Transformations which are Products of Two Involutions

MARIA J. WONENBURGER

Communicated by G.-C. ROTA

We are going to give a necessary and sufficient condition for a linear transformation of a finite dimensional vector space M over a field F to be the product of two involutions. *It will always be assumed* in this paper *that the characteristic of* $F \neq 2$. When we have a non-degenerate symmetric bilinear form over M, we will see that the orthogonal transformations satisfy the condition and the two involutions can be chosen to be orthogonal involutions. In the case of a non-degenerate skew-symmetric bilinear form the condition is also satisfied by the sympletic transformations but in the decomposition the involutions are not sympletic transformations but skew-sympletic according to the definition given below.

We assume that the reader is familiar with the theory of invariant factors, similarity of transformations and bilinear forms. Some of the relevant definitions and concepts will be recalled in the sequel, but the reader who wants a more thorough information may consult [2] specially chapters III and V, or [3].

1. It will be convenient to recall first some properties of polynomials with coefficients in the field F and introduce some definitions.

We will say that the polynomial $\tilde{p}(x)$ is the reciprocal of the polynomial $p(x)$ if $\tilde{p}(x)$ is monic, that is, its leading coefficient is 1, and its roots are the inverses of the roots of $p(x)$ with the corresponding multiplicities. It is clear then that a polynomial $p(x)$ has a reciprocal if and only if its roots are different from zero, that is, $p(0) \neq 0$. When $\deg p(x) = m$, $\tilde{p}(x) = p(0)^{-1}x^m p(1/x)$ and $\tilde{\tilde{p}}(x) = p(x)$ if $p(x)$ is monic. *A monic polynomial will be called self-reciprocal if* $p(x) = \tilde{p}(x)$; then $p(0) = \pm 1$.

When the monic polynomial $p(x)$ is self-reciprocal, if $\alpha \neq 0$ is a root of $p(x)$ of multiplicity h, α^{-1} is also a root of multiplicity h. Thus we can write

$$p(x) = r(x)(x+1)^s(x-1)^t, \tag{1}$$

where $r(x)$ is a polynomial of even degree $2m$, such that $r(1) \neq 0$, $r(-1) \neq 0$ and

Journal of Mathematics and Mechanics, Vol. 16, No. 4 (1966).

$$r(x) = \sum_{i=0}^{2m} a_i x^i$$

with $a_i = a_{2m-i}$ and $a_{2m} = 1$. In general we will call a monic polynomial $g(x)$ of degree n symmetric if $g(x) = \sum_0^n a_i x^i$ with $a_i = a_{n-i}$. It is clear that any symmetric polynomial is self-reciprocal.

Any monic irreducible polynomial $g(x)$ of the ring $F[x]$ is either self-reciprocal or it can not contain as roots an element $\alpha \neq 0$ and its inverse, for the monic greatest common divisor of $g(x)$ and $\tilde{g}(x)$ must be either $g(x)$ or 1. Let $p(x)$ be a reciprocal polynomial and

$$\prod_{i=1}^{t} g_i(x)^{h_i}$$

its decomposition in powers of distinct irreducible polynomials. Assume that for $1 \leqq i \leqq f$, $g_i(x)$ is self-reciprocal and that for $i > f$, $\tilde{g}_{f+2v-1}(x) = g_{f+2v}(x)$, so that we must have $h_{f+2v-1} = h_{f+2v}$. Denoting by $r_i(x)$ the self-reciprocal polynomial $g_i(x)$ and by $r_{f+v}(x)$ the self-reciprocal polynomial $g_{f+2v-1}(x)g_{f+2v}(x)$ we have

$$p(x) = \prod_{1}^{m} r_i(x)^{v_i}. \tag{2}$$

The expression (2) will be called the decomposition of $p(x)$ in irreducible self-reciprocal factors.

2. Let M be a finite dimensional vector space over the field F. It is well-known that any involution H, that is, a linear transformation whose square equals the identity, defines and it is defined by a decomposition of M in a direct sum of two subspaces $M = M^+ \oplus M^-$, where $M^+ = \{x \in M \mid xH = x\}$ and $M^- = \{x \in M \mid xH = -x\}$. If a linear transformation $L = H_1H_2$, where H_1 and H_2 are involutions, then $L^{-1} = H_2H_1 = H_1LH_1$, that is, L is an invertible linear transformation which is similar to its inverse. We will show presently that the converse is also true.

A subspace M_1 of the vector space M is invariant with respect to the linear transformation L if $M_1L \subset M_1$ where $M_1L = \{u \in M \mid u = vL \text{ for some } v \in M\}$. Let $M = M_1 \oplus M_2 \oplus \cdots \oplus M_t$ be a decomposition of M in direct sum of subspaces invariant with respect to L, then we will denote by L_i the restriction of L to M_i and will write $L = L_1 \oplus L_2 \oplus \cdots \oplus L_t$. In general, given a decomposition $M = \sum \oplus M_i$ we will denote by $U = \sum \oplus U_i$ the linear transformation of M whose restriction to M_i coincides with U_i. Clearly, if $V = \sum \oplus V_i$, then $UV = \sum \oplus U_iV_i$.

We recall also that a subspace N of dimension n, invariant with respect to the transformation L, is called cyclic if there exists an element u such that u, uL, uL^2, $\cdots$, uL^{n-1} is a basis of N. We say that u generates N. When M is cyclic we say that L is a cyclic linear transformation.

Theorem 1. *Let M be a finite dimensional vector space and L a linear transformation of M into itself. Then L is the product of two involutions if and only if L is invertible and similar to L^{-1}.*

Proof. We have just remarked that the condition is necessary. To prove that it is sufficient we must remember that if $\delta_1(x)$, $\delta_2(x)$, $\cdots$, $\delta_t(x)$ are the the invariant factors of L the invariant factors of L^{-1} are their reciprocals $\bar{\delta}_1(x)$, $\cdots$, $\bar{\delta}_t(x)$ (see *e.g.* [3, Section 65]). Now if L^{-1} is similar to L both transformations must have the same invariant factors, therefore every $\delta_i(x)$ is self-reciprocal. Let us decompose M in direct sum of subspaces

$$M = \sum_1^t \oplus M_i ,$$

where M_i is cyclic subspace with respect to L such that the restriction L_i of L to M has minimum polynomial $\delta_i(x)$. Hence $L = \sum \oplus L_i$ and if we show that $L_i = H_{i1}H_{i2}$, where H_{i1} and H_{i2} are involutions for $i = 1, 2, \cdots, t$, then $L = H_1H_2$, where $H_j = \sum_{i=1}^t H_{ij}$ is an involution for $j = 1, 2$.

So the problem is to show that each L_i is the product of two involutions when L_i is a cyclic linear transformation whose characteristic polynomial $\delta_i(x)$ is self-reciprocal. Decomposing $\delta_i(x) = r(x)(x + 1)^{s_1}(x - 1)^{s_{-1}}$ as in (1) we get

$$M_i = N_0 \oplus N_1 \oplus N_{-1}$$

where the terms in the right are the null spaces of the transformations $r(L_i)$, $(L_i + 1)^{s_1}$ and $(L_i - 1)^{s_{-1}}$ respectively. Let $L_i = U = U_0 \oplus U_1 \oplus U_{-1}$ be the corresponding decomposition of L_i. We only need prove that each U_i is the product of two involutions. We consider two cases.

Case 1. S is a cyclic transformation of the linear space N whose characteristic polynomial is symmetric and of even degree $2m$. This is the situation of the U_0 considered above and of U_ϵ if s_ϵ is even, $\epsilon = \pm 1$. We choose a vector u which generates N. Then $u, uS, \cdots, uS^{2m-1}$ is a basis of N which is represented by $yS^{-m}, yS^{-m+1}, \cdots, y, \cdots, yS^{m-1}$, if we take $y = uS^m$. We take a new basis consisting of the two sequences of vectors.

$$y, y(S + S^1), \cdots, y(S^{m-1} + S^{-m+1}) \tag{3}$$

and

$$y(S - S^{-1}), y(S^2 - S^{-2}), \cdots, y(S^m - S^{-m}) \tag{4}$$

which is also a basis since the independent term of the characteristic polynomial is 1.

Now it is easily verified that the subspaces P and Q spanned by the vectors (3) and (4) respectively are invariant with respect to the transformation $S + S^{-1}$. For

$$y(S^i + S^{-i})(S + S^{-1}) = y(S^{i+1} + S^{-(i+1)}) + y(S^{i-1} + S^{-(i-1)})$$

which also belongs to P if $0 < i < m - 1$, and when $i = m - 1$ this is also the case since

$$S^m + S^{-m} = -a_m - \sum_1^{m-1} a_{m-i}(S^i + S^{-i}).$$

Similarly we see that the transformation $S - S^{-1}$ takes any vector $y(S^i + S^{-i})$ into

$$y(S^i + S^{-i})(S - S^{-1}) = y(S^{i+1} - S^{-i-1}) - y(S^{i-1} - S^{-i+1})$$

which obviously belongs to Q for $0 \leqq i \leqq m - 1$ and hence

$$P(S - S^{-1}) = Q. \tag{5}$$

This equality together with

$$P(S + S^{-1}) \subset P \tag{6}$$

implies

$$Q(S + S^{-1}) = P(S - S^{-1})(S + S^{-1}) \subset P(S - S^{-1}) = Q \tag{7}$$

and

$$Q(S - S^{-1}) = P(S - S^{-1})^2 = P[(S + S^{-1})^2 + 4] \subset P. \tag{8}$$

Now we define H as the involution of N whose plus and minus-spaces are P and Q respectively. It follows from (6) and (7) that

$$(S + S^{-1})H = H(S + S^{-1}), \tag{9}$$

and from (5) and (8) that

$$(S - S^{-1})H = -H(S - S^{-1}). \tag{10}$$

Adding (9) and (10) and dividing by 2 we get

$$SH = HS^{-1}$$

which implies that $H' = HS$ is an involution, for $H'^2 = HSHS = HHS^{-1}S =$ identity. Hence $S = HH'$ is the product of two involutions.

Case 2. S is a cyclic transformation of the linear space N and its minimum polynomial is of the form $(x - \epsilon)^{2m+1}$, $\epsilon = \pm 1$. Then if $v, vS, \cdots, vS^{2m}$ is a basis, taking $y = vS^m$ it is represented by $yS^{-m}, \cdots, y, \cdots, S^m$. Thus the two sequences

$$y, y(S + S^{-1}), \cdots, y(S^m + S^{-m})$$

and

$$y(S - S^{-1}), \cdots, y(S^m - S^{-m})$$

together form a basis of N. We denote again by P and Q the subspaces spanned

by the first and second sequences, respectively. As in the previous case we get that

$$P(S + S^{-1}) \subset P$$

for clearly $y(S^i + S^{-i})(S + S^{-1}) \subset P$ if $i < m$ and for $i = m$,

$$y(S^m + S^{-m})(S + S^{-1}) = y(S^{m+1} + S^{-m-1}) + y(S^{m-1} + S^{-m+1}).$$

But $(S - \epsilon)^{2m+1} = 0$ implies that $(S - \epsilon)^{2m+2} = 0 = (S^2 - 2\epsilon S + 1)^{m+1}$ and multiplying by $S^{-(m+1)}$ we get

$$(S + S^{-1} - 2\epsilon)^{m+1} = 0 = \sum_{i=0}^{m+1} c_i(S^i + S^{-i}), \quad \text{with} \quad c_{m+1} = 1.$$

Hence

$$S^{m+1} + S^{-m-1} = -\sum_{i=0}^{m} c_i(S^i + S^{-i})$$

and $y(S^{m+1} + S^{-m-1}) \in P$.

Similarly $P(S - S^{-1}) \subset Q$ for clearly $y(S^i + S^{-i})(S - S^{-1})$ belongs to Q for $i < m$, and for $i = m$, we obtain $y(S^{m+1} - S^{-m-1}) - y(S^{m-1} - S^{-m+1})$. Now, since $(S - \epsilon)^{2m+1} = 0$, $(S - \epsilon)^{2m}(S^2 - 1) = 0$ which gives

$$(S + S^{-1} - 2\epsilon)^m(S - S^{-1}) = 0 = \sum_{i=1}^{m+1} d_i(S^i - S^{-i}) \quad \text{with} \quad d_{m+1} = 1.$$

Hence

$$S^{m+1} - S^{-m-1} = -\sum_{i=1}^{m} d_i(S^i - S^{-i})$$

and $y(S^{m+1} - S^{-m-1}) \in Q$. Thus $P(S - S^{-1}) = Q$ and since we have established (5) and (6) we can apply the rest of the argument of the previous case to get the conclusion. Now dim P = dim Q + 1 and since $P(S - S^{-1}) = Q$, we know that the elements of order $S - \epsilon$ belong to P.

Remark: The proof of the theorem shows that given an invertible linear transformation S of a vector space M, if there exists a decomposition $M = P \oplus Q$ such that $P(S + S^{-1}) \subset P$ and $P(S - S^{-1}) = Q$, and H is the involution with plus- and minus-spaces P and Q, then $S = HH'$ is the product of two involutions. When S is a cyclic transformation whose minimum polynomial is self-reciprocal, if $u \in M$ generates M we can take P as the space spanned by the vectors of the form $u(S^i + S^{-i})$ and Q as the subspace spanned by the vector $u(S^i - S^{-i})$, $i = 0, 1, \cdots$.

Conversely, if a transformation $S = HH'$ is the product of two involutions, then H and H' commute with $S + S^{-1}$ and anticommutes with $S - S'$, since

$$H(HH' + H'H) = (HH' + H'H)H; \quad H(HH' - H'H) = -(HH' - H'H)H$$

and we can write equivalent equations for H'.

As an application of the ideas developed above we are going to show that *a unitary transformation U of a finite dimensional Hilbert space is the product of two unitarian involutions if and only if its spectrum counting multiplicities, is symmetric with respect to the real axis.* For a proof of this result without the assumption that the space is finite dimenional see [1, Theorem 6.3].

It is clear that the condition is necessary. On the other hand it is well-known that a unitary transformation of a finite dimensional Hilbert space admits an orthonormal basis of characteristic vectors and the characteristic values are complex numbers of norm 1. Our condition says that if $\alpha = a + bi$ is a characteristic value with multiplicity r, then $\bar{\alpha} = a - bi$ is a characteristic value with multiplicity r. The basis vectors corresponding to the characteristic values 1 and -1 span an invariant subspace and the restriction of U to this subspace is an involution; therefore the problem is obvious for this subspace. As to its orthogonal complement, the subspace spanned by the other characteristic vectors, we can decompose it in direct sum of orthogonal planes P_i spanned by pairs of orthonormal vectors u and v satisfying $uU = \alpha u$ and $vU = \bar{\alpha}v$, $|\alpha| = 1$. The minimum polynomial of the restriction U_i of U to such a plane is $(x-\alpha)(x-\bar{\alpha})$ and $u+v$ and $(u+v)(U-U^{-1}) = 2biu - 2biv = 2bi(u-v)$ form a basis for this plane. Moreover the involution H_i defined by $(u + v)H_i = u + v$ and $(u - v)H_i = -(u - v)$ is a unitarian involution, since $(u + v, u - v) = (u, u) - (v, v) = 0$. Consequently H_iU_i is also a unitarian involution H_i', Thus $U = HH'$, where H and H' are the unitarian involutions whose restrictions to each P_i coincide with H_i and H_i' respectively.

3. *From now on* when we say that we have *a bilinear form on M* without further specification we *will mean a non-degenerate bilinear form* which is *either symmetric or skew-symmetric* and will be represented by (x, y). A linear transformation S of M into itself such that $(xS, yS) = (x, y)$ for all $x, y \in M$ will be called a form preserving transformation. With respect to a basis $u_1, u_2, \cdots, u_m$ of M the bilinear form is represented by a non-singular $m \times m$ matrix $B = (b_{ij})$ with $b_{ij} = (u_i, u_j)$ and a linear transformation which takes u_i into $u_iS = \sum a_{ij}u_j$ is defined by the matrix $A = (a_{ij})$. The transformation is form preserving if and only if $ABA^t = B$, where A^t denotes the transpose of A. This equality implies that A is non-singular and $B^{-1}AB = (A^t)^{-1} = (A^{-1})^t$. Since a matrix is similar to its transpose, we have that a form preserving transformation is similar to its inverse; hence its minimum polynomial is self-reciprocal.

As usual if (x, y) is symmetric we call the form preserving transformations orthogonal transformations. *When the form is skew-symmetric* we call the form preserving transformations sympletic and *we will say that a linear transformation S is skew-sympletic if $(xS, yS) = -(x, y)$.*

A subspace N of M is non-degenerate if the restriction of the bilinear form to N is non-degenerate.

Given a linear transformation S of M, we denote by $K(g(S))$ the kernel

or null space of the transformation $g(S)$ and by $Mg(S)$ its image or rank space.

Two subspaces M_1 and M_2 are mutually orthogonal if $(v_1, v_2) = 0$ for any $v_i \in M_i$ and we denote by $M_1^\perp = \{u \in M \mid (u, v_1) = 0 \text{ for all } v_1 \in M_1\}$, the subspace orthogonal to M_1. When M_1 is non-degenerate, we have $M = M_1 \oplus M_1^\perp$ and the subspace $M_1^\perp$ is called the orthogonal complement of M_1.

When S is a form preserving transformation we have $(uS^{-1}, v) = (u, vS)$. More generally, if $g(x) = \sum_i a_i x^i$,

$$(u, vg(S)) = \sum a_i(u, vS^i) = \sum a_i(uS^{-i}, v) = (ug(S^{-1}), v).$$

Proposition. *Let M be a finite dimensional vector space with a bilinear form and S a form preserving transformation. If $r(x)$ is a polynomial satisfying $r(0) \neq 0$, the subspaces $Mr(S)$ and $K(\tilde{r}(S))$ are mutually orthogonal.*

Proof. Let $u \in Mr(S)$ and $v \in K(\tilde{r}(S))$, then $u = yr(S)$. Thus, if $n = \deg r(x)$,

$$(v, u) = (v, yr(S)) = (vr(S^{-1}), y) = (vr(S^{-1})S^n, yS^n) = r(0)(v\tilde{r}(S), yS^n)$$
$$= r(0)(0, yS^n) = 0.$$

Corollary. *Let M be a finite dimensional vector space with a bilinear form, S a form preserving transformation and $p(x)$ its minimum polynomial. Let $p(x) = \prod_i r(x)^{h_i}$ be the decomposition of $p(x)$ into irreducible self-reciprocal factors. Then $M = \sum \oplus K(r_i(S)^{h_i})$ is a direct decomposition of M into non-degenerate mutually orthogonal invariant subspaces.*

Proof. It is well-known that $M = \sum \oplus K(r_i(S)^{h_i})$. Since

$$Mr_j(S)^{h_j} = \sum_{i \neq j} K(r_i(S)^{h_i})$$

and $r_i(x) = \tilde{r}_i(x)$, the proposition implies that the subspaces $K(r_i(S)^{h_i})$ are mutually orthogonal. It follows from this fact that each $K(r_i(S)^{h_i})$ is non-degenerate.

Theorem 2. *Let M be a finite dimensional vector space with a non-degenerate bilinear form and let S be a form preserving transformation. Then*

(a) *if the bilinear form is symmetric, S is the product of two orthogonal involutions.*

(b) *if the bilinear form is skew symmetric, S is the product of two skew-sympletic involutions.*

Taking the decomposition of M given in the corollary we can write $S = \sum \oplus S_i$ where each S_i is a form preserving linear transformation with minimum polynomial $r_i(x)^{h_i}$. Hence, in order to establish the theorem, it is enough to show that it is true for each S_i, that is, we have to prove it in the following cases.

Case I. S is a form preserving transformation whose minimum polynomial $r(x)^h = (g(x)\tilde{g}(x))^h$ is a power of the product $g(x)\tilde{g}(x)$ of two distinct irreducible polynomials.

Case II. S is a form preserving transformation whose minimum polynomial is the power of an irreducible polynomial $r(x)$, which consequently must be self-reciprocal.

The next two lemmas will take care of Case I.

Lemma 1. *Let M be a finite dimensional vector space with a bilinear form and S a form preserving transformation whose minimum polynomial is the h-th power of the product of two distinct irreducible polynomials $g(x)$ and $\tilde{g}(x)$. Then M can be decomposed into a direct sum of cyclic subspaces which are mutually orthogonal.*

Proof. We have $M = K(g(S)^h) \oplus K(\tilde{g}(S)^h)$ and by the proposition

$$K(g(S)^h)^\perp \supset M\tilde{g}(S)^h = K(g(S)^h),$$

that is, each subspace is totally isotropic. Now, if u is an element of order $g(S)^h$, then $ug(S)^{h-1} \neq 0$ and there exists an element $v \in K(\tilde{g}(S)^h)$ such that $(ug(S)^{h-1}, v) \neq 0$. That is,

$$0 \neq (u, vg(S^{-1})^{h-1}) = g(0)^{h-1}(uS^{(h-1)\deg g(x)}, v\tilde{g}(S)^{h-1}), \tag{11}$$

which implies that v has order $\tilde{g}(x)^h$. Therefore $u + v$ has order $(g(x)\tilde{g}(x))^h$.

We are going to show that the restriction of the bilinear form to the cyclic subspace N generated by $u + v$ is non-degenerate. For any element $0 \neq w \in N$ is of the form $w = ug(S)^t q(S)S^m + v\tilde{g}(S)^{t'}q'(S)S^{m'}$, where $q(x)$ and $q'(x)$ are polynomials relatively prime to $g(x)$ and $\tilde{g}(x)$, respectively, and $q(0) \neq 0$, $q'(0) \neq 0$; since $w \neq 0$, one of the terms, say, $ug(S)^t q(S)S^m \neq 0$.

Now we can find polynomials $a(x)$ and $b(x)$ such that

$$a(x)\tilde{q}(x) + b(x)\tilde{g}(x)^h = 1,$$

since $\tilde{q}(x)$ is relatively prime to $\tilde{g}(x)$. This means that $va(S)\tilde{q}(S) = v$.

Let $z = v\tilde{g}(S)^{h-t-1}a(S)S^r$, then

$$\begin{aligned}(w, z) &= (ug(S)^t q(S)S^m, v\tilde{g}(S)^{h-t-1}a(S)S^r)\\ &= (u, v\tilde{g}(S)^{h-t-1}g(S^{-1})^t a(S)q(S^{-1})S^{r-m})\\ &= q(0)\tilde{g}(0)^t(uS^{(h-1)\deg g(x)}, v\tilde{g}(S)^{h-1}) \neq 0 \quad \text{by (11)}\end{aligned}$$

if $r = m + (r - h + 1)\deg g(x) + \deg q(S)$.

Similarly, if $w = v\tilde{g}(S)^{t'}q'(S)S^{m'}$ we can find $a(x)$ and an integer f such that $z = ug(S)^{h-t'-1}a(S)S^f$ gives $(w, z) \neq 0$.

Once that we have found a non-degenerate cyclic subspace N we have $M = N \oplus N^\perp$. If $N^\perp$ is cyclic we are through, but, in any case the restriction of S to $N^\perp$ satisfies again the condition of the lemma and we can apply the same process to $N^\perp$, to decompose it in the sum of a non-degenerate cyclic subspace and its orthogonal complement. Continuing this process we arrive at a decomposition of M in direct sum of mutually orthogonal cyclic subspaces.

Lemma 2. *Let M be a finite dimensional vector space with a bilinear form and S a cyclic and form preserving transformation. Then*

(i) *if the bilinear form is symmetric S is the product of two orthogonal involutions.*

(ii) *if the bilinear form is skew-symmetric S is the product of two skew-sympletic involutions.*

Proof. In the proof of theorem 1 to decompose the cyclic transformation S in the product of two involutions H_1 and H_2, we choose a vector u which generates the space and then we take H_1 as the involution whose plus-space P is the subspace spanned by the vectors $u(S^i + S^{-i})$ and whose minus-space Q is the subspace spanned by the vectors $u(S^i - S^{-i})$. When the bilinear form is symmetric, since

$$\begin{aligned}(u(S^i + S^{-i}), u(S^j - S^{-j})) &= (u(S^i + S^{-i}), uS^j) - (u(S^i + S^{-i})S^j, u) \\ &= (u(S^i + S^{-i}), uS^j) - (uS^j, u(S^i + S^{-i}) = 0\end{aligned}$$

the subspaces P and Q are mutually orthogonal, hence H_1 is an orthogonal involution and the involution $H_2 = H_1S$ is also an orthogonal involution because it is the product of two orthogonal transformations.

When the bilinear form is skew-symmetric, we have

$$\begin{aligned}(u(S^i + S^i), u(S^j + S^{-j})) &= (u(S^i + S^{-i}), uS^j) + (u(S^i + S^{-i})S^j, u) \\ &= (u(S^i + S^{-i}), uS^j) + (uS^j, u(S^{-i} + S^i)) = 0.\end{aligned}$$

Hence if $v, w \in P$, $(v, w) = 0$. Similarly

$$\begin{aligned}(u(S^i - S^{-i}), u(S^j - S^{-j})) &= (u(S^i - S^{-i}), uS^j) \\ -(u(S^i - S^{-i})S^j, u) &= (u(S^i - S^{-i}), uS^j) - (uS^j, u(S^{-i} - S^i)) = 0,\end{aligned}$$

so that if $v', w' \in Q$, then $(v', w') = 0$. Hence if $z = v + v'$ and $y = w + w'$,

$$(z, y) = (v, w') + (v', w)$$

while

$$(zH_1, yH_1) = (v - v', w - w') = -(v, w') - (v', w) = -(z, y),$$

which shows that H_1 is a skew-sympletic involution. Therefore $H_2 = H_1S$ is also skew-sympletic and the proof is complete.

To deal with case II we are going to establish first a couple of lemmas.

Lemma 3. *Let M be a finite dimensional vector space with a bilinear form and let S be a form preserving transformation whose minimum polynomial $p(x)^n$ is the power of an irreducible polynomial. Let $u \in M$ be a vector of order $p(x)^n$, then the subspace U generated by u is non-degenerate if and only if there exists a vector $v \in U$ such that $(up(S)^{n-1}, v) \neq 0$. This inequality implies that v has order $p(x)^n$.*

Proof. Notice that $p(x)$ must be self-reciprocal. Since the "only if" part is obvious we only need establish the sufficiency of the condition. Thus we will show that, if the condition holds, for any vector $0 \neq w \in U$, there exists a $z \in U$ such that $(w, z) \neq 0$.

Since $v \in U$, $v = uh(S)$ and any $0 \neq w \in U$ can be expressed as

$$w = up(S)^k g(S) S^r$$

with $k < n$, $g(S)$ relatively prime to $p(S)$ and $g(0) \neq 0$. Then we take $z = up(S)^{n-k-1} h(S) a(S) S^f$, where $f = \deg g(S) - (n - k - 1) \deg p(x) + r$ and $a(x)\tilde{g}(x) + b(x)p(x)^n = 1$. Hence

$$(w, z) = (up(S)^k g(S) S^r, up(S)^{n-k-1} h(S) a(S) S^f)$$

$$p(0)^{n-k-1} g(0) (up(S)^{n-1}, uh(S)) = p(0)^{n-k-1} g(0) (up(S)^{n-1}, v) \neq 0.$$

It is clear that v must have order $p(x)^n$.

Lemma 4. *Let M be a finite dimensional vector space with a bilinear form and let S be a form preserving transformation whose minimum polynomial is the n-th power of an irreducible polynomial. Then either*

(i) *there exists a vector u of order $p(x)^n$ which generates a non-degenerate subspace U, or*

(ii) *there exists two vectors u and v of order $p(S)^n$ which generate the subspaces U and V, respectively, whose intersection $U \cap V = 0$ and whose sum $U \oplus V$ is non-degenerate.*

Proof. Let U be the subspace generated by a vector u of order $p(x)^n$. If U is non-degenerate there is nothing to prove. So let us assume that U is degenerate, then if v is a vector such that $(up(S)^{n-1}, v) \neq 0$, we know by lemma 3 that $v \notin U$, and clearly v has order $p(x^n)$. Let V be the subspace generated by v. Let us assume that $0 \neq y \in U \cap V$; then $y = up(S)^t g(S) = vp(S)^{t'} g'(S)$ where $g(x)$ and $g'(x)$ are both relatively prime to $p(x)$, which implies that the order of y is $n - t = n - t'$, that is, $t = t'$. Now, if $a(x)g(x) + b(x)p(x)^n = 1$, we have

$$ya(S)p(S)^{n-t-1} = up(S)^{n-1} = vp(S)^{n-1} g'(S) a(S),$$

and since $(up(S)^{n-1}, v) \neq 0$ we have

$$(vp(S)^{n-1} g'(S) a(S), v) \neq 0.$$

Hence, by lemma 3, V is non-degenerate, so that (i) holds. So to conclude the proof of the lemma we have to show that if $U \cap V = 0$, then $U + V$ is non-degenerate, that is, that for any vector $0 \neq w \in U + V$, there exists a $z \in U + V$ such that $(w, z) \neq 0$.

Let

$$w = up(S)^t g(S) S^m + vp(S)^{t'} g'(S) S^{m'}$$

with the usual assumptions on $g(x)$ and $g'(x)$, if $t' < t$ taking

$$z = up(S)^{n-t'-1}a(S)S^{t}$$

we get

$$(z, vp(S)^{t'}g'(S)S^{m'}) \neq 0$$

for $a(x)$ and f conveniently chosen. On the other hand

$$(z, up(S)^{t}g(S)S^{m}) = (up(S)^{n-1+t-t'}, uh(S)) = 0$$

because $up(S)^{n-1+t-t'} = 0$ if $t > t'$, and by lemma 3 if $t = t'$. Hence

$$(z, w) = (z, vp(S)^{t'}g'(S)S^{m'}) \neq 0.$$

The case $t' > t$ is handled in similar manner taking

$$z = vp(S)^{n-t-1}a'(S)S^{t'}.$$

So the lemma is established.

Once we have a non-degenerate subspace M_1 we decompose $M = M_1 \oplus M_1^{\perp}$ and the restriction of S to M_1 satisfies again the condition of the lemma so that by repeated applications of this lemma we have that in case II we can decompose the space M in a direct sum $\sum \oplus M_i$ of mutually orthogonal subspaces. Each one of the M_i is either cyclic or is a direct sum of two degenerate cyclic subspaces of the same order. Now lemma 2 takes care of the decomposition of the restriction of S to the cyclic subspace into a product of two orthogonal or skew-sympletic involutions. Hence to complete the proof of the theorem we have to show that such decomposition is also possible for the other kind of spaces. This will be our last lemma.

Lemma 5. *Let M be a vector space with a bilinear form and S a form preserving transformation such that $M = U \oplus V$ is the direct sum of two cyclic subspaces of order $p(x)^n$. Then*

(i) *if the form is symmetric, S is the product of two orthogonal involutions.*

(ii) *if the form is skew-symmetric, S is the product of two skew-sympletic involutions.*

Proof. If there exists in M a vector of order $p(x)^n$ which generates a non-degenerate subspace N then $M = N \oplus N^{\perp}$ is the direct sum of two cyclic subspaces and the assertion of the lemma follows from lemma 2. Thus we can assume that for any vector $u_1 \in M$ of order $p(x)^n$ the cyclic space U_1 generated by u_1 is degenerate. Then we have seen in the proof of the previous lemma that, if u_2 is a vector satisfying $(u_1p(S)^{n-1}, u_2) \neq 0$, $M = U_1 \oplus U_2$ where U_2 is the cyclic subspace generated by u_2.

Let us decompose $U_1 = P_1 \oplus Q_1$, where P_1 is the subspace spanned by the vectors of the form $u_1(S^k + S^{-k})$ and Q_1 is spanned by the vectors of the form $u_1(S^k - S^{-k})$. Now if $\deg p(x) = 2m$, we take the vector $w = u_1p(S)^{n-1}S^{-m(n-1)} \in P_1$, and, if $\deg p(x) \neq 2m$, $p(x) = x \pm 1$, we take $w = u_1(S \pm 1)^{n-1} \in P_1$, since

it has order $x \pm 1$. Therefore in any case $w \notin Q_1$ and we can find a vector u_2 in $Q_1^\perp$ satisfying $(w, u_2) \neq 0$. This implies that u_2 has order $p(x)^n$, and $M = U_1 \oplus U_2$. Let $U_2 = P_2 \oplus Q_2$ where P_2 and Q_2 have the obvious meaning.

When S is an orthogonal transformation we have $P_i^\perp \supset Q_1 + Q_2$, $i = 1, 2$. For

$$(12) \qquad (u_1(S^k + S^{-k}), u_2(S^h - S^{-h})) = -(u_1(S^k + S^{-k})(S^h - S^{-h}), u_2) = 0,$$

since $u_1(S^k + S^{-k})(S^h - S^{-h}) \in Q_1$ and $u_2 \in Q_1^\perp$; similarly

$$(13) \qquad (u_2(S^k + S^{-k}), u_1(S^h - S^{-h})) = 0.$$

Hence if H is the involution with plus-space $P = P_1 \oplus P_2$ and minus space $Q = Q_1 \oplus Q_2$, H is an orthogonal transformation and $S = HH'$ where H' is another involution.

When S is a sympletic transformation, (12) and (13) imply that P_i and Q_i, $i \neq j$, are mutually orthogonal in this case also. Since now $P_i^\perp \supset P_i$, the involution H with plus-space $P = P_1 \oplus Q_2$ and minus space $Q = P_2 \oplus Q_1$ is skew-sympletic and $S = HH'$ where H' is again an involution.

The proof of the theorem is complete.

***Remark* I.** Lemma 5 is not superfluous, that is, M can not always be decomposed in direct sum of mutually orthogonal cyclic subspaces. Following the methods used in the proofs of the preceding lemmas it is easy to show that such decomposition is impossible only in the following cases:

(a) the bilinear form is symmetric and $(x \pm 1)^{2m}$ is an elementary divisor of S,

(b) the bilinear form is skew-symmetric and $(x \pm 1)^{2m+1}$ is an elementary divisor of S.

Hence such elementary divisors appear always an even number of times.

***Remark* II.** In the case of a symmetric bilinear form, if we could be sure that the subspaces involved in the proof are non-degenerate, the proof of Theorem 2 becomes considerably simpler. This is the situation if the form has Witt index 0, but for this case the reader can find a more elementary proof in [4].

In the case of a skew-symmetric bilinear form our arguments indicate that it is not possible to decompose any sympletic transformation into the product of two sympletic involutions. This is also seen more clearly in the case of a two dimensional space since the only sympletic involutions are plus and minus the identity.

References

[1] Davis, C., Separation of two linear subspaces, *Acta Scientiarum Mathematicarum*, **XIX** (1958) 172–187.

[2] Jacobson, N., *Lectures in Abstract Algebra, Vol. II*, New York, 1953.

[3] Malcev, A. I., *Foundations of Linear Algebra*, San Francisco, 1963.

[4] Wonenburger, M. J., A decomposition of orthogonal transformations, *Canadian Mathematical Bulletin*, **7** (1964) 379–383.

University of Toronto

Date Communicated: March 9, 1966