A DECOMPOSITION OF ORTHOGONAL TRANSFORMATIONS

María J. Wonenburger

(received December 6, 1963)

The purpose of the present note is to give a partial answer to a question raised by Professor Coxeter, namely, if an orthogonal transformation is expressed as a product of orthogonal involutions, how many involutions do we need? Our answer is partial because we are going to consider only non-degenerate symmetric bilinear forms of index 0 and fields of characteristic $\neq 2$. Under these conditions we prove that any orthogonal transformation is the product of at most two orthogonal involutions, which implies that we can write any orthogonal transformation as the product of two involutions.

In section 1 we recall the relevant definitions. For more detail see [1] or [2].

1. Let M be a left vector space of dimension n over a commutative field k of characteristic $\neq 2$, and (x, y), where $x, y \in M$, a non-degenerate symmetric bilinear form. The linear transformations T of M which satisfy $(xT, yT) = (x, y)$ for all $x, y \in M$ are called orthogonal transformations. They form a group called the orthogonal group of M relative to the bilinear form (x, y). The most simple orthogonal transformations are the ones whose square is the identity I; such transformations are called orthogonal involutions. Now, if T is an orthogonal involution, M can be decomposed in the direct sum of two subspaces, $M = M^+ \oplus M^-$, such that $xT = x$ if $x \in M^+$ and $yT = -y$ if $y \in M^-$. Moreover, since $(x, y) = (xT, yT) = (x, -y) = -(x, y)$, any vector x in M^+ is orthogonal to any vector y in M^-, that is $(x, y) = 0$. This condition together

Canad. Math. Bull. vol. 7, no. 3, July 1964.

with $M = M^+ \oplus M^-$ implies that M^+ and M^- are orthogonal complements of each other, and the restrictions of (x,y) to M^+ and M^- are non-degenerate bilinear forms. Conversely, given a subspace N such that the restriction of the bilinear form to N is non-degenerate, let $N^\perp$ be its orthogonal complement, that is, $N^\perp = \{y \mid (x,y) = 0 \text{ for all } x \in N\}$; then $M = N \oplus N^\perp$, and the transformation T which leaves invariant any vector of N and $yT = -y$ for all $y \in N^\perp$ is an orthogonal involution with $M^+ = N$ and $M^- = N^\perp$. T can be simply described as the reflection in the subspace M^+. In particular, if $(x,x) \neq 0$ and H is the hyperplane orthogonal to the subspace $[x]$ generated by x, the reflection in H is called the symmetry relative to H.

Let $x_1, x_2, \ldots, x_r$ be non-isotropic orthogonal vectors, that is, $(x_i, x_i) \neq 0$, $i = 1, 2, \ldots, r$ and $(x_i, x_j) = 0$ for $i \neq j$; then the product of the symmetries, $S_1 S_2 \ldots S_r$, where S_i is the reflection in the hyperplane H_i orthogonal to $[x_i]$, is the involution T with $M^+ = H_1 \cap H_2 \cap \ldots \cap H_r$ and $M^- = [x_1, x_2, \ldots, x_r]$ the subspace spanned by the x_i. A theorem of E. Cartan and J. Dieudonné asserts that any orthogonal transformation is the product of at most n symmetries (n=dimension of vector space), and there exist orthogonal transformations which can not be expressed using less than n symmetries. If instead of symmetries we use any kind of involutions, how many do we need? Since the product of symmetries relative to orthogonal hyperplanes is an involution, our problem in connection with Cartan-Dieudonné theorem is to choose carefully the symmetries so that their product is decomposed in a minimum number of involutions.

2. From now on we always assume that the bilinear form (x,y) has index 0; this means that $(x,x) = 0$ if and only if $x = 0$. Then the restriction of (x,y) to any subspace $N \neq 0$ is non-degenerate.

https://doi.org/10.4153/CMB-1964-036-1 Published online by Cambridge University Press

If T is an orthogonal transformation of M, not necessarily an involution, we still define the plus- and minus-spaces as $M^{+} = \{x \mid xT = x\}$ and $M^{-} = \{x \mid xT = -x\}$. When we want to specify that these are the plus- and minus-spaces of T we write M_T^{+} and M_T^{-}. Now if T is not an involution $M^{+} \oplus M^{-} \neq M$, but we can write $M = M^{+} \oplus M^{-} \oplus M'$, where M' is the orthogonal complement of $M^{+} \oplus M^{-}$. We will call this decomposition of M the canonical decomposition of M relative to T. The subspace $M^{+} \oplus M^{-}$ can be characterized as the kernel of the linear transformation $I - T^2$.

The idea of the proof of the next lemma rests on the following well-known facts:

(a) If $x - xT \neq 0$ then $xTS = x$, where S is the symmetry relative to the hyperplane orthogonal to $x-xT$, and if $x+xT \neq 0$ and S' is the symmetry relative to the hyperplane orthogonal to $x+xT$ $xTS' = -x$. This follows immediately from $xT = \frac{x+xT}{2} - \frac{x-xT}{2}$ and $(x-xT, x+xT) = (x, x) - (xT, xT) = 0$.

(b) Conversely, if $xTS = x$ and $xT \neq x$ then the symmetry S must be the symmetry relative to a hyperplane orthogonal to $x-xT$, and if $xT = x$ S must be a symmetry relative to a hyperplane containing x. If $xTS = -x$, then, when $x+xT \neq 0$, S is the symmetry relative to the hyperplane orthogonal to $x+xT$ and, when $x+xT = 0$, S must be a symmetry relative to any hyperplane containing x.

When the transformation $I - T^2$ is $1 - 1$, that is, $M^{+} = M^{-} = 0$, for any $x \in M$ we get $x = y(I-T^2)$ and if S is the symmetry relative to the hyperplane orthogonal to x the plus-space of TS is $[y(I+T)]$ and the minus-space is $[y(I-T)]$.

LEMMA. Let M be a finite dimensional vector space over a commutative field k of characteristic $\neq 2$, with a non-degenerate symmetric bilinear form (x,y) of index 0. Then given a vector u and an orthogonal transformation T, such that $x = xT^2$ if and only if $x = 0$, there exists a symmetry S

https://doi.org/10.4153/CMB-1964-036-1 Published online by Cambridge University Press

such that $u \in M^+_{TS} + M^-_{TS}$, and u belongs also to the hyperplane which defines S.

Proof. If $u = 0$ any symmetry will satisfy the properties. So we assume $u \neq 0$. Then by our assumption on T, $uT^{-1} - uT \neq 0$; moreover

$$(1) \qquad (u, uT^{-1} - uT) = (u, uT^{-1}) - (u, uT) = (uT, u) - (u, uT) = 0 .$$

Let S be the symmetry relative to the hyperplane orthogonal to $uT^{-1} - uT$. Then (1) shows that S satisfies the last condition. Now $(uT^{-1})TS = uS = u$ and since $(uT^{-1} + uT, uT^{-1} - uT) = 0$, $uTS = \left(\frac{uT^{-1} + uT}{2} - \frac{uT^{-1} - uT}{2}\right) S = uT^{-1}$; hence if $y = u + uT^{-1}$, $yTS = (uT^{-1} + u)TS = u + uT^{-1} = y$, so $y \in M^+_{TS}$ and if $z = u - uT^{-1}$ then $zTS = uT^{-1} - u = -z$, that is, $z \in M^-_{TS}$. Therefore $u = \frac{y+z}{2} \in M^+_{TS} + M^-_{TS}$.

THEOREM. Let M, k and (x, y) be as in the lemma. Then any orthogonal transformation T is the product of at most two involutions.

Proof. Let $M = M^+_T \oplus M^-_T \oplus M'$ be the canonical decomposition of M relative to T. If $M' = 0$, T is an involution and there is nothing to be proved. So we assume $M' \neq 0$. Since M' is taken onto itself by $I - T^2$ for any non-zero vector $z_1 \in M'$, we get $z_1 = x_1(I - T^2)$ with $0 \neq x_1 \in M'$. Let S_1 be the symmetry relative to the hyperplane H_1 orthogonal to z_1, then the canonical decomposition of M relative to TS_1 is

$$M = (M^+_T + [x_1(I+T)])^+_{TS_1} \oplus (M^-_T + [x_1(I-T)])^-_{TS_1} \oplus M'' .$$

Let u_1 be the projection of z_1 on M'' relative to this decomposition. By the lemma we know that we can choose an element $z_2 \in M''$ such that $(u_1, z_2) = 0$, and if S_2 is the symmetry relative to the hyperplane H_2 orthogonal to z_2, and

$$M'' = [x_2] \oplus [y_2] \oplus M'''$$

is the canonical decomposition of M'' relative to TS_1S_2, then $u_1 \in [x_2] + [y_2]$. Since $(u_1, z_2) = 0$ and $z_2 \in M''$ we have $(z_1, z_2) = 0$.

Now let u_2 be the orthogonal projection of z_2 on M''' and take $z_3 \in M'''$ such that $(u_2, z_3) = 0$ and u_2 belongs to $[x_3] \oplus [y_3]$ where $M''' = [x_3] \oplus [y_3] \oplus M^{(iv)}$ is the canonical decomposition of M''' relative to $TS_1S_2S_3$. Since $(u_2, z_3) = 0$ and $z_3 \in M'''$ we have $(z_1, z_3) = (z_2, z_3) = 0$. Proceeding in this way we get a transformation $TS_1S_2 \ldots S_r$, where $r = \frac{1}{2} \dim M'$, which is an involution U_1. Since $S_1S_2 \ldots S_r = U_2$ is also an involution we obtain $T = U_1U_2$. Now, U_1 is the product of $r + \dim M_T^-$ symmetries, therefore T is a rotation if and only if $\dim M_T^-$ is even. Hence when T is not a rotation, $M_T^- \neq 0$.

The proof shows also that S_1 can be any symmetry whose hyperplane contains $M_T^+ \oplus M_T^-$.

REFERENCES

1. E. Artin, Geometric Algebra, Interscience, New York, (1957).

2. J. Dieudonné, La géométrie des groupes classiques, Springer, Berlin, (1955).

University of Toronto