LINEAR ALGEBRA FROM MODULE THEORY
PERSPECTIVE

KIM, SUNGJIN

1. Introduction

We provide here a list of linear algebra theorems that can be done easily by structure theorems.

Lemma 1.1 (Smith Normal Form). Let \( A \) be a nonzero \( m \times n \) matrix over a principal ideal domain (PID) \( R \). There exist invertible \( m \times m \) and \( n \times n \) matrices \( S, T \) so that

\[
SAT = \text{Diag}(\alpha_1, \cdots, \alpha_r),
\]

where \( \alpha_i | \alpha_{i+1} \) for \( i < r \), here the last few terms can be 0.

The proof uses the property of PID, but basically it is elementary row-column operation.

Lemma 1.2 (Structure Theorem over PID, Invariant factor decomposition). Every finitely generated module \( M \) over a PID \( R \) is isomorphic to a unique one of the form

\[
R^f \bigoplus \bigoplus_{i=1}^r R/(d_i),
\]

where \( d_i | d_{i+1} \), and \( d_i \neq (0) \). The summands are called the invariant factors.

Lemma 1.3 (Structure Theorem over PID, Primary decomposition). Conditions are the same as above, \( M \) is isomorphic to a unique one of the form

\[
R^f \bigoplus \bigoplus_{i=1}^s R/(p_i^{r_i}),
\]

where \( p_i \) are prime ideals.

This is an application of Smith Normal Form to a presentation \( R^r \longrightarrow R^s \).

2. Theorems

The key here is to look at a \( n \times n \) matrix \( A \) over a field \( \mathbb{F} \) as \( \mathbb{F}[x] \)-module element, namely \( x \). We can regard \( \mathbb{F}^n \) as \( \mathbb{F}[x] \)-module with \( p(x) \in \mathbb{F}[x] \) acting as \( p(A) \in M_{n \times n}(\mathbb{F}) \), denote it as \( M^A \). Note that for any field \( \mathbb{F} \), the polynomial ring \( \mathbb{F}[x] \) is a PID. Our application of the structure theorem in invariant factor form is
Theorem 2.1 (Rational Canonical Form-Invariant factor form). Let $A$ be a $n \times n$ matrix over a field $\mathbb{F}$. Then $A$ is similar to a unique block diagonal matrix of the form
\begin{equation}
\oplus_{i=1}^{r} C(f_i),
\end{equation}
where $f_i \mid f_{i+1}$, and $C(f_i)$ is the companion matrix associated to $f_i$.

Using primary decomposition, we have

Theorem 2.2 (Rational Canonical Form-Primary decomposition). Conditions are the same as above, $A$ is similar to a unique block diagonal matrix of the form
\begin{equation}
\oplus_{i=1}^{s} C(p_i^{r_i}),
\end{equation}
where $p_i$ are irreducible polynomials in $\mathbb{F}[x]$.

For the proof, use structure theorem to the $\mathbb{F}[x]$-module $M_A$ as described above.

If the ground field is algebraically closed, then we have Jordan Canonical Form.

Theorem 2.3 (Jordan Canonical Form). Let $A$ be a $n \times n$ matrix over a field $\mathbb{F}$. Then $A$ is similar to a unique block diagonal matrix of the form
\begin{equation}
\oplus_{i=1}^{s} J(\lambda_i, r_i),
\end{equation}
where $\lambda_i$ are the eigenvalues of $A$, and $J(\lambda_i, r_i)$ is the Jordan block of diagonal $\lambda_i$ with size $r_i \times r_i$.

Now, the problem reduces to determining invariant factors. We use Smith Normal Form to do this.

Theorem 2.4 (Invariant Factors). Let $A$ be a $n \times n$ matrix over a field $\mathbb{F}$. Then invariant factors can be recovered from the Smith Normal Form of $xI - A$. More precisely, if $S(xI - A)T = \text{Diag}(f_1, \cdots, f_n)$ for some invertible matrices $S, T$ and $f_i \mid f_{i+1}$, then $f_i$ are the invariant factors of $A$.

Here, first few terms can be 1. The proof starts from investigating the exact sequence
\begin{equation}
0 \rightarrow \mathbb{F}[x]^n \xrightarrow{xI - A} \mathbb{F}[x]^n \xrightarrow{\pi} \mathbb{F}[x]^n / \text{Im}(xI - A) \rightarrow 0.
\end{equation}

Then we see that
\[ M^A \simeq \mathbb{F}[x]^n / \text{Im}(xI - A). \]

Corollary 2.1 (Similarity of transpose). Let $A$ be a $n \times n$ matrix over a field $\mathbb{F}$. Then $A$ and its transpose $A^T$ are similar.

Proof. Write $xI - A = PDQ$ where $P, Q$ are invertible in $M_{n \times n}(\mathbb{F}[x])$ and $D$ diagonal. Taking transpose, we have
\[ xI - A^T = Q^T D^T P^T = Q^T DP^T. \]

Since $Q^T, P^T$ are also invertible, we see that $xI - A$ and $xI - A^T$ have the same invariant factors. \qed
Corollary 2.2 (Similarity Preserved by Field Extension). Let $A$ and $B$ be $n \times n$ matrices over a field $K$. Let $L$ be a field extension of $K$. Then $A$ and $B$ are similar over $K$ if and only if they are similar over $L$.

Proof. $\Rightarrow$ is obvious.
$\Leftarrow$ Let $\{A_i\}$ be the complete set of invariant factors of $A$, and $\{B_i\}$ that of $B$. Then we have
\[
L \otimes_K (\bigoplus_i K[x]/(A_i)) = \bigoplus_i L[x]/(A_i),
\]
and
\[
L \otimes_K (\bigoplus_i K[x]/(B_i)) = \bigoplus_i L[x]/(B_i).
\]
Since $A$ and $B$ are similar over $L$, we see that the RHS of the above formulas should be equal. Hence the sets of invariant factors $\{A_i\}$ and $\{B_i\}$ are identical, yielding that $A$ and $B$ are similar over $K$. □

Theorem 2.5 (Centralizer of a matrix). Let $A$ be a $n \times n$ matrix over $F$. Let $C_A = \{B \in M_{n \times n}(F) \mid AB = BA\}$. Then the minimal dimension of $C_A$ over $F$ is $n$, and this is obtained precisely when the minimal polynomial and characteristic polynomial of $A$ coincide.

The idea of proof is interpreting $C_A$ as an $F[x]$-endomorphism algebra of the $F[x]$-module $M_A$ (as described above). Use the Rational Canonical Form-Primary decomposition. We have the following formula for $\dim_F C_A$.

\[
\dim_F C_A = \dim_F \text{End}_F[x]M_A = \sum_p (\deg p) \sum_{i,j} \min\{\lambda_{p,i}, \lambda_{p,j}\},
\]

where the first sum is over all irreducible polynomials $p$ that divides the characteristic polynomial of $A$, and the indices $i, j$ of second double sum is from the partition $\lambda_p = \sum_i \lambda_{p,i}$ that indicates the powers of $p$ in $p$-primary part of $M_A$.

We can generalize this idea to solve the Sylvester Equation.

Theorem 2.6 (Sylvester Equation). Let $A$ be a $m \times m$ matrix, $B$ be a $n \times n$ matrix, and $C$ be a $m \times n$ matrix over $F$. Consider a matrix equation $AX + XB = C$. Then

- The matrix equation $AX + XB = C$ has a unique solution if and only if primary decompositions of $M^A$ and $M^{-B}$ have no common irreducible polynomial.
- Let $C_{A,B} = \{X \in M_{m \times n}(F) \mid AX + XB = 0\}$. Then we have

\[
\dim_F C_{A,B} = \dim_F \text{Hom}_F[x](M^{-B}, M^A) = \sum_p (\deg p) \sum_{i,j} \min\{\lambda_{p,i}, \mu_{p,j}\},
\]

where the first sum is over all irreducible polynomials $p$ which are common in the primary decompositions of $M^A$ and $M^{-B}$, and the indices $i, j$ of second double sum is from the partition $\lambda_p = \sum_i \lambda_{p,i}$ that indicates the powers of $p$ in $p$-primary part of $M^A$, $\mu_p = \sum_j \mu_{p,j}$ that of powers of $p$ in $p$-primary part of $M^{-B}$. 
Corollary 2.3 (Symmetric Similarity transform, [2]). Let $A$ be a $n \times n$ matrix over $\mathbb{F}$. Suppose also that the minimal polynomial and characteristic polynomial of $A$ coincide. Then any invertible matrix $X$ satisfying $XA = A^T X$ is symmetric.

Proof. Consider the following system $(\Sigma A)$ of matrix equations.

(9) $XA = A^T X,$

(10) $X = X^T.$

Note that the below system is equivalent to $(\Sigma A)$.

(11) $XA = A^T X^T,$

(12) $X = X^T.$

The linear transform $X \mapsto (XA - A^T X^T, X - X^T)$ has rank at most $\frac{n^2 - n}{2}$ since both components are skew-symmetric. Thus, the solution space of the system $(\Sigma A)$ has dimension at least $n$.

Now, fix a non-singular transform $X_0$ such that $X_0 A = A^T X_0$. Then

$XA = A^T X$ if and only if $X_0^{-1} X A = AX_0^{-1} X$.

This yields an isomorphism $X \mapsto X_0^{-1} X$ between \{ $X$ | $XA = A^T X$ \} and $C_A = \{ X' | X' A = A X' \}$. Since $\dim C_A = n$, the solution space for (9) has dimension $n$. Since the solution space for $(\Sigma A)$ has dimension $\geq n$, the dimension must be exactly $n$. Hence, every matrix $X$ satisfying (9) must also satisfy (10). □

Theorem 2.7 (Double Commutant Theorem, [3]). Let $A, B$ be $n \times n$ matrix over a field $\mathbb{F}$ such that any matrix that commutes with $A$ also commutes with $B$. Then $B = p(A)$ for some $p \in \mathbb{F}[x]$.

Proof. We use rational canonical form-invariant factor form(Theorem 2.1). Then we have

$M^A \simeq \mathbb{F}[x]/P_1 \oplus \cdots \oplus \mathbb{F}[x]/P_r,$

where $P_i = (p_i), p_i | p_{i+1}$. This gives invariant subspace decomposition,

$M^A = \bigoplus_{i=1}^r M_i,$

where $M_i \simeq \mathbb{F}[x]/P_i$.

Let $\pi_i : M^A \mapsto M_i$ be the projection, and $\pi_{ij} : M_i \mapsto M_j$ be the natural projection for $i > j$. Extend $\pi_{ij}$ linearly to $M^A$ by assigning 0 on all $M_k (k \neq i)$. Then all $\pi_i$ and $\pi_{ij}$ commute with $A$, thus commute with $B$. Therefore, each $M_i$ is $A$-invariant, thus it is also $B$-invariant. Let $e_i \in M_i$ be the element corresponding to $1 + P_i \in \mathbb{F}[x]/P_i$.

We see that there is $p(x) \in \mathbb{F}[x]$ such that $Be_r = p(A)e_r$. We claim that $Be_i = p(A)e_i$ for all $i < r$, and hence $B = p(A)$.

$Be_i = B\pi_{r,i}e_r = \pi_{r,i}Be_r = \pi_{r,i}p(A)e_r = p(A)\pi_{r,i}e_r = p(A)e_i.$
This completes the proof of our claim.

Note that [1] also contains proof of Theorem 2.6, 2.7 using Jordan canonical form. However, the proofs provided here are more elegant and conceptual.

References