Products of Involutions

Dedicated to Olga Taussky Todd

W. H. Gustafson, P. R. Halmos*,
Indiana University, Bloomington, Indiana

and

H. Radjavi†
Dalhousie University, Halifax, Nova Scotia

Submitted by Hans Schneider

ABSTRACT

Every square matrix over a field, with determinant \( \pm 1 \), is the product of not more than four involutions.

THEOREM. Every square matrix over a field, with determinant \( \pm 1 \), is the product of not more than four involutions.

DISCUSSION

An involution is a matrix (or, more generally, in any group, an element) whose square is the identity. Halmos and Kakutani proved that in the group of all unitary operators on an infinite-dimensional complex Hilbert space every element is the product of four involutions [3]. Radjavi obtained the same conclusion for the group of all unitary operators with determinant \( \pm 1 \) on any finite-dimensional complex Hilbert space [5]. Sampson proved that every square matrix over the field of real numbers, with determinant \( \pm 1 \), is the product of a finite number of involutions [6], and Waterhouse asserted

*Research supported in part by a grant from the National Science Foundation.
†Research supported in part by a grant from the National Research Council of Canada.
the same conclusion over any division ring [7]. The theorem as stated above is the best possible one along these lines, in the sense that “four” cannot be changed to “three”; this has been known for a long time [3]. Since a product of involutions has determinant $\pm 1$, the condition of the theorem is necessary as well as sufficient.

The proof of the theorem uses two basic involutions and one factoring device. The basic involutions are the matrices of the forms

$$
\begin{pmatrix}
0 & x \\
1/x & 0
\end{pmatrix}
$$

and

$$
\begin{pmatrix}
-1 & 0 & 0 & \cdots & 0 & 0 \\
x_1 & 1 & 0 & \cdots & 0 & 0 \\
x_2 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n-2} & 0 & 0 & \cdots & 1 & 0 \\
x_{n-1} & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}
$$

where $x \neq 0$, and $x_1, \ldots, x_{n-1}$ are arbitrary scalars. The factoring device is to write a cyclic permutation $\sigma (i \mapsto i+1 \mod n)$ in the form

$$
\sigma = \gamma \delta,
$$

where $\gamma$ and $\delta$ are the involutions $i \mapsto 1-i \mod n$ and $i \mapsto -i \mod n$, respectively. This device is the discrete version of the well known geometric fact that a rotation is the product of two reflections.

**Proof.** In view of the theory of the rational canonical form [4, p. 352], it is sufficient to prove the conclusion for matrices of the form

$$
T = P_1 \oplus \cdots \oplus P_k \oplus Q,
$$
where each $P_i$ is a companion matrix of size at least 2,

\[
P_i = \begin{bmatrix}
0 & 0 & 0 & \cdots & 0 & p_i \\
1 & 0 & 0 & \cdots & 0 & * \\
0 & 1 & 0 & \cdots & 0 & * \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & * \\
0 & 0 & 0 & \cdots & 1 & *
\end{bmatrix},
\]

and $Q$ is diagonal,

\[
Q = \begin{bmatrix}
q_1 & 0 & 0 & \cdots & 0 & 0 \\
0 & q_2 & 0 & \cdots & 0 & 0 \\
0 & 0 & q_3 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & q_{m-1} & 0 \\
0 & 0 & 0 & \cdots & 0 & q_m
\end{bmatrix};
\]

it is understood that either the $P_i$'s or $Q$ may be absent.

(1) The first step of the proof is to perform the following sequence of operations: divide the last column of $P_i$ by $-p_i$ and move it to the left of the other columns, so as to place it first; replace the diagonal entries $q_i$ of $Q$ by 1's, and permute neighboring columns so as to convert the result into the direct sum of copies of the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ of size 2, with possibly one 1 left over, to be used as a direct summand of size 1. The direct sum of the altered matrices is an involution $A$.

The matrix $T$ can be recaptured from $A$ by a suitable right multiplication. The factor $R$ that yields

\[
T = AR
\]

is a weighted permutation matrix, in the following sense: each row and each column of $R$ contains exactly one non-zero entry. Among those non-zero entries each $p_i$ and each $q_i$ occurs exactly once (possibly with a minus sign); the other non-zero entries of $R$ are equal to 1. It follows that, except possibly
for sign, the determinant of $R$ is the product of all the $p$’s and all the $q$’s. Since, except possibly for sign, the determinant of $T$ is the same product, it follows that $\det R = \pm 1$.

Permutation matrices (weighted or not) are in a natural correspondence with permutations of the indices: the permutation corresponding to $R$ maps the index $u$ onto the index $v$ in case the non-zero entry of column $u$ is in row $v$. The way the particular weighted permutation matrix $R$ was constructed implies that the corresponding permutation $\rho$ has at most one fixed point.

The last two steps of the proof are as follows: (2) $\rho = \beta \sigma$, where $\beta$ is an involution and $\sigma$ is a cyclic permutation with no fixed points, so that, correspondingly, $R = BS$, where $B$ is a permutation matrix and $S$ is a weighted permutation matrix, such that $B$ is an involution and $\det S = \pm 1$; and (3) $S = CD$, where $C$ and $D$ are weighted permutation matrices that are involutions. (The idea for this step is based on a suggestion of J. E. McLaughlin.) These facts obviously imply that $T (= ABCD)$ is a product of four involutions.

(2) Suppose that $\rho$ is a permutation with at most one fixed point. To simplify the notation, but with no conceptual loss, assume that $\rho$ consists of three non-trivial cycles, and, possibly, one additional cycle of length 1 (a fixed point). If

$$\rho = (w)(x_1, \ldots, x_p)(y_1, \ldots, y_q)(z_1, \ldots, z_r),$$

write

$$\beta = (w, x_1)(x_p, y_1)(y_q, z_1).$$

[If $(w)$ is absent from $\rho$, omit $(w, x_1)$ from $\beta$.] It follows that

$$\beta \rho = (w, x_1, \ldots, x_p, 1, y_1, \ldots, y_q, 1, z_1, \ldots, z_r, 1, y_q, z_1)$$

[or the same thing without $w$, in case there was no $(w)$ in $\rho$]; this completes the proof of (2).

(3) Suppose finally that $S$ is a weighted permutation matrix with determinant $\pm 1$ such that the corresponding permutation $\sigma$ is cyclic and has no fixed points. To be specific, let $\sigma$ be the permutation $i \rightarrow i + 1 \mod n$. It follows that $\sigma = \gamma \delta$, where $\gamma$ and $\delta$ are the involutions $i \rightarrow 1 - i \mod n$ and $i \rightarrow -i \mod n$, respectively.

The weighted permutation matrix $S$ is determined by a suitable basis of vectors $e_0, \ldots, e_{n-1}$ via equations such as

$$Se_i = s_i e_{i+1},$$
where the product of all the $s_i$'s is $\pm 1$. Such a matrix is similar to an "almost unweighted" permutation matrix in which $s_i = 1$ when $i \neq 0$ and $s_0 = \pm 1$. Indeed: replace $e_1$ by $s_0 e_1$, replace $e_2$ by $(s_0 s_1) e_2$, etc., and, finally, replace $e_0$ by $(s_0 \cdots s_{n-1}) e_0 \ (= \pm e_0)$; the matrix of $S$ with respect to the new basis so obtained is almost unweighted. Assume therefore, with no loss, that $S$ is almost unweighted to begin with. Then $S$ is the product of two involutions in almost the same way as $\sigma$: if $Ce_i = e_{i-1}$ for all $i$, and $De_i = e_{i-1}$ when $i \neq 0$ and $De_0 = s_0 e_0$, then $C$ and $D$ are involutions and $CD = S$.

**QUESTIONS**

I

Wonenburger [8] proved that over a field of characteristic different from 2 a square matrix is a product of two involutions if and only if it is invertible and is similar to its inverse; Djoković [2] proved it for arbitrary fields. The corresponding result for unitary matrices is due to Davis [1]: a unitary matrix is the product of two unitary involutions if and only if it is similar (and therefore unitarily equivalent) to its adjoint. By the theorem of this note, a square matrix is a product of four involutions if and only if its determinant is $\pm 1$. There are, therefore, simple algebraic characterizations of involutions, of products of two involutions, and of products of four involutions. Is there a similar intrinsic algebraic characterization of products of three involutions? Is this an interesting question? The answer depends on the answer. (Some special facts are known. For example: if the rational canonical form of a matrix with determinant $\pm 1$ has one block, i.e., if it is cyclic, or two blocks, then it is a product of three involutions; if the number of elements in the field is not 2, 3, or 5, then there exists a matrix with determinant 1 that is not the product of three involutions.)

II

From standard results on the normal subgroups of the general linear group, it follows easily that if $\text{GL} (n, F)$ contains an element of finite order $k$, then every element of $\text{SL} (n, F)$ is the product of finitely many elements of order $k$ (at least if $n > 2$ or $F$ has more than three elements). How many factors are needed when $k > 2$? The same arguments would even show that all the factors could be taken as conjugates of a single (non-scalar) element of order $k$. How many factors are needed in this case?
What are the facts for infinite-dimensional spaces, and, in particular, for Hilbert space? What is known is interesting, different from the finite-dimensional case, and incomplete. For example: every invertible bounded operator on an infinite-dimensional complex Hilbert space is the product of seven involutions; four are not enough. What is the right number?

REFERENCES