King Fahd University of Petroleum & Minerals

DEPARTMENT OF MATHEMATICAL SCIENCES

Technical Report Series

TR 109

April 1989

A Constructive Proof of the Cyclic Decomposition Theorem in Linear Algebra

Ersan Akyildiz

DHAHRAN 31261 ● SAUDI ARABIA ● www.kfupm.edu.sa/math/ ● E-mail: mathdept@kfupm.edu.sa

0. Introduction.

The purpose of this note is to give some relations between the Cyclic decomposition and the Primary decomposition theorems in Linear Algebra. One of the important relations between these theorems appears already in finding the Jordan cononical form of an nxn triangulable matrix A over the field F. Here, we produce an algorithm to show how to obtain the Cyclic decomposition theorem for the linear operator T on a finite dimensional vector space V over F from the Primary decomposition theorem for T.

There are already several different proofs of the Cyclic decomposition theorem in the literature, and we expect that the approach given here is already known to the experts. But we do not know if it exists in print. While teaching a course on Linear algebra we couldn't find any reference, which enables one to obtain $\alpha_1,\ldots,\alpha_r$ systematically so that $V=\overset{r}{\underset{i=1}{\oplus}} Z(\alpha_i;T)$. Here $Z(\alpha_i;T)=\{\ f(T)(\alpha_i)\colon\ f(X)\in F[X]\}$ is the T-cyclic subspace of V generated by $\alpha_i \in V$. Our only reference for the material is the classic book of K.Hoffman and R.Kunze, we shall follow their notations.

1.Preliminaries.

Let $T:V \longrightarrow V$ be a linear operator on the finite dimensional vector space V over the field F,and let f be the minimal polynomial for T, and

$$f = p_1^{m_1} \ldots\ldots p_k^{m_k}$$

be the primary decomposition of f (i.e.,for each i=1,...,k, p_i is a monic irreducible polynomial over F, $p_i \neq p_j$, $i \neq j$, and $m_i \geq 1$).

Let W_i denote the null space of $p_i(T)^{m_i}$, for i=1,...,k.

THEOREM A (Primary Decomposition Theorem).

(i) $V=W_1 \oplus W_2 \oplus \ldots \oplus W_k$;

(ii) each W_i is invariant under T ;

(iii) if T_i is the operator induced on W_i by T, then the minimal polynomial for T_i is $p_i^{m_i}(x)$.

Proof.[1,p.220].

The decomposition $V=W_1 \oplus W_2 \oplus \ldots \oplus W_k$ given above is called The Primary decomposition of (T,V). For a given vector α in V, the polynomial p_α denotes the T-annihilator of α , and $Z(\alpha,T)$ denotes the T-cyclic subspace $\{f(T)(\alpha) : f(x) \in F[X]\}$ of V generated by α.

THEOREM B (Cyclic Decomposition Theorem). There exists non zero vectors $\alpha_1,\ldots,\alpha_r$ in V with respective T-annihilators $p_1,\ldots,p_r$ such that

(i) $V=Z(\alpha_1,T)\oplus \ldots\ldots \oplus Z(\alpha_r,T)$;

(ii) p_i divides p_{i-1} , i=2,...r.

Furthermore, the integer r and the annihilators $p_1,\ldots,p_r$ are uniquely determined by (i),(ii), and the fact that no α_k is 0.

The decompositon $V=Z(\beta_1,T)\oplus \ldots\ldots \oplus Z(\beta_r,T)$ is said to be <u>a cyclic decomposition of (T,V)</u> if for each i=1,...,r , $\beta_i \neq 0$, and p_{β_m} divides $p_{\beta_{m-1}}$, m=2,...,r.

II. <u>Proof of Theorem B</u>.

We keep the notation of section 1, and moreover for the linear operator $T:V\longrightarrow V$ on a finite dimensional vector space V over F, let $V= W_1\oplus \ldots\ldots \oplus W_k$ stand for the primary decomposition of (T,V), and T_i be the operator induced on W_i by T, i=1,...,k. The following Proposition reduces the existence part of the proof of Theorem B to the case where the minimal polynomial of T is a power of a monic irreducible polynomial.

PROPOSITION 2.1. Let $W_i= Z(\alpha_{i,1},T_i)\oplus \ldots\ldots \oplus Z(\alpha_{i,d_i},T_i)$ be a cyclic decomposition of (T_i,W_i), i=1,...,k. Then

$V= Z(\alpha_1,T)\oplus.....\oplus Z(\alpha_r,T)$ is a cyclic decomposition of (T,V),

where $r=\max_i d_i$, and $\alpha_j=\sum_{d_i\geq j}\alpha_{i,j}$, $j=1,...,r$.

The Proposition 2.1 follows from the following Lemma, where the details are left to the reader.

LEMMA 2.1. Let $\alpha=\sum_{i=1}^{k}\alpha_i$, $\beta=\sum_{i=1}^{k}\beta_i$ be two vectors in V, where α_i and β_i are in W_i for each $i=1,...,k$. Then we have

(a) $p_\alpha=\prod_{\alpha_i\neq 0} p_{\alpha_i}$,

(b) p_α divides P_β if and only if p_{α_i} divides p_{β_i} for each $i=1,...,k$.

(c) $Z(\alpha,T)=\overset{k}{\underset{i=1}{\oplus}} Z(\alpha_i,T_i)$.

PROPOSITION 2.2. Let $V=\overset{r}{\underset{s=1}{\oplus}} Z(\alpha_s,T)$ be a cyclic decomposition of (T,V), and let $E_i:V\longrightarrow W_i$ be the projection map on W_i associated to the direct sum $V=\overset{k}{\underset{i=1}{\oplus}} W_i$. Then we have

(a) if $E_i(\alpha_m)=0$, then $E_i(\alpha_{m+1})= .....=E_i(\alpha_r)=0$,

(b) for each $i=1...,k$, $W_i=\overset{m_i}{\underset{j=1}{\oplus}} Z(E_i(\alpha_j),T_i)$ is a cyclic decomposition of (T_i,W_i), where m_i is the smallest integer in $\{1,...,r\}$ such that $E_i(\alpha_{m_i})\neq 0$, but $E_i(\alpha_{m_i+1})=0$.

Proof. It follows from Lemma 2.1.

It is easy to check that Propositions 2.1,2.2 and Lemma 2.1 reduce the proof of Theorem B completely to the the case where the minimal polynomial f(x) of T is a power of a monic irreducible polynomial p(x). Throughout the rest of the paper we assume that the minimal polynomial of the operator $T:V \longrightarrow V$ is equal to $p(x)^k$, where p(x) is a monic irreducible polynomial over F. We denote the null space of $p(T)^i:V \longrightarrow V$ by V_i for i=0,1,...,k. It is clear that each V_i is T-invariant, and thus T induces a linear operator on V_i , which we denote it by T_i. Since $V_{i-1} \subseteq V_i$, $T_i:V_i \longrightarrow V_i$ induces a linear operator on the quotient space V_i/V_{i-1} , which is denoted by $\bar{T}_i$. We denote the elements of the quotient space W/W_1 by $\bar{\alpha}$, $\alpha \in W$.

LEMMA 2.2. For each i=1,...,k, we have

(a) $V_{i-1} \neq V_i$,

(b) the minimal polynomial of the operator $\bar{T}_i$ is p(x),

(c) the minimal polynomial of the operator T_i is $p(x)^i$.

Proof. For each i=1,...,k, the linear map T induces the linear transformation $p(\bar{T})^{k-i}:V_k/V_{k-1} \longrightarrow V_i/V_{i-1}$. Since $V_k/V_{k-1} \neq (0)$

and $p(\bar{T})^{k-i}$ is an injective map, we get $V_{i-1} \neq V_i$. Part (b) follows from (a) and the fact that $p(T)V_i \subseteq V_{i-1}$. Part (c) follows easily from (a) and (b).

LEMMA 2.3. Let $T:V \longrightarrow V$ be a linear map on a finite dimensional vector space V with the minimal polynomial p(x). Then there exists non zero vectors α_i , i=1,...,r , such that $V=Z(\alpha_1,T) \oplus \ldots . \oplus Z(\alpha_r,T)$, and the T-annihilator p_{α_i} of $\alpha_i = p(x)$ for each i=1,...,r. In particular, the integer r and the polynomials p_{α_i} are independent than the decomposition of V into the direct sum of cyclic subspaces $Z(\beta_j,T)$.

Proof. Let $\alpha_1 \neq 0$ vector in V. Since the minimal polynomial p(x) is irreducible, $p_{\alpha_1}=p(x)$. If $V \neq Z(\alpha_1,T)$, choose an element $\alpha_2 \in V \setminus Z(\alpha_1,T)$. We claim that the sum $Z(\alpha_1,T)+Z(\alpha_2,T)$ is direct. If $f(T)(\alpha_2) \in Z(\alpha_1,T)$, then $f=p(x)g(x)$ for some polynomial g(x), because the T-conductor of α_2 in $Z(\alpha_1,T)$ is equal to p(x). Thus $Z(\alpha_1,T) \cap Z(\alpha_2,T)=\{0\}$, and the sum $W= Z(\alpha_1,T)+ Z(\alpha_2,T)$ is direct. If $W \neq V$, we choose an element $\alpha_3 \in V \setminus W$. With an argument similar to above it is easy to check that the sum $Z(\alpha_3,T)+W$ is direct. Since V is a finite dimensional space, by continuing this way , it is clear that there exists $\alpha_1,\ldots,\alpha_r$, where r=dim V/deg p, such that $V=Z(\alpha_1,T) \oplus \ldots . \oplus Z(\alpha_r,T)$ with $p_{\alpha_i} = p(x)$ for each i=1,..,r. The

number r and the polynomials p_{α_i} are uniquely determined by the decomposition follows from the fact that the minimal polynomial p(x) of T is irreducible.

In the general case $T:V \longrightarrow V$, where the minimal polynomial f(x) of T is equal to $p(x)^k$, we apply the algorithm above to each $\bar{T}_j:V_j/V_{j-1} \longrightarrow V_j/V_{j-1}$ to obtain the following:

PROPOSITION 2.3. For each $j=1,\ldots,k$, there exists positive integers $m_j,\ldots,m_k$, and for each $m_s>0$,there exists non zero vectors $\alpha_{s,i}$, $s=j,\ldots,k$, $i=1,\ldots,m_s$ such that $V_j/V_{j-1}=\oplus\ Z(p(T)^{s-j}(\bar{\alpha}_{s,i}), \bar{T}_j)$, where the sum is over all $j\le s\le k$ such that $m_s>0$, and $1\le i\le m_s$. In particular , dim $V_j/V_{j-1}=(m_j+\ldots+m_k)\deg p(x)$, and $V_1=\oplus\ Z(p(T)^{s-1}(\alpha_{s,i}), T_1)$, where the sum is over all $1\le s\le k$ such that $m_s>0$, and $1\le i\le m_s$.

Proof. For j=k, it follows from Lemma 2.3 that there exists non zero vectors $\bar{\alpha}_{k,i}$, $i=1,\ldots,m_k$, such that $V/V_{k-1}=Z(\bar{\alpha}_{k,1},\bar{T}_k)\oplus \ldots\oplus Z(\bar{\alpha}_{k,m_k},\bar{T}_k)$. It easy to check that the inclusion map $p(\bar{T}):V/V_{k-1} \longrightarrow V_{k-1}/V_{k-2}$ preserves this direct sum decomposition. That is, the subspaces $Z(p(\bar{T})(\bar{\alpha}_{k,i}), \bar{T}_{k-1})$, $i=1,\ldots,m_k$, are linearly independent in V_{k-1}/V_{k-2}. If $V_{k-1}/V_{k-2}=$

$p(\bar{T})(V/V_{k-1})$,we take $m_{k-1}=0$. Otherwise , by Lemma 2.3 we can find non zero vectors $\bar{\alpha}_{k-1,i}$, $i=1,\ldots,m_{k-1}$, such that $V_{k-1}/V_{k-2} = \overset{\oplus}{1\le i\le m_k} Z(p(\bar{T})(\bar{\alpha}_{k,i}), \bar{T}_{k-1}) \quad \overset{\oplus}{1\le i\le m_{k-1}} Z(\bar{\alpha}_{k-1,i}, \bar{T}_{k-1})$.

Now, we apply the same algorithm to the inclusion $p(\bar{T}_{k-1}):V_{k-1}/V_{k-2} \longrightarrow V_{k-2}/V_{k-3}$ to obtain an integer $m_{k-2}\ge 0$ with the following properties: $m_{k-2}=0$, if $p(\bar{T}_{k-1})$ is an isomorphism. Otherwise there exists non zero vectors $\alpha_{k-2,i}$, $i=1,\ldots,m_{k-2}$, such that

$$V_{k-2}/V_{k-3} = \overset{\oplus}{1\le i\le m_k} Z(p(\bar{T})^2(\bar{\alpha}_{k,i}), \bar{T}_{k-2})$$

$\overset{\oplus}{1\le i\le m_{k-1}} Z(p(\bar{T})(\bar{\alpha}_{k-1,i}), \bar{T}_{k-2}) \quad \overset{\oplus}{1\le i\le m_{k-2}} Z(\bar{\alpha}_{k-2,i}, \bar{T}_{k-2})$. It is clear that by continuing this way we get the claim.

TEOREM B (Existence). There exists positive integers $m_1,\ldots,m_k$ and non zero vectors $\alpha_{j,i}$ for each $m_j>0$,where $j=1,\ldots,k$, $i=1,\ldots,m_j$, such that

$$V=\overset{m_k}{\underset{i=1}{\oplus}} Z(\alpha_{k,i},T) \oplus \ldots\ldots\ldots \overset{m_1}{\underset{i=1}{\oplus}} Z(\alpha_{1,i},T)$$

with $p(x)_{\alpha_{j,i}} = p(x)^j$, when $m_j>0$.

<u>Proof</u>. Let $m_1,\ldots,m_k$ and $\alpha_{j,i}$ be as in Proposition 2.3

corresponding to the space V_1. We first show that the subspaces $Z(\alpha_{j,i},T)$,where $j=1,\ldots,k$, $m_j>0$, and $i=1,\ldots,m_j$, span the space V. Let α be an element of V. It follows from Proposition 2.3, that there exists polynomials f_i such that $\alpha=\sum_{i=1}^{m_k} f_i(T)(\alpha_{k,i}) + \alpha_1$ for some α_1 in V_{k-1}. Similarily we can write α_1 as $\sum_{i=1}^{m_k} g_i(T)p(T)(\alpha_{k,i}) + \sum_{i=1}^{m_{k-1}} h_i(T)(\alpha_{k-1,i}) + \alpha_2$ for some α_2 in V_{k-2}. Thus $\alpha = \sum_{i=1}^{m_k} (f_i+g_ip)(T)(\alpha_{k,i}) + \sum_{i=1}^{m_{k-1}} h_i(T)(\alpha_{k-1,i}) + \alpha_2$. By continuing like this, it is easy to see that α is in the space spanned by the subspaces $Z(\alpha_{j,i},T)$. Now, we show that the subspaces $Z(\alpha_{j,i},T)$ are linearly independent in V. For each $j=1,\ldots,k$ such that $m_j>0$, let $W_j=\sum_{i=1}^{m_j} Z(\alpha_{j,i}, T)$. We claim that $W_j=\oplus_{i=1}^{m_j} Z(\alpha_{j,i}, T)$ in V_j. To see this, let $\beta = \Sigma\ \beta_i=0$,where β_i is in $Z(\alpha_{j,i},T)$. Then $\Sigma\ \bar{\beta}_i=0$ in V_j/V_{j-1}. Thus by Lemma 2.3 we get $\bar{\beta}_i=0$ for each i. This implies that $\beta_i=f_{i,1}(T)p(T)(\alpha_{j,i})$ for some polynomial $f_{i,1}(x)$. Therefore $\Sigma\ \bar{\beta}_i= \Sigma\ f_{i,1}(\bar{T})p(\bar{T})(\bar{\alpha}_{j,i})=0$ in V_{j-1}/V_{j-2}. Thus $f_{i,1}=f_{i,2}p$ for some polynomial $f_{i,2}$. This gives $\beta_i=f_{i,2}(T)p^2(T)(\alpha_{j,i})$, which is in V_{j-2}, and $\Sigma\ \bar{\beta}_i =0$ in

V_{j-2}/V_{j-3}. Continuing in this way, we get $\beta_i = f_{i,j-1}(T)p(T)^{j-1}(\alpha_{j,i})$ for some polynomial $f_{i,j-1}$. This implies β_i is in V_1 for each $i=1,\ldots,m_j$, and $\Sigma\ \beta_i=0$ in V_1. It follows from Proposition 2.3 that each $\beta_i=0$. This proves the claim. To prove the subspaces $Z(\alpha_{j,i},T)$, where $j=1,\ldots,k$, $m_j>0$, and $i=1,\ldots,m_j$, are linearly independent in V , it is enough to show whenever $\Sigma\ w_j=0$, $w_j \epsilon W_j$, then each $w_j=0$. In what follows, to avoid a possible confusion , we take $w_j=0$ if $m_j=0$. Let $\Sigma\ w_j=0$. and let $w_j=\Sigma\ f_{j,i;0}(T)(\alpha_{j,i})$, $j=1,\ldots,k$. Since $\Sigma\ \bar{w}_j=0$ in V/V_{k-1}, we get $\bar{w}_k=0$ in V/V_{k-1}. This implies that we can write w_k in the form $\Sigma\ f_{k,i;1}(T)\ p(T)(\alpha_{k,i})$, where $f_{k,i;0}= f_{k,i;1}p$ for some polynomial $f_{k,i;1}$. This gives us that w_k is in V_{k-1}, and therefore $w_k+w_{k-1}= -(w_{k-2}+\ldots+w_1)$ is in V_{k-2}. This implies that $\Sigma\ f_{k,i;1}(T)\ p(T)(\alpha_{k,i}) + \Sigma\ f_{k-1,i;0}(T)(\alpha_{k-1,i}) =0$ in V_{k-1}/V_{k-2}. From Proposition 2.3, we obtain $f_{k,i;1}= f_{k,i;2}\ p$, and $f_{k-1,i;0}= f_{k-1,i;1}\ p$, for some polynomials $f_{k,i;2}$ and $f_{k-1,i;1}$. Thus $w_k= \sum_{i=1}^{m_k} f_{k,i;2}(T)\ p(T)^2(\alpha_{k,i})$, $w_{k-1}= \sum_{i=1}^{m_{k-1}} f_{k-1,i;1}(T)\ p(T)(\alpha_{k-1,i})$. It is clear continuing this

way we obtain polynomials $f_{s,i;s-1}$, $s=1,\ldots,k$, $i=1,\ldots,m_s$, such that $w_s = \sum_{i=1}^{m_s} f_{s,i;s-1}(T)\ p(T)^{s-1}(\alpha_{s,i})$. This implies that each w_s is in V_1, and $w_k+\ldots.+w_1=0$. It follows from Proposition 2.3 that each $w_s=0$. This completes the proof of the Theorem.

Proof of the Uniqueness.

Let $V= \oplus_{i=1}^{r} Z(\alpha_i,T)$ be a cyclic decomposition of (T,V), with $p_{\alpha_i} = p(x)^{k_i}$, and $k_1\geq\ldots..\geq k_r$.

PROPOSITION 2.4. For each $j=1,\ldots,k$,

$V_j = \oplus_{k_i\geq j} Z(p(T)^{k_i-j}(\alpha_i),\ T_j)\ \oplus_{k_m<j} Z(\alpha_m,\ T_j)$ is a cyclic decomposition of (V_j,T_j).

Proof. It is enough to show that any element α of V_j is in the form $\sum_{k_i\geq j} f_i(T)\ p(T)^{k_i-j}(\alpha_i) + \sum_{k_m<j} g_m(T)(\alpha_m)$ for some polynomials f_i and g_m. From the direct sum decomposition of V , we can write α in the form $\sum_{i=1}^{r} h_i(T)(\alpha_i)$ for some polynomial $h_i(x)$. Since $p(T)^j(\alpha)=0$ and the sum is direct , we get $h_i(T)\ p(T)^j(\alpha_i)=0$ for each i such that $k_i\geq j$. This gives us

$h_i = q_i\ p^{k_i-j}$ when $k_i \geq j$, because $p_{\alpha_i} = p^{k_i}$. Thus $\alpha =$

$\sum_{k_i \geq j} q_i(T)\ p(T)^{k_i-j}(\alpha_i) + \sum_{k_m < j} h_m(T)(\alpha_m)$, which finishes

the proof.

COROLLARY 1. For each $j=1,\ldots k$,

$$V_j/V_{j-1} = \oplus_{k_i \geq j} Z(p(\bar{T}_i)^{k_i-j}(\bar{\alpha}_i),\ \bar{T}_j).$$

For $j=1,\ldots,k$, let $m_j = \#\ \{i \in (1,\ldots,r) : k_i=j\}$. The following

gives the uniqueness of the number r and the polynomials $p(x)^{k_i}$.

COROLLARY 2. For each $j=1,\ldots,k$, $\dim V_j/V_{j-1} = (m_j+\ldots.+m_k)\deg p(x)$.

In particular , $r= m_1+\ldots.+m_k$, and

$k_1 \geq \ldots\ldots \geq k_r$ is dual to the partition $n_1 \geq \ldots\ldots \geq n_k$ of

$\dim(V)/\deg p(x)$, where $n_i = m_i+\ldots.+m_k$, for $i=1,\ldots,k$.

REFERENCES

1. K.Hoffman and R.Kunze,Linear Algebra ,second edition,

Prentice-Hall,Inc.Englewood Cliffs,New Jersey,1971.