Sur une généralisation du groupe orthogonal à quatre variables

Par JEAN DIEUDONNÉ à Nancy

1. On sait que les groupes orthogonaux à quatre variables sur un corps commutatif *quelconque* K ont une structure tout à fait distincte de celle des groupes orthogonaux à n variables, pour $n > 2$ et $n \neq 4$ ([2], p. 18—26). On peut rattacher ce phénomène au fait que le groupe linéaire à 4 variables qui, dans l'espace vectoriel K^4, laisse invariant le cône d'équation $\xi_1 \xi_4 - \xi_2 \xi_3 = 0$, est quotient par un groupe abélien du produit de deux groupes linéaires $\mathbf{GL}_2(K)$ (loc. cit.). Nous nous proposons de montrer dans ce qui suit que ce résultat est un cas particulier d'un théorème qui caractérise toute une famille de groupes linéaires, le groupe orthogonal précité apparaissant en quelque sorte comme l'intersection de cette famille et de la famille des groupes orthogonaux à n variables.

De façon précise, soit $n \geqslant 1$ un entier quelconque, et considérons, dans l'espace vectoriel K^{n^2}, que nous identifierons à l'ensemble des *matrices carrées d'ordre* n, $X = (x_{ij})$, à éléments dans K, le cône Σ_n d'équation $\det(X) = 0$; soit Γ_n le groupe de toutes les transformations linéaires à n^2 variables [sous-groupe de $\mathbf{GL}_{n^2}(K)$] qui laissent invariant Σ_n. Nous nous proposons de montrer que Γ_n est identique au groupe des transformations de la forme

$$X \to PXQ \tag{1}$$

ou de la forme

$$X \to P \cdot {}^tX \cdot Q \tag{2}$$

où P et Q sont deux matrices inversibles quelconques d'ordre n, et où ${}^tX$ désigne la matrice *transposée* de X.

2. Comme pour le cas classique $n = 2$, notre démonstration reposera, dans le cas général, sur l'étude des *sous-espaces vectoriels de dimension maximale* contenus dans le cône Σ_n. On aperçoit aussitôt dans Σ_n des sous-espaces vectoriels de dimension $n^2 - n$, savoir l'ensemble des matrices ayant une ligne (ou une colonne) nulle. Plus généralement, considérons l'ensemble M_n des matrices carrées d'ordre n sur K comme l'anneau des endomorphismes de l'espace vectoriel $E = K^n$. Il est bien connu que, dans M_n, un *idéal maximal à gauche* $\mathfrak{l}$ est formé des endomorphismes u de E qui s'annulent dans un sous-espace donné à 1 dimension de E, et un *idéal maximal à droite* $\mathfrak{r}$ est formé des endomorphismes u tels que $u(E)$ soit contenu

dans un hyperplan donné de E (voir par exemple [1], p. 64—65); il est clair qu'il existe une matrice carrée inversible P telle que $\mathfrak{l}P$ soit formé des matrices ayant leur première colonne nulle, et une matrice carrée inversible Q telle que $Q\mathfrak{r}$ soit formé des matrices ayant leur première ligne nulle.

Théorème 1. — *Tout sous-espace vectoriel contenu dans Σ_n a une dimension au plus égale à $n^2 - n$, et les seuls sous-espaces de dimension $n^2 - n$ sont les idéaux maximaux (à gauche et à droite) de M_n.*

Nous déduirons le th. 1 d'un théorème plus précis:

Théorème 2. — *Toute variété linéaire contenue dans Σ_n a une dimension au plus égale à $n^2 - n$; en outre, sauf dans le cas où $n = 2$ et où K est un corps à 2 éléments, les seules variétés linéaires de dimension $n^2 - n$ contenues dans Σ_n sont les idéaux maximaux de M_n.*

Soit $X_0 + V$ une variété linéaire contenue dans Σ_n, V étant le sous-espace vectoriel parallèle à cette variété linéaire. Désignons par E_{ij} $(1 \leqslant i, j \leqslant n)$ la matrice dont le seul élément non nul est dans la i-ème ligne et la j-ème colonne et est égal à 1; les E_{ij} forment la *base canonique* de l'espace $M_n = K^{n^2}$; soit $n^2 - m$ la dimension de V; d'après le théorème d'échange, il existe un ensemble J de m couples (i, j) tels que les E_{ij} correspondant à ces couples forment la base d'un sous-espace W supplémentaire de V; on peut en outre supposer prise dans V une base de $n^2 - m$ matrices A_{hk} correspondant aux couples (h, k) non dans J, et telles que A_{hk} se projette sur E_{hk} parallèlement à W; en d'autres termes $A_{hk} = E_{hk} + \sum_{(i,j) \in J} \alpha_{hk,\,ij} E_{ij}$. Les matrices X appartenant à $X_0 + V$ peuvent donc être caractérisées de la façon suivante: ce sont les matrices $X = (x_{ij})$, où les x_{hk} correspondant aux couples (h, k) non dans J sont *arbitraires* dans K, et où les x_{ij} correspondant aux couples $(i, j) \in J$ sont des fonctions linéaires non homogènes des x_{hk}, soit $x_{ij} = \sum_{h,k} \alpha_{hk,\,ij} x_{hk} + \beta_{ij}$.

a) Montrons d'abord, par récurrence sur n, que l'on ne peut avoir $m < n$; la proposition est évidente pour $n = 1$. Raisonnons par l'absurde et supposons que J ait $m < n$ éléments; il existe alors une ligne de X ne contenant aucun des x_{ij} $[(i, j) \in J]$. Par une permutation des lignes et des colonnes [qui revient à effectuer sur les éléments de Σ_n une transformation (1)], on peut supposer que c'est la première ligne de X et que dans la première colonne de X il y a au moins un x_{ij} d'indices $(i, j) \in J$. Faisons alors $x_{11} = 1$, $x_{1k} = 0$ pour $k > 1$; il vient $\det X = \det X'$, où X' est la matrice carrée d'ordre $n - 1$ obtenue en supprimant la première ligne et la première colonne de X. Par hypothèse, on aurait $\det X' = 0$ quand on donne aux x_{hk} d'indices (h, k) non dans J et > 1 des valeurs arbitraires; or ceci est contraire à l'hypothèse de récurrence, puisqu'il y a au plus $m - 1$ des couples $(i, j) \in J$ tels que $i > 1$ et $j > 1$.

b) Pour établir la seconde partie du th. 2, supposons d'abord que K ait au moins 3 éléments. Pour $n = 2$, les identités

$$\begin{vmatrix} a\,x + b\,y + c & x \\ a'x + b'y + c' & y \end{vmatrix} = 0 \qquad \begin{vmatrix} \alpha\,x + \beta\,y + \gamma & x \\ y & \alpha'\,x + \beta'\,y + \gamma' \end{vmatrix} = 0$$

ne sont possibles que si $b = c = a' = c' = 0$ et $a = b'$ dans la première identité, et $\beta = \gamma = \alpha' = \gamma' = 0$, $\alpha\,\beta' = 1$, ou $\alpha = \gamma = \beta' = \gamma' = 0$, $\alpha'\,\beta = 1$ dans la seconde (comme on le voit en faisant successivement $x = 0$ et $y = 0$); il est immédiat de voir que dans les deux cas, on définit de la sorte un idéal maximal de M_2. Procédons alors par récurrence sur $n \geqslant 3$; J ayant n éléments, il peut se faire d'abord qu'il y ait exactement un élément de J dans chaque ligne et dans chaque colonne; par une transformation (1) sur Σ_n, on peut supposer que J soit identique aux couples d'indices (i, i) de la diagonale principale. Il peut alors se produire a priori plusieurs cas:

1) il existe un couple (h, k) où $h \neq k$ et un indice i tels que $\alpha_{hk,\,ii} \neq 0$; on peut alors exprimer x_{hk} en fonction linéaire (non homogène) de x_{ii} et des autres éléments $x_{h'k'}$ $(h' \neq k')$; les matrices de $X_0 + V$ ont alors leurs éléments arbitraires pour les couples d'indices distincts de ceux d'une partie J' de n éléments qui cette fois n'a pas d'élément dans la ligne (ou la colonne) d'indice i; nous sommes alors ramenés au cas qui sera examiné plus loin;

2) tous les $\alpha_{hk,\,ii}$ sont nuls; donnons alors aux x_{hk} des valeurs nulles, sauf pour $1 \leqslant h \leqslant n-1$, $k = h+1$, et $h = n$, $k = 1$; l'équation $\det X = 0$ s'écrit

$$x_{n1}\,x_{12}\,x_{23}\ldots x_{n-1,n} + (-1)^{n-1}\,\beta_{11}\,\beta_{22}\ldots\beta_{nn} = 0$$

qui visiblement ne peut être une identité par rapport aux x_{hk} qui y figurent.

Nous sommes ramenés ainsi au cas où une ligne (ou une colonne) ne contient aucun élément de J; supposons par exemple que ce soit la première colonne; en outre, on peut toujours supposer que la première ligne contient au moins un élément de J. Faisons alors $x_{11} = 1$, $x_{h1} = 0$ pour $2 \leqslant h \leqslant n$; l'équation $\det X = 0$ devient $\det Y_1 = 0$, où Y est la matrice d'ordre $n-1$ obtenue en supprimant dans X la première ligne et la première colonne, et Y_1 la matrice obtenue en donnant dans Y aux x_{h1} les valeurs précédentes. D'après a), la matrice Y_1 ne peut contenir plus de $(n-1)^2 - (n-1)$ termes arbitraires, ce qui montre d'abord que la première ligne de X contient exactement *un seul* élément de J (cela s'applique naturellement à *toutes* les lignes de X, par un raisonnement analogue fait à partir d'une ligne quelconque, en remarquant que si une ligne ne contenait aucun élément de J, une autre ligne en contiendrait deux au moins). Appliquons maintenant l'hypothèse de récurrence à Y_1, qui contient exactement $(n-1)^2 - (n-1)$ termes arbitraires, dont les autres termes sont fonctions linéaires: on voit alors qu'il existe une matrice

inversible P_1 d'ordre $n-1$ telle que les matrices Y_1P_1 soient les matrices ayant leur première colonne nulle, ou que les matrices P_1Y_1 soient les matrices ayant leur première ligne nulle. Examinons d'abord la première hypothèse, et soit P la matrice $\begin{pmatrix} 1 & 0 \\ 0 & P_1 \end{pmatrix}$; il est clair que les éléments de YP_1 se déduisent chacun de l'élément correspondant de Y_1P_1 par addition d'une fonction linéaire des x_{h1} $(1 \leqslant h \leqslant n)$. Par suite, dans $X' = XP$ les éléments x'_{h1} $(1 \leqslant h \leqslant n)$ et x'_{hk} $(2 \leqslant h \leqslant n,$ $3 \leqslant k \leqslant n)$ sont arbitraires; les x'_{h2} $(2 \leqslant h \leqslant n)$ sont fonctions linéaires des x'_{h1} $(1 \leqslant h \leqslant n)$; enfin, parmi les $n-1$ éléments x'_{1k} $(2 \leqslant k \leqslant n)$, $n-2$ sont arbitraires, et le dernier, soit x'_{1r}, est fonction linéaire de tous les éléments arbitraires de X', $x'_{1r} = \sum_{h,k} \gamma_{hk} x'_{hk} + \delta_{1r}$. Remarquons d'abord qu'on a nécessairement $\gamma_{hk} = 0$ pour $h \geqslant 2$; sans quoi, dans X', les éléments de la première ligne et les éléments d'une colonne au moins seraient *tous* arbitraires, ce qu'on a vu plus haut être impossible. En second lieu, montrons qu'on ne peut avoir $r > 2$; faisons en effet $x'_{12} = 1$, $x'_{1k} = 0$ dans X' pour $k \neq 2$ et $k \neq r$, et soit λ la valeur que prend alors x'_{1r}; retranchant dans X' la 2e colonne multipliée par λ de la r-ème colonne, la relation $\det X' = 0$ devient $\det Z = 0$, où Z est une matrice d'ordre $n-1$ dont *tous* les éléments sont arbitraires, ce qui est absurde. On a donc $r = 2$; si on avait $\gamma_{1s} \neq 0$ pour un $s > 2$ dans l'expression de x'_{12}, on en déduirait que dans la première ligne de X' tous les éléments à l'exception de x'_{1s} sont arbitraires, ce qu'on vient de voir impossible. On a donc $x'_{12} = \gamma_{11} x'_{11} + \delta_{12}$; d'autre part, toutes les lignes dans X' jouent alors le même rôle, donc, pour $h \geqslant 2$, on a $x'_{h2} = \gamma_{h1} x'_{h1} + \delta_{h2}$. Ceci posé, donnons aux x'_{hk} où $k \geqslant 3$ la valeur 0 sauf pour $x'_{kk} = 1$ $(3 \leqslant k \leqslant n)$; il vient la relation $x'_{11}(\gamma_{21} x'_{21} + \delta_{22}) - x'_{21}(\gamma_{11} x'_{11} + \delta_{12}) = 0$ qui doit être une identité en x'_{11} et x'_{21}; faisant successivement $x'_{11} = 0$ et $x'_{21} = 0$, on voit que ce n'est possible que si $\delta_{22} = \delta_{12} = 0$ et $\gamma_{21} = \gamma_{11}$ (on observera que ce raisonnement est valable même si K a seulement deux éléments).

Le même raisonnement peut être fait pour tout couple de lignes et prouve que tous les δ_{h2} sont nuls, tous les γ_{h1} égaux à un même élément μ (indépendant des x'_{hk}). Retranchant alors de la 2e colonne la première multipliée par μ [ce qui revient à faire sur X' une transformation (1)], on obtient l'ensemble de toutes les matrices ayant leur seconde colonne nulle.

Si au contraire les matrices P_1Y_1 étaient les matrices ayant leur première ligne nulle, les matrices $X' = PX$ auraient leur première colonne arbitraire ainsi que leurs lignes d'indice > 2, et nous avons vu plus haut que c'est impossible.

Reste enfin à examiner le cas où K n'a que 2 éléments; le cas $n = 2$ est alors exceptionnel, car on a identiquement en x et y

$$\begin{vmatrix} x & y+1 \\ y & 0 \end{vmatrix} = 0 .$$

Mais, si le th. 2 est vrai pour $n = 3$, il l'est aussi pour $n > 3$, la récurrence pouvant procéder comme ci-dessus, ainsi qu'on l'a remarqué. Tout revient donc à traiter le cas $n = 3$. On commence par éliminer comme ci-dessus le cas où toute ligne et toute colonne contiendrait exactement un élément de J; on peut donc se ramener soit au cas où J est formé des indices de la première colonne $(h, 1)$ $(1 \leqslant h \leqslant 3)$, soit au cas où il est formé des indices (1, 2), (2, 1) et (3, 1): on voit en effet comme précédemment qu'il n'est pas possible que tous les éléments d'une ligne *et* d'une colonne de X soient arbitraires. Cette même remarque montre que, dans le premier cas, la fonction linéaire à laquelle est égale x_{h1} est nécessairement de la forme $\alpha_{h2}\, x_{h2} + \alpha_{h3}\, x_{h3} + \beta_h$ $(1 \leqslant h \leqslant 3)$; en retranchant de la première colonne des multiples des deux autres, on peut donc supposer que $x_{11} = \beta_1$ soit indépendant des x_{hk}; mais alors, en faisant $x_{13} = x_{23} = 0$, $x_{33} = 1$, la relation $\det X = 0$ devient

$$\beta_1\, x_{22} - x_{12}(\alpha_{22}\, x_{22} + \beta_2) = 0$$

ce qui ne peut être une identité en x_{12} et x_{22} que si $\beta_1 = \alpha_{22} = \beta_2 = 0$ comme on le voit en faisant successivement $x_{12} = 0$ et $x_{12} = 1$. De la même manière, on prouve que tous les α_{h2}, α_{h3} et β_h sont nuls, d'où la proposition dans ce cas.

Si on est dans le second cas, la même remarque montre d'abord qu'on a nécessairement $x_{12} = \alpha\, x_{11} + \beta\, x_{13} + \gamma$, et en retranchant de la deuxième colonne un multiple convenable de la troisième colonne, on peut toujours supposer que $\beta = 0$; alors, si $\alpha \neq 0$, on se ramène aussitôt au premier cas. Supposons donc que $x_{12} = \gamma$ soit indépendant des x_{hk}; toujours d'après la même remarque, on doit avoir $x_{21} = a\, x_{13} + b\, x_{22} + c\, x_{23} + d\, x_{33} + e$; si on fait $x_{13} = x_{23} = 0$, $x_{33} = 1$, la relation $\det X = 0$ devient $x_{11}\, x_{22} - \gamma(b\, x_{22} + d + e) = 0$, qui ne peut pas être une identité en x_{11} et x_{22}; le second cas considéré est donc impossible, et la démonstration du th. 2 est achevée.

Pour démontrer complètement le th. 1, il reste à considérer le cas où $n = 2$ et K a deux éléments, où la vérification est immédiate.

3. Nous allons déduire le résultat annoncé au n° 1 du théorème plus général suivant:

Théorème 3. — *Toute transformation semi-linéaire biunivoque de K^{n^2} en lui-même, qui laisse invariant Σ_n, a nécessairement l'une des formes*

$$X \to P\, X^{\sigma}\, Q \tag{3}$$

$$X \to P \cdot {}^{t}X^{\sigma} \cdot Q \tag{4}$$

où P et Q sont deux matrices inversibles d'ordre n, et σ un automorphisme du corps K.

En effet, soit φ une application semi-linéaire de K^{n^2} sur lui-même, laissant invariant Σ_n. D'après le th. 2, φ transforme un idéal maximal à gauche ou à droite de M_n en un idéal maximal à gauche ou à droite; en outre, φ transforme deux idéaux maximaux de même espèce en deux idéaux maximaux de même espèce, car l'inter-

section de deux idéaux à gauche maximaux distincts est un sous-espace vectoriel de dimension $n^2 - 2n$, tandis que l'intersection d'un idéal à droite maximal et d'un idéal à gauche maximal est un sous-espace vectoriel de dimension $(n-1)^2$. En remplaçant au besoin $\varphi(X)$ par ${}^t\varphi(X)$, on peut donc supposer que φ transforme les idéaux maximaux à gauche (resp. à droite) en idéaux maximaux à gauche (resp. à droite). Or ([1], p. 65—66) les idéaux maximaux à gauche correspondent biunivoquement aux sous-espaces à une dimension (droites) de $E = K^n$; et si trois droites D, D', D'' sont dans un même plan (sous-espace à 2 dimensions), les idéaux maximaux correspondants ont une intersection de dimension $n^2 - 2n$, et réciproquement. La donnée de φ détermine donc une application biunivoque ψ_1 de l'espace projectif à $n-1$ dimensions $P(E)$ sur lui-même, qui transforme 3 points en ligne droite en 3 points en ligne droite. D'après le théorème fondamental de la géométrie projective ([2], p. 9), ψ_1 provient, par passage à l'espace projectif, d'une transformation semi-linéaire v de E si $n \geqslant 3$. De même, les idéaux maximaux à droite correspondent biunivoquement aux hyperplans (sous-espaces de dimension $n-1$) de E, ou encore aux droites de l'espace E^* dual de E; φ détermine donc une seconde application ψ_2 de $P(E)$ sur lui-même, provenant encore d'une transformation semi-linéaire u de E. Soient σ et τ les automorphismes de K auxquels correspondent u et v, et soient A et B les matrices de u et v respectivement; il résulte alors de la définition de u et v que la transformation semi-linéaire

$$X \to A^{-1}[\varphi(X)]^{\sigma^{-1}} B^{\sigma^{-1}} = \varphi'(X)$$

laisse *invariant* tout idéal maximal (à gauche ou à droite) de M_n, et par suite aussi *tout idéal*, puisqu'un idéal est toujours intersection d'idéaux maximaux dans M_n. En particulier, l'ensemble des matrices λE_{ij}, intersection d'un idéal minimal à droite et d'un idéal minimal à gauche, est transformé en lui-même par φ', d'où $\varphi'(E_{ij}) = \mu_{ij} E_{ij}$ pour tout couple (i, j). Mais pour $j \neq k$, l'ensemble des matrices $\lambda(E_{ij} + E_{ik})$ est aussi intersection d'un idéal minimal à droite et d'un idéal minimal à gauche; le même raisonnement montre donc que $\mu_{ij} = \mu_{ik}$, et on prouve de même que $\mu_{ij} = \mu_{kj}$ pour $h \neq i$, si bien que finalement, tous les μ_{ij} sont égaux à un même élément $\mu \in K$, et on a $\varphi'(X) = \mu X^\varrho$ pour tout $X \in M_n$, ϱ étant l'automorphisme de K qui correspond à l'application semi-linéaire φ'.

Le théorème 3 est ainsi complètement démontré pour $n \geqslant 3$. Pour $n = 2$, il est démontré dans [2], p. 19—20, et par suite il est vrai dans tous les cas.

Bibliographie

[1] J. Dieudonné, Sur le socle d'un anneau et les anneaux simples infinis, Bull. Soc. Math. France, **70** (1942), p. 46—75.

[2] B. L. van der Waerden, Gruppen von linearen Transformationen, Erg. der Math., Bd. IV, Berlin (Springer), 1935.

(Eingegangen am 12. 11. 1948)