mathfrak{O}$, alors $\dim \mathfrak{O}(A, 1) \geq r$ (r est la dimension
 de $\mathfrak{h}$).

Le lemme est vrai lorsque A est voisin de l'identité dans $\text{Int } \mathfrak{O}$, car
 alors $A = e^{\text{ad } X}$, avec $X \in \mathfrak{O}$ et donc $\mathfrak{O}(A, 1) = \mathfrak{O}(X, 0)$. Mais nous avons
 vu que $\dim \mathfrak{O}(X, 0) \geq r$ (Exposé n° 10). Toutefois, puisque $\text{Int } \mathfrak{O}$ est un
 groupe de Lie connexe, le résultat est encore vrai dans $\text{Int } \mathfrak{O}$ tout entier car
 on a $\det(A - \lambda 1) = \sum (\lambda - 1)^p \varphi_p(A)$ où φ_p est une fonction analytique et
 $\dim \mathfrak{O}(A, 1) \geq r$ signifie $0 = \varphi_0(A) = \dots = \varphi_{r-1}(A)$ donc si cette identité
 est valable dans un voisinage de l'origine elle est vraie sur tout $\text{Int } \mathfrak{O}$.

Appliquons le lemme en prenant AB au lieu de A . On a donc $\mathfrak{g}(AB, 1) \subset \mathfrak{h}$ et $\dim \mathfrak{g}(AB, 1) \geq r$; cela implique $\mathfrak{g}(AB, 1) = \mathfrak{h}$. Autrement dit, AB induit l'identité sur $\mathfrak{h}$; mais, en vertu de la proposition 1, cela signifie qu'il existe $H' \in \mathfrak{h}$ tel que $AB = e^{\text{ad } H'}$, d'où : $A = e^{\text{ad } H'} B^{-1} = e^{\text{ad}(H'-H)} \in \text{Exp ad } \mathfrak{h}$.

C.Q.F.D.

Nous pouvons donc énoncer le théorème :

Théorème 2.- Le groupe $\text{Aut } \mathfrak{g} / \text{Int } \mathfrak{g}$ est fini et isomorphe à $\mathbb{C}^*/\mathbb{C}$; autrement dit les transformations linéaires de $\mathfrak{h}$ induites par les automorphismes intérieurs de $\mathfrak{g}$ qui conservent $\mathfrak{h}$ constituent exactement le groupe de Weyl. Le groupe de Weyl est simplement transitif sur les chambres de Weyl.
