PSEUDO-DISCRIMINANT AND DICKSON INVARIANT

JEAN DIEUDONNÉ

1. Let E be a vector space of finite dimension over a field K. To a bilinear symmetric form $f(x, y)$ defined over $E \times E$ is attached classically the notion of *discriminant*: it is an element of K which is not entirely defined by f; however, it is entirely determined when in addition a basis of E is chosen, and when the basis is changed, the discriminant is multiplied by a *square* in K. More precisely, let u be a linear mapping of E into E, and let $f_1(x, y) = f(u(x), u(y))$ the form "transformed" by u; if $\Delta(f)$, $\Delta(f_1)$ are the discriminants of f and f_1 with respect to the *same* basis of E, and $D(u)$ the determinant of u with respect to that basis, then one has the classical relation

$$\Delta(f_1) = (D(u))^2 \Delta(f) . \tag{1}$$

When K has characteristic $\neq 2$, the preceding results may be expressed in terms of the "quadratic form" $f(x, x)$ associated to $f(x, y)$. However, when K has characteristic 2, the one-to-one association between bilinear symmetric forms and quadratic forms no longer subsists. More precisely, to a given *alternate* symmetric form $f(x, y)$ (that is, $f(x, x) = 0$ for all $x \in E$) is associated a whole family of quadratic forms $Q(x)$, satisfying the fundamental identity

$$Q(x+y) = Q(x) + Q(y) + f(x, y) \tag{2}$$

and to all these Q is associated the same discriminant of f (with respect to a given basis).

Now C. Arf [1] has introduced an element $\Delta(Q)$ attached to Q and to a given *symplectic basis* of E (with respect to the form f) which we shall call the *pseudo-discriminant* of Q. He proved moreover that under a change of symplectic basis, $\Delta(Q)$ is transformed in the following way: let $\wp$ be the homomorphism $\xi \to \xi + \xi^2$ of the additive group K into itself; then the pseudo-discriminants of Q with respect to two different symplectic bases have a *difference* which has the form $\wp(\lambda)$. Arf's proof is rather lengthy and proceeds by induction on n. We propose to show how the pseudo-discriminant is related to the *Clifford algebra* of Q in a way which parallels the well-known relation between the discriminant of f and the Clifford algebra of f over a field of characteristic $\neq 2$. At the same time, this will clear up the origin of a curiously isolated result obtained by L. E. Dickson for the orthogonal

Received May 11, 1954.

group $O_n(K, Q)$ over a finite field of characteristic 2: the transformations u of that group are defined by the condition $Q(u(x))=Q(x)$, and Dickson showed [4, p. 206] that a certain bilinear polynomial $D(u)$ in the elements of the matrix of u (with respect to a symplectic basis), turns out to be always equal to 0 or 1 for elements of $O_n(K, Q)$ (the first case occurring if and only if u is a product of an *even* number of transvections of $O_n(K, Q)$; see [6, p. 301]). Now the connection with the Clifford algebra which we mentioned above leads one in a natural way to form the polynomial $D(u)$ for an arbitrary *symplectic* transformation u; if $Q_1(x)=Q(u(x))$ is then the "transformed" of Q by u, and $\Delta(Q)$, $\Delta(Q_1)$ and $D(u)$ are computed with respect to the *same* symplectic basis, we will prove the following identity, which can be considered as the counter-part of (1)

$$\Delta(Q_1)=\Delta(Q)+\wp(D(u)). \tag{3}$$

Dickson's result follows obviously from this relation.

2. **We shall** always suppose that the alternate form f is nondegenerate, which implies that $n=2m$ is *even*, and that the forms Q associated with f are *nondefective* [5, p. 39–40]. For the definition of the *Clifford algebra* $C(Q)$ of a quadratic form Q associated to f, we refer the reader to [3] or [6]. If $(e_i)_{1\leq i\leq n}$ is a symplectic basis of E, such that

$$f(e_i, e_{m+j})=\delta_{ij}, \quad f(e_i, e_j)=0, \quad f(e_{m+i}, e_{m+j})=0 \qquad 1\leq i, j\leq m,$$

then the unit element and the e_i $(1\leq i\leq n)$ constitute a system of generators for $C(Q)$, with the relations

$$\begin{cases} e_i^2=Q(e_i), \quad e_{m+i}^2=Q(e_{m+i}), \quad e_ie_j=e_je_i \\ e_{m+i}e_{m+j}=e_{m+j}e_{m+i}, \quad e_ie_{m+j}+e_{m+j}e_i=\delta_{ij} \qquad 1\leq i, j\leq m. \end{cases} \tag{4}$$

From this it follows that $C(Q)$ is an algebra of rank 2^{2m} over K. Moreover, the elements of *even degree* of $C(Q)$ (generated by the products of an even number of the e_i's) constitute a subalgebra $C^+(Q)$ of rank 2^{2m-1} over K, and it can be shown that the center Z of that algebra has rank 2 over K [3, p. 44]. Now, it is readily verified from (4) that the element

$$z=e_1e_{m+1}+e_2e_{m+2}+\cdots+e_me_{2m} \tag{5}$$

commutes with all products e_he_k, and therefore constitutes with the unit element a basis for Z over K. From (4) it follows that $z^2+z=\Delta(Q)$, where

$$\Delta(Q)=Q(e_1)Q(e_{m+1})+Q(e_2)Q(e_{m+2})+\cdots+Q(e_m)Q(e_{2m}) \tag{6}$$

is precisely the *pseudo-discriminant* of Q relative to the basis (e_i) considered by Arf. Now the fact that $\Delta(Q)$ has the form $\wp(\lambda)$ expresses the fact that the equation $z^2+z=\Delta(Q)$ has a solution in K, in other words, that Z is not a field. When Z is a field, it is a separable quadratic field over K, and if it is generated by the roots of any equation $t^2+t=\mu$, then μ and $\Delta(Q)$ differ by an element of the form $\wp(\lambda)$ [2, p. 177, exerc. 8]. This proves immediately that when the pseudo-discriminant is computed with respect to two different symplectic bases, the values obtained have a difference of the form $\wp(\lambda)$.

3. **We are now** going to make the above result more precise by proving (3). If u is a symplectic transformation, the elements $u(e_i)$ $(1\leq i\leq 2m)$ constitute again a symplectic basis for E, hence also a system of generators for the Clifford algebra $C(Q)$, satisfying relations similar to (4) (with $Q(u(e_i))$ replacing $Q(e_i)$). The element

$$z'=u(e_1)u(e_{m+1})+\cdots+u(e_m)u(e_{2m}) \tag{7}$$

constitutes therefore, with the unit element, a basis for Z over K, in other words, z' has the form $p+qz$, where p, q are in K. Now it is easy to compute z' as a function of the coefficients of the matrix of u with respect to (e_i): let

$$u(e_i)=\sum_{j=1}^m a_{ij}e_j+\sum_{j=1}^m b_{ij}e_{m+j}$$
$$u(e_{m+i})=\sum_{j=1}^m c_{ij}e_j+\sum_{j=1}^m d_{ij}e_{m+j}\,.$$

Let on the other hand $Q(e_i)=\alpha_i$, $Q(e_{m+i})=\beta_i$. Then z' is a linear combination of elements e_he_k, and it follows from (4) and (5) that we need only consider among those elements the squares e_i^2 and the products e_ie_{m+i}, $e_{m+i}e_i$ since we know in advance that z' can contain no other elements from the basis of $C^+(Q)$. We thus obtain

$$p=\sum_{i=1}^m\sum_{j=1}^m(\alpha_ja_{ij}c_{ij}+\beta_jb_{ij}d_{ij}+b_{ij}c_{ij}) \tag{8}$$

$$q=\sum_{i=1}^m(a_{ij}d_{ij}+b_{ij}c_{ij})\,. \tag{9}$$

But it follows, from the fact that the transposed matrix of u is again the matrix of a symplectic transformation, that $q=1$. The expression on the right of (8) is the *Dickson invariant* $D(u)$; as the relation $z'=p+z$ yields $z'^2+z'=z^2+z+p^2+p$, the identity (3) follows immediately from (6).

4. **We cannot expect,** of course, that the mapping $u\to D(u)$ should be a homomorphism of the symplectic group $Sp_{2m}(K)$ into the additive group of K, if only because we know that $Sp_{2m}(K)$ is a simple group. However, there are some relations between the Dickson invariants of

two symplectic transformations u, v and the Dickson invariant of their product. In fact, it follows immediately from the expression of z' obtained in § 3, that we have

$$D(vu)=D(u)+D_u(v) \tag{10}$$

where $D(u)$ and $D(vu)$ are the Dickson invariants of u and vu with respect to the basis (e_i), and $D_u(v)$ the Dickson invariant of v *with respect to the basis* $(u(e_i))$. This general formula takes a simpler shape when u is an *orthogonal transformation*, because then $Q(u(e_i))=Q(e_i)$ for $1\leq i\leq 2m$; on the other hand, the matrix of v with respect to the basis $(u(e_i))$ is the same as the matrix of $u^{-1}vu$ with respect to (e_i), and we thus obtain

$$D(vu)+D(u^{-1}vu)=D(u)\,. \tag{11}$$

But in this identity we can replace v by uvu^{-1}; therefore we also have

$$D(uv)=D(u)+D(v) \tag{12}$$

when u is an *orthogonal* transformation, v an arbitrary *symplectic* transformation ($D(u)$ being equal to 0 or 1, as recalled above).

REFERENCES

1. C.Arf, *Untersuchungen über quadratische Formen in Körpern der Charakteristik 2 (Teil I)*, J. Reine Ang. Math., **183** (1941), 148–167.
2. N.Bourbaki, *Eléments de Mathématique, Livre II: Algèbre, chap.* IV–V, Actual. Scient. et Ind., n° 1102, Paris (Hermann), 1950.
3. C.Chevalley, *The algebraic theory of spinors*, Columbia Univ. Press, New-York, 1954.
4. L.E.Dickson, *Linear groups*, Leipzig (Teubner), 1901.
5. J. Dieudonné, *Sur les groupes classiques*, Actual. Scient. et. Ind., n° 1040, Paris (Herman), 1948.
6. ———, *Algebraic homogeneous spaces over fields of characteristic two.* Proc. Amer. Math. Soc., **2** (1951), 295–304.

NORTHWESTERN UNIVERSITY

Added in proof (November 1955): Since this paper was submitted for publication, the following papers, containing substantially the result of § 2, have appeared:

M. Kneser, *Bestimmung des Zentrums der Cliffordschen Algebren einer quadratischen Form über einem Körper der Charakteristik* 2, J. Reine Angew. Math., **193** (1954), 123-125.

E. Witt, *Über eine Invariante quadratische Formen mod.* 2, J. Reine Angew. Math., **193** (1954), 119-120.

E. Witt and W. Klingenberg, *Über die Arfsche Invariante quadratischer Formen mod.* 2, J. Reine Angew. Math., **193** (1954), 121-122.