The Product of Two Involutions in the Unitary Group of a Hermitian Form

D. Ž. DJOKOVIĆ

Communicated by P. R. HALMOS

In this paper we denote by V a finite dimensional vector space over a field K . By J we denote an automorphism of K such that $J^2 = 1$. In particular, one can take $J = 1$. By $\Phi: V \times V \rightarrow K$ we denote a non-degenerate hermitian form. Thus we have

$$\Phi(\lambda x, \mu y) = \lambda \mu^J \Phi(x, y), \quad \Phi(x, y) = \Phi(y, x)^J$$

for all $\lambda, \mu \in K$ and $x, y \in V$. If $J = 1$, then Φ is in fact a non-degenerate symmetric bilinear form.

We denote by $U(\Phi)$ the unitary group of the form Φ . If A is a linear transformation of V , then A^* will denote the adjoint of A with respect to Φ . Hence we have $\Phi(xA, y) = \Phi(x, yA^*)$ for all $x, y \in V$. A linear transformation A of V is an *involution* if A^2 is the identity transformation I .

Let X be an indeterminate over K . If

$$f(X) = \sum_{i=0}^m \alpha_i X^i \in K[X],$$

we define

$$f^J(X) = \sum_{i=0}^m \alpha_i^J X^i.$$

If, in addition $\alpha_0 \neq 0$ and $\alpha_m = 1$, then we put

$$\tilde{f}(X) = \alpha_0^{-1} X^m f(X^{-1}).$$

The object of this paper is to prove the following.

Theorem 1. *Let $A \in U(\Phi)$ and assume that either*

- (i) $J = 1$, or
- (ii) $J \neq 1$, A is similar to A^* and $f \neq \tilde{f}^J$ for every monic irreducible factor of the minimal polynomial of A .

Then A is a product of two unitary involutions.

The proof will be given in a sequence of lemmas. In the case $J = 1$ the assertion of the theorem was proved by M. J. Wonenburger [4] under the restriction $\text{char } K \neq 2$. When $J = 1$, then $A \in U(\Phi)$ implies that A and A^* are similar [4].

The involutions $\sim$ and J act on monic polynomials $f \in K[X]$ such that $f(0) \neq 0$. There exist five possibilities:

- (1) $f, \tilde{f}, f^J, \tilde{f}^J$ are distinct,
- (2) $f = \tilde{f} \neq f^J = \tilde{f}^J$,
- (3) $f = f^J \neq \tilde{f} = \tilde{f}^J$,
- (4) $f = \tilde{f}^J \neq \tilde{f} = f^J$,
- (5) $f = \tilde{f} = f^J = \tilde{f}^J$.

Note that $\sim$ and J commute. An A -invariant subspace $W \subset V$ is *cyclic* if there exists $x \in W$ such that W is spanned by $x, xA, xA^2, \dots$. Then we write $W = \langle x \rangle$. The *order* of an A -invariant subspace is the minimum polynomial of the restriction of A to this subspace. If f is the order of V , then (5) holds because $A \in U(\Phi)$ and A^{-1} is similar to A .

We shall distinguish six special types of *non-degenerate* A -invariant subspaces $W \neq 0$.

Type 1. $W = W_1 \oplus W_2 \oplus W_3 \oplus W_4$ where the summands are cyclic, totally isotropic and $(W_1 \oplus W_2) \perp (W_3 \oplus W_4)$. The orders of the summands are

$$f^m, (\tilde{f}^J)^m, \tilde{f}^m, (f^J)^m \quad (m \geq 1),$$

respectively, where f is a monic irreducible polynomial such that (1) holds.

Type 2. $W = W_1 \oplus W_2$ where the summands are cyclic and totally isotropic. The orders of the summands are f^m and $(\tilde{f}^J)^m$, respectively, where f is a monic irreducible polynomial such that (2) holds.

Type 3. The same as type 2 except that (3) holds instead of (2).

Type 4. $W = W_1 \oplus W_2$ where the summands are cyclic, non-degenerate and $W_1 \perp W_2$. The orders of the summands are f^m and $\tilde{f}^m$, respectively, where f is a monic irreducible polynomial such that (4) holds.

Type 5. W is cyclic of order f^m where f is a monic irreducible polynomial such that (5) holds.

Type 6. $J = 1$, $W = W_1 \oplus W_2$ where the summands are cyclic and degenerate. The summands W_1 and W_2 have the same order $(X + \epsilon)^m$, $\epsilon = \pm 1$, and if $\text{char } K \neq 2$, then m is even.

Lemma 1. *If the order of V has a monic irreducible factor f such that (1) (resp. (2), (3)) holds, then V has a subspace of type 1 (resp. type 2, type 3).*

Proof. Let the order of V be $f^m g$ where $f \nmid g$. Let $W_1 = \langle a_1 \rangle$ be a cyclic

subspace of order f^m , and let

$$b_1 = a_1 \tilde{f}(A^{-1})^{m-1}, \quad b'_1 = b_1 \tilde{g}(A^{-1}).$$

Since $b'_1 \neq 0$, we can choose $a'_2 \in V$ such that $\Phi(b'_1, a'_2) \neq 0$. If

$$a_2 = a'_2 \tilde{g}^J(A),$$

then

$$\Phi(a_1, a_2 \tilde{f}^J(A)^{m-1}) \neq 0, \quad \Phi(b_1, a_2) \neq 0,$$

which implies that $W_2 = \langle a_2 \rangle$ has the order $(\tilde{f}^J)^m$. Hence $W_1 \cap W_2 = 0$. From $W_1 \subset \text{Ker } f^m(A)$, we derive that

$$W_1^\perp \supset (\text{Ker } f^m(A))^\perp = \text{Im } (f^m(A))^* = \text{Im } (f^J(A^{-1}))^m = \text{Im } (\tilde{f}^J(A))^m \supset W_1,$$

i.e., W_1 is totally isotropic. Similarly, W_2 is totally isotropic. Let $W_0 = W_1 \oplus W_2$ and assume that $\text{Rad } (W_0) \neq 0$. Then $\text{Rad } (W_0)$ meets non-trivially W_1 or W_2 . If, say, $W_1 \cap \text{Rad } (W_0) \neq 0$ then $\langle b_1 \rangle \subset \text{Rad } (W_0)$ which contradicts the fact that $\Phi(b_1, a_2) \neq 0$. This proves that W_0 is non-degenerate.

If (2) (resp. (3)) holds, then $W = W_0$ is of type 2 (resp. type 3). In the remaining part of the proof we assume that (1) holds.

Note that the order of $W_0^\perp$ has factorization $\tilde{f}^m h$ where $\tilde{f} \nmid h$. Now, we can choose W_3 and W_4 in $W_0^\perp$ in the same way as we chose W_1 and W_2 so that $W = W_1 \oplus W_2 \oplus W_3 \oplus W_4$ is of type 1.

Lemma 2. *If the order of V has a monic irreducible factor f such that (4) or (5) holds, then V has a subspace of type 4, 5 or 6.*

Proof. Let $f^m g$, $f \nmid g$, be the order of V .

We shall first consider the case in which every cyclic subspace of V of order f^m is degenerate. Let W_1, W_2, a_1, a_2, b_1 be as in the proof of Lemma 1. Note that because $\tilde{f}^J = f$ the subspace W_2 also has order f^m . Since W_2 is degenerate and $\Phi(b_1, a_2) \neq 0$, we have $W_1 \cap W_2 = 0$.

Let $W_0 = W_1 \oplus W_2$ and assume that $\text{Rad } (W_0) \neq 0$. There exists $x \neq 0$, $x \in \text{Rad } (W_0)$ which has order f . Let $x = x_1 + x_2$, $x_1 \in W_1$, $x_2 \in W_2$. Then x_1 and x_2 are in $\text{Rad } (W_0)$. If, say, $x_1 \neq 0$, then also $b_1 \in \text{Rad } (W_0)$; this leads to a contradiction because $\Phi(b_1, a_2) \neq 0$. This proves that W_0 is non-degenerate.

If s is an integer and $x \in W_0$, then

$$\Phi(x, xA^s f(A)^{m-1}) = 0$$

since otherwise $\langle x \rangle$ would be a non-degenerate subspace of order f^m . If $x = x_1 + x_2$, $x_1 \in W_1$, $x_2 \in W_2$, then, by using the fact that W_1 and W_2 are degenerate, we obtain

$$\Phi(x_1, x_2 A^s f(A)^{m-1}) + \Phi(x_2, x_1 A^s f(A)^{m-1}) = 0$$

and

$$(6) \quad \Phi(y_1, x_2 f(A)^{m-1}) + \Phi(x_2, y_1 A^{2s} f(A)^{m-1}) = 0,$$

where $y_1 = x_1 A^{-s}$ is an arbitrary element of W_1 and x_2 an arbitrary element of W_2 . By putting $s = 1$ and $s = 0$ and subtracting, we get

$$\Phi(x_2, y_1(A^2 - I)f(A)^{m-1}) = 0.$$

Since $W_1 \cap W_2^\perp = 0$, we must have

$$y_1(A^2 - I)f(A)^{m-1} = 0.$$

We can choose $y_1 \in W_1$ so that $z_1 = y_1 f(A)^{m-1} \neq 0$. From $z_1(A^2 - I) = 0$ we can conclude that 1 or -1 is a root of f , and consequently $f(X) = X + \epsilon$, $\epsilon = \pm 1$.

We can rewrite (6) as follows:

$$\begin{aligned} \Phi(y_1 \epsilon^{m-1} A^{-m+1}(A + \epsilon)^{m-1}, x_2) + \Phi(x_2, y_1 A^{2s}(A + \epsilon)^{m-1}) &= 0, \\ \epsilon^{m-1} \Phi(z_1 A^{-m+1}, x_2) + \Phi(x_2, z_1 A^{2s}) &= 0. \end{aligned}$$

Since $z_1 A = -\epsilon z_1$ we get

$$(-1)^{m-1} \Phi(z_1, x_2) + \Phi(x_2, z_1) = 0$$

for all $x_2 \in W_2$. For m even, this equality implies that $J = 1$. If m is odd, we replace x_2 by λx_2 where $\lambda \in K$ to conclude that again $J = 1$, but in addition we get $2\Phi(x_2, z_1) = 0$, i.e., $\text{char } K = 2$.

Hence, we have proved that in this case $W = W_0$ is a subspace of type 6. Note that $f(x) = X + \epsilon$, $\epsilon = \pm 1$, implies that (5) holds.

Now, we take up the case when V has a cyclic subspace, say W_1 , of order f^m , which is non-degenerate.

If (4) holds, then V must also have a non-degenerate cyclic subspace W_2 of order $\tilde{f}^m$. From $W_1 \subset \text{Ker } f(A)^m$ we deduce that $W_1^\perp \supset W_2$. This proves that $W = W_1 \oplus W_2$ is a subspace of type 4. If (5) holds, there is nothing to prove.

By using induction one easily proves that Lemmas 1 and 2 have as a consequence the following.

Lemma 3. *There exists an orthogonal splitting $V = V_1 \oplus \cdots \oplus V_s$ such that every summand is of one of the types 1–6.*

Note that we have not used the hypothesis $f \neq \tilde{f}'$ made in the statement of Theorem 1.

Lemma 4. *If V is of type 1, then A is a product of two unitary involutions.*

Proof. Since W_1 and W_3 are cyclic of orders f^m and $\tilde{f}^m$, respectively, there exists a vector space isomorphism $S: W_1 \rightarrow W_3$ such that

$$xSA^{-1} = xAS \quad \text{for all } x \in W_1.$$

We can identify W_2 and W_4 with the duals of W_1 and W_3 , respectively. Therefore there exists a unique vector space isomorphism $S^*: W_4 \rightarrow W_2$ such that

$$\Phi(xS, u) = \Phi(x, uS^*) \quad \text{for all } x \in W_1, u \in W_4.$$

There exists a unique $C \in GL(V)$ such that $C^2 = I$ and

$$xS = xC, \quad uS^* = uC,$$

for all $x \in W_1, u \in W_4$.

If $x \in W_1, y \in W_2, z \in W_3, u \in W_4$, then

$$\Phi(xC, yC) = \Phi(xS, yC) = \Phi(x, yCS^*) = \Phi(x, y),$$

and

$$\Phi(zC, uC) = \Phi(zC, uS^*) = \Phi(zCS, u) = \Phi(z, u).$$

Hence, C is unitary. Then also $B = CA^{-1}$ is unitary. Moreover, from

$$xB^2 = xCA^{-1}B = xSA^{-1}B = xASB = xACB = x,$$

$$zB^2 = zBCA^{-1} = zBSA^{-1} = zBAS = zBAC = z,$$

$$\Phi(x, yB^2) = \Phi(xB^{-2}, y) = \Phi(x, y),$$

$$\Phi(z, uB^2) = \Phi(zB^{-2}, u) = \Phi(z, u),$$

we deduce that $B^2 = I$.

Lemma 5. *If V is of type 2, then A is a product of two unitary involutions.*

Proof. Let $A = A_1 \oplus A_2$ correspond to $V = W_1 \oplus W_2$. Since W_1 is cyclic and $f = \bar{f}$, we have ([2], Lemma 1; [1]) $A_1 = ST$ where $S^2 = T^2 = I$ and $S, T \in GL(W_1)$. There exist unique $S^*, T^* \in GL(W_2)$ such that

$$\Phi(xS, y) = \Phi(x, yS^*), \quad \Phi(xT, y) = \Phi(x, yT^*)$$

for all $x \in W_1, y \in W_2$. It is evident that also $S^{*2} = T^{*2} = I$.

From

$$\Phi(x, yA) = \Phi(xA^{-1}, y) = \Phi(xTS, y) = \Phi(x, yS^*T^*),$$

we get $A_2 = S^*T^*$. Hence, we have $A = BC$ with

$$B^2 = C^2 = I, \quad B = S \oplus S^*, \quad C = T \oplus T^*.$$

Since W_1 and W_2 are totally isotropic and

$$\Phi(xB, yB) = \Phi(xS, yS^*) = \Phi(xS^2, y) = \Phi(x, y)$$

for all $x \in W_1, y \in W_2$, we infer that B is unitary.

Lemma 6. *If V is of type 3, then A is a product of two unitary involutions.*

Proof. Let $A = A_1 \oplus A_2$ correspond to $V = W_1 \oplus W_2$. It was proved in [3] that in this situation there exists a vector space isomorphism $H: W_1 \rightarrow W_2$ such that

$$A_2^{-1} = H^{-1}A_1H \quad \text{and} \quad H^* = H$$

where $H^*: W_1 \rightarrow W_2$ is defined by the condition

$$\Phi(xH, y) = \Phi(x, yH^*)$$

for all $x, y \in W_1$. We define $C \in GL(V)$ by the conditions $C^2 = I$ and

$$xC = xH \quad \text{for all } x \in W_1.$$

Then

$$\Phi(xC, zC) = \Phi(xH, zC) = \Phi(x, zCH^*) = \Phi(x, zCH) = \Phi(x, z)$$

for all $x \in W_1$ and $z \in W_2$. This implies that C is unitary.

Then $B = CA^{-1}$ is also unitary, and we have

$$xB^2 = xCA^{-1}B = xHA^{-1}B = xAHB = xACB = x,$$

$$zB^2 = zBCA^{-1} = zBHA^{-1} = zBAH = zBAC = z,$$

for all $x \in W_1$ and $z \in W_2$. Hence $B^2 = I$.

Lemma 7. *If $J = 1$ and V is of type 5, then A is a product of two unitary involutions.*

Proof. Since V is cyclic, there exist ([2], Lemma 1) $S, T \in GL(V)$ such that

$$A = ST \quad \text{and} \quad S^2 = T^2 = I.$$

We claim that S and T must be unitary. Let $x, y \in V$ be arbitrary and, for instance, $y \in \langle x \rangle$. Then $y = xg(A)$ for some $g \in K[X]$. We have

$$\begin{aligned} \Phi(xS, y) &= \Phi(xS, xg(A)) = \Phi(xSg(A^{-1}), x) \\ &= \Phi(xg(A)S, x) = \Phi(yS, x) = \Phi(x, yS). \end{aligned}$$

Thus $S^* = S = S^{-1}$, and so $S \in U(\Phi)$.

Lemma 8. *If V is of type 6, then A is a product of two unitary involutions.*

Proof. Let $A = A_1 \oplus A_2$ correspond to $V = W_1 \oplus W_2$. Since $f(X) = X + \epsilon$, $\epsilon = \pm 1$ and W_1 is cyclic, there exists ([2], Lemma 1) $S, T \in GL(W_1)$ such that

$$A_1 = ST \quad \text{and} \quad S^2 = T^2 = I.$$

If $x, y \in W_1$, then $x \in \langle y \rangle$ or $y \in \langle x \rangle$. If, for instance $y \in \langle x \rangle$, then this implies that also $yT \in \langle x \rangle T = \langle x \rangle$ because $T^{-1}A_1T = A_1^{-1}$.

Hence there exists $g \in K[X]$ such that $yT = xg(A)$. Since $J = 1$ we have

$$\begin{aligned} \Phi(xT, yT) &= \Phi(xT, xg(A)) = \Phi(xTg(A^{-1}), x) \\ &= \Phi(xg(A)T, x) = \Phi(y, x) = \Phi(x, y), \end{aligned}$$

and similarly $\Phi(xS, yS) = \Phi(x, y)$.

There exist unique $S^*, T^* \in GL(W_2)$ such that

$$\Phi(xS, z) = \Phi(x, xS^*), \quad \Phi(xT, z) = \Phi(x, zT^*)$$

holds for all $x \in W_1$ and $z \in W_2$. Evidently, $S^{*2} = T^{*2} = 1$. Then $A = BC$ where

$$B^2 = C^2 = I \quad \text{and} \quad B = S \oplus S^*, \quad C = T \oplus T^*.$$

From

$$\Phi(x, zA) = \Phi(xA^{-1}, z) = \Phi(xTS, z) = \Phi(x, xS^*T^*)$$

we deduce that $A_2 = S^*T^*$. The same argument as above gives that

$$\Phi(zS^*, uS^*) = \Phi(z, u) \quad \text{for all } z, u \in W_2.$$

We also have

$$\Phi(xB, zB) = \Phi(xS, zS^*) = \Phi(xS^2, z) = \Phi(x, z)$$

for all $x \in W_1$ and $z \in W_2$. Hence B is unitary.

It is clear that Theorem 1 follows from these eight lemmas.

We conclude with two examples which show that the restriction on the irreducible factors of the minimal polynomial of A are indeed necessary in Theorem 1. Note that V in the first example is of type 4 and in second of type 5.

Example 1. Let a, b be a basis of V and let K be the complex field, J the conjugation. Let the hermitian form Φ be defined by the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If $\xi \in K$, $|\xi| = 1$, $\xi \neq \bar{\xi}$, then the transformation A with matrix

$$\begin{pmatrix} \xi & 0 \\ 0 & \bar{\xi} \end{pmatrix}$$

is unitary. Assume that $A = BC$ where B and C are unitary involutions. Then

$$aBA = aC = aC^{-1} = aA^{-1}B = \bar{\xi}aB$$

implies that $aB = \lambda b$ for some $\lambda \in K$. Since B is unitary we must have

$$1 = \Phi(a, a) = \Phi(aB, aB) = \Phi(\lambda b, \lambda b) = -|\lambda|^2$$

which is impossible. Hence A is unitary and similar to A^{-1} , but it is not a product of two unitary involutions.

Example 2. Let V, a, b, K, J be as in Example 1, and define Φ and A by their matrices

$$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then A is unitary and similar to A^{-1} . If $A = BC$ where B and C are unitary involutions, then $BA^{-1} = AB$. If

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

is the matrix of B , then $BA^{-1} = AB$ implies that $\gamma = 0$, $\delta = -\alpha$. Since also $B^2 = I$, we must have $\alpha = \pm 1$. Hence B must be of the form

$$\pm \begin{pmatrix} 1 & \epsilon \\ 0 & -1 \end{pmatrix}.$$

Then $i = \Phi(a, b) = \Phi(aB, bB) = \Phi(a, -b) = -i$ gives a contradiction. Hence A is not a product of two unitary involutions.

I am indebted to W. Nichols for several very useful remarks.

REFERENCES

1. N. Bourbaki, *Éléments de mathématique, Algèbre*, Chap. VII, §5, Ex. 16, Hermann, Paris 1964.
2. D. Ž. DJOKOVIĆ, *Product of two involutions*, Arch. Math. **18** (1967), 582–584.
3. D. Ž. DJOKOVIĆ, *On the similarity between a linear transformation and its adjoint*, Linear Algebra and Appl. (to appear).
4. M. J. WONENBURGER, *Transformations which are products of two involutions*, J. Math. Mech. **16** (1966), 327–338.

This work was supported by the Summer Research Fellowship (1970) of the University of Waterloo.

University of Waterloo
Waterloo, Ontario, Canada
Date communicated: JULY 12, 1971