P. Cartier

Groupes finis engendrés par des symétries

Séminaire Claude Chevalley, tome 2 (1956-1958), exp. nº 14, p. 1-12
<http://www.numdam.org/item?id=SCC_1956-1958__2__A1_0>

GROUPES FINIS ENGENDRÉS PAR DES SYMÉTRIES

(Exposé de P. CARTIER, le 1.4.57)

1.- Symétries.

Soit V un espace de dimension finie $n > 0$ sur le corps des nombres réels. Si S est une transformation linéaire involutive de V, c'est-à-dire si $S^2 = 1$, nous poserons $E_+ = (S+1)/2$, $E_- = (1-S)/2$; on a alors

(1) $$E_+ + E_- = 1 \qquad E_+E_- = E_-E_+ = 0 \qquad S = E_+ - E_-$$

et par suite E_+ et E_- sont les projecteurs associés à une décomposition de V en somme directe de sous-espaces V_+ et V_- ; on a alors

(2) $$S(x_+ + x_-) = x_+ - x_-$$

pour $x_\pm \in E_\pm$. Les éléments de $E_\pm$ sont caractérisés par la condition $S(x) = \pm x$. Inversement, si V est somme directe des sous-espaces V_+ et V_-, la formule (2) définit un opérateur involutif.

De plus, si l'on a donné un produit scalaire $(x \mid y)$ sur V, pour que l'opérateur S défini par la formule (2) soit orthogonal, il faut et il suffit que l'on ait

$$(x_+ + x_- \mid x_+ + x_-) = (x_+ - x_- \mid x_+ - x_-)$$

soit $(x_+ \mid x_-) = 0$ pour $x_\pm \in V_\pm$ ce qui signifie que les sous-espaces V_+ et V_- de V sont orthogonaux.

Nous appellerons symétrie un opérateur linéaire S dans V, involutif et dont l'ensemble des points fixes est un hyperplan.

Si l'on s'est donné un produit scalaire $(x \mid y)$ défini positif sur V, pour tout $a \in V$ non nul, il existe une symétrie S_a et une seule qui soit une transformation orthogonale et qui applique a sur $-a$. En effet, soit H_a l'hyperplan orthogonal à a ; on devra avoir $V_+ = H_a$ et $V_- = \underline{R}.a$ et la symétrie cherchée sera de la forme $1 - 2E$, E étant le projecteur de V sur la droite $\underline{R}.a$ nul sur H_a. Or si $Ex = \lambda a$, on doit avoir $x - \lambda a \in H_a$, i.e. $(x - \lambda a \mid a) = 0$, d'où en résolvant par rapport à λ, la formule

(3) $$S_a(x) = x - 2(x \mid a)/(a \mid a)$$

Il est clair que la formule (3) définit une symétrie répondant à la question. S_a est la seule transformation orthogonale $\neq 1$ qui induise l'identité sur H_a.

2.- Systèmes de racines.

L'espace vectoriel V restera fixé jusqu'à la fin de cet exposé.

Nous appèllerons système de racines un ensemble fini Δ contenu dans V vérifiant les conditions suivantes :

1) L'espace vectoriel V est engendré par Δ.

2) Si $a \in \Delta$, on a $-a \in \Delta$, mais aucun autre vecteur proportionnel à a ne peut appartenir à Δ

3) Pour tout $a \in \Delta$, il existe une symétrie S_a appliquant a sur $-a$ et telle que $S_a \Delta = \Delta$.

Il résulte immédiatement de ces conditions que $0 \notin \Delta$ et que le groupe G d'opérateurs dans V engendré par les symétries S_a est fini. De plus, on définit sur le dual V^* de V un produit scalaire défini positif par la formule :

$$(f \mid g) = \sum_{a \in \Delta} f(a)g(a) \tag{4}$$

Par dualité, on définit donc aussi un produit scalaire $(x \mid y)$ défini positif sur V, qui sera invariant par tout opérateur linéaire dans V conservant l'ensemble Δ. En particulier, S_a est la symétrie orthogonale changeant a en $-a$, et c'est donc l'unique transformation linéaire dans V changeant a en $-a$ et conservant Δ. On en déduit $gS_ag^{-1} = S_{g.a}$ pour toute transformation linéaire g conservent Δ.

Les éléments de Δ seront appelés racines ; on posera $u(a, b) = -2(a \mid b)/(a \mid a)$ pour tout couple de racines a, b ; on aura donc :

$$u(a, a) = -2 \tag{5}$$

$$S_a b = b + u(a, b)a \tag{6}$$

3.- Racines fondamentales.

Comme l'ensemble Δ est fini, il existe $x \in V$ tel que l'on ait $(x \mid a) \neq 0$ pour toute racine a ; nous noterons Σ l'ensemble des racines a telles que $(x \mid a) > 0$. Les ensembles Σ et $-\Sigma$ forment donc une partition de Δ. Nous munirons V de la relation d'ordre (partielle) compatible avec sa structure d'espace vectoriel réel pour laquelle les éléments positifs sont les combinaisons linéaires à coefficients $\geqslant 0$ d'éléments de Σ. Il est clair que Σ est l'ensemble des racines positives.

Considérons l'ensemble $\underline{P}$ des parties F de Σ telles que tout élément de Σ soit combinaison linéaire à coefficients ≥ 0 d'éléments de F et soit π un élément minimal de l'ensemble $\underline{P}$ ordonné par inclusion. On supposera numérotés les éléments de π sous la forme $a_1, a_2, \ldots, a_m$ et l'on posera $S_i = S_{a_i}$.
On a alors la proposition fondamentale suivante :

<u>PROPOSITION 1</u> : <u>L'ensemble</u> π <u>jouit des propriétés suivantes</u> :

a) π <u>est une base de</u> V (donc $m = n$)

b) <u>Toute racine est de la forme</u> $\pm \sum \lambda_i a_i$ avec $\lambda_i \geq 0$.

c) <u>Les scalaires</u> $u_{ij} = u(a_i , a_j)$ <u>sont</u> ≥ 0 <u>pour</u> $i \neq j$.

Le b) résulte de la définition de π ; remarquons ensuite que l'on ne peut avoir $\lambda_i a_i - \lambda_j a_j \geq 0$ avec $\lambda_i , \lambda_j > 0$ et $i \neq j$; on aurait en effet dans ce cas $\lambda_i a_i = \lambda_j a_j + \sum \mu_k a_k$. On ne pourrait avoir $\lambda_i \leq \mu_i$, car on en déduirait $\sum \nu_k a_k = 0$ avec $a_k > 0$, $\nu_k \geq 0$ et $\nu_j > 0$, ce qui est contradictoire ; on ne peut non plus avoir $\lambda_i > \mu_i$ car il en résulterait
$(\lambda_i - \mu_i) a_i = \sum_{k \neq i} \pi_k a_k$ avec $\pi_k \geq 0$, et par suite a_i serait combinaison linéaire à coefficients ≥ 0 des a_k pour $k \neq i$, ce qui contredirait le caractère minimal de π .

Comme on a $S_i a_j > 0$ ou $-S_i a_j < 0$, et que $S_i a_j = a_j + u_{ij} a_i$, on déduit c) de ce qui précède.

Comme Δ engendre V , il en est de même de π , d'après b) . Il suffit donc pour prouver a) de montrer que les $a_i \in \pi$ sont linéairement indépendants. Dans le cas contraire, on aurait une relation de la forme

$$\sum_{i \in I} \lambda_i a_i = \sum_{j \in J} \mu_j a_j = u$$

avec $I \cap J = \emptyset$, $\lambda_i , \mu_j > 0$ et $I , J \neq \emptyset$. On a donc $(a_i \mid a_j) \leq 0$ pour $i \in I$ et $j \in J$, et par suite de $\sum \lambda_i \mu_j (a_i \mid a_j) = (u \mid u) \geq 0$, on déduit $\lambda_i = \mu_j = 0$, ce qui est contradictoire.

C.Q.F.D.

<u>COROLLAIRE 1</u> : <u>Pour qu'une racine</u> $a > 0$ <u>appartienne à</u> π , <u>il faut et il suffit qu'elle ne soit pas combinaison linéaire à coefficients</u> > 0 <u>de</u> $r \geq 2$ <u>racines positives</u>.

En effet, pour que a ne soit pas combinaison linéaire à coefficients > 0 de $r \geq 2$ racines positives, il faut et suffit qu'il ne soit pas une telle combinaison de racines a_i d'après b) . Ceci signifie donc que a est proportionnelle à une des racines a_i donc lui est égale, d'après la condition 2) de la définition des systèmes de racines.

<u>COROLLAIRE 2</u> : <u>Soit</u> π' <u>une partie de</u> Σ ; <u>pour que toute racine</u> a <u>soit de la forme</u> $\pm \sum_{b\in\pi} \lambda_b b$ avec $\lambda_b \geq 0$, <u>il faut et il suffit que</u> $\pi' \supset \pi$.

La condition est suffisante d'après le b) de la proposition 1 ; elle est nécessaire, car d'après le corollaire 1 toute racine $a_i \in \pi$ est proportionnelle à une racine appartenant à π' , donc lui est égale.

<u>COROLLAIRE 3</u> : <u>Soit</u> a <u>une racine positive</u> ; <u>si</u> $a \neq a_i$, <u>on a</u> $S_i a > 0$.

Posons $a = \sum \lambda_j a_j$, d'où $S_i a = a - \mu a_i = \sum_{j\neq i} \lambda_j a_j + (\lambda_i - \mu) a_i$; mais comme a n'est pas proportionnelle à a_i , les scalaires λ_j pour $j \neq i$ sont ≥ 0 et l'un au moins n'est pas nul. Comme $S_i a$ est une racine, tous ses coefficients en fonction des a_j doivent être de même signe ; comme l'un d'eux est > 0 , ils sont tous > 0 et $S_i a > 0$.

On notera que $S_i a_i = - a_i < 0$, donc a_i est la seule racine > 0 dont la transformée par S_i soit < 0 .

D'après le corollaire 2, la partie π de Δ ne dépend que de Σ ; on dit que les éléments de π sont les <u>racines fondamentales ou simples</u> et que π est un système de racines simples. On peut caractériser ainsi les systèmes de racines simples :

<u>PROPOSITION 2</u> : <u>Soient</u> $b_1 , \ldots , b_n$ <u>des racines</u> ; <u>pour que</u> $\pi' = \{b_i\}_{1 \leq i \leq n}$ <u>contienne un système de racines simples</u> (pour un ensemble Σ convenable de racines positives), <u>il faut et il suffit que toute racine soit de la forme</u> $\pm \sum \lambda_i b_i$ avec $\lambda_i \geq 0$.

En effet, comme Δ engendre V , les b_i forment une base de V et par suite, il existe $x \in V$ telle que $(x \mid b_i) > 0$ pour $1 \leq i \leq n$; les racines a de la forme $\sum \lambda_i b_i$ avec $\lambda_i \geq 0$ sont caractérisées par la formule $(x \mid a) > 0$; la proposition résulte alors du corollaire 2 de la proposition 1.

Nous caractériserons au numéro suivant les ensembles possibles de racines positives.

4.- Relation d'ordre dans V .

Nous supposons toujours fixé l'ensemble Σ des racines positives. A côté de l'ordre déjà introduit dans V , nous considérerons l'ordre lexicographique dans V par rapport à la base $(a_1 , \dots , a_n)$ que nous noterons $x \succcurlyeq y$. C'est une relation d'ordre total dans V compatible avec la structure d'espace vectoriel réel et les éléments $x \succcurlyeq 0$ sont par définition les éléments de la forme $x = \lambda_k a_k + \sum_{j>k} \lambda_j a_j$ avec $\lambda_k > 0$. Notons aussi que la relation $x \geqslant y$ entraîne la relation $x \succcurlyeq y$ et que pour $a \in \Delta$, $a \succcurlyeq 0$ équivaut à $a \in \Sigma$.

PROPOSITION 3 : Soit $x > 0$ un élément de V ; il existe un entier i compris entre 1 et n tel que $x > S_i x$.

Si l'on avait $(x \mid a_i) \leqslant 0$ pour toute racine simple a_i , on en déduirait $(x \mid y) \leqslant 0$ pour tout $y \geqslant 0$, d'où en particulier $(x \mid x) \leqslant 0$, ce qui contredit la condition $x \neq 0$; il y a donc un entier i tel que $(x \mid a_i) > 0$ d'où $x > S_i x$ par la formule (3) .

COROLLAIRE : Toute racine est de la forme $S_{i_1} \dots S_{i_p} a_{i_{p+1}}$.

Soit W l'ensemble des racines de la forme $S_{i_1} \dots S_{i_p} a_{i_{p+1}}$; il est clair que W contient les racines simples et que $S_i W \subset W$ pour tout i . Soit a une racine positive et supposons que W contienne toutes les racines positives $b \prec a$; il existe i tel que $S_i a < a$, donc $S_i a \prec a$; si $a \neq a_i$, on a $S_i a > 0$, donc $S_i a \in W$ et $a \in W$ et si $a = a_i$, on a aussi $a \in W$. De là résulte par récurrence que $W \supset \Sigma$; de plus si $a \in W$, on a aussi $-a \in W$ car $- S_{i_1} \dots S_{i_p} a_{i_{p+1}} = S_{i_1} \dots S_{i_p} S_{i_{p+1}} a_{i_{p+1}}$. On a donc bien $W = \Delta$.

PROPOSITION 4 : Soient F une partie de Π et $x \in V$ tels que $x > S_a x$ (resp $x \geqslant S_a x$) pour $a \in F$; si H est le sous-groupe de G engendré par les symétries S_a pour $a \in F$, on a $x > g.x$ (resp $x \geqslant g.x$) pour tout $g \in H$ différent de 1 .

Supposons démontrée l'inégalité $x > g.x$ (resp $x \geqslant g.x$) pour $g = S_{a_1} \dots S_{a_q} \neq 1$ quelle que soit la suite $(a_1 , \dots , a_q)$ de $q < p$ éléments de F et soit $h = S_{b_1} \dots S_{b_p} \neq 1$ avec $b_i \in F$. Posons $h = h' S_{b_p}$ d'où

$$h.x = h'.S_{b_p} x = h'.x - \lambda h'.b_p \tag{8}$$

avec $\lambda > 0$ (resp $\lambda \geq 0$) puisque $\lambda b_p = x - S_{b_p}.x > 0$ (resp ≥ 0) . Dans ces conditions, si $h'.b_p > 0$, on aura $h.x < h'.x < x$ (resp $h.x \leq h'.x \leq x$) par l'hypothèse de récurrence.

Si $h'b_p < 0$, nous appliquerons le lemme suivant :

LEMME : Soient $b_1 , \dots , b_p$ des racines simples telles que

(9) $$b = S_{b_1} \dots S_{b_{p-1}} b_p < 0$$

Il existe un indice k tel que $1 \leq k \leq p$ et que

(10) $$b = - S_{b_1} \dots S_{b_{k-1}} b_k$$

(11) $$S_{b_1} \dots S_{b_p} = S_{b_1} \dots S_{b_{k-1}} S_{b_{k+1}} \dots S_{b_{p-1}}$$

Posons $c_j = S_{b_{j+1}} \dots S_{b_{p-1}} b_p$ et soit k le plus petit indice tel que $c_k > 0$; on a $k > 0$ d'après l'hypothèse faite et $S_{b_k} c_k = c_{k-1} < 0$; d'après le corollaire 3 de la proposition 1 , ceci implique $b_k = c_k$; c'est-à-dire la formule (10) puisque $S_{b_k} b_k = - b_k$. De là, la formule $S_{g.a} = gS_a g^{-1}$ pour $g \in G$ permet de déduire la formule

(12) $$S_{b_k} = (S_{b_{k+1}} \dots S_{b_{p-1}}) S_{b_p} (S_{b_{k+1}} \dots S_{b_{p-1}})^{-1}$$

d'où $S_{b_k} \dots S_{b_{p-1}} = S_{b_{k+1}} \dots S_{b_p}$; comme $(S_{b_k})^2 = 1$, la formule (11) se déduit immédiatement de là.

Revenant à la démonstration de la proposition 4, ce lemme montre que si $h'.b_p < 0$, h est le produit de $p-2$ symétries associées à des éléments de F , et la formule $x > h.x$ (resp $x \geq h.x$) résulte alors de l'hypothèse de récurrence. Comme on a $x > S_a x$ (resp $x \geq S_a.x$) pour $a \in F$, la proposition 4 est bien démontrée par récurrence.

COROLLAIRE : Soit $x \in V$; pour que l'on ait $x > g.x$ pour tout $g \in G$ différent de 1 , il faut et suffit que l'on ait $(x \mid a_i) > 0$ pour $1 \leq i \leq n$.

En effet, comme on a $x - S_i x = + 2 \ (x \mid a_i)/(a_i \mid a_i)$, les conditions $x > S_i x$ et $(x \mid a_i) > 0$ sont équivalentes.

On remarquera que la condition $(x \mid a_i) > 0$ pour $1 \leq i \leq n$ équivaut à la condition $(x \mid a) > 0$ pour toute racine $a > 0$, ou encore à la condition $(x \mid y) > 0$ pour tout $y > 0$.

Venons-en à la caractérisation des ensembles Σ de racines positives.

PROPOSITION 5 : Soit Σ_o un ensemble de racines vérifiant les deux conditions :

a) Si $b_j \in \Sigma_o$ $(1 \leq j \leq m)$ et si $\sum \lambda_j b_j$ avec $\lambda_j > 0$ est une racine, cette racine appartient à Σ_o.

b) Si a est une racine, on a $a \in \Sigma_o$ ou $-a \in \Sigma_o$.

Alors, il existe $g \in G$ tel que $\Sigma \subset g.\Sigma_o$.

Si Σ_o vérifie les conditions a) et b) ci-dessus, il en est de même de $g.\Sigma_o$ pour tout $g \in G$; il suffit donc de prouver que si $\Sigma \not\subset \Sigma_o$ et si $\Sigma \cap \Sigma_o$ possède r éléments, il existe une symétrie S_i telle que $\Sigma \cap S_i \Sigma_o$ ait $r + 1$ éléments au moins ; or, comme $\Sigma \not\subset \Sigma_o$, il existe une racine simple $a_i \notin \Sigma_o$, puisque toute racine positive est combinaison linéaire à coefficients > 0 de racines simples et que Σ_o satisfait à a.

Si $b \in \Sigma \cap \Sigma_o$ est différente de a_i, on a $S_i b \in \Sigma \cap S_i \Sigma_o$ (corollaire 3 de la proposition 1) ; mais comme $a_i \notin \Sigma_o$, on a $-a_i \in \Sigma_o$ d'après la condition b) et par suite $a_i \in \Sigma \cap S_i \Sigma_o$; comme $a_i \neq S_i b$ si $b > 0$, on a bien prouvé que $\Sigma \cap S_i \Sigma_o$ possède au moins $r + 1$ éléments. Ceci achève la démonstration.

COROLLAIRE : Pour qu'un ensemble Σ_o de racines soit un ensemble de racines positives, il faut et il suffit qu'il vérifie les conditions a) et b) ci-dessus et la condition

c) Si a est une racine, on ne peut avoir $a \in \Sigma_o$ et $-a \in \Sigma_o$.

De plus, si ces conditions sont remplies, il existe $g \in G$ tel que $\Sigma_o = g.\Sigma$.

Les conditions énoncées sont évidemment nécessaires ; pour montrer la suffisance de la dernière assertion, on peut supposer $\Sigma \subset \Sigma_o$ d'après la proposition 5. Si l'on avait $\Sigma \neq \Sigma_o$, il existerait une racine $a \in \Sigma_o$ non positive ; on aurait alors $-a \in \Sigma \subset \Sigma_o$, ce qui contredirait la condition c).

5.- Génération du groupe G .

THEOREME 1 : Le groupe G est engendré par les symétries S_i $(1 \leq i \leq n)$; si a_{ij} est l'ordre (fini) de l'élément $S_i S_j$ de G , toutes les relations entre les S_i sont conséquences des relations :

$$(S_i S_j)^{a_{ij}} = 1 \tag{14}$$

Introduisons le groupe $\underline{G}$ défini par les générateurs T_i $(1 \leq i \leq n)$ et les relations $(T_i T_j)^{a_{ij}} = 1$ et l'homomorphisme π de $\underline{G}$ dans G qui applique T_i sur S_i . On notera que $a_{ii} = 1$, donc que $(T_i)^2 = 1$.

a) π est surjectif : toute racine est de la forme $b = S_{i_1} \ldots S_{i_p} a_{i_{p+1}}$ d'où l'on déduit par la formule $g S_a g^{-1} = S_{g.a}$ que $S_b = (S_{i_1} \ldots S_{i_p}) S_{i_{p+1}} (S_{i_1} \ldots S_{i_p})^{-1}$ appartient au sous-groupe de G engendré par les S_i . Comme G est engendré par les symétries S_b , on a bien montré que π est surjectif.

b) π induit un isomorphisme du sous-groupe $\underline{H}_{ij}$ de $\underline{G}$ engendré par T_i et T_j sur le sous-groupe H_{ij} de G engendré par S_i et S_j : il est clair que $\pi(\underline{H}_{ij}) = H_{ij}$; de plus si l'on pose $U = T_i T_j$ et $k = a_{ij}$, on aura $U^k = 1$ et $T_i U T_i U = 1$, d'où $T_i U = U^{-1} T_i$ et par récurrence sur m , $T_i U^m = U^{-m} T_i$. Il en résulte immédiatement que les éléments U^m et $U^m T_i$ forment un sous-groupe de $\underline{G}$, qui contient T_i et T_j donc est égal à $\underline{H}_{ij}$. Or les éléments $\pi(U^m) = (S_i S_j)^m$ pour $1 \leq m < k$ sont tous distincts et de déterminant 1 , tandis que les éléments $(U^m T_i) = (S_i S_j)^m S_i$ sont tous distincts et de déterminant -1 pour $1 \leq m < k$; il en résulte bien que la restriction de π à $\underline{H}_{ij}$ est injective

c) A toute racine positive a on peut associer un élément $T_a \in \underline{G}$ de manière à vérifier les conditions :

$$T_i T_a T_i^{-1} = T_{S_i a} \qquad \text{pour } a \neq a_i \tag{15}$$

$$\pi(T_a) = S_a \tag{16}$$

$$T_{a_i} = T_i \tag{17}$$

Les T_a seront construits par récurrence au moyen de l'ordre lexicographique supposons donc construits des T_a pour $0 \prec a \prec b$ de telle sorte que les formules (15) à (17) soient vérifiées lorsqu'elles ont un sens $(0 \prec S_i a \prec b$, $0 \prec a \prec b$ et $a_i \prec b)$. Si b est simple, soit $b = a_i$, nous poserons $T_b = T_i$; dans le cas contraire, nous choisirons un indice i tel que $b > S_i b$, donc $b \succ S_i b \succ 0$ puisque $b \neq a_i$ et nous poserons

$$T_b = T_i T_{S_i b} T_i^{-1}$$

d'où $\pi(T_b) = S_b$ et il suffira pour continuer la récurrence de vérifier que pour tout indice j tel que $b \succcurlyeq S_j b$, on a $T_j T_b T_j^{-1} = T_{S_j b}$ (on notera que les relations $b \succcurlyeq S_j b$, $b \geqslant S_j b$ et $(b \mid b_j) \geqslant 0$ sont équivalentes).

Si $S_b \in H_{ij}$, la formule précédente résultera alors des formules $\pi(T_a) = S_a$ et de l'assertion b) qui précède.

Dans le cas contraire, il résulte du corollaire 3 de la proposition 1 que les racines $h.b$ sont > 0 pour $h \in H_{ij}$ et de la proposition 4 que ces racines sont $\leqslant b$ donc $\preccurlyeq b$. De plus, on peut évidemment se limiter au cas où $i \neq j$. Nous distinguerons alors deux cas :

$b \succ S_j b$: on a alors $h.b \prec b$ pour $h \neq 1$ dans H_{ij} d'où $S_j b = (S_j S_i)^{k-1} S_i b$ avec $k = a_{ij}$ et les racines $(S_i S_j)^{\ell} S_i b$ et $S_j (S_i S_j)^{\ell-1} S_i b$ pour $0 < \ell \leqslant k-1$ sont toutes $\prec b$. De la formule (15) , on déduit alors

$$T_{S_j b} = (T_i T_j)^{k-1} T_{S_i b} (T_i T_j)^{1-k} = U T_b U^{-1}$$

avec $U = (T_i T_j)^{k-1} \quad T_i = T_j$ puisque $(T_i T_j)^k = 1$ et $(T_i)^2 = 1$. On a bien prouvé notre assertion dans ce cas.

$b = S_j b$: soit P le sous-espace de dimension 2 de V engendré par a_i et a_j et soit W le sous-espace de dimension $n-2$ de V orthogonal à P . Tout $h \in H_{ij}$ induit l'identité sur W ; de plus de $S_j b = b$, on déduit que b est orthogonal à a_j , donc aussi que la projection orthogonale b' de b sur P est orthogonale à a_j . Les conditions $h.b = b$ et $h.b' = b'$ pour $h \in H_{ij}$ sont équivalentes puisque $b - b' \in W$; elles signifient que h coïncide sur P avec la symétrie associée à un vecteur de P orthogonal à b' et non nul, donc que $h = S_j$. On a donc $b \succ h.b$ pour $h \in H_{ij}$ différent de 1 et de S_j . Posant toujours $k = a_{ij}$, on aura $b = S_j b = (S_i S_j)^{k-1} S_i b$; comme $u_\ell = S_j (S_i S_j)^{\ell-1} S_i$ et $v_\ell = (S_i S_j)^{\ell} S_i$ sont différentes de 1 et S_j pour $1 \leqslant \ell < k$, on a $u_\ell . b \prec b$ et $v_\ell . b \prec b$ pour $1 \leqslant \ell < k$, d'où en appliquant la formùle (15) un certain nombre de fois

$$T_{S_j b} = (T_i T_j)^{k-1} T_{S_i b} (T_i T_j)^{1-k}$$

et on achève la démonstration comme dans le premier cas.

d) Si l'on a $g \in \underline{G}$ et $\pi(g).\Sigma = \Sigma$, on a $g = 1$.

Supposons démontré que pour $q < p$, l'égalité $S_{i_1} \ldots S_{i_q} . \Sigma = \Sigma$ implique $T_{i_1} \ldots T_{i_q} = 1$ pour toute suite $(i_1 , \ldots , i_q)$ d'entiers compris entre 1 et n et supposons que l'on ait $S_{i_1} \ldots S_{i_p} .a > 0$ pour toute racine $a > 0$. Appliquant à $a = a_{i_p}$, on voit qu'il existe un entier k tel que $S_{i_m} \ldots S_{i_p} a_{i_p}$ soit négatif pour $k < m \leq p$ mais que $S_{i_k} \ldots S_{i_p} a_{i_p} > 0$. Utilisant le corollaire 3 de la proposition 1, on en conclut que $a_{i_k} = S_{i_{k+1}} \ldots S_{i_{p-1}} a_{i_p}$; mais d'après c) , ceci implique $T_{i_k} = (T_{i_{k+1}} \ldots T_{i_{p-1}}) T_{i_p} (T_{i_{k+1}} \ldots T_{i_{p-1}})^{-1}$, d'où $T_{i_k} \ldots T_{i_{p-1}} = T_{i_{k+1}} \ldots T_{i_p}$ et finalement $T_{i_p} \ldots T_{i_p} = T_{i_1} \ldots T_{i_{k-1}} T_{i_{k+1}} \ldots T_{i_p}$
D'après l'hypothèse de récurrence, on en déduit bien $T_{i_1} \ldots T_{i_p} = 1$.

Le théorème résulte alors immédiatement de d) .

6.- Chambres.

Soit V' le complémentaire dans V de la réunion des hyperplans H_a $(a \in \Delta)$. Une chambre est une partie convexe maximale de V' ; comme une forme linéaire conserve un signe constant sur une partie convexe, on voit immédiatement qu'une chambre C_o est définie par les conditions :

$$e(a)(x \mid a) > 0 \qquad \text{pour tout } a \in \Delta$$

$e(a)$ étant un scalaire égal à $+1$ ou -1 et tel que $e(a) = -e(-a)$. Il est clair que l'ensemble Σ_o des racines a telles que $e(a) = +1$, ou ce qui revient au même, $(x \mid a) > 0$ pour $x \in C$, vérifie les conditions a) b) et c) du corollaire de la proposition 5 , donc est de la forme $g.\Sigma$ avec $g \in G$.
De plus, la chambre C définie par les conditions $(x \mid a) > 0$ pour toute racine positive a , est aussi définie par les conditions $(x \mid a_i) > 0$ pour $1 \leq i \leq n$.
Utilisant le corollaire de la proposition 4 et le d) de la démonstration du théorème du numéro 5 , on en conclut :

PROPOSITION 6 : L'ensemble C des $x \in V$ tels que $(x \mid a) > 0$ pour toute racine $a \in \Sigma$ est une chambre ; les ensembles $g.C$ $(g \in G)$ forment une partition du complémentaire V' dans V de la réunion des hyperplans H_a . Toute partie convexe de V' est contenue dans une chambre et les chambres sont de la forme $g.C$.

7.- Remarques finales.

1) Soit G un groupe fini de transformations linéaires dans V engendré par des symétries et ne laissant aucun vecteur non nul fixe.

Soit $S \in G$ une symétrie et D la droite de V formée des $x \in V$ tels que $S(x) = -x$; si $g \in G$ conserve la droite D comme il est d'ordre fini, il ne peut induire que 1 ou -1 sur D ; par suite si l'on considère l'ensemble P de toutes les droites D ainsi définies et une partition

$P = \bigcup_{i=1}^{m} G.D_i$, prenant un élément $a_i \neq 0$ dans chaque droite D_i et posant

$\Delta = \bigcup_{i=1}^{m} (G.a_i \cup G.(-a_i))$, on définit un ensemble Δ vérifiant les conditions 1)

2) et 3) du numéro 2 . Par suite le théorème du numéro 5 s'applique à tout groupe fini engendré par des symétries. Problème : Existe-t-il un sous-ensemble $P' \subsetneq P$ stable par G et tel que les symétries correspondantes engendrent G ?

2) Soit Δ un système de racines dans V tel que le sous-groupe de V engendré par Δ soit discret, ou ce qui revient au même, soit de rang n sur l'anneau des entiers, ou bien supposons que Δ soit un sous-ensemble d'un espace vectoriel sur le corps des nombres rationnels vérifiant les conditions 1) à 3) du numéro 2 . Remplaçant au besoin les éléments de Δ par des multiples entiers convenables, on peut toujours supposer que les nombres $u(a , b)$ sont entiers ; il résulte alors immédiatement du corollaire de la proposition 3 que toute racine est de la forme $\pm \sum m_i a_i$ avec m_i entier ≥ 0 .

3) Les racines simples a_i $(1 \leq i \leq n)$ forment une base de V et pour i et j quelconques, l'angle de a_i et a_j est de la forme $\pi - \pi/n_{ij}$ avec n_{ij} entier ≥ 2 ; on peut, par une méthode analogue à celle de l'exposé 13 du Séminaire S. LIE 1954/55 classer les systèmes de vecteurs a_i d'un espace euclidien linéairement indépendant dont les angles deux à deux sont la forme $\pi - \pi/n_{ij}$ $(n_{ij}$ entier $\geq 2)$. En dehors des cas étudiés dans loc. cit. et du cas $n = 2$, on trouve sauf erreur, trois systèmes nouveaux.

Problème : Démontrer, sans utiliser la classification, que pour un tel système de vecteur a_i , le groupe de transformations orthogonales engendré par les symétries S_{a_i} est fini (si l'on avait la proposition 6 , il suffirait d'utiliser une considération simple de volume).