Notes on the Cyclic Decomposition Theorem

We have been studying a general linear operator $T\colon V \to V$ on a finite dimensional vector space. We showed using the Primary Decomposition Theorem (page 220) that V is a direct sum of invariant subspaces W_i so that the restriction T_{W_i} of T to each W_i has minimal polynomial $(x-c_i)^{e_i}$ for some characteristic value c_i of T. Thus we have reduced to the case where $T\colon V \to V$ has minimal polynomial $(x-c)^e$. Letting $N = T - cI$ we note that the minimal polynomial of N is then x^e and hence N is what is called nilpotent. We will study such a nilpotent N, and then infer properties of T by setting $T = N + cI$.

So from now on in these notes we will suppose that $N\colon V \to V$ is an operator with minimal polynomial x^e and V is finite dimensional. This is a special case of the general operator studied in 7.1 and 7.2 of the book, but it is all we need to obtain the Jordan form in 7.3. In these notes I will also illustrate general statements with their meanings for a particular example, $N = \begin{bmatrix} 0&0&0&0&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&1&0 \end{bmatrix}$.

For any $\alpha \in V$, I will say the depth of α is the smallest d so that $N^d\alpha = 0$. Thus only $\alpha = 0$ has depth 0, nonzero vectors in $\mathrm{NS}(N)$ have depth 1, vectors in $\mathrm{NS}(N^2) - \mathrm{NS}(N)$ have depth 2 and so on. Since $N^e = 0$ we know the depth is always $\leq e$. Using the book's terminology, α has depth d if and only if the N-annihilator of α is x^d (page 228). In particular, if $g(N)\alpha = 0$ for some polynomial g we know that g is divisible by x^d. In our example, ε_1 has depth 3 since $N\varepsilon_1 = \varepsilon_2 \neq 0$, $N^2\varepsilon_1 = \varepsilon_3 \neq 0$, and $N^3\varepsilon_1 = 0$.

We let $Z(\alpha; N)$ denote the subspace of all vectors of the form $g(N)\alpha$ for $g \in \mathbb{F}[x]$ a polynomial. Since $N^d\alpha = 0$ for d the depth of α we know that $g(N)\alpha = h(N)\alpha$ where h is the sum of the terms of g of degree less than d. Hence $Z(\alpha; N)$ is the subspace spanned by $\alpha, N\alpha, N^2\alpha, \ldots, N^{d-1}\alpha$. But I claim that $\{\alpha, N\alpha, N^2\alpha, \ldots, N^{d-1}\alpha\}$ is linearly independent. To see this, set $c_0\alpha + c_1N\alpha + c_2N^2\alpha + \cdots + c_{d-1}N^{d-1}\alpha = 0$. Then $g(N)\alpha = 0$ where $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{d-1}x^{d-1}$. But $g(N)\alpha = 0$ implies g must be divisible by x^d so in fact $g = 0$ and thus all $c_i = 0$.

So $\{\alpha, N\alpha, N^2\alpha, \ldots, N^{d-1}\alpha\}$ is a basis of $Z(\alpha; N)$. (this is all a special case of Thm 1, page 228). In our example, suppose $\alpha = [1\ 2\ 3\ 4\ 5]^T$. Then $N\alpha = [0\ 1\ 2\ 0\ 4]^T$, $N^2\alpha = [0\ 0\ 1\ 0\ 0]^T$ so $Z(\alpha; N)$ is the span of $\alpha, [0\ 1\ 2\ 0\ 4]^T, \varepsilon_3$. By Gaussian elimination, we know a vector $[a_1\ a_2\ a_3\ a_4\ a_5]^T$ is in $Z(\alpha; N)$ if and only if $a_4 = 4a_1$ and $a_5 = -3a_1 + 4a_2$.

Following the book, we say a subspace $W \subset V$ is N-admissible if W is invariant under N and whenever $f \in \mathbb{F}[x]$ is a polynomial and $\beta \in V$ are chosen so that $f(N)\beta \in W$, there is a vector $\gamma \in W$ so that $f(N)\beta = f(N)\gamma$. Recall (page 201) that $S_N(\beta; W)$ is the set of all polynomials f so that $f(N)\beta \in W$. So we may rephrase the definition of N-admissible by saying that W is invariant under N and for all $\beta \in V$ and all $f \in S_N(\beta; W)$, there is a $\gamma \in W$ so that $f(N)\beta = f(N)\gamma$. Since the minimal polynomial x^e is in $S_N(\beta; W)$ we know that the generator of the ideal $S_N(\beta; W)$ must be x^b for some $b \leq e$. It then suffices to show that there is a $\gamma \in W$ so that $N^b\beta = N^b\gamma$, for if $f(N)\beta \in W$ we must have $f(x) = g(x)x^b$ for some polynomial g and then $f(N)\beta = g(N)N^b\beta = g(N)N^b\gamma = f(N)\gamma$. Let us call b the W-depth of β. So the W-depth of β is the smallest b so that $N^b\beta \in W$.

So, we may finally rephrase the definition of N-admissible as follows. We say a subspace $W \subset V$ is N-admissible if W is invariant under N and for each $\beta \in V$ there is a $\gamma \in W$ so that $N^b\beta = N^b\gamma$ where b is the W-depth of β.

Let us see whether or not $W = Z([1\ 2\ 3\ 4\ 5]^T; N)$ is N-admissible. It is certainly invariant, since N of any basis vector is either 0 or another basis vector. Now take any $\beta = [b_1\ b_2\ b_3\ b_4\ b_5]^T$.

- If the W-depth of β is 0 then $\beta = N^0\beta \in W$. We can take $\gamma = \beta$ since $N^0\beta = \beta = \gamma = N^0\gamma$.
- If the W-depth of β is 1 then $N\beta \in W$. We have $N\beta = [0\ b_1\ b_2\ 0\ b_4]^T$ so $N\beta \in W$ if and only if $b_4 = 4b_1$. We may let $\gamma = b_1[1\ 2\ 3\ 4\ 5]^T + (b_2 - 2b_1)[0\ 1\ 2\ 0\ 4]^T$, then $\gamma \in W$ and $N\beta = N\gamma$.

- Suppose the W-depth of β is greater than 1. Since $N^2\beta = [0\ 0\ b_1\ 0\ 0] \in W$, the W-depth of β must then be 2. Let $\gamma = b_1[1\ 2\ 3\ 4\ 5]^T$ then $\gamma \in W$ and $N^2\beta = N^2\gamma$.

So we see that W is N-admissible.

For a nonadmissible example, let W be the span of ε_3. Then W is invariant under N since $N\varepsilon_3 = 0$, but if $\beta = \varepsilon_2$ we have $N\beta = \varepsilon_3 \in W$ but there is no $\gamma \in W$ so that $N\beta = N\gamma$, since $N\gamma = 0$ for all $\gamma \in W$.

Now instead of proving the Cyclic Decomposition Theorem all at once as is done in the text, we do just one step and deduce the theorem by performing that one step as often as needed. This is the idea alluded to at the bottom of page 232 of the text.

Here is the crucial step. Suppose W is an N-admissible subspace and $W \neq V$. Then there is an $\alpha \in V$ so that:

a) W and $Z(\alpha; N)$ are independent.

b) $W \oplus Z(\alpha; N)$ is N-admissible.

To get the Cyclic Decomposition Theorem (or rather, our special case of it), we apply the above step many times. In particular, we start out by setting $W_0 = 0$ and then perform the step, finding an $\alpha_1 \in V$ so that $W_1 = Z(\alpha_1; N)$ is N-admissible. If $W_1 \neq V$, we perform the step again, finding an $\alpha_2 \in V$ so that W_1 and $Z(\alpha_2; N)$ are independent and $W_2 = W_1 \oplus Z(\alpha_2; N)$ is N-admissible. If $W_2 \neq V$, we perform the step again, finding an $\alpha_3 \in V$ so that W_2 and $Z(\alpha_3; N)$ are independent and $W_3 = W_2 \oplus Z(\alpha_3; N)$ is N-admissible. And so on. At the end, we have found $\alpha_1, \ldots, \alpha_k$ so that $Z(\alpha_1; N), Z(\alpha_2; N), \ldots, Z(\alpha_k; N)$ are independent and $V = W_k = Z(\alpha_1; N) \oplus Z(\alpha_2; N) \oplus \cdots \oplus Z(\alpha_k; N)$.

So it remains to prove the crucial step given above. So suppose W is an N-admissible subspace and $W \neq V$. Choose a $\beta \in V$ so that the W-depth of β is as large as possible. Call this W-depth b. Since W is N-admissible, there is a $\gamma \in W$ so that $N^b\beta = N^b\gamma$. Let $\alpha = \beta - \gamma$. Note that $N^b\alpha = 0 \in W$. If $N^i\alpha \in W$ for some i then $N^i\beta = N^i\alpha + N^i\gamma \in W + W = W$ so $i \geq b$. Thus the depth of α is b and the W-depth of α is also b. We must show W and $Z(\alpha; N)$ are independent, in other words $W \cap Z(\alpha; N) = \{0\}$. Suppose $\alpha' \in W \cap Z(\alpha; N)$ then $\alpha' \in W$ and $\alpha' = g(N)\alpha$ for some polynomial g. Then $g \in S_N(\alpha; W)$ and since $S_N(\alpha; W)$ is generated by x^b we must have $g(x) = f(x)x^b$ for some polynomial f. But then $\alpha' = g(N)\alpha = f(N)N^b\alpha = f(N)0 = 0$, so we have $W \cap Z(\alpha; N) = \{0\}$.

Now let us show that $W \oplus Z(\alpha; N)$ is N-admissible. First of all, $W \oplus Z(\alpha; N)$ is invariant under N since both W and $Z(\alpha; N)$ are invariant. Pick any $\delta \in V$ and let d be the $W \oplus Z(\alpha; N)$-depth of δ. So $N^d\delta = \delta_1 + f(N)\alpha$ where $\delta_1 \in W$ and $f \in \mathbb{F}[x]$. Since b was the largest possible W-depth we know $N^b\delta \in W$. But $N^b\delta = N^{b-d}N^d\delta = N^{b-d}\delta_1 + N^{b-d}f(N)\alpha$ so we have $N^{b-d}f(N)\alpha = N^b\delta - N^{b-d}\delta_1 \in W$. Since W and $Z(\alpha; N)$ are independent we must have $N^{b-d}f(N)\alpha = 0$, so $x^{b-d}f(x) \in S_N(\alpha; 0)$. But $S_N(\alpha; 0)$ is generated by x^b since the depth of α is b. So $x^{b-d}f(x)$ is divisible by x^b which means $f(x) = x^d g(x)$ for some polynomial g. Thus $f(N)\alpha = N^d g(N)\alpha$. Let $\delta' = \delta - g(N)\alpha$, then $N^d\delta' = N^d\delta - N^d g(N)\alpha = N^d\delta - f(N)\alpha = \delta_1 \in W$. So there is a $\gamma' \in W$ so that $N^d\gamma' = \delta_1$. Then $\gamma' + g(N)\alpha \in W \oplus Z(\alpha; N)$ and $N^d\delta = N^d(\gamma' + g(N)\alpha)$ so $W \oplus Z(\alpha; N)$ is N-admissible.

Let us do all thus for our example. We start out with $W_0 = 0$ and choose β_1 with maximal depth, for example $\beta_1 = [1\ 2\ 3\ 4\ 5]^T$ which has depth 3. Since $W_0 = 0$ we need no γ correction so we just let $\alpha_1 = \beta_1$ and W_1 is the span of $\alpha, N\alpha, N^2\alpha$ which we looked at above. Now we choose β_2 with maximal W_1 depth which we saw above is 2. We also saw above that we can take any $\beta_2 = [b_1\ b_2\ b_3\ b_4\ b_5]^T$ as long as $b_4 \neq 4b_1$. So what the heck, take $\beta_2 = [1\ 1\ 1\ 1\ 1]^T$. We saw above that $N^2\beta_2 = N^2[1\ 2\ 3\ 4\ 5]^T$ and $[1\ 2\ 3\ 4\ 5]^T \in W_1$. We now let $\alpha_2 = [1\ 1\ 1\ 1\ 1]^T - [1\ 2\ 3\ 4\ 5]^T = [0\ -1\ -2\ -3\ -4]^T$. At this point $\mathbb{F}^{5\times 1} = Z(\alpha_1; N) \oplus Z(\alpha_2; N)$ and we are done. Note that we have found a basis of $\mathbb{F}^{5\times 1}$, namely $\alpha_1, N\alpha_1, N^2\alpha_1, \alpha_2, N\alpha_2$. You can verify that the matrix of N with respect to this basis is N itself.

I deliberately chose odd looking vectors for β_1 and β_2. A nicer choice would be $\beta_1 = \varepsilon_1$ and $\beta_2 = \varepsilon_4$. Then $\alpha_i = \beta_i$.