A Minimal Property of the Jordan Canonical Form*

HANS F. BÜCKNER
General Electric Company
Schenectady, New York

Communicated by Alan J. Hoffman

Let V be a complex linear space of dimension $n > 0$ and T a linear transformation of V into V. T can be represented with the aid of a basis of V and of a matrix describing the effect of T on the basis elements. As it is well known the matrix takes a particularly simple form if the basis $v_1, v_2, \ldots, v_n$ can be so chosen that

$$Tv_k = \alpha_k v_k + \beta_k v_{k-1} \qquad \text{for} \quad k = 1, 2, \ldots, n-1, \qquad Tv_n = \alpha_n v_n \quad (1)$$

with suitable scalars α_i, β_k of which β_k is restricted to the values 0 and 1, while $\alpha_{k+1} = \alpha_k$ if $\beta_k = 1$. The matrix so determined is said to have Jordan normal or Jordan canonical form. This note will deal with the basis in (1) and with an associated decomposition of V into subspaces invariant under T. To this end we introduce

DEFINITION 1. A subspace V' of V with dimension $p > 0$ is called Jordan or Jordan subspace with respect to T, if V' has a basis $e_1, e_2, \ldots, e_p$ such that $Te_p = \alpha e_p$, $Te_k = \alpha e_k + e_{k+1}$ for $k = 1, 2, \ldots, p-1$. We denote α as eigenvalue of V'.

It is easily verified that $e \in V'$ and $Te = \beta e$ imply either $\beta = \alpha$ or $e = \theta$, where θ denotes the null element of the space. Therefore a Jordan subspace with respect to T has but one eigenvalue. Definition 1 permits us to express some of the features of the Jordan normal form by

* Dedicated to Professor A. M. Ostrowski on his 75th birthday.

Linear Algebra and Its Applications 1, 503–510 (1968)

THEOREM 1. *V is the direct sum of Jordan subspaces $V_1, V_2, \ldots, V_s$ with respect to T. If V is also the direct sum of Jordan subspaces $W_1, W_2, \ldots, W_t$ with respect to T then $t = s$; moreover a $1:1$ correspondence between the V_i and the W_k exists such that corresponding subspaces have dimension and eigenvalue in common.*

The customary proofs of the theorem use concepts and results from the theory of polynomials and Abelian groups as tools. Typical examples appear in the books [1, 2]. In this note a *new* derivation of the theorem will be given. It will be related to the circumstance that the decomposition in Theorem 1 can be characterized by a minimum property. Our tools are confined to elementary results from the theory of polynomials with complex coefficients. We list them right here:

1. Latin letters followed by (z) denote a polynomial of z. The letters may have subscripts. If $p(z) = a_0 + a_1 z + \cdots + a_m z^m$ and $a_m \neq 0$, we call m the degree of $p(z)$. If $m \geqslant 1$ we can write

$$p(z) = a_m \prod_{k=1}^{l} (z - z_k)^{m_k}, \qquad z_i \neq z_j \quad \text{if} \quad i \neq j, \tag{2}$$

with positive integers m_k. The number l over the product sign as well as the numbers m_k, z_k are unique. We call l the *width* of $p(z)$. If $m = 0$, we assign width zero to the polynomial. We introduce the linear transformation (linear operator)

$$p(T) = a_0 I + a_1 T + \cdots + a_m T^m, \qquad I = \text{unit operator}.$$

Relations between polynomials such as $f(z) = g(z) + h(z)$, $p(z) = q(z)r(z)$ imply $f(T) = g(T) + h(T)$, $p(T) = q(T)r(T)$ and $f(T)u = g(T)u + h(T)u$, $p(T)u = q(T)r(T)u$ for any $u \in V$.

2. If $p(z) \not\equiv 0$, $q(z) \not\equiv 0$ are given, we may write as a result of the well-known division algorithm $p(z) = a(z)q(z) + b(z)$, where $b(z)$ either vanishes identically or has degree less than $q(z)$. The polynomials $a(z)$, $b(z)$ are unique. $p(z), q(z)$ can be represented in the form $p(z) = d(z)r(z)$, $q(z) = d(z)s(z)$, where $r(z)$ and $s(z)$ have no zero in common. The so-called largest common divisor $d(z)$ of $p(z)$ and $q(z)$ admits a representation $d(z) = f(z)p(z) + g(z)q(z)$; a constant factor disregarded, $d(z)$ is unique. We write $p|q = 1$, if $d(z) \equiv \text{const}$.

3. Let J be an ideal of polynomials, i.e., $f(z)p(z) + g(z)q(z) \in J$ whenever $p(z), q(z)$ belong to J. If J contains polynomials $p(z) \not\equiv 0$, then a

polynomial $m(z) \not\equiv 0$ of smallest degree exists in J. It divides any polynomial of J. A constant factor disregarded, $m(z)$ is unique. It is called the minimum polynomial of J.

The following two definitions are known [2].

DEFINITION 2. $f(z)$ is a null polynomial of $v \in V$ with respect to T if $f(T)v = \theta$; $g(z)$ is a null polynomial of T if $g(T) = O$, where O is the null operator.

Example. The basis elements of the Jordan subspace V' of V in Definition 1 satisfy relations $e_{k+1} = Se_k$, $S = T - \alpha I$, for $k = 1, 2, \ldots, p - 1$ and $Se_p = \theta$. It follows that $Se_p = S^q e_{p+1-q} = \theta$, and $(z - \alpha)^q$ is seen to be a null polynomial of e_{p+1-q}. Any element $v \in V'$ has $(z - \alpha)^p$ as null polynomial. If $V' = V$ then $(z - \alpha)^p$ is also a null polynomial of T.

The null polynomials of v with respect to T form an ideal $J(v, T)$, and the null polynomials of T form an ideal $J(T)$. We have $J(T) \subset J(v, T)$, where $\subset$ means inclusion or equality. Since $v, Tv, \ldots, T^n v$ are linearly dependent, $J(v, T)$ contains polynomials of degree n. If $v_1, v_2, \ldots, v_n$ is a basis of V then $f(z) = f_1(z) f_2(z) \cdots f_n(z)$ with $f_k(z) \in J(v_k, T)$ belongs to $J(T)$.

DEFINITION 3. We denote the minimum polynomial of $J(v, T)$ by $f(z, v)$ and call it also the minimum polynomial of v with respect to T. The minimum polynomial of $J(T)$ is denoted by $F(z)$. We also refer to it as the minimum polynomial of T. If $W \subset V$ is a subspace invariant under T, the restriction T' of T to W gives rise to an ideal of null polynomials of T'. We write $F(z, W)$ for the minimum polynomial of that ideal and call it the minimum polynomial of T'.

We observe that $F(z, W)$ divides $F(z)$ and that $f(z, v)$ divides $F(z)$; $f(z, v)$ divides $F(z, W)$ if $v \in W$.

LEMMA 1. *Let $u \in V$ and $f(z), g(z)$ be such that $f | g = 1$, $g(T)u = \theta$; then $v = f(T)u$ implies $u = a(T)v$ with a suitable $a(z)$, which depends on $f(z), g(z)$ only.*

Proof. $a(z)f(z) + b(z)g(z) = 1$ with suitable $a(z), b(z)$; therefore $u = a(T)f(T)u + b(T)g(T)u = a(T)f(T)u = a(T)v$.

Let $U = (u_1, u_2, \ldots, u_m)$ be a sequence of elements u_k of V. We introduce $T[U]$ as the set of all elements of the form $u = \sum_{i=1}^{m} g_i(T)u_i$, where the $g_k(z)$ run through all polynomials. Evidently $T[U]$ is a subspace of V, invariant under T. If $U = (u)$ we write $T[U] = T[u]$.

Example. $V' = T[e_1]$ in the situation of Definition 1. Indeed $g(z) = \sum_k c_k(z-\alpha)^{k-1}$ for any $g(z)$; hence $g(T)e_1 = \sum_{k=1}^{v} c_k e_k \in V'$; since the c_k can be arbitrarily chosen, all elements $g(T)e_1$ exhaust V'.

DEFINITION 4. If $f(z, v)$ has degree k and width l, then $\omega(v) = |k + l - 1|$ is the degree of v under T. $\omega(U) = \omega(u_1) + \omega(u_2) + \cdots + \omega(u_m)$ is the degree of U under T.

DEFINITION 5. The sequence U is called

(1) minimal, if $T[U] \subset T[U']$ implies $\omega(U) \leqslant \omega(U')$ for any sequence U';

(2) T-independent, if $T[U]$ is the direct sum of the subspaces $T[u_k]$, $k = 1, 2, \ldots, m$;

(3) X-yielding, if $T[U]$ contains the set $X \subset V$.

It is easy to show the existence of minimal sequences. Given $X \subset V$ consider all X-yielding sequences U. Such sequences exist; e.g., take for U a basis of V. Among the X-yielding sequences U there is at least one of smallest degree. That sequence is obviously minimal. Here we introduce the statement that any V-yielding minimal sequence provides Jordan subspaces $T[u_k]$ in accordance with Theorem 1. Apart from the case $U = (\theta)$ no minimal sequence can contain θ, since $\omega(\theta) = 1$. We assume $U \neq (\theta)$ from here on. No minimal sequence can contain the same element twice, and for this reason we shall speak of minimal sets rather than of minimal sequences.

In what follows dim W denotes the dimension of the subspace $W \subset V$.

LEMMA 2. (a) $\dim T[U] \leqslant \omega(U)$; (b) *$U$ is minimal if* $\dim T[U] = \omega(U)$.

Proof. We have $\dim T[U] \leqslant \sum_{k=1}^{m} \dim T[u_k]$. In order to prove (a) it suffices to show that $\dim T[u] \leqslant \omega(u)$. Let $f(z, u)$ have degree p. Then $u, Tu, \ldots, T^{p-1}u$ form a set of linearly independent elements in $T[u]$. Now any $g(z)$ can be written in the form $g(z) = a(z)f(z, u) + b(z)$;

$b(z) = \sum_{k=0}^{p-1} b_k z^k$; hence $g(T)u = b(T)u = \sum_{k=0}^{p-1} b_k T^k u$, and $u, Tu, \ldots, T^{p-1}u$ are even a basis of $T[u]$. Thus $\dim T[u] = p \leqslant \omega(u)$. This completes the proof of (a). Statement (b) is a trivial consequence of (a) and of $\dim T[U] = \omega(U)$.

LEMMA 3. *$U = (u)$ is minimal if and only if $f(z, u)$ has width one.*

Proof. Let $f(z, u)$ have width one and degree p. The proof of Lemma 2 shows that $\dim T[u] = p$; but $\omega(u) = p$, and (u) is minimal by Lemma 2. Let us now assume that $f(z, u)$ has width $l > 1$. In this case we can derive from the decomposition (2) for $f(z, u)$ that $f(z, u) = f_1(z) f_2(z)$ with $f_1 | f_2 = 1$, f_k having degree $p_k \geqslant 1$ and width $l_k \geqslant 1$. The degree of $f(z, u)$ is $p = p_1 + p_2$, and the width of $f(z, u)$ is $l = l_1 + l_2$. We have $a_1(z), a_2(z)$ such that $a_1(z) f_1(z) + a_2(z) f_2(z) = 1$. Set now $u_1 = a_2(T) f_2(T) u$, $u_2 = a_1(T) f_1(T) u$, and $U' = (u_1, u_2)$. We have $u = u_1 + u_2$, whence $T[U] \subset T[U']$. Since $f_k(z)$ is a null polynomial of u_k, we find $\omega(u_k) \leqslant p_k + l_k - 1$ and thus $\omega(U') = \omega(u_1) + \omega(u_2) \leqslant p_1 + l_1 - 1 + p_2 + l_2 - 1 < p + l - 1 = \omega(u)$. It follows that (u) cannot be minimal if $f(z, u)$ has width > 1. This completes the proof.

LEMMA 4. *If $f(z, u)$ has width one, $T[u]$ is Jordan, and vice versa.*

Proof. We can assume $f(z, u) = (z - \alpha)^p$; set $S = T - \alpha I$ and $e_k = S^{k-1} u$, $k = 1, 2, \ldots, p$. The elements e_k form a basis of $T[u]$ in accordance with Definition 1. The example to Definition 2 shows that the inverse statement is also true.

LEMMA 5. *If $U = (u_1, u_2, \ldots, u_m)$ is a minimal set, then any non-empty subset of U is also minimal.*

Proof. It suffices to consider a subset of the form $U' = (u_1, u_2, \ldots, u_r)$, $r < m$. If U' were not minimal we would have W such that $\omega(W) < \omega(U')$, $T[U'] \subset T[W]$. But then we can construct a set U^* out of the elements of W and of $u_{r+1}, \ldots, u_m$, such that $T[U] \subset T[U^*]$, while $\omega(U^*) < \omega(U)$, which contradicts the assumption on U.

Lemmas 3, 4, 5 yield the result that any minimal set $U = (u_1, u_2, \ldots, u_m)$ has the property that all $T[u_k]$ are Jordan. We proceed to look for other properties. A minimal set will be called *pure* if all $T[u_k]$ have the same eigenvalue, which we shall denote as the eigenvalue of the pure set. If U is not pure, it can be split into disjoint pure subsets $U_1, U_2, \ldots, U_x$ with distinct eigenvalues $\alpha_1, \alpha_2, \ldots, \alpha_x$ respectively. Introducing the abbreviations $W = T[U]$, $W_k = T[U_k]$, $k = 1, 2, \ldots, x$, we introduce

LEMMA 6. *W is the direct sum of $W_1, W_2, \ldots,$ and W_x. The subspaces W_k are uniquely determined by W and T.*

Proof. Any element $w_k \in W_k$ has null polynomials of the form $(z-\alpha_k)^{m'}$; therefore $f(z, w_k) = (z-\alpha_k)^{m''}$ with some integer $m'' \leqslant n$. Let p_k be the largest of all m'', as w_k runs through W_k. Set $P_k(z) = (z-\alpha_k)^{p_k}$, $P(z) = \prod_{k=1}^{x} P_k(z)$, and $Q_k(z) = P(z)/P_k(z)$. We can interpret $P_k(z)$ as minimum polynomial of the restriction of T to W_k, i.e., $P_k(z) = F(z, W_k)$. In similar vein $P(z) = F(z, W)$. The latter relation shows at once that $P(z)$ depends on W and T only, and the same is true with respect to the polynomials $P_k(z)$, $Q_k(z)$, since these are uniquely determined by $P(z)$. Consider now $w = w_1 + w_2 + \cdots + w_x$, $w_k \in W_k$. Any element $w \in W$ can be written that way, and vice versa any sum of elements w_i belongs to W. We find $Q_k(T)w = Q_k(T)w_k$ together with $P_k(T)w_k = \theta$. By virtue of $P_k | Q_k = 1$ and of Lemma 1 we can find a polynomial $a_k(z)$, depending on P_k, Q_k only, such that $w_k = a_k(T)w$. Thus w_k is uniquely determined by w; W_k is obviously the range of the restriction of $a_k(T)$ to W. This completes the proof.

LEMMA 7. *If $U = (u_1, u_2, \ldots, u_m)$ is pure, it is also T-independent.*

Proof. Let α be the eigenvalue of U. Let polynomials $g_k(z)$ exist such that $\sum_{k=1}^{x} g_k(T)u_k = \theta$ while not all $g_k(T)u_k = \theta$. We write $g_k(z) = (z-\alpha)^{q_k} h_k(z)$, where $h_k(\alpha) \neq 0$. We have $q_k < \omega(u_k)$ for at least one k. Without loss of generality we can assume $q_1 < \omega(u_1)$ and also $q_1 \leqslant q_k$ for $k = 2, 3, \ldots, m$. Since $h_1(z) | f(z, u_1) = 1$, Lemma 1 yields $u_1 = a(T)h_1(T)u_1$ with some $a(z)$. This leads to $\sum_{k=1}^{m} a(T)g_k(T)u_k = \theta$ or $S^{q_1}u^* = \theta$ with $S = T - \alpha I$, and $u^* = u_1 + \sum_{k=2}^{m} r_k(T)u_k$; $r_k(z) = a(z)h_k(z)(z-\alpha)^{q_k - q_1}$. Introduce $U^* = (u^*, u_2, u_3, \ldots, u_m)$. Clearly $T[U] \subset T[U^*]$. If $u^* = \theta$ then U cannot be minimal; if $u^* \neq \theta$, we have $q_1 > 0$ and $\omega(U) - \omega(U^*) = \omega(u_1) - \omega(u^*) \geqslant \omega(u_1) - q_1 > 0$, which also contradicts the minimal property of U. This means that the polynomials $g_k(z)$, as specified above, do not exist, and U is T-independent as asserted.

Using the denotations of Lemma 7 and its proof we form the sets $X_i = (S^i u_1, S^i u_2, \ldots, S^i u_m)^*$, $i = 0, 1, \ldots$; the asterisk indicates that elements $S^i u_k \neq \theta$ only are to be listed. It follows from Lemma 7 that X_i, if not empty, is T-independent. Therefore if $D_i = \dim T[X_i]$,

$$D_i = \sum_{k=1}^{m} \dim T[S^i u_k]. \tag{3}$$

Now $T[S^i u_k]$ is evidently Jordan, and

$$\dim T[S^i u_k] = \omega(S^i u_k) = \omega(u_k) - i; \qquad S^i u_k \neq \theta. \tag{4}$$

Let us now introduce a function $\rho(d)$ of the nonnegative integers d as follows: $\rho(d) = 0$ if $d \neq \omega(u_k)$ for all k; otherwise $\rho(d)$ shall equal the number of those elements u_i for which $d = \omega(u_i)$. Relations (3), (4) can now be rewritten as

$$D_i = \sum_{d=i+1}^{D_0} \rho(d)(d - i), \qquad i = 0, 1, \ldots, D_0 - 1. \tag{5}$$

Interpreted as a system of linear equations for the unknowns $\rho(1), \rho(2), \ldots,$ the relations (5) have Gaussian form and yield the unique solution

$$\rho(i) = D_{i+1} - 2D_i + D_{i-1}. \tag{6}$$

Now $T[X_i]$ can be interpreted as the image of $T[U]$ under the transformation S^i. This implies that D_i is uniquely determined by $T[U]$ and T. Thus (6) implies

LEMMA 8. *The numbers $\omega(u_k)$, associated with a pure set $U = (u_1, u_2, \ldots, u_m)$, their order disregarded, are uniquely determined by $T[U]$ and by T.*

The results from some of the preceding lemmas can be summed up by

THEOREM 2. *Any minimal set $U = (u_1, u_2, \ldots, u_m)$ is T-independent; the subspaces $T[u_k]$ are Jordan; the numbers $\omega(u_k)$ are uniquely determined by $T[U]$ and T. If, vice versa, a sequence U is T-independent and if the $T[u_k]$ are Jordan, then U is minimal.*

Theorem 2 yields Theorem 1 in every detail if the minimal set is V-yielding. We have already remarked that the existence of such sets is trivial.

REFERENCES

1 G. Birkhoff and S. Mac Lane, *A Survey of Modern Algebra*, Macmillan, New York, 1955.
2 F. R. Gantmacher, *Theory of Matrices* (in Russian), Chapter 7, Moscow, 1954.

Received March 22, 1968