

BULLETIN de l'Association des Professeurs de Mathématiques de l'Enseignement Public



I. ÉTUDES

GROUPES CLASSIQUES *

1. LE GROUPE LINÉAIRE A n VARIABLES SUR UN CORPS K .

Soit $K^n = E$ l'espace vectoriel des vecteurs $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ à n composantes dans un corps K commutatif. Considérons la transformation

linéaire $\vec{x} \rightarrow \vec{x}' = A\vec{x}$ définie par :

$$\begin{cases} x'_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ x'_2 = a_{21}x_1 + \dots + a_{2n}x_n \\ \vdots \\ x'_n = a_{n1}x_1 + \dots + a_{nn}x_n \end{cases}$$

les coefficients a_{ij} appartenant au corps K .

Les transformations dont la matrice A a un déterminant non nul forment un groupe qu'on appelle le *groupe linéaire général à n variables défini sur K* , et qu'on note $GL_n(K)$.

En particulier, les transformations linéaires dont le déterminant vaut 1 forment un sous-groupe du précédent qu'on appelle le *groupe linéaire spécial à n variables*, ou *groupe unimodulaire* ; on le note $LS_n(K)$.

Les groupes que nous allons considérer ici, et qui sont devenus classiques depuis H. WEYL [1], sont tous des sous-groupes du groupe linéaire général, K étant le corps des nombres complexes ou celui R des nombres réels. Le cas d'un corps quelconque a fait l'objet de travaux plus récents dont les principaux résultats ont été rassemblés dans les livres de VAN DER WAERDEN [2 et 3] et J. DIEUDONNÉ [4 et 5].

2. TRANSFORMATIONS LINÉAIRES INVOLUTIVES.

Ce sont les transformations linéaires qui coïncident avec leur inverse ; c'est dire que leur matrice A vérifie :

$$A^2 = I, \text{ où } I \text{ désigne la matrice unité.}$$

D'après cette relation, $(\det A)^2 = 1$ et A est bien inversible.

(*) Conférence prononcée le 14 juin 1956 à l'Institut Henri-Poincaré, huitième conférence du cycle sur l'Algèbre organisé par la Société Mathématique de France en accord avec l'A.P.M., à l'intention spéciale des professeurs.

Les matrices ayant une structure d'anneau par rapport à l'addition et la multiplication, la relation $A^2 = I$ s'écrit :

$$A^2 - I = 0, \quad \text{ou } (A - I)(A + I) = 0.$$

Ceci conduit à considérer les vecteurs \vec{x} tels que :

$$(A - I)\vec{x} = 0, \quad \text{ou } A\vec{x} = \vec{x},$$

et les vecteurs \vec{y} tels que :

$$(A + I)\vec{y} = 0, \quad \text{ou } A\vec{y} = -\vec{y}.$$

Les premiers forment un sous-espace vectoriel V de E, et les derniers un sous-espace vectoriel W. Ces deux sous-espaces V et W n'ont aucun vecteur non nul commun, car :

$\vec{x} = \vec{y}$ entraîne $A\vec{x} = A\vec{y}$, c'est-à-dire $\vec{x} = -\vec{y}$, d'où $2\vec{x} = 0$, et $\vec{x} = 0$, cette division par 2 étant permise pour un corps quelconque de caractéristique différente de 2.

D'autre part, V et W engendrent l'espace E, c'est-à-dire que tout vecteur \vec{v} de E se met sous la forme :

$$\vec{v} = \vec{x} + \vec{y}, \quad \vec{x} \in \tilde{V} \quad \text{et} \quad \vec{y} \in \tilde{W};$$

en effet, il suffit d'écrire :

$$\vec{v} = \frac{1}{2}(\vec{v} + A\vec{v}) + \frac{1}{2}(\vec{v} - A\vec{v});$$

on vérifie que $\vec{v} + A\vec{v}$ appartient à V, car $A(\vec{v} + A\vec{v}) = A\vec{v} + \vec{v}$,

et que $\vec{v} - A\vec{v}$ appartient à W, car $A(\vec{v} - A\vec{v}) = A\vec{v} - \vec{v} = -(\vec{v} - A\vec{v})$.

Ces deux propriétés se notent sous la forme :

$$V \cap W = 0, \quad V \cup W = E \quad (1),$$

et s'expriment en disant que V et W sont *complémentaires*.

On a donc le théorème suivant :

THÉORÈME 1 : *A étant une transformation linéaire involutive, il existe deux sous-espaces complémentaires V et W tels que $A\vec{x} = \vec{x}$ pour tout vecteur de V et $A\vec{x} = -\vec{x}$ pour tout vecteur de W.*

Si V est de dimension p, W est de dimension n - p ; en choisissant un repère $\vec{e}_1, \dots, \vec{e}_p$ dans V et un repère $\vec{e}_{p+1}, \dots, \vec{e}_n$ dans W, les équations de la transformation prennent la forme :

$$(1) \quad \begin{cases} x'_1 = & x_1 \\ x'_2 = & x_2 \\ \vdots & \\ x'_p = & x_p \\ x'_{p+1} = & -x_{p+1} \\ \vdots & \\ x'_n = & -x_n \end{cases}$$

(1) Le signe \cup n'est pas le signe de réunion de la théorie des ensembles, mais le signe d'union de la théorie des treillis. (Cf. M.-L. DUBREIL-JACOTIN, L. LESIEUR, R. CROISOT : *Théorie des treillis*, 1953, pages 9 et 25, exemple 6).

Exemple dans E^3 .

$$\left\{ \begin{array}{l} x'_1 = x_1 \\ x'_2 = x_2 \\ x'_3 = -x_3 \end{array} \right. \quad (\text{symétrie par rapport au plan } \vec{e}_1, \vec{e}_2 \text{ parallèlement à } \vec{e}_3).$$

3. LE GROUPE ORTHOGONAL.

On appelle transformation orthogonale une transformation linéaire qui conserve la forme quadratique :

$$\varphi(\vec{x}) = x_1^2 + x_2^2 + \dots + x_n^2.$$

La matrice A correspondante est dite orthogonale. Pour qu'une matrice A soit orthogonale, il faut et il suffit qu'elle vérifie :

$$A^T A = I$$

en désignant par A^T la matrice transposée de A (matrice déduite de A par symétrie par rapport à la diagonale principale).

Vérifions-le pour $n = 2$. Les conditions pour que la transformation

$$\begin{array}{l} x'_1 = a_{11}x_1 + a_{12}x_2 \\ x'_2 = a_{21}x_1 + a_{22}x_2 \end{array} \quad \text{satisfasse à } x'_1{}^2 + x'_2{}^2 \equiv x_1^2 + x_2^2$$

quels que soient x_1 et x_2 , sont : $\begin{cases} a_{11}^2 + a_{21}^2 = 1, & a_{12}^2 + a_{22}^2 = 1 \\ a_{11}a_{12} + a_{21}a_{22} = 0 \end{cases}$

Ce sont celles qui expriment que :

$$A^T A = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{est la matrice unité } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On en déduit : $\det A = \pm 1$,

et, par suite, une matrice orthogonale est inversible. Son inverse est d'ailleurs sa transposée A qui vérifie aussi : $A A^T = 1$, et qui est donc aussi orthogonale.

Comme le produit de deux transformations orthogonales est une transformation orthogonale, on voit que les transformations orthogonales forment un groupe qu'on appelle le *groupe orthogonal* $O_n(K)$. On distingue les transformations orthogonales à déterminant $+1$ qui s'appellent *rotations* et qui forment le sous-groupe $O_n^+(K)$, et les transformations orthogonales à déterminant -1 qui s'appellent *retournements* (et naturellement qui ne forment pas un sous-groupe).

Le *groupe orthogonal réel* $O_n(R)$ correspondant au corps R des nombres réels est évidemment un sous-groupe de $O_n(K)$, si K est le corps des nombres complexes.

PROPRIÉTÉ : Une transformation orthogonale conserve le produit scalaire de deux vecteurs.

Le produit scalaire des vecteurs \vec{x} et \vec{y} est l'expression :

$$f(\vec{x}, \vec{y}) = x_1y_1 + x_2y_2 + \dots + x_ny_n,$$

forme bilinéaire symétrique des coordonnées des vecteurs.

En effet, cette forme s'écrit comme produit de matrices :

$$f(\vec{x}, \vec{y}) = (x_1 x_2 \dots x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = X^T \cdot Y$$

Par la transformation A, ceci devient (d'après l'associativité) :

$$(A X)^T \cdot A Y = (X^T A^T)(A Y) = X^T \cdot (A^T A) \cdot Y = X^T \cdot Y$$

Sous-espace conjugué d'un sous-espace V : C'est le sous-espace V^* des vecteurs \vec{y} tels que l'on ait :

$$f(\vec{x}, \vec{y}) = 0 \text{ pour tout } \vec{x} \in V.$$

C'est un sous-espace, car f est bilinéaire, et la relation est symétrique, de sorte que V est le conjugué de V^* .

Si V ne contient qu'un vecteur x , V^* est l'hyperplan orthogonal. Plus généralement, si V est de dimension p , V^* est de dimension $n - p$. (En effet, V étant défini par les p vecteurs indépendants $\vec{e}_1 \dots \vec{e}_p$, V^* est l'intersection des p hyperplans indépendants $f(\vec{e}_i, \vec{y}) = 0$, avec $i = 1, 2, \dots, p$).

Lorsque K est le corps des réels, on a $V \cap V^* = 0$ et les deux sous-espaces conjugués sont complémentaires. Il n'en est plus de même lorsque K est le corps des complexes ; dans ce cas, il existe des sous-espaces V tels que $V \cap V^* \neq 0$; on les appelle *sous-espaces isotropes*.

4. TRANSFORMATIONS INVOLUTIVES ORTHOGONALES.

Soit A une matrice involutive orthogonale (elle vérifie donc $A^2 = I$, d'où $A = A^{-1} = A^T$). C'est une transformation involutive particulière à laquelle s'applique le théorème 1. Nous allons préciser les résultats de ce théorème en montrant que V et W sont conjugués.

Le produit scalaire de $\vec{x} \in V$ et $\vec{y} \in W$ est :

$$f(\vec{x}, \vec{y}) = f(A\vec{x}, A\vec{y}) = f(\vec{x}, -\vec{y}) = -f(\vec{x}, \vec{y}),$$

d'où $2f(\vec{x}, \vec{y}) = 0$ et $f(\vec{x}, \vec{y}) = 0$ pour un corps K de caractéristique différente de 2.

Il en résulte $\vec{y} \in V^*$, donc $W \leq V^*$. Mais W et V ont la même dimension $n - p$, et par suite $W = V^*$. Ainsi, V et W sont bien conjugués.

On sait d'ailleurs que $V \cap W = 0$; donc $V \cap V^* = 0$, et par suite V est non isotrope. Il en est de même de W . D'où :

THÉORÈME 2 : *A étant une transformation orthogonale involutive, il existe un sous-espace non isotrope V (pouvant être réduit à 0), tel que $A\vec{x} = \vec{x}$ pour tous les vecteurs de V et $A\vec{x} = -\vec{x}$ pour tous les vecteurs du sous-espace conjugué V^* .*

En prenant un repère orthonormé (1) dans V et un repère orthonormé dans W , on obtient alors un repère orthonormé dans E tel que les équations de la transformation prennent la forme (1). La transformation est une rotation ou un retournement suivant que $n - p$ est pair ou impair.

(1) C'est-à-dire constitué de vecteurs \vec{e}_i tels que $f(\vec{e}_i, \vec{e}_j) = 0$ si $i \neq j$
 $= 1$ si $i = j$

5. SYMÉTRIES.

En particulier, lorsque V est de dimension $n - 1$, la transformation orthogonale involutive laisse invariant V . Elle s'appelle *symétrie par rapport à l'hyperplan* V (que nous savons ne pas être isotrope). Le théorème connu de géométrie élémentaire sur la génération du groupe orthogonal au moyen des symétries a été généralisé pour n quelconque dans le cas du corps K des complexes ou R des réels par Elie CARTAN [6] et par J. DIEUDONNÉ pour un corps quelconque de caractéristique différente de 2. C'est la propriété suivante :

THÉORÈME 3 : *Toute transformation orthogonale à n variables est un produit de n symétries au plus.*

Démontrons-le pour le corps des réels par récurrence sur n . La propriété est immédiate pour $n = 1$. Supposons-la vraie pour $n - 1$. S'il existe un vecteur $\vec{x} \neq 0$ tel que $A\vec{x} = \vec{x}$, A laisse invariant globalement l'hyperplan H conjugué de \vec{x} , et la restriction de A à H est une transformation orthogonale produit de $n - 1$ symétries au plus. Celles-ci définissent des symétries dans E , en nombre $n - 1$ au plus. Si aucun vecteur différent de 0 n'est invariant, on considère un vecteur quelconque \vec{x}_0 , d'où $A\vec{x}_0 \neq \vec{x}_0$, qui vérifie :

$$\varphi(\vec{x}_0) = f(\vec{x}_0, \vec{x}_0) = \varphi(A\vec{x}_0).$$

L'hyperplan d'équation $f(\vec{x}, \vec{x}_0 - A\vec{x}_0) = 0$ définit une symétrie S qui transforme \vec{x}_0 en $A\vec{x}_0 \neq 0$. La transformation produit S_0A laisse invariant \vec{x}_0 , donc est le produit de $n - 1$ symétries au plus. Il en résulte que A est le produit de n symétries au plus.

6. LE GROUPE UNITAIRE.

Reprenant l'espace $E = K^n$ où K est le corps des complexes, on considère cette fois la forme hermitienne :

$$\varphi(\vec{x}) = x_1\bar{x}_1 + x_2\bar{x}_2 + \dots + x_n\bar{x}_n,$$

où \bar{x}_i désigne le nombre complexe conjugué de x_i . Les transformations unitaires sont les transformations linéaires qui conservent $\varphi(\vec{x})$. Leur matrice A vérifie la relation :

$$\bar{A}^T \cdot A = I,$$

en désignant par \bar{A}^T la matrice transposée de la conjuguée de A . La matrice A est donc inversible ; son inverse est \bar{A}^T qui vérifie $A\bar{A}^T = I$, et qui est donc aussi une matrice hermitienne. Le produit de deux transformations unitaires étant également unitaire, les transformations unitaires forment un groupe : *le groupe unitaire* $U_n(K)$.

Une transformation unitaire laisse invariante l'expression :

$$f(\vec{x}, \vec{y}) = \sum_{i=1}^n x_i \bar{y}_i$$

qu'on appelle *produit scalaire hermitien* des vecteurs \vec{x} et \vec{y} ; c'est une forme bilinéaire des deux vecteurs ; elle n'est pas symétrique, mais elle vérifie :

$$f(\vec{x}, \vec{y}) = \overline{f(\vec{y}, \vec{x})},$$

de sorte que les conditions $f(\vec{x}, \vec{y}) = 0$ et $f(\vec{y}, \vec{x}) = 0$ sont équivalentes. Ces propriétés permettent de définir la notion de sous-espaces V et V^* conjugués et d'étendre au groupe unitaire le théorème 3 pour obtenir la structure d'une transformation unitaire quelconque.

Les transformations unitaires de déterminant égal à 1 forment un sous-groupe du groupe unitaire et du groupe spécial linéaire : *le groupe unitaire spécial* $US_n(K)$.

7. LE GROUPE SYMPLECTIQUE.

Supposons paire la dimension de l'espace E : $n = 2m$. Les coordonnées d'un vecteur \vec{x} seront : $x_1, x'_1, x_2, x'_2, \dots, x_m, x'_m$.

A deux vecteurs \vec{x} et \vec{y} nous associons :

$$f(\vec{x}, \vec{y}) = x_1 y'_1 - x'_1 y_1 + x_2 y'_2 - x'_2 y_2 + \dots + x_m y'_m - x'_m y_m ;$$

c'est une *forme bilinéaire alternée* des deux vecteurs :

$$f(\vec{y}, \vec{x}) = -f(\vec{x}, \vec{y}).$$

On appelle transformation symplectique une transformation linéaire qui conserve $f(x, y)$. Elle est donc définie par :

$$f(\vec{x}, \vec{y}) = f(A\vec{x}, A\vec{y}).$$

La matrice A est dite symplectique. Le produit de deux transformations symplectiques est une transformation symplectique. Pour démontrer que ces transformations forment un groupe, montrons qu'elles sont inversibles.

Dans le cas $n = 2$, les transformations ne sont autres que celles qui conservent les aires orientées, donc celles du groupe linéaire spécial $LS_2(K)$. Dans le cas général $n = 2m$, considérons les vecteurs colonnes de la matrice A , c'est-à-dire :

$$\vec{\alpha}_1 = A\vec{e}_1, \vec{\alpha}'_1 = A\vec{e}'_1, \dots, \vec{\alpha}_m = A\vec{e}_m, \vec{\alpha}'_m = A\vec{e}'_m.$$

Des relations : $f(\vec{e}_i, \vec{e}_j) = 0$, $f(\vec{e}_i, \vec{e}'_j) = \delta_{ij}$, $f(\vec{e}'_i, \vec{e}'_j) = 0$ (où δ_{ij} vaut 1 pour $i = j$ et 0 pour $i \neq j$), l'on déduit :

$$f(\vec{\alpha}_i, \vec{\alpha}_j) = 0, f(\vec{\alpha}_i, \vec{\alpha}'_j) = \delta_{ij}, f(\vec{\alpha}'_i, \vec{\alpha}'_j) = 0.$$

Ce sont des conditions nécessaires et suffisantes pour que A soit symplectique. Or, les vecteurs $\vec{\alpha}_1, \vec{\alpha}'_1, \dots, \vec{\alpha}_m, \vec{\alpha}'_m$ sont indépendants, car, s'il existait des λ tels que $\vec{x} = \lambda_1 \vec{\alpha}_1 + \lambda'_1 \vec{\alpha}'_1 + \dots + \lambda_m \vec{\alpha}_m + \lambda'_m \vec{\alpha}'_m$ soit nul, on en déduirait $f(\vec{x}, \vec{\alpha}'_1) = \lambda_1 = 0$, et de même $\lambda_i = \lambda'_i = 0$ pour tout i . Donc, la matrice A est inversible ; mais son inverse conserve aussi $f(\vec{x}, \vec{y})$, donc est symplectique. Ainsi, *les transformations symplectiques forment un groupe*, qu'on appelle *le groupe symplectique* $S_p(n, K)$.

On définit encore, comme pour le groupe orthogonal, la notion de

sous-espaces conjugués V et V^* , ainsi que celle de sous-espaces isotropes V tel que $V \cap V^* \neq 0$.

Transformations symplectiques involutives : Le théorème 2 s'étend au groupe symplectique en utilisant la même démonstration. Mais nous pouvons donner une précision supplémentaire : *Les espaces V et W qui interviennent dans la structure d'une transformation symplectique involutive sont de dimension paire.*

En effet, V et W sont non isotropes et un sous-espace de dimension impaire ne peut être qu'isotrope. Un tel espace U , défini par un repère $\vec{e}_1, \dots, \vec{e}_{2p+1}$, contient en effet un vecteur non nul :

$$\vec{x} = \lambda_1 \vec{e}_1 + \dots + \lambda_{2p+1} \vec{e}_{2p+1}$$

appartenant à son conjugué, car le système de $2p + 1$ équations homogènes :

$$f(\vec{x}, \vec{e}_i) = \lambda_1 f(\vec{e}_1, \vec{e}_i) + \dots + \lambda_{2p+1} f(\vec{e}_{2p+1}, \vec{e}_i), \text{ pour } i = 1, 2, \dots, 2p+1,$$

a un déterminant antisymétrique d'ordre impair, donc nul ; il existe alors une solution non nulle $\lambda_1, \lambda_2, \dots, \lambda_{2p+1}$ du système, qui donne un vecteur \vec{x} non nul.

En particulier, tout vecteur est isotrope, de même que tout hyperplan.

8. TRANSVECTION SYMPLECTIQUE.

Ce qui précède montre qu'il n'y a pas de « symétrie » symplectique, mais on peut aussi considérer une symétrie orthogonale comme une transformation orthogonale qui laisse invariants les vecteurs d'un hyperplan, et se proposer de même de chercher les transformations symplectiques qui laissent invariants les vecteurs d'un hyperplan.

Soit A une telle transformation, H un hyperplan, \vec{x}_0 un vecteur non situé dans H ; à tout vecteur \vec{x} correspond un vecteur \vec{h} de H tel que $\vec{x} = \vec{h} + r(\vec{x})\vec{x}_0$, d'où $A\vec{x} = \vec{h} + r(\vec{x})A\vec{x}_0$, et, par soustraction :

$$A\vec{x} - \vec{x} = r(\vec{x})\vec{a}, \text{ avec } \vec{a} = A\vec{x}_0 - \vec{x}_0.$$

Ce vecteur \vec{a} est conjugué de H , car, quel que soit un vecteur \vec{e} de H , $f(\vec{a}, \vec{e}) = f(A\vec{x}_0 - \vec{x}_0, \vec{e}) = f(A\vec{x}_0, \vec{e}) - f(\vec{x}_0, \vec{e}) = 0$, par définition de A . Mais, tout vecteur étant isotrope, ceci entraîne que \vec{a} appartient à H . Ainsi, pour toute transformation A , il existe un vecteur \vec{a} conjugué de H et un vecteur \vec{x}_0 n'appartenant pas à H , tels que

$\vec{x} = \vec{h} + r(\vec{x})\vec{x}_0$, $A\vec{x} = \vec{x} + r(\vec{x})\vec{a}$. Ces formules définissent la transformation cherchée. Réciproquement, la transformation définie par ces formules, dans lesquelles \vec{x}_0 n'est pas dans H et où \vec{a} est le conjugué de H , est bien une transformation symplectique conservant tout vecteur de H , car : $f(A\vec{x}, A\vec{y}) = f(\vec{x}, \vec{y}) + r(\vec{y})f(\vec{x}, \vec{a}) + r(\vec{x})f(\vec{a}, \vec{y}) = f(\vec{x}, \vec{y})$.

Soient $2m - 1$ vecteurs \vec{e}_i formant un repère de H (nous prenons $\vec{e}_1 = \vec{a}$) et un vecteur \vec{e}_{2m} hors de H (nous prenons $\vec{e}_{2m} = \vec{x}_0$) ; les for-

mules précédentes donnent : $\vec{h} = \vec{x}_1 \vec{e}_1 + \dots + \vec{x}_{2m-1} \vec{e}_{2m-1}$, $r(\vec{x}) = \vec{x}_{2m}$;
donc, pour les coordonnées de $A\vec{x}$:

$$X_1 = x_1 + x_{2m}, X_2 = x_2, \dots, X_{2m-1} = x_{2m-1}, X_{2m} = x_{2m}.$$

La transformation obtenue se nomme *transvection symplectique* d'hyperplan H. Les équations écrites prouvent que le déterminant de A vaut 1.

L'on peut déterminer une transvection symplectique qui applique un vecteur donné \vec{x}_0 sur un vecteur donné \vec{y}_0 tel que $f(\vec{x}_0, \vec{y}_0) \neq 0$. En effet, d'après ce qui précède, l'hyperplan H doit être le conjugué de $\vec{y}_0 - \vec{x}_0$. Cet hyperplan ne contient pas \vec{x}_0 et A est défini par :

$$\vec{x} = \vec{h} + r(\vec{x})\vec{x}_0, \quad A\vec{x} = \vec{h} + r(\vec{x})\vec{y}_0.$$

9. GÉNÉRATION DU GROUPE SYMPLECTIQUE.

THÉORÈME 4 : *Toute transformation symplectique A est le produit de transvections symplectiques en nombre fini.*

Supposons d'abord que l'on ait, pour tout \vec{x} , $f(\vec{x}, A\vec{x}) = 0$. Alors A est une involution, car, de la relation : $f[\vec{x} + \vec{y}, A(\vec{x} + \vec{y})] = 0$, on tire : $f(\vec{x}, A\vec{y}) = f(A\vec{x}, \vec{y}) = f(A\vec{x}, A^2\vec{y})$, et, comme le vecteur $A\vec{x}$ est quelconque, $A^2\vec{y} = \vec{y}$, quel que soit \vec{y} , donc $A^2 = I$. La réciproque résulte de $f(\vec{x}, \vec{y}) = -f(\vec{y}, \vec{x})$. D'où l'énoncé :

LEMME 1 : *Si $f(\vec{x}, A\vec{x}) = 0$ pour tout \vec{x} , A est une involution, et réciproquement.*

On peut dans ce cas considérer les deux sous-espaces V et $W = V^*$ qui interviennent dans la structure d'une transformation symplectique involutive. En supposant $A \neq I$, on a $W \neq 0$. Comme W est de dimension paire et est non isotrope, on peut trouver deux vecteurs \vec{x}_0 et \vec{y}_0 dans W tels que $f(\vec{x}_0, \vec{y}_0) \neq 0$. De $A\vec{x}_0 = -\vec{x}_0$ (qui exprime $\vec{x}_0 \in W$), on déduit $f(A\vec{x}_0, \vec{y}_0) \neq 0$, et il existe une transvection symplectique T transformant $A\vec{x}_0$ en \vec{y}_0 . De même, $f(\vec{y}_0, \vec{x}_0) \neq 0$ entraîne l'existence d'une transvection symplectique T' transformant \vec{y}_0 en \vec{x}_0 . Il en résulte que T' T A laisse \vec{x}_0 invariant.

Nous allons montrer que, dans le cas général, ce résultat est encore vrai :

LEMME 2 : *A étant une transformation symplectique, il existe deux transvections symplectiques T et T' telles que T' T A laisse invariant au moins un vecteur \vec{x}_0 .*

La propriété vient d'être démontrée si A est involutive. Sinon, d'après le lemme 1, il existe au moins un vecteur \vec{x}_0 tel que $f(\vec{x}_0, A\vec{x}_0) \neq 0$. Il y a donc une transvection symplectique T transformant $A\vec{x}_0$ en \vec{x}_0 , de sorte que le produit T A laisse \vec{x}_0 invariant.

Soit donc B une transformation symplectique laissant invariant un vecteur \vec{x}_0 .

a) Supposons d'abord qu'il existe un vecteur \vec{y}_0 tel que :

$$f(\vec{x}_0, \vec{y}_0) \neq 0, \text{ et } f(\vec{y}_0, \vec{B}\vec{y}_0) \neq 0.$$

Il existe une transvection symplectique T_1 transformant $\vec{B}\vec{y}_0$ en \vec{y}_0 , et le produit $T_1 B$ laisse invariant \vec{y}_0 . Le vecteur \vec{x}_0 est aussi invariant par ce produit. Pour le montrer, il suffit de vérifier qu'il est dans l'hyperplan invariant de la transvection T_1 , c'est-à-dire qu'il est conjugué du vecteur $\vec{B}\vec{y}_0 - \vec{y}_0$. Ceci résulte des égalités :

$$f(\vec{x}_0, \vec{B}\vec{y}_0 - \vec{y}_0) = f(\vec{x}_0, \vec{B}\vec{y}_0) - f(\vec{x}_0, \vec{y}_0) = f(\vec{B}\vec{x}_0, \vec{B}\vec{y}_0) - f(\vec{x}_0, \vec{y}_0) = 0.$$

Nous venons, non seulement de démontrer, dans le cas envisagé, le lemme 2, mais l'énoncé plus complet :

LEMME 3 : *S'il existe un vecteur \vec{y}_0 tel que $f(\vec{x}_0, \vec{y}_0) \neq 0$ et $f(\vec{y}_0, \vec{B}\vec{y}_0) \neq 0$, il existe un produit de transvections symplectiques dont le produit par A laisse invariants deux vecteurs \vec{x}_0 et \vec{y}_0 .*

b) Supposons maintenant que, pour tout vecteur \vec{y}_0 tel que $f(\vec{x}_0, \vec{y}_0) \neq 0$, l'on ait $f(\vec{y}_0, \vec{B}\vec{y}_0) = 0$. On utilisera une transvection symplectique qui transforme $\vec{B}\vec{y}_0$, non plus en \vec{y}_0 , mais en $\vec{x}_0 + \vec{y}_0$. Cette transformation T existe bien, puisque :

$$f(\vec{B}\vec{y}_0, \vec{x}_0 + \vec{y}_0) = f(\vec{B}\vec{y}_0, \vec{x}_0) = f(\vec{y}_0, \vec{x}_0) \neq 0.$$

Alors, le produit $T.B = C$ transforme \vec{y}_0 en $\vec{x}_0 + \vec{y}_0$, avec :

$$f(\vec{y}_0, \vec{C}\vec{y}_0) = f(\vec{y}_0, \vec{x}_0 + \vec{y}_0) = f(\vec{y}_0, \vec{x}_0) \neq 0.$$

C laisse du reste \vec{x}_0 invariant, car \vec{x}_0 appartient à l'hyperplan invariant de la transvection, puisque l'on a :

$$f(\vec{x}_0, \vec{B}\vec{y}_0 - \vec{x}_0 - \vec{y}_0) = f(\vec{x}_0, \vec{B}\vec{y}_0) - f(\vec{x}_0, \vec{y}_0) = 0.$$

Les deux vecteurs \vec{x}_0 et \vec{y}_0 sont donc tels que :

$$f(\vec{x}_0, \vec{y}_0) \neq 0 \text{ et } f(\vec{y}_0, \vec{C}\vec{y}_0) \neq 0.$$

Ce sont les conditions d'application du lemme 3, d'où l'énoncé :

LEMME : *A étant une transformation symplectique quelconque, il existe un produit de transvections symplectiques dont le produit par A laisse invariant deux vecteurs \vec{x}_0 et \vec{y}_0 tels que $f(\vec{x}_0, \vec{y}_0) \neq 0$.*

De cet énoncé, on déduit le théorème 4 de la façon suivante : Soit P le plan déterminé par \vec{x}_0 et \vec{y}_0 supposés invariants par C et tels que $f(\vec{x}_0, \vec{y}_0) \neq 0$. Ce plan n'est pas isotrope, et le sous-espace P^* conjugué de P est complémentaire de P ; or, il est de dimension $2m - 2$. La transformation C laisse P^* invariant et sa restriction à ce sous-ensemble est une transformation symplectique que l'on étudie comme plus haut. Si cette restriction est un produit de transvections symplectiques, comme toute transvection symplectique de ce sous-espace est la restriction d'une

transvection symplectique de E , le théorème sera démontré. Or, par induction sur m , on est ramené à l'espace de dimension 2, et le lemme permet de conclure dans ce cas. Le théorème est donc démontré.

Comme conséquence du théorème 4, on remarque que le déterminant de toute transformation symplectique est égal à 1. C'est dire que le groupe symplectique $S_p(n, K)$ est un sous-groupe du groupe linéaire spécial $LS_n(K)$.

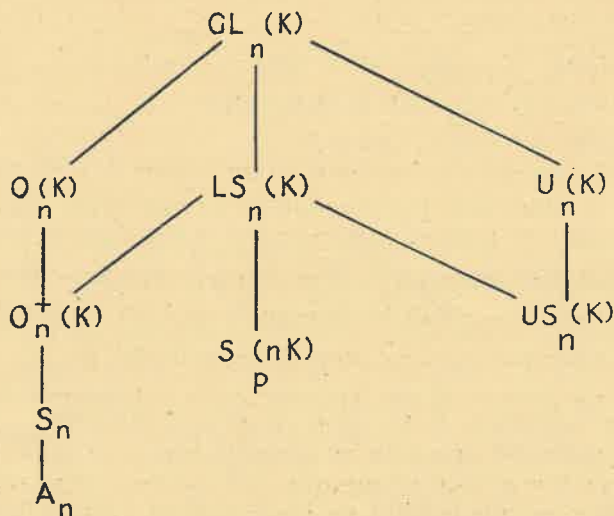
10. LE GROUPE SYMÉTRIQUE.

On appelle *groupe symétrique* S_n le groupe des *substitutions* d'un ensemble fini de n éléments. C'est donc un groupe fini possédant $n!$ éléments. Il peut être réalisé par des transformations linéaires de K^n ; en effet, on a par exemple, en considérant l'ensemble de trois éléments (x_1, x_2, x_3) , la substitution $\{x_1, x_2, x_3\} \rightarrow \{x_3, x_2, x_1\}$ réalisée par :

$$\begin{pmatrix} x_3 \\ x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

et représentée par une matrice n'ayant dans toute ligne et colonne qu'un élément non nul, cet élément étant égal à 1. Cette remarque vaut quel que soit n . Il en résulte que le groupe S_n peut être considéré comme un sous-groupe du groupe orthogonal; les rotations de ce groupe, en nombre $1/2 n!$, correspondent aux substitutions paires et forment un sous-groupe de S_n : le *groupe alterné* A_n .

On pourra trouver une étude sommaire de ce groupe, ainsi que des indications sur la *théorie de la représentation* et ses applications à la physique dans [7]. Des applications du groupe orthogonal et du groupe unitaire au calcul opérationnel se trouvent dans [8]. Quelques exercices sont proposés ici après la bibliographie. Indiquons pour terminer le diagramme des groupes rencontrés dans cette conférence :



L. LESIEUR,

Professeur à la Faculté des Sciences de Poitiers.

BIBLIOGRAPHIE

- [1] H. WEYL. — *The classical groups* (Princeton, 2^e édition, 1946).
- [2] B. L. VAN DER WAERDEN. — *Die Gruppentheoretische Methode in der Quantenmechanik* (Ergebnisse der Math., 1932).
- [3] B. L. VAN DER WAERDEN. — *Gruppen von linearen transformationen* (Ergebnisse der Mathematik, 1935).
- [4] J. DIEUDONNÉ. — *Sur les groupes classiques* (Paris, Hermann, 1948).
- [5] J. DIEUDONNÉ. — *La géométrie des groupes classiques* (Ergebnisse der Mathematik, 1955).
- [6] E. CARTAN. — *Leçons sur la théorie des spineurs* (Act. Sc. et Ind., n° 643, p. 13-17).
- [7] *Conférences du Séminaire de Mathématiques de la Faculté des Sciences de Poitiers* (1954-1955).
- [8] M. JANET. — *Précis de Calcul matriciel et opérationnel* (Hrresses Universitaires, Collection Euclide, 1954).

EXERCICES

1. R étant un retournement, il existe toujours un vecteur $\vec{x} \neq 0$ tel que $R\vec{x} = -\vec{x}$. Autre forme : -1 est une valeur propre de la matrice d'un retournement quelconque.

2. Si n est impair, une rotation possède toujours un axe de points invariants passant par l'origine. Autre forme : $+1$ est une valeur propre de la matrice d'une rotation quelconque lorsque n est impair.

3. Montrer que les valeurs propres d'une matrice orthogonale, c'est-à-dire les racines de l'équation $\det(A - sI) = 0$, ont toutes un module égal à 1.

4. Soient V et V^* les sous-espaces intervenant dans la structure d'une transformation orthogonale involutive (théorème 2). Lorsque V^* est de dimension 2, donc V de dimension $n - 2$, on obtient une rotation qu'on appelle *renversement* d'axe V . Montrer que toute rotation est un produit de renversements lorsque $n > 2$.

5. Avec les notations de l'exercice précédent, si V est une droite et V^* un hyperplan, on obtient une rotation ou un retournement suivant que n est impair ou pair, qu'on appelle *transposition* d'axe V . Montrer que si n est impair, toute rotation est un produit de transpositions ; si n est pair, tout retournement est un produit de transpositions ($n \geq 3$).

6. Montrer que toutes les matrices du groupe unitaire spécial sont données pour $n = 2$ par $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, où les nombres complexes a et b vérifient $a\bar{a} + b\bar{b} = 1$.

7. Soit J la matrice carrée d'ordre $2m$ constituée par m blocs $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ situés sur la diagonale principale ; par exemple :

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

Montrer que la condition nécessaire et suffisante pour qu'une matrice A soit symplectique est :

$$A^T J A = J.$$

8. Montrer que les conditions nécessaires et suffisantes pour qu'une transformation soit à la fois symplectique et involutive peuvent se mettre sous la forme :

$$A^2 = I, A^T J = J A,$$

J étant la matrice de l'exercice 7.

9. On appelle base (ou repère) symplectique, dans $E = K^m$ de base $\vec{e}_1, \vec{e}'_1, \vec{e}_2, \vec{e}'_2, \dots, \vec{e}_m, \vec{e}'_m$ ($n = 2m$), toute base $A\vec{e}_i$ ($i = 1, \dots, 2m$) déduite des \vec{e}_j et \vec{e}'_j par une transformation symplectique. Montrer que si \vec{x}_1 et \vec{x}'_1 sont deux vecteurs quelconques tels que $f(\vec{x}_1, \vec{x}'_1)$ ne soit pas nul, il existe une base symplectique dont les deux premiers vecteurs sont \vec{x}_1 et \vec{x}'_1 .

10. Montrer que la matrice $\begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix}$ est celle d'une transvection symplectique ($n = 2$). Vérifier que $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est le produit des trois transvections symplectiques $\begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

La transformation symplectique $-I$ peut-elle être le produit de deux transvections symplectiques seulement ?