ON WITT'S THEOREM FOR NONALTERNATING SYMMETRIC BILINEAR FORMS OVER A FIELD OF CHARACTERISTIC 2

VERA PLESS

I. **Introduction.** The purpose of this note is to show that an analogue to Witt's theorem holds for a nondegenerate, nonalternating, symmetric bilinear form f over a field K of characteristic 2 where $f(x, x)$ takes its values in a subfield K^* such that K contains the square root of any element in K^*. As is known [2, p. 171] Witt's theorem does not hold in general for a field of characteristic 2. However, the following shows that an isometry of a subspace can be extended if it leaves a certain unique vector invariant. The invariants of a subspace of V with respect to the orthogonal group are determined.

II. **Definitions and background.** All forms considered will be bilinear and either symmetric or skew symmetric. For a field of characteristic 2 a symmetric form is skew symmetric and vice versa.

The terminology and notation are as in [1, Chapter III].

A bilinear form f defined on a vector space V is called nondegenerate if $f(x, v)=0$ for all v in V implies $x=0$. A subspace U of V is called nonsingular if f restricted to U is nondegenerate.

A form f is called alternating if $f(x, x)=0$ for all x in V. Otherwise f is called nonalternating.

If U is a subspace of V, U^* is the set of all x in V such that $f(x, u)=0$ for all u in U, and U^* is a subspace.

A one-one linear transformation σ from V onto W such that $f'(\sigma(x), \sigma(y))=f(x, y)$ for all x and y in V is called an isometry, where f' is a form on W.

LEMMA 1. *If V is nonsingular and $U \subset V$, then $U^{**}=U$ and* $\dim U + \dim U^* = \dim V$.

LEMMA 2. *If V is nonsingular and $U \subset V$, then U is nonsingular if and only if U^* is and in that case $V = U \perp U^*$.*

LEMMA 3. *If $U \subset V$, then $U=(U \cap U^*) \perp A$ where A is any complement of $U \cap U^*$ in U. A is nonsingular.*

Lemmas 1, 2 and 3 are proved in Artin [1, Chapter III] for symmetric nonalternating forms over a field of characteristic $\neq 2$ and for

Presented to the Society, July 16, 1963; received by the editors July 10, 1963.

skew symmetric alternating forms over any field. These proofs are also valid for symmetric nonalternating forms over a field of characteristic 2.

A space with an alternating bilinear form defined on it is called symplectic. Witt's theorem, which we will now state, holds for symplectic spaces over fields of any characteristic.

WITT'S THEOREM (FOR SYMPLECTIC SPACES) [1, p. 121]. *Let V and V' be nonsingular symplectic spaces which are isometric under some isometry ρ. Let σ be an isometry of a subspace U of V into V'. Then σ can be extended to an isometry of V onto V'.*

Note that two nonsingular symplectic spaces of the same dimension and over the same field are hyperbolic spaces and hence isometric [1, p. 119].

III. **Characteristic 2 case.** In this section we let V (V') be a vector space, nonsingular with respect to a nonalternating form f (f'), of dimension n over a field K of characteristic 2. Let $f(x, x)$ ($f'(x', x')$) take its values in a subfield K^* contained in or equal to K. Then we assume (unless otherwise stated) that K contains the square root of any element of K^*. Note that this is automatically satisfied if K^* is a finite field since all finite fields of characteristic 2 are perfect.

THEOREM 1. *V has an orthonormal basis.*

PROOF. Under the assumption that f is a nonalternating, nondegenerate form on a vector space V over a field of characteristic 2, Jacobson [2, p. 170] proves that V has an orthogonal basis e_i. If $f(e_i, e_i) = \alpha_i$ we can replace e_i by $e_i/\sqrt{\alpha_i}$ by our assumption on K.

COROLLARY 1. *If V and V' have the same dimension and are over the same field they are isometric.*

THEOREM 2. *There exists a unique vector h in V such that $f(h, x) = \sqrt{f(x, x)}$ for all x in V. In addition $h = \sum_{i=1}^{n} e_i$, where the e_i are the members of any orthonormal basis in V.*

PROOF. Let $e_1, \cdots, e_n$ be such a basis and let $h = \sum_{i=1}^{n} e_i$. If x is in V, $x = \sum_{i=1}^{n} \alpha_i e_i$ so that $f(h, x) = \sum_{i=1}^{n} \alpha_i$. But $f(x, x) = \sum_{i=1}^{n} \alpha_i^2 = (\sum_{i=1}^{n} \alpha_i)^2$. Hence $f(h, x) = \sqrt{f(x, x)}$ for all x in V. If g were another vector such that $f(g, x) = \sqrt{f(x, x)}$ for all x in V, then $f(h-g, x) = 0$ for all x in V and $h-g=0$ by the nondegeneracy of f. An interesting consequence of this is that h has the representation as the all-one vector regardless of the orthonormal basis chosen.

COROLLARY 2.1. *If f is a nonalternating, nondegenerate form on a vector space V over a field of characteristic 2, then V has an orthonormal basis if and only if K contains the square root of every element of K*.*

COROLLARY 2.2. *Let V be as in the theorem. Let $N=\{x \text{ in } V \mid f(x, x)=0\}$. Then N is a subspace of V. In addition $N=\langle h\rangle^*$ and hence* dim $N=n-1$. *If n is odd, N is nonsingular. If n is even, h is in N.*

PROOF. That $N=\langle h\rangle^*$ follows from the equation $f(h, x)=\sqrt{f(x, x)}$. If n is odd, $f(h, h)=1$ and $\langle h\rangle$ is nonsingular so that $N=\langle h\rangle^*$ is nonsingular by Lemma 2. If n is even, $f(h, h)=0$ and h is in N.

If V is of odd dimension, note that $V=\langle h\rangle \perp N$ and $N=\langle h\rangle^*$ is symplectic.

If V is of even dimension, and s is such that $f(s, s)=1$, then $f(s, h)=1$ and $\langle h, s\rangle$ is nonsingular. Hence $V=\langle h, s\rangle \perp H$, where $H=\langle h, s\rangle^*$ is nonsingular and symplectic.

THEOREM 3. *Let V and V' be of the same dimension and defined over the same field K. Let ρ be the isometry between V and V' given by Corollary* 1. *Let σ be an isometry of a subspace U of V into V'. Then σ can be extended to an isometry on all of V if and only if*

(1) *h is in U if and only if $\rho(h)$ is in $\sigma(U)$ and*

(2) *in case h is in U, $\sigma(h)=\rho(h)$.*

PROOF. If h is not in U, $\rho(h)$ is not in $\sigma(U)$ and in that event we can extend σ to $\langle h\rangle + U$ by defining $\sigma(h)=\rho(h)$. σ is still an isometry since $f(h, u)=\sqrt{f(u, u)}=\sqrt{f(\sigma(u), \sigma(u))}=f(\rho(h), \sigma(u))=f(\sigma(h), \sigma(u))$ for all u in U and $f(h, h)=f(\rho(h), \rho(h))$. Hence we may assume that h is in U, $\rho(h)$ is in $\sigma(U)$ and $\sigma(h)=\rho(h)$.

If W is a subspace of U we shall write σ_W for the restriction of σ to W.

If V is the direct sum of mutually orthogonal subspaces V_i, and τ_i are isometries defined on the respective V_i, then the mapping τ given by $\tau(v)=\tau(\sum v_i)=\sum \tau_i(v_i)$ is an isometry on V (v_i in V_i). For two subspaces this will be denoted as $\tau_1 \perp \tau_2$.

Consider three cases. The first case is V of odd dimension. Then $U=\langle h\rangle \perp (U \cap N)$ and σ induces an isometry between $U \cap N$ and $\sigma(U) \cap N'$ which can be extended to an isometry τ on all of N by Witt's theorem in the symplectic case. Then $1_{\langle h\rangle} \perp \tau$ is the desired extension.

The second case is V of even dimension and U contains an element s such that $f(s, s) \neq 0$. Then we can assume $f(s, s)=f(h, s)=1$. Now

$U=\langle h, s\rangle\perp(U\cap H)$ and $U'=\langle\rho(h), \sigma(s)\rangle\perp(\sigma(U)\cap\langle\rho(h), \sigma(s)\rangle^*)$. The isometry induced by σ between $U\cap H$ and $\sigma(U)\cap\langle\rho(h), \sigma(s)\rangle^*$ can again be extended to an isometry τ of H onto $\langle\rho(h), \sigma(s)\rangle^*$. Then $\sigma_{H^*}\perp\tau$ is an extension of σ.

The third case is V of even dimension and U contained in N. Here we write U as $\langle h\rangle\perp C$ where C is any complement of h in U. Write U' as $\langle\rho(h)\rangle\perp\sigma(C)$. There is an s (s') in C^* ($\sigma(C)^*$) such that $f(s, s)=f(h, s)=1$ and $f'(s', s')=f'(\rho(h), s')=1$. Extend σ to $U+\langle s\rangle$ by defining $\sigma(s)=s'$. Now we are reduced to the second case.

It is clear that any isometry of V onto V' sends an orthonormal basis onto an orthonormal basis and hence must send the sum h into the sum $\rho(h)$. By the preceding theorem, h is the sum of any orthonormal basis.

COROLLARY 3.1. *Any isotropic space is contained in an isotropic space of maximal dimension ν. If n is odd, $\nu=(n-1)/2$. If n is even, $\nu=n/2$.*

PROOF. If n is odd, the isotropic space W cannot contain h and so any one-one linear transformation of W into a maximal isotropic space M is an isometry which can be extended to an isometry σ on V, and W is then contained in the maximal isotropic space $\sigma^{-1}(M)$.

If n is even, h is in any maximal isotropic space and if h is not in the given isotropic space W, we can adjoin it to W and make sure the one-one linear transformation sends h into h. Then we are in the same situation as above.

If $e_1, \cdots, e_n$ is an orthonormal basis of V and n is odd, e_1+e_2, $e_3+e_4, \cdots, e_{n-2}+e_{n-1}$ generate an isotropic space of $\dim(n-1)/2$ and it can be shown by direct computation that there is no self-orthogonal vector orthogonal to it so that it must be maximal isotropic. If n is even, $e_1+e_2, e_3+e_4, \cdots, e_{n-1}+e_n$ generate a maximal isotropic space of dim $n/2$ for similar reasons.

If U and U' are subspaces of V, then we say $U\sim U'$ if there is an isometry on V sending U onto U'. This is an equivalence relation.

The set of isometries with respect to a given f from V onto V form a group called the orthogonal group of V.

COROLLARY 3.2. *A subspace U of V has exactly four invariants under the orthogonal group. They are the four numbers* dim U, $\dim(U\cap U^*)$, $\dim(U\cap N)$, $\dim(U\cap\langle h\rangle)$.

Hence $U\sim U'$ if and only if they have the same invariant numbers.

PROOF. The necessity is obvious. To prove the sufficiency we consider two situations.

SUPPOSITION A. $U\cap\langle h\rangle = U'\cap\langle h\rangle = 0$.

Because of Theorem 3 we have only to prove that there is an isometry sending U onto U'.

By Lemma 3 we can write U as $(U\cap U^*)\perp A$ and U' as $(U'\cap U'^*)\perp A'$ where A and A' are nonsingular. Since $U\cap U^*$ and $U'\cap U'^*$ are isotropic and have by assumption the same dimension, they are isometric.

Case 1. Assume $U\subset N$. Then by assumption $U'\subset N$ and A and A' are isometric since they are nonsingular symplectic spaces of the same dimension.

Case 2. Assume $U\not\subset N$. Then $U'\not\subset N$ and it follows that A and A' have orthonormal bases and so are isometric.

SUPPOSITION B. $U\cap\langle h\rangle = U'\cap\langle h\rangle = \langle h\rangle$.

Here we have to show that there is an isometry of U onto U' which sends h into h.

Case 3. Assume dim V is odd. Then $U=\langle h\rangle\perp(U\cap N)$ and $U'=\langle h\rangle\perp(U'\cap N)$. Let $A=U\cap N$ and $A'=U'\cap N$.

Since $A\cap A^*=U\cap U^*$ and $A'\cap A'^*=U'\cap U'^*$, $\dim(A\cap A^*)=\dim(A'\cap A'^*)$. Now A and A' have the same properties as U and U' in Case 1 and hence are isometric. We extend this isometry to all of U by sending h into h.

Case 4. Assume dim V is even and $U\subset N$. Then by assumption $U'\subset N$. As in Theorem 3 we write U as $\langle h\rangle\perp C$ and U' as $\langle h\rangle\perp C'$. Now $\dim(C\cap C^*)=\dim(U\cap U^*)-1$ and $\dim(C'\cap C'^*)=\dim(U'\cap U'^*)-1$ so that $\dim(C\cap C^*)=\dim(C'\cap C'^*)$. Hence C and C' play the roles of U and U' in Case 1 and are isometric. Again we send h into h.

Case 5. Assume dim V is even and $U\not\subset N$. This implies $U'\not\subset N$. We then have $U=\langle h, s\rangle\perp(U\cap H)$ and $U'=\langle h, s'\rangle\perp(U'\cap\langle h, s'\rangle^*)$ where $f(s, s)=f(s, h)=f(s', s')=f(s', h)=1$ as in Theorem 3. Let $A=U\cap H$ and $A'=U'\cap\langle h, s'\rangle^*$. Both A and A' are contained in N. Since $A\cap A^*=U\cap U^*$ and $A'\cap A'^*=U'\cap U'^*$, $\dim(A\cap A^*)=\dim(A'\cap A'^*)$. Again, by Case 1, A and A' are isometric. We extend this isometry to all of U by sending h into h and s into s'.

I wish to acknowledge several stimulating discussions with Professor A. M. Gleason and Mr. E. Prange. I wish to thank the referee for suggestions in simplifying Theorem 3 and Corollary 3.2.

REFERENCES

1. E. Artin, *Geometric algebra*, Interscience Tracts in Pure and Applied Mathematics No. 3, Interscience, New York, 1957.

2. N. Jacobson, *Lectures in abstract algebra*, Vol. II, Van Nostrand, New York, 1953.

AIR FORCE CAMBRIDGE RESEARCH LABORATORIES, BEDFORD, MASSACHUSETTS