ON THE INVARIANTS OF A VECTOR SUBSPACE OF A VECTOR SPACE OVER A FIELD OF CHARACTERISTIC TWO

VERA PLESS

1. Introduction. Witt's theorem is concerned with the extension of an isometry between subspaces to an isometry on the whole space. The most general form of Witt's theorem is Theorem 1.2.1 in Wall [3]. Theorem 1 of this paper extends Theorem 1.2.1 and is identical to it in case the characteristic of the division ring is not 2. Theorem 2 is a variant of Theorem 1. Theorems 1 and 2 are concerned with sesquilinear forms. Theorems 3 and 4 are concerned with bilinear forms on a finite dimensional vector space over a field of characteristic 2. Theorem 3 gives necessary and sufficient conditions for two (possibly degenerate) forms to be equivalent. Theorem 4 gives necessary and sufficient conditions for two subspaces to be equivalent.

The original results of this paper were based on results in Dieudonné [1]. However, the referee kindly pointed out that the proofs can be simplified and some of the results generalized by using results in Wall [3]. In particular he pointed out that Wall's proof is valid for the results stated in Theorem 1 as the restrictions contained in Theorem 1.2.1, are not necessary. He also suggested the variant on Theorem 1 which is Theorem 2. The proof of Theorem 4 has been considerably simplified by the use of Theorem 2. I wish to thank the referee for these suggestions as it allows me to present these results in a more elegant and simplified form.

I also wish to thank Professor A. M. Gleason for stimulating discussions and advice, and Mr. E. Prange for discussions and for pointing out to me a proof of a weaker version of Theorem 1.

2. Notation. Let \( V \) be a vector space of possibly infinite dimension over a division ring \( D \) with a fixed involutory anti-automorphism \( J \), that is, a one-to-one mapping \( \alpha \rightarrow \alpha' \) of \( D \) onto itself such that \( (\alpha + \beta)' = \alpha' + \beta' \), \((\alpha\beta)' = \beta'\alpha' \), and \( \alpha'^2 = \alpha \). An Hermitian (skew-Hermitian) sesquilinear form on \( V \) is a mapping \( f: V \times V \rightarrow D \) such that \( f(x, y) \) is linear in \( x \) for each fixed \( y \) and \( f(y, x) = f(x, y)' \) \( (f(y, x) = -f(x, y)) \). If the characteristic of \( D \) is two, the distinction between Hermitian and skew-Hermitian forms disappears.

Two forms \( f_1 \) and \( f_2 \) are called equivalent if there is a linear trans-
formation $\sigma$ of $V_1$ onto $V_2$ with the property that

$$f_1(x, y) = f_2(\sigma(x), \sigma(y))$$

for all $x$ and $y$ in $V_1$; and $\sigma$ is called an isometry.

If $W \subset V$, $W^\perp$ is the set of all $y$ in $V$ such that $f(x, y) = 0$ for all $x$ in $W$.

A form $f$ is called nondegenerate if $V^\perp = 0$. Otherwise $f$ is called degenerate.

3. Witt's theorem. Let $f$ be a nondegenerate Hermitian or skew-Hermitian form on $V$. The set of all isometries of $V$ onto itself forms the unitary group $U(f)$. If $\sigma$ is in $U(f)$ and the range of $I - \sigma$ is finite dimensional, then $\sigma$ is said to be finite dimensional. The finite dimensional elements of $U(f)$ form a normal subgroup of $U_h(f)$.

If $x$ is in $V$, we call $x$ trace-valued if $f(x, x) = \lambda + e\lambda'$, $e = \pm 1$, for some $\lambda$ in $D$. By Lemma 1.2.1 in [3] the set of trace-valued vectors in $V$ forms a subspace $V^r$ of $V$. If the characteristic of $D$ is not 2, $V^r = V$.

The most general form of Witt's theorem is Wall's Theorem 1.2.1 [3] which we now state.

**Theorem 1.2.1 (Witt).** Let $W_1$, $W_2$ be finite dimensional subspaces of $V^r$ such that $W_1 \cap (V^r)^\perp = W_2 \cap (V^r)^\perp = \{0\}$. Then every isometry $\sigma$ of $W_1$ onto $W_2$ can be extended to an element of $U_h(f)$.

The following is an extension of the preceding theorem and a generalization of the characteristic two case in [2].

**Theorem 1 (Witt).** Let $W_1$, $W_2$ be finite dimensional subspaces of $V$ such that $W_1 \cap (V^r)^\perp = W_2 \cap (V^r)^\perp$. Then every isometry of $W_1$ onto $W_2$ which is the identity on $W_1 \cap (V^r)^\perp$ can be extended to an element of $U_h(f)$.

**Proof.** By Lemma 1.2.2, Corollary [3], every element in $U(f)$ leaves $(V^r)^\perp$ pointwise invariant. Hence it is enough to be able to extend the isometry to an element of $U_h(f)$ under the assumption that $W_1 \cap (V^r)^\perp = W_2 \cap (V^r)^\perp = \{0\}$. This can be proved by following Wall's proof of Theorem 1.2.1 and deleting the restriction that $W_1, W_2 \subset V^r$. This restriction is nowhere needed in the proof. Q.E.D.

If $W_1$ and $W_2$ are subspaces of $V$ and $W_1$ is isometric to $W_2$ by an isometry in $U_h(f)$ we will call $W_1$ and $W_2$ equivalent. Theorem 2 is a variant of Theorem 1.

**Theorem 2.** If $W_1$ and $W_2$ are finite dimensional subspaces of $V$, then $W_1$ is equivalent to $W_2$ if, and only if, (1) $W_1 \cap (V^r)^\perp = W_2 \cap (V^r)^\perp$ and (2) $W_1$ is isometric to $W_2$. 
Proof. The first condition is necessary by Lemma 1.2.2, Corollary in [3]. To prove the sufficiency we need only show that there is an isometry $\omega$ sending $W_1$ onto $W_2$ which sends $W_1 \cap (V^\perp)^\perp$ onto $W_2 \cap (V^\perp)^\perp$. Then $\omega$ would send a complement of $W_1 \cap (V^\perp)^\perp$ in $W_1$ onto a complement of $W_2 \cap (V^\perp)^\perp$ in $W_2$. Hence by the proof of Theorem 1, there exists a $\sigma$ in $U_2(f)$ sending $W_1$ onto $W_2$.

To establish the existence of $\omega$, let $\rho$ be an isometry of $W_1$ onto $W_2$ such that the subspace $X = \{x \mid x \text{ is in } W_1 \cap (V^\perp)^\perp \text{ and } \rho(x) \text{ is in } W_2 \cap (V^\perp)^\perp\}$ have as large a dimension as possible. We assert $X$ equals $W_1 \cap (V^\perp)^\perp$. We will prove this by contradiction. Suppose that $X$ does not equal $W_1 \cap (V^\perp)^\perp$. Then there is an $a$ in $W_1 \cap (V^\perp)^\perp$ with $\rho(a)$ not in $W_2 \cap (V^\perp)^\perp$. Hence it is possible to find an $a$ such that in addition to $a \in W_1 \cap (V^\perp)^\perp$, $\rho(a) \in W_2 \cap (V^\perp)^\perp$, we have $a = \rho(b)$ where $b \in W_1$, $b \in W_2 \cap (V^\perp)^\perp$. Let $Y'$ be the subspace generated by $a$ and $b$. Then $\dim Y' = 2$ and $X \cap Y' = 0$. Hence we can choose a complement $Y$ of $Y'$ in $W_1$ such that $X \subset Y$.

Now we define a new isometry $\psi$ of $W_1$ onto $W_2$ as follows. $\psi(x) = \rho(x)$ for $x$ in $Y$, $\psi(a) = a$. $\psi(b) = \rho(a)$. If $\psi$ is indeed an isometry we will have our contradiction. Clearly $\psi$ is one-to-one so we have to verify that $f(\psi(x), a) = f(x, a)$ and $f(\psi(x), \rho(a)) = f(x, b)$ for all $x$ in $W_1$. By Lemma 1.2.2, Corollary [3], $\rho(x) - x$ is in $V^\perp$ for all $x$ in $V$ so that $f(\rho(x), a) = f(x, a)$ for all $x$ in $W_1$. If $x$ is in $Y$, $f(\psi(x), a) = f(\rho(x), a) = f(x, a)$. It can be shown that $f(\psi(b), a) = f(b, a)$ also, so that $f(\psi(x), a) = f(x, a)$ for all $x$ in $W_1$. For $x$ in $Y$, $f(\psi(x), \rho(a)) = f(\rho(x), \rho(a)) = f(x, a) = f(\rho(x), a) = f(\rho(x), \rho(b)) = f(x, b)$. It can also be shown that $f(\psi(a), \rho(a)) = f(a, b)$, so that $f(\psi(x), \rho(a)) = f(x, b)$ for all $x$ in $W_1$. Q.E.D.

A subspace $W \subset V$ is called isotropic if $f(x, y) = 0$ for all $x$ and $y$ in $W$.

Corollary 2.1. If $W_1$ and $W_2$ are two isotropic subspaces of $V$ such that $W_1 \cap (V^\perp)^\perp = W_2 \cap (V^\perp)^\perp$, $W_1$ and $W_2$ are equivalent.

4. Invariants. In this section we assume that $V$ is finite dimensional, $J$ is the identity, and $D$ is a field of characteristic two. Under these assumptions $f$ is a nondegenerate symmetric bilinear form, and $V^\perp$ is the set of all $x$ such that $f(x, x) = 0$. Let $m = \dim V$.

Since $\lambda \mapsto \lambda^2$ is an automorphism of $D$ into $D^2$, the mapping $\theta: x \mapsto f(x, x)$ is a semi-linear transformation of $V$ into the vector space $D$ over the field $D^2$. Let $W = \theta(V)$. Clearly $W$ is a subspace of $D$ over $D^2$. $V^\perp$ equals $\theta^{-1}(0)$. Let $U = \theta((V^\perp)^\perp)$ and let $l = \dim U$.

Corollary 2.2. Any isotropic space is contained in an isotropic space of maximal dimension $\nu$. In addition $\nu = (m - l)/2$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Given any isotropic space $U$, we can find a subspace $U'$ of a maximal isotropic space $M$ such that $U \cap (V^r)^\perp = U' \cap (V^r)^\perp$. Hence there is a $\sigma$ in $U(f)$ such that $\sigma(U) = U'$ and $U$ is thus contained in the maximal isotropic space $\sigma^{-1}(M)$.

It can be shown that the direct sum of a maximal isotropic space in a complement of $Vr \cap (V^r)^\perp$ in $V^r$ and $Vr \cap (V^r)^\perp$ is a maximal isotropic subspace of $V$. Hence,

\[ v = \dim V^r \cap (V^r)^\perp + \frac{\dim V^r - \dim V^r \cap (V^r)^\perp}{2} \]
\[ \quad = \frac{\dim V^r + \dim V^r \cap (V^r)^\perp}{2} \]
\[ \quad = \frac{m - (\dim(V^r)^\perp - \dim V^r \cap (V^r)^\perp)}{2} \]
\[ \quad = \frac{m - 1}{2}. \]

On p. 51 of [3], Wall has shown that $\langle f(x, x), f(y, y) \rangle = f(x, y)$ for $x$ and $y$ in $(V^r)^\perp$ uniquely defines a function $\gamma = (\lambda, \mu)$ of the variables $\lambda, \mu$ in $U$. Lemma 3.4.2 of [3] states that two nondegenerate forms are equivalent if, and only if, they have the same $W$, $U$, and $\gamma$. If $f$ is a degenerate form let $d(f) = \dim V \cap V^\perp$. Then it follows that two (possibly degenerate) forms are equivalent if, and only if, they have the same $W$, $U$, $\gamma$, and $d$.

If $f_1$ and $f_2$ are two forms on $V$, let $V'_1$ denote the $V^r$ for $f_1$ and $V'_2$ denote the $V^r$ for $f_2$.

Theorem 3. Two (possibly degenerate) forms $f_1$ and $f_2$ are equivalent if, and only if,

1. $\{f_1(x, x)\} = \{f_2(x, x)\}$
2. $(V'_1)^\perp$ is isometric to $(V'_2)^\perp$.

Proof. By the above discussion on $W$, $U$, $\gamma$, and $d$, it is enough to show that if two forms $f_1$ and $f_2$ satisfy conditions (1) and (2) they have the same $W$, $U$, $\gamma$, and $d$.

Clearly if $f_1$ and $f_2$ satisfy condition (1) they have the same $W$. Also if $f_1$ and $f_2$ satisfy condition (2) it is not hard to see that they must have the same $U$ and $\gamma$.

To see that $f_1$ and $f_2$ have the same $d$ note that

\[ d(f_i) = \dim V'_i + \dim(V'_i)^\perp - \dim V \]
\[ = m - \dim W + \dim(V'_i)^\perp - m \]
\[ = \dim(V'_i)^\perp - \dim W. \quad \text{Q.E.D.} \]
In [2] it was shown that any two nondegenerate forms $f_1$ and $f_2$ are equivalent under the condition that $f_1(x, x)$ and $f_2(x, x)$ both take their values in a perfect subfield of $D$. The next corollary shows that this is true for any two nondegenerate forms whose $W$'s are the same one-dimensional subspace of $D$.

**Corollary 3.1.** If $f_1$ and $f_2$ are nondegenerate forms, each with a one-dimensional $W$, then $f_1$ is equivalent to $f_2$ if, and only if, condition (1) holds.

**Proof.** Since $\dim(V_1) = \dim(V_2)$, $\dim((V_1)^\perp) = \dim((V_2)^\perp) = 1$. Hence $(V_1)^\perp$ is isometric to $(V_2)^\perp$ if, and only if, either both are isotropic or both are not isotropic. It is known (p. 50 of [3]) that $\dim((V_1)^\perp) = m(2)$ and $\dim((V_2)^\perp) = m(2)$ so that $(V_1)^\perp$ and $(V_2)^\perp$ will be isotropic when $m$ is even, not isotropic when $m$ is odd.

**Remark.** If $f_1$ and $f_2$ are (possibly degenerate) forms, each with a one-dimensional $W$, then $f_1$ is equivalent to $f_2$ if, and only if condition (1) holds and $d(f_1) = d(f_2)$.

**Theorem 4.** Let $W_1, W_2$ be subspaces of $V$. Then $W_1$ is equivalent to $W_2$ if, and only if:

1. $\dim W_1 = \dim W_2$, and
2. $W_1 \cap (V^\perp) = W_2 \cap (V^\perp)$, and
3. $W_1^\perp \cap (V^\perp) = W_2^\perp \cap (V^\perp)$, and
4. $W_1 \cap V^\perp$ is isometric to $(W_2 \cap V^\perp)$.

**Proof.** Conditions (2) and (3) are necessary by Lemma 1.2.2, Corollary [3]. Conditions (1) and (4) are obviously necessary.

To prove the sufficiency we will first show that conditions (1), (3), and (4) imply that $W_1$ is isometric to $W_2$. Then the theorem follows from condition (2) and Theorem 2. Theorem 3 shows that $W_1$ and $W_2$ are isometric. This follows since condition (4) gives us condition (2) in Theorem 3 immediately. Condition (3) is equivalent to $W_1 + V^\perp = W_2 + V^\perp$ which implies condition (1) in Theorem 3.

The next corollary shows that these conditions are somewhat simpler for the situation where $\dim W = 1$ and is a generalization of Corollary 3.2 in [2].

**Corollary 4.1.** If $\dim W = 1$, then two subspaces $W_1$ and $W_2$ of $V$ are equivalent if, and only if:

1. $\dim W_1 = \dim W_2$, and
2. $W_1 \cap (V^\perp) = W_2 \cap (V^\perp)$, and
3. $W_1 \cap V^\perp = W_2 \cap V^\perp$, and
4. $W_1 \cap W_1^\perp = W_2 \cap W_2^\perp$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. These conditions are necessary by Theorem 4. The sufficiency is proved in a fashion similar to the proof of Theorem 4.

By (1) and (3) \( \dim \theta(W_1) = \dim \theta(W_2) \). Since \( \dim W = 1 \), either \( \dim \theta(W_1) \) and \( \dim \theta(W_2) \) are both 1 or both 0. Since condition (3) implies \( W_1 + V_r = W_2 + V_r \), if both dimensions are 1, \( W_1 \) and \( W_2 \) are isometric by the Remark to Corollary 3.1. In case both dimensions are 0, conditions (1) and (4) are the known conditions for two symplectic spaces to be isometric.

Noting that condition (2) implies \( W_1 \cap (V_r)^\perp = W_2 \cap (V_r)^\perp \), Theorem 2 tells us that \( W_1 \) and \( W_2 \) are equivalent.

Remark. If \( (V_r)^\perp = 0 \), Theorems 3 and 4 are known [1] theorems for nondegenerate, alternating forms on spaces over fields of any characteristic.

References