# 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.