LINEAR ALGEBRA AND ITS APPLICATIONS 7, 279–280 (1973)

A Note on Minimal Polynomials

MICHAEL HEYMANN AND JOHN A. THORPE
Mobil Research and Development Corporation
Central Research Division Laboratories
Princeton, New Jersey

Communicated by Hans Schneider

It is a standard theorem in linear algebra that, given a finite dimensional vector space V and a linear operator L on V with minimal polynomial ψ, there exists a vector $v \in V$ such that the monic polynomial φ of smallest degree such that $\varphi(L)(v) = 0$ is precisely ψ. However, the standard proofs of this theorem (see e.g. [2]) do not indicate how much freedom one has in choosing the vector v. The theorem below, which is useful in the theory of dynamical systems (see [1]), implies that, except for the case when the underlying field is finite, such a vector v can be found in the linear span of any subset S of V with the property that the minimal L-invariant subspace of V containing S is V itself.

Given a linear operator $L: V \to V$ and a subset S of V we shall denote by ψ_S the monic polynomial φ of smallest degree such that $\varphi(L)(S) = 0$. Thus ψ_S is the minimal polynomial of the restriction of L to the L-invariant subspace of V generated by S. For $v \in V$ we shall denote $\psi_{\{v\}}$ by ψ_v. For $S \subseteq V$, $\mathscr{L}(S)$ will denote the linear span of S.

THEOREM. *Let V be a finite dimensional vector space over an infinite field F, let L be a linear operator on V, and let S be a subset of V. Then there exists $v \in \mathscr{L}(S)$ such that $\psi_v = \psi_S$.*

This theorem is an immediate consequence of the following two lemmas.

LEMMA 1. *Let V be a finite dimensional vector space over an arbitrary field, let $L: V \to V$ be linear, and let $S \subseteq V$. Then*

$$\{v \in \mathscr{L}(S) \mid \psi_v \neq \psi_S\}$$

is a union of k proper subspaces of $\mathscr{L}(S)$, where k is the number of distinct prime factors in ψ_S.

Proof. Let $\psi_S = \prod_{j=1}^k p_j^{r_j}$ be the prime decomposition of ψ_S. Letting $W = \mathscr{L}(S)$, $\psi_W = \psi_S$. Hence, for each $v \in W$, ψ_v divides ψ_S, i.e. $\psi_v = \prod_{j=1}^k p_j^{s_j(v)}$ where $s_j(v) \leqslant r_j$ for all j. For each j $(1 \leqslant j \leqslant k)$ let

$$W_j = \{v \in W | s_j(v) < r_j\}.$$

Clearly $\psi_v \neq \psi_S$ if and only if $v \in \bigcup_{j=1}^k W_j$. W_j is a subspace of W because, for $v, w \in W_j$, $\psi_{\{v,w\}}$ is the least common multiple of ψ_v and ψ_w. Similarly, $W_j \neq W$ since ψ_{W_j} is the least common multiple of $\{\psi_v | v \in W_j\}$. ■

LEMMA 2. *Let W be a vector space over an infinite field F. Then W is not a finite union of proper subspaces.*

Proof. It is clearly enough to prove the lemma for subspaces of codimension 1. In this case, the result is given by [3, Lemma 2 or Lemma 3]. ■

REMARK. That the theorem above is not valid over finite fields is illustrated by the following example. Let V be a vector space over Z_2 of dimension at least 4. Let $e_1, \ldots, e_4$ be linearly independent in V and let $L: V \to V$ be such that $Le_1 = e_2$, $Le_2 = e_1 + e_2$, $Le_3 = e_3$, and $Le_4 = 0$. Let $S = \{v_1, v_2\}$ where $v_1 = e_1 + e_3$ and $v_2 = e_3 + e_4$. Then $\psi_S = X(X + 1)(X^2 + X + 1)$ but the only nonzero vectors in $\mathscr{L}(S)$ are v_1, v_2 and $v_3 = v_1 + v_2 = e_1 + e_4$ with $\psi_{v_1} = (X + 1)(X^2 + X + 1)$, $\psi_{v_2} = X(X + 1)$ and $\psi_{v_3} = X(X^2 + X + 1)$.

REFERENCES

1 M. Heymann, On the input and output reducibility of multivariable linear systems, *IEEE Trans. Aut. Control* **AC15**(1970), 563–569.

2 N. Jacobson, *Lectures in Abstract Algebra*, Vol. II, Van Nostrand, Princeton, N. J. (1953).

3 E. C. Posner and H. Schneider, Hyperplanes and prime rings, *Archiv. Math.* **11**(1960), 322–326.

Received June, 1968