

# 多変数の円分多項式

竹内珠佑<sup>†</sup>

## 概要

この論文では, 多変数多項式

$$\prod_{b_2, b_3, \dots, b_m=0}^{n-1} \left( x_1 + \sum_{i=2}^m \zeta^{b_i} x_i \right) \text{ where } m, n \in \mathbb{Z}_{>1}, \zeta = \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$$

について考える. ここではこれの各項の各変数の次数が  $n$  の倍数であることや  $\mathbb{Z}$ -係数であることを証明する (この多項式の約数についても同様のことを証明する). 後者については二つの証明方法を提示する.

**キーワード:** 円分多項式, 多変数多項式, ヘロンの公式

## 1 はじめに

1977TOT 秋 SA で次のような問題があった [1].

$\sqrt{1} \pm \sqrt{2} \pm \dots \pm \sqrt{100}$  で表される (符号の組み合わせをすべて考えた) ものをすべてかけ合せたものは整数であることを示せ.

この問題については,

条件 1. 各項の各変数の次数が  $n$  の倍数である

を示せばいいが, この一般化である予想 1 はこれだけでは十分でない. なぜなら,  $\mathbb{Z}$ -係数であるかが明らかではないからである. したがって,

条件 2.  $f_m(\mathbf{x}_m) \in \mathbb{Z}[\mathbf{x}_m]$

も示す必要がある.

## 2 予想

**予想 1.**  $m, n \in \mathbb{Z}_{>1}, a_i \in \mathbb{Z}_{>0}, \zeta = \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$ . この時, 以下の数は整数か?

$$f_m(\sqrt[n]{a_1}, \sqrt[n]{a_2}, \dots, \sqrt[n]{a_m}) = \prod_{b_2, b_3, \dots, b_m=0}^{n-1} \left( \sqrt[n]{a_1} + \sum_{i=2}^m \zeta^{b_i} \sqrt[n]{a_i} \right)$$

右辺は,  $n^{m-1}$  個の積を表している.

---

<sup>†</sup>大阪公立大学工業高等専門学校 2 年

予想 2.

$$g_m(\mathbf{x}_m) = \prod_{\substack{0 < b_2, b_3, \dots, b_m \leq n \\ (b, n) = 1}} \left( x_1 + \sum_{i=2}^m \zeta^{b_i} x_i \right) \in \mathbb{Z}[\mathbf{x}_m] ?$$

ただし,  $\mathbf{x}_m = (x_1, \dots, x_m)$ ,  $\mathbb{Z}[\mathbf{x}_m]$  で,  $(x_i)_{i=1, \dots, m}$  を不定元とする  $\mathbb{Z}$ -係数多項式環を表すものとする.

### 3 証明

#### 3.1 予想 1.

**Part 1.** 任意の  $i (1 \leq i \leq m)$  に対して,

$$f_m(x_1, \dots, \zeta x_i, \dots, x_m) = f_m(x_1, \dots, x_i, \dots, x_m)$$

が成り立ち, これは条件 1. を意味している. □

**Part 2.** 数学的帰納法によって証明する. まずは,  $n$  を任意にとってきて固定する. 次に,  $m = m_1 - 1$  で条件 2. が満足していると仮定して,  $m = m_1 \in \mathbb{Z}_{>2}$  でも成り立つことを示す.  $b_{m_1}$  を固定すると次がわかる:

$$f_{m_1}(\mathbf{x}_{m_1}) = f_{m_1-1}(\mathbf{x}_{m_1-1,0}) f_{m_1-1}(\mathbf{x}_{m_1-1,1}) \cdots f_{m_1-1}(\mathbf{x}_{m_1-1,n-1}).$$

ここで,  $\mathbf{x}_{m_1-1,i} = (x_1 + \zeta^i x_{m_1}, x_2, \dots, x_{m_1-1})$  とした. 仮定より,  $f_{m_1-1}(\mathbf{x}_{m_1-1}) \in \mathbb{Z}[\mathbf{x}_{m_1-1}]$  であるから:

$$f_{m_1}(\mathbf{x}_{m_1}) = \prod_{i=0}^{n-1} (a_0 + \zeta^i a_1 + \zeta^{2i} a_2 + \cdots + \zeta^{(n-1)i} a_{n-1}) \quad (a_i \in \mathbb{Z}[\mathbf{x}_{m_1}]). \quad (1)$$

と書ける.

**補題 3.1** (ヴォルデモンドの行列式).

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i < j} (x_j - x_i).$$

**補題 3.2.**  $l \in \mathbb{Z}_{>0}, \eta = \exp\left(\frac{2\pi\sqrt{-1}}{l}\right),$

$$\begin{vmatrix} x_0 & x_1 & \cdots & x_{l-1} \\ x_{l-1} & x_0 & \cdots & x_{l-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{vmatrix} = \prod_{i=0}^{l-1} (x_0 + \eta^i x_1 + \eta^{2i} x_2 + \cdots + \eta^{(l-1)i} x_{l-1}).$$

**Proof.**

$$\begin{vmatrix} x_0 & x_1 & \cdots & x_{l-1} \\ x_{l-1} & x_0 & \cdots & x_{l-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{vmatrix} \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \eta & \eta^{2 \cdot 1} & \cdots & \eta^{l-1} \\ 1 & \eta^{1 \cdot 2} & \eta^{2 \cdot 2} & \cdots & \eta^{(l-1) \cdot 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta^{l-1} & \eta^{2(l-1)} & \cdots & \eta^{(l-1)(l-1)} \end{vmatrix} \\
= \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \eta & \eta^{2 \cdot 1} & \cdots & \eta^{l-1} \\ 1 & \eta^{1 \cdot 2} & \eta^{2 \cdot 2} & \cdots & \eta^{(l-1) \cdot 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta^{l-1} & \eta^{2(l-1)} & \cdots & \eta^{(l-1)(l-1)} \end{vmatrix} \prod_{i=0}^{l-1} (x_0 + \eta^i x_1 + \eta^{2i} x_2 + \cdots + \eta^{(l-1)i} x_{l-1})$$

であるから, 最初の式の二つ目の行列式および, 二つ目の式の最初の行列式が 0 出ないことを示せばよく, これは補題 3.1 と  $\eta$  が 1 の原始  $l$  乗根であることよりわかる:

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \eta & \eta^{2 \cdot 1} & \cdots & \eta^{l-1} \\ 1 & \eta^{1 \cdot 2} & \eta^{2 \cdot 2} & \cdots & \eta^{(l-1) \cdot 2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta^{l-1} & \eta^{2(l-1)} & \cdots & \eta^{(l-1)(l-1)} \end{vmatrix} = \prod_{i < j} (\eta^j - \eta^i) \neq 0. \quad \square$$

補題 3.2 と式 (1) より,  $f_{m_1}(\mathbf{x}_{m_1}) \in \mathbb{Z}[\mathbf{x}_{m_1}]$  が示される:

$$f_{m_1}(\mathbf{x}_{m_1}) = \begin{vmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{vmatrix} \in \mathbb{Z}[\mathbf{x}_m]. \quad (2)$$

あとは,  $f_2(\mathbf{x}_2) \in \mathbb{Z}[\mathbf{x}_2]$  を示せばいい:

$$\begin{aligned} f_2(\mathbf{x}_2) &= \prod_{i=0}^{n-1} (x_1 + \zeta^i x_2) = (-x_2)^n \prod_{i=0}^{n-1} \left( \frac{x_1}{-x_2} - \zeta^i \right) = (-x_2)^n \left( \left( \frac{x_1}{-x_2} \right)^n - 1 \right) \\ &= x_1^n - (-1)^n x_2^n \in \mathbb{Z}[\mathbf{x}_2]. \quad \square \end{aligned}$$

### 3.2 予想 2.

予想 2 についても, 同様の手法を用いて解くことができる.

**Proof.**  $m = m_1 - 1$  で成り立っていると仮定して,  $m = m_1$  でも成り立つことを示す.  $b_m$  を固定すると:

$$g_{m_1}(\mathbf{x}_{m_1}) = \prod_{\substack{0 < i \leq n \\ (i, n)=1}} g_{m_1-1}(\mathbf{x}_{m_1-1, i})$$

がわかる. ここで, 仮定より,  $g_{m_1-1}(\mathbf{x}_{m_1-1}) \in \mathbb{Z}[\mathbf{x}_{m_1-1}]$  であるから:

$$g_{m_1}(\mathbf{x}_{m_1}) = \prod_{\substack{0 < i \leq n \\ (i, n)=1}} (a_0 + \zeta^i a_1 + \zeta^{2i} a_2 + \cdots + \zeta^{(n-1)i} a_{n-1}) \quad (a_i \in \mathbb{Z}[\mathbf{x}_{m_1}]) \quad (3)$$

と書ける.

**補題 3.3.**  $L/K$  は体の拡大.

$$K(x) \cap L[x] = K[x].$$

**Proof.** 明らかに  $K(x) \cap L[x] \supset K[x]$  であるから,  $K(x) \cap L[x] \subset K[x]$  を示す. 任意に  $F(x) \in K(x) \cap L[x]$  をとる.  $F(x) \in K(x)$  であるから,  $G(x), H(x) \in K[x]$  が存在して,

$$F(x) = \frac{G(x)}{H(x)}$$

をみます. また,

$$G(x) = q(x)H(x) + r(x) \text{ and } \deg r < \deg H$$

をみます. これを上式に代入にすると,

$$\begin{aligned} F(x) &= q(x) + \frac{r(x)}{H(x)} \\ \iff H(x)[F(x) - q(x)] &= r(x). \end{aligned}$$

$0 \neq F(x) - q(x) \in L[x]$  であれば,  $\deg(F - q) \geq 0$  であるから  $\deg H \geq \deg r$  となり矛盾する. よって,

$$F(x) = q(x) \in K[x] \text{ i.e. } K(x) \cap L[x] \subset K[x] \quad \square$$

**補題 3.4.**  $L/K$  は体の拡大.

$$K(\mathbf{X}) \cap L[\mathbf{X}] = K[\mathbf{X}].$$

**Proof.**  $\mathbf{X}_k = (X_1, \dots, X_k)$  とする. 数学的帰納法で証明する. 補題 3.3 があるので, 任意の  $k \geq 2$  に対して,

$$K(\mathbf{X}_{k-1}) \cap L[\mathbf{X}_{k-1}] = K[\mathbf{X}_{k-1}] \implies K(\mathbf{X}_k) \cap L[\mathbf{X}_k] = K[\mathbf{X}_k]$$

を示せば十分である.  $K(\mathbf{X}_k) \cap L[\mathbf{X}_k] \supset K[\mathbf{X}_k]$  は明らかであるから  $K(\mathbf{X}_k) \cap L[\mathbf{X}_k] \subset K[\mathbf{X}_k]$  を示す. さて,

$$\begin{aligned} K(\mathbf{X}_k) \cap L[\mathbf{X}_k] &\subset K(X_1)(X_2, \dots, X_k) \cap L(X_1)[X_2, \dots, X_k] = K(X_1)[X_2, \dots, X_k] \quad (\because \text{仮定}) \\ &\subset K(X_2)(X_1, \dots, X_k) \cap L(X_2)[X_1, \dots, X_k] = K(X_2)[X_1, \dots, X_k] \quad (\because \text{仮定}) \\ \implies K(\mathbf{X}_k) \cap L[\mathbf{X}_k] &\subset K(X_1)[X_2, \dots, X_k] \cap K(X_2)[X_1, \dots, X_k] \\ &= K(X_1)[X_2][X_3, \dots, X_k] \cap K(X_2)[X_1][X_3, \dots, X_k] \end{aligned}$$

であるから,  $K(X_1)[X_2] \cap K(X_2)[X_1] \subset K[\mathbf{X}_2]$  を示せばいい. ( $k = 2$  のときは,  $K(X_1)[X_2][X_3, \dots, X_k] = K(X_1)[X_2]$  などとする.) 任意に  $F(\mathbf{X}_2) \in K(X_1)[X_2] \cap K(X_2)[X_1]$  をとる. このとき,

$$F(\mathbf{X}_2) = \sum_{i=0}^{l_1} \left[ q_{i,1}(X_1) + \frac{r_{i,1}(X_1)}{G_{i,1}(X_1)} \right] X_2^i = \sum_{i=0}^{l_2} \frac{H_{i,2}(X_2)}{G_{i,2}(X_2)} X_1^i.$$

と書ける. ( $l_i \in \mathbb{Z}_{\geq 0}, q_{i,1}, r_{i,1}, G_{i,1} \in K[X_1], H_{i,2}, G_{i,2} \in K[X_2], \deg r_{i,1} < \deg G_{i,1}$ ) 右二つを変形していくと,

$$\sum_{i=0}^{l_1} r_{i,1}(X_1) X_2^i \prod_{j \neq i} G_{j,1}(X_1) = \prod_{i=0}^{l_1} G_{i,1}(X_1) \left[ \sum_{i=0}^{l_2} \frac{H_{i,2}(X_2)}{G_{i,2}(X_2)} X_1^i - \sum_{i=0}^{l_1} q_{i,1}(X_1) X_2^i \right]$$

となつて、 $\sum_i \frac{H_{i,2}(X_2)}{G_{i,2}(X_2)} X_1^i - \sum_i q_{i,1}(X_1) X_2^i \neq 0$  であるとき、この両辺を  $X_1$  の一変数多項式として見たときの  $\deg$  を考えると矛盾する:

$$\deg(LHS) < \sum_i \deg G_{i,1} \leq \deg(RHS).$$

よつて、

$$\sum_{i=0}^{l_1} r_{i,1}(X_1) X_2^i \prod_{j \neq i} G_{j,1}(X_1) = 0 \implies r_{0,1} = \cdots = r_{l_1,1} = 0 \quad (\because G_{i,1} \neq 0)$$

$$\implies F(\mathbf{X}_2) = \sum_{i=0}^{l_1} q_{i,1}(X_1) X_2^i \in K[\mathbf{X}_2]. \quad \square$$

**系 3.5.**  $\mathbb{Q}(\mathbf{X}) \cap \mathbb{C}[\mathbf{X}] = \mathbb{Q}[\mathbf{X}]$ .

**定義 3.6.**  $P(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}]$  が **monic-like** であるとは、次をみたすことを言う。

- 任意の  $i$  に対して、 $P(X_i) \in \mathbb{Q}[\cdots, X_{i-1}, X_{i+1}, \cdots][X_i]$  として見たときに、 $P, -P$  の何れかが monic である。

**補題 3.7.**  $F(\mathbf{X}), G(\mathbf{X}) \in \mathbb{Q}[\mathbf{X}], F, G$  :monic-like.

- $F(\mathbf{X})G(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}] \implies F(\mathbf{X}), G(\mathbf{X}) \in \mathbb{Z}[\mathbf{X}]$

**Proof.** UFD 上のガウスの補題を考えるといい。 □

**定義 3.8.**  $l \in \mathbb{Z}_{>0}, \eta = \exp\left(\frac{2\pi\sqrt{-1}}{l}\right),$

$$h_l(\mathbf{x}) := \prod_{\substack{0 < i \leq l \\ (i,l)=1}} (x_1 + \eta^i x_2 + \eta^{2i} x_3 + \cdots).$$

**系 3.9.**  $h$  は monic-like.

**Proof.**  $l \neq 1$  の時は、

$$\sum_{\substack{0 < i \leq l \\ (i,l)=1}} i = \frac{l}{2} \cdot \varphi(l)$$

から従う。 $l = 1$  は明らか。 □

**補題 3.10.**  $h_l(\mathbf{x}_k) \in \mathbb{Z}[\mathbf{x}_k]$ .

**Proof.**  $h_l(\mathbf{x}) = h_l(x_1 + x_{l+1} + \cdots, x_2 + x_{l+2} + \cdots, \cdots, x_l + x_{2l} + \cdots)$  であるから、 $k = l$  だけ示せば十分である。数学的帰納法によって証明する。 $l = 1$  では明らかに成り立つ。 $l = 1, \cdots, l_1 - 1$  で主張が成り立つと仮

定したとき,  $l = l_1 \in \mathbb{Z}_{>1}$  でも成り立つことを示していく. 補題 3.2 より,

$$\prod_{d|l_1} h_d(\mathbf{x}_{l_1}) \in \mathbb{Z}[\mathbf{x}_{l_1}]. \quad (4)$$

また, 仮定より,

$$\prod_{l_1 \neq d|l_1} h_d(\mathbf{x}_{l_1}) \in \mathbb{Z}[\mathbf{x}_{l_1}]. \quad (5)$$

よって, 系 3.5 より,

$$h_{l_1}(\mathbf{x}_{l_1}) = \frac{\prod_{d|l_1} h_d(\mathbf{x}_{l_1})}{\prod_{l_1 \neq d|l_1} h_d(\mathbf{x}_{l_1})} \in \mathbb{Q}[\mathbf{x}_{l_1}]. \quad (6)$$

式 (4), (5), (6), 補題 3.7 及び系 3.9 より,  $h_{l_1}(\mathbf{x}_{l_1}) \in \mathbb{Z}[\mathbf{x}_{l_1}]$ .  $\square$

式 (3) と補題 3.10 より目標が達成される:

$$g_{m_1}(\mathbf{x}_{m_1}) = h_n(a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}[\mathbf{x}_{m_1}] \quad (7)$$

$\square$

## 4 別の証明

**Proof.** 予想 1 が  $\mathbb{Z}$ -係数であることだけを証明する. 各項の係数について考察する.

**補題 4.1.**  $A_l := \left\{ \exp\left(\frac{2k\pi\sqrt{-1}}{l}\right) : 0 < k \leq l \text{ and } (k, l) = 1 \right\}$ .  $A_{i_1}, \dots, A_{i_j}$  のすべての元の基本対称式は整数である.

**Proof.**  $i$  番目の円分多項式を  $\Phi_i$  とおく.

$$\prod_{k=1}^j \Phi_{i_k}(x) \in \mathbb{Z}[x]$$

より明らか.  $\square$

**補題 4.2** (対称式の基本定理).  $R$  を可換環, 対称式  $F(\mathbf{X}) \in R[\mathbf{X}]$ ,  $\mathbf{X}$  の  $i$  次の基本対称式を  $\sigma_i$  とする. この時,  $G(\mathbf{X}) \in R[\mathbf{X}]$  が一意に存在して次をみたす:

$$F(\mathbf{X}) = G(\sigma_1, \dots).$$

**系 4.3.**  $k$  変数の  $\mathbb{Z}$ -係数の対称多項式  $p$  であるとき,

$$p(1, \dots, \eta^{k-1}) \in \mathbb{Z}.$$

ただし,  $\eta = \exp\left(\frac{2\pi\sqrt{-1}}{k}\right)$  とした.

**定義 4.4** (順序  $\alpha$ ). 全単射  $\alpha: \mathbb{Z} \rightarrow \mathbb{Z}$  に対して,  $\mathbb{Z}$  上の順序  $<_\alpha$  を次のように定める:

$$x <_\alpha y \stackrel{\text{def}}{\iff} \alpha^{-1}(x) < \alpha^{-1}(y).$$

$\alpha(x) < \alpha(y)$  ではなく  $\alpha^{-1}(x) < \alpha^{-1}(y)$  を定義にした理由は,

$$\cdots <_{\alpha} \alpha(-1) <_{\alpha} \alpha(0) <_{\alpha} \alpha(1) <_{\alpha} \cdots$$

となるようにしたかったからである.

**定義 4.5** (辞書順  $\alpha$ ).  $\mathbb{Z}^k$  上の順序  $\prec_{\alpha}$  を次のように定める:

$$(x_1, \dots, x_k) \prec_{\alpha} (y_1, \dots, y_k) \stackrel{\text{def}}{\iff} \exists j, x_i = y_i \ (\forall i < j) \text{ and } x_j <_{\alpha} y_j.$$

**定義 4.6.** 予想 1 において,  $x_1^{d_1} \cdots x_m^{d_m}$  の係数の  $\frac{n^{m-1}!}{\prod_i d_i!}$  個の和のうち,  $(\zeta^0)^{c_0} \cdots (\zeta^{n-1})^{c_{n-1}}$  の個数を  $\mathcal{P}_{c,d}$  で表す.

$(\zeta^0)^{c_0} \cdots (\zeta^{n-1})^{c_{n-1}}$  は値で区別されず,  $\zeta^i x_j$  が選ばれた回数が  $c_i$  ということを表す. 特に,

$$\sum_c \mathcal{P}_{c,d} = \frac{n^{m-1}!}{\prod_i d_i!}$$

が成り立つことに注意する.

**定義 4.7.** 予想 1 において,  $(i_1, \dots, i_{n^{m-1}})_{\prec_{\alpha}}$  で,  $n^{m-1}$  個の組  $(0, b_2, \dots, b_m)$  全体 (i.e.  $\{0\} \times \{0, \dots, n-1\}^{m-1}$ ) を  $\prec_{\alpha}$  で並び替えたときに  $j$  番目に小さい組に対応する多項式  $x_1 + \sum_i \zeta^{b_i} x_i$  の  $x_{i_j}$  が選ばれた単項式を表すものとする.

**定義 4.8.**  $k, l \in \mathbb{Z}, \beta_{k,l} : \mathbb{Z} \rightarrow \mathbb{Z}$ ,

$$\beta_{k,l}(x) := \begin{cases} x & (x \neq k, l) \\ l & (x = k) \\ k & (x = l) \end{cases}.$$

**補題 4.9.** 予想 1 の各係数は  $1, \zeta, \dots, \zeta^{n-1}$  について対称である.

**Proof.**  $\mathcal{P}_{(\dots, c_k, \dots, c_l, \dots), d} = \mathcal{P}_{(\dots, c_l, \dots, c_k, \dots), d}$  を示せばいい.

$$(i_1, \dots, i_{n^{m-1}})_{\prec_{\text{id}}} = \cdots (\zeta^k)^{c_k} \cdots (\zeta^l)^{c_l} \cdots \prod_i x_i^{d_i} \iff (i_1, \dots, i_{n^{m-1}})_{\prec_{\beta_{k,l}}} = \cdots (\zeta^k)^{c_l} \cdots (\zeta^l)^{c_k} \cdots \prod_i x_i^{d_i}$$

であるから, これらの  $(i_1, \dots, i_{n^{m-1}})_{\prec_{\text{id}}}$  と  $(i_1, \dots, i_{n^{m-1}})_{\prec_{\beta_{k,l}}}$  を一対一に対応させることができ,

$$\mathcal{P}_{(\dots, c_k, \dots, c_l, \dots), d} = \mathcal{P}_{(\dots, c_l, \dots, c_k, \dots), d}. \quad \square$$

補題 4.9 より,  $f_m$  の各係数に系 4.3 を使うことができるから,  $f_m(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}_m]$ .  $\square$

同様にして, 予想 2 も示すことができる.

## 5 新たに得られる事実

命題 5.1.  $\{1, \dots, n-1\}$  の順列全体を  $S_{n-1}$  とする.

$$f_n^S(\mathbf{x}_n) = \prod_{\sigma \in S_{n-1}} \left( x_1 + \sum_{i=1}^{n-1} \zeta^{\sigma(i)} x_{i+1} \right) \in \mathbb{Z}[\mathbf{x}_n].$$

命題 5.2.  $\{i : 1 \leq i < n, (i, n) = 1\}$  の順列全体を  $S'_n$  とする.

$$g_n^S(\mathbf{x}_n) = \prod_{\sigma \in S'_n} \left( x_1 + \sum_{i=1}^{n-1} \zeta^{\sigma(i)} x_{i+1} \right) \in \mathbb{Z}[\mathbf{x}_n].$$

## 6 新たな予想

予想 3.  $h$  は  $\mathbb{Z}$  上既約か?

予想 4.  $g_n^S$  は  $\mathbb{Z}$  上既約か?

## 参考文献

- [1] 財団法人数学オリンピック財団 (2020). 数学オリンピック事典 (p. 131). 朝倉書店.
- [2] 小寺 平治 (2022). 明解演習 線形代数 (pp. 132-133). 共立出版.
- [3] 福井 敏純 (2008). 集合と位相空間入門 (pp. 47-48). [http://www.rimath.saitama-u.ac.jp/lab.jp/Fukui/lectures/Set\\_Topsp.pdf](http://www.rimath.saitama-u.ac.jp/lab.jp/Fukui/lectures/Set_Topsp.pdf) (最終確認 2023-06-22).
- [4] 安藤 哲哉. 代数学統論講義ノート (pp. 21-22). <http://www.math.s.chiba-u.ac.jp/~ando/DAISU3.pdf> (最終確認 2023-6-22).
- [5] 柳田 五夫 (2017). 初等整数論 (Instructor's Notes) (pp. 235-236). [http://izumi-math.jp/I\\_Yanagita/Instructor's\\_Notes.pdf](http://izumi-math.jp/I_Yanagita/Instructor's_Notes.pdf) (最終確認 2023-6-22).
- [6] よしいず (2012). 多項式についての命題. <https://yoshiiz.blog.fc2.com/blog-entry-585.html> (最終確認 2023-6-17).