巡回行列の性質と離散フーリエ変換

@Metachick_2021

2026 年 5 月 7 日

1 演算の性質

【定義 1.1】巡回行列

体 K 上の n 次元正方行列 C が、ある n 個の係数 $a_0, \cdots, a_{n-1}$ を用いて、以下のように表現できるとき、C を巡回行列という。また、n 次元の巡回行列の全体を $\mathcal{C}_n(K)$ と表記する。

$$C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

以降の命題や定理において、断りのない限り C は n 次巡回行列であり、上のような $a_0, \cdots, a_{n-1}$ による表示を持つものとする。

簡単な成分計算により、加法と乗法で閉じていることがわかる。また、加法と乗法の結合律や分配律などは $M_n(K)$ の構造を引き継いでいるから成立する。これにより、$\mathcal{C}_n(K)$ は環を成すことがわかる。あるいは、次に証明する定理 1.2 に登場する行列 P を用いれば成分計算を回避することもできる。これにより、可換性も直ちにわかる。

【定理 1.2】演算の構造

以下の環同型が成り立つ。

$$\mathcal{C}_n(K) \cong K[x]/(x^n - 1)$$

証明　行列 $P, C \in \mathcal{C}_n(K)$ を

$$P = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix}$$

で定める。このとき、

$$C = a_0 P^0 + a_1 P^1 + \cdots + a_{n-1} P^{n-1}$$

となる。写像 $\varphi\colon\ K[x] \longrightarrow \mathcal{C}_n(K)$ を以下で定める。

$$\varphi\colon\ K[x] \longrightarrow \mathcal{C}_n(K), \qquad \varphi\left(\sum_{i=0}^{m} c_i x^i\right) = \sum_{i=0}^{m} c_i P^i,$$

このとき φ は準同型である。また、φ は全射であり、$\mathrm{Ker}\varphi = (x^n - 1)$ となる。よって、準同型定理より、$\mathcal{C}_n(K) \cong K[x]/(x^n - 1)$ を得る。 □

【定理 1.3】

以下の環同型が成り立つ。

$$\mathcal{C}_n(\mathbb{R}) \cong \mathbb{R}[x]/(x^n - 1), \quad \mathcal{C}_n(\mathbb{C}) \cong \mathbb{C}^n$$

証明　$\mathbb{C}$ 上では、$x^n - 1$ は n 個の一次式の積に因数分解できるので、中国剰余定理を用いれば、

$$\mathcal{C}_n(\mathbb{C}) \cong \mathbb{C}[x]/(x^n - 1) \cong \mathbb{C}[x]/(x-1) \times \mathbb{C}[x]/(x - e^{\frac{2i\pi}{n}}) \times \cdots \times \mathbb{C}[x]/(x - e^{\frac{2i\pi(n-1)}{n}}) \cong \mathbb{C}^n$$

を得る。 □

2　行列式の計算

巡回行列の行列式は比較的簡単に計算することができる。

【定理 2.1】

巡回行列 $C \in \mathcal{C}_n(\mathbb{C})$ に対して、$\xi = e^{\frac{2i\pi}{n}}$, $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ とすれば次が成り立つ。

$$\det(C) = f(1) f(\xi) f(\xi^2) \cdots f(\xi^{n-1})$$

証明　行列 $Z \in \mathcal{C}_n(\mathbb{C})$ を

$$Z = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \\ 1 & \xi^2 & \xi^4 & \cdots & \xi^{2(n-1)} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ 1 & \xi^{n-1} & \xi^{2(n-1)} & \cdots & \xi^{(n-1)^2} \end{pmatrix}$$

で定める。このとき、ヴァンデルモンドの公式より Z は正則である。積 CZ を計算すると

$$CZ = \begin{pmatrix} f(1) & f(\xi) & f(\xi^2) & \cdots & f(\xi^{n-1}) \\ f(1) & f(\xi)\xi & f(\xi^2)\xi^2 & \cdots & f(\xi^{n-1})\xi^{n-1} \\ f(1) & f(\xi)\xi^2 & f(\xi^2)\xi^4 & \cdots & f(\xi^{n-1})\xi^{2(n-1)} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ f(1) & f(\xi)\xi^{n-1} & f(\xi^2)\xi^{2(n-1)} & \cdots & f(\xi^{n-1})\xi^{(n-1)^2} \end{pmatrix}$$

となる。これより、行列式の多重線型性と併せて

$$\det(C) = \frac{\det(CZ)}{\det(Z)} = \frac{f(1)f(\xi)f(\xi^2)\cdots f(\xi^{n-1})\det(Z)}{\det(Z)} = f(1)f(\xi)f(\xi^2)\cdots f(\xi^{n-1})$$

を得る。 □

この Z で定まるような線型変換を離散フーリエ変換と呼ぶ。

3　複素ベクトル空間上の巡回行列

定理 1.3 より、$\mathcal{C}_n(\mathbb{C}) \cong \mathbb{C}^n$ であった。具体的に、どのような n 個の複素数と対応しているのかを見てみる。

【定理 3.1】巡回行列の対角化

巡回行列 $C \in \mathcal{C}_n(\mathbb{C})$ に対して、行列 Z を定理 2.1 と同様に定めれば、$Z^{-1}CZ$ は対角行列となる。また、C は正規行列である。

証明　λ_k を $\lambda_k = f(\xi^k)$ $(k = 0, \ldots, n-1)$ で定める。

$$CZ = Z\,\mathrm{diag}(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}).$$

であるから、$Z^{-1}CZ = \mathrm{diag}(\lambda_0, \ldots, \lambda_{n-1})$ が得られる。

行列 Z を正規化する。

$$F = \frac{1}{\sqrt{n}}\left(\xi^{jk}\right)_{j,k=0}^{n-1}$$

を用いると F はユニタリであり（$F^{-1} = F^*$）、同様に

$$F^* C F = \mathrm{diag}(\lambda_0, \ldots, \lambda_{n-1})$$

が成り立つ。したがって任意の複素巡回行列はユニタリ対角化可能で、特に正規行列。 □

【定理 3.2】同型の明示

以下で定まる写像 Φ は環同型である。

$$\Phi : \mathcal{C}_n(\mathbb{C}) \longrightarrow \mathbb{C}^n, \qquad \Phi(C) = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$$

証明　定理 3.1 より、複素巡回行列は Z によって同時対角化可能である。Z の正則性により固有ベクトルが基底を成すため写像 $\Phi(C) = (\lambda_0, \ldots, \lambda_{n-1})$ は全射かつ単射であり、行列の和と積はそれぞれ成分ごとの和と積に写る。すなわち、C_1, C_2 に対して

$$\Phi(C_1 + C_2) = \Phi(C_1) + \Phi(C_2), \qquad \Phi(C_1 C_2) = \Phi(C_1) \odot \Phi(C_2),$$

ここで $\odot$ は成分ごとの積である。従って Φ は環同型である。 □

Φ の逆写像を考えれば、固有値 λ_k から元の係数 $(a_0, \ldots, a_{n-1})$ を復元する式が得られる。この操作は逆離散フーリエ変換と呼ばれる。

$$a_j = \frac{1}{n}\sum_{k=0}^{n-1} \lambda_k\, \xi^{-jk} \qquad (j = 0, \ldots, n-1)$$

4　離散フーリエ変換の性質

【定義 4.1】離散フーリエ変換（DFT）

ベクトル $x = (x_0, \ldots, x_{n-1})^T \in \mathbb{C}^n$ に対して離散フーリエ変換を行列 Z により定まる線形写像、すなわち、次で定義する。

$$(\mathcal{F}x)_k := \sum_{j=0}^{n-1} x_j\, \xi^{jk}, \qquad (k = 0, \ldots, n-1)$$

【定理 4.2】畳み込み定理

任意の $x, y \in \mathbb{C}^n$ に対し、添え字を n を法として考える巡回畳み込み

$$(x * y)_m := \sum_{j=0}^{n-1} x_j \, y_{m-j} \qquad (m = 0, \dots, n-1)$$

を定める。このとき、離散フーリエ変換 $\mathcal{F}$ について次が成り立つ。

$$\mathcal{F}(x * y) = (\mathcal{F}x) \odot (\mathcal{F}y)$$

証明　定義から

$$\begin{aligned}(\mathcal{F}(x * y))_k &= \sum_{m=0}^{n-1} (x * y)_m \, \xi^{mk} = \sum_{m=0}^{n-1} \Bigl(\sum_{j=0}^{n-1} x_j \, y_{m-j} \Bigr) \xi^{mk} \\ &= \sum_{j=0}^{n-1} x_j \sum_{m=0}^{n-1} y_{m-j} \, \xi^{mk}\end{aligned}$$

添字を $r = m - j$ と置き換えると、

$$\sum_{m=0}^{n-1} y_{m-j} \, \xi^{mk} = \sum_{r=0}^{n-1} y_r \, \xi^{(r+j)k} = \xi^{jk} \sum_{r=0}^{n-1} y_r \, \xi^{rk}.$$

これを代入すると

$$(\mathcal{F}(x * y))_k = \Bigl(\sum_{j=0}^{n-1} x_j \, \xi^{jk} \Bigr) \Bigl(\sum_{r=0}^{n-1} y_r \, \xi^{rk} \Bigr) = (\mathcal{F}x)_k (\mathcal{F}y)_k,$$

すなわち、$\mathcal{F}(x * y) = (\mathcal{F}x) \odot (\mathcal{F}y)$ が得られる。 □

上のような直接的な計算以外にも、線形代数の知識を使って工夫することもできる。

証明　x を係数とする巡回行列 $C(x) \in \mathcal{C}_n(\mathbb{C})$ を $C(x)_{m,j} = x_{m-j \pmod n}$ と定めれば、線型作用としての畳み込みは行列積にほかならない。

$$C(x) \, y = x * y$$

一方、定理 3.1 の対角化より

$$Z^{-1} C(x) Z = \mathrm{diag}(\mathcal{F}x),$$

したがって $\mathcal{F}(x * y) = \mathcal{F}(C(x)y) = \mathrm{diag}(\mathcal{F}x) \, \mathcal{F}y$ となり、成分ごとの積への対応が得られる。 □

【定理 4.3】

任意の $x, y \in \mathbb{C}^n$ に対して、離散フーリエ変換 $\mathcal{F} = Z$ とその像 $X = \mathcal{F}x,\ Y = \mathcal{F}y$ について次の等式が成り立つ。

$$\sum_{j=0}^{n-1} x_j \overline{y_j} \ = \ \frac{1}{n} \sum_{k=0}^{n-1} X_k \overline{Y_k}$$

証明　非正規化行列 Z の列ベクトルは互いに直交で、各列のノルムは $\sqrt{n}$ であるから

$$Z^* Z = nI.$$

よって $X = Zx,\ Y = Zy$ とおくと

$$X^* Y = x^* Z^* Z y = n\, x^* y$$

両辺を n で割れば

$$x^* y = \frac{1}{n} X^* Y$$

が得られる。 □

【定理 4.4】パーセバルの等式

任意の $x, y \in \mathbb{C}^n$ に対して、離散フーリエ変換 $\mathcal{F} = Z$ とその像 $X = \mathcal{F}x,\ Y = \mathcal{F}y$ について次の等式が成り立つ。

$$\sum_{j=0}^{n-1} |x_j|^2 \ = \ \frac{1}{n} \sum_{k=0}^{n-1} |X_k|^2$$

証明　定理 4.3 において、$x = y$ とすればよい。 □