10/22 課題の復習

※ p 素数 このとき ${}_pC_k$ は p で割り切れる.

これは p が素数でないときは成立しない.

$${}_4C_2 = \frac{4\cdot 3}{2\cdot 1} = 6 \leftarrow 4\text{で割れない}$$

※の証明

$${}_pC_k = \frac{p!}{k!(p-k)!}$$

← p で割り切れる.

← p で割り切れない

Fermat の小定理

a 整数 p 素数 a と p は互いに素とする.

このとき $a^{p-1} \equiv a \pmod p$

証明 1.

帰納法で示す. $a=1$ のとき. O.K.

$a=k$ のとき, 成立すると仮定.

$$(k+1)^p = k^p + \sum_{j=0}^{p-1} {}_pC_j k^j + 1$$

$$\equiv k+1 \pmod p$$

← 全て p で割り切れる.

となり $k+1$ でも成り立つ.

証明 2. $a, 2a, 3a, \cdots, (p-1)a$ を全て

計算あわせるaだが, その前に

$\{1, \cdots, p-1\} \xrightarrow{a\text{倍}} \{a, 2a \cdots, (p-1)a\}$

↓ p で割った剰

$\{1, \cdots, p-1\}$

これは 1:1 の写像となる.

$ak \equiv ak' \pmod p \iff k \equiv k' \pmod p$

この考察をする. すると,

$$a\times 2a\times\cdots\times(p-1)a \equiv 1\cdot 2\cdots(p-1) \pmod p$$

$$\iff a^{p-1}(p-1)! \equiv (p-1)! \pmod p$$

$$\iff a^{p-1} \equiv 1 \pmod p$$

本日のキーワード 座標, 基底の変換

※ 行列 A, P があったとき, $P^{-1}AP$ には

どのような意味があるのか?

定義　ベクトル空間 V　$\{v_1 \cdots v_n\}$ 基底

Vの元 $v \in V$ の $\{v_1 \cdots v_n\}$ に関する座標

とは，基底の定義から

$$v = \sum_{i=1}^{n} a_i v_i$$

と書けるが，この a_i を並べた $(a_1 \cdots a_n)$ のこと．

例・$V = \mathbb{R}^3$　基底 $\{(1,0,0), (0,1,0), (0,0,1)\}$

$V \ni (a, b, c)$

$= a(1,0,0) + b(0,1,0) + c(0,0,1)$

座標は　(a, b, c)

・$V = \mathbb{R}^3$　基底 $\{(1,0,1), (1,0,-1), (0,1,0)\}$

$V \ni (2, 1, 1)$

$= \frac{3}{2}(1,0,1) + \frac{1}{2}(1,0,-1) + 1\cdot(0,1,0)$

座標は　$(\frac{3}{2}, \frac{1}{2}, 1)$

Q　V に2つの基底 $\{v_1 \cdots v_n\}$ $\{w_1 \cdots w_n\}$ があったとき，$v \in V$ の2つの座標の間にはどのような関係があるか？

A.　$\mathbb{R}^n$ から $\mathbb{R}^n$ への写像 F を

$V \ni v = (a_1 \cdots a_n) \in \mathbb{R}^n$ ← $\{v_1 \cdots v_n\}$ に関する座標

F ↓

$V \ni v = (b_1 \cdots b_n) \in \mathbb{R}^n$ ← $\{w_1 \cdots w_n\}$ に関する座標

まず F が線型写像であることを確認する．

$F((a_1 \cdots a_n) + (a_1', \cdots, a_n')) = F((a_1+a_1', \cdots, a_n+a_n'))$

を確かめる．

$F((a_1 \cdots a_n)) = (b_1 \cdots b_n)$　$F((a_1' \cdots a_n')) = (b_1' \cdots b_n')$

とすると　$v = \sum a_i v_i = \sum b_i w_i$

$v' = \sum a_i' v_i = \sum b_i' w_i$　となる．

$v + v' = \sum (a_i + a_i') v_i = \sum (b_i + b_i') w_i$

よって $F((a_1+a_1', \cdots, a_n+a_n')) = (b_1+b_1', \cdots, b_n+b_n')$

又 $F((a_1 \cdots a_n)) + F((a_1', \cdots, a_n'))$ //

$= (b_1 \cdots b_n) + (b_1' \cdots, b_n') = (b_1+b_1', \cdots, b_n+b_n')$

$\alpha \in k$ に対して

$F(\alpha(a_1 \cdots a_n)) = \alpha F((a_1 \cdots a_n))$ は略

次に F の表現行列を求める。これは、$n \times n$ 行列 A で

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

をみたすものであった。 $A = (a_{ij})$ とする

A の成分を求めるためには、$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

との積がどうなるか見れば良い。

$F((1,0,\cdots,0)) = (b_{11} \cdots b_{1n})$ とすると、

$V_1 = \sum_{j=1}^{n} b_{1j} w_j$

同様に

$F((0 \cdots \overset{i\text{番目}}{1} \cdots 0)) = (b_{i1} \cdots b_{in})$ とすると、

$V_i = \sum_{j=1}^{n} b_{ij} w_j$

$B = (b_{ij})$ とすれば

${}^tB = A \cdot E$ となる。つまり

$A = {}^tB$ である。さらに $V_i = \begin{pmatrix} V_{1i} \\ \vdots \\ V_{ni} \end{pmatrix}$ $W_i = \begin{pmatrix} W_{1i} \\ \vdots \\ W_{ni} \end{pmatrix}$

の場合に A を具体的に求めてみよう。このとき、

$V_i = \sum_{j=1}^{n} b_{ij} w_j$ であったが、これは

$$\begin{pmatrix} V_{i1} \\ \vdots \\ V_{in} \end{pmatrix} = b_{i1} \begin{pmatrix} W_{11} \\ \vdots \\ W_{n1} \end{pmatrix} + \cdots + b_{in} \begin{pmatrix} W_{1n} \\ \vdots \\ W_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} W_{11} & \cdots & W_{1n} \\ & & \\ W_{n1} & \cdots & W_{nn} \end{pmatrix} \begin{pmatrix} b_{i1} \\ \vdots \\ b_{in} \end{pmatrix}$$

$P = QB$ $P = (V_{ij})$ $Q = (W_{ij})$

$B = Q^{-1}P$ となる。

例題　$V=\mathbb{R}^3$　　V から V への線形写像 F を

$$F\left(\begin{pmatrix}x\\y\\z\end{pmatrix}\right)=\underbrace{\begin{pmatrix}6&-3&-7\\-1&2&1\\5&-3&-6\end{pmatrix}}_{A}\begin{pmatrix}x\\y\\z\end{pmatrix}$$

と定める．この線型写像の基底 $\left\{\begin{pmatrix}2\\1\\1\end{pmatrix}\begin{pmatrix}1\\-1\\1\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}$

に関する表現行列を求めよ．

解) V の点 (a,b,c) の基底 $\left\{\begin{pmatrix}2\\1\\1\end{pmatrix},\begin{pmatrix}1\\-1\\1\end{pmatrix},\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}$

に関する座標は $P=\begin{pmatrix}2&1&1\\1&-1&0\\1&1&1\end{pmatrix}$ とすれば

$P^{-1}\begin{pmatrix}a\\b\\c\end{pmatrix}$ となる．逆に基底 $\left\{\begin{pmatrix}2\\1\\1\end{pmatrix},\begin{pmatrix}1\\-1\\1\end{pmatrix},\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}$

で (a',b',c') となる点は 普通の座標では

$P\begin{pmatrix}a'\\b'\\c'\end{pmatrix}$ となる．　以上をまとめると

$$\begin{array}{ccc}\mathbb{R}^3 & \xrightarrow{F} & \mathbb{R}^3 \\ {\scriptstyle\times P}\uparrow & & \uparrow{\scriptstyle\times P} \\ \mathbb{R}^3 & \xrightarrow[F]{} & \mathbb{R}^3\end{array}\qquad \begin{array}{l}\leftarrow \times A\\ \text{右の図式となる．}\\ \text{よって求める表現行列}\\ \text{を } B \text{ とすれば}\end{array}$$

$$B=P^{-1}AP$$

まとめの演習

Q　$A^2=A$ をみたす行列は ある行列 P があり，

$P^{-1}AP=\begin{pmatrix}E&O\\O&O\end{pmatrix}$　　$E=\begin{pmatrix}1&&0\\&\ddots&\\0&&1\end{pmatrix}$ 単位行列

O ← 全ての成分が0

解　A を $n\times n$ 行列とし，$V=\mathbb{R}^n$ とする．

$V_1=\{x\in V \mid Ax=x\}$

$V_2=\{x\in V \mid Ax=0\}$

すると　$V=V_1\oplus V_2$ となる 実際

$V\ni y=(y-Ay)+Ay$　　より　$V=V_1+V_2$

$\in V_2$　　$\in V_1$

又　$V_1\cap V_2\ni y$ とすれば　$Ay=y=0$　　$V_1\cap V_2=0$

そこで V_1 と V_2 の基底であわせると V の基底 となるもの

を取り，それを並べたものを P とする．定義より $P^{-1}AP=\begin{pmatrix}E&O\\O&O\end{pmatrix}$