31. *Sur l'invariant de Dickson*

Par Akiko YOSHIOKA
Université de la Préfecture d'Osaka

(Comm. by Kenjiro SHODA, M. J. A., March 12, 1969)

1. Dans son célèbre livre "*Linear Groups*" [1], L.E. Dickson a introduit un certain polynôme bilinéaire $D(u)$ défini par les coefficients de la matrice correspondant à une transformation symplectique u définie sur un corps de caractéristique 2, et il a montré qu'il existe un sous-groupe du groupe symplectique laissant invariante la valeur de $D(u)$. Nous ne savons pas le fond de sa considération de $D(u)$. Quarante ans après, C. Arf a introduit le pseudo-discriminant $\Delta(Q)$ associé à une forme quadratique Q et il a montré qu'à une classe d'équivalence de formes quadratiques non dégénérées et non défectives, correspond un pseudo-discriminant modulo $\mathfrak{p}(K)$ où $\mathfrak{p}(K)$ désigne l'ensemble des éléments de K^* ayant la forme $\mathfrak{p}(a)=a^2+a$, $a\in K^*$. Plus précisément, si Q_u est une forme quadratique transformée de Q par une transformation symplectique u, on a la relation $\Delta(Q_u)\equiv\Delta(Q)$ (mod $\mathfrak{p}(K)$) [2]. En utilisant l'algèbre de Clifford, J. Dieudonné a montré dans [4] que cette relation peut être écrite sous la forme

$$\Delta(Q_u)=\Delta(Q)+\mathfrak{p}(D(u)). \tag{1}$$

Ce fait montre que $D(u)$ joue un rôle important dans les recherches du groupe orthogonal et de la classe d'équivalence de formes quadratiques. Dans ce travail nous étudions les propriétés de $D(u)$ dans le groupe des similitudes orthogonales.

2. Soient K un corps commutatif de caractéristique 2 et E un espace vectoriel à droite sur K de dimension paire $2m$. Soit Q une forme quadratique sur E:

$$Q(x\alpha+y\beta)=Q(x)\alpha^2+Q(y)\beta^2+f(x,y)\alpha\beta,\quad x,y\in E;\ \alpha,\beta\in K, \tag{2}$$

où f est une forme bilinéaire alternée sur $E\times E$. Désignons par $GS_{p_{2m}}(f)$, $S_{p_{2m}}(f)$, $GO_{2m}(Q)$ et $O_{2m}(Q)$ (ou simplement, par GS_p, S_p, GO et O), le groupe des similitudes symplectiques, le groupe symplectique, le groupe des similitudes orthogonales et le groupe orthogonal. Une fois pour toutes, nous fixons une forme quadratique non dégénérée et non défective sur E. Par conséquent, nous entendons la base symplectique, les groupes GS_p, S_p etc., toujours définis par rapport à la forme f déterminée entièrement par Q. On trouve les définitions et les notions dans [5].

Fixons une base symplectique $\langle e_1, \cdots, e_m, e'_1, \cdots, e'_m\rangle$. Soit

$U=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, $A=(a_{ij})$, $B=(b_{ij})$, $C=(c_{ij})$, $D=(d_{ij})$, la matrice correspondant à une transformation linéaire u de E par rapport à cette base. On voit facilement que, pour que u soit une similitude symplectique de multiplicateur μ_u, il faut et il suffit que U satisfasse à la condition ${}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} O & E \\ E & O \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} O & \mu_u E \\ \mu_u E & O \end{pmatrix}$, c'est-à-dire aux relations suivantes:

$$(3) \qquad {}^tCA+{}^tAC=O, \quad {}^tAD+{}^tCB=\mu_u E, \quad {}^tDB+{}^tBD=O;$$

$$(4) \qquad B{}^tA+A{}^tB=O, \quad D{}^tA+C{}^tB=\mu_u E, \quad D{}^tC+C{}^tD=O^{1)}.$$

En écrivant $Q(e_i)=\alpha_i$ et $Q(e_i')=\beta_i$, $1\leqq i\leqq m$, on appelle *l'invariant de Dickson* de u $D(u)=\sum_{i,j=1}^{m}(\alpha_i a_{ij}b_{ij}+\beta_i c_{ij}d_{ij}+b_{ij}c_{ij})$, et *le pseudo-discriminant* de Q $\Delta(Q)=\sum_{i=1}^{m}\alpha_i\beta_i$.

Considérons *l'algèbre de Clifford* $C(Q)$ associée à Q. C'est une algèbre engendrée par $e_1, \cdots, e_m, e_1', \cdots, e_m'$ et l'unité, de rang 2^{2m} sur K et définie par les relations

$$(5) \qquad \begin{aligned} &e_i^2=\alpha_i, \quad e_i'^2=\beta_i; \\ &e_ie_j=e_je_i, \quad e_i'e_j'=e_j'e_i'; \\ &e_ie_j'+e_j'e_i=\delta_{ij}, \quad 1\leqq i, j\leqq m. \end{aligned}$$

Les éléments de degré pair de $C(Q)$ forment une sous-algèbre $C^+(Q)$ de $C(Q)$, de rang 2^{2m-1} sur K. Elle est engendrée par les produits e_ie_j, e_ie_j', $e_i'e_j'$, $1\leqq i, j\leqq m$ et l'unité.

Soit u une similitude symplectique de multiplicateur μ_u. Au moyen de (3) et (4) on obtient les relations suivantes:

$$(6) \qquad \begin{aligned} &u(e_i)^2=Q(u(e_i)), \quad u(e_i')^2=Q(u(e_i')); \\ &u(e_i)u(e_j)=u(e_j)u(e_i), \quad u(e_i')u(e_j')=u(e_j')u(e_i'); \\ &u(e_i)u(e_j')+u(e_j')u(e_i)=\delta_{ij}\mu_u, \quad 1\leqq i, j\leqq m. \end{aligned}$$

Comme $\langle u(e_1), \cdots, u(e_m), u(e_1'), \cdots, u(e_m')\rangle$ est une base symplectique, les relations (6) montrent que $u(e_1), \cdots, u(e_m), u(e_1'), \cdots, u(e_m')$ et l'unité sont aussi les générateurs de $C(Q)$. D'autre part, si l'on pose $Q_u(x)=Q(u(x))$ pour tout x de E, Q_u est une forme quadratique non dégénérée et non défective sur E. Alors, l'algèbre de Clifford $C(Q_u)$ associée à Q_u coïncide à $C(Q)$, et sa sous-algèbre $C^+(Q_u)$ coïncide à $C^+(Q)$.

Le lemme suivant donne l'identité correspondant à (1) pour les similitudes symplectiques.

Lemme 1. *Pour tout u de $GS_{p_{2m}}(f)$ on a*

$$(7) \qquad \Delta(Q_u)=\Delta(Q)\mu_u^2+D(u)^2+D(u)\mu_u.$$

Soit $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ la matrice correspondant à u par rapport à la base symplectique $\langle e_1, \cdots, e_m, e_1', \cdots, e_m'\rangle$.

1) Comme ${}^tU$ est aussi la matrice correspondant à une similitude symplectique de même multiplicateur μ_u.

Nous avons remarqués qu'on peut obtenir directement cette identité par le calcul de $\Delta(Q_u)=\sum_{i=1}^{m}Q(u(e_i))Q(u(e_i'))$, au moyen des relations (3) [6]. Mais ici, nous allons le démontrer en appliquant au groupe GS_p la méthode de Dieudonné qui utilise l'algèbre de Clifford, c'est parce que cette méthode est utile pour montrer le théorème ultérieur.

Considérons les éléments $z=\sum_{i=1}^{m}e_ie_i'$ et $u(z)=\sum_{i=1}^{m}u(e_i)u(e_i')$ dans l'algèbre $C^+(Q)=C^+(Q_u)$. Alors, on a $\Delta(Q)=\sum_{i=1}^{m}Q(e_i)Q(e_i')=\sum_{i=1}^{m}e_i^2e_i'^2=z^2+z$. Les relations (3), (4) et (5) entraînent $u(z)=\sum_i u(e_i)u(e_i')=\sum_i\{\sum_h(e_ha_{hi}+e_h'c_{hi})\sum_k(e_kb_{ki}+e_k'd_{ki})\}=\sum_{h,i}Q(e_h)a_{hi}b_{hi}+\sum_{h,i}Q(e_h')c_{hi}d_{hi}+(\sum_h e_he_h')\mu_u+\sum_{h,i}b_{hi}c_{hi}=D(u)+z\mu_u$. En utilisant les relations (5), on a $u(z)^2=\sum_{i\neq j}u(e_i)u(e_i')u(e_j)u(e_j')+\sum_i u(e_i)u(e_i')u(e_i)u(e_i')=\sum_i u(e_i)\{u(e_i)u(e_i')+\mu_u\}u(e_i')=\Delta(Q_u)+u(z)\mu_u$. D'où on a $\Delta(Q_u)=u(z)^2+u(z)\mu_u=\{D(u)+z\mu_u\}^2+\{D(u)+z\mu_u\}\mu_u=(z^2+z)\mu_u^2+D(u)^2+D(u)\mu_u=\Delta(Q)\mu_u^2+D(u)^2+D(u)\mu_u$.

Théorème. *Pour tout u de $GO_{2m}(Q)$ et pour tout v de $GS_{p_{2m}}(f)$ on a l'identité*

$$(D)\qquad D(uv)=D(u)\mu_v+D(v)\mu_u.$$

En effet, pour un élément arbitraire u de GS_p posons $\varepsilon_i=u(e_i)$, $\varepsilon_i'=u(e_i')$, $1\leqq i\leqq m$ et $\zeta=\sum_{i=1}^{m}\varepsilon_i\varepsilon_i'$. Soit $\begin{pmatrix}A & B\\ C & D\end{pmatrix}$ la matrice correspondant à un élément w de GS_p, par rapport à la base symplectique $\langle\varepsilon_1,\cdots\cdots,\varepsilon_m,\varepsilon_1',\cdots,\varepsilon_m'\rangle$. En utilisant les relations (3), (4) et (6) on peut calculer $w(\zeta)$ de même que $u(z)$: $w(\zeta)=\sum_i w(\varepsilon_i)w(\varepsilon_i')=\sum_{i,j}Q(\varepsilon_i)a_{ij}b_{ij}+\sum_{i,j}Q(\varepsilon_i')c_{ij}d_{ij}+(\sum_{i,j}b_{ij}c_{ij})\mu_u+(\sum_i\varepsilon_i\varepsilon_i')\mu_w$. Si u appartient à GO, on a $Q(\varepsilon_i)=\alpha_i\mu_u$ et $Q(\varepsilon_i')=\beta_i\mu_u$. Alors, on a $w(\zeta)=\{\sum_{i,j}(\alpha_ia_{ij}b_{ij}+\beta_ic_{ij}d_{ij}+b_{ij}c_{ij})\}\mu_u+\zeta\mu_w=D_u(w)\mu_u+\zeta\mu_w$ où $D_u(w)=\sum_{i,j}(\alpha_ia_{ij}b_{ij}+\beta_ic_{ij}d_{ij}+b_{ij}c_{ij})$. Comme $\zeta=u(z)=D(u)+z\mu_u$, on en déduit que $wu(z)=w(\zeta)=D_u(w)\mu_u+(D(u)+z\mu_u)\mu_w=D_u(w)\mu_u+D(u)\mu_w+z\mu_u\mu_w$. D'autre part, on a $wu(z)=D(wu)+z\mu_{wu}=D(wu)+z\mu_w\mu_u^{2)}$. Donc on a $D(wu)=D_u(w)\mu_u+D(u)\mu_w$. Comme $\begin{pmatrix}A & B\\ C & D\end{pmatrix}$ est la matrice correspondant à w par rapport à la base $\langle u(e_1),\cdots,u(e_m),u(e_1'),\cdots,u(e_m')\rangle$, elle est aussi la matrice correspondant à $u^{-1}wu$ par rapport à la base $\langle e_1,\cdots,e_m,e_1',\cdots\cdots,e_m'\rangle$. On a alors $D(wu)=D(u^{-1}wu)\mu_u+D(u)\mu_w$. Si l'on pose $v=u^{-1}wu$, on a $v\in GS_p$, $\mu_w=\mu_{uvu^{-1}}=\mu_v$ et on a $D(uv)=D(v)\mu_u+D(u)\mu_v$.

2) L'application $u\to\mu_u$ est un homomorphisme de GS_p dans le groupe multiplicatif K^* formé des éléments non nuls de K.

Grâce au lemme 1, pour tout u de GO on a $D(u)^2+D(u)\mu_u=0$, c'est-à-dire $D(u)=0$ ou $=\mu_u$. Un élément u de GO tel que $D(u)=0$ est appelé *similitude directe orthogonale*. Pour u et v de GO tels que $D(u)=0$ et $D(v)=0$, l'identité (D) entraîne $D(uv)=D(vu)=0$. Alors, les similitudes directes orthogonales forment un sous-groupe de GO. On l'appelle *le groupe des similitudes directes orthogonales* et on le désigne par $GO^+_{2m}(Q)$ ou par GO^+. Dans le groupe orthogonal O, on peut définir O^+ comme le sous-groupe formé des éléments qui se représentent comme produit d'un nombre pair de transvections orthogonales (par exemple, cf. [3]). Mais, dans le groupe des similitudes orthogonales GO, comme GO n'est pas en général produit direct de O et du groupe des homothéties, il existe un élément qui ne peut être représenté comme produit de transvections orthogonales et d'une homothétie. Pour cette raison, il n'est pas juste de définir GO^+ comme le sous-groupe formé des éléments qui se représentent comme produit d'un nombre pair de transvections orthogonales et d'une homothétie.

Pour une homothétie h_a associée à un élément a de K^*, on a $D(h_a)=0$. Alors, le groupe des homothéties H est contenu dans GO^+. Soit $u\in GO$. Si $D(u)=\mu_u$, comme $0=D(1)=D(uu^{-1})=D(u)\mu_{u^{-1}}+D(u^{-1})\mu_u=1+D(u^{-1})\mu_u$ d'après (D), on a $D(u^{-1})=\mu_u^{-1}=\mu_{u^{-1}}$. Si $D(u)=O$, comme $D(u^{-1})\mu_u=0$, on a $D(u^{-1})=0$. Soient u un élément de GO^+ et v un élément arbitraire de GO. Pour v tel que $D(v)=0$, de l'identité (D) on a $D(vuv^{-1})=D(v)\mu_{uv^{-1}}+\{D(u)\mu_{v^{-1}}+D(v^{-1})\mu_u\}\mu_v=D(u)=0$. Pour v tel que $D(v)=\mu_v$, de l'identité (D) on a $D(vuv^{-1})=\{D(v)\mu_u+D(u)\mu_v\}\mu_{v^{-1}}+D(v^{-1})\mu_{vu}=\mu_v\mu_u\mu_{v^{-1}}+D(u)+\mu_v^{-1}\mu_{vu}=D(u)=0$. Donc, GO^+ est un sous-groupe distingué dans GO.

Soit $\boldsymbol{a}$ un vecteur non singulier de E tel que $\boldsymbol{a}=\sum_{i=1}^{m}\boldsymbol{e}_i a_i+\sum_{i=1}^{m}\boldsymbol{e}'_i a'_i$ et soit u une transvection orthogonale définie par $\boldsymbol{a}$: $u(\boldsymbol{x})=\boldsymbol{x}+\boldsymbol{a}\alpha f(\boldsymbol{x},\boldsymbol{a})$ pour tout $\boldsymbol{x}$ de E, où α désigne $Q(\boldsymbol{a})^{-1}$. Comme on a $u(\boldsymbol{e}_i)=\boldsymbol{e}_i+\boldsymbol{a}\alpha a'_i$ et $u(\boldsymbol{e}'_i)=\boldsymbol{e}'_i+\boldsymbol{a}\alpha a_i$, la matrice correspondant à u par rapport à la base $\langle \boldsymbol{e}_1,\cdots,\boldsymbol{e}_m,\boldsymbol{e}'_1,\cdots,\boldsymbol{e}'_m\rangle$ a la forme $\begin{pmatrix}\delta_{ij}+\alpha a_i a'_j & \alpha a_i a_j\\ \alpha a'_i a'_j & \delta_{ij}+\alpha' a_i a_j\end{pmatrix}$. On en déduit $D(u)=1$.

Lemme 2. *Pour deux u, v de GS_p, on a l'identité*

$$(D')\qquad D(uv)=D(u)\mu_v+D(v)\mu_u+\sum_{i=1}^{m}\{Q(u(\boldsymbol{e}_i))+\alpha_i\mu_u\}\xi_i+\sum_{i=1}^{m}\{Q(u(\boldsymbol{e}'_i))+\beta_i\mu_u\}\eta_i,$$

où ξ_i et η_i sont les i-ièmes coefficients diagonaux de $A{}^tB$ et de $C{}^tD$, pour la matrice $\begin{pmatrix}A & B\\ C & D\end{pmatrix}$ correspondant à v par rapport à la base $\langle \boldsymbol{e}_1,\cdots,\boldsymbol{e}_m,\boldsymbol{e}'_1,\cdots,\boldsymbol{e}'_m\rangle$.

En effet, comme on a déjà vu, si $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ est la matrice correspondant à un élément w de GS_p par rapport à la base symplectique $\langle u(e_1), \cdots, u(e_m), u(e_1'), \cdots, u(e_m') \rangle$, on a $wu(z) = \sum_{i,j} Q(u(e_i))a_{ij}b_{ij} + \sum_{i,j} Q(u(e_i'))c_{ij}d_{ij} + (\sum_{i,j} b_{ij}c_{ij})\mu_u + (D(u) + z\mu_u)\mu_w$. D'autre part on a $wu(z) = D(wu) + z\mu_{wu}$, $\sum_{i,j} b_{ij}c_{ij} = D_u(w) + \sum_{i,j} \alpha_i a_{ij}b_{ij} + \sum_{i,j} \beta_i c_{ij}d_{ij}$ et $D_u(w) = D(u^{-1}wu)$. D'où on a $D(wu) = D(u)\mu_w + D(u^{-1}wu)\mu_u + \sum_{i,j} \{Q(u(e_i)) + \alpha_i\mu_u\}a_{ij}b_{ij} + \sum_{i,j} \{Q(u(e_i')) + \beta_i\mu_u\}c_{ij}d_{ij}$. En posant $\sum_{j=1}^{m} a_{ij}b_{ij} = \xi_i$, $\sum_{j=1}^{m} c_{ij}d_{ij} = \eta_i$ et $v = u^{-1}wu$ on obtient (D').

Considérons les transformations linéaires v_h, w_k, $1 \leqq h, k \leqq m$ telles que $v_h(e_i) = e_i$, $v_h(e_i') = e_i\delta_{ih} + e_i'$, $w_k(e_i) = e_i + e_i'\delta_{ik}$, $w_k(e_i') = e_i'$, $1 \leqq i \leqq m$. Alors on voit que v_h, $w_k \in S_p$ et que $D(v_h) = \alpha_h$ et $D(w_k) = \beta_k$. Les matrices $\begin{pmatrix} E & E_{hh} \\ O & E \end{pmatrix}$, $\begin{pmatrix} E & O \\ E_{kk} & E \end{pmatrix}$ correspondent à v_h, w_k respectivement, où E_{ll} est la matrice dont le (l, l)-coefficient est égal à 1 et tous les autres sont nuls. Comme on a $Q(v_h(e_h')) = \alpha_h + \beta_h + 1$ et $Q(w_k(e_k)) = \alpha_k + \beta_k + 1$, en général v_h, w_k n'appartiennent pas à O.

Proposition. *Pour qu'un élément u de GS_p appartienne à GO, il faut et il suffit que u satisfasse à l'identité (D) pour tous les v_h, w_k, $1 \leqq h, k \leqq m$.*

La condition nécessaire est évidente d'après le théorème. Supposons que (D) soit établi pour un élément u de GS_p et pour les v_h, w_k, $1 \leqq h, k \leqq m$. De l'identité (D'), on a les équations suivantes:

$$(8) \qquad \begin{aligned} &\sum_{i=1}^{m} \{Q(u(e_i)) + \alpha_i\mu_u\}\xi_i + \sum_{i=1}^{m} \{Q(u(e_i')) + \beta_i\mu_u\}\eta_i = 0, \\ &\sum_{i=1}^{m} \{Q(u(e_i)) + \alpha_i\mu_u\}\xi_i' + \sum_{i=1}^{m} \{Q(u(e_i')) + \beta_i\mu_u\}\eta_i' = 0, \end{aligned}$$

où ξ_i, η_i, ξ_i', η_i' sont les i-ièmes coefficients diagonaux des matrices EE_{hh}, OE, EO, $E_{kk}E$, respectivement. Les équations (8) ont les $2m$ solutions $(0 \cdots 0 \overset{l}{1} 0 \cdots 0)$, $1 \leqq l \leqq 2m$, non triviales et linéairement indépendantes. Donc, tous les coefficients de (8) sont nuls, c'est-à-dire $Q(u(e_i)) = \alpha_i\mu_u$, $Q(u(e_i')) = \beta_i\mu_u$, $1 \leqq i \leqq m$, et $u \in GO$.

Références

[1] L. E. Dickson: Linear Groups. B. G. Teubner, Leipzig (1901).

[2] C. Arf: Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I). J. reine angew. Math., **183**, 148–167 (1941).

[3] J. Dieudonné: Algebraic homogeneous spaces over fields of characteristic two. Proc. Amer. Math. Soc., **2**, 295–304 (1951).

[4] ——: Pseudo-discriminant and Dickson invariant. Pacific J. Math., **5**, 907–910 (1955).

[5] ——: La géométrie des groupes classiques. Springer, Berlin (1955).

[6] A. Ohara: La structure du groupe des similitudes directes $GO_6^+(Q)$ sur un corps de caractéristique 2. Osaka Math. J., **10** (2), 239–257 (1958).