# Linear Algebra

Ze Dian Xiao

September 25, 2019

# Contents

An important part of linear algebra is the study of vector spaces and the "homomorphisms" between them.

$\mathscr{X}, \mathscr{Y}$

## §1 Review Fields

**Definition 1.1.** A ring $R$ is a non-empty set with two binary operations $R$ x $R \to R$, $+$ addition and $\cdot$ multiplication satisfying

1. $(a+b)+c = a+(b+c)$ Associativity of addition
2. $a+b = b+a$ Commutativity of addition
3. $\exists$ an element $0_R \in R$ such that $a \cdot 0_R = a \forall a \in R$ $0_R$ is the neutral element of addition
4. $\forall a \in R$, there exists $b \in R$ such that $a+b = 0_R$, $b$ is called the additive inverse of $a$ and we write $b = (-a)$
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ Associativity of multiplication
6. There exists an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a, \forall a \in R$ $1_R$ is the identity of multiplication.
7. $a \cdot (b+c) = a \cdot b + a \cdot c$
   $(b+c) \cdot a = b \cdot a + b \cdot c$
   $\forall a, b, c$ in $R$

**Definition 1.2.** A ring $R$ is said to be commutative if $a \cdot b = b \cdot a \forall a, b \in R$

**Definition 1.3.** A commutative R is said to be an integral domain if $\forall a, b \in R, a \cdot b = 0_R \implies a = 0_R$ or $b = 0_R$ (eg. $\mathbb{Z}$ is an integral domain)

**Definition 1.4.** A field is a commutative ring $R$ if $\forall a \in R, a \neq 0_R$, there exists $b \in R$ such that $a \cdot b = b \cdot a = 1_R$.

**Definition 1.5.** A field F is an integral domain.
Let $a, b \in F$ such that $a \cdot b = 0_F$
If $b \neq 0$, there exists $y \in F$ such that $b \cdot y = 1_F$
$a \cdot b = 0_F \implies$

$$\begin{aligned} a \cdot b \cdot y &= 0_F \\ a \cdot (b \cdot y) &= 0_F \\ a \cdot 1_F &= 0_F \\ a &= 0_F \end{aligned}$$

**Example 1.6** (Example of Fields)
$\mathbb{Z}_5, \mathbb{R}, \mathbb{Q}, \mathbb{C}$

**Example 1.7** (Finite FIelds)

$\mathbb{Z}_n$ is the ring of integers modulo $n$ with addition and multiplication modulo n.
$\mathbb{Z}_4$ is the ring of integer $mod4$
$\mathbb{Z}_4 = \{0, 1_4, 2_4, 3_4\}$

**Proposition 1.8** (When is $\mathbb{Z}_n$ a field)

$\mathbb{Z}_n$ is a field $\iff$ $n$ is prime.

*Proof.* Assume that $n$ is prime. Write $n = p$ Let $a \in \mathbb{Z}_p$ such that $a \neq 0_P$, Let $X \in \mathbb{Z}$ such that $[x]_p = a$ So $x \not\equiv 0 modp$, so $p$ does not divide $x$. Since $p$ is prime and $p$ does not divide $x$, then $gcd(p, x) = 1$. Then there exists $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} xu + pv &= 1 \\ xu &\equiv 1 \pmod p \\ [xu]_p &= 1_p \\ [x]_p[u]_p &= 1_p \\ a \cdot [u]_p &= 1_p \end{aligned}$$

We prove tha tif $n$ is not prime, then $\mathbb{Z}_n$ is not a field, hence $\mathbb{Z}_4$ is not an integral domain(since $2_4 \cdot 2_4 = 0_4$) hence not a field. $\mathbb{Z}_6$ is not an integral domain(since $2_6 \cdot 3_6 = 0_6$) hence not a field. If $n$ is not prime , there exists$x, y \in \mathbb{Z}$ such that

$$1 \leq x, y \lneq n, n = xy$$

$xy \equiv 0 \bmod n$, so $[x]_n[y]_n = [0]_n$, $[x]_n \neq 0_n, [y]_n \neq 0_n$

- A field $F$ is called finite if $|F| \lneq +\inf$
- We will show that if $F$ is a finite field then $|F| = p^n$ for some prime $p$ and $n \in \mathbb{N}$ (No field with 6 elements, no field with 10 elements)
- Conversely, for every prime $p$ and $n \in \mathbb{N}$, there exists a finite field with $p^n$ elements (Not easy to show)

$$f(x) = x + y$$

□

**Definition 1.9** (Complex Numbers)**.** A complex number is an element of the form $a + ib$ where $a, b \in \mathbb{Z}$ and $i^2 = -1$
The set of complex numbers is denoted by $\mathbb{C}$

**Example 1.10**

Operation on complex numbers:

$$\begin{aligned} (a + ib) + (c + id) &= (a + c) + i(b + d) \\ (a + ib) \cdot (c + id) &= (ac + bd) + i(ad + bc) \end{aligned}$$

IMPORTANT

$$f(x) = \frac{f(x)+f(-x)}{2} + \frac{f(x)-f(-x)}{2}$$

Observe that the function

$$f_e : x \to \frac{f(x)+f(-x)}{2}$$

is even and

$$f_o : x \to \frac{f(x)-f(-x)}{2}$$

is odd

Suppose that

**Theorem 1.11**
Show that

$$det(C) = det(A)det(B)$$

*Proof.*

$$det(C) = \sum_{\sigma \in S_{n+m}} c_{1,\sigma(1)} \cdots c_{n+m,\sigma(n+m)}$$

□

**Definition 1.12** (Characteristic Polynomial)**.** Let $A \in M_n(\mathbb{F})$ The characteristic polynomial $\Delta_A(x)$ is defined by $\Delta_A(x) = det(xI_n - A)$

$\Delta_A$ has degree $n$

$$\Delta_A(0) = det(-A) = (-1)^n det(A) \text{ (constant term)}$$
$$\Delta_A(0) \neq 0 \iff det(A) \neq 0 \iff \text{ A is invertible}$$

**Example 1.13**
Let $A$ be an invertible $nxn$ matrix, Show that for all $t \neq 0$,

$$\Delta_A^{-1}(t) = \frac{t^n}{\Delta_A(0)} \Delta_A(\frac{1}{t})$$

*Solution.*

$$\begin{aligned}
\Delta_A^{-1}(t) &= det(tI_{nxn} - A^{-1}) \\
&= det(A^{-1}(tA - I_{nxn}) \\
&= det(tA^{-1}(A - \frac{1}{t}I_{nxn}) \\
&= det(-tA^{-1}(\frac{1}{t}I_{nxn} - A)) \\
&= det(-tA^{-1})det(\frac{1}{t}I_{nxn} - A) \\
&= t^n det(-A^{-1})det(\frac{1}{t}I_{nxn} - A) \\
&= \frac{t^n}{\Delta_A(0)} \Delta_A(\frac{1}{t})
\end{aligned}$$

□

**Theorem 1.14** (Cailey-Hamilton Theorem)

Let $A \in M_n(\mathbb{F})$ and $\Delta_A$ be the characteristic polynomial. Then the Cailey-Hamilton states that

$$\Delta_A(A) = 0_{nxn}$$

in the $n = 2$ case,

$$\Delta_A(A) = A^2 - (tr(A)A) + det(A)I_{nxn}$$

**Example 1.15**

Let $A$ be and $nxn$ invertible matrix. Show that $A^{-1} = f(A)$ for some polynomial f of degree $n - 1$ at most.

*Solution.* Let

$$\Delta_A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

Given $A$ is invertible, $a_0 = \Delta_A(0) \neq 0$
By Cailey-Hamilton, $\Delta_A(A) = 0_{nxn}$

$$\begin{aligned} A^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0I_{nxn} = 0 \\ A^n + a_{n-1}A^{n-1} + \cdots + a_1A = -a_0I_{nxn} \\ A(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1) = -a_0I_{nxn} \\ A\left\{\frac{-1}{a_0}(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1I_{nxn})\right\} = I_{nxn} \end{aligned}$$

$$A^{-1} = -\frac{1}{a_0}(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1I_{nxn}) = f(A)$$

where $f(x) = -\frac{1}{a_0}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$ □

**Example 1.16**

Let $A$ be an $nxn$ matrix and $B$ be an $mxm$ matrix.

$$C = \begin{bmatrix} A & X \\ 0 & B \end{bmatrix} \text{ where } X \text{ is } nxm$$

Such that $det(C) = det(A)det(B)$
It follows that:

$$det(C) = \sum_{\sigma \in S_{n+m}} sgn(\sigma) c_{1,\sigma(1)} \cdots c_{n+m,\sigma(n+m)}$$

$c_{x1} = 0$ for $x \geq n+1$
$c_{x2} = 0$ for $x \geq n+1$
$c_{xn} = 0$ for $x \geq n+1$
Pick a certain $x \geq n+1$ If $\sigma(x) \in \{1, \ldots, b\}$, $c_{x,\sigma x} = 0$
If $x \geq n+1$, $\sigma(x) \in \{n+1, \ldots, n+m\}$ If $1 \leq c \leq b$, $\sigma(x) \in \{1, \ldots, n\}$

$$= \sum_{\sigma_1, \sigma_2 : \sigma_1 \in S_n, \sigma_2 \in S_{\{n+1, \ldots, n+m\}}} sgn(\sigma_1 \sigma_2) c_{1,\sigma_1(1)} \cdots c_{n,\sigma_1(n)} c_{n,\sigma_2(n+1)} \cdots c_{n+m,\sigma_2(n+m)}$$

define $\sigma = \sigma_1 \sigma_2$
$= det(A)det(B)$

**Theorem 1.17**

$$det(AB) = det(A)det(B)$$

*Proof.*

$$\begin{aligned} det(AB) &= \sum_{\sigma \in S_n} sgn(\sigma)(AB)_{1,\sigma(1)} \cdots (AB)_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n} sgn(\sigma) \end{aligned}$$

□

**Example 1.18**

Extras Ex. 1 - Ex.3 Done!

**Definition 1.19.** Let $A \in M_n(\mathbb{F})$ $\lambda$ is called an eigenvalue of $A$ if $\exists v \neq 0$ st $Av = \lambda v$ is an eigenvector for the eigenvalue $\lambda$

**Theorem 1.20**

$\lambda$ is an eigenvalue of $A$ *iff* $\Delta_A(\lambda) = 0$

**Example 1.21** (Extras II, Final 2018)

Let $P$ be an $nxn$ matrix over $\mathbb{F}$ such that $P^2 = P$

1. Show that if $\lambda$ is an eigenvalue of $P$, then $\lambda \in \{0, 1\}$
2. Show that $\mathbb{F}^n = K_1 \oplus K_2$, where $K_1 = Null(P)$ and $K_2 = Ran(P)$
3. Show that $P$ is similar to a diagonal matrix with entries 1 and 0's over the diagonal (Note: the diagonal contains all zeros or all 1s)

*Solution.*

1. Let $\lambda$ is an eigenvalue of $P$. Then $\exists v \neq 0$ st $Pv = \lambda v \implies PPv = P(\lambda v) \implies P^2 v = \lambda P v = \lambda^2 v$

   Hence, $P^2 v = \lambda^2 v$. $P^2 = P$ so $P^2 v = Pv = \lambda v$, so $\lambda^2 v = \lambda v \implies (\lambda^2 - \lambda)v = 0$

   And so,
$$(\lambda^2 - \lambda) = 0 \implies \lambda^2 = \lambda \implies \lambda \in \{0, 1\}$$

2. Show that
$$\mathbb{F}^n = Ran(P) \oplus Null(P)$$

   Let $v \in \mathbb{F}^n$ $v = v - Pv + Pv$. Where $Pv \in Ran(P)$ and $v - Pv \in Null(P)$.
$$P(v - Pv) = Pv - P^2 v = 0$$

   We have shown that $\mathbb{F}^n = Ran(P) + Null(P)$

   To show $Ran(P) \cap Null(P) = \{0\}$, there are two approaches.

   - $$dim\mathbb{F}^n = dim(Null(P) + Ran(P))$$

     From the dimension argument,
$$\underbrace{dimNull(P) + dimRan(P)}_{n} - dim(Ran(P) \cap Null(P)) = dim(Null(P) + Null(P))$$

$$\text{from Rank-Nullity}$$
$$dim(Ran(P) \cap Null(P)) = n - n = 0$$
$$\therefore Ran(P) \cap Null(P) = \{0\}$$

   - Without dimension argument

     Let $v \in Ran(P) \cap Null(P)$, then $v \in Ran(P)$. Hence $\exists u \in \mathbb{F}^n$ st $v = Pu$
$$Pv = P^2 u = Pu$$
$$Pu = v$$
$$\therefore Pv = v$$

     but also, $v \in Null(P)$, hence $Pv = 0 \implies v = 0$

3. $\mathbb{F}^n = Null(P) \oplus Ran(P)$. Let $v_1, \ldots, v_k$ be a basis of $Null(P)$, and $v_{k+1}, \ldots, v_n$ be a basis of $Ran(P)$.

   Then,

$$B = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

   is a basis of $\mathbb{F}^n$.

$$Pv_1 = 0, Pv_{k+1} = v_{k+1} = 0v_1 + \cdots + 1v_{k+1} + 0v_{k+2} + \cdots + 0v_n$$

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

   Two same representations of a matrix are similar

□

**Example 1.22**

Find all eigenvalues and corresponding eigenspaces of the $nxn$ matrix of $\mathbb{C}$

$$A_n = \begin{bmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix}$$

*Solution.* Let $\lambda$ be an eigenvalue of $A_n$. Then there exists $v \in \mathbb{C}^n$ non zero, such that $A_n v = \lambda v$.

$$\begin{bmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} \lambda v_1 \\ \vdots \\ \vdots \\ \lambda v_n \end{bmatrix}$$

**Note.** Assume $A \in M_n(\mathbb{F})$ not invertible, then $A$ is not injective, then $Ker(A) \neq \{0\}$. Then there exists $v \neq 0$, st $Av = 0$. Then 0 is an eigenvalue of $A$.

If $\lambda = 0$, then the first line becomes $v_2 + \cdots + v_n = 0$. Second to last line we have $v_1 = 0$.

Then the eigenspace attached to 0 is

$$E_0 = \{(v_1, \ldots, v_n) \in \mathbb{F}^n : v_1 = 0, v_2 + \cdots + v_n = 0\}$$

where $dim(E_0) = n - 2$

If $\lambda \neq 0$, then the second to the last line are such that $v_2 = \cdots = v_n = \frac{1 v_1}{\lambda}$. Then plugging back into the first line we get that $v_2 + v_3 + \cdots + v_n = \lambda v_1$

$$\frac{n-1}{\lambda} v_1 = \lambda v_1$$

If $v_1 = 0$, then it follows that $v_i = 0 : i = 2, \ldots, n$. But this does not respect the definition of an eigenspace.

If $v_1 \neq 0 \implies \frac{n-1}{\lambda} = \lambda \implies \lambda^2 = n-1 \implies \lambda = \pm\sqrt{n-1}$

**Note.** The field here is $\mathbb{C}$ because in the case of another field, it could be that some eigenvalues do not exist.

What is the eigenspace attached to $\sqrt{n-1}$

$$E_{\sqrt{n-1}} = \{(v_1, \ldots, v_n) \in \mathbb{C}^n : v_2 = \cdots = v_n = \frac{1}{\sqrt{n-1}} v_1$$

Eigenspace attached to $-\sqrt{n-1}$

$$E_{-\sqrt{n-1}} = \{(v_1, \ldots, v_n) \in \mathbb{C}^n : v_2 = \cdots = v_n = \frac{1}{-\sqrt{n-1}} v_1$$

$\square$

**Example 1.23** (Final Exam 2018)

Let $V$ be an inner product space over $\mathbb{R}$ of dimension $n$. Show that there exists an isomorphism $f : V \to \mathbb{R}^n$, such that $< v, v' >= f(v) \cdot f(v')$

*Solution.* Let $\{v_1, \ldots, v_n\}$ be an orthonormal basis of $V$.

Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{R}^n$.

Consider $f : V \to \mathbb{R}^n$, $f(v) = [v]_B$. From theorem, we know that $f$ is an isomorphism.

$$< v, v' >= [v]_b [v']_B (Assignment) = f(v) \cdot f(v')$$

From assignment, given an orthonormal basis, then the inner product of two vectors is the product of the coordinates. $\square$

## §2 Tutorial 2

**Theorem 2.1** (Spectral Theorem for symmetric real matrices)

Let $A \in M_n(\mathbb{R})$ be a symmetric matrix. (ie $A = A^T$)

Then, $A$ is diagonalizable over $\mathbb{R}$

**Definition 2.2.** A matrix $A \in M_n(\mathbb{F})$ is diagonalizable if $\exists P \in GL_n(\mathbb{R})$ and a diagonal matrix $D \in M_n(\mathbb{R})$ such that

$$A = PDP^{-1}$$

**Example 2.3** (Diagonalizable matrix)

1. Any diagonal matrix $D \in M_n(\mathbb{R})$ is diagonalizable
2. Any symmetric matrix $A \in M_n(\mathbb{R})$ is diagonalizable
3. Any matrix $A \in M_n(\mathbb{R})$ with $n$ distinct eigenvalues (Converse is not true)

**Theorem 2.4**
If $A \in M_n(\mathbb{F})$ is diagonalizable, then there exists a orthonormal basis of $\mathbb{F}^n$ consisting of eigenvectors of $A$

**Theorem 2.5**
If $A \in M_n(\mathbb{R})$ is symmetric, then there exists a basis of $\mathbb{R}^n$ consisting of eigenvectors of $A$.

Every single linear algebra exam has a question about diagonalizing a matrix.(Be comfortable with computing)

**Example 2.6**
Let

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 0 \\ 2 & -4 & 2 \end{bmatrix}$$

*Solution.*

$$\Delta_A(x) = det(xI_3 - A) = \begin{bmatrix} x-1 & 2 & 0 \\ 0 & x-3 & 0 \\ 2 & -4 & x-2 \end{bmatrix} = (x-1)(x-2)(x-3)$$

Since we have 3 distinct eigenvalues, $A$ is diagonalizable over $\mathbb{R}$. Eigenvalues:

$$\lambda_1 = 1 \ \lambda_2 = 2 \ \lambda_3 = 3$$

Now we want to find a matrix $P$ such that $A = PDP^{-1}$
Eigenvectors of distinct eigenvalues are linearly independent.
Eigenvector for $\lambda_1 = 1$
We find $v \in \mathbb{R}^3$ such that $(I_3 - A)v = 0_{\mathbb{R}}$

$$\begin{aligned} (I - A)\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 & -2 & 0 \\ 0 & -2 & 0 \\ -2 & 4 & -1 \end{bmatrix}\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ \implies -2v_2 &= 0 \\ \implies -2v_2 &= 0 \\ \implies -2v_1 + 4v_2 - v_3 &= 0 \\ \therefore v_2 &= 0 \\ v_3 &= -2v_1 \end{aligned}$$

$$E_1 = \{(v_1, 0, -2v_1) : v \in \mathbb{R}\} = span\,\{1, 0, -2\}$$

Eigenvector for $\lambda_2 = 2$ We find $E_2$ □