

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 symplectic transformations but in the decomposition the involutions are not symplectic transformations but skew-symplectic 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

$$(1) \quad p(x) = r(x)(x+1)^s(x-1)^t,$$

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