Linear Algebra

Donghyun Park

December 10, 2025

These notes are based on 선형대수와 군 by 이인석 which is highly intuitive and instructive book for understanding linear algebra.

1 Problems of Linear Algebras

Linear Algebra concerns about **Linear Maps on Vector Space**. As many studied the Linear Algebra, usually matrices become the central object. However, matrices and basis are supplementary tools for **understanding Linear Maps**. Matrices and basis are useful for understanding Linear Algebra by **Hands** but the one who is only used to these **by Hands** method will fail to understand what really the **Linear Algebra wants to talk about**. However, it is also important to being used to handle matrices.
In this article F stands for **Fields**. So $F = \mathbb{F}_q$, $\mathbb{Q}_p$ fields are also possible. If $F = \mathbb{R}$ or $F = \mathbb{C}$ is needed, then I will clarify it.

The main topics concerning matrices are :
- **Classification of Matrices by Solution space**
- **Classification of Square Matrices by similar relation**

The main topics concerning Linear Algebras are:
- **Classification of Finite Dimensional Vector Space**
- **Dimension Theorem, Rank Theorem, Perp theorem**
- **Dual Space**
- **Philosophy of Bilinear form and Hermittian form, Quadratic form**
- **Transpose of Linear Map**

In my journey of studying Linear Algebra, at the **first studying** I learned how to deal with matrices (multiplication, row reduced transform, diagonalization). **Second studying**, I understood linear map is **equivalent** to matrices. To now the **third studying** I understood linear map is **not equivalent** to matrices, rather much abstract and nice concept. Matrices are just useful tool for 'calculating' linear map but linear map and vector space can be handled with much **canonical** way and beautiful harmony exists.

2 Vector Space

2.1 Existence of Basis

Theorem 1. *Every non-trivial vector space over F admits basis (proof needs Zorn's lemma)*

However, this does not mean basis is constructable. For example, function space $C^0(\mathbb{R})$ admits basis, but we cannot formulate it.

Theorem 2 (Basis Extension lemma)**.** *If S is linearly independent subset of V over F then there exists basis of V that contains S.*

Theorem 3. *If S generates V which S is subset of non-zero vector space V, then there exists basis of V that is contained at S.*

3 Linear Transform and Matrix

3.1 Classification of f.d.v.s

Theorem 4. *If V is a vector field over F and $dimV = n$, then $V \approx F^n$*

Thus, **invariant** of equivalence class of finite dimensional vector spaces with relation defined by isomorphism is **dimension**. We can also think any vector space as a representative : F^n

3.2 Linear Transform can be represented by Matrix

Theorem 5. *Every linear map $L : F^n \to F^m$ is form of L_A. Furthermore, A is unique.*

3.3 Dimension Theorem

Dimension Theorem is one **Central Theorem** of Linear Algebra.

Theorem 6 (Dimension Theorem)**.** *If V is f.d.v.s over F and $L : V \to W$ is linear map, then*

$$\dim V = \dim \ker L + \dim \operatorname{im} L$$

4 The Classification of $\mathcal{M}_{m,n}(F)$: In perspective of Solution Space

4.1 Rank Theorem

Theorem 7 (Rank Theorem)**.** *For $A \in \mathcal{M}_{m,n}(F)$, Row rank (defined by the dimension of row vector space) and Column rank (defined by the dimension of column vector space) are equal.*

Proof 1. Suppose A is $m \times n$ matrix. Then if we prove $m = \dim(kerA) + (\text{row rank})$ then since $\dim(imA) = (\text{col rank})$, proof is over. $m = \dim(kerA) + (\text{row rank})$ can be shown by row-reduced echelon form.
Proof 2. If A can be transformed to row-reduced echelon form R, then its row rank is invariant. Also, in the row-reduced echelon form R, row rank is clearly identical to column rank. Thus, one should prove that column space of A and R have the same rank. Since $EA = R$, $L_A = L_E^{-1} \circ L_R$ so $im(L_A) = im(L_E^{-1} \circ L_R) = L_E^{-1}(im(L_R))$. So as the vector space, isomorphism $L_A \approx L_R$ holds. They have the same rank.

4.2 Representative of the classification

Theorem 8. *Define $A \asymp B$ for*

$$A, B \in \mathcal{M}_{m,n}(F)$$

by $B = PAQ$ for some invertible $P \in \mathcal{M}_{m,m}(F)$, $Q \in \mathcal{M}_{n,n}(F)$. Then $A \asymp B$ if and only if $rank(A) = rank(B)$. Representative form of these equivalence classes is

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

5 The Classification of $\mathcal{M}_{n,n}(F)$: In Similar relation

Here, the equivalence relation is defined by $A \sim B$ if $A = UBU^{-1}$ for some matrix $U \in \mathcal{M}_{n,n}(F)$.

5.1 Minimal Polynomial

Minimal polynomial is the **minimum degree monic polynomial of annihilator ideal**. For T a linear operator, annihilator ideal

$$\mathcal{I}_T = \{f(t) \in F[t] \| f(T) = 0\}$$

. This minimal polynomial $m_T(t)$ generates annihilator ideal.

Theorem 9. *Characteristic polynomial $\phi_T(t)$ and minimal polynomial $m_T(t)$ have the same* ***monic irreducible divisors*** *(over field F)*

Minimal Polynomial admits **Induction** on matrix size.

5.2 Primary Decomposition Theorem

Theorem 10 (Primary Decomposition Theorem)**.** *If T is linear operator (or matrix) then for $\phi_T(t) = p_1(t)^{e_1} p_2(t)^{e_2} \cdots p_k(t)^{e_k}$ and $m_T(t) = p_1(t)^{f_1} p_2(t)^{f_2} \cdots p_k(t)^{f_k}$ ($p_i(t)$ are monic irreducible polynomial)*

$$\begin{aligned} V &= ker(p_1(T)^{e_1}) \oplus ker(p_2(T)^{e_2}) \oplus \cdots \oplus ker(p_k(T)^{e_k}) \\ &= ker(p_1(T)^{f_1}) \oplus ker(p_2(T)^{f_2}) \oplus \cdots \oplus ker(p_k(T)^{f_k}) \end{aligned}$$

Moreover, if we let $W_i = ker(p_i(T))^{e_i}$ and $T_i = T|_{W_i}$, then $\phi_{T_i}(t) = p_i(t)^{e_i}$ and $m_{T_i}(t) = p_i(t)^{f_i}$

If we admit this theorem, for basis $\mathcal{B}_\rangle$ of W_i, we have

$$[T]^{\mathcal{B}}_{\mathcal{B}} = \begin{pmatrix} [T_1]^{\mathcal{B}_1}_{\mathcal{B}_1} & 0 & \cdots & 0 \\ 0 & [T_2]^{\mathcal{B}_2}_{\mathcal{B}_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & [T_k]^{\mathcal{B}_k}_{\mathcal{B}_k} \end{pmatrix}$$

This is the consequence of following lemma which is immediate by $d(t) = g_1(t)f_1(t) + \cdots + g_k(t)f_k(t)$ holds for $d(t)$ the greatest common divisor.

Lemma 1. *If $f_1(t), \cdots, f_k(t) \in F[t]$ are monic, mutally relative prime and $\xi(t) = f_1(t)f_2(t)\cdots f_k(t) \in \mathcal{I}_T$ then*

$$V = ker(f_1(T)) \oplus ker(f_2(T)) \oplus \cdots \oplus ker(f_k(T))$$

5.3 Diagonalizability

Corollary 1. *T is diagonalizable if and only if the minimal polynomial $m_T(t)$ can be decomposed into 1st order monic polynomial and does not have multiple root.*

Thus, diagonalizability is fully determined by 'Minimal Polynomial'
Also, simiulataneous diagonalizability can be deduced by induction.

Theorem 11. *For $\{T_i\}_{i\in I}$, If $T_iT_j = T_jT_i$ and T_i are all diagonalizable, then $\{T_i\}_{i\in I}$ is simultaneously diagonalizable.*

Proof uses induction on dimension of V. Fix $T \in \{T_i\}_{i\in I}$ and decompose $V = E^T_{\lambda_1} \oplus \cdots \oplus E^T_{\lambda_k}$. Then $E^T_{\lambda_j}$ is T_i invariant space for all $i \in I$. So by induction hypothesis, $T_i\big|_{E^T_{\lambda_j}}$ are simultaneously diagonalizable with basis $\{\mathfrak{B}_j\}$. Now consider $\mathfrak{B} = \cup_{j=1}^k \mathfrak{B}_j$.
This can be used on finding center of groups, for example $O(n), U(n), SU(n)$.

5.4 T-Cyclic Subspace

Furthermore decomposition on linear operator uses T-Cyclic subspace terminology.

$$V = F[t]v = \{f(T)v \in V | f(t) \in F[t]\}$$

T-Cyclic space satisfies $deg(m_T) = dimV$ and $\phi_T(t) = m_T(t)$ (**I think this property, minimal polynomial equals to characteristic polynomial, is very important feature of Cyclic space**) because basis of $F[t]v$ is just

$$\mathfrak{B} = \{v, Tv, \cdots, T^{deg(m_T)-1}v\}$$

. For each T-Cyclic space, its companion matrix is defined, if $m_T(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0$ or $T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 = 0$, companion matrix is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

which is just a $[T]^{\mathfrak{B}}_{\mathfrak{B}}$.
For any T-invariant space V, we can define T-cyclic subspace W, which is cyclic via $T|_W$. If $W = F[t]w$, we notate $m_w(t) = m_{T|_W}(t)$.

5.5 Cyclic Decomposition Theorem

Theorem 12 (Cyclic Decomposition Theorem)**.** *If T is linear transform and $m_T(t) = p(t)^f$ where $p(t)$ is monic irreducible polynomial. Then*

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_h$$

$U_1, \cdots U_h$ are T-Cyclic subspace and for

$$\phi_{T|_{U_j}}(t) = m_{T|_{U_j}}(t) = p(t)^{r_j}$$

$$f = r_1 \geq r_2 \geq \cdots \geq r_h \geq 1$$

h and $r_1, \cdots, r_h$ are uniquely determined.

Thus, T-invariant space can be decomposed into direct sum of T-cyclic spaces and $h, r_1, \cdots, r_h$ are invariant on decomposition

5.6 Primary Decomposition Theorem $\oplus$ Cyclic Decomposition Theorem

For T, by **Primary Decomposition Theorem**

$$V = W_1 \oplus \cdots \oplus W_k$$

Where $W_i = ker(p_i(T)^{f_i})$. Next, $T_i = T|_{W_i}$ can be applied **Cyclic Decomposition theorem** so

$$W_i = U_{i1} \oplus \cdots \oplus U_{ih_i}$$

Where $f_i = r_{i1} \geq \cdots \geq r_{ih_i} \geq 1$ with

$$\phi_{T|_{U_{ij}}}(t) = m_{T|_{U_{ij}}}(t) = p_i(t)^{r_{ij}}$$

This is the **Best Answer to Decompose arbitrary**

$$\mathcal{M}_{n,n}(F)$$

Matrix. Equivalence relation $\sim$ is totally determined by $p_i(t), h_i, r_{ij}$.

5.7 Jordan Canonical Form

Jordan Canonical Form is Representative Form of $\mathcal{M}_{n,n}(F)$. One assumption that cannot be dropped is that F is Algebraically closed
After applying Primary Decomposition Theorem, $V = W_1 \oplus \cdots \oplus W_k$ and if we suppose $\phi_T(t)$ is multiple of linear polynomials(**Here the fact that F being algebraically closed is used**) then $\phi_{T_i}(t) = p_i(t)^{e_i}$ and $m_{T_i}(t) = p_i(t)^{f_i}$.
If we apply Cyclic Decomposition Theorem to $N = T - \lambda I$, $W = U_1 \oplus U_2 \oplus \cdots \oplus U_h$ and each $\phi_{N|_{U_j}}(t) = m_{N|_{U_j}}(t) = t^{r_j}$ so companion matrices last column is zero.

$$\begin{aligned} T|_{W_i} &\sim J_{(r_{i1}, r_{i2}, \cdots, r_{ih_i})} \\ &= \begin{pmatrix} \begin{matrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{matrix} & & & \\ & \begin{matrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{matrix} & & \\ & & \ddots & \\ & & & \begin{matrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{matrix} \end{pmatrix} \end{aligned}$$

Each block size is $r_{ij} \times r_{ij}$.

6 Duality, Nondegenerate Bilinear Form, Hermitian Form

The matrix is useful tool for visualizing abstract object 'Linear map'. In this chapter we want to give up this view. We again look at abstract view on Linear maps.

6.1 Nondegenerate Bilinear Form

We give vector space a bilinear form B. The condition **Nondegeneracy** able us to find a duality of V and V^*
First, we do not give nondegeneracy. Bilinear form has one-to-one correspondence with quadratic form. They are related by $Q(v) = \frac{1}{2}B(v, v)$, $B(v, w) = Q(v+w) - Q(v) - Q(w)$. With this bilinear form (or quadratic form), much rich structure can be given **Orthogonal group** and **Symplectic group**. They are defined by

$$O(V, B) = \{L \in GL(V) | B(Lv, Lw) = B(v, w)\}$$

for B symmetric bilinear form.

$$Sp(V, B) = \{L \in GL(V) | B(Lv, LW) = B(v, w)\}$$

for B alternating bilinear form.
Now we define orthogonality by using bilinear form B. v, w are orthogonal if $B(v, w) = 0$. Non-trivial theorem is that (V, B) has an orthogonal basis. However, we cannot extend arbitrary given orthogonal elements into orthogonal basis. This is because the Gram-Schmidt orthogonalization does not work. There is no reason that B to satisfy $B(v, v) \neq 0$.
Without nondegerate condition, $W \leq V$ the $W^{\perp}$ is strange. Indeed, since $B(v, v) = 0$ is possible, $W \cap W^{\perp} \neq 0$ and moreover, what we expect : $\dim W^{\perp} + \dim W = \dim V$ do not hold.
Thus we give **Nondegenerate** condition on B. Now, the following theorem holds.

Theorem 13. *Let V be a f.d.v.s and B be a nondegenerate bilinear form. For $W \leq V$*

$$\dim W + \dim W^{\perp} = \dim V$$

6.2 Duality

With the nondegenerate bilinear form, we can argue **duality**.
Let us first give a brief definition of the dual space. V^* is defined as a F-linear functionals over V. This is again a vector space structure.
Our first motivation starts from the **natural isomorphism** of V and V^{**}. They are the same!! Again, we gave up the language basis and matrix but this **natural isomorphism** does hold so we could think they are **the same**.
However, when thinking about V and V^*, we know by the classification of vector spaces that they can given an isomorphism if we declare basis. But we gave up the language of basis... Luckily, there also exists a **natural isomorphism with something** that makes us to identify V and V^*. This is the **nondegenerate bilinear form**.
The duality is given by

$$v \longleftrightarrow B(\cdot, v)$$

Thus the bridge between V and V^* was a nondegenerate bilinear form!

6.3 Transpose operator

Now we introduce what the **transpose** means in Linear map. (Not a matrix!) We can easily define a dual map. $L : V \to W$ then

$$L^* : W^* \to V^*$$

by

$$L^*(g) = g \circ L$$

.
With the **nondegenerate symmetric bilinear form** (V, B) and (W, C) we can identify V^* to V and W^* to W. This gives **transpose** operator $L^t : W \to V$. Transpose operator is the only operator satisfying

$$C(Lv, w) = B(v, L^t w)$$

$$C(w, Lv) = B(L^t w, v)$$

Here, in the definition of transpose, **symmetric** is not used for defining the transpose map. However, if we admit symmetric properties, then $(L^t)^t = L$ holds.
With the transpose, we know can write the orthogonal group into decent definition.

$$O(V, B) = \{L \in GL(V) | L^t \circ L = I\}$$

6.4 Hermitian Form

Hermitian form is complex version of bilinear form. Note that in the definition of bilinear form, we did not have any restriction on the field F.
In Hermitian form, we let $F = \mathbb{C}$ (or the same holds for the field with nontrivial involution)
The difference to symmetric bilinear form is $H(v, cw) = \bar{c}H(v, w)$ and $H(v, w) = \bar{H(w, v)}$.
The unitary group is defined on Hermitian space (V, H)

$$U(V, H) = \{L \in GL(V) | H(Lv, Lw) = H(v, w)\}$$

Within the nondegeneracy of H,

Theorem 14. *If $W \leq V$ and (V, H) nondegenerate Hermitian form*

$$\dim W + \dim W^{\perp} = \dim V$$

Moreover, the identification of V and V^* by

$$v \longleftrightarrow H(\cdot, v)$$

This identification is **conjugate linear** and gives **natural bijection** on V and V^*. And we define the **adjoint map** $L^\star$. Under the identification above, (V, H) with (W, K) nondegenerate Hermitian form the $L^\star$ is an dual map L^*. It is a unique linear map satisfying

$$K(Lv, w) = H(v, L^\star w)$$

$$K(w, Lv) = H(L^\star w, v)$$

7 Triangularization

7.1 Triangularization Theorem of algebraically closed F

Theorem 15. *If F an algebraically closed field then for linear transform T, there exists basis $\mathfrak{B}$ of V such that $[T]_{\mathfrak{B}}^{\mathfrak{B}}$ is a upper-triangular matrix.*

Actually to prove this, we need the quotient vector space to adapt an induction. The point is finding an eigenvector and eigenvalue so that with quotient the subspace generated by eigenvector, induction can hold.

8 Spectral Theorem

We shall use the spectral theorem to analyze the **structure of unitary group, orthogonal group**.
First, we are interested in **Complex vector space with positive definite Hermitian Form**

Theorem 16. *If (V, H) is complex vector space with positive definite Hermitian form, then FSAE for linear operator T.*
- T is normal. i.e.

$$TT^* = T^*T$$

- There exists an orthonormal basis which are all eigenvectors of T.

The proof depends heavily on **Positive definite** property. By using the Gram-Schmidt orthogonalization, we can do the induction.
So, we can reveal the structure of unitary group.

Theorem 17 (Spectral Theorem for $U(n)$)**.** *Let $\mathbb{T}_{U(n)}$ be the diagonal elements of $U(n)$ which is subgroup (and which is* ***the maximal torus****). Then every element in $U(n)$ is conjugate to maximal torus.*

Theorem 18 (Spectral Theorem for $SU(n)$)**.** *Let $\mathbb{T}_{SU(n)}$ be the diagonal elements of $SU(n)$ which is subgroup (and which is* ***the maximal torus****). Then every element in $SU(n)$ is conjugate to maximal torus.*

Now, we look on the real vector spaces. The analogous statement of T having orthonormal basis consist of eigenvectors; is following.

Theorem 19. *If (V, B) is real vector space with positive symmetric bilinear form, then FSAE for linear operator T*
- T is symmetric
- There exists an orthonormal basis which are all eigenvectors of T.

However, it is insufficient to analyze the orthogonal group $O(n)$. We need a spectral theorem for real orthogonal operator. In this case, we might not have an eigenvalue because $\mathbb{R}$ is not algebraically closed. Instead,

Theorem 20. *(V, B) be a real vector space with positive symmetric bilinear form. If T is an orthogonal operator, there exists $W_1, \cdots, W_s \leq V$ such that*
- $V = W_1 \oplus \cdots \oplus W_s$
- $W_1, \cdots, W_s$ are T-invariant and mutually orthogonal
- $\dim W_i = 1$ or 2

In this sense, we can reveal the structure of $O(n)$. For notational convenience we state $SO(n)$ case. The **maximal torus** is slightly modified.

$$\mathbb{T}_{SO(2n)} = \{\mathrm{diag}(A_1, \cdots, A_n) | A_1, \cdots, A_n \in SO(2)\}$$

$$\mathbb{T}_{SO(2n+1)} = \{\mathrm{diag}(1, A_1, \cdots, A_n) | A_1, \cdots, A_n \in SO(2)\}$$

Theorem 21 (Spectral Theorem for $SO(n)$)**.** *Every element in $SO(n)$ is conjugate to the element on maximal torus.*

This topic will be extended when analyzing the **compact Lie groups**.