

STRUCTURE DU GROUPE DES SIMILITUDES ORTHOGONALES

AKIKO YOSHIOKA

1. Nous avons un théorème, ce qu'on appelle le théorème de Cartan-Dieudonné, sur les générateurs du groupe orthogonal: Toute transformation orthogonale à n variables sur un corps de caractéristique $\neq 2$ est un produit de n symétries au plus, et sur un corps de caractéristique 2 elle est un produit au plus de n transvections orthogonales, sauf un seul cas, [1] ou [3]. C'est une généralisation d'un résultat obtenu par E. Cartan, relatif au corps des nombres réels ou au corps des nombres complexes [4]. Il nous semble qu'il soit important d'étudier les involutions des groupes classiques, non seulement pour savoir la structure de ces groupes eux-mêmes, mais aussi pour déterminer les automorphismes ou les isomorphismes de ces groupes. Parce que la plupart des méthodes pour déterminer ces automorphismes ou ces isomorphismes repose sur la considération des involutions et sur le fait qu'un automorphisme ou un isomorphisme transforme une involution en involution. Comme il est possible qu'un produit de deux symétries ou bien de deux transvections orthogonales devienne une involution orthogonale, il est naturel d'avoir la question suivante: Si une transformation orthogonale se représente comme produit des involutions orthogonales, combien d'involutions sont-elles nécessaires au minimum pour représenter une transformation orthogonale? C'est une question posée par Prof. H.S.M. Coxeter. Un résultat obtenu par M. J. Wonenburger donne une réponse dans un cas, c'est-à-dire, dans le cas où le corps est de caractéristique $\neq 2$ et que la forme quadratique est non dégénérée d'indice nul. Dans ce cas, une transformation orthogonale peut se représenter comme produit de deux involutions orthogonales [5].

D'autre part, si n est impair, le groupe des similitudes orthogonales est produit direct du groupe orthogonal et du groupe des homothéties. Mais, si au contraire n est pair, le groupe des similitudes orthogonales n'est pas

Received July 30, 1969.

en général produit direct du groupe orthogonal et du groupe des homothéties. Ce produit direct est un sous-groupe distingué dans le groupe des similitudes orthogonales. On ne connaissait peu le groupe quotient du groupe des similitudes orthogonales par ce produit direct, surtout dans le cas où le corps est de caractéristique 2. Alors, dans ce travail, nous allons étudier le groupe des similitudes orthogonales sur un corps de caractéristique 2, en étant en connexion avec une généralisation du théorème de Cartan-Dieudonné et la question de Coxeter.

2. Rappelons d'abord les notions et les notations dont nous aurons à nous servir. Soient K un corps commutatif de caractéristique 2 et E un espace vectoriel à droite de dimension n . Une forme quadratique sur E est définie comme une application Q de E dans K qui satisfait à une identité de la forme

$$(1) \quad Q(\mathbf{x}\alpha + \mathbf{y}\beta) = Q(\mathbf{x})\alpha^2 + Q(\mathbf{y})\beta^2 + f(\mathbf{x}, \mathbf{y})\alpha\beta$$

pour tous $\alpha, \beta \in K$ et tous $\mathbf{x}, \mathbf{y} \in E$, où f est une forme bilinéaire sur $E \times E$. Cette forme est *alternée* et entièrement déterminée par Q . Pour tout sous-espace vectoriel V de E , l'ensemble V^0 des vecteurs de E qui sont orthogonaux à tous les vecteurs de V par rapport à f , est dit *sous-espace orthogonal* à V . On dit qu'un sous-espace V est *isotrope* ou *totalement isotrope*, suivant que $V \cap V^0 \neq \{\mathbf{o}\}$ ou $V \subseteq V^0$. Un vecteur \mathbf{x} de E est dit *singulier* si $Q(\mathbf{x}) = 0$; un sous-espace V de E est encore dit *singulier* si $Q(\mathbf{x}) = 0$ pour tout \mathbf{x} dans V . On appelle *l'indice* de Q la dimension maxima des sous-espaces singuliers de E et on le désigne par ν .

Dans tout ce travail, on fixe une forme quadratique Q non dégénérée et non défective. En conséquence, l'orthogonalité dans E soit toujours entendue par rapport à la forme alternée f définie par la formule

$$(2) \quad f(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x}) + Q(\mathbf{y}) + Q(\mathbf{x} + \mathbf{y}).$$

Dans ce cas, E^0 se réduit à \mathbf{o} et n doit être pair: $n = 2m$. Une fois pour toutes, on fixe une base symplectique $\langle \mathbf{e}_1, \dots, \mathbf{e}_m, \mathbf{e}'_1, \dots, \mathbf{e}'_m \rangle$ telle qu'on ait $f(\mathbf{e}_i, \mathbf{e}'_j) = \delta_{ij}$, $f(\mathbf{e}_i, \mathbf{e}_j) = 0$, $f(\mathbf{e}'_i, \mathbf{e}'_j) = 0$, $1 \leq i, j \leq m$.

Le Lemme suivant est bien connu (par exemple, cf. [2] p. 33).

LEMME 1. *Pour tout vecteur singulier \mathbf{a} de E et tout plan non isotrope P contenant \mathbf{a} , il existe dans P un vecteur singulier et un seul \mathbf{b} tel que $f(\mathbf{a}, \mathbf{b}) = 1$.*

De ce lemme et de l'hypothèse $E^0 = \{\mathbf{o}\}$, on déduit immédiatement le

lemme suivant.

LEMME 2. Soit ν l'indice de Q . On peut choisir dans E une base symplectique $\langle e_1, \dots, e_m, e'_1, \dots, e'_m \rangle$ telle que $e_1, \dots, e_\nu, e'_1, \dots, e'_\nu$ soient les vecteurs singuliers.

On appelle *similitude symplectique* (relativement à la forme f) une transformation linéaire u de E vérifiant la relation

$$(3) \quad f(u(\mathbf{x}), u(\mathbf{y})) = f(\mathbf{x}, \mathbf{y})\mu_u \quad \text{pour tous } \mathbf{x}, \mathbf{y} \in E,$$

où μ_u est un élément du groupe multiplicatif K^* des éléments non nuls de K , appelé le *multiplicateur* de u . Les similitudes symplectiques forment le *groupe des similitudes symplectiques*, noté $GS_{p_{2m}}(f)$, ou simplement GS_p . Les similitudes symplectiques de multiplicateur 1 sont appelées *transformations symplectiques*; elles forment un sous-groupe distingué $S_{p_{2m}}(f)$ (ou S_p) de $GS_{p_{2m}}(f)$; $S_{p_{2m}}(f)$ est dit le *groupe symplectique*.

LEMME 3. Soient V un sous-espace non isotrope de E et \bar{V} le sous-espace orthogonal à V . Alors, on a la somme directe $E = V \oplus \bar{V}$. Si une transformation u de $GS_{p_{2m}}(f)$ laisse globalement invariant V , u laisse aussi globalement invariant \bar{V} .

Le premier énoncé est facile à voir, comme on peut étendre une base symplectique de V à celle de E . Ensuite, pour un vecteur $\bar{\mathbf{y}}$ de \bar{V} , soit $u(\bar{\mathbf{y}}) = \mathbf{x} + \bar{\mathbf{x}}$, $\mathbf{x} \in V$, $\bar{\mathbf{x}} \in \bar{V}$. Supposons que $\mathbf{x} \neq \mathbf{o}$. Comme V est non isotrope, il existe dans V un vecteur \mathbf{x}' tel que $f(\mathbf{x}, \mathbf{x}') \neq 0$. Soit \mathbf{x}'' le vecteur de V tel que $u(\mathbf{x}'') = \mathbf{x}'$. Alors, on aurait que $f(u(\bar{\mathbf{y}}), u(\mathbf{x}'')) = f(\mathbf{x} + \bar{\mathbf{x}}, \mathbf{x}') = f(\mathbf{x}, \mathbf{x}') + f(\bar{\mathbf{x}}, \mathbf{x}') = f(\mathbf{x}, \mathbf{x}') \neq 0$. D'autre part, on a $f(u(\bar{\mathbf{y}}), u(\mathbf{x}'')) = f(\bar{\mathbf{y}}, \mathbf{x}'')\mu_u = 0$. Donc, on a nécessairement $\mathbf{x} = \mathbf{o}$.

Remarque 1. Soit u une transformation linéaire de E et soit $U = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ la matrice correspondant à u par rapport à la base $\langle e_1, \dots, e_m, e'_1, \dots, e'_m \rangle$, où A, B, C, D soient les matrices carrées à m lignes et m colonnes: $u(e_j) = \sum_{i=1}^m e_i a_{ij} + \sum_{i=1}^m e'_i c_{ij}$; $u(e'_j) = \sum_{i=1}^m e_i b_{ij} + \sum_{i=1}^m e'_i d_{ij}$, $1 \leq j \leq m$. La condition que u appartienne à GS_p équivaut à celle que $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ laisse $\begin{pmatrix} O & E \\ E & O \end{pmatrix}$ semi-invariant: ${}^t \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} O & E \\ E & O \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} O & \mu_u E \\ \mu_u E & O \end{pmatrix}$. Donc, pour que u soit une similitude symplectique de multiplicateur μ_u , il faut et il suffit que les matrices A, B, C, D vérifient les conditions suivantes:

$$(4) \quad \begin{aligned} {}^tCA + {}^tAC &= O, \\ {}^tAD + {}^tCB &= \mu_u E, \\ {}^tDB + {}^tBD &= O. \end{aligned}$$

On appelle *similitude orthogonale* (relativement à la forme quadratique Q) une transformation linéaire u de E vérifiant la relation

$$(5) \quad Q(u(x)) = Q(x)\mu_u \quad \text{pour tout } x \in E,$$

où $\mu_u \in K^*$ est encore dit *le multiplicateur* de u . Le groupe formé de toutes les similitudes orthogonales est dit *le groupe des similitudes orthogonales* et noté $\mathbf{GO}_{2m}(Q)$ ou \mathbf{GO} . Les similitudes orthogonales de multiplicateur 1 sont appelées *transformations orthogonales* et forment un sous-groupe distingué $\mathbf{O}_{2m}(Q)$ (ou \mathbf{O}) de $\mathbf{GO}_{2m}(Q)$; $\mathbf{O}_{2m}(Q)$ est dit *le groupe orthogonal*.¹⁾

Pour un vecteur non singulier \mathbf{a} de E , considérons une transformation linéaire v de E définie par $v(\mathbf{X}) = \mathbf{X} + \mathbf{a} \frac{f(\mathbf{X}, \mathbf{a})}{Q(\mathbf{a})}$. Comme on a $Q(v(x)) = Q(x) + Q(\mathbf{a}) \frac{f(x, \mathbf{a})^2}{Q(\mathbf{a})^2} + f(x, \mathbf{a}) \frac{f(x, \mathbf{a})}{Q(\mathbf{a})} = Q(x)$ pour tout x de E , v est une transformation orthogonale: $\mu_v = 1$. De plus, v laisse invariants tous les vecteurs de l'hyperplan orthogonal à \mathbf{a} . Nous dirons qu'une telle transformation est *une transvection orthogonale définie par le vecteur \mathbf{a}* .

Remarque 2. La formule (2) montre qu'une similitude orthogonale est une similitude symplectique de même multiplicateur, dès que la forme quadratique est supposée non défective. Alors, on a $\mathbf{GO} \subseteq \mathbf{GS}_p$, $\mathbf{O} \subseteq \mathbf{S}_p$. Il est facile à voir que, pour un élément u de \mathbf{GS}_p , les conditions $Q(u(e_i)) = Q(e_i)\mu_u$, $Q(u(e'_i)) = Q(e'_i)\mu_u$, $1 \leq i \leq m$, sont équivalentes à celle qu'on a $u \in \mathbf{GO}$.

3. Dans tout ce numéro, supposons que l'indice ν de Q soit non nul.

PROPOSITION 1. *Pour tout u de $\mathbf{GO}_{2m}(Q)$, il existe un vecteur singulier \mathbf{x} dans E et au plus de deux transvections orthogonales v_1, v_2 tels que l'on ait $u_1(\mathbf{x}) = \mathbf{x}\mu_u$ où $u_1 = v_1u$ ou $u_1 = v_1v_2u$.*

Modifiant la méthode due à E. Cartan, nous démontrerons la proposition.

¹⁾ Dans la théorie des groupes en question, le corps de base sur lequel on se pose joue un rôle essentiel. Donc il faudrait noter les groupes $\mathbf{GO}_{2m}(K, Q)$, $\mathbf{GS}_{p_{2m}}(K, f)$, etc., avec le corps K . Mais, dans ce travail, le corps sera fixé toujours, alors, pour la simplicité on les notera $\mathbf{GO}_{2m}(Q)$, $\mathbf{GS}_{p_{2m}}(f)$, etc.

Cas I: Il existe un vecteur singulier \mathbf{x} tel que $f(\mathbf{x}, u(\mathbf{x})) \neq 0$.

Si l'on pose $\mathbf{a} = u(\mathbf{x}) + \mathbf{x}\mu_u$, on a $Q(\mathbf{a}) = Q(\mathbf{x})\mu_u + Q(\mathbf{x})\mu_u^2 + f(u(\mathbf{x}), \mathbf{x})\mu_u = f(u(\mathbf{x}), \mathbf{x})\mu_u \neq 0$. Alors, on peut définir une transvection orthogonale v telle que $v(\mathbf{X}) = \mathbf{X} + \mathbf{a} \frac{f(\mathbf{X}, \mathbf{a})}{Q(\mathbf{a})}$. Dès que $v(u(\mathbf{x})) = u(\mathbf{x}) + \mathbf{a} \frac{f(u(\mathbf{x}), \mathbf{a})}{Q(\mathbf{a})} = u(\mathbf{x}) + (u(\mathbf{x}) + \mathbf{x}\mu_u) \frac{f(u(\mathbf{x}), u(\mathbf{x}) + \mathbf{x}\mu_u)}{f(u(\mathbf{x}), \mathbf{x})\mu_u} = \mathbf{x}\mu_u$ pour tout vecteur \mathbf{x} de E , $u_1 = vu$ est une transformation cherchée.

Cas II: Pour tout vecteur singulier \mathbf{x} on a $f(\mathbf{x}, u(\mathbf{x})) = 0$.

Le sous-espace engendré par \mathbf{x} et $u(\mathbf{x})$ est singulier. Alors, il existe un vecteur \mathbf{z} dans E tel que $f(\mathbf{x}, \mathbf{z}) \neq 0$ et $f(u(\mathbf{x}), \mathbf{z}) \neq 0$, parce que l'on a supposé que $E^0 = \{\mathbf{o}\}$. Le plan P engendré par \mathbf{x} et \mathbf{z} est non isotrope. D'après le lemme 1, il existe un vecteur singulier \mathbf{y} dans P tel que $f(\mathbf{x}, \mathbf{y}) = 1$. Comme \mathbf{y} s'écrit $\mathbf{x}\alpha + \mathbf{z}\beta$, avec $\beta \neq 0$, $\alpha, \beta \in K$, on a $f(u(\mathbf{x}), \mathbf{y}) = f(u(\mathbf{x}), \mathbf{x}\alpha + \mathbf{z}\beta) = f(u(\mathbf{x}), \mathbf{x})\alpha + f(u(\mathbf{x}), \mathbf{z})\beta = f(u(\mathbf{x}), \mathbf{z})\beta \neq 0$. Posons $\mathbf{a}_1 = \mathbf{x} + \mathbf{y}$ et $\mathbf{a}_2 = u(\mathbf{x}) + \mathbf{y}\mu_u$. Comme $Q(\mathbf{a}_1) = f(\mathbf{x}, \mathbf{y}) \neq 0$ et $Q(\mathbf{a}_2) = f(u(\mathbf{x}), \mathbf{y})\mu_u \neq 0$, les vecteurs singuliers \mathbf{a}_1 et \mathbf{a}_2 définissent les transvections orthogonales v_1 et v_2 , respectivement: $v_i(\mathbf{X}) = \mathbf{X} + \mathbf{a}_i \frac{f(\mathbf{X}, \mathbf{a}_i)}{Q(\mathbf{a}_i)}$, $i = 1, 2$.

On voit alors comme ci-dessus que $v_1(\mathbf{y}) = \mathbf{x}$ et $v_2(u(\mathbf{x})) = \mathbf{y}\mu_u$. On a donc $v_1(v_2(u(\mathbf{x}))) = v_1(\mathbf{y}\mu_u) = v_1(\mathbf{y})\mu_u = \mathbf{x}\mu_u$. En posant $u_1 = v_1v_2u$, on a $u_1(x) = \mathbf{x}\mu_u$.

PROPOSITION 2. *Sauf dans le cas où $m = 2$, $K = F_2$, pour tout u de $\mathbf{GO}_{2m}(\mathbb{Q})$ il existe des vecteurs singuliers \mathbf{x}, \mathbf{y} dans E et un nombre fini de transvections orthogonales w_1, \dots, w_s , tels que l'on ait $f(\mathbf{x}, \mathbf{y}) \neq 0$, $u_2(\mathbf{x}) = \mathbf{x}\mu_u$, $u_2(\mathbf{y}) = \mathbf{y}$, où $u_2 = (\prod_{i=1}^s w_i)u$. Dans le cas où $m = 2$, $K = F_2$, pour tout u de $\mathbf{O}_{2m}(\mathbb{Q})$ il existe des vecteurs singuliers \mathbf{x}, \mathbf{y} dans E et un nombre fini d'involutions orthogonales w_1, \dots, w_s , tels que l'on ait $f(\mathbf{x}, \mathbf{y}) \neq 0$, $u_2(\mathbf{x}) = \mathbf{x}$, $u_2(\mathbf{y}) = \mathbf{y}$, où $u_2 = (\prod_{i=1}^s w_i)u$.*

Etant donné un élément u de $\mathbf{GO}_{2m}(\mathbb{Q})$, soient \mathbf{x} et u_1 un vecteur singulier et une similitude orthogonale satisfaisant aux conditions de la proposition 1. Soit H_x l'hyperplan orthogonal à \mathbf{x} . D'après le lemme 1, il existe au moins un vecteur singulier \mathbf{y} qui n'appartient pas à H_x . De la proposition 1, on a que $f(u_1(\mathbf{x}), u_1(\mathbf{y})) = f(\mathbf{x}, \mathbf{y})\mu_{u_1} = f(\mathbf{x}, \mathbf{y})\mu_u^2$, et que $f(u_1(\mathbf{x}), u_1(\mathbf{y})) = f(\mathbf{x}\mu_u, u_1(\mathbf{y})) = f(\mathbf{x}, u_1(\mathbf{y}))\mu_u$. Alors on a $f(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}, u_1(\mathbf{y}))$, ce qui entraîne $f(\mathbf{x}, \mathbf{y} + u_1(\mathbf{y})) = 0$, c'est-à-dire que $\mathbf{y} + u_1(\mathbf{y})$ appartient à H_x .

²⁾ Par la définition du multiplicateur, on a $\mu_{uv} = \mu_u\mu_v$ et $\mu_{u^{-1}} = \mu_u^{-1}$, pour tous u, v de $\mathbf{GS}_{\mathbf{P}_{2m}}(f)$.

Cas I. Il existe un vecteur singulier \mathbf{y} n'appartenant pas à H_x tel qu'on ait $f(\mathbf{y}, u_1(\mathbf{y})) \neq 0$.

Si l'on pose $\mathbf{a} = \mathbf{y} + u_1(\mathbf{y})$, on a $Q(\mathbf{a}) = f(\mathbf{y}, u_1(\mathbf{y})) \neq 0$ et on a une transvection orthogonale w définie par $\mathbf{a} : w(\mathbf{X}) = \mathbf{X} + \mathbf{a} \frac{f(\mathbf{X}, \mathbf{a})}{Q(\mathbf{a})}$. Cette transvection w transforme $u_1(\mathbf{y})$ en $\mathbf{y} : w(u_1(\mathbf{y})) = \mathbf{y}$. Comme on a $\mathbf{a} \in H_x$, on a $w(\mathbf{x}) = \mathbf{x}$. Si l'on pose $u_2 = wu_1$, on obtient que $u_2(\mathbf{x}) = w(u_1(\mathbf{x})) = w(\mathbf{x}\mu_u) = w(\mathbf{x})\mu_u = \mathbf{x}\mu_u$, $u_2(\mathbf{y}) = w(u_1(\mathbf{y})) = \mathbf{y}$. On a une transformation cherchée $u_2 = wu_1 = wvu$ ou $= wv_1v_2u$.

Cas II. Pour tout vecteur singulier \mathbf{y} n'appartenant pas à H_x , on a $f(\mathbf{y}, u_1(\mathbf{y})) = 0$.

(i) $m = 1$. Soit \mathbf{x} un vecteur singulier tel que $u_1(\mathbf{x}) = \mathbf{x}\mu_u$. Par le lemme 1, il existe un vecteur singulier \mathbf{y} tel que \mathbf{x}, \mathbf{y} se composent une base symplectique. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice correspondant à u_1 par rapport à cette base. Des conditions auxquelles \mathbf{x}, u_1 satisfont, on constate que $a = \mu_u, c = 0$. De plus, l'équation $f(\mathbf{y}, u_1(\mathbf{y})) = 0$ entraîne $f(\mathbf{y}, \mathbf{x}b + \mathbf{y}d) = b = 0$. Puisque u_1 est dans $GO_2(Q)$, on a $Q(\mathbf{x} + \mathbf{y})\mu_{u_1} = Q(u_1(\mathbf{x} + \mathbf{y})) = Q(u_1(\mathbf{x}) + u_1(\mathbf{y})) = Q(\mathbf{x}\mu_u + \mathbf{y}d) = \mu_u d$. D'autre part, comme les v_i appartiennent à $O_2(Q)$, on a $\mu_u = \mu_{u_1}$ et $Q(\mathbf{x} + \mathbf{y})\mu_{u_1} = Q(\mathbf{x} + \mathbf{y})\mu_u = \mu_u$. Donc, on a $d = 1$, c'est-à-dire qu'on a $u_1(\mathbf{y}) = \mathbf{y}$. On prend u_1 comme $u_2 : u_2 = vu$ ou $= v_1v_2u$.

(ii) $m > 1$; \mathbf{y} et $u_1(\mathbf{y})$ sont linéairement dépendants. Soit $u_1(\mathbf{y}) = \mathbf{y}\alpha$. Comme on a que $f(\mathbf{x}, \mathbf{y})\mu_u = f(\mathbf{x}, \mathbf{y})\mu_{u_1} = f(u_1(\mathbf{x}), u_1(\mathbf{y})) = f(\mathbf{x}\mu_u, \mathbf{y}\alpha) = f(\mathbf{x}, \mathbf{y})\mu_u\alpha$, on a nécessairement $\alpha = 1$. D'où on a $u_1(\mathbf{y}) = \mathbf{y}$, $u_1(\mathbf{x}) = \mathbf{x}\mu_u$. On prend u_1 comme $u_2 : u_2 = vu$ ou $= v_1v_2u$.

(iii) $m > 1$; \mathbf{y} et $u_1(\mathbf{y})$ sont linéairement indépendants; sauf pour $m=2$, $K = F_2$.

D'abord, nous allons vérifier dans le cas $K \neq F_2$.

Supposons en premier qu'on ait $H_y = H_{u_1(y)}$, où H_y et $H_{u_1(y)}$ désignent les hyperplans orthogonaux à \mathbf{y} et à $u_1(\mathbf{y})$, respectivement. Dès que $E = H_y \oplus \mathbf{x}K = H_{u_1(y)} \oplus \mathbf{x}K$ tout vecteur arbitraire \mathbf{z} de E peut être écrit comme $\mathbf{z} = \mathbf{h} + \mathbf{x}\alpha$, $\mathbf{h} \in H_y = H_{u_1(y)}$, $\alpha \in K^*$. En conséquence, on a que $f(\mathbf{y} + u_1(\mathbf{y}), \mathbf{z}) = f(\mathbf{y} + u_1(\mathbf{y}), \mathbf{h} + \mathbf{x}\alpha) = f(\mathbf{y}, \mathbf{h}) + f(u_1(\mathbf{y}), \mathbf{h}) + f(\mathbf{y} + u_1(\mathbf{y}), \mathbf{x})\alpha = 0$. Ceci signifie que $H_{y+u_1(y)} = E$, où $H_{y+u_1(y)}$ est l'hyperplan orthogonal à $\mathbf{y} + u_1(\mathbf{y})$. C'est contradictoire à l'hypothèse que $E^0 = \{\mathbf{o}\}$. Par conséquent

on a $H_y \cong H_{u_1(y)}$. De plus on a $H_x \cong H_y$, $H_x \cong H_{u_1(y)}$, parce que l'on a $f(x, u_1(y)) = f(x, y) \cong 0$. Soient $M = H_x \cap H_y$, $N = H_x \cap H_{u_1(y)}$ ³⁾. Les sous-espaces M et N sont non isotropes de dimension $2m - 2$. Si l'on suppose que $M = N$, pour un vecteur arbitraire m de M , on aurait $f(m, y) = 0$, $f(m, u_1(y)) = 0$, par suite $f(m, y + u_1(y)) = 0$. D'autre part, on a $f(x, y + u_1(y)) = 0$ et $f(y, y + u_1(y)) = 0$. Donc, x, y, M seraient contenus dans l'hyperplan $H_{y+u_1(y)}$, ce qui entraîne la contradiction. En conséquence, il existe un vecteur z contenu dans M mais non contenu dans N . Supposons ensuite qu'on ait $f(z, m) = 0$ pour tout vecteur arbitraire m de M . Comme tout vecteur arbitraire e de E peut s'écrire $e = x\alpha + y\beta + m\gamma$, $\alpha, \beta, \gamma \in K$, on aurait $f(z, e) = f(z, x)\alpha + f(z, y)\beta + f(z, m)\gamma = 0$, contrairement à l'hypothèse $E^0 = \{o\}$. Donc, il existe un vecteur z' dans M tel qu'on ait $f(z, z') \cong 0$. Si z est singulier, par le lemme 1 il existe un vecteur singulier z'' dans le plan engendré par z et z' tel qu'on ait $f(z, z'') \cong 0$. Soit $\bar{z} = z + z''$. Comme $Q(\bar{z}) = Q(z) + Q(z'') + f(z, z'') \cong 0$, \bar{z} est un vecteur non singulier dans M . Nous allons montrer qu'on peut choisir \bar{z} tel que $\bar{z} \notin H_{u_1(y)}$. D'abord soit $z'' \in H_{u_1(y)}$. Si \bar{z} était dans $H_{u_1(y)}$, $z = \bar{z} + z''$ serait contrairement dans $H_{u_1(y)}$. Donc, dans ce cas \bar{z} n'appartient pas à $H_{u_1(y)}$. Ensuite soit $z'' \notin H_{u_1(y)}$. Si \bar{z} est dans $H_{u_1(y)}$, on a $0 = f(\bar{z}, u_1(y)) = f(z, u_1(y)) + f(z'', u_1(y))$, alors on a $f(z, u_1(y)) = f(z'', u_1(y)) \cong 0$. Comme on a supposé que $K \cong F_2$, on peut prendre un autre vecteur $\bar{z}' = z + z''\alpha$, $\alpha \cong 1, 0$ dans M . On en déduit que $f(\bar{z}', u_1(y)) = f(z, u_1(y)) + f(z'', u_1(y))\alpha = f(z, u_1(y))(1 + \alpha) \cong 0$ et que $Q(\bar{z}') = Q(z + z''\alpha) = f(z, z'')\alpha \cong 0$.

Partons d'un vecteur non singulier \bar{z} choisi comme ci-dessus: $\bar{z} \in M$, $\bar{z} \notin H_{u_1(y)}$. Comme K a plus de deux éléments, on peut trouver un élément $\alpha \cong 0$ de K tel que $t = x\alpha + \bar{z}$ satisfait à la condition: $f(u_1(y), t) = f(u_1(y), x\alpha + \bar{z}) = f(u_1(y), x)\alpha + f(u_1(y), \bar{z}) \cong 0$. Alors, t est non singulier, $f(y, t) = f(y, x)\alpha + f(y, \bar{z}) = f(y, x)\alpha \cong 0$ et $f(x, t) = f(x, \bar{z}) = 0$. Comme y est singulier, d'après le lemme 1 il existe un vecteur singulier \bar{t} tel que $\bar{t} = y + t\beta$, $\beta \cong 0 \in K$ et $f(y, \bar{t}) \cong 0$. On en déduit que $f(u_1(y), \bar{t}) = f(u_1(y), y) + f(u_1(y), t)\beta = f(u_1(y), t)\beta \cong 0$.

Posons $a_1 = y + \bar{t}$ et $a_2 = u_1(y) + \bar{t}$. Comme $Q(a_1) = f(y, \bar{t}) \cong 0$ et $Q(a_2) = f(u_1(y), \bar{t}) \neq 0$, les vecteurs non singuliers a_1 et a_2 définissent les transvections orthogonales w_1 et w_2 , respectivement: $w_i(X) = X + a_i \frac{f(X, a_i)}{Q(a_i)}$, $i = 1, 2$.

³⁾ Nous suivons le même raisonnement que celui qui fait partie de la démonstration de la proposition 14 (de la première ligne jusqu'à la 19-ème ligne de p. 43, [1]).

On a alors que $w_1(\bar{t}) = \bar{t} + (\mathbf{y} + \bar{t}) \frac{f(\bar{t}, \mathbf{y} + \bar{t})}{f(\mathbf{y}, \bar{t})} = \mathbf{y}$ et $w_2(u_1(\mathbf{y})) = u_1(\mathbf{y}) + (u_1(\mathbf{y}) + \bar{t}) \frac{f(u_1(\mathbf{y}), u_1(\mathbf{y}) + \bar{t})}{f(u_1(\mathbf{y}), \bar{t})} = \bar{t}$. Comme on a que $f(\mathbf{x}, \mathbf{a}_1) = f(\mathbf{x}, \mathbf{y} + \bar{t}) = f(\mathbf{x}, \mathbf{y} + \mathbf{y} + \mathbf{t}\beta) = f(\mathbf{x}, \mathbf{t})\beta = 0$ et $f(\mathbf{x}, \mathbf{a}_2) = f(\mathbf{x}, u_1(\mathbf{y}) + \bar{t}) = f(\mathbf{x}, u_1(\mathbf{y}) + \mathbf{y} + \mathbf{t}\beta) = f(\mathbf{x}, u_1(\mathbf{y}) + \mathbf{y}) + f(\mathbf{x}, \mathbf{t})\beta = 0$, on a $w_1(\mathbf{x}) = \mathbf{x}$ et $w_2(\mathbf{x}) = \mathbf{x}$. On en conclut que $w_1(w_2(u_1(\mathbf{x}))) = w_1(w_2(\mathbf{x}\mu_u)) = \mathbf{x}\mu_u$, $w_1(w_2(u_1(\mathbf{y}))) = w_1(\bar{t}) = \mathbf{y}$. On arrive à une transformation cherchée $u_2 = w_1w_2u_1 = w_1w_2v_u$ ou $= w_1w_2v_2u$.

Ensuite, nous allons vérifier dans le cas $K = F_2$, $m > 2$. Le sous-espace V défini par \mathbf{x} et $M \cap N$ est de dimension $2m - 2$. Comme $2m - 2 > m$, V n'est pas singulier et il existe un vecteur non singulier \mathbf{z} dans V tel que $\mathbf{z} = \mathbf{x} + \mathbf{t}$, $\mathbf{t} \in M \cap N$. Comme $Q(\mathbf{z}) = Q(\mathbf{t})$, \mathbf{t} est un vecteur non singulier. Avec ces deux vecteurs non singuliers \mathbf{z} et \mathbf{t} , on peut suivre le même raisonnement qu'après la ligne 28 de la page dernière, et on peut arriver à la même conclusion.

(iv) $m = 2$, $K = F_2$; \mathbf{y} et $u_1(\mathbf{y})$ sont linéairement indépendants. Avec le même raisonnement et les mêmes notations que (iii), dans ce cas on obtient $\dim V = 2$. Donc, nous avons la possibilité que V soit singulier, et nous n'y pouvons pas continuer la même démonstration que dans la page dernière. En réalité, dans ce cas, on a nécessairement $\nu = 2$. Car, comme \mathbf{y} , $u_1(\mathbf{y})$ sont singuliers avec $f(\mathbf{y}, u_1(\mathbf{y})) = 0$ et que \mathbf{y} , $u_1(\mathbf{y})$ sont linéairement indépendants, le sous-espace défini par \mathbf{y} , $u_1(\mathbf{y})$ est singulier et de dimension 2. Alors, d'après le lemme 2, il existe une base symplectique $\langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}'_1, \mathbf{e}'_2 \rangle$, composée de vecteurs singuliers. De plus, on peut prendre \mathbf{x} comme $\mathbf{e}_1 : u_1(\mathbf{e}_1) = \mathbf{e}_1$. Soit $u_1(\mathbf{e}'_1) = \mathbf{e}_1\alpha + \mathbf{e}_2\beta + \mathbf{e}'_1\alpha' + \mathbf{e}'_2\beta'$. L'hypothèse $f(\mathbf{e}'_1, u_1(\mathbf{e}'_1)) = 0$ entraîne $\alpha = 0$. L'équation $0 = Q(\mathbf{e}'_1) = Q(u_1(\mathbf{e}'_1)) = Q(\mathbf{e}'_1\alpha' + \mathbf{e}'_2\beta') + \beta\beta' = \beta\beta'$ entraîne $\beta = 0$ ou $\beta' = 0$. Si on avait $\alpha' = 0$, on aurait $0 \neq f(\mathbf{e}_1, \mathbf{e}'_1) = f(u_1(\mathbf{e}_1), u_1(\mathbf{e}'_1)) = f(\mathbf{e}_1, \mathbf{e}_2\beta + \mathbf{e}'_2\beta') = 0$. Donc, on a $\alpha' = 1$. Pour $\beta = 0$, $\beta' = 0$, on a $u_1(\mathbf{e}'_1) = \mathbf{e}'_1$, et on prend u_1 comme u_2 .

D'abord, soient $\beta = 1$, $\beta' = 0 : u_1(\mathbf{e}'_1) = \mathbf{e}_2 + \mathbf{e}'_1$. Prenons une transformation w_1 telle que $w_1(\mathbf{e}_1) = \mathbf{e}_1$, $w_1(\mathbf{e}_2) = \mathbf{e}_2$, $w_1(\mathbf{e}'_1) = \mathbf{e}_2 + \mathbf{e}'_1$, $w_1(\mathbf{e}'_2) = \mathbf{e}_1 + \mathbf{e}'_2$. Cette transformation w_1 correspond à la matrice $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, par rapport à $\langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}'_1, \mathbf{e}'_2 \rangle$. En vertu des remarques 1, 2, on a $w_1 \in \mathcal{O}_4$. On voit que $w_1(u_1(\mathbf{e}_1)) = w_1(\mathbf{e}_1) = \mathbf{e}_1$ et que $w_1(u_1(\mathbf{e}'_1)) = w_1(\mathbf{e}_2 + \mathbf{e}'_1) = w_1(\mathbf{e}_2) + w_1(\mathbf{e}'_1) = \mathbf{e}_2 + \mathbf{e}_2 + \mathbf{e}'_1 = \mathbf{e}'_1$.

On voit facilement que w_1 est une involution orthogonale. On obtient $u_2 = w_1vu$ ou $= w_1v_1v_2u$.

Ensuite, soient $\beta=0, \beta'=1 : u_1(e'_1) = e'_1 + e'_2$. Prenons une transformation w_2 telle que $w_2(e_1) = e_1, w_2(e_2) = e'_2, w_2(e'_1) = e'_1, w_2(e'_2) = e_2$, dont la matrice est $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$. En vertu des remarques 1, 2, on a encore $w_2 \in O_4$, et w_2 est une involution orthogonale. Enfin, on a $w_1(w_2(u_1(e_1))) = w_1(w_2(e_1)) = w_1(e_1) = e_1$ et $w_1(w_2(u_1(e'_1))) = w_1(w_2(e'_1 + e'_2)) = w_1(w_2(e'_1) + w_2(e'_2)) = w_1(e'_1 + e_2) = w_1(e'_1) + w_1(e_2) = e_2 + e'_1 + e_2 = e'_1$. En posant $u_2 = w_1vu$ ou $= w_1v_1v_2u$ ou $= w_1w_2vu$ ou $= w_1w_2v_1v_2u$, la proposition est entièrement démontrée.

4. Désignons par h_a l'homothétie associée à un élément a de K^* : $h_a(x) = xa$. On appelle semi-involution une transformation linéaire w de E telle que $w^2 = h_a$ pour un élément a de K^* .

THÉORÈME 1. Pour tout u de $GO_{2m}(Q)$, il existe une semi-involution w dans $GO_{2m}(Q)$ telle que $w^2 = h_{\mu_u}$.

Nous sommes amenés à distinguer deux cas I, II, suivant que Q est d'indice $\nu = 0$ ou d'indice $\nu > 0$.

Cas I-1: $\nu = 0$; pour tout x de E on a $f(x, u(x)) = 0$.

Si l'on pose $u(x) = x + y$, on a $f(u(x), u(y)) = f(x, y)\mu_u = f(x, u(x))\mu_u = 0, 0 = f(x + y, u(y)) = f(x, u(y)) = f(x, u^2(x) + u(x)) = f(x, u^2(x))$. D'autre part, on a $Q(u^2(x)) = Q(x)\mu_u^2$. D'où on a $Q(u^2(x) + x\mu_u) = Q(u^2(x)) + Q(x)\mu_u^2 + f(u^2(x), x)\mu_u = 0$. Selon l'hypothèse que $\nu = 0$, on a $u^2(x) + x\mu_u = 0$ pour tout x dans E , c'est-à-dire que u est elle-même une semi-involution orthogonale telle que $u^2 = h_{\mu_u}$.⁴⁾

Remarque 3. Dans ce cas I-1, si u n'est pas identique u ne peut appartenir à $O_{2m}(Q)$. Car, si $u \in O$, on aurait $Q(x + u(x)) = Q(x) + Q(u(x)) + f(x, u(x)) = Q(x) + Q(x) + f(x, u(x)) = 0$. En conséquence, il existe un vecteur singulier, contrairement à l'hypothèse $\nu = 0$.

Remarque 4. Soit $U = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ la matrice correspondant à u . De la condition $f(x, u(x)) = 0$, les matrices A, B, C, D doivent être telles que ${}^tB = B, {}^tC = C, {}^tA = D$. En considérant les relations (4) on arrive aussi à $U^2 = \mu_u E$.

⁴⁾ Pourtant ce fait est vrai aussi pour $\nu > 0$.

Cas I-2: $\nu = 0$; il existe un vecteur x_0 dans E tel que $f(x_0, u(x_0)) \neq 0$. Nous procéderons par récurrence sur m .

$m = 1$. Soit $\langle e, e' \rangle$ une base symplectique, et soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matrice correspondant à u par rapport à cette base. Comme $u \in \mathbf{GO}_2$, on a $Q(e)\mu_u = Q(u(e)) = Q(e)a^2 + Q(e')c^2 + ac$ et $Q(e')\mu_u = Q(u(e')) = Q(e)b^2 + Q(e')d^2 + bd$. Si $c = 0$ on a $\mu_u = a^2$ et si $b = 0$ on a $\mu_u = d^2$. Dans ces cas, on peut prendre h_a ou h_d comme w , où h_a et h_d désignent les homothéties associées aux éléments a et d , respectivement.

Prenons une matrice W ayant la forme $\begin{pmatrix} a & \frac{1}{c}(a^2 + \mu_u) \\ c & a \end{pmatrix}$. Soit w la transformation dont la matrice par rapport à la base $\langle e, e' \rangle$ est W . On voit aisément que w est une similitude symplectique de multiplicateur μ_u et que w est une semi-involution telle que $w^2 = h_{\mu_u}$. Montrons ensuite que $w \in \mathbf{GO}$. Comme on a $w(e) = ea + e'c = u(e)$, on a $Q(w(e)) = Q(u(e)) = Q(e)\mu_u$ et $Q(e)\mu_u = Q(e)a^2 + Q(e')c^2 + ac$. Si $\mu_u = a^2$, on peut prendre l'homothétie h_a comme w . Donc, on peut supposer que $a^2 + \mu_u \neq 0$, et $Q(e) = \frac{1}{a^2 + \mu_u} \{Q(e')c^2 + ac\}$. Alors, on a $Q(w(e')) = Q\left(e \frac{1}{c}(a^2 + \mu_u) + e'a\right) = Q(e) \frac{1}{c^2}(a^2 + \mu_u)^2 + Q(e')a^2 + \frac{a}{c}(a^2 + \mu_u) = \{Q(e')c^2 + ac\} \frac{1}{c^2}(a^2 + \mu_u) + Q(e')a^2 + \frac{a}{c}(a^2 + \mu_u) = Q(e')\mu_u$. De la remarque 2, on constate que $w \in \mathbf{GO}$.

$m - 1$. Revenons à x_0 tel que $f(x_0, u(x_0)) \neq 0$. Posons $f(x_0, u(x_0)) = \lambda$, $x_0 \frac{1}{\lambda} = e_1$ et $u(x_0) = e'_1$. Prenons le vecteur $\alpha = e_1\lambda + e'_1 \frac{1}{Q(e_1)\lambda\mu_u} + u(e'_1) \frac{1}{\mu_u}$. Si le vecteur α est nul, on a $u(e'_1) = e_1\lambda\mu_u + e'_1 \frac{1}{Q(e_1)\lambda}$. D'autre part, on a $u(e_1) = e'_1 \frac{1}{\lambda}$. Dans ce cas, posons $u_1 = u$. Si le vecteur α n'est pas nul, comme on a $Q(\alpha) = \frac{1}{Q(e_1)\mu_u} + f(e_1, u(e'_1)) \frac{\lambda}{\mu_u} \neq 0$ ($\nu = 0$!), le vecteur non singulier α définit la transvection orthogonale $v : v(X) = X + \alpha \frac{f(X, \alpha)}{Q(\alpha)}$. Comme on a $f(e'_1, \alpha) = f\left(e'_1, e_1\lambda + e'_1 \frac{1}{Q(e_1)\lambda\mu_u} + u(e'_1) \frac{1}{\mu_u}\right) = \lambda + f(e'_1, u(e'_1)) \frac{1}{\mu_u} = \lambda + \lambda\mu_u \frac{1}{\mu_u} = 0$, on a $vu(e_1) = v(u(e_1)) = v\left(e'_1 \frac{1}{\lambda}\right) = v(e'_1) \frac{1}{\lambda} = e'_1 \frac{1}{\lambda}$. Ensuite, on a $f(u(e'_1), \alpha) = f\left(u(e'_1), e_1\lambda + e'_1 \frac{1}{Q(e_1)\lambda\mu_u} + u(e'_1) \frac{1}{\mu_u}\right) = f(u(e'_1), e_1)\lambda + f(u(e'_1), e'_1) \frac{1}{Q(e_1)\lambda\mu_u} = f(u(e'_1), e_1)\lambda + \frac{1}{Q(e_1)}$. On a donc $vu(e'_1) =$

$v(u(e'_1)) = u(e'_1) + \left\{ e_1 \lambda + e'_1 \frac{1}{Q(e_1) \lambda \mu_u} + u(e'_1) \frac{1}{\mu_u} \right\} \mu_u = e_1 \lambda \mu_u + e'_1 \frac{1}{Q(e_1) \lambda}$. Dans ce cas, posons $u_1 = vu$. Il est facile à voir que $\mu_{u_1} = \mu_u$.

Considérons le plan P engendré par les vecteurs e_1 et e'_1 , et prenons une base symplectique $\langle e_1, e_2, \dots, e_m, e'_1, e'_2, \dots, e'_m \rangle$. Alors, P est non isotrope et $e_2, \dots, e_m, e'_2, \dots, e'_m$ engendrent le sous-espace \bar{P} orthogonal à P . Comme u_1 laisse invariant P , u_1 laisse aussi invariant \bar{P} , d'après le lemme 3. Désignons par \bar{u}_1 et \bar{Q} les restrictions à \bar{P} de u_1 et de Q , et par \bar{f} la forme alternée déterminée par \bar{Q} . C'est évident que \bar{Q} est de l'indice nul et que \bar{Q} est non dégénérée et non défective. Ainsi, s'il existe un vecteur \bar{x}_0 dans \bar{P} tel que $\bar{f}(\bar{x}_0, \bar{u}_1(\bar{x}_0)) \neq 0$ d'après l'hypothèse de récurrence il existe une semi-involution \bar{w} sur \bar{P} telle que $\bar{w}^2 = h_{\mu_{\bar{u}_1}}$ et $\bar{w} \in GO_{2(m-1)}(\bar{Q})$. Mais, si pour tout vecteur \bar{x} dans \bar{P} on a $\bar{f}(\bar{x}, \bar{u}_1(\bar{x})) = 0$, en vertu de I-1, on a $\bar{u}_1^2 = h_{\mu_{\bar{u}}}$. En tous les cas, il existe une semi-involution \bar{w} dans $GO_{2(m-1)}(\bar{Q})$ telle que $\bar{w}^2 = h_{\mu_{\bar{u}_1}} = h_{\mu_{\bar{u}}} = h_{\mu_u}$.

Soit $\begin{pmatrix} \bar{A} & \bar{B} \\ \bar{C} & \bar{D} \end{pmatrix}$ la matrice correspondant à \bar{w} par rapport à la base $\langle e_2, \dots, e_m, e'_2, \dots, e'_m \rangle$. Des propriétés de \bar{w} telles que $\bar{w} \in GS_{P_2(m-1)}(\bar{f})$ et $\bar{w}^2 = h_{\mu_u}$, les matrices $\bar{A}, \bar{B}, \bar{C}, \bar{D}$ doivent satisfaire aux conditions suivantes:

$$\begin{aligned}
 & {}^t \bar{C} \bar{A} + {}^t \bar{A} \bar{C} = O, \\
 (6) \quad & {}^t \bar{A} \bar{D} + {}^t \bar{C} \bar{B} = \mu_u E, \\
 & {}^t \bar{D} \bar{B} + {}^t \bar{B} \bar{D} = O; \\
 & (\bar{A})^2 + \bar{B} \bar{C} = \bar{C} \bar{B} + \bar{D}^2 = \mu_u E, \\
 (7) \quad & \bar{A} \bar{B} + \bar{B} \bar{D} = O, \\
 & \bar{C} \bar{A} + \bar{D} \bar{C} = O.
 \end{aligned}$$

m. Considérons la transformation w sur E dont la matrice par rapport

à la base $\langle e_1, e_2, \dots, e_m, e'_1, e'_2, \dots, e'_m \rangle$ est de la forme $\begin{pmatrix} o & \bar{A} & \lambda \mu_u & \bar{B} \\ \lambda^{-1} & o & o & \bar{D} \\ & \bar{C} & & \end{pmatrix}$. En uti-

lisant les relations (6), on voit que cette matrice satisfait aux relations (4) et donc que w est une similitude symplectique de multiplicateur μ_u . En utilisant les relations (7), on voit que le carré de cette matrice est égal à $\begin{pmatrix} \mu_u E & O \\ O & \mu_u E \end{pmatrix}$, et donc que w est une semi-involution telle que $w^2 = h_{\mu_u}$. Montrons finalement que $w \in GO_{2m}(Q)$. Comme $\bar{w}^2 = h_{\mu_u}$ et $\bar{w} \in GO_{2(m-1)}(\bar{Q})$, on a $\bar{Q}(\bar{x}) \mu_{\bar{w}}^2 = \bar{Q}(\bar{w}^2(\bar{x})) = \bar{Q}(\bar{x} \mu_u) = \bar{Q}(\bar{x}) \mu_u^2$ pour tout \bar{x} de \bar{P} et on a donc $\mu_{\bar{w}} = \mu_u$. Pour tout $i, 2 \leq i \leq m$, on a $Q(w(e_i)) = Q(\bar{w}(e_i)) = \bar{Q}(\bar{w}(e_i)) = \bar{Q}(e_i) \mu_{\bar{w}}$

$= Q(e_i)\mu_u$ et de même $Q(w(e'_i)) = Q(e'_i)\mu_u$. De plus, comme on a $e'_1 = u(x_0) = u(e_1)\lambda = u(e_1)\lambda$, on a $Q(w(e_1)) = Q\left(e'_1 \frac{1}{\lambda}\right) = Q(u(e_1))Q(e_1)\mu_u$ et $Q(w(e'_1)) = Q(e_1\lambda\mu_u) = Q(e_1\lambda)\mu_u^2 = Q(u(e_1)\lambda)\mu_u = Q(e'_1)\mu_u$. D'après la remarque 2, on a $w \in \mathbf{GO}_{2m}(\mathbb{Q})$.

Cas II: $\nu > 0$.

Montrons le théorème par récurrence sur m .

Soit $\langle e, e' \rangle$ une base symplectique composée de vecteurs singuliers. Prenons la transformation w à laquelle correspond la matrice $\begin{pmatrix} 0 & \mu_u \\ 1 & 0 \end{pmatrix}$. On voit aisément que $w \in \mathbf{GO}_2$ et que $w^2 = h_{\mu_u}$.

Soit \bar{E} un sous-espace de E de dimension $2(m-1)$, et soit \bar{Q} une forme quadratique définie sur \bar{E} , non dégénérée, non défective et d'indice $\bar{\nu} > 0$. Supposons maintenant que pour tout \bar{u} de $\mathbf{GO}_{2(m-1)}(\bar{Q})$, il existe une semi-involution \bar{w} dans $\mathbf{GO}_{2(m-1)}(\bar{Q})$ telle que $\bar{w}^2 = h_{\mu_{\bar{u}}}$. Soient x, y des vecteurs singuliers et soit u_2 une similitude orthogonale, obtenus dans la proposition 2. Signalons que $\mu_{u_2} = \mu_u$. En posant $x = e_1$ et $y = \frac{1}{f(x,y)}e'_1$, on a $u_2(e_1) = e_1\mu_u$ et $u_2(e'_1) = e'_1$. Soit $\langle e_1, e_2, \dots, e_m, e'_1, e'_2, \dots, e'_m \rangle$ une base symplectique de E . De même que dans le cas I, soient P et \bar{P} les sous-espaces engendrés par $\langle e_1, e'_1 \rangle$ et $\langle e_2, \dots, e_m, e'_2, \dots, e'_m \rangle$, respectivement. D'après le lemme 3, u_2 laisse invariant \bar{P} . Soient \bar{u}_2 et \bar{Q} les restrictions à \bar{P} de u_2 et de Q . Si l'indice $\bar{\nu}$ de \bar{Q} est positif, l'hypothèse de récurrence assure l'existence d'une semi-involution \bar{w} telle que $\bar{w}^2 = h_{\mu_{\bar{u}_2}}$ et $\bar{w} \in \mathbf{GO}_{2(m-1)}(\bar{Q})$. Si l'indice $\bar{\nu}$ de \bar{Q} est nul, d'après le cas I, il existe aussi une telle semi-involution \bar{w} dans $\mathbf{GO}_{2(m-1)}(\bar{Q})$. De plus, comme $\mu_{\bar{u}_2} = \mu_{u_2} = \mu_u$, on a $\bar{w}^2 = h_{\mu_u}$ et $\mu_{\bar{w}} = \mu_u$.

Soit $\begin{pmatrix} \bar{A} & \bar{B} \\ \bar{C} & \bar{D} \end{pmatrix}$ la matrice correspondant à \bar{w} par rapport à la base $\langle e_2, \dots, e_m, e'_2, \dots, e'_m \rangle$. Alors $\bar{A}, \bar{B}, \bar{C}, \bar{D}$ satisfont aux conditions (6) et (7). Prenons la transformation w sur E dont la matrice par rapport à $\langle e_1, e_2, \dots,$

$e_m, e'_1, e'_2, \dots, e'_m \rangle$ est $\begin{pmatrix} 0 & \bar{A} & \mu_u & \bar{B} \\ 1 & \bar{C} & 0 & \bar{D} \end{pmatrix}$. Comme dans le cas I, on voit que

$w \in \mathbf{GS}_{p_{2m}}(f)$ et $w^2 = h_{\mu_u}$. De plus, pour tout $i, 2 \leq i \leq m, Q(w(e_i)) = Q(e_i)\mu_u$ et $Q(w(e'_i)) = Q(e'_i)\mu_u$. Pour e_1, e'_1 , on a $Q(w(e_1)) = Q(e_1) = 0 = Q(e_1)\mu_u$ et $Q(w(e'_1)) = Q(e_1\mu_u) = Q(e_1)\mu_u^2 = 0 = Q(e'_1)\mu_u$. On constate donc que $w \in \mathbf{GO}_{2m}(\mathbb{Q})$.

Nous avons complété la démonstration.

5. Dans tout ce numéro, nous supposons que $K \cong F_2$.

L'application $u \rightarrow \mu_u$ de $\mathbf{GO}_{2m}(\mathbb{Q})$ dans K^* est un homomorphisme dont le noyau est le groupe orthogonal \mathbf{O} et que l'image est un sous-groupe $M(\mathbb{Q})$ du groupe multiplicatif K^* . Pour un élément arbitraire s de K^* , on a $Q(h_s(\mathbf{x})) = Q(\mathbf{x}s) = Q(\mathbf{x})s^2$, et donc $\mu_{h_s} = s^2$. Alors, on a toujours $K^{*2} \subseteq M(\mathbb{Q})$. Désignons par \mathbf{H} le groupe formé de toutes les homothéties.

LEMME 4. *Pour qu'une similitude orthogonale appartienne à $\mathbf{O} \times \mathbf{H}$ il faut et il suffit que son multiplicateur soit un élément carré dans K^* .*

En effet, si un élément u de \mathbf{GO} appartient à $\mathbf{O} \times \mathbf{H}$, u s'écrit $u = u'h_s$, $u' \in \mathbf{O}$, $s \in K^*$, et on a $\mu_u = \mu_{u'}\mu_{h_s} = s^2$. Inversement, si μ_u est un élément carré s^2 dans K^* , du fait que $\mu_{uh_{s^{-1}}} = \mu_u\mu_{h_{s^{-1}}} = s^2s^{-2} = 1$, $u' = uh_{s^{-1}}$ appartient à \mathbf{O} . Donc $u = u'h_s$ appartient à $\mathbf{O} \times \mathbf{H}$.

De ce lemme, on voit que le groupe $\mathbf{O} \times \mathbf{H}$ est un sous-groupe distingué dans \mathbf{GO} . En effet, pour un élément $u'h_s$ de $\mathbf{O} \times \mathbf{H}$ et pour un élément arbitraire v de \mathbf{GO} , on a $\mu_{vu'h_s v^{-1}} = \mu_v\mu_{u'}\mu_{h_s}\mu_v^{-1} = s^2$. Donc, $vu'h_s v^{-1}$ appartient à $\mathbf{O} \times \mathbf{H}$.

Si $M(\mathbb{Q})$ coïncide à K^{*2} , \mathbf{GO} coïncide au produit direct $\mathbf{O} \times \mathbf{H}$. Mais, en général, on a l'isomorphisme non trivial de $\mathbf{GO} / \mathbf{O} \times \mathbf{H}$ sur $M(\mathbb{Q}) / K^{*2}$.

THÉORÈME 2. *On peut prendre des semi-involutions orthogonales comme représentants du groupe quotient $\mathbf{GO}_{2m}(\mathbb{Q}) / \mathbf{O}_{2m}(\mathbb{Q}) \times \mathbf{H}$: Une similitude orthogonale u peut être écrite sous la forme $u = wh_\beta \prod_{i=1}^r w_i$, où $\mu_u = \alpha\beta^2$, α est un élément non carré dans K^* , w est une semi-involution orthogonale telle que $w^2 = h_\alpha$, et w_1, \dots, w_r sont des transvections orthogonales, $r \leq 2m$.*

Pour un élément u de \mathbf{GO} , en vertu du théorème 1, il existe une semi-involution w' dans \mathbf{GO} telle que $w'^2 = h_{\mu_u}$. Comme on a $Q(\mathbf{x})\mu_{w'^2} = Q(w'^2(\mathbf{x})) = Q(h_{\mu_u}(\mathbf{x})) = Q(\mathbf{x}\mu_u) = Q(\mathbf{x})\mu_u^2$ pour tout vecteur non singulier \mathbf{x} , on a $\mu_{w'} = \mu_u$. En conséquence, comme $\mu_{w'^{-1}u} = \mu_{w'}^{-1}\mu_u = \mu_u^{-1}\mu_u = 1$, $w'^{-1}u = u'$ appartient à \mathbf{O} . Soit $\mu_u = \alpha\beta^2$, α n'étant pas d'élément carré dans K^* . Si l'on pose $w = w'h_{\beta^{-1}}$, on a que $w \in \mathbf{GO}$ et que $\mu_w = \mu_{w'}\mu_{h_{\beta^{-1}}} = \mu_u\mu_{h_{\beta^{-1}}} = \alpha\beta^2 \cdot \beta^{-2} = \alpha$. On a alors que $w^2 = w'h_{\beta^{-1}}w'h_{\beta^{-1}} = w'^2h_{\beta^{-2}} = h_{\mu_u}h_{\beta^{-2}} = h_{\alpha\beta^2}h_{\beta^{-2}} = h_\alpha$. D'où u peut être écrit comme $u = w'u' = wh_\beta u'$ où $w^2 = h_\alpha$, $u' \in \mathbf{O}$. D'après le théorème de Cartan-Dieudonné, u' est produit de $2m$ transvections orthogonales au plus. On établit le théorème.

6. Dans le cas $K = F_2$, on a $GO = O$. Sauf pour $m = 2$, $\nu = 2$, le théorème de Cartan-Dieudonné est établi. Nous allons vérifier le cas $K = F_2$, $m = 2$, $\nu = 2$. Soit $u \in O$. D'après le cas I dans la démonstration de la proposition 1, s'il existe un vecteur singulier x tel que $f(x, u(x)) \neq 0$, il existe une transvection orthogonale v telle que $u_1 = vu$ laisse invariant x . Pour le cas II dans la proposition 1, comme on peut trouver une base symplectique composée de vecteurs singuliers, on a $f(e, u(e)) = 0$ pour tout vecteur de cette base. Alors, on peut appliquer le cas I-1 dans la démonstration du théorème 1 où la valeur de l'indice est indépendante du calcul. Par conséquent on constate que u est une involution orthogonale. Supposons maintenant que u ne soit pas d'involution orthogonale. Voyons le cas II-(iv) dans la démonstration de la proposition 2. Soient e_1, e'_1, w_1 et w_2 tels que $f(e_1, e'_1) = 1$, $u_2(e_1) = e_1$, $u_2(e'_1) = e'_1$, $u_2 = w_1w_2u_1$ ou $= w_1u_1$ et soit $\langle e_1, e_2, e'_1, e'_2 \rangle$ une base symplectique composée de vecteurs singuliers. Comme u_2 laisse invariant le plan non isotrope engendré par e_1 et e'_1 , u_2 laisse aussi invariant le plan engendré par e_2 et e'_2 , d'après le lemme 3. La matrice correspondant à u_2 par rapport à cette base doit être de la forme

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \beta \\ 0 & 0 & 1 & 0 \\ 0 & \gamma & 0 & \delta \end{pmatrix}, \quad \alpha, \beta, \gamma, \delta \in F_2. \quad \text{Comme } u_2 \in S_p, \text{ cette matrice doit satisfaire à (4):}$$

$\alpha\delta + \beta\gamma = 1$. Il y a six possibilités: (A) $\alpha = 0, \beta = 1, \gamma = 1, \delta = 1$; (B) $\alpha = 0, \beta = 1, \gamma = 1, \delta = 0$; (C) $\alpha = 1, \beta = 1, \gamma = 1, \delta = 0$; (D) $\alpha = 1, \beta = 0, \gamma = 1, \delta = 1$; (E) $\alpha = 1, \beta = 0, \gamma = 0, \delta = 1$; (F) $\alpha = 1, \beta = 1, \gamma = 0, \delta = 1$. Parmi ces six matrices, celles qui appartiennent à O sont les seules deux (B) et (E). On voit que (E) est la matrice d'unité et que (B) est la matrice correspondant à w_2 dans le cas II-(iv). Donc, u_2 est une transformation identique ou une involution orthogonale. Comme u peut être écrit $u = vw_2w_1u_2$ ou $= vw_1u_2$, donc $u = vw_2w_1w_2$, ou $= vw_2w_1$ ou $= vw_1w_2$ ou $= vw_1$. On voit facilement que $w_2w_1w_2$ est une involution orthogonale w_3 qui correspond

à la matrice $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$, et que w_1w_2 et w_2w_1 ne sont pas d'involutions or-

thogonales. On en conclut que tout u de O peut se représenter comme produit de trois involutions orthogonales au plus.⁵⁾

⁵⁾ Du fait que O est isomorphe au groupe alterné de degré 8, on peut aussi constater le résultat de ce numéro.

7. *Remarque 5.* Dans le cas de caractéristique $\neq 2$, peut-être l'énoncé du théorème 1 est aussi vrai.

BIBLIOGRAPHIE

- [1] J. Dieudonné: Sur les groupes classiques, Actual. Scient. et Ind., n°1040, Hermann, Paris (1948).
- [2] J. Dieudonné: La géométrie des groupes classiques, Springer, Berlin (1955).
- [3] C. Chevalley: The algebraic theory of spinors, Columbia Univ. Press, New York (1954).
- [4] E. Cartan: Leçons sur la théorie des spineurs I, Actual. Scient. et Ind., n°643, Hermann, Paris (1938).
- [5] M.J. Wonenburger: A decomposition of orthogonal transformations, Canad. Math. Bull. 7(3), 379–383(1964).

Université de la Préfecture d'Osaka