A PROOF OF A THEOREM ON COMMUTATIVE MATRICES

PACO LAGERSTROM

The following theorem is well known (see, for example, Wedderburn, *Lectures on matrices*, p. 106):

"*If the matrix B commutes with every matrix that commutes with A, then B is a scalar polynomial of A.*"

It is thought, however, that the proof given below is simple enough to be of interest. The proof is based on the main theorem for abelian groups with a finite number of generators. The version of this theorem given in van der Waerden, Moderne Algebra, vol. 2, pp. 114 and 122, is especially well suited for our purpose. Let $\mathfrak{M}$ be a finite-dimensional vector space over a commutative field K. Let A be a fixed linear endomorphism of $\mathfrak{M}$. All endomorphisms of the form $P(A)$, where $P(x)$ is a polynomial with coefficients in K, form a euclidean ring of operators on $\mathfrak{M}$. "Admissible subgroups" (van der Waerden, Moderne Algebra, vol. 1, p. 145) with respect to this set of operators are those subspaces of $\mathfrak{M}$ which are invariant under A. The main theorem about the decomposition of abelian groups, as applied to $\mathfrak{M}$, then reads: There exist a finite number of subspaces $\mathfrak{M}_i$ and polynomials over K, $P_i(x)$, such that:

(1a) $\mathfrak{M}$ is a direct sum of the $\mathfrak{M}_i$.

(1b) $\mathfrak{M}_i$ is invariant under A.

(1c) Each $\mathfrak{M}_i$ is cyclic. This means that there exist elements e_i such that each element of $\mathfrak{M}_i$ is of the form $P(A)e_i$.

(1d) $P_i(x)$ generates the annihilating ideal of $\mathfrak{M}_i$.

(1e) $P_{i+1}(x)$ divides $P_i(x)$.

It follows that $P_1(A)=0$ and that $P(A)=0$ implies that $P_1(x)$ divides $P(x)$. (In a terminology sometimes used $P_i(x)$ is the order of e_i with respect to A and $P_1(x)$ is the minimal polynomial of A. Thus the order of e_1 is the minimal polynomial of A. Conversely, once the existence of an element with this property has been demonstrated, the decomposition theorem is easily proved.)

We denote by E_i the projection on $\mathfrak{M}_i$, that is, the linear endomorphism uniquely defined by: $E_if=f$ if f is in $\mathfrak{M}_i$ and $E_if=0$ if f is in $\mathfrak{M}_j$, $j\neq i$. It follows that f is in $\mathfrak{M}_i$ if and only if $E_if=f$. An endomorphism C which commutes with E_i leaves $\mathfrak{M}_i$ invariant because if f is in $\mathfrak{M}_i$, then $E_iCf=CE_if=Cf$. Conversely, if all $\mathfrak{M}_i$ are invariant un-

Received by the editors September 7, 1944, and, in revised form, March 8, 1945.

der C, then $CE_i = E_iC$. Also, if E is the identity mapping, then $E = \Sigma E_i$.

After these preliminaries we are ready to give a concise formulation and a proof of the theorem stated at the very beginning of this note:

THEOREM 1. *Let $\mathfrak{M}$ be a finite-dimensional vector space over a commutative field K and A and B linear endomorphisms of $\mathfrak{M}$ such that B commutes with every endomorphism that commutes with A. Then there exists a polynomial $\overline{Q}(x)$ with coefficients in K such that $B = \overline{Q}(A)$.*

Using the notation explained above we first prove a lemma:

LEMMA. *A polynomial $Q(x)$ may be found satisfying the relation $Be_1 = Q(A)e_1$ (where as remarked above any element whose order is the minimal polynomial of A may be taken as e_1). $Q(x)$ also satisfies the relation $BE_1 = Q(A)E_1$.*

PROOF. Since each $\mathfrak{M}_i$ is invariant under A, each E_i commutes with A and hence with B. Thus each $\mathfrak{M}_i$ is also invariant under B, in particular Be_1 is in $\mathfrak{M}_1$ from which the existence of $Q(x)$ follows by (1c). Now let f be in $\mathfrak{M}_1$. Then for some polynomial $P(x)$, $f = P(A)e_1$ and $BE_1f = Bf = BP(A)e_1 = P(A)Be_1 = P(A)Q(A)e_1 = Q(A)f = Q(A)E_1f$. If f is in $\mathfrak{M}_i$, $i \neq 1$, then $BE_1f = Q(A)E_1f = 0$ which concludes the proof of the lemma.

In order to prove that the $Q(x)$ defined in the lemma may be taken as the $\overline{Q}(x)$ of Theorem 1, we have to show that $BE_i = Q(A)E_i$ for any i. For this purpose we define a mapping M_i by:

(2a) $M_iR(A)e_1 = R(A)e_i$ for any polynomial $R(x)$.

(2b) $M_if = 0$ for f in $\mathfrak{M}_j$, $j \neq 1$.

(2c) M is a linear endomorphism of $\mathfrak{M}$.

Condition 2a defines a one-valued mapping because if $R(A)e_1 = S(A)e_1$, then $R(x) - S(x)$ is divisible by $P_1(x)$ (by 1d) and by $P_i(x)$ (by 1e) and hence $R(A)e_i = S(A)e_i$. Evidently M_i commutes with A and hence with B. From this follows: $Be_i = BM_ie_1 = M_iBe_1 = M_iQ(A)e_1 = Q(A)e_i$. Since $Be_i = Q(A)e_i$, we may prove as above that $BE_i = Q(A)E_i$.

The proof is now complete since $B = \Sigma BE_i = \Sigma Q(A)E_i = Q(A)$.

The above proof suggests a generalization. Namely, in Theorem 1 the vector space $\mathfrak{M}$ and the ring of polynomials of A may be replaced by any abelian group with a commutative ring of operators for which the decomposition theorem is valid. It can then be seen easily that the proof given in this note remains valid without essential changes.

PRINCETON UNIVERSITY