Primary and Cyclic Decomposition Theorems – Part II (Proof)

Alexander "Olin" Slávik

MFF UK

April 14, 2013 / Spring School of Algebra

Table of Contents

Statement of the theorem

Theorem (Cyclic Decomposition Theorem, CDT)

Let T be a linear operator on the finite dimensional vector space V over $\mathbb{F}$. Then there are vectors $v_1, v_2, \ldots, v_r \in V$ with T-annihilators $f_j = f_{v_j}$ so that

1. $V = Z(v_1) \oplus Z(v_2) \oplus \cdots \oplus Z(v_r)$,
2. $f_{j+1} \mid f_j$, $j = 1, 2, \ldots, r-1$,
3. $v_r \neq 0$.

Furthermore, the listed properties uniquely determine r and the T-annihilators.

Table of Contents

Handling the general case

Suppose that the theorem holds when $m_T = p^k$, $k \in \mathbb{N}$, $p \in \mathbb{F}[x]$ irreducible. We want to handle the case when $m_T = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where all the p_is are distinct irreducible.

Recall the Primary decomposition theorem:

Theorem (Primary Decomposition Theorem)

Suppose that minimal polynomial m_T of a linear operator T equals $p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, where $p_1, p_2, \dots, p_s$ are distinct irreducible polynomials. Put $V_i = \operatorname{Ker} p_i(T)^{k_i}$. Then

1. *each V_i is T-invariant,*
2. *for $T_i = T|_{V_i}$ the minimal polynomial m_{T_i} equals $p_i^{k_i}$,*
3. $V = \bigoplus_1^s V_i$.

Decomposition

The subspaces V_i obtained by applying the Primary decomposition theorem are T-invariant, thus CDT may be appplied on each of them independently and for each $i \leq s$ we have

$$V_i = Z(v_{i1}) \oplus Z(v_{i2}) \oplus \cdots \oplus Z(v_{ir_i})$$

for vectors $v_{ij} \in V_i$ and the annihilator f_{ij} of each v_{ij} is $p_i^{k_ij}$, $k_{i1} \geq k_{i2} \geq \cdots \geq k_{ir_i}$.

Note: each V_i is a sum of different number (r_i) of cyclic subspaces, but by adding spaces $Z(0)$ if necessary we may assume that $r_i = r \in \mathbb{N}$.

Composing the space back

Let $v_j = v_{1j} + v_{2j} + \cdots + v_{sj}$ and recall the following Lemma:

Lemma

If $u, v \in V$ have relatively prime T-annihilators f_u, f_v, then $Z(u+v) = Z(u) \oplus Z(v)$ and $f_{u+v} = f_u f_v$.

Hence we have $Z(v_j) = \bigoplus_{i \leq s} Z(v_{ij})$ and $f_{v_j} = \prod_{i \leq s} p_i^{k_{ij}}$.
Finally,

$$V = \bigoplus_{i \leq s} V_i = \bigoplus_{i \leq s} \bigoplus_{j \leq r} Z(v_{ij}) = \bigoplus_{j \leq r} \bigoplus_{i \leq s} Z(v_{ij}) = \bigoplus_{j \leq r} Z(v_j)$$

and $f_{j+1} \mid f_j$.

Table of Contents

Power of irreducible polynomial case

Now the hard part: proof when $m_T = p^k$, p being irreducible. Denote $d = \deg p$.
Observe that we do not have to take care about the condition (2) in CDT.

Strategy

We proceed by induction on $\dim V$. The inductive step consists of the following:

- Firstly, construct a T-invariant subspace $V_1 \subseteq V$ of codimension d containing $\operatorname{Im} p(T)$.
- By the induction hypothesis, V_1 can be decomposed in the CDT-fashion.
- Repair the complement of V_1 so that it fits into the overall decomposition.

Construction of V_1

Denote V^* the dual of V and T^T the transpose of T. As $m_T = m_{T^\mathsf{T}} = p^k$, $p(T^\mathsf{T})$ has to be singular.

Observation

If $0 \neq v^* \in \operatorname{Ker} p(T^\mathsf{T})$, then T^T-annihilator of v^* is p, therefore $\dim Z(v^*) = d$.

We let
$V_1 = Z(v^*)^\perp = \{v \in V \mid w^*(v) = 0 \text{ for all } w^* \in Z(v^*)\}$.

Properties of V_1

Observation

$Z(v^*) \subseteq \operatorname{Ker} p(T^\mathsf{T})$, therefore
$\operatorname{Im} p(T) = (\operatorname{Ker} p(T^\mathsf{T}))^\perp \subseteq Z(v^*)^\perp = V_1$

Observation

$Z(v^*)$ is T^T-invariant, hence V_1 is T-invariant.

Observation

Denote $Y(v) = \langle v, Tv, \ldots, T^{d-1}v \rangle$. Then $Y(v) \cap V_1 = 0$, if $v \notin V_1$.

Proof.

$J = \{f \in \mathbb{F}[x] \mid f(T)v \in V_1\}$ is an ideal containing m_T, therefore its generator is a power of p. Thus if $\deg f < d$, then $f(T)v \in V_1$ only if $f = 0$. □

Properties of V_1 contd.

As dim $Y(v) = d$ for any $v \neq 0$, we have $V = V_1 \oplus Y(v)$.

Applying the induction hypothesis

Put $T_1 = T|_{V_1}$. By the induction hypothesis, there is a decomposition

$$V_1 = \bigoplus_{j \leq r} Z(v_j)$$

with $v_j \in V_1$. Note that by the T-invariance of V_1, $Z(v_j) = Z(v_j, T) = Z(v_j, T_1)$.
We may further assume that p^{k_j} is the T-annihilator of v_j and $k_1 \geq k_2 \geq \cdots \geq k_r$.

Picking suitable v for $Y(v)$

Pick $v \notin V_1$. Since $p(T)v \in \operatorname{Im} p(T) \subseteq V_1$, there are polynomials $f_1, f_2, \ldots, f_r \in \mathbb{F}[x]$ such that

$$p(T)v = \sum_{i \leq r} f_j(T)v_j.$$

If we write $f_j = g_j p + h_j$, $\deg h_j < d$ and let $v' = v - \sum_{j \leq r} g_j(T)v_j$, then $v' \notin V_1$ as well and

$$p(T)v' = \sum_{i \leq r} h_j(T)v_j.$$

Observation

If $p(T)v' = 0$, then $Y(v') = Z(v')$, thus $V = \bigoplus_{j \leq r} Z(v_j) \oplus Z(v')$ and we are done.

What if $p(T)v' \neq 0$?

If $p(T)v' = \sum_{i \leq r} h_j(T)v_j \neq 0$, then there is a smallest $c \leq r$ such that $h_c(T)v_c \neq 0$.

Denote $U = \bigoplus_{j=c+1}^{r} Z(v_j)$ and observe that $p(T)v' \in Z(v_c) \oplus U$.

Further plans

Our goal is to deduce $Z(p(T)v') \oplus U = Z(v_c) \oplus U$; if that were true, then by applying the Lemma 2 we would obtain

$$V = V_1 \oplus Y(v') = \bigoplus_{j \leq c-1} Z(v_j) \oplus U \oplus Z(v_c) \oplus Y(v') =$$

$$= \bigoplus_{j \leq c-1} Z(v_j) \oplus U \oplus Z(p(T)v') \oplus Y(v') = \bigoplus_{j \leq c-1} Z(v_j) \oplus U \oplus Z(v'),$$

which is the desired decomposition.

Lemma for repairing the decomposition

Lemma (2)

Let p be an irreducible factor of f_v of degree d. Then $\{v, Tv, \ldots, T^{d-1}v\}$ is a linearly independent set, and if $Y(v) = \langle v, Tv, \ldots, T^{d-1}v \rangle$, then $Z(v) = Y(v) \oplus Z(p(T)v)$.

The setting in the previous frame is $v = v'$, $f_v =$ some power of p.

Facts about $Z(p(T)v')$

Observation

$Z(p(T)v') \cap U = 0$.

Proof.

If $f(T)p(T)v' \in U$, then $f(T)h_c(T)v_c = 0$, which implies $p^{k_c} \mid f h_c$. As $\deg h_c < d$, we infer $p^{k_c} \mid f$, thus $f(T)v_j = 0$ for $c \geq j \geq r$ and $f(T)p(T)v' = 0$. $\square$

Thus we have a direct sum $Z(p(T)v') \oplus U$.

Facts about $Z(p(T)v')$ contd.

Observation

$Z(p(T)v') \oplus U = Z(h_c(T)v_c) \oplus U.$

Proof.

The T-invariance of $Z(h_j(T)v_j)$ implies $Z(p(T)v') \oplus U \subseteq Z(h_c(T)v_c) \oplus U$ (since $p(T)v' \in Z(h_c(T)v_c) \oplus U$).

On the other hand, $h_c(T)v_c = p(T)v' - \sum_{j=k+1}^{r} h_j(T)v_j \in Z(p(T)v') \oplus U$, and the T-invariance of the subspaces provides the reverse inclusion. $\square$

Final step

Observation

$Z(h_c(T)v_c) = Z(v_c)$.

Proof.

Clearly $Z(h_c(T)v_c) \subseteq Z(v_c)$. If f is the T-annihilator of $h_c(T)v_c$, then $p^{k_c} \mid f h_c$. As (again) $\deg h_c < d$, we have $p^{k_c} \mid f$, thus

$$\dim Z(h_c(T)v_c) = \deg f \geq \deg p^{k_c} = \dim Z(v_c),$$

from which we infer the equality of the two spaces. □

To sum up, we have
$Z(p(T)v') \oplus U = Z(h_c(T)v_c) \oplus U = Z(v_c) \oplus U$ as desired.

Table of Contents

Uniqueness

Suppose that there are two sets of vectors, $v_1, v_2, \ldots, v_r$, $w_1, w_2, \ldots, w_s$, with T-annihilators $f_1, f_2, \ldots, f_r$, $g_1, g_2, \ldots, g_s$ respectively.

Firstly note that $f_1 = g_1 = m_T$. To see how the induction proceeds, observe that from the two decompositions of V we obtain two decompositions of $\operatorname{Im} f_2(T)$:

$$\operatorname{Im} f_2(T) = Z(f_2(T)v_1) \quad (f_2 \mid f_i \text{ for } i \geq 2),$$
$$\operatorname{Im} f_2(T) = Z(f_2(T)w_1) \oplus Z(f_2(T)w_2) \oplus \cdots \oplus Z(f_2(T)w_s).$$

As v_1 and w_1 share the same T-annihilator, $Z(f_2(T)v_1) = Z(f_2(T)w_1)$, thus $Z(f_2(T)w_i) = 0$ for $i \geq 2$. We conclude that $f_2(T)w_2 = 0$ and $g_2 \mid f_2$. By reversing, $g_2 = f_2$.