1201 Algbra 1 Notes

Based on the 2016 autumn lectures by Prof F E A Johnson

The Author(s) has made every effort to copy down all the content on the board during lectures. The Author(s) accepts no responsibility whatsoever for mistakes on the notes nor changes to the syllabus for the current year. The Author(s) highly recommends that the reader attends all lectures, making their own notes and to use this document as a reference only.

Mon. 03/10/16

Algebra MATH1201

Prof. Francis Johnson

CHAPTER 1. § Elementary Linear Algebra § (Equations)

1.1 A note about linear equations and notation

$x+y=1$ (✓) $\qquad$ $\underset{\uparrow 1}{x^2+y^2=1}$ (X) $\qquad$ $x+y+z=1$ plane (✓)

Recommended Textbooks:
- H. Anton
  Linear Algebra & Geometry
- Schaum Outline Series
  Linear Algebra
- Lang's Algebra V. good

$x^2+y^2-z^2=1$ surface (X)

, we need 6 variables to illustrate the relationship

um of one point.

of letters. So we subscript variables.

$=1$

$X = (x_1, \ldots$ $\qquad$ OR $\qquad$ $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{pmatrix}$ Column Vector

Row Vector

It can also be $x_1+x_2-x_3-x_4+2x_5-3x_6=1$

- The general equation in n-dimensions looks like

$\boxed{a_1x_1+a_2x_2+\cdots+a_nx_n=b}$ where $x_1, \cdots x_n$ are variables

Think as follows:

$\underset{\sim}{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ represents "variables"

$\underset{\sim}{a} = (a_1, a_2, \cdots a_n)$ represents "constants"

- How about 2 equations in n unknowns?

$a_1x_1+a_2x_2+a_3x_3+\cdots+a_nx_n=b$

$c_1x_1+c_2x_2+c_3x_3+\cdots+c_nx_n=d$

Eventually, we will run out of letters.

Answer: Use double indices for coefficients.

$$S = \begin{cases} a_{11}x_1+a_{12}x_2+a_{13}x_3+\cdots+a_{1n}x_n=b_1 \\ a_{21}x_1+a_{22}x_2+a_{23}x_3+\cdots+a_{2n}x_n=b_2 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_{m1}x_1+a_{m2}x_2+a_{m3}x_3+\cdots+a_{mn}x_n=b_m \end{cases}$$

General System of m linear equations in n unknowns.

Cayley C. 1830 :

- Go back to a single equation.

$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$

$\underset{\sim}{a} = (a_1, a_2, \cdots, a_n)$ Row Vector

$\underset{\sim}{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ Column Vector

- Define $\boxed{\begin{aligned} a.x &= a_1x_1 + a_2x_2 + \cdots + a_nx_n \\ &= \sum_{r=1}^{n} a_r x_r \end{aligned}}$

So a single equation looks like $\boxed{a.x = b}$

- In a general system S,

these coefficients are arranged as an $m \times n$ matrix.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \quad \underline{\underline{OR}} \quad (a_{kl})_{\substack{1 \le k \le m \\ 1 \le l \le n}}$$

Note: The 1st index represents the row number.

The 2nd index represents the column number.

- EXAMPLE:

$$\begin{cases} x_1 - x_2 + 2x_3 - x_4 = 1 \\ 2x_1 + x_2 - x_3 - x_4 = 2 \\ -x_1 - x_2 \quad\quad + x_4 = 0 \end{cases}$$ (3 equations in 4 variables)

Coefficient matrix $= \begin{pmatrix} 1 & -1 & 2 & -1 \\ 2 & 1 & -1 & -1 \\ -1 & -1 & 0 & 1 \end{pmatrix}$

1·2 Matrix Product

Cayley's Great Idea

$A = (a_{ij})$ $\substack{1 \le i \le m \\ 1 \le j \le n}$ $m \times n$ matrix

$B = (b_{jk})$ $\substack{1 \le j \le n \\ 1 \le k \le p}$ $n \times p$ matrix

AB is then the $m \times p$ matrix defined as follows

$$\begin{aligned} (AB)_{ik} &= (i^{th} \text{ row of } A)(k^{th} \text{ column of } B) \\ &= (a_{i1}, a_{i2}, a_{i3}, a_{i4}, \cdots a_{in}) \begin{pmatrix} b_{1k} \\ b_{2k} \\ \vdots \\ b_{nk} \end{pmatrix} \\ &= a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} \\ &\boxed{= \sum_{j=1}^{n} a_{ij}b_{jk}} \end{aligned}$$

EXAMPLE:

$$A = \begin{pmatrix} 1 & 0 & 5 \\ -1 & 7 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & -1 \\ 0 & 7 \\ 5 & 2 \end{pmatrix}$$

$[2\times 3]$ $\qquad$ $[3\times 2]$

$$AB = \begin{pmatrix} 26 & 9 \\ 9 & 54 \end{pmatrix} \qquad BA = \begin{pmatrix} 2 & -7 & 3 \\ -7 & 49 & 14 \\ 3 & 14 & 29 \end{pmatrix}$$

Fri. 07/10/16

Algebra MATH1201

Prof. Francis Johnson

Recap:

$$S = \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

$\underset{\sim}{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ variable factor $n\times 1$ matrix

$\underset{\sim}{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$ $m\times 1$ matrix

$A = (a_{ij})$ $\begin{matrix} 1\le i\le m \\ 1\le j\le n \end{matrix}$ coefficient matrix $\qquad \boxed{S = A\underset{\sim}{x} = \underset{\sim}{b}}$

Matrix Multiplication

$A = (a_{ij})$ $\begin{matrix} 1\le i\le m \\ 1\le j\le n \end{matrix}$ $\qquad B = (b_{jk})$ $\begin{matrix} 1\le j\le n \\ 1\le k\le p \end{matrix}$

no. of columns A = no. of rolls B

So product AB is defined.

$$(AB)_{ik} = \sum_{j=1}^{n} A_{ij}B_{jk}$$

EXAMPLE: $\quad A = \begin{pmatrix} 1 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 1 \\ -1 & 2 \\ 2 & -1 \end{pmatrix}$

$$AB = \begin{pmatrix} 2 & -1 \\ 0 & 3 \end{pmatrix} \quad 2\times 2 \text{ matrix}$$

$$BA = \begin{pmatrix} 3 & -1 & -1 \\ 3 & 1 & -2 \\ 0 & -2 & 1 \end{pmatrix} \quad 3\times 3 \text{ matrix}$$

1·3 Basic Facts about Matrix Multiplication

(0) If A is $m\times n$, B is $n'\times p$, $\qquad$ "iff" ≡ if and only if

then AB is defined iff $n = n'$

(1) Suppose A is $m\times n$, B is $n\times p$,

then AB is defined, but BA is defined iff $p = m$

(2) If AB, BA both defined, then in general they have different sizes.

If AB, BA have the same size, then A and B are both square ($n\times n$ say)

(3) If A is $n\times n$, B is $n\times n$, both products are defined, but in general $AB \neq BA$

EXAMPLE:

$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\Rightarrow AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

In this case, $BA = -AB$. BUT this is very unusual.

Matrix Addition

$A = (A_{ij})$ $\begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix}$ $B = (B_{ij})$ $\begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix}$

$\boxed{(A+B)_{ij} = A_{ij} + B_{ij}}$ (Adding corresponding indices)

EXAMPLE: $A = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & 4 \end{pmatrix}$ $B = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -3 & -2 \end{pmatrix}$

$A + B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix}$

(4) A, B are $m \times n$, C is $n \times p$

$(A+B).C = AC + BC$ Right Distributivity

Also, A, B are $m \times n$, D is $p \times m$

$D(A+B) = DA + DB$ Left Distributivity

(5) Associativity of Multiplication

A is $m \times n$, B is $n \times p$, C is $p \times q$

$(AB).C = A.(BC)$ Associativity

(6) Zero Matrix

For each size (any m, n), there is a zero matrix $0_{ij} = 0$

2×3 $0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ 3×2 $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$

$0.A = 0$

$A.0 = 0$

Beware: Let A be $m \times n$,

so $A^2 = A.A$ is defined Nilpotent Matrix

There are many cases where $A^2 = 0$ but $A \neq 0$.

EXAMPLE: $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ but $A \neq 0$

(7) Identity Matrix (I_n)

- For each $n \geq 2$, there was a special $n \times n$ matrix I_n.

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

- Formal Def : $(I_n)_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

- Traditional Notation:

$$\boxed{\delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}}$$ Kronecker Delta

- <u>Properties of I_n</u> :

Let A be $m \times n$,

then AI_n is defined and $AI_n = A$

Likewise, if B is $n \times p$, $I_n B = B$

- Prove that $AI_n = A$ if A is $m \times n$.

Proof : $A = (A_{ij})$ $\begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix}$

$I_n = (\delta_{jk})$ $\begin{matrix} 1 \le j \le n \\ 1 \le k \le p \end{matrix}$

Use definition.

$$(AI_n)_{ik} = \sum_{j=1}^{n} A_{ij} (I_n)_{jk}$$

$$= \sum_{j=1}^{n} A_{ij} \delta_{jk}$$

k is fixed while j varies from 1 to n so picked out the fixed terms (1)

$$= A_{ik} \delta_{\boxed{kk}} + \sum_{\boxed{j \neq k}}^{n} A_{ij} \delta_{jk}$$

when $j \neq k$, $\delta_{jk} = 0$

$$= A_{ik} + 0$$

$$= A_{ik}$$

$\therefore (AI_n)_{ik} = A_{ik}$

$\Rightarrow \boxed{AI_n = A}$

- EXAMPLE : $\begin{cases} 2x_1 + 3x_2 = 1 \\ x_1 + 2x_2 = 2 \end{cases}$

Three Basic Operations :

(I) Add $\lambda Eq^n(i)$ to $Eq^n(j)$ where λ is some number

(II) Multiply $Eq^n(i)$ by $\lambda \neq 0$

(III) Permute the order in which the equations are written.

Add $(-2)Eq^n(2)$ to $Eq^n(1)$: $\begin{matrix} -x_2 = -3 \\ x_1 + 2x_2 = 2 \end{matrix}$

Add $2Eq^n(1)$ to $Eq^n(2)$: $\begin{cases} -x_2 = -3 \\ x_1 = -4 \end{cases}$

Swap $Eq^n(1)$ and $Eq^n(2)$: $\begin{cases} x_1 = -4 \\ -x_2 = -3 \end{cases}$

Multiply $Eq^n(2)$ by -1: $\begin{cases} x_1 = -4 \\ x_2 = 3 \end{cases}$

1.4 Elementary Row Operations

- Consider a system of linear equations:

$$x_1 + x_2 + x_3 = 1$$
$$x_1 - x_2 + x_3 = 3$$
$$x_1 + x_2 - x_3 = -1$$

- What can we do? Three things:

(I) $\mathcal{E}(i,j;\lambda)$ Adds $\lambda \text{Row}(j)$ to $\text{Row}(i)$

i.e. new $\text{Row}(i)$ = old $\text{Row}(i) + \lambda \text{Row}(j)$

All other rows stay the same.

(II) $\mathcal{D}(i;\lambda)$ Multiplies $\text{Row}(i)$ by λ, provided $\lambda \neq 0$.

(III) $\mathcal{P}(i,j)$ Swaps $\text{Row}(i)$ and $\text{Row}(j)$

- We are going to show that we can perform these three operations by multiplying on LEFT by a suitable matrix.

$$A = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} \qquad \cancel{j=1 \quad i=2}$$

$\mathcal{E}(2,1;\lambda)$ Adds $\lambda \text{Row}(1)$ to $\text{Row}(2)$

$$\begin{pmatrix} 1 & 0 & 0 \\ \lambda & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} = \begin{pmatrix} a & b \\ \lambda a + c & \lambda b + d \\ e & f \end{pmatrix}$$

$\mathcal{E}(1,3;\mu)$

$$\begin{pmatrix} 1 & 0 & \mu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix} = \begin{pmatrix} a+\mu e & b+\mu f \\ c & d \\ e & f \end{pmatrix}$$

QUESTION. Which matrix perform $\mathcal{E}(i,j;\lambda)$?

Elementary Matrices

- 2×2: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Greek letter "epsilon" → $\epsilon(1,1)$ $\epsilon(1,2)$ $\epsilon(2,1)$ $\epsilon(2,2)$

3×3: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$\epsilon(1,1)$ $\epsilon(1,3)$ $\epsilon(2,1)$ $\epsilon(3,3)$

- Informal Def:

$\epsilon(i,j)$ is $n\times n$ matrix which has 1 in position (i,j) and 0s everywhere else.

- Formal Def :

$$\epsilon(i,j) = \left(\epsilon(i,j)_{rs}\right) \quad \begin{matrix} 1 \le r \le n \\ 1 \le s \le r \end{matrix}$$

$$\boxed{\epsilon(i,j)_{rs} = \delta_{ir}\delta_{js}}$$

Check:

$$\epsilon(i,j)_{rs} = \begin{cases} 1 & r=i \text{ and } s=j \\ 0 & \text{otherwise} \end{cases}$$

QUESTION: Let A be $m \times n$

Let $\epsilon(i,j)$ be elementary $m \times m$.

What is $\epsilon(i,j)A$?

EXAMPLE: $$\underset{\epsilon(1,3)}{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}} \underset{A}{\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}} = \begin{pmatrix} e & f \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

" takes out the j^{th} row & put it into the i^{th} row & kills everything else "

- Proposition: Let $A = (a_{st})$ $\begin{matrix} 1 \le s \le m \\ 1 \le t \le n \end{matrix}$

Let $\epsilon(i,j)$ be elementary $m \times m$ matrix.

$\epsilon(i,j)A$ is the matrix where

i^{th} row $= j^{th}$ row of A

All other rows $\equiv 0$

Proof: $$[\epsilon(i,j)A]_{rt} = \sum_{s=1}^{m} \epsilon(i,j)_{rs} A_{st}$$ $(AB)_{rt} = A_{rs} B_{st}$

$$= \sum_{s=1}^{m} \delta_{ir}\delta_{js} A_{st}$$

sum over s separate cases $s=j$ & $s \ne j$

the case where $s=j$.

$$= \delta_{ir}\delta_{jj}A_{jt} + \sum_{s \ne j}^{m} \delta_{ir}\delta_{js}A_{st}$$

$\delta_{jj} = 1$

$$= \delta_{ir}A_{jt} + 0$$

when $s \ne j$ $\delta_{js} = 0$ by def

$$= \begin{cases} A_{jt} & r = i \\ 0 & r \ne i \end{cases}$$

Q.E.D.

Mon. 10/10/16

Algebra I MATH1201

Prof. Francis Johnson

- Recap: Elementary Row Operations

Basic Matrices

- Corollary: If λ is a "number",

then $\lambda\epsilon(i,j)A$ is a matrix whose i^{th} row $= \lambda$ (j^{th} row of A)

All other rows = 0

- Def: $E(i,j;\lambda) = I_m + \lambda \epsilon(i,j)$

  e.g. $m=3$, then:
  $E(2,3;\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix}$

- Th: Let A be $m \times n$,
  then the matrix $E(i,j;\lambda)A$ is the matrix obtained from A by performing the operation $\mathcal{E}(i,j;\lambda)$

  $\mathcal{E} \equiv$ operation $E \equiv$ matrix
  (Curly letters) (Straight letters)

Proof: $[I_m + \lambda\epsilon(i,j)]A = A + \lambda\epsilon(i,j)A$

so k^{th} row of $[I_m + \lambda\epsilon(i,j)]A = k^{th}$ row of A, where $k \neq i$ and k is a numbe

(This is because k^{th} row of $\lambda\epsilon(i,j)A = 0$)

and i^{th} row of $[I_m + \lambda\epsilon(i,j)]A = i^{th}$ row of A + i^{th} row of $\lambda\epsilon(i,j)A$

$= i^{th}$ row of $A + \lambda . j^{th}$ row of A QED

EXAMPLE: $E(2,3;\lambda) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{bmatrix}$ $A = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$

$\Rightarrow E(2,3;\lambda)A = \begin{pmatrix} a & b \\ c+\lambda e & d+\lambda f \\ e & f \end{pmatrix}$

- Def: Let A be an $m \times n$ matrix,
  we say that A is invertible when there exists a matrix B $(m \times m)$ s.t. $AB = I_m$ and $BA = I_m$.
  When this happens, write $\boxed{B = A^{-1}}$

EXAMPLE: $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$

$\Rightarrow AB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

In this case, A is invertible and $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$

$A = E(1,2;2)$

$B = E(1,2;-2)$

- Prop: $E(i,j;\lambda)$ is invertible
  and $E(i,j;\lambda)^{-1} = E(i,j;-\lambda)$

Proof: coming soon ◡̈

Operation		Matrix $(i \neq j)$
① $\mathcal{E}(i,j;\lambda)$	$\sim$	$E(i,j;\lambda) = I_m + \lambda\epsilon(i,j)$
② $\mathcal{D}(i;\lambda)$ $(\lambda \neq 0)$	$\sim$	$\Delta(i;\lambda) = I_m + (\lambda - 1)\epsilon(i,i)$

EXAMPLE: $A = \begin{pmatrix} a & b \\ c & d \\ e & f \\ g & h \end{pmatrix}$ perform $\mathcal{D}(2;\lambda)$

Get $\begin{pmatrix} a & b \\ c & d \\ e & f \\ g & h \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ (\lambda-1)c & (\lambda-1)d \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ \lambda c & \lambda d \\ e & f \\ g & h \end{pmatrix}$

$\boxed{A + (\lambda-1)\epsilon(i,i)A}$

- k^{th} row of $\epsilon(i,i)A = 0$ $(k \neq i)$

  i^{th} row of $\epsilon(i,i)A = i^{th}$ row of A

- k^{th} row of $(\lambda-1)\epsilon(i,i)A = 0$ $(k \neq i)$

  i^{th} row of $(\lambda-1)\epsilon(i,i)A = (\lambda-1)(i^{th}$ row of $A)$

This can be transformed into

$[I_m + (\lambda-1)\epsilon(i,i)]A$

- k^{th} row of $[I_m + (\lambda-1)\epsilon(i,i)]A = k^{th}$ row of A $(k \neq i)$

  i^{th} row of $[I_m + (\lambda-1)\epsilon(i,i)]A = i^{th}$ row of $A + (\lambda-1)(i^{th}$ row of $A)$

  $= \lambda.(i^{th}$ row of $A)$

- $\mathcal{D}(i;\lambda)$ multiplies i^{th} row of A by $\lambda \neq 0$

  $\mathcal{D}(i;\frac{1}{\lambda})$ multiplies i^{th} row of A by $\frac{1}{\lambda} \neq 0$

  $\Delta(i;\lambda)$ invertible and

  $\boxed{\Delta(i;\lambda)^{-1} = \Delta(i,\frac{1}{\lambda})}$

③ $\mathcal{P}(i,j)$ interchanges i^{th} & j^{th} row

- We expect that $P(i,j)$ = matrix obtained from I_m by swapping i^{th} & j^{th} rows.

EXAMPLE: $m=4$, then $P(2,3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

- Does it work?

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \\ e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a & b \\ e & f \\ c & d \\ g & h \end{pmatrix}$$

$I_m - \epsilon(i,i) - \epsilon(j,j) + \epsilon(i,j) + \epsilon(j,i)$

$P(i,j)^{-1} = P(i,j)$

Fri. 14/10/16

MATH1401 Algebra I

Prof. Francis Johnson

Operation		Matrix
$\mathcal{E}(i,j;\lambda)$	$\sim$	$E(i,j;\lambda) = I_m + \lambda\epsilon(i,j)$

$\mathcal{D}(i;\lambda) \quad (\lambda\neq 0) \qquad \sim \qquad \Delta(i;\lambda) = I_m + (\lambda-1)\in(i,i)$

$\mathcal{P}(i,j) \qquad \sim \qquad P(i,j) = I_m - \in(i,i) - \in(j,j) + \in(i,j) + \in(j,$

$(i\neq j)$

- On Exercise 2,

we need to show $\boxed{\in(i,j)\in(k,l) = \begin{cases} \in(i,l) & j=k \\ 0 & j\neq k \end{cases}}$

Assume this is true, we have

corollary $\quad \in(i,j)\in(i,j) = 0 \quad i\neq j$

$\in(i,i)\in(i,i) = \in(i,i)$

- Prop. If $i\neq j$, then

$E(i,j;\lambda)$ is invertible

and $E(i,j;\lambda)^{-1} = E(i,j;-\lambda)$

Proof: $E(i,j;\lambda)E(i,j;-\lambda)$

$= [I_m + \lambda\in(i,j)][I_m - \lambda\in(i,j)]$

$= I_m^2 + \lambda I_m\in(i,j) - \lambda I_m\in(i,j) - \lambda^2\in(i,j)\in(i,j)$

$= I_m - \lambda^2\in(i,j)\in(i,j) \qquad \in(i,j)\in(i,j)=0 \quad i\neq j$

$= I_m$

$\Rightarrow E(i,j;\lambda)E(i,j;-\lambda) = I_m = E(i,j;-\lambda)E(i,j;\lambda)$ QED

- Prop. If $\lambda\neq 0$, then

$\Delta(i;\lambda)$ is invertible

and $\Delta(i;\lambda)^{-1} = \Delta(i;\frac{1}{\lambda})$

Proof: $\Delta(i;\lambda) = I_m + (\lambda-1)\in(i,i)$

$\Delta(i;\frac{1}{\lambda}) = I_m + (\frac{1}{\lambda}-1)\in(i,i) = I_m + \left(\frac{1-\lambda}{\lambda}\right)\in(i,i)$

$\Rightarrow \Delta(i;\lambda)\Delta(i,\frac{1}{\lambda})$

$= [I_m + (\lambda-1)\in(i,i)][I_m + \left(\frac{1-\lambda}{\lambda}\right)\in(i,i)]$

$= I_m^2 + (\lambda-1)I_m\in(i,i) + (\frac{1-\lambda}{\lambda})I_m\in(i,i) + (\lambda-1)\left(\frac{1-\lambda}{\lambda}\right)\in(i,i)\in(i,i)$

$= I_m + (\lambda-1+\frac{1-\lambda}{\lambda})I_m\in(i,i) + (\lambda-1)(\frac{1-\lambda}{\lambda})\in(i,i)$

$= I_m + \frac{(\lambda-1)^2}{\lambda}I_m\in(i,i) - \frac{(\lambda-1)^2}{\lambda}\in(i,i)$

$= I_m$ QED

- Prop. If $i\neq j$, then

$P(i,j)$ is invertible

and $P(i,j)^{-1} = P(i,j)$ self-inverse

Proof: $P(i,j)P(i,j)$

$= [I_m - \in(i,i) - \in(j,j) + \in(i,j) + \in(j,i)][I_m - \in(i,i) - \in(j,j) + \in(i,j) + \in(j,i)]$

$$= I_m^2 + 2[\epsilon(i,j) + \epsilon(j,i) - \epsilon(i,i) - \epsilon(j,j)] I_m + \epsilon(i,i) + 0 - \epsilon(j,j) - 0 + \epsilon(j,j) - 0$$
$$- \epsilon(j,i) - 0 - \epsilon(i,j) + 0 + \epsilon(i,i) - \epsilon(j,i) - 0 + \epsilon(j,j) + 0$$
$$= I_m$$

QED

1.4 How to solve a system of linear equations?

$$S = \begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 + \cdots + a_{mn}x_n = b_m \end{cases} \qquad S = \{A\underset{\sim}{x} = \underset{\sim}{b}\}$$

- Prop.- Suppose that I operate on the left by an invertible matrix P, then the solutions don't change.

  $S = \{A\underset{\sim}{x} = \underset{\sim}{b}\}$ $\qquad S' = \{PA\underset{\sim}{x} = P\underset{\sim}{b}\}$

  - If $\underset{\sim}{x}$ is a solution to S, then $\underset{\sim}{x}$ is also a solution to S'.
  - Conversely, if $\underset{\sim}{x}$ is a solution to S',

  $$PA\underset{\sim}{x} = P\underset{\sim}{b}$$

  - Multiply on the left by P^{-1} to get

  $$P^{-1}PA\underset{\sim}{x} = P^{-1}P\underset{\sim}{b} \qquad \text{where } P^{-1}P = I_m$$

  So, $\qquad A\underset{\sim}{x} = \underset{\sim}{b}$

  - So $\underset{\sim}{x}$ is a solution to S. QED

- (0) For some systems, solutions are obvious.

  EXAMPLE: $\left\{ \underset{\sim}{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ satisfying } x_1 + x_2 + x_3 = 1 \right\}$

  $$x_1 = 1 - x_2 - x_3$$

  $$\underset{\sim}{x} = \begin{pmatrix} 1 - x_2 - x_3 \\ x_2 \\ x_3 \end{pmatrix} \qquad \text{(has infinitely many solutions)}$$

  As x_2 and x_3 vary, we can get all possible solutions. (2-dimension)

(I) $\begin{cases} x_1 \quad + x_3 + x_4 + x_5 + x_6 - x_7 = 1 \\ x_2 - x_3 - x_4 + x_5 - x_6 + x_7 = 2 \end{cases}$

$$\underset{\sim}{x} = \begin{bmatrix} 1 - x_3 - x_4 - x_5 - x_6 + x_7 \\ 2 + x_3 + x_4 - x_5 + x_6 - x_7 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} \qquad \text{(infinitely many solutions)} \quad \text{(5-dimension)}$$

1·4·1 How do you recognise in advance which systems have obvious solutions?

Reduced Row Echelon Form

$$\begin{pmatrix} 1 & ? & 0 & ?? & 0 \\ 0 & 0 & 1 & ??? & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

EXAMPLE : $\begin{pmatrix} 1 & 2 & 0 & 5 & 3 & 0 & 1 \\ 0 & 0 & 1 & -2 & 7 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}$ ← Reduced Row Echelon

$\begin{pmatrix} 1 & 2 & 1 & 5 & 3 & 0 & 1 \\ 0 & 0 & 1 & -2 & 7 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}$ ← NOT reduced row echelon

- A reduced row echelon matrix satisfies the following criteria:

① In any non-zero row, the 1st non-zero entry is 1 (leading 1)

② In the column of leading 1, all other entries must be 0.

③ Rows must be "stepped" (Echelon)

④ Zero rows finish last

- EXAMPLE 1:

Consider the system $\begin{cases} x_1 + 2x_2 \quad + 5x_4 + 3x_5 = 1 \\ x_3 - 2x_4 + 7x_5 = 2 \\ x_6 = 3 \end{cases}$

$A\underset{\sim}{x} = \underset{\sim}{b}$

$$A = \begin{pmatrix} 1 & 2 & 0 & 5 & 3 & 0 \\ 0 & 0 & 1 & -2 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \underset{\sim}{b} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

$x_1 \; x_2 \; x_3 \; x_4 \; x_5 \; x_6$

- Write the variables underneath
  & circle the variables under leading 1s.
- Eliminate circled variables

$x_1 = 1 - 2x_2 - 5x_4 - 3x_5$

$x_2 = x_2$

$x_3 = 2 + 2x_4 - 7x_5$

$x_4 = x_4$

$x_5 = x_5$

$x_6 = 3$

Canonical Solution

$$\begin{pmatrix} 1 - 2x_2 - 5x_4 - 3x_5 \\ x_2 \\ 2 + 2x_4 - 7x_5 \\ x_4 \\ x_5 \\ 3 \end{pmatrix}$$

- EXAMPLE 2: (More typical)

$$S = \begin{cases} x_1 + x_2 + x_3 - x_4 - x_5 = 1 \\ x_1 + x_2 - x_3 - x_4 + x_5 = 1 \\ x_1 + x_2 + 3x_3 - x_4 - 3x_5 = 1 \end{cases}$$

$S = \{A\underset{\sim}{x} = \underset{\sim}{b}\}$ $\quad A = \begin{pmatrix} 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 3 & -1 & -3 \end{pmatrix} \quad \underset{\sim}{b} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

<u>Step 1.</u> Form augmented matrix $(A|b)$

$$(A|b) = \left(\begin{array}{ccccc|c} 1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 3 & -1 & 3 & 1 \end{array}\right)$$

<u>Step 2.</u> Perform row operations until I get to reduced row Echelon form.

$$\xrightarrow{\mathcal{E}(2,1,-1),\ \mathcal{E}(3,1;-1)} \left(\begin{array}{ccccc|c} 1 & 1 & 1 & -1 & -1 & 1 \\ 0 & 0 & -2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & -2 & 0 \end{array}\right) \xrightarrow{\mathcal{E}(3,2;1)} \left(\begin{array}{ccccc|c} 1 & 1 & 1 & -1 & -1 & 1 \\ 0 & 0 & -2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{D}(2;-\frac{1}{2})} \left(\begin{array}{ccccc|c} 1 & 1 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{\mathcal{E}(1,2;-1)} \left(\begin{array}{ccccc|c} 1 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$x_1 \ x_2 \ x_3 \ x_4 \ x_5$

<u>Step 3.</u> Write variables underneath & circle variables under leading 1

<u>Step 4.</u> Eliminate circled variables & write out canonical solution.

$$\begin{cases} x_1 + x_2 - x_4 = 1 \\ x_3 - x_5 = 0 \end{cases}$$

Canonical solution: $\begin{pmatrix} 1 - x_2 + x_4 \\ x_2 \\ x_5 \\ x_4 \\ x_5 \end{pmatrix}$

- EXAMPLE 3:

$$S = \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 1 \\ x_1 + 2x_2 + 3x_4 + 4x_4 + 5x_5 = 2 \\ x_1 - x_3 - 2x_4 - 3x_5 = 0 \end{cases}$$

Augmented matrix $(A|b) = \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 2 \\ 1 & 0 & -1 & -2 & -3 & 0 \end{array}\right) \xrightarrow[\mathcal{E}(3,1;-1)]{\mathcal{E}(2,1;-1)} \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 1 \\ 0 & -1 & -2 & -3 & -4 & -1 \end{array}\right)$

$$\xrightarrow{\mathcal{E}(3,2;1)} \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{\mathcal{E}(1,2;-1)} \left(\begin{array}{ccccc|c} 1 & 0 & -1 & -2 & -3 & 0 \\ 0 & 1 & 2 & 3 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$x_1 \ x_2 \ x_3 \ x_4 \ x_5$

$$\begin{cases} x_1 - x_3 - 2x_4 - 3x_5 = 0 \\ x_2 + 2x_3 + 3x_4 + 4x_5 = 1 \end{cases}$$

Canonical solution: $\begin{pmatrix} x_3+2x_4+3x_5 \\ 1-2x_3-3x_4-4x_5 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$

Mon. 17/10/16

MATH1201: Algebra I

Prof. Francis (Johnson)

EXAMPLE 4:

$$S=\begin{cases} x_1+x_2+x_3+x_4=1 \\ x_1+x_2-x_3+x_4=1 \\ x_1+x_2-x_3-x_4=1 \end{cases}$$

$A\underset{\sim}{x}=\underset{\sim}{b}$ $\qquad A=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$ $\qquad \underset{\sim}{b}=\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

augmented matrix $\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 \end{array}\right)$

$$\xrightarrow[\mathcal{E}(3,1;-1)]{\mathcal{E}(2,1;-1)} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & -2 & 0 \end{array}\right)$$

$$\xrightarrow[\mathcal{D}(3;-\frac{1}{2})]{\mathcal{D}(2;\frac{1}{2})} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[\mathcal{E}(3,2;1)]{\mathcal{E}(1,2;1)} \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{D}(2;-1)} \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{E}(1,3;-1)} \left(\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right) \text{ is in reduced form}$$

$\quad x_1 \; x_2 \; x_3 \; x_4$

- Write variables underneath & circle variables under leading 1^s.
- Eliminate

$$S'=\begin{cases} x_1+x_2 = 1 \\ x_3 = 0 \\ x_4 = 0 \end{cases}$$

※ If you start with 4 variables, you should end up with 4.

Canonical solution is $\begin{pmatrix} 1-x_2 \\ x_2 \\ 0 \\ 0 \end{pmatrix}$

All solutions obtained by letting x_2 vary.

1.5 Inverting a matrix

How to find the inverse of an invertible matrix?

- EXAMPLE: $A=\begin{pmatrix}0&0&1\\0&1&1\\-1&1&0\end{pmatrix}$ is a 3×3 matrix

Form "big augmented matrix" $(A|I_3)$ (3×6 matrix)

$$(A|I_3)=\left(\begin{array}{ccc|ccc}0&0&1&1&0&0\\0&1&1&0&1&0\\-1&1&0&0&0&1\end{array}\right)$$

Reduce: $\xrightarrow{\mathcal{P}(1,3)}\left(\begin{array}{ccc|ccc}-1&1&0&0&0&1\\0&1&1&0&1&0\\0&0&1&1&0&0\end{array}\right)$

$\xrightarrow{\mathcal{E}(1,2;-1)}\left(\begin{array}{ccc|ccc}-1&0&\boxed{-1}&0&-1&1\\0&1&\boxed{1}&0&1&0\\0&0&1&1&0&0\end{array}\right)$

$\xrightarrow[\mathcal{E}(1,3;1)]{\mathcal{E}(2,3;-1)}\left(\begin{array}{ccc|ccc}-1&0&0&1&-1&1\\0&1&0&-1&1&0\\0&0&1&1&0&0\end{array}\right)$

$\xrightarrow{\mathcal{D}(1;-1)}\left(\begin{array}{ccc|ccc}1&0&0&-1&1&-1\\0&1&0&-1&1&0\\0&0&1&1&0&0\end{array}\right)$

"$(A_3|I_3)\to(I_3|A^{-1})$"

Claim: $A^{-1}=\begin{pmatrix}-1&1&-1\\-1&1&0\\1&0&0\end{pmatrix}$

Check: $AA^{-1}=\begin{pmatrix}0&0&1\\0&1&1\\-1&1&0\end{pmatrix}\begin{pmatrix}-1&1&-1\\-1&1&0\\1&0&0\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$

- Why does this method work?

 - Prop: If A,B are invertible $n\times n$ matrices, then the product AB is invertible and $(AB)^{-1}=B^{-1}A^{-1}$

 Proof: $(AB)(B^{-1}A^{-1})=A(BB^{-1})A^{-1}$
 $=AI_nA^{-1}$
 $=AA^{-1}$
 $=I_n$

 NEVER write $A^{-1}=\frac{1}{A}$

 $(B^{-1}A^{-1})(AB)=B^{-1}(A^{-1}A)B$
 $=B^{-1}I_nB$
 $=B^{-1}B$
 $=I_n$ QED

 Note: reversal in order

 - Generalisation:

 If $A_N,A_{N-1},\cdots A_2,A_1$ are all invertible $n\times n$ matrices, then the product $A_NA_{N-1}\cdots A_2A_1$ is invertible and its inverse $(A_NA_{N-1}\cdots A_2A_1)^{-1}=A_1^{-1}A_2^{-1}\cdots A_{N-1}^{-1}A_N^{-1}$

Again, note reversal of order.

- Here's why this method works

✓ Start with an $n\times n$ matrix A

Form "big augmented matrix" $(A|I_n)$ ($n\times 2n$ matrix)

Now reduce.

✓ Every time I do a row operation, I multiply on the LEFT by invertible matrix.

✓ Start with $(A|I_n)$

After 1st operation $\to (X_1A|X_1)$ where X_1 is invertible

After 2nd operation $\to (X_2X_1A|X_2X_1)$ where X_2 & X_1 are invertible

$\vdots$

After N^{th} operation $\to (X_NX_{N-1}\cdots X_2X_1A|X_NX_{N-1}\cdots X_2X_1)$ and all x_i are invertible

✓ Suppose after N operations, the left hand side of the "big augmented matrix" is I_n, i.e.

$(X_NX_{N-1}\cdots X_2X_1A|X_NX_{N-1}\cdots X_2X_1) = (I_n|B)$

then $B = X_NX_{N-1}\cdots X_2X_1$

$(A|I_n) \rightsquigarrow (BA|B) = (I_n|B)$

$BA = I_n \Rightarrow B = A^{-1}$

✓ I should really check that $AB=I_n$, but as we'll see, if A,B are $n\times n$ and $BA=I_n$, then $AB=I_n$ (preview)

- EXAMPLE: $A=\begin{pmatrix}2&3\\1&2\end{pmatrix}$

$$(A|I_2)=\left(\begin{array}{cc|cc}2&3&1&0\\1&2&0&1\end{array}\right)\xrightarrow{\mathcal{P}(1,2)}\left(\begin{array}{cc|cc}1&2&0&1\\2&3&1&0\end{array}\right)\xrightarrow{\mathcal{E}(2,1;-2)}\left(\begin{array}{cc|cc}1&2&0&1\\0&-1&1&-2\end{array}\right)$$

$$\xrightarrow{\mathcal{E}(1,2;2)}\left(\begin{array}{cc|cc}1&0&2&-3\\0&-1&1&-2\end{array}\right)\xrightarrow{\mathcal{D}(2;-1)}\left(\begin{array}{cc|cc}1&0&2&-3\\0&1&-1&2\end{array}\right)$$

$\therefore A^{-1}=\begin{pmatrix}2&-3\\-1&2\end{pmatrix}$

Fri. 21/10/16

MATH1401: Algebra I

Prof. Francis Johnson

- EXAMPLE ①:

$A=\begin{pmatrix}2&3\\1&2\end{pmatrix}$

We know that $A^{-1}=\begin{pmatrix}2&-3\\-1&2\end{pmatrix}$

Start with $(A|I_n)=\left(\begin{array}{cc|cc}2&3&1&0\\1&2&0&1\end{array}\right)$

$$\xrightarrow{\mathcal{P}(1,2)} \left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 2 & 3 & 1 & 0 \end{array}\right)$$

Reduce & keep record

$$\xrightarrow{\mathcal{E}(2,1;-2)} \left(\begin{array}{cc|cc} 1 & 2 & 0 & 1 \\ 0 & -1 & 1 & -2 \end{array}\right)$$

$$\xrightarrow{\mathcal{E}(1,2;2)} \left(\begin{array}{cc|cc} 1 & 0 & 2 & -3 \\ 0 & -1 & 1 & -2 \end{array}\right)$$

$$\xrightarrow{\mathcal{D}(2;-1)} \left(\begin{array}{cc|cc} 1 & 0 & 2 & -3 \\ 0 & 1 & -1 & 2 \end{array}\right)$$

$\therefore \Delta(2;-1)E(1,2;2)E(2,1;-2)P(1,2)(A|I_2)$

$\downarrow$

$(I|\Delta(2;-1)E(1,2;2)E(2,1;-2)P(1,2)) = A^{-1}$

So I've written A^{-1} as a product of elementary invertible matrices.

So $A^{-1} = \Delta(2;-1)E(1,2;2)E(2,1;-2)P(1,2)$

So $A = P(1,2)^{-1}E(2,1;-2)^{-1}E(1,2;2)^{-1}\Delta(2;-1)^{-1}$

Note: reversal of order

$A = P(1,2)E(2,1;2)E(1,2;-2)\Delta(2;-1)$

Check: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$= \begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$= \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} = A$

- EXAMPLE ②: $A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 3 & 1 \\ 0 & -2 & -1 \end{pmatrix}$

1) Find A^{-1}

2.) Express A^{-1} as a product of elementary matrices.

3) Thereby, express A as a product.

1). $(A|I_n) = \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 1 & 3 & 1 & 0 & 1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 1 \end{array}\right)$

$$\xrightarrow{\mathcal{E}(2,1;-1)} \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[\mathcal{E}(3,2;2)]{\mathcal{E}(1,2;-2)} \left(\begin{array}{ccc|ccc} 1 & 0 & -2 & 3 & -2 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -2 & 2 & 1 \end{array}\right)$$

$$\xrightarrow[\mathcal{E}(2,3;-1)]{\mathcal{E}(1,3;2)} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 2 & 2 \\ 0 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & -2 & 2 & 1 \end{array}\right)$$

$A^{-1} = \begin{pmatrix} -1 & 2 & 2 \\ 1 & -1 & -1 \\ -2 & 2 & 1 \end{pmatrix}$

Check: $A^{-1}A = \begin{pmatrix} -1 & 2 & 2 \\ 1 & -1 & -1 \\ -2 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 0 \\ 1 & 3 & 1 \\ 0 & -2 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

2.) $A^{-1} = E(2,3;-1)E(1,3;2)E(3,2;2)E(1,2;-2)E(2,1;-1)$

3) $A = \underbrace{E(2,1;1)}_{} E(1,2;2) E(3,2;-2) \underbrace{E(1,3;-2)}_{} E(2,3;1)$

2^{nd} row, 1^{st} column is 1. 1^{st} row, 3^{rd} column is -2.

Check:

$$\underbrace{\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&2&0\\0&1&0\\0&0&1\end{pmatrix}}_{X}\underbrace{\begin{pmatrix}1&0&0\\0&1&0\\0&-2&1\end{pmatrix}\begin{pmatrix}1&0&-2\\0&1&0\\0&0&1\end{pmatrix}}_{Y}\underbrace{\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}}_{Z}$$

$$X = \begin{pmatrix}1&2&0\\1&3&0\\0&0&1\end{pmatrix} \quad Y = \begin{pmatrix}1&0&-2\\0&1&0\\0&-2&1\end{pmatrix} \quad Z = \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&-2\\1&3&-2\\0&-2&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix} = \begin{pmatrix}1&2&0\\1&3&1\\0&-2&-1\end{pmatrix}$$

※ If a matrix is not invertible, then after row operations, we'll get

$$\left(\begin{array}{cccc|c}1&0&0&\cdots&\cdots\\0&1&0&\cdots&\cdots\\ &\vdots& & &\\0&0&0&\cdots&\cdots\end{array}\right)$$

0^s row at the end

i.e. we cannot get I_n

Fri. 21/10/16 (continued)

MATH1401: Algebra I

Prof. Francis Johnson

Chapter 2. § Propositional Logic §

2·1 Truth Tables

① 'NOT': '$\neg$' (negation)

- p is a basic statement

e.g. p = 'It is raining.' then $\neg p$ = 'It is not raining.'

-

p	$\neg p$	$\neg\neg p$
T	F	T
F	T	F

called truth tables

- $\neg\neg p$ is the same as p $\boxed{\neg\neg p \equiv p}$

② 'AND': '$\wedge$' (conjunction)

- q = 'It is cold.' '$p \wedge q$' ≡ 'p and q'

Note: p & q are independent of each other

-

p	q	$p \wedge q$
T	T	T
	F	F
F	T	F
	F	F

③ 'OR':

- Exclusive 'or' / Latin 'aut'

-

p	q	$p \S q$
T	T	F
	F	T
F	T	T
	F	F

Johnson's notation ☺ ➡ We DON'T use it.

'either p or q, but not both'

- '$\vee$' (disjunction)

- Inclusive 'or' / Latin 'vel'

-

p	q	$p \vee q$
T	T	T
	F	T
F	T	T
	F	F

'either p or q, possibly both'

④ 'IMPLIES': '$\Rightarrow$' (implication)

- '$p \Rightarrow q$' ≡ 'if p, then q'
-

p	q	$p \Rightarrow q$
T	T	T
	F	F
F	T	T
	F	T

- Explanation:

p	q	$(\neg p) \vee q$	$\neg p$
T	T	T	F
	F	F	F
F	T	T	T
	F	T	T

So $\neg p \vee q$ has the same truth table as $p \Rightarrow q$

p	$\neg p$	$(\neg p) \vee p$
T	F	T
F	T	T

$p \Rightarrow q$ means raughly if p happens then q happens.

Since $(\neg p) \vee p$ is always true,

$p \Rightarrow q$ is true as long as q is true OR p is true.

- Say two statements are equivalent ('≡') when they have the same truth table.

2.2 Standard Identities

(I). $p \wedge q \equiv q \wedge p$
  . $p \vee q \equiv q \vee p$

} commutativity

(II). $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
  . $p \vee (q \vee r) \equiv (p \vee q) \vee r$

} associativity

(III). $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  equivalent to $p.(q+r) = pq + pr$
  . $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

} distributivity

(IV). $p \equiv p \wedge p$
  . $p \equiv p \vee p$

} idempotent

Proof of $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$:

p	q	r	$p\vee(q\wedge r)$ $\equiv$	$(p\vee q)\wedge(p\vee r)$	$p\vee q$	$p\vee r$	$q\wedge r$
T	T	T	T	T	T	T	T
		F	F	T	T	T	F
	F	T	T	T	T	T	F
		F	F	T	T	T	F
F	T	T	T	T	T	T	T
		F	F	F	T	F	F
	F	T	F	F	F	T	F
		F	F	F	F	F	F

same!

De Morgan's Laws

- How does 'negation' behave ?

$\neg(p\wedge q)\equiv(\neg p)\vee(\neg q)$
$\neg(p\vee q)\equiv(\neg p)\wedge(\neg q)$ } duality

Proof.

p	q	$p\wedge q$	$\neg(p\wedge q)$ $\equiv$	$(\neg p)\vee(\neg q)$	$\neg p$	$\neg q$
T	T	T	F	F	F	F
	F	F	T	T	F	T
F	T	F	T	T	T	F
	F	F	T	T	T	T

same!

p	q	$\neg(p\vee q)$	$(\neg p)\wedge(\neg q)$	$\neg p$	$\neg q$
T	T	F	F	F	F
	F	F	F	F	T
F	T	F	F	T	F
	F	T	T	T	T

same!

2.3 • How many signs do we need ? Switching between logical symbols

(1) $p\Rightarrow q \equiv (\neg p)\vee q$

$\neg p\Rightarrow q \equiv (\neg\neg p)\vee q \equiv p\vee q$

So $\boxed{p\vee q \equiv \neg p \Rightarrow q}$

(2) $\neg(p\wedge q) \equiv (\neg p)\vee(\neg q)$

$\neg\neg(p\wedge q) \equiv \neg(\neg p\vee\neg q)$

$p\wedge q \equiv \neg(p\Rightarrow\neg q)$

So $\boxed{p\wedge q \equiv \neg(p\Rightarrow\neg q)}$

(3) $p \wedge \neg q \equiv \neg(p \Rightarrow \neg\neg q)$

$\equiv \neg(p \Rightarrow q)$

So $\boxed{p \Rightarrow q \equiv \neg(p \wedge \neg q)}$

Mon. 24/10/16

MATH1401: Algebra I

Prof. Francis Johnson

- Propositional logic is logic of constant propositions.
- Recap (switching between logical symbols):

We can get by with just 2 signs: $\neg, \Rightarrow$ (✓)

$\neg, \vee$ (✓)

$\neg, \wedge$ (✓)

For example, if I just take $\neg, \Rightarrow$, then

$p \vee q \equiv \neg\neg p \vee q$

$\boxed{p \vee q \equiv \neg p \Rightarrow q}$

$p \wedge q \equiv \neg\neg p \wedge q$

$\equiv \neg(\neg p \vee \neg q)$

$\boxed{p \wedge q \equiv \neg(p \Rightarrow \neg q)}$

also called 'nand' sometimes

- In fact, we just need one sign. Historically called <u>Sheffer's Stroke Function</u>.

p	q	$p \mid q$	$p \mid (p \mid q)$	$p \Rightarrow q$
T	T	F	T	T
	F	T	F	F
F	T	T	T	T
	F	T	T	T

$\boxed{p \mid q \equiv \neg(p \wedge q)}$

$\boxed{p \mid (p \mid q) \equiv p \Rightarrow q}$

p	$p \mid p$
T	F
F	T

$\boxed{p \mid p \equiv \neg p}$

2.4 Proof by Contradiction

- $p \Rightarrow q \equiv (\neg p) \vee q$

$\equiv (\neg p) \vee (\neg\neg q)$

$\equiv (\neg\neg q) \vee (\neg p)$

$\boxed{p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)}$ ← principle of proof by contradiction

- ✓ $(\neg q) \Rightarrow (\neg p)$ is the <u>contrapositive</u> of $p \Rightarrow q$
  and they are equivalent (have the same truth table)
  ✓ $q \Rightarrow p$ is called <u>converse</u> of $p \Rightarrow q$
  $q \Rightarrow p \not\equiv p \Rightarrow q$
- <u>Def.</u> $\boxed{p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)}$ '$\Leftrightarrow$' $\equiv$ 'iff'
- $p, q, r, s \ldots$ are basic propositions that can be T or F.
  However, $p \wedge q \Rightarrow r$ is called a <u>composite proposition</u>.

<u>Def.</u> Composite propositions can be either
(I) always T tautology
(II) sometimes T, sometimes F contingent
(III) always F contradiction

eg. (I) $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$ tautology
(II) $p \wedge q \Rightarrow r$ contingent
since if p, q are F, r is T, true
if p, q are T, r is F. false
(III) $p \wedge (\neg p)$ contradiction

Note: <u>A contradiction is the same as the negation of a tautology.</u>
e.g. $p \vee (\neg p)$ is always T | $\neg(p \vee \neg p) \equiv \neg p \wedge \neg\neg p$
$\equiv p \wedge \neg p$ is always F

2.5 Valid Arguments

- e.g. a) If it is cold or raining, we shall stay inside.
  b) We are outside and it is not cold.
  c) Therefore, it is not raining.

✓ Is this argument valid?
✓ Let p be 'it is cold'
q be 'it is raining'
r be 'we are inside', then
✓ a) is $p \vee q \Rightarrow r$
b) is $(\neg r) \wedge (\neg p)$
The whole argument is then $\underbrace{(p \vee q \Rightarrow r) \wedge (\neg r) \wedge (\neg p)}_{LHS} \Rightarrow \neg q$

✓ Calculate truth table.

p	q	r	$p \vee q \Rightarrow r$	$(\neg r)\wedge(\neg p)$	LHS	$\neg q$	LHS $\Rightarrow \neg q$
T	T	T	T	F	F	F	T
		F	F	F	F	F	T
	F	T	T	F	F	T	T
		F	F	F	F	T	T
F	T	T	T	F	F	F	T
		F	F	T	F	F	T
	F	T	T	F	F	T	T
		F	T	T	T	T	T

- e.g.(2).

  a) $p \wedge q \Rightarrow r$

  b) $\neg r \wedge \neg p$

  The whole statement is $(p\wedge q \Rightarrow r) \wedge (\neg r) \wedge (\neg p) \Rightarrow \neg q$

p	q	r	$p\wedge q \Rightarrow r$	$(\neg r)\wedge(\neg p)$	LHS	$\neg q$	LHS $\Rightarrow \neg q$
T	T	T	T	F	F	F	T
		F	F	F	F	F	T
	F	T	T	F	F	T	T
		F	T	F	F	T	T
F	T	T	T	F	F	F	T
		F	T	T	T	F	F
	F	T	T	F	F	T	T
		F	T	T	T	T	T

This argument is not valid (because at least one line gives a false)

Fri. 28/10/16

MATH1401: Algebra I

Prof. Johnson

- Textbook: Notes on Logics by P.T. Johnstone

We have done logic of constant propositions. $\neg, \wedge, \vee, \Rightarrow$

2.6 Logic of Variable Propositions (Predicate Logic)

- $P(x)$ where x varies.
  - ✓ Suppose $x \in \{0,1\}$, $P(x) = 'x^2>0'$.
    In this case, $P(0)$ is false, but $P(1)$ is true.
  - ✓ Suppose $x \in \{0,1,2\}$, $P(x) = 'x^2>0'$
    $P(0)$ F $\quad$ $P(1)$ T $\quad$ $P(2)$ T
  - ✓ Suppose $x \in \{1,2\}$, $P(x) = 'x^2>0'$
    $P(1)$ T $\quad$ $P(2)$ T
- The values over which x is allowed to vary is called the domain (of discussion). Denoted by $\mathcal{D}$.
  - Then $P(x)$ is a statement about objects in $\mathcal{D}$.
  - We are allowed to use $\neg, \wedge, \vee, \Rightarrow$.
    Plus 2 new signs.
  - ✓ '$\forall$' Universal Quantifier ($\equiv$ 'for all')
    $(\forall x)P(x)$ means that for any value of x in $\mathcal{D}$, $P(x)$ is true.
  - ✓ '$\exists$' Existential Quantifier ($\equiv$ 'these exists')
    $(\exists x)P(x)$ means that for at least one x in $\mathcal{D}$, $P(x)$ is true.
- EXAMPLE:
  - ✓ $\mathcal{D} = \{0,1\}$
    Clearly, I can form $P(0)$ and I can form $P(1)$.
    $(\forall x)P(x)$, in this case, means $P(0) \wedge P(1)$.
    $(\exists x)P(x)$, in this case, means $P(0) \vee P(1)$.
  - ✓ $\mathcal{D} = \{0,1,2\}$
    $(\forall x)P(x)$, in this case, means $P(0) \wedge P(1) \wedge P(2)$
    $(\exists x)P(x)$, in this case, means $P(0) \vee P(1) \vee P(2)$

The Convention (for algebra)
$\mathbb{N} = \{0, 1, 2, \cdots\}$

  - ✓ Suppose $\mathcal{D} = \mathbb{N}$,
    $(\forall x)P(x) \sim P(0) \wedge P(1) \wedge P(2) \wedge P(3) \wedge \cdots \wedge P(n) \wedge P(n+1) \wedge \cdots$ formulae of ∞ length (infinite)
    $(\exists x)P(x) \sim P(0) \vee P(1) \vee P(2) \vee P(3) \vee \cdots \vee P(n) \vee P(n+1) \vee \cdots$
    We introduce '$\forall$', '$\exists$' predicator to avoid formulae of ∞ length.

2.6.1 <u>How to negate a quantifier?</u>

- Start with $\mathcal{D} = \{0,1\}$,
  $(\forall x)P(x) = P(0) \wedge P(1)$
  $\neg(\forall x)P(x) = \neg(P(0) \wedge P(1))$

$= \neg P(0) \vee \neg P(1)$

$= (\exists x) \neg P(x)$

✓ $\mathcal{D} = \{0,1,2\}$

$(\forall x) P(x) = P(0) \wedge P(1) \wedge P(2)$

$\neg(\forall x) P(x) = \neg P(0) \vee \neg P(1) \vee \neg P(2)$

$= (\exists x) \neg P(x)$

- First rule of negation

$$\boxed{\neg(\forall x) P(x) = (\exists x) \neg P(x)}$$

- Second rule of negation

$$\boxed{\neg(\exists x) P(x) = (\forall x) \neg P(x)}$$

e.g. $(\exists x) P(x) = P(0) \vee P(1)$

$\neg(\exists x) P(x) = \neg(P(0) \vee P(1))$

$= \neg P(0) \wedge \neg P(1)$

$\Rightarrow \neg(\exists x) P(x) = (\forall x) \neg P(x)$

2·6·2 Interchange of Order of Quantifiers

- The order in which quantifiers come is extremely important.

EXAMPLE: Suppose $\mathcal{D} = \{0,1\}$, $P(x,y) =$ '$x \neq y$'

Compare $(\forall x)(\exists y) P(x,y) \leftarrow$ TRUE

and $(\exists y)(\forall x) P(x,y) \leftarrow$ FALSE

✓ $(\exists y) P(x,y) = P(x,0) \vee P(x,1)$

$\therefore (\forall x)(\exists y) P(x,y) = (\forall x) [P(x,0) \vee P(x,1)]$

$= [P(0,0) \vee P(0,1)] \wedge [P(1,0) \vee P(1,1)]$

$= (F \vee T) \wedge (T \vee F)$

$= T \wedge T$

$= T$

✓ $(\forall x) P(x,y) = P(0,y) \wedge P(1,y)$

$\therefore (\exists y)(\forall x) P(x,y) = [P(0,0) \wedge P(1,0)] \vee [P(0,1) \wedge P(1,1)]$

$= [F \wedge T] \vee [T \wedge F]$

$= F \vee F$

$= F$

$$\boxed{\text{Axiom: } (\exists y)(\forall x) P(x,y) \Rightarrow (\forall x)(\exists y) P(x,y)}$$

- However, two quantifiers of same type commute.

i.e. $\boxed{\begin{array}{l}(\forall x)(\forall y)P(x,y) = (\forall y)(\forall x)P(x,y) \\ (\exists x)(\exists y)P(x,y) = (\exists y)(\exists x)P(x,y)\end{array}}$

MATH1201 Propositional Logic

Basic Propositions

1. Commutativity: $p \wedge q \equiv q \wedge p$

   $p \vee q \equiv q \vee p$

2. Associativity: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

   $p \vee (q \vee r) \equiv (p \vee q) \vee r$

3. Distributivity: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

   $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

4. Idempotent: $p \equiv p \wedge p$

   $p \equiv \quad p \vee p$

De Morgan Laws

1. duality: $\neg (p \wedge q) \equiv (\neg p) \vee (\neg q)$

   $\neg (p \vee q) \equiv (\neg p) \wedge (\neg q)$

2. $p \vee q \equiv \neg p \Rightarrow q$

   $p \wedge q \equiv \neg (p \Rightarrow \neg q)$

   $p \Rightarrow q \equiv \neg (p \wedge \neg q)$

Sheffers Stroke Function

$p | q \equiv \neg (p \wedge q)$

$p | (p | q) \equiv p \Rightarrow q$

$p | p \equiv \neg p$

Proof by Contradiction / iff

Contrapositive: $p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$

$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Logic of Variable Propositions

$\neg (\forall x) P(x) = (\exists x) \neg P(x)$

$\neg (\exists x) P(x) = (\forall x) \neg P(x)$

$(\exists y)(\forall x) P(x, y) \Rightarrow (\forall x)(\exists y) P(x, y)$

$(\forall x)(\forall y) P(x, y) \equiv (\forall y)(\forall x) P(x, y)$

$(\exists x)(\exists y) P(x, y) \equiv (\exists y)(\exists x) P(x, y)$

MATH1201 Propositional Logic

Basic Propositions

1. commutativity: $p \wedge q \equiv q \wedge p$
   $p \vee q \equiv q \vee p$

2. associativity: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
   $p \vee (q \vee r) \equiv (p \vee q) \vee r$

3. distributivity: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
   $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

4. idempotent: $p \equiv p \wedge p$
   $p \equiv p \vee p$

De Morgan Laws

1. $\neg (p \wedge q) \equiv (\neg p) \vee (\neg q)$ duality
   $\neg (p \vee q) \equiv (\neg p) \wedge (\neg q)$

2. $p \vee q \equiv \neg p \Rightarrow q$
   $p \wedge q \equiv \neg (p \Rightarrow \neg q)$
   $p \Rightarrow q \equiv \neg (p \wedge \neg q)$

Sheffer's Stroke Function

$p | q \equiv \neg (p \wedge q)$

$p | (p | q) \equiv p \Rightarrow q$

$p | p \equiv \neg p$

Proof by Contradiction / iff

$p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$ contrapositive

$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Logic of Variable Propositions

$\neg (\forall x) P(x) = (\exists x) \neg P(x)$

$\neg (\exists x) P(x) = (\forall x) \neg P(x)$

$(\exists y)(\forall x) P \Rightarrow (\forall x)(\exists y) P$

$(\forall x)(\forall y) P \equiv (\forall y)(\forall x) P$

$(\exists x)(\exists y) P \equiv (\exists y)(\exists x) P$

Fri. 28/10/16 (continued)

MATH1401: Algebra I

Prof. Johnson

Chapter 3 § Set Theory §

3.1 Sets

- '$\in$' : '$x \in A$' $\equiv$ 'x is a member of A' 'belongs to' / 'is a member of'

  ✓ Every set starts & ends with a curly bracket.

  e.g. $\{0,1,2,3,5,7\} = \{7,5,2,1,3,0\}$

  ① In a set, the order in which elements are written is NOT significant.

  Note: To stress order, use round brackets.

  e.g. $(0,1,2) \neq (2,1,0)$

  ② If A and B are sets, then $A=B$ iff $x \in A \Leftrightarrow x \in B$

  i.e. a set is determined by its members and nothing else.

  Two sets are the same if all of their elements are the same.

- '$\subset$' : ※ Do not confuse '$\in$' with '$\subset$'.

  ✓ Def. $B \subset A$ iff $x \in B \Rightarrow x \in A$, 'is a subset of'

  so $A=B$ iff $(A \subset B) \wedge (B \subset A)$

- EXAMPLE: $A = \{0, 1, \{0,1\}, \{0,2\}, \{2\}\}$

Question.	$0 \in A$	T	
	$\{0\} \in A$	F	$\leftarrow$ $\{0\}$ is not an element of A
	$2 \in A$	F	
	$\{2\} \in A$	T	$\leftarrow$ $\{2\}$ is an element of A
	$\{2\} \subset A$	F	$\leftarrow$ because $\{2\} \subset A$ iff $2 \in A$ but $2 \notin A \Rightarrow \{2\} \not\subset A$
	$\{\{2\}\} \subset A$	T	$\leftarrow$ because $\{2\} \in A \Rightarrow \{\{2\}\} \subset A$

Note. $\{0,1,1\} = \{0,1\}$

- To list elements of a set is quite naive.

More usually, we define sets by means of properties possessed by elements.

eg. $\{x \mid x \text{ is a TFL bus}\}$

✓ In general, $\left\{ \begin{array}{c|c} \text{typical} & \text{defined} \\ \text{element} & \text{property} \end{array} \right\}$

e.g. $\{x \in \mathbb{R} \mid x^2 > 3\}$

✓ $A = \{x \mid P_A(x)\}$ where P_A is the defining property of A.

Note. $\boxed{\{x \in \mathbb{R} \mid x^2 < 0\}}$ is an example of an <u>empty set</u>.
Notation: $\emptyset$

So if you're defining sets by properties, you will inevitably get an empty set.

Note: $\emptyset \subset A \quad \forall A$

✓ $|A|$ = number of elements in A

Note: $X = \{\emptyset\}$ is <u>non-empty</u>, since $\emptyset \in X$

so $0 = |\emptyset| \Rightarrow$ <u>0 is natural</u>

3.2 Predicates of Sets

- $A = \{x \mid P_A(x)\}$

  $B = \{x \mid P_B(x)\}$

✓ Union: $\boxed{A \cup B = \{x \mid P_A(x) \vee P_B(x)\}}$ i.e. $A \cup B$ consists of those elements that are in A or in B.

$P_{A \cup B}(x) = P_A(x) \vee P_B(x)$

✓ Intersection: $\boxed{A \cap B = \{x \mid P_A(x) \wedge P_B(x)\}}$

✓ Difference: $\boxed{A - B = \{x \mid P_A(x) \wedge \neg P_B(x)\}}$ i.e. $A - B$ consists of those elements which are in A but not in B.

$P_{A-B} = P_A(x) \wedge \neg P_B(x)$

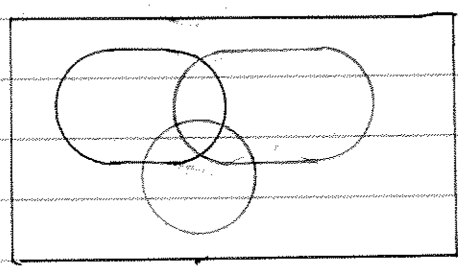
Note: Union / Intersection / Difference of sets ≡ another <u>set</u>.

- <u>Venn Diagram</u>

  A (black) B (red) C (green)

   $\equiv A \cap B$  $\equiv A \cap B \cap C$

   $\equiv C - A \cup B$

  Note: disadvantage = cannot represent ≥ 4 sets because 4 sets requires 3D.

- <u>Direct Product of Sets</u>

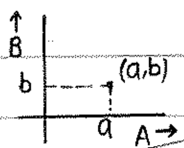
  ✓ Formally, $(a,b) = (a',b')$ iff $a = a'$ <u>AND</u> $b = b'$ called 'ordered pair'.

  so $(a,b) = (b,a)$ iff $a = b$

  ✓ $A = \{x \mid P_A(x)\}$

  $B = \{x \mid P_B(x)\}$

  $\boxed{A \times B = \{(x,y) \mid P_A(x) \wedge P_B(y)\}}$

  1st element from 1st set (A)

  2nd element from 2nd set (B)

  In general, $\boxed{B \times A \neq A \times B}$

e.g. $A = \{0,1,2\}$, $B = \{0,1,2,3\}$

$$\begin{array}{ccc}
(0,3) & (1,3) & (2,3) \\
(0,2) & (1,2) & (2,2) \\
(0,1) & (1,1) & (2,1) \\
(0,0) & (1,0) & (2,0)
\end{array}$$

✓ $|A|$ = card of A = number of elements in A

$$\boxed{|A \times B| = |A| . |B|}$$

- Which of the following is a function?

$$\left.\begin{array}{l} f(x) = x+1 \\ g(x) = \dfrac{1}{x+1} \\ h(x) = \sqrt{x+1} \end{array}\right\} \text{These are formulae.}$$

Mon. 31/10/16

MATH1201: Algebra I

Prof. Johnson

3.3 Mappings (Functions)

3.3.1 <u>What are mappings?</u>

- Informal Def.

  Let A, B be sets.

  By a mapping / function

$$f : \underset{\text{domain of } f}{A} \rightarrow \underset{\text{codomain of } f}{B}$$

  we mean a rule which assigns to each $a \in A$ a single element $f(a) \in B$.

EXAMPLE:

$A = B = \mathbb{Q}$ (rationals)

✓ could take as my rule $f(a) = a+1$

✓ whereas for $g(a) = \frac{1}{a+1}$, this isn't going to work

✓ However, if I take $A = \mathbb{Q} - \{1\}$, ← means A contains all rationals but 1

then $g : \mathbb{Q} - \{1\} \rightarrow \mathbb{Q}$

$g(a) = \frac{1}{a+1}$ is a mapping.

✓ Take $A = \{x \in \mathbb{R} \mid x \geq -1\}$, then

$h : A \rightarrow \mathbb{R}$

$h(x) = +\sqrt{x+1}$

Note. $\cancel{h: \mathbb{C} \to \mathbb{C}}$ ← This example is related to Riemann Surface.

$\cancel{h(x) = \sqrt{x+1}}$

- <u>Composition of mappings</u>:

Let A, B, C be sets.

$f: A \to B$ $\quad\quad$ $g: B \to C$

Therefore, $g \circ f: A \to C$ is the mapping

$\boxed{(g \circ f)(a) = g(f(a))}$ Composition

circle

✓ EXAMPLE:

$f: \mathbb{R} \longrightarrow \mathbb{R}$ $\quad\quad$ $g: \mathbb{R} \longrightarrow \mathbb{R}$

$f(x) = x^2+1$ $\quad\quad$ $g(x) = \cos x$

$(g \circ f)(x) = \cos(x^2+1)$

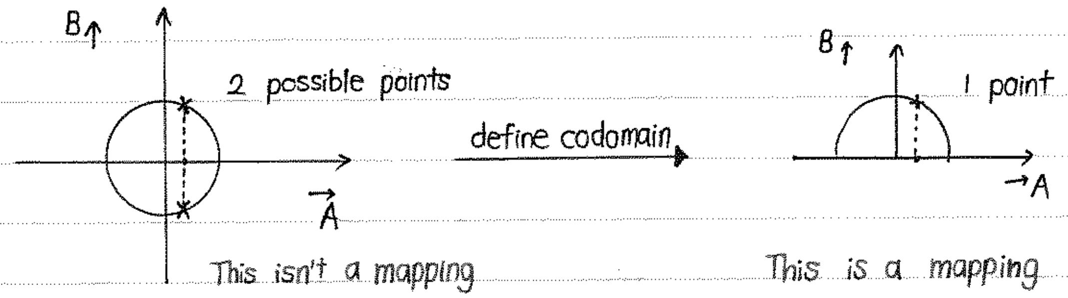
where $(f \circ g)(x) = \cos^2 x + 1$

Are they the same ?

$(g \circ f)(0) = \cos 1 < 1$

$(f \circ g)(0) = 2$

$f \circ g \neq g \circ f$



This isn't a mapping $\quad\quad$ This is a mapping

✓ Composition is associative.

$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$

Then $h \circ g: B \to D$ $\quad\quad$ $g \circ f: A \to C$

$(h \circ g) \circ f: A \to D$ $\quad\quad$ $h \circ (g \circ f): A \to D$

Preposition: $\boxed{h \circ (g \circ f) = (h \circ g) \circ f}$

Proof: Let $a \in A$

$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$

$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$ $\quad\quad$ QED

- <u>Identity mapping</u>

A set

$$\boxed{\begin{array}{l} Id_A : A \to A \\ Id_A(a) = a \quad \forall\, a \in A \end{array}}$$

'Id_A' ≡ 'I_A' ≡ 'Id'

- <u>Invertible mapping</u>

  Suppose A, B are sets and $f: A \to B$ is the mapping,

  We say that f is invertible where there exists mapping $g: B \to A$

  $$A \xrightarrow{f} B \xrightarrow{g} A \xrightarrow{f} B$$

  such that $\boxed{\begin{array}{l} g \circ f = Id_A \\ f \circ g = Id_B \end{array}}$ and

  If this is the case, we say that g is inverse mapping to f.

  Notation: $g = f^{-1}$ Note: $f^{-1} \neq \frac{1}{f}$

✓ EXAMPLE ①.

$f: \mathbb{R} \to \mathbb{R}$

$f(x) = 2x+1$

Q. Is f invertible? If so, what is f^{-1}?

$g(x) = \frac{x-1}{2}$

$$(f \circ g)(x) = f\left(\frac{x-1}{2}\right) = 2\left(\frac{x-1}{2}\right) + 1 = x$$

$$(g \circ f)(x) = \frac{(2x+1)-1}{2} = \frac{2x}{2} = x$$

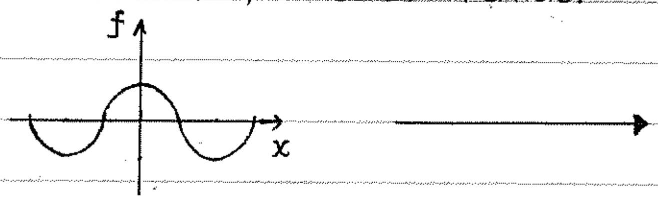
$\Rightarrow f^{-1}(x) = \frac{x-1}{2}$

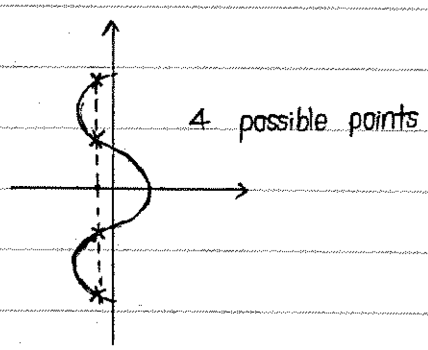
✓ EXAMPLE ②:

$f: \mathbb{R} \to \mathbb{R}$

$f(x) = \cos x$

In this case, f is not invertible.





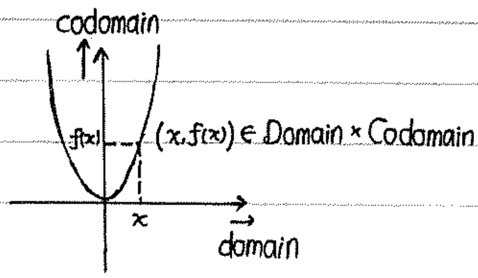
We'll deal with this formally very soon.

- <u>Formal Def.</u>

  ✓ Graph of a mapping.

  $f: \mathbb{R} \to \mathbb{R}$

  $f(x) = x^2$



✓ Formal Def.

Let A, B be sets.

By a mapping $f: A \to B$, I mean a subset

$$f \subset A \times B$$

with the following properties:

1) $\forall a \in A, \exists b \in B$ s.t. $(a, b) \in f$

(I then write $b = f(a)$) $\longrightarrow$ It is defined.

2) $\forall a \in A$, $(a, b) \in f$ and $(a, b') \in f$

$\Rightarrow b = b'$ $\longrightarrow$ There is only one point. (one-to-one)

✓ $f: A \to B$

Suppose I have an inverse $f^{-1}: B \to A$.

$f^{-1} \subset B \times A$

I)' $\forall b \in B, \exists a \in A$ s.t. $ba \in f^{-1}$

II)' $\forall b \in B, (b, a) \in f^{-1} \mid (b, a') \in f^{-1} \Rightarrow a = a'$

Question. Given a mapping $f: A \to B$.

What do I need to check before I can conclude that f is invertible?

3.3.2 Injectivity, Surjectivity and Bijectivity

① Injectivity: '单射函数'

Say that $f: A \to B$ is injective when given $a, a' \in A$,

$\boxed{f(a) = f(a') \Rightarrow a = a'}$ 'one-to-one'

✓ EXAMPLE ①:

$f: \mathbb{Q} \to \mathbb{Q}$

$f(x) = 2x + 1$

Then f is injective because

$f(x) = f(x') \Rightarrow 2x + 1 = 2x' + 1$

$x = x'$

✓ EXAMPLE ②:

$g: \mathbb{Q} \to \mathbb{Q}$

$g(x) = x^2 + 1$

Is g injective?

$g(1) = 2 = g(-1) = 2$

BUT $1 \neq -1 \Rightarrow$ not injective

Fri. 04/11/16

MATH1201: Algebra I

Prof. Johnson

② Surjectivity: 「满射函数」

We say that f is surjective when

$$\boxed{\forall b \in B,\ \exists a \in A \text{ s.t. } b = f(a)}$$

✓ Informally, surjectivity means every element of codomain is hit by something in the domain.

✓ EXAMPLE: $f: \mathbb{R} \to \mathbb{R}$

$f(x) = 2x+1$ is surjective.

Let $y \in \mathbb{R}$.

Then, we need to write $y = 2x+1$

$x = \frac{y-1}{2}$ — x in terms of y

$\therefore \forall y \in \mathbb{R},\ \exists x = \frac{y-1}{2}$ s.t. $f(x) = y$

• Recall: $f: A \to B$ is invertible when $\exists$ mapping $g: B \to A$ s.t. $g \circ f = Id_A$ and $f \circ g = Id_B$

<u>Prop.</u> Let $f: A \to B$ be invertible, then

1) f is injective and

2) f is surjective

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

Proof:

1.) Let $g: B \to A$ s.t. $g \circ f = Id_A$ and $f \circ g = Id_B$

Suppose $f(a) = f(a')$,

apply g to both sides: $g(f(a)) = g(f(a'))$

$(g \circ f)(a) = (g \circ f)(a')$

$Id_A(a) = Id_A(a')$

$a = a'$ QED

2) Let $b \in B$, put $a = g(b)$

$f(a) = f(g(b)) = (f \circ g)(b) = Id_B(b) = b$

$\Rightarrow f$ is surjective QED

③ Bijectivity

A mapping f is said to be bijective when it is both injective and surjective.

- Def. So by the previous example, I've shown that

  An invertible mapping is bijective.

- In fact, the converse is also true.

$p \Rightarrow q$

'converse'

$\equiv$

$q \Rightarrow p$

✓ Recall: $\boxed{\begin{array}{l} f: A \to B \text{ is a mapping} \\ \Leftrightarrow f \subset A \times B \text{ s.t.} \\ \text{I) } \forall a \in A, \exists b \in B, (a,b) \in f \\ \text{II) If } (a,b) \in f \text{ and } (a,b') \in f \\ \quad \Rightarrow b = b' \end{array}}$

✓ So if $f \subset A \times B$,

we define $f^{-1} \subset B \times A$ ← Note: this definition does not yet assume f is mapping.

$\Leftrightarrow f^{-1} = \{(b,a) \mid (a,b) \in f\}$

$f \subset A \times B$	$f^{-1} \subset B \times A$
I) $\forall a \in A, \exists b \in B$ s.t $(a,b) \in f$	I)' $\forall a \in A, \exists b \in B$ s.t $(b,a) \in f^{-1}$ ← implies f^{-1} is surjective
II) $(a,b) \in f$ and $(a,b') \in f \Rightarrow b = b'$	II)' $(b,a) \in f^{-1}$ and $(b',a) \in f^{-1} \Rightarrow b = b'$ ← implies f^{-1} is injective
III) $(a,b) \in f$ and $(a',b) \in f \Rightarrow a = a'$	III)' $(b,a) \in f^{-1}$ and $(b,a') \in f^{-1} \Rightarrow a = a'$
IV) $\forall b \in B, \exists a \in A$ s.t. $(a,b) \in f$	(IV)' $\forall b \in B, \exists a \in A$ s.t. $(b,a) \in f^{-1}$

Note: I), II) are conditions for f to be a mapping.

III) is the condition for f to be injective.

IV) is the condition for f to be surjective.

WHILE

III)', IV)' are conditions for f^{-1} to be a mapping.

✓ So if f satisfies I), II), III) & IV), then

f^{-1} satisfies I)', II)', III)' & IV)'

$\Rightarrow f^{-1}$ is a mapping and also f^{-1} is bijective

- Th. I) Let $f: A \to B$ be a mapping, then

  f is invertible $\Leftrightarrow$ f is bijective

II) If that is the case, then

f^{-1} is also a bijective mapping.

- <u>Prop.</u> Let $\left.\begin{array}{l} f: A \to B \\ g: B \to C \end{array}\right\}$ mappings

If f, g are invertible / bijective, then

$g \circ f$ is also invertible / bijective.

Proof:

If f, g are invertible with inverses f^{-1}, g^{-1},

$$A \underset{f^{-1}}{\overset{f}{\rightleftarrows}} B \underset{g^{-1}}{\overset{g}{\rightleftarrows}} C$$

$$\begin{aligned}
(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\
&= f^{-1} \circ Id_B \circ f \\
&= f^{-1} \circ f \\
&= Id_A
\end{aligned}$$

$$\begin{aligned}
(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\
&= g \circ Id_B \circ g^{-1} \\
&= g \circ g^{-1} \\
&= Id_C
\end{aligned}$$

QED

Notice that

$\boxed{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$ reversal of order !

3.4 Permutations

- $f: \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ mappings

If $n = 3 = m$, Identity permutation

$Id \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}$

$\begin{pmatrix} 1 \to 1 \\ 2 \searrow\nearrow 2 \\ 3 \quad\; 3 \end{pmatrix}$ can be written as $\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$

- <u>Def.</u> A permutation on n letters is a bijective mapping

$\boxed{f: \{1, \cdots, n\} \to \{1, \cdots, n\}}$

Convention: $f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$

e.g. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$

means $f(1) = 5$

$f(2) = 3$

$f(3) = 4$

$f(4) = 1$

$f(5) = 2$

- Composition of permutation:

$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$ $\qquad g = \begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix}$

e.g. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$

How to calculate $g \circ f$?

$\overleftarrow{g \circ f} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cancel{5} & \cancel{3} & \cancel{4} & \cancel{1} & \cancel{2} \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} \begin{matrix} \downarrow f \\ \downarrow g \end{matrix}$ $\qquad f$ come 1^{st}, g comes 2^{nd}

Then cross out the middle line (row)

i.e. $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$

How to calculate f^{-1} ?

$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$ $\qquad$ 'upside-down'

sigma

- $\sigma_n = \{ f : \{1, \cdots, n\} \to \{1, \cdots, n\} \}$, f is bijective

σ_n is the self of permutations on n letters

$|\sigma_n| = n!$

This is because $f(n)$ has n possibilities

$f(n-1)$ $\cdots$ $(n-1)$ $\cdots$

$\vdots$ $\qquad$ $\vdots$

$f(1)$ $\cdots$ 1 $\cdots$

3.4.1 Cyclic Permutations

e.g. $f(1)=3$, $f(3)=5$, $f(5)=4$, $f(4)=1$ can be written as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$

Shorthand: $(1,3,5,4)$ goes to

leave out 2 since $f(2)=2$

- Formal Def.

Let $a_1, a_2, \cdots, a_n \in \{1, \cdots, n\}$,

By the cycle $(a_1, a_2, \cdots, a_m)$,

$$(a_1, a_2, \cdots, a_m)(a_1) = a_2$$

$$(a_1, a_2, \cdots, a_m)(a_2) = a_3$$

$$\vdots \qquad \vdots$$

$$(a_1, a_2, \cdots, a_m)(a_{m-1}) = a_m$$

$$(a_1, a_2, \cdots, a_m)(a_m) = a_1$$

$$(a_1, a_2, \cdots, a_m)(x) = x \quad \text{if} \quad x \notin \{a_1, a_2, \cdots, a_m\}$$

✓ $\{a_1, a_2, \cdots, a_m\}$ is called support of the cycle

$C = (a_1, a_2, \cdots, a_n)$ is called a cycle of length n

✓ Def.

If $s \in \sigma_n$, then the order of s is the smallest integer $n \geq 1$ s.t.

$$\underbrace{s \circ s \circ \cdots \circ s}_{n} = Id$$

$$s^n = Id$$

* EXAMPLE: $s = (1,3,7)$ ← a shorthand

by def.

Then $\boxed{s(1)=3, \ s(3)=7, \ s(7)=1}$, $s(x)=x$ otherwise

$s^2(1)=7$, $s^2(3)=1$, $s^2(7)=3$, $s^2(x)=x$ otherwise

$s^3(1)=1$, $s^3(3)=3$, $s^3(7)=7$, $s^3(x)=x$ otherwise

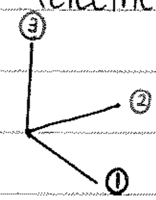
In this case, the order of s is 3.

*The order of cyclic permutation $(a_1, a_2, \cdots a_m)$ is simply m.

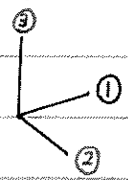
i.e. The order of a cyclic permutation is the length of the cycle.

✓ Applications:

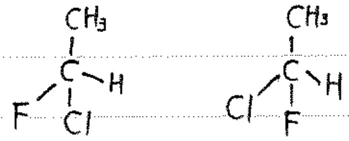
* Physics: Fleming's Right-hand Rule: (electric generators)



Fleming's Left-hand Rule: (electric motors)



$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

* Chemistry:  stereoisomer '立体异构'

3·4·1 Transposition

- Def. A transposition is a cycle of length 2.

e.g. $\tau = (3,5)$ ⟵ shorthand

$$(3,5)(x) = \begin{cases} 5 & x = 3 \\ 3 & x = 5 \\ x & x \notin \{3,5\} \end{cases}$$

$\tau^2 = Id$

✓ Prop. Any cycle is a product of transpositions.

Proof:

$C = (a_1, a_2, \cdots, a_m)$

$C = (a_1, a_m) \cdots (a_1, a_3)(a_1, a_2)$ QED

$$\left(\begin{array}{cccccc} a_1 & a_2 & a_3 & \cdots & a_{m-1} & a_m \\ a_2 & a_1 & a_3 & \cdots & a_{m-1} & a_m \\ a_2 & a_3 & a_1 & \cdots & a_{m-1} & a_m \\ & & & \vdots & & \\ a_2 & a_3 & a_4 & \cdots & a_1 & a_m \\ a_2 & a_3 & a_4 & \cdots & a_m & a_1 \end{array}\right) \begin{array}{l} \\ (a_1, a_2) \\ (a_1, a_3) \\ \\ (a_1, a_{m-1}) \\ (a_1, a_m) \end{array}$$

- In fact,

A cycle of length m is a product of $(m-1)$ transpositions.

✓ sign (of) transposition $= -1$

sign (of) cycle of length $m = (-1)^{m-1}$

i.e. a cycle of even length has sign -1

a cycle of odd length has sign 1

3·4·2 Disjoint Cycles

- Def.

We say two cycles

$C_1 = (a_1, a_2, a_3, \cdots, a_m)$
$C_2 = (b_1, b_2, b_3, \cdots, b_k)$ are disjoint

when $\{a_1, a_2, \cdots, a_m\} \cap \{b_1, b_2, \cdots, b_k\} = \emptyset$

e.g. $(1,3,7)$ & $(2,5,9,4)$ are disjoint.

- <u>Prop.</u> If C_1 and C_2 are disjoint cycles, then

$$C_1C_2 = C_2C_1$$

- <u>Th.</u> Any permutation can be written (uniquely up to order) as a product of disjoint cycles.

EXAMPLE ①:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 5 & 9 & 7 & 3 & 10 & 8 & 1 & 2 & 12 & 6 & 11 \end{pmatrix}$$

$\sigma = \underbrace{(1,4,7,8)}_{4}(2,5,3,9)\underbrace{(6,10,12,11)}_{4}$ <u>shorthand</u>

sign = $(-1)(-1)(-1) = (-1)^3 = -1$

order = 4

EXAMPLE ②:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 5 & 9 & 7 & 3 & 10 & 8 & 1 & 2 & 13 & 6 & 11 & 14 & 13 \end{pmatrix}$$

$\sigma = \underbrace{(1,4,7,8)}_{4}(2,5,3,9)\underbrace{(6,10,13,14,12,11)}_{6}$

sign = $(-1)^3 = -1$

'最小公倍数'

order = 12 ← lowest common multiples of the order of disjoint cycles.

In this case, 4 and 6 ⇒ lowest common multiple = 12

Note: { Laplace's Theorem

Any transposition is a product of an add no. of adjacent transpositions.

see "Chapter 7. Basis Theorem"

Mon. 14/11/16

MATH1201 Algebra I

Prof. Johnson

Chapter 4. § Fields and Vector Spaces §

4.1 Fields

- $\mathbb{N} = \{0, 1, 2, \cdots, n, n+1, \cdots\}$

  ✓ cardinals of finite sets 'cardinal' ≡ '基数'

  ✓ can $\begin{cases} \text{add} \\ \text{multiply} \end{cases}$, but cannot always $\begin{cases} \text{subtract} \\ \text{divide} \end{cases}$

$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots, \pm n, \pm(n+1), \cdots\}$

✓ can add, subtract, multiply, but cannot always divide (by non-zero)

$\mathbb{Q} = \{\frac{p}{q}, \ p, q \in \mathbb{Z}, q \neq 0\}$ rationals

✓ rule of equality: $\frac{p}{q} = \frac{p'}{q'} \Rightarrow pq' = p'q$

✓ $\mathbb{Q}$ is the first example of a field.

- Def.

域 By a field $\mathbb{F}$, I mean a 5-tuple $\mathbb{F} = (\mathbb{F}, +, \cdot, 0, 1)$ where

(i) $\mathbb{F}$ is a set

(ii) $0, 1 \in \mathbb{F}$, $0 \neq 1$

(iii) $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ (means + is a mapping)

Write $a + b \equiv +(a, b)$

(iv) $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

Write $a \cdot b = \cdot(a, b)$

An n-tuple is a (ordered) sequence of n elements

- These must satisfy the following rules.

✓ Additive Axioms

I) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{F}$ associativity

II) $a + 0 = a = 0 + a \quad \forall a \in \mathbb{F}$ 0 is an additive identity

III) $\forall a \in \mathbb{F}, \exists (-a) \in \mathbb{F}$ s.t. additive inverse

$a + (-a) = 0 = (-a) + a$

IV) $\forall a, b \in \mathbb{F}, \ a + b = b + a$ commutativity

✓ Multiplicative Axioms

I)' $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{F}$ associativity

II)' $a \cdot 1 = 1 \cdot a = a \quad \forall a \in \mathbb{F}$ 1 is a multiplicative identity

III)' $a \cdot a^{-1} = 1 = a^{-1} \cdot a \quad \forall a \in \mathbb{F},\ a \neq 0$ multiplicative inverses

IV)' $\forall a, b \in \mathbb{F},\ a \cdot b = b \cdot a$ commutativity

✓ Distributive Axioms

$a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{F}$

$(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in \mathbb{F}$

e.g. 1) $\mathbb{Q}$ is a field

2) $\mathbb{R}$ is also a field

3) $\mathbb{C}$ is a field

4.1.1 Finite fields

• ✓ $\mathbb{F}_2$ arithmetic mod 2 ← modulus arithmetic 同余

- $\mathbb{F}_2 = \{\text{even}, \text{odd}\}$

$+ : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$

+	even	odd
even	even	odd
odd	odd	even

$\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$

·	even	odd
even	even	even
odd	even	odd

- In future, we write

$0 \equiv$ even

$1 \equiv$ odd

i.e. $\mathbb{F}_2 = \{0, 1\}$ a field with 2 elements

Thus,

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

(Addition mod 2)

✓ $\mathbb{F}_3$ arithmetic mod 3

$\mathbb{F}_3 = \{0, 1, 2\}$ ← possible remainders mod 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

e.g. $7 + 5 = 12 \equiv 0$

$7 \div 3$: remainder 1; $5 \div 3$: remainder 2; $12 \div 3$: no remainder

e.g. $5 \times 8 = 40 \equiv 1$

$5 \div 3$: remainder 2; $8 \div 3$: remainder 2; $40 \div 3$: remainder 1

✓ $\mathbb{F}_5$ arithmetic mod 5

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$2^{-1} = 3 \mod 5$

$4^{-1} = 4 \mod 5$

e.g. $4+4 = 8 \equiv 3$

e.g. $3 \cdot 4 = 12 \equiv 2$

$\mathbb{F}_5$ is a field

✓ $\mathbb{Z}_4$ arithmetic mod 4

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

NOT a field

because 2 has no multiplicative inverse

✓ When is arithmetic mod a field ?

$\Leftrightarrow$ n is prime (Gauss)

Fri. 18/11/16

MATH1201: Algebra I

Prof. Johnson

4·1·2 Quadratic Fields

- Let $\mathbb{F}$ be a field which you understand, e.g. take $\mathbb{F} = \mathbb{Q}$ / $\mathbb{F} = \mathbb{R}$,

  If $\alpha \in \mathbb{F}$, ask:

  does the eqn $x^2 = \alpha$ have a solution in $\mathbb{F}$?

  e.g. $\mathbb{F} = \mathbb{R}$, $x^2 = -1$ has no solution in $\mathbb{R}$.

✓ Informal Idea:

- Construct a new element $\sqrt{\alpha}$.

- Consider expressions $x_1 + x_2\sqrt{\alpha}$: $x_i \in \mathbb{F}$
- Add & multiply in usual way.

① $(x_1 + x_2\sqrt{\alpha}) + (y_1 + y_2\sqrt{\alpha}) = (x_1 + y_1) + (x_2 + y_2)\sqrt{\alpha}$

② $(x_1 + x_2\sqrt{\alpha}) \cdot (y_1 + y_2\sqrt{\alpha}) = (x_1 y_1 + x_2 y_2 \alpha) + (x_1 y_2 + x_2 y_1)\sqrt{\alpha}$

③ zero: $0 = 0 + 0\sqrt{\alpha}$

$1 = 1 + 0\sqrt{\alpha}$

$(1 + 0\sqrt{\alpha})(x_1 + x_2\sqrt{\alpha}) = x_1 + x_2\sqrt{\alpha} \longrightarrow$ This implies 1 is an identity

✓ Do inverses exist?

- Trick: $(x_1 + x_2\sqrt{\alpha})(x_1 - x_2\sqrt{\alpha}) = x_1^2 - x_2^2\alpha + 0$

[Need to know that $x_1^2 - x_2^2\alpha \neq 0$.
Otherwise, $x_1^2 = x_2^2\alpha \Rightarrow \left(\frac{x_1}{x_2}\right)^2 = \alpha$
Contradiction.]

$$(x_1 + x_2\sqrt{\alpha})\left(\frac{x_1}{x_1^2 - x_2^2\alpha} + \frac{x_2}{x_1^2 - x_2^2\alpha}\sqrt{\alpha}\right) = 1$$

$x_1 - x_2\sqrt{\alpha}$ is called the <u>conjugate</u> to $x_1 + x_2\sqrt{\alpha}$.

- If you guarantee that $x_1^2 - x_2^2\alpha \neq 0$, when $(x_1, x_2) \neq (0,0)$, then you get a field called $\boxed{\mathbb{F}(\sqrt{\alpha})}$

Construct $\sqrt{\alpha}$ as follows.

<u>Formal Def.</u>

$F(\sqrt{\alpha}) = \mathbb{F} \times \mathbb{F}$

① Addition $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$

zero $0 = (0, 0)$

Think $\boxed{\begin{array}{l} x_1 + x_2\sqrt{\alpha} = (x_1, x_2) \\ \text{so } 1 = (1, 0) \\ \sqrt{\alpha} = (0, 1) \end{array}}$

② Multiplication $\boxed{(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1 + x_2 y_2 \alpha,\ x_1 y_2 + x_2 y_1)}$

$(0,1) \cdot (0,1) = (\alpha, 0) = \alpha(1, 0) = \alpha \cdot 1$

✓ EXAMPLE ①:

$\mathbb{F} = \mathbb{R}$, $\alpha = -1$

'$x^2 = \alpha$ has no solution in $\mathbb{F}$'
$\Downarrow$
'$\mathbb{F}(\sqrt{\alpha})$ is a field'

$x^2 = -1$ has no solution in $\mathbb{R}$.

So $\mathbb{R}(\sqrt{-1})$ is a field.
$\quad\ \ \ \|$
$\quad\ \ \mathbb{C}$

✓ EXAMPLE ②:

$$\mathbb{F} = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

$0^2 = 0$

$1^2 = 1$

$2^2 = \boxed{4 = -1}$ → This is because $4+1=0$, $4=-1$

$3^2 = 4 = -1$

$4^2 = 1$

$x^2 = 2$ has <u>no solution</u> in $\mathbb{F}_5$.

So $\mathbb{F}_5(\sqrt{2})$ <u>is a field</u> with <u>25 elements</u>

since $\mathbb{F}_5 = \underbrace{\mathbb{F}_5}_{5 \text{ elements}} \times \underbrace{\mathbb{F}_5}_{5 \text{ elements}}$

4.2 Vector Spaces

• Def.

Fix a field. (eg. $\mathbb{F} = \mathbb{Q}$)

By a vector space V over $\mathbb{F}$, I mean a 4-tuple $V = (V, +, \underline{0}, \cdot)$ where

1) V is a set

2) $\underline{0} \in V$

3) $+ : V \times V \to V$ mapping

$\underline{v} + \underline{w} = +(\underline{v}, \underline{w})$ addition

4) $\cdot : \mathbb{F} \times V \to V$ mapping

$\lambda \cdot \underline{v} = \cdot(\lambda, \underline{v})$ scalar multiplication

s.t. the following rules are held:

I) $\underline{u} + (\underline{v} + \underline{w}) = (\underline{u} + \underline{v}) + \underline{w} \quad \forall \underline{u}, \underline{v}, \underline{w} \in V$ associative

II) $\underline{u} + \underline{0} = \underline{u} = \underline{0} + \underline{u} \quad \forall \underline{u} \in V$ additive identity

III) $\forall \underline{u} \in V$, $\exists (-\underline{u})$ s.t.

$\underline{u} + (-\underline{u}) = \underline{0} = (-\underline{u}) + \underline{u}$ additive inverse

IV) $\underline{u} + \underline{v} = \underline{v} + \underline{u} \quad \forall \underline{u}, \underline{v} \in V$ commutative

I') $\lambda \cdot (\mu \cdot \underline{v}) = (\lambda\mu) \cdot \underline{v} \quad \forall \lambda, \mu \in \mathbb{F}, \forall \underline{v} \in V$

II') $1 \cdot \underline{u} = \underline{u} \quad \forall \underline{u} \in V$

III') $-\underline{u} = (-1) \cdot \underline{u}$

Plus two distributive laws.

D1) $\lambda \cdot (\underline{u} + \underline{v}) = \lambda \underline{u} + \lambda \underline{v} \quad \forall \lambda \in \mathbb{F}, \forall \underline{u}, \underline{v} \in V$

i.e. multiplication of λ distributes over addition

D2) $(\lambda+\mu).\underline{u} = \lambda\underline{u} + \mu\underline{u}$ $\quad\quad \forall \lambda,\mu \in \mathbb{F},\ \forall \underline{u} \in V$

✓ <u>Basic Example:</u>

($\mathbb{F}$ is fixed in advance)

$$\mathbb{F}^n = \left\{ \underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \mathbb{F} \right\}$$

means vector space

$\mathbb{F}^n \neq \mathbb{F}_n$

means fields

① $\underline{x}+\underline{y} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ \vdots \\ x_n+y_n \end{pmatrix}$ addition

② $\lambda.\underline{x} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$ scalar multiplication

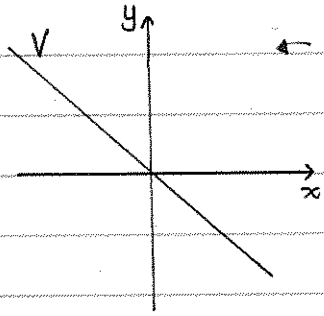
③ $\underline{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

$\Rightarrow \mathbb{F}^n$ is a vector space over $\mathbb{F}$

✓ <u>EXAMPLE:</u>

$\mathbb{F} = \mathbb{R}$

$= \{\underline{x} \in \mathbb{R}^2 : x_1 + x_2 = 0\}$



← an 1-direction vector space sits in $\mathbb{F}^2$

Note: '$V \subset \mathbb{F}^2$ BUT $V \neq \mathbb{F}^2$' in this example.

means 'Every $\mathbb{F}^n$ is a vector space.

But not every vector space is an $\mathbb{F}^n$.'

V is a vector space.

Any $\underline{x} \in V$ can be written as $\underline{x} = \begin{pmatrix} x_1 \\ -x_1 \end{pmatrix}$.

If $\underline{y} = \begin{pmatrix} y_1 \\ -y_1 \end{pmatrix} \in V$, then

$$\underline{x}+\underline{y} = \begin{pmatrix} x_1+y_1 \\ -(x_1+y_1) \end{pmatrix}$$

$$\underline{0} = \begin{pmatrix} 0 \\ -0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \in V$$

$$\lambda\underline{x} = \lambda \begin{pmatrix} x_1 \\ -x_1 \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ -\lambda x_1 \end{pmatrix}$$

$\Rightarrow V \subset \mathbb{F}^2$, but $V \neq \mathbb{F}^2$ (counterexample: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \notin V$)

- $\mathbb{F}$ is a fixed field.

Let $A = \left(a_{ij} \,\middle|\, \begin{smallmatrix} 1 \le i \le m \\ 1 \le j \le n \end{smallmatrix}\right)$ $\quad m \times n$ matrix

$a_{ij} \in \mathbb{F}$

Consider the homogenous system S

$S = (A\underline{x} = \underline{0})$

$$S = \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases}$$

✓ Temporary Notation:

$K_A = \{\underline{x} \in \mathbb{F}^n : A\underline{x} = \underline{0}\}$ solution set

$K_A \subset \mathbb{F}^n$

If $A \neq 0$, then $K_A \neq \mathbb{F}^n$.

✓ Prop

K_A is a vector space over $\mathbb{F}$.

Proof: - If $\underline{x} \in K_A$ and $\underline{y} \in K_A$, then $\underline{x} + \underline{y} \in K_A$

$$\left.\begin{array}{l} A\underline{x} = \underline{0} \text{ and } A\underline{y} = \underline{0} \Rightarrow A\underline{x} + A\underline{y} = \underline{0} + \underline{0} = \underline{0} \\ \qquad\qquad\qquad \Leftrightarrow A(\underline{x} + \underline{y}) = \underline{0} \end{array}\right\} \text{addition } (\checkmark)$$

- If $\underline{x} \in K_A$ and $\lambda \in \mathbb{F}$, then

$A \cdot (\lambda \underline{x}) = \lambda A \cdot \underline{x} = \lambda \cdot \underline{0} = \underline{0}$

So $\lambda \underline{x} \in K_A$ scalar multiplication (✓)

- Zero: $A \cdot \underline{0} = \underline{0}$

So $\underline{0} \in K_A$ zero (✓)

- The remaining axioms are automatically satisfied.

(satisfied already in $\mathbb{F}^n$).

Hence, K_A is a vector space over $\mathbb{F}$ ▨

4.2.1 Linear Independence

- Def.

Let V be a vector space over $\mathbb{F}$

Suppose $\underline{v}_1, \underline{v}_2, \underline{v}_3, \dots, \underline{v}_n \in V$

An expression of the form

$\boxed{\underline{v} = \lambda_1 \underline{v}_1 + \lambda_2 \underline{v}_2 + \lambda_3 \underline{v}_3 + \dots + \lambda_n \underline{v}_n}$ $\lambda_i \in \mathbb{F}$

is called a linear combination in $\underline{v}_1, \dots, \underline{v}_n$.

✓ Notice that I can always get $\underline{0}$ as a linear combination.

$\underline{0} = 0\underline{v}_1 + 0\underline{v}_2 + 0\underline{v}_3 + \dots + 0\underline{v}_n$

✓ Informal Def.

$\{\underline{v}_1, \dots, \underline{v}_n\}$ is said to be linearly independent (L.I.) when the ONLY way to get

$\underline{0}$ is with all coefficients $= 0$.

- Formal Def.

  $\{\underline{v_1}, \dots, \underline{v_n}\}$ is linearly independent (LI) when

  $$\boxed{\begin{array}{l} \lambda_1 \underline{v_1} + \lambda_2 \underline{v_2} + \dots + \lambda_n \underline{v_n} = \underline{0} \\ \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n = 0 \end{array}}$$

✓ EXAMPLE:

$$V = \mathbb{F}^4$$

$$\underline{e_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \underline{e_2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \underline{e_3} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad \underline{e_4} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Then $\{\underline{e_1}, \underline{e_2}, \underline{e_3}, \underline{e_4}\}$ are LI.

Proof: $\lambda_1 \underline{e_1} + \lambda_2 \underline{e_2} + \lambda_3 \underline{e_3} + \lambda_4 \underline{e_4}$ $(*)$

$$= \begin{pmatrix} \lambda_1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \lambda_2 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \lambda_3 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \lambda_4 \end{pmatrix}$$

$$= \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{pmatrix}$$

So, if $(*) = 0$, then $\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$\Rightarrow \lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$

$\Rightarrow \{\underline{e_1}, \underline{e_2}, \underline{e_3}, \underline{e_4}\}$ is LI. $\blacksquare$

- Generalisation:

$$V = \mathbb{F}^n$$

$$\underline{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \underline{e_2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad \underline{e_n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Then $\{\underline{e_1}, \underline{e_2}, \dots, \underline{e_n}\}$ is LI.

✓ EXAMPLE ①:

$$V = \mathbb{F}^3$$

$$\underline{\varphi_1} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \qquad \underline{\varphi_2} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \qquad \underline{\varphi_3} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Then, $\{\underline{\varphi_1}, \underline{\varphi_2}, \underline{\varphi_3}\}$ is LI.

Proof: $\lambda_1 \underline{\varphi_1} + \lambda_2 \underline{\varphi_2} + \lambda_3 \underline{\varphi_3} = \begin{pmatrix} \lambda_1 \\ \lambda_1 \\ \lambda_1 \end{pmatrix} + \begin{pmatrix} \lambda_2 \\ \lambda_2 \\ 0 \end{pmatrix} + \begin{pmatrix} \lambda_3 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 + \lambda_2 + \lambda_3 \\ \lambda_1 + \lambda_2 \\ \lambda_1 \end{pmatrix}$

So if $\lambda_1 \underline{\varphi_1} + \lambda_2 \underline{\varphi_2} + \lambda_3 \underline{\varphi_3} = \underline{0}$, then $\begin{pmatrix} \lambda_1 + \lambda_2 + \lambda_3 \\ \lambda_1 + \lambda_2 \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

So $\lambda_1 = 0$ | $\lambda_1 + \lambda_2 = 0$, But $\lambda_1 = 0$, So $\lambda_2 = 0$ | $\lambda_1 + \lambda_2 + \lambda_3 = 0$, But $\lambda_1 + \lambda_2 = 0$, So $\lambda_3 = 0$

$\Rightarrow \{\underline{\psi_1}, \underline{\psi_2}, \underline{\psi_3}\}$ is LI. ▨

✓ EXAMPLE ②:

$\underline{\psi_1} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \underline{\psi_2} = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \quad \underline{\psi_3} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \underline{\psi_4} = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}$

Then $\{\underline{\psi_1}, \underline{\psi_2}, \underline{\psi_3}, \underline{\psi_4}\}$ is not LI.

(It is linearly dependent)

Work over $\mathbb{Q}$

Proof: Solve $\lambda_1\underline{\psi_1} + \lambda_2\underline{\psi_2} + \lambda_3\underline{\psi_3} + \lambda_4\underline{\psi_4} = \underline{0}$

$$\begin{pmatrix} \lambda_1 + \lambda_2 \qquad + 2\lambda_4 \\ \lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 \\ \lambda_1 + \lambda_2 + \lambda_3 + 3\lambda_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\left(\begin{array}{cccc:c} 1 & 1 & 0 & 2 & 0 \\ 1 & -1 & 1 & -1 & 0 \\ 1 & 1 & 1 & 3 & 0 \end{array}\right)$$

Reduce to row echelon form:

$$\xrightarrow[\mathcal{E}(3,1;-1)]{\mathcal{E}(2,1;-1)} \left(\begin{array}{cccc:c} 1 & 1 & 0 & 2 & 0 \\ 0 & -2 & 1 & -3 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{D}(2;\frac{1}{2})} \left(\begin{array}{cccc:c} 1 & 1 & 0 & 2 & 0 \\ 0 & -1 & 1/2 & -3/2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{E}(1,2;1)} \left(\begin{array}{cccc:c} 1 & 0 & 1/2 & 1/2 & 0 \\ 0 & -1 & 1/2 & -3/2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[\mathcal{E}(2,3;-\frac{1}{2})]{\mathcal{E}(1,3;-\frac{1}{2})} \left(\begin{array}{cccc:c} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{\mathcal{D}(2;-1)} \left(\begin{array}{cccc:c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

$\lambda_1 \quad \lambda_2 \quad \lambda_3 \quad \lambda_4$

$\lambda_1 = 0$	Take $\lambda_1 = 0$
$\lambda_2 = -2\lambda_4$	$\lambda_2 = -2$
$\lambda_3 = -\lambda_4$	$\lambda_3 = -1$
$\lambda_4 = \lambda_4$	$\lambda_4 = 1$

Then $\quad \underline{0} - 2\underline{\psi}_2 - \underline{\psi}_3 + \underline{\psi}_4 = \underline{0}$

Since $-2 \neq 0,\ -1 \neq 0,\ 1 \neq 0,$

We have a linear combination in which not all $\lambda_i = 0$. ▨

- Def.

✓ $\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n\}$ are linearly dependent (LD) when $\exists$ linear combination

$$\lambda_1 \underline{v}_1 + \lambda_2 \underline{v}_2 + \lambda_3 \underline{v}_3 + \dots + \lambda_n \underline{v}_n = \underline{0}$$

in which at least one $\lambda_i \neq 0$.

✓ Such an expression in which some $\lambda_i \neq 0$ is called a dependence relation.

✓ In the previous example,

$0\underline{\psi}_1 - 2\underline{\psi}_2 - \underline{\psi}_3 + \underline{\psi}_4 = \underline{0}$ is a dependence relation.

Mon. 21/11/16

MATH1201 : Algebra I

Prof. Johnson

Recap:

Def 1. linearly independent

V is a vector space over $\mathbb{F}$.

$\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n\} \subset V$.

$\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n\}$ is LI when

$$\sum_{i=1}^{n} \lambda_i \underline{v}_i = \underline{0} \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n = 0$$

4.2.2 Spanning

- Def.

V is a vector space over $\mathbb{F}$.

$\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_n\} \subset V$.

We say $\{\underline{v}_1, \underline{v}_2, \dots \underline{v}_n\}$ spans V when

$\forall \underline{w} \in V,\ \exists \lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{F}$ s.t. $\underline{w} = \sum_{i=1}^{n} \lambda_i \underline{v}_i$

✓ In English, (informal)

Every vector $\underline{w} \in V$ can be expressed as a linear combination $\{\underline{v_1}, \cdots, \underline{v_n}\}$.

✓ EXAMPLE ①:

Let $\underline{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\quad \underline{e_2} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\quad \cdots \quad$ $\underline{e_n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

be the standard vectors in $\mathbb{F}^n$, then $\{\underline{e_1}, \underline{e_2}, \cdots, \underline{e_n}\}$ spans $\mathbb{F}^n$.

Proof:

Let $\underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{F}^n$

$$\underline{x} = x_1 \underline{e_1} + x_2 \underline{e_2} + \dots + x_n \underline{e_n}$$

$$= \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + \dots + \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ x_n \end{pmatrix}$$ ▨

✓ EXAMPLE ②.

$$V = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{F}^3 ; \ x_1 + x_2 + x_3 = 0 \right\}$$

$\underline{\varphi_1} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ $\qquad \underline{\varphi_2} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$

Then $\{\underline{\varphi_1}, \underline{\varphi_2}\}$ spans V.

Proof: · $x_1 + x_2 + x_3 = 0 \longrightarrow$ could substitute either x_1, x_2 or x_3

$$\begin{cases} x_1 = -x_2 - x_3 \\ x_2 = \ \ x_2 \\ x_3 = \qquad x_3 \end{cases}$$

Then $\underline{x} = x_2 \underline{\varphi_1} + x_3 \underline{\varphi_2}$

$$= \begin{pmatrix} -x_2 \\ x_2 \\ 0 \end{pmatrix} + \begin{pmatrix} -x_3 \\ 0 \\ x_3 \end{pmatrix}$$

$$= \begin{pmatrix} -x_2 - x_3 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$\Rightarrow \{\underline{\varphi_1}, \underline{\varphi_2}\}$ spans V.

take out the coefficients of $\underline{\varphi}$

$M(\mathrm{Id})^{\mathcal{E}}_{\Phi} = [M(\mathrm{Id})^{\Phi}_{\mathcal{E}}]$

standard basis

To show $\underline{\Phi}$ spans V.

① express $\underline{\mathcal{E}}$ in terms of $\underline{\Phi}$

e.g. $\underline{e_n} = \lambda_1 \underline{\varphi_1} + \dots + \lambda_n \underline{\varphi_n}$

② $\forall \underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V$, we have

$$\underline{x} = x_1 \underline{e_1} + \dots + x_n \underline{e_n}$$

$$= x_1 (\lambda_1 \underline{\varphi_1} + \dots + \lambda_n \underline{\varphi_n}) + \dots$$

$$= \underline{\varphi_1} (\qquad) + \dots + \underline{\varphi_n} (\qquad)$$ ▨

4·2·3 Basis and Dimensions

· Def. $\qquad$ '/$\mathbb{F}$' ≡ 'over $\mathbb{F}$'

Let V be a vector space over $\mathbb{F}$

Let $\{\underline{E_1}, \underline{E_2}, \cdots, \underline{E_n}\} \subset V$.

We say that $\{\underline{E_1}, \underline{E_2}, \cdots, \underline{E_n}\}$ is a basis for V when

1) $\{\underline{E}_1, \underline{E}_2, \ldots, \underline{E}_n\}$ is LI.

and 2) $\{\underline{E}_1, \underline{E}_2, \cdots, \underline{E}_n\}$ spans V.

- Prop.

Let $\underline{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $\underline{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $\cdots$, $\underline{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ be the standard vectors in $\mathbb{F}^n$. Then $\{\underline{e}_1, \underline{e}_2, \cdots, \underline{e}_n\}$ is the basis for $\mathbb{F}^n$.

Proof:

$\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ is LI. (proved in last lecture)

$\{\underline{e}_1, \cdots, \underline{e}_n\}$ spans $\mathbb{F}^n$. (just proved) ▨

✓ EXAMPLE(②):

$$V = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{F}^3 \,\wedge\, : x_1 + x_2 + x_3 = 0 \right\}$$

$$\underline{\varphi}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \qquad \underline{\varphi}_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

Then $\{\underline{\varphi}_1, \underline{\varphi}_2\}$ is the basis for $\mathbb{F}^3$.

Proof:

$\{\underline{\varphi}_1, \underline{\varphi}_2\}$ spans V (shown in the previous pg)

$$\lambda_1 \underline{\varphi}_1 + \lambda_2 \underline{\varphi}_2 = \underline{0}$$

$$\begin{pmatrix} -\lambda_1 \\ \lambda_1 \\ 0 \end{pmatrix} + \begin{pmatrix} -\lambda_2 \\ 0 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Rightarrow \lambda_1 = \lambda_2 = 0$

$\Rightarrow \{\underline{\varphi}_1, \underline{\varphi}_2\}$ is LI. ▨

- Main Theorem. The Basis Theorem

Let V be a (non-zero) vector space over $\mathbb{F}$, then

(i) V has at least one basis.

(ii) Any two basis for V have the same number of elements.

- Def.

The number of elements in a basis for V is called the dimension of V, written

$\dim(V)$ (or $\dim_{\mathbb{F}}(V)$)

so $\dim(\mathbb{F}^n) = n$ because it has a basis $\underline{e}_1, \cdots, \underline{e}_n$ with n elements.

✓ EXAMPLE ①:

$$V = \left\{ \underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : x_1 + x_2 + x_3 = 0 \right\}$$

$\underline{\varphi}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ $\underline{\varphi}_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ is a basis for V.

Then $\dim(V) = 2$.

✓EXAMPLE ②:

$$W = \left\{ \underline{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{F}^2 : x_1 + x_2 = 0 \right\}$$

Then $\dim(W) = 1$, since

$$W = \left\{ x_2 \begin{pmatrix} -1 \\ 1 \end{pmatrix} : x_2 \in \mathbb{F} \right\}$$

$\Rightarrow \left\{ \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$ is a basis for W.

✓EXAMPLE ③:

$A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ $m \times n$ matrix over $\mathbb{F}$

$$K_A = \{ \underline{x} \in \mathbb{F}^n : A\underline{x} = \underline{0} \}$$

Compute $\dim(K_A)$, so first find a basis for K_A.

e.g. Easy Case.

Assume $A = \begin{pmatrix} 1 & -1 & 0 & 3 & 0 & -1 \\ 0 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ 3×6

Take $\mathbb{F} = \mathbb{Q}$.

$x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6$

$A\underline{x} = \underline{0}$ Write out general solution.

$$\begin{aligned} x_1 &= x_2 - 3x_4 + x_6 \\ x_2 &= x_2 \\ x_3 &= -2x_4 - x_6 \\ x_4 &= x_4 \\ x_5 &= -x_6 \\ x_6 &= x_6 \end{aligned}$$

$$\underline{x} = \begin{pmatrix} x_2 - 3x_4 + x_6 \\ x_2 \\ -2x_4 - x_6 \\ x_4 \\ -x_6 \\ x_6 \end{pmatrix}$$

Therefore, the obvious basis for K_A:

1st choice:

$x_2 = 1 \quad x_4 = 0 \quad x_6 = 0$

$$\underline{\varphi}_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

2^{nd} choice:

$x_2 = 0 \qquad x_4 = 1 \qquad x_6 = 0$

$$\underline{\varphi_2} = \begin{pmatrix} -3 \\ 0 \\ -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

3^{rd} choice:

$x_2 = 0 \qquad x_4 = 0 \qquad x_6 = 1$

$$\underline{\varphi_3} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

$\therefore \underline{x} = x_2 \underline{\varphi_1} + x_4 \underline{\varphi_2} + x_6 \underline{\varphi_3}$

$\Rightarrow \{\underline{\varphi_1}, \underline{\varphi_2}, \underline{\varphi_3}\}$ spans K_A.

We know that

$$\underline{x} = x_2 \underline{\varphi_1} + x_4 \underline{\varphi_2} + x_6 \underline{\varphi_3}$$

$$= \begin{pmatrix} ? \\ x_2 \\ ? \\ x_4 \\ ? \\ x_6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

So, $x_2 = x_4 = x_6 = 0$

Hence, $\{\underline{\varphi_1}, \underline{\varphi_2}, \underline{\varphi_3}\}$ is LI.

Fri. 25/11/16

MATH1201, Algebra I

Prof. Johnson

- Basis Theorem (Coming Soon)
  1) V has at least one basis for V
  2) Any two basis for V have the same number of elements. ($\dim V$)

✓ $\{\underline{E_1}, \dots, \underline{E_n}\}$ is a basis for V when

(i) $\{\underline{E_1}, \dots, \underline{E_n}\}$ is LI.

(ii) $\{\underline{E_1}, \dots, \underline{E_n}\}$ spans V.

If $\underline{x} \in V$, we can write

$$\underline{x} = x_1\underline{E_1} + x_2\underline{E_2} + x_3\underline{E_3} + \dots + x_n\underline{E_n} \quad \text{①} \quad \text{where } x_1, \dots, x_n \in \mathbb{F}.$$

Linear independence tells us that this expression is unique.

i.e. if $\underline{x} = y_1 \underline{E_1} + y_2 \underline{E_2} + y_3 \underline{E_3} + \dots + y_n \underline{E_n}$, then $\quad \cdots ②$

$x_1 = y_1, \ x_2 = y_2, \ \dots, \ x_n = y_n$

Proof. $① - ②: \ 0 = \sum_{i=1}^{n} (x_i - y_i) \underline{E_i}$

$\Rightarrow x_i - y_i = 0 \quad \forall i$

$\Rightarrow x_i = y_i \quad \forall i$ ▨

- Prop.

If $\{E_1, \dots, E_n\}$ is a basis for V, then for each $x_i \in V$, there is a unique expression

$$\boxed{\underline{x} = x_1 \underline{E_1} + \dots + x_n \underline{E_n}}$$

Fri. 25/11/16 (cont.)

MATH1201 : Algebra I

Prof. Johnson

Chapter 5. § Linear Mapping §

5·1 Linear Mappings and Connection to Matrices

5·1·1 Def.

Let V, W be vector spaces over $\mathbb{F}$.

$T: V \to W$ is a mapping.

We say that T is linear when

(i) $T(\underline{x}+\underline{y}) = T(\underline{x}) + T(\underline{y}) \quad \forall\, \underline{x}, \underline{y} \in V$

(ii) $T(\lambda \underline{x}) = \lambda T(\underline{x})$

✓ Standard Example:

$V = \mathbb{F}^n \qquad W = \mathbb{F}^m$

$A = (a_{ji})_{\substack{1\le j\le m \\ 1\le i\le n}} \qquad a_{ji} \in \mathbb{F} \qquad$ ~~$m \times n$ matrix~~

Define $T_A : \mathbb{F}^n \to \mathbb{F}^m$ by $T_A(\underline{x}) = \underset{\substack{\uparrow \\ \text{matrix provided}}}{A}\underline{x}$ where $\underline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$

T_A is obviously linear.

Proof: $T_A(\underline{x}+\underline{y}) = A(\underline{x}+\underline{y})$

$= A\underline{x} + A\underline{y}$

$= T_A(\underline{x}) + T_A(\underline{y})$

$T_A(\lambda \underline{x}) = A(\lambda \underline{x})$

$= \lambda A \underline{x}$

$= \lambda T_A(\underline{x})$ ▨

· <u>To what extent does an arbitrary linear map look like a standard example?</u>

✓ EXAMPLE ②: (Differentiation)

Let $V = \{a_0.1 + a_1 x + a_2 x^2 + a_3 x^2 : a_0, a_1, a_2, a_3 \in \mathbb{F}\}$

Define $D: V \to V$ to be differentiation.

Denote $a(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$, then

differentiate $a(x)$ $\longrightarrow D(a) = a_1 + 2a_2 x + 3a_3 x^2$

Then we can prove that $D(a+b) = D(a) + D(b)$

$D(\lambda a) = \lambda D(a)$ ▨

- Take V be a vector space with basis $\{\underline{E_1}, \dots, \underline{E_n}\}$,
  W be some other vector space.

What do I need to do to specify a linear map $T: V \to W$?

✓ Ans. It is enough to specify the values $T(\underline{E_1}), \dots, T(\underline{E_n})$.

✓ Proof:

Let $\underline{w_1}, \dots, \underline{w_n} \in W$.

Consider the following mapping

$$T: V \to W$$

$T(\underline{x}) = x_1 \underline{w_1} + x_2 \underline{w_2} + \dots + x_n \underline{w_n}$ where $\underline{x} = x_1 \underline{E_1} + x_2 \underline{E_2} + x_3 \underline{E_3} + \dots + x_n \underline{E_n}$ is the unique expression for $\underline{x}$.

Claim. (1) T is linear.

(2) $T(\underline{E_i}) = \underline{w_i}$

Proof of (1):

$$\underline{x} = \sum_{i=1}^{n} x_i \underline{E_i}, \quad \underline{y} = \sum_{i=1}^{n} y_i \underline{E_i}$$

Then,

$$\underline{x} + \underline{y} = \sum_{i=1}^{n} x_i \underline{E_i} + \sum_{i=1}^{n} y_i \underline{E_i} = \sum_{i=1}^{n} (x_i + y_i) \underline{E_i}$$

Since $T(\underline{x}) = \sum_{i=1}^{n} x_i \underline{w_i}$, $T(\underline{y}) = \sum_{i=1}^{n} y_i \underline{w_i}$,

$$T(\underline{x} + \underline{y}) = \sum_{i=1}^{n} (x_i + y_i) \underline{w_i} = T(\underline{x}) + T(\underline{y})$$

$\Rightarrow T$ is additive.

$$\lambda \underline{x} = \sum_{i=1}^{n} (\lambda x_i) \underline{E_i}$$

So, $T(\lambda \underline{x}) = \sum_{i=1}^{n} (\lambda x_i) \underline{w_i} = \lambda \sum_{i=1}^{n} x_i \underline{w_i} = \lambda T(\underline{x})$

Therefore, T is linear. ▨ (1)

Proof of (2): effectively replace "j" with "i"

$\underline{E_i} = \sum_{j=1}^{n} \delta_{ij} \underline{E_j}$ is the unique expression of $\underline{E_i}$ in terms of $\underline{E_1}, \underline{E_2}, \dots, \underline{E_n}$.

$$T(\underline{E_i}) = \sum_{j=1}^{n} \delta_{ij} \underline{w_j} = \underline{w_i}$$ ▨ (2)

So we have shown the following.

✓ Th.

A linear map T is determined (uniquely) by the values $T(\underline{E_1}), T(\underline{E_2}), \ldots, T(\underline{E_n})$, where $\{\underline{E_1}, \ldots, \underline{E_n}\}$ is a basis for domain.

- Property 1:

If $T: V \to W$ is linear, then $T(0) = 0$

Proof: $0\underline{v} = 0\underline{v} + 0\underline{v}$

$T(0\underline{v}) = T(0\underline{v} + 0\underline{v}) = T(0\underline{v}) + T(0\underline{v})$ by def.

Add $-T(0\underline{v})$ to both sides:

$0 = T(0\underline{v}) + T(0\underline{v}) - T(0\underline{v})$

$0\underline{w} = T(0\underline{v}) + 0$

So, $T(0\underline{v}) = 0\underline{w} \Rightarrow T(0) = 0$ ▨

- Property 2: Matrix Multiplication

Let $T: U \to V$; $S: V \to W$ be linear, then

$S \circ T: U \to W$ is also linear

Proof: Let $\underline{x}, \underline{y} \in U$

$$
\begin{aligned}
(S\circ T)(\underline{x}+\underline{y}) &= S(T(\underline{x}+\underline{y})) \\
&= S(T(\underline{x}) + T(\underline{y})) \quad \text{since } T \text{ is linear} \\
&= S(T(\underline{x})) + S(T(\underline{y})) \quad \text{since } S \text{ is linear} \\
&= (S\circ T)(\underline{x}) + (S\circ T)(\underline{y})
\end{aligned}
$$

$$
\begin{aligned}
(S\circ T)(\lambda\underline{x}) &= S(T(\lambda\underline{x})) \\
&= S(\lambda T(\underline{x})) \\
&= \lambda S(T(\underline{x})) \\
&= \lambda (S\circ T)(\underline{x})
\end{aligned}
$$

▨

5.1.2 Associating a Matrix with a Linear Map

- Let V be a vector space with basis $\mathscr{E} = \{\underline{E_1}, \underline{E_2}, \ldots, \underline{E_n}\}$,

  W be a vector space with basis $\Phi = \{\underline{\varphi_1}, \underline{\varphi_2}, \ldots, \underline{\varphi_m}\}$.

Then $\dim(V) = n$, $\dim(W) = m$.

Let $T: V \to W$ be linear.

Let $\underline{w_1}, \underline{w_2}, \ldots, \underline{w_n} \in W$ be the vectors s.t.

$$T(\underline{E_i}) = \underline{w_i}$$

Then $\underline{w_i}$ has a unique expression in terms of $\underline{\varphi_1}, \underline{\varphi_2}, \ldots, \underline{\varphi_m}$.

$$\underline{w_i} = \sum_{j=1}^{m} a_{ji} \underline{\varphi_j}$$

$$\text{So,} \quad T(\underline{E_i}) = \sum_{j=1}^{m} a_{ji}\,\underline{\varphi_j}$$

- Def.

$$M(T)^{\Phi}_{\mathcal{E}} = (a_{ji})_{\substack{1\le j\le m\\ 1\le i\le n}} \qquad \text{where } T: V\to W \text{ is linear}$$

called "matrix of T wrt $\mathcal{E}$ on the left and Φ on the right"

$\mathcal{E} = \{\underline{E_1}, \underline{E_2}, \dots, \underline{E_m}\}$ is a basis for V

$\Phi = \{\underline{\varphi_1}, \underline{\varphi_2}, \dots, \underline{\varphi_n}\}$ is a basis for W

determined by $\boxed{T(\underline{E_i}) = \sum_{j=1}^{m} a_{ji}\,\underline{\varphi_j}}$

✓ Convention chosen so as to coincide with standard example.

i.e. Let $A = (a_{ji})_{\substack{1\le j\le m\\ 1\le i\le n}}$ $\quad a_{ji}\in\mathbb{F}$

Take $\{\underline{E_1}, \underline{E_2}, \dots, \underline{E_n}\}$ to be standard basis for $\mathbb{F}^n$.

$$\underline{E_1} = \begin{pmatrix}1\\0\\ \vdots\\ 0\end{pmatrix}, \quad \underline{E_2} = \begin{pmatrix}0\\1\\ \vdots\\ 0\end{pmatrix}, \dots, \quad \underline{E_{n-1}} = \begin{pmatrix}0\\ \vdots\\ 1\\ 0\end{pmatrix}, \quad \underline{E_n} = \begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix}$$

Take $\{\underline{\varphi_1}, \underline{\varphi_2}, \dots, \underline{\varphi_n}\}$ to be standard basis for $\mathbb{F}^m$.

$$T_A : \mathbb{F}^n \to \mathbb{F}^m$$

$$T_A(\underline{x}) = A\underline{x}$$

so that $\boxed{M(T_A)^{\Phi}_{\mathcal{E}} = A}$

Proof: Calculate $T_A(\underline{E_i})$

$$T_A(\underline{E_i}) = \begin{pmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n}\\ \vdots & & \vdots & & \vdots\\ a_{j1} & \cdots & a_{ji} & \cdots & a_{jn}\\ \vdots & & \vdots & & \vdots\\ a_{m1} & \cdots & a_{mi} & \cdots & a_{mn}\end{pmatrix} \cdot \begin{pmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix} \leftarrow i^{th} \text{ position (row)}$$

$$= \begin{pmatrix}a_{1i}\\ a_{2i}\\ \vdots\\ a_{mi}\end{pmatrix}$$

$$= \sum_{j=1}^{m} a_{ji}\,\underline{\varphi_j}$$

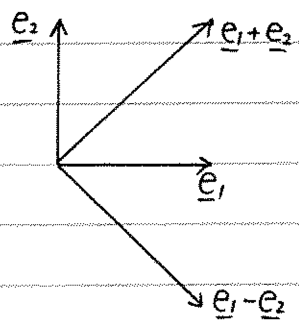
That is $M(T_A)^{\Phi}_{\mathcal{E}} = A$. ▨

✓ EXAMPLE:

Let $A = \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}$. $\quad 2\times 2$ matrix over $\mathbb{Q}$.

Take $\underline{e_1} = \begin{pmatrix}1\\0\end{pmatrix}$, $\underline{e_2} = \begin{pmatrix}0\\1\end{pmatrix}$

$\underline{\varphi_1} = \underline{e_1} + \underline{e_2}$, $\underline{\varphi_2} = \underline{e_1} - \underline{e_2}$



Then

$$T_A(\underline{e_1}) = \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}2\\1\end{pmatrix} = 2\underline{e_1} + \underline{e_2}$$

$$T_A(\underline{e_2}) = \underline{e_1} + 2\underline{e_2}$$

Since T is linear,

$$T_A(\underline{\varphi_1}) = T_A(\underline{e_1}+\underline{e_2})$$
$$= 3\underline{e_1} + 3\underline{e_2}$$
$$= 3\underline{\varphi_1}$$
$$T_A(\underline{\varphi_2}) = T_A(\underline{e_1}-\underline{e_2})$$
$$= \underline{e_1} - \underline{e_2}$$
$$= \underline{\varphi_2}$$

$$M(T_A)_{\mathcal{E}}^{\mathcal{E}} = A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

However, $M(T_A)_{\Phi}^{\Phi} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ called diagonalisation

choose a new basis!

5.2 Composition Formula

- Take U to be a vector space with basis $\{\underline{E_1}, \dots, \underline{E_n}\} = \mathcal{E}$

  V $\{\underline{\varphi_1}, \dots, \underline{\varphi_m}\} = \Phi$

  W $\{\underline{\psi_1}, \dots, \underline{\psi_p}\} = \Psi$

  $T: U \to V$ is linear and $S: V \to W$ is also linear.

  Let $M(T)_{\mathcal{E}}^{\Phi} = (a_{ji})_{\substack{1 \le j \le m \\ 1 \le i \le n}}$

  $M(S)_{\Phi}^{\Psi} = (b_{kj})_{\substack{1 \le k \le p \\ 1 \le j \le m}}$, then we also have

  $M(S \circ T) = (c_{ki})_{\substack{1 \le k \le p \\ 1 \le i \le n}}$

  (because $S \circ T$ is also linear)

- Ques.

  What's the relation between

  $M(S \circ T)_{\mathcal{E}}^{\Psi}$, $M(S)_{\Phi}^{\Psi}$ and $M(T)_{\mathcal{E}}^{\Phi}$?

Ans. $M(S \circ T)_{\mathcal{E}}^{\Psi} = M(S)_{\Phi}^{\Psi} \cdot M(T)_{\mathcal{E}}^{\Phi}$

Proof: [Compute $M(S \circ T)_{\mathcal{E}}^{\Psi}$]

$$(S \circ T)(\underline{E_i}) = S(T(\underline{E_i}))$$
$$= S\Big(\sum_{j=1}^{m} a_{ji}\underline{\varphi_j}\Big) \qquad T: U \to V$$
$$= \sum_{j=1}^{m} a_{ji} S(\underline{\varphi_j}) \qquad \text{since } S \text{ is linear}$$
$$= \sum_{j=1}^{m} a_{ji}\Big(\sum_{k=1}^{p} b_{kj}\underline{\psi_k}\Big) \qquad S: V \to W$$
$$= \sum_{j=1}^{m}\sum_{k=1}^{p} a_{ji} b_{kj}\underline{\psi_k}$$

Put $\boxed{a_{ji} b_{kj} = b_{kj} a_{ji} \text{ in } \mathbb{F}}$ ← commutativity

So $(S \circ T)(\underline{E_i}) = \sum_{j=1}^{m} \sum_{k=1}^{p} b_{kj} a_{ji} \underline{\psi_k}$

change the order of summation

$$= \sum_{k=1}^{p} \sum_{j=1}^{m} b_{kj} a_{ji} \underline{\psi_k} \qquad (\#)$$

If $B = (b_{kj}) = M(S)_{\Phi}^{\Psi}$

$A = (a_{ji}) = M(T)_{\mathcal{E}}^{\Phi}$, then $(BA) = (BA)_{ki}$ when

$$(BA)_{ki} = \sum_{j=1}^{m} b_{kj} a_{ji} \qquad (*)$$

sub $(*)$ into $(\#)$:

$$(S \circ T)(\underline{E_i}) = \sum_{k=1}^{p} (BA)_{ki} \underline{\psi_k}$$

So, $BA = M(S \circ T)_{\mathcal{E}}^{\Psi}$ since $M(S \circ T)_{\mathcal{E}}^{\Psi} = (BA)_{ki}$ $\quad 1 \leq k \leq p$, $1 \leq i \leq n$

$$\Rightarrow M(S)_{\Phi}^{\Psi} \cdot M(T)_{\mathcal{E}}^{\Phi} = M(S \circ T)_{\mathcal{E}}^{\Psi} \qquad ▨$$

- Interchanging the order of summation

✓ Let $A = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix}$

$\sum_{j=1}^{3} c_{ij}$: For $i=1$, $= c_{11} + c_{12} + c_{13}$

For $i=2$, $= c_{21} + c_{22} + c_{23}$

So, $\sum_{i=1}^{2} \sum_{j=1}^{3} c_{ij} = (c_{11} + c_{12} + c_{13}) + (c_{21} + c_{22} + c_{23})$

$\sum_{i=1}^{2} c_{ij}$: For $j=1$, $= c_{11} + c_{21}$

For $j=2$, $= c_{12} + c_{22}$

For $j=3$, $= c_{13} + c_{23}$

So, $\sum_{j=1}^{3} \sum_{i=1}^{2} c_{ij} = (c_{11} + c_{21}) + (c_{12} + c_{22}) + (c_{13} + c_{23})$

✓ Claim:

$$\sum_{i=1}^{2} \sum_{j=1}^{3} c_{ij} = \sum_{j=1}^{3} \sum_{i=1}^{2} c_{ij}$$

Proof:

$$(c_{11} + c_{12} + c_{13}) + (c_{21} + c_{22} + c_{23}) = (c_{11} + c_{21}) + (c_{12} + c_{22}) + (c_{13} + c_{23})$$

✓ If addition is associative & commutative, you can interchange order of summation.

Mon. 28/11/16

MATH1201: Algebra I

Prof. Johnson

Recap:

- $T: V \to W$ is linear.

$\mathcal{E} = \{E_1, \dots, E_n\}$ basis for V

$\Phi = \{\varphi_1, \dots, \varphi_m\}$ basis for W

$M(T)_{\mathcal{E}}^{\Phi} = (a_{ji})_{\substack{1 \le j \le m \\ 1 \le i \le n}}$ $m \times n$ matrix $\rightarrow$ "transformation matrix"

$T(\underline{E_i}) = \sum_{j=1}^{m} \underbrace{a_{ji}}_{\text{"transformation matrix"}} \underline{\varphi_j}$

EXAMPLE 1:

- $\mathbb{F}$ is a field.

$P_n = \{a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n : a_i \in \mathbb{F}\}$ This means P_n is the set of polynomials of degree $\le n$ with coefficients in $\mathbb{F}$.

Then,

basis: $\{1, x, x^2, \dots, x^n\}$

$\dim(P_n) = n+1$

$D: P_3 \to P_3$ Note: derivative of sum = sum of derivative

$D \equiv$ differentiation $\equiv \frac{d}{dx}$

✓We want $\underline{M(D)_{\mathcal{E}}^{\mathcal{E}}}$ $\longleftarrow$ a matrix D with $\mathcal{E}$ on the left and $\mathcal{E}$ on the right

$D(1) = 0$	$\underline{E_1} = 1$
$D(x) = 1$	$\underline{E_2} = x$
derivative of x^2 $\rightarrow D(x^2) = 2x$	$\underline{E_3} = x^2$
$D(x^3) = 3x^2$	$\underline{E_4} = x^3$

$$D(\underline{E_i}) = \sum_{j=1}^{4} a_{ji} \underline{E_j}$$

Since $D(1) = 0\underline{E_1} + 0\underline{E_2} + 0\underline{E_3} + 0\underline{E_4}$

$(a_{11}\underline{E_1} + a_{21}\underline{E_2} + a_{31}\underline{E_3} + a_{41}\underline{E_4}) \longleftarrow 1^{st}$ column

$$\Rightarrow M(D)_{\mathcal{E}}^{\mathcal{E}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

put the coefficients in the 1^{st} column (NOT the 1^{st} row)

$D(\underline{E_2}) = D(x) = 1\underline{E_1} + 0\underline{E_2} + 0\underline{E_3} + 0\underline{E_4} \longleftarrow 2^{nd}$ column

$D(\underline{E_3}) = D(x^2) = 0\underline{E_1} + 2\underline{E_2} + 0\underline{E_3} + 0\underline{E_4} \longleftarrow 3^{rd}$ column

$D(\underline{E_4}) = D(x^3) = 0\underline{E_1} + 0\underline{E_2} + 3\underline{E_3} + 0\underline{E_4} \longleftarrow 4^{th}$ column

✓ How about $D^2 = D.D$ $\frac{d^2}{dx^2}$ 2^{nd} derivative ?

$$M(D^2)^{\mathcal{E}}_{\mathcal{E}} = M(D.D)^{\mathcal{E}}_{\mathcal{E}}$$

$$= M(D)^{\mathcal{E}}_{\mathcal{E}} . M(D)^{\mathcal{E}}_{\mathcal{E}}$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Check using the same method.

$D^2(1) = 0$

$D^2(x) = 0$

$D^2(x^2) = 2$

$D^2(x^3) = 6x$

$$\Rightarrow M(D^2)^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

✓ EXAMPLE 2:

$$V = \{(a_1 + a_2 x + a_3 x^2)\exp(x) : a_1, a_2, a_3 \in \mathbb{Q}\}$$

Then $\begin{cases} \text{basis: } \{\underset{(\underline{E}_1)}{\exp(x)}, \underset{(\underline{E}_2)}{x\exp(x)}, \underset{(\underline{E}_3)}{x^2\exp(x)}\} \\ \dim_{\mathbb{Q}}(V) = 3 \end{cases}$

Again, take $D: V \to V$ differentiation is always linear

Then,

$D(\underline{E}_1) = \exp(x) = \underline{E}_1$

$D(\underline{E}_2) = \exp(x)(1+x) = \underline{E}_1 + \underline{E}_2$

$D(\underline{E}_3) = \exp(x)(x^2+2x) = 2\underline{E}_2 + \underline{E}_3$

$$\Rightarrow M(D)^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

So,

$$\boxed{M(D^2)^{\mathcal{E}}_{\mathcal{E}}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

means

2nd derivative

$$= \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

Similarly,

$$M(D^3)^{\mathcal{E}}_{\mathcal{E}} \left(= M(D^2)^{\mathcal{E}}_{\mathcal{E}} . M(D)^{\mathcal{E}}_{\mathcal{E}}\right)$$

$$= M(D)^{\mathcal{E}}_{\mathcal{E}} . M(D^2)^{\mathcal{E}}_{\mathcal{E}}$$

$$= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix}$$

✓ EXAMPLE 3:

Calculate $\frac{d^3}{dx^3}\big(\underbrace{2\exp(x) - 3x\exp(x) + 5x^2\exp(x)}_{a(x)}\big)$

Soln: Represent $a(x) = \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix}$

Then, $D^3(a(x)) = \begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix}$

$= \begin{pmatrix} 23 \\ 27 \\ 5 \end{pmatrix}$

This means $23\exp(x) + 27x\exp(x) + 5x^2\exp(x)$.

- <u>Integration</u>

$D \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ differentiation

Find D^{-1}.

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{\mathcal{E}(2,3;-2)} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & -2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{\mathcal{E}(1,2;-1)} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 2 \\ 0 & 1 & 0 & 0 & 1 & -2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Therefore, $D^{-1} = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$ integration

✓ EXAMPLE:

$$\int \{2\exp(x) - 3x\exp(x) + 5x^2\exp(x)\}\,dx$$

Soln: $\begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix} = \begin{pmatrix} 15 \\ -13 \\ 5 \end{pmatrix}$

$$\Rightarrow \int \{2\exp(x) - 3x\exp(x) + 5x^2\exp(x)\}\,dx$$

$$\sim 15\exp(x) - 13x\exp(x) + 5x^2\exp(x) + C$$

5.3 Change of Basis Formula

- Let V be a vector space with basis

$\mathcal{E} = \{\underline{E}_1, \underline{E}_2, \ldots, \underline{E}_n\}$
$\Phi = \{\underline{\varphi}_1, \underline{\varphi}_2, \ldots, \underline{\varphi}_n\}$ } both are basis for V.

✓ <u>1^{st} step</u>:

Express $\underline{\varphi_1}$ as a linear combination in $\{\underline{E_1}, \dots, \underline{E_n}\}$.

$$\underline{\varphi_1} = \sum_{j=1}^{n} a_{j1} \underline{E_j}$$

Likewise,

$$\underline{\varphi_2} = \sum_{j=1}^{n} a_{j2} \underline{E_j}$$

$$\vdots$$

In general, $\underline{\varphi_i} = \sum_{j=1}^{n} a_{ji} \underline{E_j}$

So we get a matrix

$$(a_{ji})_{\substack{1 \le j \le n \\ 1 \le i \le n}}$$

(a_{ji}) is simply $(a_{ji}) = M(U)_{\underline{\Phi}}^{\underline{\mathcal{E}}}$

$$\underline{\varphi_i} = Id(\underline{\varphi_i}) = \sum_{j=1}^{n} a_{ji} \underline{E_j}$$

Now, express $\underline{E_i}$ in terms of $\{\underline{\varphi_1}, \dots, \underline{\varphi_n}\}$

$$\underline{E_1} = \sum_{j=1}^{n} b_{j1} \underline{E_j}$$

Then, $\underline{E_i} = \sum_{j=1}^{n} b_{ji} \underline{E_j}$

Then, $b_{ji} = M(Id)_{\underline{\mathcal{E}}}^{\underline{\Phi}}$.

- Prop.

$$M(Id)_{\underline{\mathcal{E}}}^{\underline{\Phi}} = \left[M(Id)_{\underline{\Phi}}^{\underline{\mathcal{E}}}\right]^{-1}$$

Proof: (use the composition formula)

$M(Id)_{\underline{\mathcal{E}}}^{\underline{\mathcal{E}}} = M(Id)_{\underline{\Phi}}^{\underline{\mathcal{E}}} \cdot M(Id)_{\underline{\mathcal{E}}}^{\underline{\Phi}}$ by composition formula.

Likewise,

$$M(Id)_{\underline{\Phi}}^{\underline{\Phi}} = M(Id)_{\underline{\mathcal{E}}}^{\underline{\Phi}} \cdot M(Id)_{\underline{\Phi}}^{\underline{\mathcal{E}}}$$

$$\Rightarrow M(Id)_{\underline{\Phi}}^{\underline{\mathcal{E}}} = I_n / M(Id)_{\underline{\mathcal{E}}}^{\underline{\Phi}}$$

Fri. 02/12/16

MATH1201: Algebra 1

Prof. Johnson

Recap:

✓ V is a vector space.

$\dim(V) = n$

$\underline{\mathcal{E}} = \{\underline{E_1}, \dots, \underline{E_n}\}$ ‖ both basis for V

$\underline{\Phi} = \{\underline{\varphi_1}, \dots, \underline{\varphi_n}\}$

$T: V \to V$ linear

✓ Suppose we have a linear mapping represented by matrix $M(T)_{\mathcal{E}}^{\mathcal{E}}$ of T wrt $\mathcal{E}$.

i.e. $T(\underline{E_i}) = \sum_{j=1}^{n} a_{ji} \underline{E_j}$

$M(T)_{\mathcal{E}}^{\mathcal{E}} = (a_{ji})$ is known.

✓ T has a matrix $M(T)_{\Phi}^{\Phi}$ wrt Φ.

$$T(\underline{\varphi_i}) = \sum_{j=1}^{n} b_{ji} \underline{\varphi_j}$$

$M(T)_{\Phi}^{\Phi} = (b_{ji})$

5.3 Change of Basis

- Q. What is the relationship between $M(T)_{\Phi}^{\Phi}$ and $M(T)_{\mathcal{E}}^{\mathcal{E}}$?

✓ We first consider

$$Id: V \to V$$

$$Id(\underline{E_i}) = \underline{E_i} = \sum_{j=1}^{n} \delta_{ji} \underline{E_j}$$

It effectively replaces j with i.

So,

$$\boxed{M(Id)_{\mathcal{E}}^{\mathcal{E}} = I_n} = (\delta_{ji})$$

Similarly,

$$M(Id)_{\Phi}^{\Phi} = I_n$$

✓ However, we can express Φ in terms of $\mathcal{E}$.

$$\underline{\varphi_i} = \sum_{j=1}^{n} c_{ji} \underline{E_j}$$

i.e. $\boxed{M(Id)_{\Phi}^{\mathcal{E}} = (c_{ji})}$ $1 \le j \le n$, $1 \le i \le n$ ← transformation matrix ($\mathcal{E} \to \Phi$)

Likewise, we can express $\mathcal{E}$ in terms of Φ.

$$\underline{E_i} = \sum_{j=1}^{n} f_{ji} \underline{\varphi_j}$$

i.e. $M(Id)_{\mathcal{E}}^{\Phi} = (f_{ji})$ $1 \le j \le n$, $1 \le i \le n$

- Prop.

$$M(Id)_{\Phi}^{\mathcal{E}} = \left[M(Id)_{\mathcal{E}}^{\Phi} \right]^{-1}$$

✓ Proof: $M(Id)_{\Phi}^{\Phi} = M(Id \circ Id)_{\Phi}^{\Phi}$

$= M(Id)_{\mathcal{E}}^{\Phi} \cdot M(Id)_{\Phi}^{\mathcal{E}}$ by composition formula

$I_n = M(Id)_{\mathcal{E}}^{\mathcal{E}}$

$= M(Id \circ Id)_{\mathcal{E}}^{\mathcal{E}}$

$= M(Id)_{\Phi}^{\mathcal{E}} \cdot M(Id)_{\mathcal{E}}^{\Phi}$ by composition formula

Therefore,

$M(Id)_{\Phi}^{\mathcal{E}} = \left[M(Id)_{\mathcal{E}}^{\Phi} \right]^{-1}$ by def. ∎

✓ Carallary: Change of Basis Formula

$T: V \to V$ linear

$\left.\begin{array}{l}\mathcal{E} = \{E_1, \dots, E_n\} \\ \Phi = \{\varphi_1, \dots, \varphi_n\}\end{array}\right\|$ both basis for V

$$\boxed{M(T)^{\Phi}_{\Phi} = M(Id)^{\Phi}_{\mathcal{E}} . M(T)^{\mathcal{E}}_{\mathcal{E}} . M(Id)^{\mathcal{E}}_{\Phi}}$$

Proof: Use composition formula.

$$\begin{aligned} M(T)^{\Phi}_{\Phi} &= M(Id \circ T \circ Id)^{\Phi}_{\Phi} \\ &= M(Id)^{\Phi}_{\mathcal{E}} . M(T \circ Id)^{\mathcal{E}}_{\Phi} \\ &= M(Id)^{\Phi}_{\mathcal{E}} . M(T)^{\mathcal{E}}_{\mathcal{E}} . M(Id)^{\mathcal{E}}_{\Phi} \end{aligned}$$ ▨

- √ EXAMPLE ①.

Consider $T: \mathbb{Q}^3 \to \mathbb{Q}^3$.

$$T\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4x_1 - 2x_2 + 2x_3 \\ 3x_2 - 2x_3 \\ -x_1 + 2x_2 - x_3 \end{pmatrix}$$

T is linear

- Take standard basis,

$$\mathcal{E} = \left\{ \underset{E_1}{\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}}, \underset{E_2}{\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}}, \underset{E_3}{\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}} \right\}$$

If this is the standard basis, just take the coefficients out.

Then,

$$M(T)^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix} 4 & -2 & 2 \\ 0 & 3 & -2 \\ -1 & +2 & -1 \end{pmatrix}$$

- Can we find a basis Φ s.t. $M(T)^{\Phi}_{\Phi}$ is 'Nice' ?

Let's try
$$\Phi = \left\{ \underset{\varphi_1}{\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}}, \underset{\varphi_2}{\begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}}, \underset{\varphi_3}{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}} \right\}$$

$M(Id)^{\varepsilon}_{\Phi}$
From standard basis to Φ:
just take the coefficients in Φ.

So, $$M(Id)^{\varepsilon}_{\Phi} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Therefore, $$M(Id)^{\Phi}_{\mathcal{E}} = \left[M(Id)^{\mathcal{E}}_{\Phi}\right]^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & -2 \\ 1 & -2 & 3 \end{pmatrix}$$

By change of basis formula,

$$M(T)^{\Phi}_{\Phi} = M(Id)^{\Phi}_{\mathcal{E}} M(T)^{\mathcal{E}}_{\mathcal{E}} M(Id)^{\mathcal{E}}_{\Phi}$$

$$= \begin{pmatrix} 1 & -1 & 1 \\ -1 & 2 & -2 \\ 1 & -2 & 3 \end{pmatrix} . \begin{pmatrix} 4 & -2 & 2 \\ 0 & 3 & -2 \\ -1 & 2 & -1 \end{pmatrix} . \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & -3 & 3 \\ -2 & 4 & -4 \\ 1 & -2 & 3 \end{pmatrix} . \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

✓ EXAMPLE ②:

Consider $T : \mathbb{Q}^3 \to \mathbb{Q}^3$

$$T = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4x_1 - 2x_2 + x_3 \\ 2x_2 \\ 3x_3 \end{pmatrix}$$

T is linear.

- Take standard basis.

$$\mathcal{E} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Then, $M(T)^{\mathcal{E}}_{\mathcal{E}} = \begin{pmatrix} 4 & -2 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

- Take another basis

$$\Phi = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$$

So, $M(Id)^{\mathcal{E}}_{\Phi} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

Therefore, $M(Id)^{\Phi}_{\mathcal{E}} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}$

So, $M(T)^{\Phi}_{\Phi} = M(Id)^{\Phi}_{\mathcal{E}} M(T)^{\mathcal{E}}_{\mathcal{E}} M(Id)^{\mathcal{E}}_{\Phi}$

$$= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix} . \begin{pmatrix} 4 & -2 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} . \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 3 \\ 4 & -4 & 4 \end{pmatrix} . \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

- Check:

$$T(\underline{\varphi_1}) = T\begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}2\\2\\0\end{pmatrix} = 2\underline{\varphi_1}$$

$$T(\underline{\varphi_2}) = T\begin{pmatrix}-1\\0\\1\end{pmatrix} = \begin{pmatrix}-3\\0\\3\end{pmatrix} = 3\underline{\varphi_2}$$

$$T(\underline{\varphi_3}) = T\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}4\\0\\0\end{pmatrix} = 4\underline{\varphi_3}$$

$$\Rightarrow M(T)_{\underline{\Phi}}^{\underline{\Phi}} = \begin{pmatrix}2 & 0 & 0\\0 & 3 & 0\\0 & 0 & 4\end{pmatrix}$$

Fri. 02/12/16 (cont)

MATH1201: Algebra I

Prof. Johnson

Chapter 6. § Kernel-Rank Theorem §

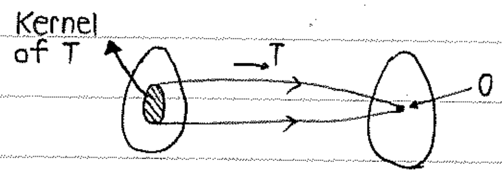
• Def.

$T: V \to W$ linear

$Ker(T) = \{\underline{v} \in V ; T(\underline{v}) = \underline{0}\}$ kernel of T

$Im(T) = \{\underline{w} \in W ; \exists \underline{v} \in V, T(\underline{v}) = \underline{w}\}$ image of T

(i.e. the set of all elements in W by T when applied to V)



• Th. Kernel-Rank Theorem

$\dim[Ker(T)] + \dim[Im(T)] = \dim(V) = \dim(\text{domain})$

• Def.

V is a vector space over $\mathbb{F}$.

$U \subset V$. We say that U is a vector subspace of V when

1) $\underline{0} \in U$

2) $\forall \underline{x}, \underline{y} \in U$, $\underline{x} + \underline{y} \in U$

3) $\forall \underline{x} \in U$, $\forall \lambda \in \mathbb{F}$, $\lambda \underline{x} \in U$

• Prop.

If $U \subset V$ is a vector subspace, then U is a vector space on its own right.

✓ Proof: – U has addition.

$+: U \times U \to U$

$(\underline{x}, \underline{y}) \to \underline{x} + \underline{y}$ by 2)

– U has scalar multiplication.

$\cdot : \mathbb{F} \times U \to U$

$(\lambda, \underline{x}) \to \lambda \underline{x}$ by 3)

– $\underline{0} \in U$ by 1)

– U has additive inverses.

$\underline{x} \in U$ then $-\underline{x} = (-1).\underline{x} \in U$ by 3)

taking $\lambda = -1$

- All remaining axioms are already satisfied because it is satisfied in V. $\boxtimes$

6·1 The Kernel is a Vector Space

• Prop.

$T: V \to W$ linear.

$Ker(T) = \{\underline{v} \in V ; T(\underline{v}) = \underline{0}\}$ is a vector subspace of V.

Proof: - $\underline{0}_V \in Ker(T)$ Ker(T) has a zero.

($since\ T(\underline{0}_V) = \underline{0}_V$)

- If $\underline{x}, \underline{y} \in Ker(T)$, then

$$T(\underline{x}+\underline{y}) = T(\underline{x}) + T(\underline{y}) \quad \text{since } T \text{ is linear}$$
$$= \underline{0} + \underline{0}$$
$$= \underline{0}$$

So, $\underline{x}+\underline{y} \in Ker(T)$ Ker(T) has addition.

- If $\underline{x} \in Ker(T)$, $\lambda \in \mathbb{F}$, then

$$T(\lambda\underline{x}) = \lambda T(\underline{x}) \quad \text{since } T \text{ is linear}$$
$$= \lambda \underline{0}$$
$$= \underline{0}$$

So, $\lambda\underline{x} \in Ker(T)$ Ker(T) has scalar multiplication. $\boxtimes$

6·2 The Image is a Vector Space

• Prop.

$T: V \to W$ linear

$Im(T) = \{\underline{w} \in W ; \exists \underline{v} \in V, T(\underline{v}) = \underline{w}\}$ is a vector subspace of W.

Proof: - $\underline{0}_W \in Im(T)$ because $T(\underline{0}_V) = \underline{0}_W$ Im(T) has a zero.

- If $\underline{w}_1, \underline{w}_2 \in Im(T)$, choose $\underline{v}_1, \underline{v}_2 \in V$ s.t. $T(\underline{v}_1) = \underline{w}_1$, $T(\underline{v}_2) = \underline{w}_2$

So,

$$T(\underline{v}_1 + \underline{v}_2) = T(\underline{v}_1) + T(\underline{v}_2)$$
$$= \underline{w}_1 + \underline{w}_2$$

So, $\underline{w}_1 + \underline{w}_2 \in Im(T)$ Im(T) has addition.

- If $\underline{w} \in Im(T)$, $\lambda \in \mathbb{F}$, choose $\underline{v} \in V$ s.t. $T(\underline{v}) = \underline{w}$.

Then,

$$T(\lambda\underline{v}) = \lambda T(\underline{v}) = \lambda \underline{w}$$

So, $\lambda \underline{w} \in Im(T)$. $Im(T)$ has scalar multiplication. ▨

6·3 The Kernel-Rank Theorem

· Standard Example:

✓ $A = (a_{ji})_{\substack{1 \le j \le m \\ 1 \le i \le n}}$ $m \times n$ matrix

$(a_{ji}) \in \mathbb{F}$

$T_A : \mathbb{F}^n \to \mathbb{F}^m$ linear

$\Leftrightarrow A\underline{x} = \underline{b}$ $\quad \underline{x} \in \mathbb{F}^n$, $\underline{b} \in \mathbb{F}^m$

$\Leftrightarrow T_A(\underline{x}) = \underline{b}$

- Suppose we have two solns, $\underline{x}$ and $\underline{y}$, then

$$\left.\begin{array}{l} A\underline{x} = \underline{b} \\ A\underline{y} = \underline{b} \end{array}\right\| \Rightarrow A(\underline{x} - \underline{y}) = \underline{b} - \underline{b} = \underline{0} \quad \text{i.e. } A\underline{z} = \underline{0}$$

- $Ker(T_A) = \{\underline{x} \in \mathbb{F}^n ; A\underline{x} = \underline{0}\}$

This is what we have previously called K_A.

i.e. In this case,

$Ker(T_A)$ = soln set to homogeneous (system) equation $A\underline{x} = \underline{0}$

- How about $Im(T_A)$?

General eqn: $A\underline{x} = \underline{b}$ $\quad \underline{x} \in \mathbb{F}^n$, $\underline{b} \in \mathbb{F}^m$

$Im(T_A) = \{\underline{b} \in \mathbb{F}^m$ s.t. $A\underline{x} = \underline{b}$ has a soln$\}$

· Th. Kernel-Rank Theorem

$T : V \to W$ linear, then

$$\boxed{\dim[Ker(T)] + \dim[Im(T)] = \dim(V)}$$

Proof: The typical case is where

$Ker(T) \neq \{\underline{0}\}$ and $Im(T) \neq \{\underline{0}\}$

Plus two special cases

(a) $Ker(T) = \{\underline{0}\}$

(b) $Im(T) = \{\underline{0}\}$

In these cases, we define dim (zero vector space) = 0.

$\{\underline{0}\}$ is the 0-dimensional vector space over $\mathbb{F}$, basis: $\emptyset$

① Typical Case:

$Ker(T) \neq \{\underline{0}\}$ so $Ker(T)$ has a basis

and $Im(T) \neq \{\underline{0}\}$ so $Im(T)$ also has a basis.

- Let $\{\underline{E}_1, \dots, \underline{E}_k\}$ be a basis for $Ker(T)$.

Let $\{\underline{\varphi}_1, \dots, \underline{\varphi}_m\}$ be a basis for $Im(T)$.

Choose $\{\underline{E}_{k+1}, \dots, \underline{E}_{k+m}\} \subset V$ so that $T(\underline{E}_{k+1}) = \underline{\varphi}_1$, …, $T(\underline{E}_{k+m}) = \underline{\varphi}_m$ $\quad \| \quad T(\underline{E}_{k+j}) = \underline{\varphi}_j$

- Claim: $\{\underline{E}_1, \underline{E}_2, \dots, \underline{E}_k, \underline{E}_{k+1}, \dots, \underline{E}_{k+m}\}$ is a basis for V.

So we need to show that

a) $\{\underline{E}_1, \dots, \underline{E}_{k+m}\}$ is LI.

and b) $\{\underline{E}_1, \dots, \underline{E}_{k+m}\}$ spans V.

- Proof of a):

Suppose $\sum_{i=1}^{k+m} \lambda_i \underline{E}_i = \underline{0}$ (*)

$\boxed{\text{Apply } T,}$ we get $\longrightarrow T\left((\lambda_1\underline{E}_1)\cup(\lambda_2\underline{E}_2)\cup\dots\cup(\lambda_{k+m}\underline{E}_{k+m})\right) = T(\underline{0})$

$\sum_{i=1}^{k+m} \lambda_i T(\underline{E}_i) = \underline{0}$ Since T is linear,

$\lambda_1 T(\underline{E}_1) + \lambda_2 T(\underline{E}_2) + \dots + \lambda_{k+m} T(\underline{E}_{k+m}) = \underline{0}$

as it is a basis for Ker(T) Since $\{\underline{E}_1, \dots, \underline{E}_k\} \subset \mathrm{Ker}(T)$,

$T(\underline{E}_1) = T(\underline{E}_2) = \dots = T(\underline{E}_k) = \underline{0}$ ⟵ by def. of Ker(T)

So $\sum_{i=1}^{m} \lambda_{k+i} T(\underline{E}_{k+i}) = \underline{0}$ (tail) ⟵ since $\sum_{i=1}^{k+m} \lambda_i T(\underline{E}_i) - \sum_{i=1}^{k} \lambda_i T(\underline{E}_i) = \underline{0} - \underline{0} = \underline{0}$

Since $T(\underline{E}_{k+i}) = \underline{\varphi}_i$,

$\sum_{i=1}^{m} \lambda_{k+i} \underline{\varphi}_i = \underline{0}$

Since $\{\underline{\varphi}_1, \underline{\varphi}_2, \dots, \underline{\varphi}_m\}$ is a basis for Im(T),

$\boxed{\{\underline{\varphi}_1, \underline{\varphi}_2, \dots, \underline{\varphi}_m\} \text{ is LI.}}$

So $\lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_{k+m} = 0$.

Substitute back into (*),

$\sum_{i=1}^{k} \lambda_i \underline{E}_i = \underline{0}$

But $\boxed{\{\underline{E}_1, \underline{E}_2, \dots, \underline{E}_k\} \text{ is LI}}$ since it is a basis for Ker(T).

So $\lambda_1 = \lambda_2 = \dots = \lambda_k = 0$

Therefore,

$\sum_{i=1}^{k+m} \lambda_i \underline{E}_i = \underline{0} \Rightarrow \forall i \quad \lambda_i = 0$ ▨ LI

- Proof of b):

Let $\underline{v} \in V$.

We need to show that $\underline{v} = \sum_{i=1}^{k+m} \lambda_i \underline{E}_i$

$\boxed{\text{Apply } T}$, we get

$\underline{w} = T(\underline{v}) \in \mathrm{Im}(T)$ by def. of Im(T)

Then, since

$\boxed{\{\underline{\varphi}_1, \dots, \underline{\varphi}_m\} \text{ is a basis}}$ for Im(T),

we have

$T(\underline{v}) = \sum_{i=1}^{m} \mu_i \underline{\varphi}_i$, $\mu_i \in \mathbb{F}$

Put $\underline{v}' = \sum_{i=1}^{m} \mu_i \underline{E}_{k+i}$

Then,

$$T(\underline{v}') = \sum_{i=1}^{m} \mu_i \underline{\varphi}_i = T(\underline{v})$$

$T(\underline{v}') = \sum_{i=1}^{m} \mu_i T(\underline{E}_{k+i})$

But we have chosen $\{\underline{E}_{k+1}, \dots, \underline{E}_{k+m}\}$ so that $T(\underline{E}_{k+j}) = \underline{\varphi}_j$

So,

$$T(\underline{v} - \underline{v}') = T(\underline{v}) - T(\underline{v}') \quad \text{since } T \text{ is linear}$$
$$= \underline{0}$$

Therefore,

$$\boxed{\underline{v} - \underline{v}' \in \mathrm{Ker}(T)} \qquad \text{by def. of } \mathrm{Ker}(T)$$

So, write

$$\underline{v} - \underline{v}' = \sum_{i=1}^{k} \lambda_i \underline{E}_i$$
$$\Leftrightarrow \quad \underline{v} = \sum_{i=1}^{k} \lambda_i \underline{E}_i + \underline{v}'$$
$$= \sum_{i=1}^{k} \lambda_i \underline{E}_i + \sum_{j=1}^{m} \mu_j \underline{E}_{k+j}$$

So, $\underline{v}$ is a linear combination in $\{\underline{E}_1, \dots, \underline{E}_{k+m}\}$.

Finally, put

$$\lambda_{k+j} = \mu_j$$

Then,

$$\underline{v} = \sum_{i=1}^{k+m} \lambda_i \underline{E}_i$$

So, $\{\underline{E}_1, \dots, \underline{E}_{k+m}\}$ spans V

- Hence, $\dim(V) = k+m = \dim[\mathrm{Ker}(T)] + \dim[\mathrm{Im}(T)]$. ▨

Mon. 05/12/16

MATH1201: Algebra I

Prof. Johnson

• Th. Kernel-Rank Theorem

$T: V \to W$ linear

$$\boxed{\dim[\mathrm{Ker}(T)] + \dim[\mathrm{Im}(T)] = \dim(V)}$$

Note: $\mathrm{Rank}(T) = \dim[\mathrm{Im}(T)]$

✓ proved when both $\mathrm{Ker}(T) \neq \{\underline{0}\}$ and $\mathrm{Im}(T) \neq \{\underline{0}\}$.

✓ Two special cases:

1). $\mathrm{Ker}(T) = \{\underline{0}\}$ i.e. $\dim[\mathrm{Ker}(T)] = 0$

So it is sufficient to show that $\dim(V) = \dim[\mathrm{Im}(T)]$.

Proof:

Take basis $\{\varphi_1, \dots, \varphi_m\}$ for $Im(T)$.

Choose $\{\underline{E}_1, \dots, \underline{E}_m\} \subset V$ s.t. $T(\underline{E}_i) = \underline{\varphi}_i$

Claim: $\{\underline{E}_1, \dots, \underline{E}_m\}$ is a basis for V.

① $\{\underline{E}_1, \dots, \underline{E}_m\}$ is LI

Suppose we have a linear combination

$$\sum_{i=1}^{m} \lambda_i \underline{E}_i = \underline{0}$$

Apply T. Then we get

$$\sum_{i=1}^{m} \lambda_i T(\underline{E}_i) = \underline{0}.$$

$$T\left(\sum_{i=1}^{m} \lambda_i \underline{E}_i\right) = T(\lambda_1 \underline{E}_1) + \dots + T(\lambda_m \underline{E}_m)$$
$$= \lambda_1 T(\underline{E}_1) + \dots + \lambda_m T(\underline{E}_m)$$
$$= \sum_{i=1}^{m} \lambda_i T(\underline{E}_i)$$

Since $T(\underline{E}_i) = \underline{\varphi}_i$,

$$\sum_{i=1}^{m} \lambda_i \underline{\varphi}_i = \underline{0}$$

But because $\{\underline{\varphi}_1, \dots \underline{\varphi}_m\}$ is a basis for $Im(T)$,

$\{\underline{\varphi}_1, \dots, \underline{\varphi}_m\}$ is LI.

So, $\lambda_1 = \lambda_2 = \dots = \lambda_m = 0$

Therefore,

$$\sum_{i=1}^{m} \lambda_i \underline{E}_i = \underline{0} \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_m = 0$$

▨ LI.

② Spanning.

We need to find $\lambda_1, \dots, \lambda_m \in \mathbb{F}$ s.t. $\underline{v} = \sum_{i=1}^{m} \lambda_i \underline{E}_i$

Apply T to $\underline{v}$:

$$T(\underline{v}) = Im(T)$$

Write $T(\underline{v}) = \sum_{i=1}^{m} \lambda_i \underline{\varphi}_i$

Put $\underline{v}' = \sum_{i=1}^{m} \lambda_i \underline{E}_i$, then

$$T(\underline{v}') = \sum_{i=1}^{m} \lambda_i T(\underline{E}_i) = \sum_{i=1}^{m} \lambda_i \underline{\varphi}_i = T(\underline{v})$$

So, we have

$$T(\underline{v} - \underline{v}') = T(\underline{v}) - T(\underline{v}') \quad \text{since } T \text{ is linear}$$
$$= \underline{0}$$

So, $\underline{v} - \underline{v}' = Ker(T) = \{\underline{0}\}$

$\Rightarrow \underline{v} - \underline{v}' = 0$

$\Leftrightarrow \underline{v} = \underline{v}'$

i.e. $\underline{v} = \sum_{i=1}^{m} \lambda_i \underline{E}_i$

▨ spanning

Therefore, $\dim(V) = \dim[Im(T)]$

▨

Special Case 2) $Im(T) = \underline{0}$

def. of $Im(T) = \{\underline{w} \in W, \exists \underline{v} \in V \text{ s.t. } T(\underline{v}) = \underline{w}\}$

So $\forall \underline{v} \in V$, $T(\underline{v}) = \underline{0}$

So $V = Ker(T)$. by def. of $Ker(T)$

Then, $\dim(V) = \dim[Ker(T)]$

i.e. $\dim(V) = \dim[Ker(T)] + \underbrace{\dim[Im(T)]}_{}$ with $\overset{0}{\shortparallel}$ ■

6.4 Connections with Injectivity, Surjectivity & Bijectivity

6.4.1 Injectivity

- Prop.

Let $T: V \to W$ be linear.

Then $Ker(T) = \{\underline{0}\} \Leftrightarrow T$ is injective.

i.e. $\dim[Ker(T)] = 0 \Leftrightarrow T$ is injective.

Injective:
$f(a_1) = f(a_2)$ $\Downarrow$ $a_1 = a_2$

✓ Proof:

($\Rightarrow$) Assume $Ker(T) = \{\underline{0}\}$

Then

$T(\underline{v}) = \underline{0} \Rightarrow \underline{v} = \underline{0}$ by def. of $Ker(T)$

Suppose $\underline{v}'$ & $\underline{v}'' \in V$ satisfy $T(\underline{v}') = T(\underline{v}'')$

Then

$T(\underline{v}' - \underline{v}'') = T(\underline{v}') - T(\underline{v}'') = \underline{0}$

So $\underline{v}' - \underline{v}'' = 0$

$\Leftrightarrow$ $\underline{v}' = \underline{v}''$

Therefore, T is injective. ■ ($\Rightarrow$)

($\Leftarrow$) Suppose $T(\underline{v}) = \underline{0}$ and $T(\underline{0}) = \underline{0}$, then

$\underline{v} = \underline{0}$

$\Rightarrow Ker(T) = \{\underline{0}\}$ ■ ($\Leftarrow$) ■

6.4.2 Surjectivity

- Prop.

Let $T: V \to W$ be linear.

Then T is surjective $\Leftrightarrow Im(T) = W$

i.e. T is surjective $\Leftrightarrow \dim[Im(T)] = \dim(W)$.

Surjective:
$\forall b \in B, \exists a \in A$
s.t. $f(a) = b$

✓ Proof: trivial

Look at def. of $Im(T)$.

✓ Corollary ①:

$T: V \to W$ linear

Then T is bijective iff $Ker(T) = \{\underline{0}\}$ & $Im(T) = W$

✓ Corollary ②:

$T: V \to W$ linear.

Then T is invertible $\Leftrightarrow$ $Ker(T) = \{\underline{0}\}$ & $Im(T) = W$

- Prop.

Let $T: V \to W$ be linear.

If T is bijective, then T^{-1} exists and $T^{-1}: W \to V$ is also linear.

✓ Proof: Let $\underline{w}_1, \underline{w}_2 \in W$, then

$$T\left(T^{-1}(\underline{w}_1 + \underline{w}_2) - T^{-1}(\underline{w}_1) - T^{-1}(\underline{w}_2)\right)$$
$$= TT^{-1}(\underline{w}_1 + \underline{w}_2) - TT^{-1}(\underline{w}_1) - TT^{-1}(\underline{w}_2) \quad \text{since } T \text{ is linear}$$
$$= \underline{w}_1 + \underline{w}_2 - \underline{w}_1 - \underline{w}_2$$
$$= \underline{0}$$

But T is injective.

$$\Rightarrow T^{-1}(\underline{w}_1 + \underline{w}_2) - T^{-1}(\underline{w}_1) - T^{-1}(\underline{w}_2) = T(\underline{0}) = \underline{0}$$
$$\Rightarrow T^{-1}(\underline{w}_1 + \underline{w}_2) = T^{-1}(\underline{w}_1) + T^{-1}(\underline{w}_2)$$

i.e. T^{-1} is additive.

Similarly,

$$T\left(T^{-1}(\lambda \underline{w}) - \lambda T^{-1}(\underline{w})\right)$$
$$= TT^{-1}(\lambda \underline{w}) - \lambda TT^{-1}(\underline{w})$$
$$= \lambda \underline{w} - \lambda \underline{w}$$
$$= \underline{0}$$

But T is injective.

$$\Rightarrow T^{-1}(\lambda \underline{w}) - \lambda T^{-1}(\underline{w}) = T(\underline{0}) = \underline{0}$$
$$\Rightarrow T^{-1}(\lambda \underline{w}) = \lambda T^{-1}(\underline{w})$$

Therefore, T^{-1} is also linear ▨

- Th.

Let A, B be $n \times n$ matrices over $\mathbb{F}$.

If $AB = I_n$, then $BA = I_n$.

✓ Proof: Let $T_A: \mathbb{F}^n \to \mathbb{F}^n$

$T_B: \mathbb{F}^n \to \mathbb{F}^n$ be linear map $T_A(\underline{x}) = A\underline{x}$

$T_B(\underline{x}) = B\underline{x}$

Therefore,

$T_{AB}(\underline{x}) = AB\underline{x}$

$= T_A T_B(\underline{x})$

Since $AB = I_n$,

$T_A T_B = Id_{\mathbb{F}^n} \leftarrow$ Identity matrix over $\mathbb{F}^n$

So T_A surjective.

If $\underline{w} \in \mathbb{F}^n$, then $T_A(T_B(\underline{w})) = \underline{w}$

Since $\dim[Ker(T_A)] + \dim[Im(T_A)] = n = \dim(\mathbb{F}^n)$,

and T_A surjective $\Rightarrow \dim[Im(T_A)] = \dim(\mathbb{F}^n)$,

$\Rightarrow \dim[Ker(T_A)] = 0$

So,

T_A is injective.

$\Rightarrow T_A$ is invertible.

$\Rightarrow T_A^{-1}$ is linear.

So we can write

$T_A^{-1} = T_C$ where $C = M(T_A^{-1})_{\mathcal{E}}^{\mathcal{E}}$ $\quad \mathcal{E}$ is the standard basis.

So $T_C T_A = Id_{\mathbb{F}^n}$

$\Rightarrow T_{CA} = Id_{\mathbb{F}^n}$

$\Rightarrow CA = Id_{\mathbb{F}^n}$

But since we have $AB = I_n$

$CA = I_n$,

$$\begin{cases} (CA)B = I_n . B = B \\ \quad \parallel \\ C(AB) = C . I_n = C \end{cases}$$

$\Rightarrow B = C$

i.e. $AB = I_n$

$BA = I_n$ $\blacksquare$

(von Neumann Property for $n \times n$ matrices)

Fri. 09/12/16

MATH1201: Algebra I

Prof. Johnson

Chapter 7. § The Basis Theorem §

- Th. Basis Theorem

  Let V be a non-zero vector space over $\mathbb{F}$, then

  (I) V has at least one basis. $\longrightarrow$ existence

  (II) Any two basis for V have the same number of elements $= \dim_{\mathbb{F}}(V)$

  $\hookrightarrow$ uniqueness

- Exchange Lemma

  V is a non-zero vector space over $\mathbb{F}$.

  $\{\underline{v}_1, \dots, \underline{v}_k\} \subset V$ is LI.

  $\{\underline{w}_1, \dots, \underline{w}_m\} \subset V$ spans.

  Then (i) $k \leq m$ and

  (ii) $\exists$ spanning set $\{\underline{w}_1', \dots, \underline{w}_m'\}$ for V s.t.

  $\underline{w}_i' = \underline{v}_i$ for $1 \leq i \leq k$

  AND $\underline{w}_i' \in \{\underline{w}_1, \dots, \underline{w}_m\}$ for $k \leq i$

7·1 Exchange Lemma

7·1·1 Baby Exchange Lemma

- Let $\underline{v} \in V$, $\underline{v} \neq \underline{0}$, and let $\{\underline{w}_1, \underline{w}_2, \dots, \underline{w}_m\}$ be a spanning set for V.

  Write $\underline{v} = \lambda_1 \underline{w}_1 + \lambda_2 \underline{w}_2 + \dots + \lambda_m \underline{w}_m$, $\lambda_j \in \mathbb{F}$. dummy variable, so subscript does not matter

  If $\lambda_i \neq 0$, then

  $\{\underline{w}_1, \dots, \underline{w}_{i-1}, \underline{v}, \underline{w}_{i+1}, \dots \underline{w}_m\}$ also spans V.

  here we swapped $\underline{w}_i$ for $\underline{v}$ as long as $\lambda_i \neq 0$

Proof: Since $\underline{v} = \sum_{j=1}^{m} \lambda_j \underline{w}_j$,

write $\underline{v} = \lambda_i \underline{w}_i + \sum_{j \neq i} \lambda_j \underline{w}_j$ where $\lambda_i \neq 0$ take out the "special" term

Then $\lambda_i \underline{w}_i = \underline{v} - \sum_{j \neq i} \lambda_j \underline{w}_j$ ($\lambda_i \neq 0$ so $\frac{1}{\lambda_i} \in \mathbb{F}$)

divide through by λ_i

$$\underline{w}_i = \left(\frac{1}{\lambda_i}\right)\underline{v} + \sum_{j \neq i} \left(-\frac{\lambda_j}{\lambda_i}\right)\underline{w}_j \quad (*)$$

We claim that $\{\underline{w}_1, \underline{w}_2, \dots, \underline{w}_{i-1}, \underline{v}, \underline{w}_{i+1}, \dots, \underline{w}_m\}$ spans V.

Let $\underline{x} \in V$, then we can write

$\underline{x} = \sum_{j=1}^{m} \xi_j \underline{w}_j$ since $\{\underline{w}_1, \dots, \underline{w}_m\}$ spans V

Then $\quad \underline{x} = \xi_i \underline{w_i} + \sum_{j\neq i} \xi_j \underline{w_j}$

substitute $\quad (*)$:

$$\underline{x} = \left(\frac{\xi_i}{\lambda_i}\right)\underline{v} + \xi_i \sum_{j\neq i}\left(-\frac{\lambda_j}{\lambda_i}\right)\underline{w_j} \quad + \sum_{j\neq i}\xi_j \underline{w_j}$$

$$= \left(\frac{\xi_i}{\lambda_i}\right)\underline{v} + \sum_{j\neq i}\left(\xi_j - \xi_i \cdot \frac{\lambda_j}{\lambda_i}\right)\underline{w_j}$$

Therefore, $\underline{x}$ is a linear combination in $\{\underline{w_1}, \underline{w_2}, \dots, \underline{w_{i-1}}, \underline{v}, \underline{w_{i+1}}, \dots, \underline{w_m}\}$.

i.e. $\{\underline{w_1}, \dots, \underline{w_{i-1}}, \underline{v}, \underline{w_{i+1}}, \dots, \underline{w_m}\}$ spans V. ▨

- We observe that

  any set which contains $\underline{0}$ cannot be LI.

  ✓ proof: Suppose $\{\underline{0}, \underline{u_2}, \dots, \underline{u_n}\}$, then we have

  $1.\underline{0} + 0.\underline{u_2} + 0.\underline{u_3} + \dots + 0\underline{u_n} = \underline{0}$ with at least one coefficient $\neq 0$.

7·1·2 Full Exchange Lemma:

- V is a non-zero vector space over $\mathbb{F}$.

  $\{\underline{v_1}, \dots, \underline{v_k}\} \subset V$ is LI,

  $\{\underline{w_1}, \dots, \underline{w_m}\} \subset V$ spans V

  Then 1) $k \leq m$ and

  2) $\exists$ spanning set $\{\underline{w_1'}, \dots, \underline{w_m'}\}$ for V s.t.

  $\underline{w_i'} = \underline{v_i}$ for $1 \leq i \leq k$

  AND $\underline{w_i'} \in \{\underline{w_1}, \dots, \underline{w_m}\}$ for $k < i$.

✓ Proof: (By induction on k)

- The case $k=1$ is precisely the Baby Exchange Lemma.

  We put $\underline{v} = \underline{v_1}$. Induction Base ✓.

  Then we get a spanning set $\{\underset{\underline{u_2}}{\underset{\downarrow}{\underline{w_1}}}, \dots, \underset{\underline{u_i}}{\underset{\downarrow}{\underline{w_{i-1}}}}, \underset{\underline{u_1}}{\underset{\downarrow}{\underline{v_1}}}, \underset{\underline{u_{i+1}}}{\underset{\downarrow}{\underline{w_{i+1}}}}, \dots, \underset{\underline{u_m}}{\underset{\downarrow}{\underline{w_m}}}\}$

  We can re-index the terms s.t.

  $\underline{u_1} = \underline{v_1}$, $\underline{u_j} = \underline{w_{j-1}}$ for $2 \leq j \leq i$ This means

  AND $\underline{u_j} = \underline{w_j}$ for $j \geq r+1$

  Then, we have

  $\{\underline{u_1}, \underline{u_2}, \dots, \underline{u_m}\}$ spans V.

  $\underline{u_1} = \underline{v_1}$
  $\underline{u_2} = \underline{w_1}$
  $\underline{u_3} = \underline{w_2}$
  $\vdots$
  $\underline{u_{i-1}} = \underline{w_{i-2}}$
  $\underline{u_i} = \underline{w_{i-1}}$

  $\underline{u_{i+1}} = \underline{w_{i+1}}$
  $\underline{u_{i+2}} = \underline{w_{i+2}}$
  $\vdots$
  $\underline{u_{m-1}} = \underline{w_{m-1}}$
  $\underline{u_m} = \underline{w_m}$

- Induction Step:

  1) Suppose true for $k-1$, so $k-1 \leq m$.

  And we have a spanning set $\{\underline{u_1}, \underline{u_2}, \dots, \underline{u_m}\}$ for V in which

  $\underline{u_i} = \underline{v_i}$ for $1 \leq i \leq k-1$ & $\underline{u_i} \in \{\underline{w_1}, \dots, \underline{w_m}\}$ for $i > k-1$.

If $k-1=m$, we would have

$\{\underline{v}_1, \dots, \underline{v}_{k-1}\}$ spans V.

Then, we could write $\underline{v}_k = \sum_{j=1}^{k-1} \mu_j \underline{v}_j$ (as a linear combination of the new spanning set)

So, $\sum_{j=1}^{k-1} \mu_j \underline{v}_j + (-1).\underline{v}_k = \underline{0}$

But this is a dependence relation in $\{\underline{v}_1, \underline{v}_2, \dots, \underline{v}_k\}$ since $-1 \neq 0$.

Contradiction, as $\{\underline{v}_1, \dots, \underline{v}_k\}$ is LI.

So we must have $k \leq m$. ▨ 1)

2) Now we can write

$$\underline{v}_k = \sum_{j=1}^{k-1} \eta_j \underline{v}_j + \sum_{j=k}^{m} \eta_j \underline{u}_j \quad (\underline{v}_k \neq \underline{0} \text{ as } \{\underline{v}_1, \dots, \underline{v}_k\} \text{ is LI})$$

We claim that

$\eta_j \neq 0$ for some j $(k \leq j)$ since $\{\underline{v}_1, \dots, \underline{v}_k\}$ is LI

Otherwise, we get

$\underline{v}_k = \sum_{j=1}^{k-1} \eta_j \underline{v}_j$ which is a dependence rel^n "relation" in $\{\underline{v}_1, \dots, \underline{v}_k\}$.

Contradiction.

So $\eta_j \neq 0$ for some j $(k \leq j \leq m)$

WLOG, we can re-index s.t. $\eta_k \neq 0$.

$$\underline{v}_k = \sum_{j=1}^{k-1} \eta_j \underline{v}_j + \eta_k \underline{u}_k + \sum_{k<j} \eta_j \underline{u}_j$$

$$(\eta_k \neq 0)$$

Use Baby Exchange Lemma again.

Swap $\underline{u}_k$ for $\underline{v}_k$.

Now we have a spanning set

$\{\underline{v}_1, \dots, \underline{v}_k, \underline{u}_{k+1}, \dots, \underline{u}_m\}$ where $\underline{u}_{k+1}, \dots, \underline{u}_m \in \{\underline{w}_1, \dots, \underline{w}_m\}$ ▨

7.2 Basis Theorem

- Corollary: Uniqueness Part of Basis Theorem

  Let V be a non-zero vector space.

  Suppose $\{\underline{E}_1, \dots, \underline{E}_m\}$ and $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$ are basis for V.

  Then $m = n$.

Proof: Since $\{\underline{E}_1, \dots, \underline{E}_m\}$ is LI and $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$ spans V,

by the exchange lemma, $m \leq n$.

Since $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$ is LI and $\{\underline{E}_1, \dots, \underline{E}_m\}$ spans V, by the exchange lemma, $n \le m$.

Then, $m \le n \le m$

So we have $m = n$. ▨

• Carollary: Existence of Basis

V is a non-zero vector space

Then V has at least one basis.

Proof:

– V has at least one spanning set, namely V itself. (i.e. V spans V)

$V = \{\underline{v}_1, \dots, \underline{v}_n\}$ is the maximal LI set of V.

If $\{\underline{v}_1, \dots, \underline{v}_n\} \subset \{\underline{w}_1, \dots, \underline{w}_N\}$ and $n < N$, then $\{\underline{w}_1, \dots, \underline{w}_N\}$ is not LI

– We need to search through all possible spanning sets and choose one with the smallest # of elements.

Write your chosen minimal spanning set $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$.

– Claim: $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$ is LI.

If not, choose a dependence relⁿ.

$\lambda_1 \underline{\varphi}_1 + \lambda_2 \underline{\varphi}_2 + \dots + \lambda_i \underline{\varphi}_i + \dots + \lambda_n \underline{\varphi}_n = \underline{0}$ where $\lambda_i \neq 0$ for some i

We claim that $\{\underline{\varphi}_1, \dots, \underline{\varphi}_{i-1}, \quad \underline{\varphi}_{i+1}, \dots, \underline{\varphi}_m\}$ still spans.

empty space

We can write

$$\underline{\varphi}_i = \sum_{j \neq i} \left(-\frac{\lambda_i}{\lambda_j}\right) \underline{\varphi}_j + 0 \qquad (\#)$$

So if $\underline{x} \in V$, we have

$$\underline{x} = \xi_i \underline{\varphi}_i + \sum_{j \neq i} \xi_j \underline{\varphi}_j$$

Substitute (#):

$$\underline{x} = \xi_i \sum_{j \neq i} \left(-\frac{\lambda_i}{\lambda_j}\right) \underline{\varphi}_j + \sum_{j \neq i} \xi_j \underline{\varphi}_j$$

$$= \sum_{j \neq i} \left(\xi_j - \frac{\xi_i \lambda_i}{\lambda_j}\right) \underline{\varphi}_j \qquad \text{(a linear combination)}$$

So, $\{\underline{\varphi}_1, \dots, \underline{\varphi}_{i-1}, \quad \underline{\varphi}_{i+1}, \dots, \underline{\varphi}_m\}$ still spans, and is smaller than any supposedly smallest spanning set.

Contradiction.

Hence, $\{\underline{\varphi}_1, \dots, \underline{\varphi}_n\}$ both spans and is LI.

Hence, it is a basis for V. ▨

7.3 Isomorphism 同构

- Def.

We say that vector spaces V, W over $\mathbb{F}$ are isomorphic when there exists an invertible linear map $T: V \to W$, i.e. a bijective linear map.

Then write $V \cong W$, when $\exists$ invertible linear map $T: V \to W$.

Note:

① $V \cong W \Rightarrow W \cong V$

This is because $T^{-1}: W \to V$ is also an invertible map.

② $\boxed{U \cong V \text{ and } V \cong W \Rightarrow U \cong W}$

This is because $S: U \to V$ is invertible & linear

$T: V \to W$ is invertible & linear

Then $T \circ S: U \to W$ is invertible & linear

$(T \circ S)^{-1} = S^{-1} \circ T^{-1}$ reversal of order

③ $V \cong V$ $Id: V \to V$

'$\cong$' is a 'equivalence relation'

✓ We will show

$$V \cong W \Leftrightarrow \dim(V) = \dim(W)$$

✓ Prop.

Let $\{E_1, E_2, \dots, E_n\}$ be a basis for V.

Let $T: V \to W$ be an invertible linear map, then

(i) $\{T(E_1), T(E_2), \dots, T(E_n)\}$ is a basis for W.

so (ii) $\dim(W) = \dim(V) = n$.

'ETP' $\equiv$ enough to prove'

Proof: ETP (i)

Suppose $\sum_{i=1}^{n} \lambda_i T(E_i) = \underline{0}$, then

$T(\sum_{i=1}^{n} \lambda_i E_i) = \underline{0}$ since T is linear

But since T is injective,

$\sum_{i=1}^{n} \lambda_i E_i = \underline{0}$ since $T(\underline{0}) = \underline{0}$

So, $\{E_1, E_2, \dots, E_n\}$ is LI.

$\Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n = 0$

So $\sum_{i=1}^{n} \lambda_i T(E_i) = \underline{0} \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n = 0$

i.e. $\{T(E_1), T(E_2), \dots, T(E_n)\}$ is LI.

Let $\underline{w} \in W$.

Put $\underline{v} = T^{-1}(\underline{w}) \in V$.

Since $\{\underline{E}_1, \underline{E}_2, \dots, \underline{E}_n\}$ spans V,

$$\underline{v} = \sum_{i=1}^{n} \lambda_i \underline{E}_i$$

So we have $\underline{w} = T(T^{-1}(\underline{w})) = T(\underline{v}) = T\left(\sum_{i=1}^{n} \lambda_i \underline{E}_i\right)$

Therefore, $\{T(\underline{E}_1), T(\underline{E}_2), \dots, T(\underline{E}_n)\}$ spans.

So, $\{T(\underline{E}_1), T(\underline{E}_2), \dots, T(\underline{E}_n)\}$ is a basis for V. ▨

✓ Carollary:

$V \cong W \Rightarrow \dim(V) = \dim(W)$

Note: converse is also true

✓ Prop.

If $\dim(V) = \dim(W)$, then $V \cong W$.

Proof: If $\dim(V) = \dim(W) = 0$, then

$V = \{\underline{0}\}$, $W = \{\underline{0}\}$

So $0 \to 0$ is iso. "iso" ≡ "isomorphic"

Suppose $\dim(V) = \dim(W) = n \geq 1$.

Let $\mathbb{F}^n$ be a standard vector space with standard basis $\{\underline{e}_1, \dots, \underline{e}_n\}$.

Let $\{\underline{E}_1, \underline{E}_2, \dots, \underline{E}_n\}$ be a basis for V.

· $\{\underline{\varphi}_1, \underline{\varphi}_2, \dots, \underline{\varphi}_n\}$ be a basis for W, then

$n = \dim(V) = \dim(W)$

Let $S: \mathbb{F}^n \to V$ be a linear map, then

$$S\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i \underline{E}_i$$

So, S is linear & bijective. (S invertible)

Note, $S(\underline{e}_i) = \underline{E}_i$

Let $T: \mathbb{F}^n \to W$ be a linear map, then

$$T\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i \underline{\varphi}_i$$

So, T is linear & bijective. (T inverible)

$\mathbb{F}^n \cong V$ and so $V \cong \mathbb{F}^n$.

Since $V \cong \mathbb{F}^n$ & $\mathbb{F}^n \cong W$,

$$V \cong W$$

$T \circ S^{-1} : V \to W$ is isomorphic. ▨

Mon. 12/12/16

MATH1201 : Algebra I

Prof. Johnson

- Compute basis for $Ker(T_A)$ and $Im(T_A)$

Suppose A : $m \times n$ matrix / $\mathbb{F}$, so $T_A : \mathbb{F}^n \to \mathbb{F}^m$

$$\boxed{T_A(\underline{x}) = A\underline{x}}$$

We can compute $Ker(T_A)$ by reducing A to row echelon form.

Then $\dim[Ker(T_A)]$ = no. of uncircled variables.

And we also know that

$$\dim[Ker(T_A)] + \dim[Im(T_A)] = \dim \mathbb{F}^n \qquad \text{Kernal-Rank Theorem}$$

$$\Leftrightarrow \dim[Im(T_A)] = \dim \mathbb{F}^n - \dim[Ker(T_A)]$$

"the rank of A" $\qquad = n -$ no. of uncircled variables

$$\Leftrightarrow \dim[Im(T_A)] = \text{no. of circled variables}$$

<u>How do we compute a basis for $Im(T_A)$?</u>

$$A\underline{x} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & & & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

the n^{th} column of A

$$T_A(\underline{x}) = x_1 Col_1(A) + x_2 Col_2(A) + \dots + x_n \boxed{Col_n(A)}$$

where $Col_j(A) = j^{th}$ column of A $= \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$

So we get

✓ <u>Prop</u>

$\{Col_j(A)\}$ $1 \le j \le n$ is a spanning set for $Im(T_A)$

✓ <u>How to find a maximal LI subset of $\{Col_j(A)\}$, $1 \le j \le n$?</u>

- To see how to do this, consider the special case where A is in reduced row echelon form.

$$\begin{array}{cccccc} \multicolumn{6}{c}{\begin{pmatrix} 1 & -1 & 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}} \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{array}$$

In this case, a basis is given the columns which lie above the circled variables.

i.e. a basis for $Im(T_A)$ is

$$\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} = \left\{ \begin{matrix} 1^{st} \text{ col.} \\ \text{of } A \end{matrix}, \ Col_3(A), \ Col_5(A), \ Col_6(A) \right\}$$

✓ In general, if A is $m \times n$ and reduced to A' (also $m \times n$), we do this by left multiplication by an invertible matrix P.

$$A' = PA$$

$$T_{A'} = T_P \circ T_A$$

Since T_P is invertible, we get

✓ Prop.

$T_P : Im(T_A) \xrightarrow{\cong} Im(T_{A'})$ is an isomorphism.

$T_P^{-1} : Im(T_{A'}) \xrightarrow{\cong} Im(T_A)$

✓ Corollary:

To obtain a basis for $Im(T_A)$,

1) reduce A to A'

2) take the columns in A which lie above circled variables in A'.

✓ EXAMPLE:

Work over $\mathbb{Q}$.

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 3 & 3 & 1 & 3 & 1 \end{pmatrix}$$

Take $T_A : \mathbb{Q}^7 \to \mathbb{Q}^3$.

Find 1) basis for $Ker(T_A)$.

2) basis for $Im(T_A)$.

Soln: $A \to \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & -2 & -2 & 0 & -2 & 0 \\ 0 & 0 & 2 & 2 & 0 & 2 & 0 \end{pmatrix}$

$$\to \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7$$

So $\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix} \right\}$ form a basis for $Im(T_A)$.

Rank $A = \dim[Im(T_A)] = 2$

General soln to $A\underline{x} = \underline{0}$:

$$\begin{pmatrix} -x_2 - x_5 - x_7 \\ x_2 \\ -x_4 - x_6 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix}$$

Make obvious choices to get basis for $Ker(T_A)$.

$$\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Chapter 3

7·4 Permutation (contd. from previous lectures)

7·4·1 Laplace's Formula for sign(σ)

- $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ is a permutation. (bijective mapping)

✓ Proof: Define $\mathcal{L}(\sigma) = \underbrace{\prod_{1 \le i < j \le n}}_{\text{"product"}} (\sigma(j) - \sigma(i))$

This has $\binom{n}{2} = \frac{n(n-1)}{2}$ terms → quite big & not practical.

greek letter "tau"

- Let τ be an adjacent transposition.

  $\tau = (k, k+1)$

  Swap k & $k+1$ for everything else.

- Prop

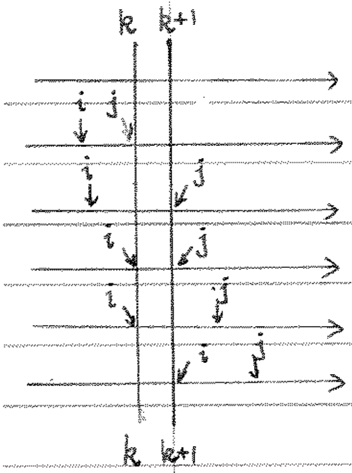
  $\mathcal{L}(\sigma\tau) = -\mathcal{L}(\sigma)$ if $\tau = (k, k+1)$ is adj trans

  adjacent transposition

- Fix τ in advance.

  $S = \{(i, j) : 1 \le i < j \le n\}$ can be decomposed into subsets.

adjacent transposition: $(i, i+1)$



$S_0 = \{(i,j) \in S : \{i,j\} \cap \{k, k+1\} = \emptyset\} \leftarrow i \neq k,\ i \neq k+1,\ j \neq k,\ j \neq k+1$

$S_1 = \{(i,k) : i < k\} \leftarrow j = k \Rightarrow (i,j) = (i,k)$

$S_2 = \{(i,k+1) : i < k\} \leftarrow j = k+1 \Rightarrow (i,j) = (i,k+1)$

$S_3 = \{(k, k+1)\} \leftarrow i = k,\ j = k+1 \Rightarrow (i,j) = (k, k+1)$

$S_4 = \{(k,j) : k+1 < j\} \leftarrow i = k \Rightarrow (i,j) = (k,j)$

$S_5 = \{(k+1, j) : k+1 < j\} \leftarrow i = k+1 \Rightarrow \ldots$

"rau"

Therefore, for any permutation ρ, we clearly have

(fixed in advance) $\boxed{\mathcal{L}(\rho) = \mathcal{L}_0(\rho)\mathcal{L}_1(\rho)\mathcal{L}_2(\rho)\mathcal{L}_3(\rho)\mathcal{L}_4(\rho)\mathcal{L}_5(\rho)}$

where $\mathcal{L}_i(\rho) = \prod_{(i,j) \in S_t} \left(\rho(j) - \rho(i)\right)$

- With $\tau = (k, k+1)$, we have

swap k & $k+1$

$\mathcal{L}_0(\sigma\tau) = \mathcal{L}_0(\sigma)$ stay the same e.g. $\mathcal{L}_1(\sigma\tau) = \{(i,k+1), i<k\}$

$= \prod_{(i,j)\in S_2} \sigma(j) - \sigma(i)$

$\mathcal{L}_1(\sigma\tau) = \mathcal{L}_2(\sigma)$ $\Big\rangle$ swap around

$\mathcal{L}_2(\sigma\tau) = \mathcal{L}_1(\sigma)$ $= \mathcal{L}_2(\sigma)$

$\mathcal{L}_3(\sigma\tau) = -\mathcal{L}_3(\sigma)$ change the sign $\mathcal{L}_3(\sigma\tau) = \{(k+1, k)\}$

$\mathcal{L}_4(\sigma\tau) = \mathcal{L}_5(\sigma)$ $\Big\rangle$ swap around $= -\{(k, k+1)\}$

$\mathcal{L}_5(\sigma\tau) = \mathcal{L}_4(\sigma)$ $= -\mathcal{L}_3(\sigma)$

✓ Corollary:

$\mathcal{L}(\sigma\tau) = -\mathcal{L}(\sigma)$ when τ is an adj trans

✓ Corollary:

If $\tau_1, \tau_2, \ldots, \tau_m$ are all adj. trans,

$\boxed{\mathcal{L}(\sigma\tau_1\tau_2\ldots\tau_m) = (-1)^m \mathcal{L}(\sigma)}$

special case: $\sigma = Id$

We cannot write Id as a product of an odd no. of adj trans.

This will give .... $\mathcal{L}(Id) = -1$

However, $\mathcal{L}(Id) = 1$.

Contradiction.

✓ Corollary. Laplace's Theorem

If $\tau_1, \ldots, \tau_m$ are all adj trans, then

$\mathcal{L}(\tau_1\tau_2\tau_3\ldots\tau_m) = (-1)^m \mathcal{L}(Id)$

- Laplace's Def. of sign(σ).

$\mathrm{sign}(\sigma) = \dfrac{\mathcal{L}(\sigma)}{\mathcal{L}(Id)}$

$$\text{sign}(\sigma) = \frac{\prod_{i<j} (\sigma(j) - \sigma(i))}{\prod_{i<j} (j-i)}$$

Fri 16/12/16

MATH1201 Algebra I

Prof. Johnson

$\sigma : \{1, \dots, n\}$ bijective

$$\text{sign}(\sigma) = \frac{\prod_{1\le i<j\le n} \sigma(j) - \sigma(i)}{\prod_{1\le i<j\le n} (j-i)} = \frac{\mathcal{L}(\sigma)}{\mathcal{L}(Id)}$$ where $\mathcal{L}(\sigma) = \prod_{1\le i<j\le n}$.

If $\sigma = \tau_1 \tau_2 \dots \tau_m$ where each τ_i is adj trans,

$$\text{sign}(\sigma) = (-1)^m.$$

7.4.2. Prop.

Any transposition is a product of an odd number of adj trans.

Proof: - (i,j) is any transposition.

Define $gap(i,j) = |j-i|$

We'll show that a transposition with $gap = k$ is a product of $(2k-1)$ adjacent transposition.

- Proof (by Induction on k).

$k=1$: nothing to prove since an odd adj trans has $gap(i,j) = 1$

This means $(i+1, j)$ with $gap = k-1$ is a product of an odd number of adj trans.

Assume true for $k-1$, and suppose $gap(i,j) = k$.

Then
$$\begin{pmatrix} i & i+1 & \dots & j \\ i+1 & i & \dots & j \\ j & i & \dots & i+1 \\ j & i+1 & \dots & i \end{pmatrix}$$
$(i, i+1)$ [adj trans]

$(i+1, j)$ according to assumption $|j-(i+1)| = |(j-i)-1| = |k-1|$ is true has $gap = k-1$

$(i, i+1)$ [adj trans]

i.e. $(i,j) = (i,i+1)(i+1,j)(i,i+1)$

By induction, since $gap(i,j) = k$, $gap(i+1,j) = k-1$

$(i+1, j)$ is a product of $2(k-1)-1 = 2k-3$ adj trans.
s.t. it's odd

So, (i,j) is a product of $\underbrace{1}_{(i,i+1)} + (2k-3) + \underbrace{1}_{(i,i+1)} = 2k-1$ adj trans. ▨

from above

✓ Corollary:

If ρ is a transposition, then

$$\text{sign}(\rho) = (-1)$$

Proof: $\rho = \tau_1\tau_2\cdots\tau_{2k-1}$ where τ_i is adjacent.

Therefore,

$$\text{sign}(\rho) = (-1)^{2k-1} = (-1).$$

$\blacksquare$

• Prop.

Let $C = (a_1, a_2, \cdots, a_n)$ be a cycle of length n.

Then C is a product of $(n-1)$ transpositions.

Proof:
$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ \vdots & \vdots & & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}$$

$$(a_1, \cdots, a_n) = \underbrace{(a_1, a_n)(a_1, a_{n-1})\cdots(a_1, a_3), (a_1, a_2)}_{(n-1)}$$

$\blacksquare$

✓ Corollary.

A cycle of length $(n-1)$ is a product of adjacent transpositions.

But every permutation is a product of (adjacent) transpositions, so

• Th.

Any permutation is a product of adjacent transpositions.

- Suppose $\sigma : \{1, 2, \cdots, n\}$ is bijective.

Then $\sigma = \tau_1\tau_2\cdots\tau_N$ where each τ_i is adj trans.

So $\text{sign}(\sigma) = (-1)^N$. ①

- Suppose $\rho : \{1, \cdots, n\}$ is also bijective.

Then $\rho = \theta_1\theta_2\cdots\theta_M$ where each θ_i is adj trans.

So $\text{sign}(\rho) = (-1)^M$ ②

- If we compose σ & ρ, we get

$$\sigma.\rho = \tau_1\tau_2\cdots\tau_N\theta_1\theta_2\cdots\theta_M \quad \text{where } \tau_i \,\&\, \theta_j \text{ adjacent}$$

Then
$$\begin{aligned} \text{sign}(\sigma\rho) &= (-1)^{N+M} \\ &= (-1)^N \cdot (-1)^M \end{aligned}$$

By ① and ②, we get

$$\text{sign}(\sigma\rho) = \text{sign}(\sigma)\text{sign}(\rho)$$

Therefore, we have proved

✓ Prop.

If $\sigma, \rho : \{1, \cdots, n\}$ bijective, then

$$\text{sign}(\sigma\rho) = \text{sign}(\sigma)\,\text{sign}(\rho)$$

✓ Corollary:

If $C = \{a_1, \dots, a_n\}$ is a cycle of length n, then

$$\text{sign}(C) = (-1)^{n-1}$$

Proof: $C = \underbrace{(a_1, a_n) \dots (a_1, a_3)(a_1, a_2)}_{(n-1)}$

and $\text{sign}(a_i, a_j) = (-1)$

$\Rightarrow \text{sign}(C) = \underbrace{(-1)(-1) \dots (-1)(-1)}_{(n-1)} = (-1)^{n-1}$ ▨

· Def.

We say a permutation σ is even when $\text{sign}(\sigma) = (+1)$

odd $\text{sign}(\sigma) = (-1)$

✓ So, a cycle of even length is odd.

a cycle of odd length is even.

✓ In general, if σ is a permutation, write

$\sigma = C_1 C_2 \dots C_M$ where C_i are disjoint cycles.

$$\boxed{\text{sign}(\sigma) = \text{sign}(C_1) \dots \text{sign}(C_M)}$$

✓ EXAMPLE:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 6 & 9 & 13 & 8 & 12 & 14 & 11 & 2 & 15 & 1 & 3 & 4 & 10 & 7 \end{pmatrix}$$

$$= \underbrace{(1,5,8,11)}_{4}\underbrace{(2,6,12,3,9)}_{5}\underbrace{(4,13)}_{2}\underbrace{(7,14,10,15)}_{4}$$

sign $= (-1) \cdot (+1) \cdot (-1) \cdot (-1) = (-1)$

order $= 20$ (lowest common multiple of 4, 5 & 2)

✓ $\sigma_n = \{ f : \{1, \dots, n\} \to \{1, \dots, n\} \}$ where f is bijective.

Then $|\sigma_n| = n!$

$\sigma_n^{\text{even}} = \{ f \in \sigma_n \,;\, \text{sign}(f) = +1 \}$

$\sigma_n^{\text{odd}} = \{ f \in \sigma_n \,;\, \text{sign}(f) = -1 \}$

✓ Prop.

$$|\sigma_n^{\text{even}}| = |\sigma_n^{\text{odd}}| = \frac{n!}{2}$$

Proof: Let τ be your favourite transposition.

Consider $\tau_* : \sigma_n \to \sigma_n$.

$\tau_*(f) = \tau f$

τ_* is bijective $\Rightarrow \tau_*^{-1} = \tau_*$

$\tau_*\tau_*(f) = \tau_*(\tau f)$

$= \tau\tau f$

$= f$

$\Rightarrow \tau^2 = 1$

Now $\left.\begin{array}{l} \tau_* : \sigma_n^{even} \longrightarrow \sigma_n^{odd} \\ \tau_* : \sigma_n^{odd} \longrightarrow \sigma_n^{even} \end{array}\right\}$ self inverse

So $\tau_* : \sigma_n^{even} \longrightarrow \sigma_n^{odd}$ is bijective

$\text{sign}(\tau_*(f)) = \text{sign}(\tau)\text{sign}(f) = -\text{sign}(f)$

$|\sigma_n^{even}| = |\sigma_n^{odd}|$

& $|\sigma_n| = |\sigma_n^{even}| + |\sigma_n^{odd}|$

$= 2|\sigma_n^{even}|$

$|\sigma_n^{even}| = \frac{n!}{2}$

Likewise, $|\sigma_n^{odd}| = \frac{n!}{2}$ ▨

Exercise 9 (HW)

$P_5 = \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5,\ a_i \in \mathbb{Q}\}$

Trick: $\mathcal{D}^6 \equiv 0$ on P_5

Factorise: $\mathcal{D}^6 - 1 = (\mathcal{D}^2 - 1)(\mathcal{D}^4 + \mathcal{D}^2 + 1)$

Therefore, on P_5: $1 - \mathcal{D}^6 = (1 - \mathcal{D}^2)(\mathcal{D}^4 + \mathcal{D}^2 + 1)$

$1 = (1 - \mathcal{D}^2)(\mathcal{D}^4 + \mathcal{D}^2 + 1)$

So, $\mathcal{D}^4 + \mathcal{D}^2 + 1$ is invertible on P_5,

and its inverse is $1 - \mathcal{D}^2$

$(\mathcal{D}^4 + \mathcal{D}^2 + 1)(f) = x^3 + x + 2$

$\Rightarrow f = (1 - \mathcal{D}^2)(x^3 + x + 2)$

$= x^3 + x + 2 - 6x$

$= x^3 - 5x + 2$