PSEUDO-DISCRIMINANT AND DICKSON INVARIAN

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

$$\Delta(f_1) = (D(u))^2 \Delta(f).$$

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

$$Q(x + y) = Q(x) + Q(y) + f(x, y)$$

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 $\mathcal{P}$ be the homomorphism $\xi \mapsto \xi + \xi^2$ 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 $\mathcal{P}(\lambda)$. 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
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 $Q_i(x) = Q(u(x))$ is then the "transformed" of $Q$ by $u$, and $\Delta(Q)$, $\Delta(Q_i)$ 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)

$$\Delta(Q_i) = \Delta(Q) + \beta'(D(u)).$$

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

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

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

$$e_i^2 = Q(e_i), \quad e_{m+i} = Q(e_{m+i}), \quad e_i e_j = e_j e_i \quad 1 \leq i, j \leq m.$$

From this it follows that $C(Q)$ is an algebra of rank $2^m$ 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 $2^{m-1}$ 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

$$z = e_i e_{m+1} + e_j e_{m+2} + \cdots + e_m e_{2m}$$

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

$$\Delta(Q) = Q(e_1)Q(e_{m+1}) + Q(e_2)Q(e_{m+2}) + \cdots + Q(e_m)Q(e_{2m})$$
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 \( \gamma(\lambda) \) 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 \( \mu \) and \( \Delta(Q) \) differ by an element of the form \( \gamma(\lambda) \) [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 \( \gamma(\lambda) \).

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

\[
z' = u(e_1)u(e_{m+1}) + \cdots + u(e_m)u(e_{2m})
\]

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

\[
p = \sum_{i=1}^{m} \sum_{j=1}^{m} (\alpha_i a_{ij} c_{ij} + \beta_j b_{ij} d_{ij} + b_{ij} e_{ij})
\]

\[
q = \sum_{i=1}^{m} (a_{ij} d_{ij} + b_{ij} e_{ij}).
\]

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 \( u \rightarrow D(u) \) 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

\[
D(vu) = D(u) + D_n(v) \tag{10}
\]

where \( D(u) \) and \( D(vu) \) are the Dickson invariants of \( u \) and \( vu \) with respect to the basis \((e_i)\), and \( D_n(v) \) 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

4. L. E. Dickson, Linear groups, Leipzig (Teubner), 1901.

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:


<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nesmith Cornett Ankeny and Theodore Joseph Rivlin</td>
<td>On a theorem of S. Bernstein</td>
<td>849</td>
</tr>
<tr>
<td>Louis Auslander</td>
<td>The use of forms in variational calculation</td>
<td>853</td>
</tr>
<tr>
<td>Paul Civin</td>
<td>Abstract Riemann sum</td>
<td>861</td>
</tr>
<tr>
<td>Paul Civin</td>
<td>Some ergodic theorems involving two operator</td>
<td>869</td>
</tr>
<tr>
<td>Eckford Cohen</td>
<td>The number of solutions of certain cubic congruence</td>
<td>877</td>
</tr>
<tr>
<td>Richard M. Cohn</td>
<td>Specializations over difference field</td>
<td>887</td>
</tr>
<tr>
<td>Jean Dieudonné</td>
<td>Pseudo-discriminant and Dickson invariant</td>
<td>907</td>
</tr>
<tr>
<td>Ky Fan</td>
<td>A comparison theorem for eigenvalues of normal matrix</td>
<td>911</td>
</tr>
<tr>
<td>Richard P. Gosselin</td>
<td>On the convergence behaviour of trigonometric interpolating polynomial</td>
<td>915</td>
</tr>
<tr>
<td>Peter K. Henrici</td>
<td>On generating functions of the Jacobi polynomial</td>
<td>923</td>
</tr>
<tr>
<td>Meyer Jerison</td>
<td>An algebra associated with a compact group</td>
<td>933</td>
</tr>
<tr>
<td>Wilhelm Magnus</td>
<td>Infinite determinants associated with Hill’s equation</td>
<td>941</td>
</tr>
<tr>
<td>G. Power and D. L. Scott-Hutton</td>
<td>The slow steady motion of liquid past a semi-elliptical bos</td>
<td>953</td>
</tr>
<tr>
<td>Lyle E. Pursell</td>
<td>An algebraic characterization of fixed ideals in certain function ring</td>
<td>963</td>
</tr>
<tr>
<td>C. T. Rajagopal</td>
<td>Additional note on some Tauberian theorems of O. Szász</td>
<td>971</td>
</tr>
<tr>
<td>Louis Baker Rall</td>
<td>Error bounds for iterative solutions of Fredholm integral equation</td>
<td>977</td>
</tr>
<tr>
<td>Shigeo Sasaki and Kentaro Yano</td>
<td>Pseudo-analytic vectors on pseudo-Kählerian manifold</td>
<td>987</td>
</tr>
<tr>
<td>Eugene Schenkman</td>
<td>On the tower theorem for finite group</td>
<td>995</td>
</tr>
<tr>
<td>P. Stein and John E. L. Peck</td>
<td>On the numerical solution of Poisson’s equation over a rectangle</td>
<td>999</td>
</tr>
<tr>
<td>Morgan Ward</td>
<td>The mappings of the positive integers into themselves which preserve divisio</td>
<td>1013</td>
</tr>
<tr>
<td>Seth Warner</td>
<td>Weak locally multiplicatively-convex algebra</td>
<td>1025</td>
</tr>
<tr>
<td>Louis Weisner</td>
<td>Group-theoretic origin of certain generating function</td>
<td>1033</td>
</tr>
</tbody>
</table>