$T: V \to V$ linear transformation

Def: A subspace W of V is called a T-invariant subspace if $T(W) \subseteq W$. i.e. $T(v) \in W$ for any $v \in W$.

Examples: $\{0\}$, V, $N(T)$.

$R(T)$: $T(R(T)) \subseteq R(T)$.

$E_\lambda = N(T-\lambda I)$: $v \in N(T-\lambda I) \Leftrightarrow Tv = \underset{\overset{\cap}{W}}{\lambda \cdot v} \Rightarrow Tv \in W$.

Def: Fix any $v \in V$. The T-cyclic ^sub^space generated by v is the subspace $\mathrm{Span}\{v, Tv, T^2v, \cdots\} = \mathrm{Span}\{T^k v;\ k=1,2,\cdots\}$

Thm: If $W = \mathrm{Span}\{v, Tv, T^2v, \cdots\}$ has dim m, then $\{v, Tv, \cdots, T^{m-1}v\}$ is a basis for W.

Proof: It suffices to prove the following statement:

Let m be the largest integer such that $\beta = \{v, Tv, \cdots, T^{m-1}v\}$ is linearly independent. Then β is a basis for W.

Proof: We only need to show β spans W.

Actually it is enough to show that $T^m v$ is a linear combination of β because we can then iteratively write $T^k v$ as a linear combination of β

for any $k \geq m$: $T^k m = T^{k-m} \cdot (T^m v) = \cdots$.

For $k = m$, because the subset $\{v, Tv, T^2v, \cdots, T^{m-1}v, T^m v\}$ is linearly dependent by the definition of m, we know that there is a nontrivial linear relation:

$$a_0 v + a_1 \cdot Tv + a_2 \cdot T^2 v + \cdots + a_{m-1} \cdot T^{m-1} v + a_m \cdot T^m v = 0$$

where not $\{a_i, i=0, \cdots, m\}$ are not all zero.

We must have $a_m \neq 0$ since $\{v, Tv, \cdots, T^{m-1}v\}$ is linearly independent.

So $T^m v = -a_m^{-1} \cdot a_0 \cdot v - a_m^{-1} \cdot a_1 \cdot Tv - \cdots - a_m^{-1} \cdot a_{m-1} \cdot T^{m-1} v$

as wanted ∎