1　巡回行列式

Frobenius によって群の表現論が始まるきっかけになった, 巡回行列式について考えよう.

- **1-1 : 巡回行列式**

$X_0, X_1, \ldots, X_{n-1}$ を不定元とする. このとき, 行列式

$$C(X_0, X_1, \ldots, X_{n-1}) = \mathsf{det} \begin{pmatrix} X_0 & X_1 & X_2 & \cdots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \cdots & X_{n-2} \\ X_{n-2} & X_{n-1} & X_0 & \cdots & X_{n-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ X_1 & X_2 & X_3 & \cdots & X_0 \end{pmatrix}$$

を n **次巡回行列式** という.

例 1-1　(1) $n = 1$ のときは

$$C(X_0, X_1) = X_0^2 - X_1^2 = (X_0 + X_1)(X_0 - X_1)$$

と因数分解される.

(2) $n = 2$ のときは

$$C(X_0, X_1, X_2) = X_0^3 + X_1^3 + X_2^3 - 3X_0X_1X_2 = (X_0 + X_1 + X_2)(X_0^2 + X_1^2 + X_2^2 - X_0X_1 - X_1X_2 - X_0X_2)$$

である. ここで, ω を 1 の原始 3 乗根のひとつとすると上の式は更に次のように因数分解される.

$$C(X_0, X_1, X_2) = (X_0 + X_1 + X_2)(X_0 + \omega X_1 + \omega^2 X_2)(X_0 + \omega^2 X_1 + \omega X_2)$$

レポート 1-1　上の因数分解が正しいことを確かめよ.

これらのことから, 巡回行列式は複素数の範囲で 1 次式の積に因数分解可能ではないか, という予想ができる. 実際, この章での目標は, 次の定理の証明を与えることである.

定理 1.1. $z \in \mathbb{C}$ を 1 の原始 n 乗根とする. このとき,

$$C(X_0, X_1, \ldots, X_{n-1}) = \prod_{j=0}^{n-1} (X_0 + z^j X_1 + \cdots + z^{(n-1)j} X_{n-1})$$

である.

- **1-2 : Vandermonde の行列式**

線形代数において, Vandermonde の行列式と呼ばれる有名な行列式について思い出しておこう.

命題 1.2. $X_0, X_1, \ldots, X_{n-1}$ を不定元とする. このとき, 行列式

$$V_n := \mathsf{det} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ X_1 & X_2 & X_3 & \cdots & X_n \\ X_1^2 & X_2^2 & X_3^2 & \cdots & X_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ X_1^{n-1} & X_2^{n-1} & X_3^{n-1} & \cdots & X_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (X_j - X_i)$$

が成り立つ.

担当：茨城大学 情報科学領域　宮本 賢伍

証明. 添字 $i \neq j$ について, $X_i = X_j$ のとき, 同じ列が現れるので行列式 V_n の値は 0 である. よって因数定理より, V_n は $X_j - X_i$ $(i < j)$ を因数にもつ. よって, ある整数係数の多項式 $f(X_1, X_2, \ldots, X_n)$ が存在して

$$V_n = f(X_1, X_2, \ldots, X_n) \prod_{1 \leq i < j \leq n} (X_j - X_i)$$

となる. 両辺は $X_1, X_2, \ldots, X_n$ に関して $\dfrac{n(n-1)}{2}$ 次式だから $f(X_1, X_2, \ldots, X_n)$ は定数である. そこで, $X_2 X_3^2 \cdots X_n^{n-1}$ の計数を比較して $f(X_1, X_2, \ldots, X_n) = 1$ を得る. □

この Vandermonde の行列式についての結果を用いて, **定理 1.1** の証明を与えよう.

$$f(t) = X_0 + X_1 t + \cdots + X_{n-1} t^{n-1}$$

とおく. このとき, 証明することは

$$C(X_0, X_1, \ldots, X_{n-1}) = \prod_{j=0}^{n-1} f(z^j)$$

である. ここで, $A = (X_{j-i})_{0 \leq i,j \leq n-1}$, $Z = (z^{ij})_{0 \leq i,j \leq n-1}$ とおき, 積 AZ を計算すると

$$\begin{aligned}
AZ &= \begin{pmatrix} X_0 & X_1 & X_2 & \cdots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \cdots & X_{n-2} \\ X_{n-2} & X_{n-1} & X_0 & \cdots & X_{n-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ X_1 & X_2 & X_3 & \cdots & X_0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z & z^2 & \cdots & z^{n-1} \\ 1 & z^2 & z^4 & \cdots & z^{2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & z^{n-1} & z^{2(n-1)} & \cdots & z^{(n-1)^2} \end{pmatrix} \\
&= \begin{pmatrix} \sum X_k & \sum z^k X_k & \sum z^{2k} X_k & \cdots & \sum z^{(n-1)k} X_k \\ \sum X_k & \sum z^{k+1} X_k & \sum z^{2(k+1)} X_k & \cdots & \sum z^{(n-1)(k+1)} X_k \\ \sum X_k & \sum z^{k+2} X_k & \sum z^{2(k+2)} X_k & \cdots & \sum z^{(n-1)(k+2)} X_k \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \sum X_k & \sum z^{k+n-1} X_k & \sum z^{2(k+n-1)} X_k & \cdots & \sum z^{(n-1)(k+n-1)} X_k \end{pmatrix} \\
&= \begin{pmatrix} f(1) & f(z) & f(z^2) & \cdots & f(z^{n-1}) \\ f(1) & f(z)z & f(z^2)z^2 & \cdots & f(z^{n-1})z^{n-1} \\ f(1) & f(z)z^2 & f(z^2)z^4 & \cdots & f(z^{n-1})z^{2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ f(1) & f(z)z^{n-1} & f(z^2)z^{2(n-1)} & \cdots & f(z^{n-1})z^{(n-1)^2} \end{pmatrix}
\end{aligned}$$

であるから,

$$\begin{aligned}
\mathsf{det}(AZ) &= f(1)f(z)f(z^2)\cdots f(z^{n-1}) \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z & z^2 & \cdots & z^{n-1} \\ 1 & z^2 & z^4 & \cdots & z^{2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & z^{n-1} & z^{2(n-1)} & \cdots & z^{(n-1)^2} \end{pmatrix} \\
&= f(1)f(z)f(z^2)\cdots f(z^{n-1})\mathsf{det}(Z)
\end{aligned}$$

を得る. ここで, z は 1 の原始 n 乗根だから $\mathsf{det}(Z) \neq 0$ である. 従って,

$$\mathsf{det}(A) = f(1)f(z)f(z^2)\cdots f(z^{n-1})$$

となり, これが示したい式であった.

レポート 1-2　z は 1 の原始 n 乗根だから $\mathsf{det}(Z) \neq 0$ となる理由を述べよ.

担当：茨城大学 情報科学領域　宮本 賢伍

- **1-3 : 3 次方程式の解の公式**

3 次方程式 $x^3+ax^2+bx+c=0$ を考える. $a\neq 0$ であれば,

$$x^3+ax^2+bx+c=\left(x+\frac{a}{3}\right)^3+\left(b-\frac{a^2}{3}\right)x+c-\frac{a^3}{27}$$

なので, $y=x+\frac{a}{3}$ とおくことで結局 $y^3+py+q=0$ の形に変形できる. 従って, 改めて $x^3+px+q=0$ の形の解放を与えれば, 任意の 3 次方程式が解けるようになる. ω を 1 の原始 3 乗根のひとつとする. このとき, **定理 1.1** から

$$C(x,-u,-v)=(x-u-v)(x-\omega u-\omega^2 v)(x-\omega^2 u-\omega v)$$

が成立する. 一方, $C(x,-u,-v)=x^3-3uvx-u^3-v^3$ だから係数比較をすると

$$p=-3uv,\quad q=-u^3-v^3$$

となる. これを満たす u,v が求まったとすれば,

$$x=u+v,\quad x=\omega u+\omega^2 v,\quad x=\omega^2 u+\omega v$$

として 3 つの解が得られたことになる. $p=-3uv$ より, $u^3v^3=-\frac{p^3}{27}$ であり, $q=-u^3-v^3$ と同時に満たすものを考えればよい. 解と係数の関係より, u^3, v^3 は 2 次方程式

$$X^2+qX-\frac{p^3}{27}=0$$

の解である. こうして u^3, v^3 の 3 乗根のうち, $p=-3uv$ を満たすものが $x^3+px+q=0$ の解である.