Cyclic Primary Decomposition for Vector Spaces

Ang Yan Sheng

In this note, we prove the cyclic primary decomposition theorem for a linear operator α on a finite-dimensional vector space V, for the case where $m_\alpha(x) = f(x)^k$ for some irreducible $f(x) \in F[x]$ and $k \in \mathbb{Z}^+$.

Lemma 1. *If $V/U = \sum_i \operatorname{span}(b_i + U)$, then $V = U + \sum_i \operatorname{span}(b_i)$.*

Proof. For any $v \in V$, let $v + U = \sum_i \lambda_i(b_i + U)$. Then $v - \sum_i \lambda_i b_i \in U$. $\square$

Lemma 2. *If $\sum_i \langle f(\alpha)(v_i')\rangle_\alpha$ is direct, and none of the summands are $\{0\}$, then $\sum_i \langle v_i'\rangle_\alpha$ is also direct.*

Proof. If we choose $u_i \in \langle v_i'\rangle_\alpha$ such that $\sum_i u_i = 0$, then $f(\alpha)(u_i) \in \langle f(\alpha)(v_i')\rangle_\alpha$ and $\sum_i f(\alpha)(u_i) = f(\alpha)(0) = 0$ implies $f(\alpha)(u_i) = 0$ for all i.

Now $u_i \in \langle v_i'\rangle_\alpha$ implies $u_i = P_i(\alpha)(v_i')$ for some polynomials P_i, and therefore $f(x)^2 \mid m_{\alpha,v_i'}(x) \mid f(x)P_i(x)$. Hence $f(x) \mid P_i(x)$, so $u_i \in \langle f(\alpha)(v_i')\rangle_\alpha$, and $\sum_i u_i = 0$ implies $u_i = 0$ for all i, as desired. $\square$

Lemma 3. *Let $U = \ker f(\alpha)$. If Z is an α-invariant subspace of U, then there exists v_i such that $U = Z \oplus \bigoplus_i \langle v_i\rangle_\alpha$.*

Proof. Induction on $\dim U - \dim Z$. If $\dim U = \dim Z$ then there is nothing to prove. If not, choose any $v_1 \in U \backslash Z$. If $P(\alpha)(v_1) = z \in Z$ for some polynomial P coprime with f, then choose polynomials A, B such that $AP + Bf = 1$, so that

$$v_1 = A(\alpha)P(\alpha)(v_1) + B(\alpha)f(\alpha)(v_1) = A(\alpha)(z) \in Z,$$

contradiction. Hence $\langle v_1\rangle_\alpha \cap Z = \{0\}$, so induction hypothesis on $Z \oplus \langle v_1\rangle_\alpha$ gives some $v_2, \ldots, v_m$ such that $U = (Z \oplus \langle v_1\rangle_\alpha) \bigoplus_{i>1} \langle v_i\rangle_\alpha = Z \oplus \bigoplus_i \langle v_i\rangle_\alpha$, as desired. $\square$

Lemma 4. *If $V = U + W$ and $U = (U \cap W) \oplus X$ then $V = W \oplus X$.*

Proof. Clearly $V = W + (U \cap W) + X = W + X$, so the statement follows from

$$\begin{aligned} \dim W + \dim X &= \dim W + \dim U - \dim(U \cap W) \\ &= \dim W + \dim U - (\dim U + \dim W - \dim V) = \dim V. \end{aligned}$$ $\square$

Theorem. *There exists $v_1, \ldots, v_s \in V \backslash \{0\}$ such that $V = \bigoplus_{i=1}^s \langle v_i\rangle_\alpha$. Furthermore, for any such decomposition, the multiset $\{m_{\alpha,v_i}(x)\}$ is uniquely determined.*

Proof. Induction on k. For $k = 1$, existence follows from Lemma 3 with $Z = \{0\}$. Now $m_{\alpha,v_i}(x) = f(x)$ for all i, and $\dim\langle v_i\rangle_\alpha = \deg f$, so the number of v_i is $\frac{\dim V}{\deg f}$ for any decomposition, and we are done.

If $k > 1$, let $U = \ker f(\alpha)$. By the first isomorphism theorem we have $V/U \cong \operatorname{Im} f(\alpha)$. Note that $m_{\alpha|_{\operatorname{Im} f(\alpha)}}(x) = f(x)^{k-1}$, so by induction hypothesis we may write $\operatorname{Im} f(\alpha) = \bigoplus_i \langle f(\alpha)(v_i')\rangle$.

Now the natural isomorphism $\phi : \operatorname{Im} f(\alpha) \to V/U$ maps $f(\alpha)(v)$ to $v + U$, so it maps $\alpha^j f(\alpha)(v_i')$ to $\alpha^j v_i' + U$. If we let $\deg m_{\alpha, f(\alpha)(v_i')} = d_i$, then

$$\begin{aligned} \operatorname{Im} f(\alpha) &= \sum_i \langle f(\alpha)(v_i') \rangle_\alpha \\ &= \sum_i \sum_{j=0}^{d_i - 1} \operatorname{span}(\alpha^j f(\alpha)(v_i')) \\ \implies V/U &= \sum_i \sum_{j=0}^{d_i - 1} \operatorname{span}(\alpha^j v_i' + U) \\ \implies V &= U + \sum_i \sum_{j=0}^{d_i - 1} \operatorname{span}(\alpha^j v_i') \quad \text{(Lemma 1)} \\ &\subseteq U + \sum_i \langle v_i' \rangle_\alpha \\ \implies V &= U + \bigoplus_i \langle v_i' \rangle_\alpha. \quad \text{(Lemma 2)} \end{aligned}$$

Now Lemma 3 with $X = U \cap \bigoplus_i \langle v_i' \rangle_\alpha$ gives some v_i'' such that

$$U = \left(U \cap \bigoplus_i \langle v_i' \rangle_\alpha \right) \oplus \bigoplus_i \langle v_i'' \rangle_\alpha,$$

so by Lemma 4 we have $V = \bigoplus_i \langle v_i' \rangle_\alpha \oplus \bigoplus_i \langle v_i'' \rangle_\alpha$, as desired.

Now we look at $f(\alpha)$ restricted to a subspace of the form $\langle v \rangle_\alpha$. If $m_{\alpha,v} = f(x)^e$, then by Lemma 4.49, $\langle v \rangle_\alpha \cap \ker(f(\alpha)^j)$ has the basis $\bigcup_{i=e-j}^{e-1} \{f(\alpha)^i(v)\}_\alpha^{\deg f}$ for $1 \leq j \leq e$. In particular,

$$\dim \left(\langle v \rangle_\alpha \cap \ker(f(\alpha)^j) \right) = \min(j, e) \deg f.$$

Thus if $V = \bigoplus_i \langle v_i \rangle_\alpha$ with $m_{\alpha, v_i} = f(x)^{e_i}$, then

$$\begin{aligned} \frac{\dim(\ker(f(\alpha)^{j+1}) - \dim(\ker(f(\alpha)^j))}{\deg f} &= \sum_i \left(\min(j+1, e_i) - \min(j, e_i) \right) \\ &= \sum_i \mathbb{1}_{e_i > j} \\ &= \sum_{e > j} \#\{i \,|\, e_i = e\}, \end{aligned}$$

from which we have

$$\#\{i \,|\, e_i = j\} = \frac{\operatorname{null}(f(\alpha)^j) - \operatorname{null}(f(\alpha)^{j-1})}{\deg f} - \frac{\operatorname{null}(f(\alpha)^{j+1}) - \operatorname{null}(f(\alpha)^j)}{\deg f}.$$

Since the RHS is independent of the decomposition, so is the LHS, and thus so is the multiset $\{m_{\alpha, v_i}(x)\}$. $\square$