The Rational and Jordan Forms
Linear Algebra Notes

Satya Mandal

November 5, 2005

1 Cyclic Subspaces

In a given context, a "cyclic thing" is an one generated "thing". For example, a cyclic groups is a one generated group. Likewise, a module M over a ring R is said to be a cyclic module if M is one generated or $M = Rm$ for some $m \in M$. We do not use the expression "cyclic vector spaces" because one generated vector spaces are zero or one dimensional vector spaces.

1.1 (Definition and Facts) Suppose V is a vector space over a field $\mathbb{F}$, with finite $\dim V = n$. Fix a linear operator $T \in L(V, V)$.

1. Write
$$R = \mathbb{F}[T] = \{f(T) : f(X) \in \mathbb{F}[X]\} \subseteq L(V, V)\}.$$
Then $R = \mathbb{F}[T]\}$ is a commutative ring. (*We did considered this ring in last chapter in the proof of Caley-Hamilton Theorem.*)

2. Now V acquires $R-$module structure with scalar multiplication as follows:
$$Define \quad f(T)v = f(T)(v) \in V \quad \forall \quad f(T) \in \mathbb{F}[T], \quad v \in V.$$

3. For an element $v \in V$ define
$$Z(v, T) = \mathbb{F}[T]v = \{f(T)v : f(T) \in R\}.$$

Note that $Z(v,T)$ is the cyclic $R-$submodule generated by v. (*I like the notation* $\mathbb{F}[T]v$, *the textbook uses the notation* $Z(v,T)$.) We say, $Z(v,T)$ is the $T-$**cyclic subspace generated by** v.

4. If $V = Z(v,T) = \mathbb{F}[T]v$, we say that that V is a $T-$**cyclic space,** and v is called the $T-$**cyclic generator** of V. (*Here, I differ a little from the textbook.*)

5. Obviosly, $Z(v,T)$ is also a vector subspace over $\mathbb{F}$. In fact,
$$Z(v,T) = Span(\{v, T(v), T^2(v), T^3(v), \ldots\}).$$
Since $\dim(Z(v,T)) \leq (\dim V) = n$, is finite, a finite subset of $\{v, T(v), T^2(v), T^3(v), \ldots\}$ will from a basis of $Z(v,T)$.

6. Also for $v \in V$, define
$$ann(v) = \{f(X) \in \mathbb{F}[X] : f(T)v = 0\}.$$
So, $ann(v)$ is an ideal of the polynomial ring $\mathbb{F}[X]$ and is called $T-$**annihilator of** v.

7. Note that, if $v \neq 0$, then $ann(v) \neq \mathbb{F}[X]$. So, there polynomial p_v such that
$$ann(v) = \mathbb{F}[X]p_v.$$
As we know, p_v is the non-constant monic polynomial polynomial in $ann(v)$. This polynomial p_v is called the minimal momic polynomial (MMP) of $ann(v)$.

8. In the next theorem 1.2, we will give a baisis of $Z(v,T)$.

1.2 (Theorem) Suppose V is a vector space over a field $\mathbb{F}$, with finite $\dim V = n$. Fix a linear operator $T \in L(V,V)$. Let $v \in V$ be a non-zero element and p_v is the mimimal momic polynomial (MMP) of $ann(v)$.

1. If $k = degree(p_v)$ then $\{v, T(v), T^2(v), \ldots, T^{k-1}(v)\}$ is a basis of $(Z(v,T))$.

2. $degree(p_v) = \dim(Z(v,T))$.

3. Note that $Z(v,T)$ is invariant under T. Also, if $U = T_{|(Z(v,T)}$ is the restriction of T to $Z(v,T)$ then the MMP of T is p_v.

4. Write
$$p_v(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1} + X^k$$
where $c_i \in \mathbb{F}$. Also write $e_0 = v, e_1 = T(v), e_2 = T^2(v), \ldots, e_{k-1} = T^{k-1}(v)$.

$$(T(e_0), T(e_1), T(e_2) \ldots, T(e_{k-1})) =$$
$$(e_0, e_1, e_2, \ldots, e_{k-1}) \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -c_{k-1} \end{pmatrix}.$$
This gives the matrix of $U = T_{|(Z(v,T)}$ with respect to the basis $e_0, e_1, e_2, \ldots, e_{k-1}$ of $Z(v, T)$.

Proof. First, we prove (1). Recall $Z(v, T) = \mathbb{F}[T]v$. Let $x \in Z(v, T)$. Then $x = f(T)v$ for some polynomial $f(X)$. Using devison algorithm, we have
$$f(X) = q(X)p_v(X) + r(X),$$
where $q, r \in \mathbb{F}[X]$ and either $r = 0$ or $degree(r) < k = degree(p_v)$. So,
$$x = f(T)v = q(T)p_v(T)v + r(T)v = r(T)v.$$

Therefore
$$Z(v, T) = Span(\{v, T(v), \ldots, T^{k-1}(v)\}).$$
Now, suppose $a_0v + a_1T(v) + \cdots + a_{k-1}T^{k-1}(v) = 0$ for some $a_i \in \mathbb{F}$. Then $f(X) = a_0 + a_1X + \cdots + a_{k-1}X^{k-1} \in ann(v)$. By minimality of p_v, we have $f(X) = 0$ and hence $a_i = 0$ for all $i = 0, \ldots, k-1$. Therefore $v, T(v), \ldots, T^{k-1}(v)$ are linearly independent and hence a basis of $Z(v, T)$. This establishes (1).

Now, (2) follows from (1).

Now, we will prove (3). Clearly, $T(Z(v, T)) = T(\mathbb{F}[T]v) \subseteq \mathbb{F}[T]v = Z(v, T)$. Therefore, $Z(v, T)$ is invariant under T. To prove that p_v is the MMP of U, we prove that $\mathbb{F}[X]p_v = ann(v) = ann(U)$. In fact, for any polynomial g we have $g(X) \in ann(v) \Leftrightarrow g(T)v = 0 \Leftrightarrow g(U)v = 0 \Leftrightarrow g(U) = 0 \Leftrightarrow g \in ann(U)$. This completes the proof of (3).

The proof of the (4) is obvious.

1.3 (Definition) Given a polynomial

$$p(X) = c_0 + c_1X + \cdots + c_{k-1}X^{k-1} + X^k \in \mathbb{F}[X]$$

with $c_i \in \mathbb{F}$. The matrix

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -c_{k-1} \end{pmatrix}.$$

is called the **companion matrix** of p.

1.4 (Theorem) Suppose W is a vector space over a field $\mathbb{F}$, with finite $\dim W = n$. Fix a linear operator $T \in L(W, W)$.

Then W is $T-$cyclic if and only if there is a basis E of W such that the matrix of T is given by the companion matrix of MMP p of T

Proof. ($\Rightarrow$): This part follows from the (4) of theorem (1.2).
($\Leftarrow$): To prove the converse let $E = \{e_0, e_1, \ldots, e_{n-1}\}$ and the matrix of T is given by the companion matrix of the MMP $p(X) = c_0 + c_1X + \cdots + c_{n-1}X^{k-1} + X^k$. Therefore, we have

$$(T(e_0), T(e_1), T(e_2) \ldots, T(e_{n-1})) =$$
$$(e_0, e_1, e_2, \ldots, e_{n-1}) \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -c_{n-1} \end{pmatrix}.$$

For $i = 1, \ldots, n-1$ we have $e_i = T(e_{i-1}) = T^i(e_0)$. Therefore

$$V = Span(e_0, \ldots, e_{n-1}) = \mathbb{F}[X]e_0.$$

Hence V is $T-$cyclic. This completes the proof.

The following is the matrix version of the above theorem 1.4.

1.5 (Theorem) Suppose $p \in \mathbb{F}[X]$ is a monic polynomial and A is the companion matrix of p. Then both the characteristic polynomial and the MMP of A is p.

Proof. Write $p(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1} + X^n$. Then

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix}.$$

Therefore the characteristic polynomial of A is $q = \det(XI_n - A)$. Expand the determinant along the first row and use induction to see

$$q = \det(XI_n - A) = p.$$

Now consider the linear operator $T : \mathbb{F}^n \to \mathbb{F}^n$ given by $T(X) = AX$. By theorem 1.4, we have $\mathbb{F}^n$ is $T-$cyclic. By (3) of theorem 1.2, MMP of T is p. So, MMP of A is also p. This completes the proof.

2 Cyclic Decomposition and Rational Forms

Given a finite dimensional vector space V and an operator $T \in L(V, V)$, the main goal of this section is to decompose

$$V = Z(v_1, T) \oplus \cdots \oplus Z(v_k, T)$$

as direct sum of $T-$cyclic subspaces.

2.1 (Remark) Suppose $T \in L(V, V)$ is an operator on a finite dimensional vector space V. Also suppose V has a direct sum decomposition $V = W \oplus W'$ where both W, W' are invariant under T. In this case, we say W' is $T-$**invariant complement** of W.

Now, let $v = w + w'$, with $w \in W, w' \in W'$ and $f(X)$ be a polynomial. In this case,

$$[f(T)v \in W] \Longrightarrow [f(T)v = f(T)w + f(T)w' = f(T)w.]$$

So, we have the the following definition.

2.2 (Definition) Suppose $T \in L(V, V)$ is an operator on a finite dimensional vector space V. A subspace W of V is said to be $T-$**admissible,** if

1. W is invariant under T;
2. For a polymonial $f(X)$ and $v \in V$,

$$[f(T)v \in W] \quad \Longrightarrow [f(T)v = f(T)w] \quad for\ some \quad w \in W.$$

2.3 (Remark) We have,

1. Obviously, $\{0\}$ and V are $T-$admissible.
2. Above remark 2.1, asserts that if an invariant subspace W has an invariant complement then W is $T-$admissible.

The following is the main theorem.

2.4 (Cyclic Decomposition Theorem) Let V be a finite dimensional vector space with $\dim(V) = n$ and $T \in L(V, V)$ be an operator. Suppose W_0 is a proper $T-$admissible subspace of V. Then there exists non-zero $w_1, \ldots, w_r \in V$, such that

1. $V = W_0 \oplus Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$;
2. Let p_k be the MMP of $ann(w_i)$. (see Part 7 of 1.1) Then $p_k \mid p_{k-1}$ for $k = 2, \ldots, r$.

Further, the integer r, and $p_1, \ldots, p_r$ are uniquely determined by (1) and (2).

Proof. We will complete the proof in several steps.
Step-I: Conductors and all: Suppose $v \in V$ and W is an invariant suspace V. Assume $v \notin W$.

1. Write
$$I(v, W) = \{f(X) \in \mathbb{F}[X] : f(T)v \in W\}.$$
2. Since W is invariant under T, we have $I(v, W)$ is an ideal of $\mathbb{F}[X]$. Also, since $v \notin W$ we have $1 \notin I(v, W)$ and $I(v, W)$ is a proper ideal. (*The textbook uses the notation $S(v, W)$. I use the notation $I(v, W)$ because it reminds us that it is an ideal.*)
3. This ideal $I(v, W)$ is called **the $T-$conductor** of v in W.
4. Let $I(v, W) = \mathbb{F}[X]p$. We say that p is the MMP of the conductor.
5. (Exercise) We have, $dim(W + \mathbb{F}[T]v) = \dim(W) + degree(p)$. So,
$$degree(p) \leq \dim(V) = n.$$

Step-II: If $V = W_0$ there is nothing to prove. So, we assume $V \neq W_0$. Let
$$d_1 = max\{degree(p) : I(v, W_0) = \mathbb{F}[X]p; v \notin W_0\}.$$
Note that the set on the right hand side is bounded by n. So d_1 is well defined and there is a $v_1 \in V$ such that $I(v_1, W_0) = \mathbb{F}[X]p_1$ and $degree(p_1) = d_1$.

Write
$$W_1 = W_0 + Z(v_1, T).$$
Then $\dim(W_0) < \dim(W_1) \leq n$ and W_1 is $T-$invariant.

Therefore, this process can be repeated and we can find $v_1, v_2, \ldots, v_k$ such that

1. We write $W_k = W_{k-1} + Z(v_k, T)$,

2. $v_k \notin W_{k-1}$,

3. p_k is the MMP of the conductor of v_k in W_{k-1}. That means $I(v_k, W_{k-1}) = \mathbb{F}[X]p_k$.

4. Also
$$d_k = degree(p_k) = max\{degree(p) : I(v, W_{k-1}) = \mathbb{F}[X]p; v \notin W_{k-1}\}.$$

5. $\dim(W_0) < \dim(W_1) < \cdots < \dim(W_r) = n$ and so $W_r = V$.

6. $V = W_0 + Z(v_1, T) + Z(v_2, T) + \cdots + Z(v_r, T)$.

Step-III: Here we prove the following for later use:

Let $v_1, \ldots, v_r$ be as above. Fix k with $1 \le k \le r$. Let $v \in V$ and $I(v, W_{k-1}) = \mathbb{F}[X]f$. Suppose
$$fv = v_0 + \sum_{i=1}^{k-1} g_i v_i \quad with \quad v_0 \in W_0, g_i \in \mathbb{F}[X].$$
Then $f \mid g_i$ and $v_0 = fx_0$ for some $x_0 \in W_0$.

To prove this, use division algorithm and let $g_i = fh_i + r_i$ where $r_i = 0$ or $degree(r_i) < degree(f)$. We will prove $r_i = 0$ for all i.

Let
$$u = v - \sum_{i=1}^{k-1} h_i v_i.$$
Note $v - u \in W_{k-1}$ and hence
$$I(u, W_{k-1}) = I(v, W_{k-1}) = \mathbb{F}[X]f.$$

Also $fu = fv + f(u - v) =$
$$v_0 + \sum_{i=1}^{k-1} (fh_i + r_i)v_i - \sum_{i=1}^{k-1} fh_i v_i = v_0 + \sum_{i=1}^{k-1} r_i v_i$$

Assume not all $r_i = 0$. Then

$$fu = v_0 + \sum_{i=1}^{j} r_i v_i \qquad (Eqn - I)$$

where $j < k$ and $r_j \neq 0$. Let

$$I(u, W_{j-1}) = \mathbb{F}[X]p$$

Since $I(u, W_{j-1}) \subseteq I(u, W_{k-1})$ we have $p = fg$ for some polynomial g.
Apply $g(T)$ to Eqn-I and get

$$pu = gfu = gv_0 + \sum_{i=1}^{j-1} gr_i v_i + gr_j v_j$$

Therefore

$$gr_j \in I(v_j, W_{j-1}) = \mathbb{F}[X]p_j.$$

By maximality of p_j we have $deg(p_j) \geq deg(p)$.

Therefore $deg(gr_j) \geq deg(p_j) \geq deg(p) = deg(fg)$. Hence $deg(r_j) \geq deg(f)$, with is a contradiction.

So, $r_i = 0$ for all $i = 1, \ldots r$. So,

$$fv = v_0 + \sum_{i=1}^{k-1} fr_i v_i.$$

Now, by admissibility of W_0, we have $v_0 = fx_0$ for some $x_0 \in W_0$. So, Stap-III is complete.

Step-IV: We will pick $w_1 \notin W_0$ such that

1. $V = W_0 + Z(w_1, T) + Z(v_2, T) + \cdots + Z(v_r, T)$ and $W_1 = W_0 + Z(w_1, T)$,
2. The ideals $\mathbb{F}[X]p_1 = I(v_1, W_0) = ann(w_1)$.
3. $W_0 \cap Z(w_1, T) = \{0\}$.
4. $W_1 = W_0 + Z(w_1, T) = W_0 \oplus Z(w_1, T)$.

To see this, first note that, by choice, $p_1 v_1 \in W_0$ and by admissibility we have $p_1 v_1 = p_1 x_1$ for some $x_1 \in W_0$. Take $w_1 = v_1 - x_1$.

Proof of (1) follows from the fact that $w_1 - v_1 \in W_0$

By choice, $p_1 \in ann(w_1)$. Therefore, $I(v_1, W_0) = \mathbb{F}[X]p_1 \subseteq ann(w_1)$. Now suppose $f \in ann(w_1)$. Then $fv_1 = fw_1 + f(v_1 - w_1) = f(v_1 - w_1) \in W_0$. Hence $ann(w_1) \subseteq I(v_1, W_0)$. Therefore (2) is established.

To prove (3), first note that $p_1 w_1 = 0$. Now, let $x \in W_0 \cap Z(w_1, T)$. Therefore, $x = fw_1$, for some polynomial f. Using division algorithm, we have $f = qp_1$. So, $x = fw_1 = qp_1 w_1 = 0$. So, (3) is established.

The last part (4), follows from (3).

Step-V: (*I wish W_1 was admissible so that we could repeat the process. But that does not seem correct.*) In any case, for $1 \leq k \leq r$, we will use Step-III and use induct to pick $w_2, \ldots, w_k$

1. $V = W_0 + Z(w_1, T) + Z(w_2, T) + \cdots + Z(w_k, T) + Z(v_{k+1}, T) + \ldots, Z(v_r, T)$ and $W_k = W_0 + Z(w_1, T) + Z(w_2, T) + \cdots + Z(w_k, T)$,
2. The ideals $\mathbb{F}[X]p_k = I(v_k, W_{k-1}) = ann(w_k)$.
3. $W_{k-1} \cap Z(w_k, T) = \{0\}$.
4. $W_k = W_0 \oplus Z(w_1, T) \oplus Z(w_2, T) \oplus \cdots \oplus Z(w_k, T)$.

To prove this, we assume the statements holds for the previous step and prove it fome the k^{th}step. So, we are assuming that we have already picked $w_1, \ldots, w_{k-1}$ with all the above properties and will pick w_k.

We use Step-III, with $f = p_k$ and $I(v_k, W_{k-1})$. We have, $p_k v_k \in W_{k-1}$ and

$$p_k v_k = v_0 + \sum_{i=1}^{k-1} g_i v_i \quad with \quad v_0 \in W_0, g_i \in \mathbb{F}[X].$$

So, $g_i = p_k h_i$ and $v_0 = p_k y_0$ for some $y_0 \in W_0$. Write

$$w_k = v_k - y_0 - \sum_{i=1}^{k-1} h_i v_i.$$

Therefore, $w_k - v_k \in W_{k-1}$. Therefore, (1) and (2) follow immediately. Also, (4) will follow from (3). Proof of (3) follows as in the previous step, because $p_k w_k = 0$.

Step-VI: In this step, we prove that $p_k \mid p_{k-1}$. We will use Step-III. We have, $I(w_k, W_{k-1}) = \mathbb{F}[X]p_k$. By our choice,

$$p_k w_k = p_{k-1} w_{k-1} = \cdots = p_2 w_2 = p_1 w_1 = 0.$$

Therefore, we have

$$p_k w_k = 0 + p_{k-1} w_{k-1} + \cdots + p_2 w_2 + p_1 w_1.$$

Hence, by Step-III, whe have $p_k \mid p_{k-1}$.

Step-VII (Uniqueness): Now, we prove the uniqueness part. Suppose $w'_1, \ldots, w'_s \in V$, such that

1. $V = W_0 \oplus Z(w'_1, T) \oplus \cdots \oplus Z(w'_s, T)$;
2. Let q_k be the MMP of $ann(w'_k)$ and $q_k \mid q_{k-1}$ for $k = 2, \ldots, s$.

We will prove that $r = s$ and $p_i = q_i$.

First, write

$$I = \{f \in \mathbb{F}[X] : f(T)V \subseteq W_0\}.$$

Clearly, I is an ideal. We claim that $I = ann(w_1)$. Note that $p_i w_i = 0$ and $p_i \mid p_1$. Therefore, $p_1 w_i = 0$ for $i = 1, \ldots, r$. Therefore,

$$p_1(T)V = p_1(T)(W_0 \oplus Z(w_1, T) \oplus \cdots \oplus Z(w_s, T)) = p_1(T)W_0 \subseteq W_0.$$

Therefore, $p_1 \in I$ and hence $ann(w_1) = \mathbb{F}[X]p_1 \subseteq I$. Conversely, suppose $f \in I$. Then $f(T)w_1 \in W_0 \cap Z(w_1, T) = \{0\}$. Therefore, $f \in ann(w_1)$. Hence $I \subseteq ann(w_1) = \mathbb{F}[X]p_1$. So, we have

$$I = ann(w_1) = \mathbb{F}[X]p_1.$$

Similarly,

$$I = ann(w'_1) = \mathbb{F}[X]q_1.$$

Since, both p_1 and q_1 are monic, we have $p_1 = q_1$. Write

$$W_1' = W_0 \oplus Z(w_1', T).$$

Now assume that $2 \leq r \leq s$. We proceed to prove $p_2 = q_2$. We start with the following observations:

1. $ann(w_1) = ann(w_1')$. **Proof.** Suppose $f \in ann(w_1)$. Then $fw_1 = 0$. Write $w_1' = w_0 + g(T)w_1$. Then $fw_1' = fw_0 \in W_0 \cap Z(w_1', T) = \{0\}$. So, $fw_1' = 0$ and $ann(w_1) \subseteq ann(w_1')$. Similarly, we prove the other inclusion and hence the equality.

2. $ann(p(T)w_1) = ann(p(T)w_1')$, for any polynomial p. **Proof.** The proof is similar to the above proof, but we will give a proof. Suppose $f \in ann(p(T)w_1)$. Then $fpw_1 = 0$. Write $w_1' = w_0 + g(T)w_1$.i Then $fpw_1' = fpw_0 \in W_0 \cap Z(w_1', T) = \{0\}$. So, $fpw_1' = 0$ and $ann(pw_1) \subseteq ann(pw_1')$. Similarly, we prove the other inclusion and hence the equality.

3. $\dim(Z(f(T)w_1, T)) = \dim(Z(f(T)w_1', T))$ for any polynomial f. This part follows from the above and (2) of theorem 1.2.

We have $V = W_0 \oplus Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$. Apply $p_2(T)$, and we have

$$p_2(V) = p_2(W_0) \oplus p_2(Z(w_1, T)) \oplus \cdots \oplus p_2(Z(w_r, T)).$$

Since, $p_2(Z(w_i, T)) = 0$ for $i \geq 1$ we have

$$p_2(V) = p_2(W_0) \oplus p_2(Z(w_1, T)) = p_2(W_0) \oplus Z(p_2(w_1), T).$$

Similar arguments also shows that

$$p_2(V) = p_2(W_0) \oplus p_2(Z(w_1', T)) \oplus p_2(Z(w_2', T)) \oplus \cdots \oplus p_2(Z(w_s', T)).$$

So,

$$p_2(V) = p_2(W_0) \oplus Z(p_2(w_1'), T) \oplus Z(p_2(w_2'), T) \oplus \cdots \oplus Z(p_2(w_s'), T).$$

By (3), $\dim(p_2(W_0) \oplus Z(p_2(w_1'), T)) = \dim(p_2(W_0) \oplus Z(p_2(w_1), T)) = \dim(p_2(V))$. Therefore, $Z(p_2(w_i'), T) = 0$ for $i = 2, \ldots, s$. So,

$$p_2 \in ann(w_2') = \mathbb{F}[X]q_2 \quad \textit{and hence} \quad q_2 \mid p_2.$$

Similarly, $p_2 \mid q_2$ and hence $p_2 = q_2$.

The proof is completed by continuing this process.

2.5 (Corollary: admissible complement) Let V be a finite dimensional vector space with $\dim(V) = n$ and $T \in L(V, V)$ be an operator. Suppose W is a $T-$admissible subspace of V. Then W has a complementary subspace W' which is also invariant under T.

Proof. By the above therem 2.4, we have $V = W \oplus Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$. The proof is complete by taking $W' = Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$.

2.6 (Corollary: Cyclicity) Let V be a finite dimensional vector space with $\dim(V) = n$ and $T \in L(V, V)$ be an operator. Let p be the MMP of T and P be the characteristic polynomial of T

1. There is a vector $w \in V$ such that $ann(w) = \mathbb{F}[X]p$.
2. V is $T-$cyclic if and only if $P = p$.

Proof. If $V = \{0\}$ then the theorem is obviously true. So, assmue $V \neq \{0\}$. By theorem 2.4, with $W_0 = \{0\}$, we have

$$V = Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$$

where $w_k \in V$ and $ann(w_k) = \mathbb{F}[X]p_k$ and $p_k \mid p_{k-1}$.

From the proof of uniqueness part of theorem 2.4, it follows that

$$\mathbb{F}[X]p_1 = ann(w_1) = \{f \in \mathbb{F}[X] : f(T) = 0\} = ann(T).$$

This means that $p_1 = p$ is the MMP of T. This establishes (1).

To prove (2), suppose $V = Z(w, T)$. By theorem 1.4, the matrix of T, with respect to a basis E, is given by the companion matrix of the MMP p of T. In this case, the characteristic polynomial $P = p$ the MMP of T.

Conversely, suppose $p = P$. By (1), there is a a $w \in V$ such that $ann(w) = \mathbb{F}[X]p$. It follows that $\dim(Z(w, T)) = degree(p) = degree(P) = \dim(V)$. So, $V = Z(w, T)$ and the proof is complete.

2.7 (Generalized Caley-Hamilton Theorem) Let V be a finite dimensional vector space with $\dim(V) = n$ and $T \in L(V, V)$ be an operator. Let p be the MMP of T and P be the characteristic polynomial of T

1. Then $p \mid P$.

2. The prime factors of p and P are same.

3. If $p = q_1^{r_1} \cdots q_l^{r_l}$ is the prime factorization of p, then $P = q_1^{d_1} \cdots q_l^{d_l}$ where
$$d_i = \frac{nullity\ q_i^{r_i}(T)}{degree(q_i)}.$$

Proof. If $V = \{0\}$ then the theorem is obviously true. So, assmue $V \neq \{0\}$. By theorem 2.4, with $W_0 = \{0\}$, we have
$$V = Z(w_1, T) \oplus \cdots \oplus Z(w_r, T)$$
where $w_k \in V$ and $ann(w_k) = \mathbb{F}[X]p_k$ and $p_k \mid p_{k-1}$.

From the proof of uniqueness part of theorem 2.4, it follows that
$$\mathbb{F}[X]p_1 = ann(w_1) = \{f \in \mathbb{F}[X] : f(T) = 0\} = ann(T).$$
This means that $p_1 = p$ is the MMP of T.

Let $T_i = T_{|Z(w_i,T)}$. Again, by cyclicity of $Z(w_i, T)$ both the MMP of T_i and characteristic polynomial of T_i is p_i. Hence, the characteristic polynomial P of T is given by $P = p_1 p_2 \cdots p_r$. So, $p = p_1 \mid P$ and (1) is established.

Since $p = p_1 \mid P$, prime factors of p are also the factors of P. Also, since $p_k \mid p_1$ it follows that the prime factors of P are also the factors of p. So, (2) is established. By an application of Primary Decomposition Theorem (see end of Chapter 6), we have if W_i is the null space of $q_i^{r_i}$ then
$$V = W_1 \oplus \cdots \oplus W_l.$$
and the MMP of the restriction $T_i = T_{|W_i}$ is $q_i^{r_i}$. If P_i is the characteristic polynomial of T_i then by (2), $P_i = q_i^{d_i}$. Since MMP divides P_i, we have $d_i \geq r_i$. Also
$$\dim(W_i) = degree(P_i) = degree(q_i)d_i$$
and
$$\dim(W_i) = Nullity\ (q_i(T)^{r_i}).$$
So, proof of (3) is complete.

2.8 (Corollary) Let V be a finite dimensional vector space with $\dim(V) = n$ and $T \in L(V, V)$ be an operator. Suppose $T \neq 0$ and is nilpotent (that means $T^N = 0$ for some integer $N \geq 1$. Then characteristic polynomial of T is X^n.

Proof. Let $T^m = 0$ and $T^{m-1} \neq 0$. Then

$$ann(T) = \mathbb{F}[X]X^m.$$

(This needs a small proof, which you can do.) So MMP of T is $p = X^m$. By Generalized Caley-Hamilton Theorem 2.7, the characteristic polynomial of T is $q = X^N$, for some $N \geq m$. Since $degree(q) = \dim(V)$ we have $N = n$. So, the proof is complete.

2.9 (Exercise) 1. Find a matrix A with characteristic polynomial X^2.

2. Find a matrix A with characteristic polynomial $(1 - X)^2$.

3. Read Exercise 1-3 from page 239.

2.1 Rational Form

We wish to consider the matrix version of the cyclic decomposition theorem 2.4. First, we give a definition.

2.10 (Definition) Suppose $p_1, \ldots, p_r \in \mathbb{F}[X]$ are non-constant monic polynomials. Let A_i be the companion matric of p_i. Also assume that

$$p_{i+1} \mid p_i \quad for \quad i = 1, \ldots, r-1.$$

Write

$$A = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & A_r \end{pmatrix}.$$

In this case, we say that the matrix A is in **rational form.**

2.11 (Theorem : Rational Form) Suppose $\mathbb{F}$ is a field (*as always in this section*). Let A an $n \times n$ matrix. Then A is similar to a matrix B which is in rational form. More over, for a given matrix A, there is only one such matrix B (*that means B is unique*).

Proof. Let $T : \mathbb{F}^n \to \mathbb{F}^n$ be the operator given by $T(X) = AX$. By cyclic decomposition theoren 2.4, There are elements $w_1, \ldots, w_r \in \mathbb{F}^n$ such that

1. $\mathbb{F}^n$ decomposes as
$$\mathbb{F}^n = Z(w_1, T) \oplus Z(w_2, T) \oplus \cdots \oplus Z(w_r, T)$$
and
2. if p_i is the MMP of $ann(w_i)$ then
$$p_{i+1} \mid p_i \quad for \quad i = 1, \ldots, r-1.$$

Now suppose $degree(p_i) = k_i$ and A_i is the companion matrix of p_i. Let $E_i = \{w_i, T(w_i), \ldots, T^{k_i-1}(w_i)\}$ and $E = E_1 \cup \cdots E_r$. Then

1. E_i is a basis of $Z(w_i, T)$ and E is a basis of of $\mathbb{F}^n$.
2. Then A_i matrix of the restriction $T_{|Z(w_i,T)}$, with respect to the basis E_i
3. So, the matrix of T with respect to E is
$$B = \begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ 0 & 0 & A_3 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & A_r \end{pmatrix}.$$

Clearly, B is in Jordan form and A is similar to B. So, it only remains to establish the uniqueness part.

Suppose A is similar to another matric C which is in rational form. So, $A = PCP^{-1}$ for some matric $P \in GL_n(\mathbb{F})$. Let $E_0 = \{e_1, \ldots, e_n\}$ be the standard basis and
$$(\epsilon_1, \ldots, \epsilon_n) = (e_1, \ldots, e_n)P.$$
Then
$$(T(\epsilon_1), \ldots, T(\epsilon_1)) = (\epsilon_1, \ldots, \epsilon_n)C.$$
This equation gives a cyclic decomposition of $\mathbb{F}^n$. Now the uniqueness follows from the uniqueness part of the cyclic decomposition theorem 2.4. This completes the proof of this theorem.

3 The Jordan Form

3.1 (Facts) Let $\mathbb{F}$ be a field and V be a finite dimensional vector space with $\dim(V) = n$. Suppose $N \in L(V, V)$ be a linear operator. By cuclic decomposition theorem 2.4, there are elments $w_1, \ldots, w_r \in V$ such that

1. V decomposes as
$$V = Z(w_1, N) \oplus Z(w_2, N) \oplus \cdots \oplus Z(w_r, N)$$
2. If p_i is the MMP of $ann(w_i)$ then $p_k \mid p_{k-1}$ for $k = 2, \ldots, r$.
3. $p_1, \ldots, p_r$ are unique.
   Now assume that N is nilpotent.
4. Since N is nilpotent, let $N^k = 0$ and $N^{k-1} \neq 0$. So, MMP of N is X^k.
5. Note $p_1 \in ann(N) = \mathbb{F}[X]X^k$. and $X^k \in ann(w_1) = \mathbb{F}[X]p_1$. Therefore $p_1 = X_k$.
6. So, $p_i = X^{k_i}$ with $k_1 = k \geq k_2 \geq \cdots \geq k_r \geq 1$. and $k_1 + k_2 + \cdots + k_r = n$.
7. The rational form of N is determined by $k_1 = k \geq k_2 \geq \cdots \geq k_r \geq 1$.
8. The companion matrix of X^{k_i} is the $k_i \times k_i$ matrix
$$A_i = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$
9. Let $E_i = \{w_i, N(w_i), \ldots, N^{k_i-1}(w_i)\}$ and $E = E_1 \cup \cdots \cup E_r$. Then E_i is a basis of $Z(w_i, N)$ and E is a basis of V.
10. With respect to the basis E the matrix of N is
$$\begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & A_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & A_3 & \ldots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 0 & A_r \end{pmatrix}.$$

11. In fact, $nullity(N) = r$. In deed, $\{N^{k_1-1}(w_i), N^{k_2-1}(w_2), \ldots, N^{k_r-1})(w_r)\}$ forms a basis of Null space of N. **Proof.** Let $\mathcal{N}$ be the null space of N and $W = Span N^{k_1-1}(w_i), N^{k_2-1}(w_2), \ldots, N^{k_r-1})(w_r)$

    Clearly, $, N^{k_i-1}(w_i) \in \mathcal{N}$ and hence $W \subseteq \mathcal{N}$.

    To see the converse, let $v \in \mathcal{N}$. From the decomposition,

    $$v = f_1(N)w_1 + f_2(N)(w_2) + \cdots + f_r(N)(w_r)$$

    for some $f_i \in \mathbb{F}[X]$. We can assume $degree(f_i) \leq k_i - 1$ or $f_i = 0$. So,

    $$0 = N(v) = Nf_1(N)w_1 + Nf_2(N)(w_2) + \cdots + Nf_r(N)(w_r).$$

    Therefore, from decomposition, $Nf_i(N)(w_i) = 0$. So, $Xf_i \in ann(w_i) = \mathbb{F}[X]X^{k_i}$. Therefore $f_i = g_i X^{k_i-1}$ for some $g_i \in \mathbb{F}[X]$.

    From degree consideration, $f_i = c_i X^{k_i-1}$ where $c_i \in \mathbb{F}$. Therefore

    $$v = c_1 N^{k_1-1} w_1 + c_2 N^{k_2-1}(w_2) + \cdots + c_r N^{k_r-1}(w_r)$$

    is in the span.So, $\mathcal{N} \subseteq W$.

Before we proceed, we define elementary Jordan matrices.

3.2 (Definition) Let $\mathbb{F}$ be a field and $c \in \mathbb{F}$. Define the $n \times n$ matrix

$$J = J(c) = J(c, n) = \begin{pmatrix} c & 0 & 0 & \ldots & 0 & 0 \\ 1 & c & 0 & \ldots & 0 & 0 \\ 0 & 1 & c & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & c \end{pmatrix}.$$

This matrix is called an **elementary Jordan matrix with eigen value** c.

Following is the jordan decomposition theorem.

3.3 (Theorem: Jordan Decomposition) Let $\mathbb{F}$ be a field and V be vector space over $\mathbb{F}$. Suppose $T \in L(V,V)$ be a linear operator on V. Assume tha characteristic polynomial q of T factorizes completely as

$$q = (X - c_1)^{d_1}(X - c_2)^{d_2} \cdots (X - c_k)^{d_k}$$

where $c_1, \ldots, c_k$ are the distinct eigen values.

1. In this case, the MMP p of T is given by

$$p = (X - c_1)^{r_1}(X - c_2)^{r_2} \cdots (X - c_k)^{r_k}$$

   where $1 \leq r_i \leq d_i$.

2. Let W_i be the null space of $(T - c_i)^{r_i}$.

3. By primary decomposition theorem $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$ and MMP of the restriction $T_i = T_{|W_i}$ is $(X - c_k)^{r_k}$.

4. Write $N_i = (T_i - c_i) \in L(W_i, W_i)$. Then N_i is nilpotent. The matrix of N_i was computed in (10) of Facts 3.1. So there is a basis E_i of W_i and the matrix of N_i is given by

$$\begin{pmatrix} A_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & A_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & A_3 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & A_{l_i} \end{pmatrix}.$$

   where A_j has the form as in (8) of Facts 3.1.

5. Now since $T_i = c_i + N_i$, the matrix of T_i with respect to E_i is given by

$$B_i = \begin{pmatrix} J_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & J_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & J_3 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & J_{l_i} \end{pmatrix}.$$

   where $J_j = c_i + A_j$ are elementary Jordan matrices with eigen values c_i.

6. Now $E = E_1 \cup \cdots \cup E_k$ is a basis of V. With respect to E the matrix of T is given by

$$B = \begin{pmatrix} B_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & B_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & B_3 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & B_k \end{pmatrix}.$$

   where B_i are as in (5).

7. Here are a few definitions.

   (a) The matrix B_i is called the **Jordan block matrix** of T, **corresponding to the eigen value** c_i.

   (b) The matrix B above (6) is the called the **Jordan matrix of** T.

   (c) Any matrix of the form in (6) is said to be in **Jordan form.**

3.4 (Theorem: Main Jordan Decomposition) Let $\mathbb{F}$ be a field and V be vector space over $\mathbb{F}$. Suppose $T \in L(V, V)$ be a linear operator on V. Assume tha characteristic polynomial q of T factorizes completely as

$$q = (X - c_1)^{d_1}(X - c_2)^{d_2} \cdots (X - c_k)^{d_k}$$

where $c_1, \dots, c_k$ are the distinct eigen values.

Then T has Jordan matrix representation with respect to some basis E. Also note that there is one Jordan block B_i corresponding to each eigen value c_i and B_i is a $d_i \times d_i$ matrix. (*The textbook talks about uniqueness that I feel is unnecessary and we will skip.*)

3.5 (Exercise) Suppose A is a (commutative) ring and $x \in A$ is a nilpotent element. Then $1 + x$ is an unit. Likewise, $c + x$ is an unit for any unit $c \in A$.