

問題 14-1 $\Phi_n(x)$ を $n=1, 2, \dots, 12$ について求めよ. \square

解答例 $\Phi_n(x) = \prod_{\substack{\omega \text{ は } 1 \text{ の原始 } n \text{ 乗根}}} (x - \omega)$ ので,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{\omega^n = 1 \text{ and} \\ \exists d \text{ s.t. } 0 < d < n \text{ and } \omega^d = 1}} (x - \omega)} = \frac{x^n - 1}{\prod_{d|n \text{ and } d < n} \Phi_d(x)} \text{ を使おう.}$$

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1, \quad \Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1, \quad \Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1,$$

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1, \quad \Phi_6(x) = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

$$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + \dots + x + 1, \quad \Phi_8(x) = \frac{x^8 - 1}{(x - 1)(x + 1)(x^2 + 1)} = x^4 + 1,$$

$$\Phi_9(x) = \frac{x^9 - 1}{(x - 1)(x^2 + x + 1)} = x^6 + x^3 + 1, \quad \Phi_{10}(x) = \frac{x^{10} - 1}{(x - 1)(x + 1)\Phi_5(x)} = x^4 - x^3 + x^2 - x + 1,$$

$$\Phi_{11}(x) = \frac{x^{11} - 1}{x - 1} = x^{10} + x^9 + \dots + x + 1,$$

$$\Phi_{12}(x) = \frac{x^{12} - 1}{(x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1.$$

\square

問題14-2 以下を示せ.

- (1) 素数 p と正の整数 e について, $\Phi_{pe}(x) = \Phi_p(x^{p^{e-1}})$.
- (2) 正の奇数 n について, $\Phi_{2n}(x) = (-1)^{\varphi(n)} \Phi_n(-x)$. ($\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$)
- (3) $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\zeta, \sqrt{2}, \sqrt{3})$. □

解答例

(1) 1 の原始 p^e 乗根の1つを ω と書くと, $\overbrace{p^e - p^{e-1}}^{= p^{e-1}(p-1)}$ 個の 1 の原始 p^e 乗根全体は ω^{k+pl} $k \in \underbrace{\{1, 2, \dots, p-1\}}_{p-1 \text{ 個}}, l \in \underbrace{\{0, 1, \dots, p^{e-1}-1\}}_{p^{e-1} \text{ 個}}$ と書ける. この p^{e-1} 乗

$$(\omega^{k+pl})^{p^{e-1}} = (\omega^{p^{e-1}})^k \quad (k \in \{1, 2, \dots, p-1\})$$

はちょうど 1 の原始 p 乗根全体に一致し,

$$\omega^{pl} = (\omega^p)^l \quad (l \in \{0, 1, \dots, p^{e-1}-1\})$$

はちょうど 1 の p^{e-1} 乗根全体に一致するので

$$\Phi_{pe}(x) = \prod_{k=1}^{p-1} \prod_{l=0}^{p^{e-1}-1} (x - \omega^{k+pl}) = \prod_{k=1}^{p-1} (x^{p^{e-1}} - (\omega^{p^{e-1}})^k) = \Phi_p(x^{p^{e-1}}). \quad \square$$

(2) n は正の奇数であるとする、このとき、次が成立していることを示そう:

$$\omega \text{ が } 1 \text{ の原始 } 2n \text{ 乗根} \iff -\omega \text{ は } 1 \text{ の原始 } n \text{ 乗根}$$

(\Rightarrow) ω は 1 の原始 $2n$ 乗根であるとする、

$$1 = \omega^{2n} = (\omega^n)^2 \text{ より } \omega^n = \pm 1 \text{ だが, } \omega \text{ は } 1 \text{ の原始 } 2n \text{ 乗根なので } \omega^n = -1.$$

$$n \text{ は奇数なので } (-\omega)^n = 1,$$

$$d|n, d < n \text{ のとき, } \omega^{2d} \neq 1 \text{ なので } (-\omega)^d \neq 1,$$

ゆえに, $-\omega$ は 1 の原始 n 乗根である、

(\Leftarrow) $-\omega$ は 1 の原始 n 乗根であるとする、

$$\text{このとき, } \omega^{2n} = ((-\omega)^n)^2 = 1^2 = 1.$$

$2n$ の $2n$ より小さな正の約数は $2d$ または d ($d|n, d < n$) と書ける、

$$\text{もしも } \omega^d = 1 \text{ ならば } (-\omega)^n = -(\omega^d)^{\frac{n}{d}} = -1 \text{ となって } (-\omega)^n = 1 \text{ に反する.}$$

$$\text{もしも } \omega^d \neq 1 \text{ かつ } \omega^{2d} = 1 \text{ ならば } \omega^d = -1 \text{ となり, } (-\omega)^d = 1 \text{ となって}$$

$-\omega$ が 1 の原始 n 乗根であることに反する、

これで, ω が 1 の原始 $2n$ 乗根であることが示された、

(2) つづき、前ページの結果より、

$$-w = w'$$



$$\Phi_{2n}(x) = \prod_{w \text{ は } 1 \text{ の原始 } 2n \text{ 乗根}} (x - w) = \prod_{w' \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (x + w')$$

$$= (-1)^{\varphi(n)} \prod_{w' \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (-x - w') = (-1)^{\varphi(n)} \Phi_n(-x),$$

ここで、 $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = (1 \text{ の原始 } n \text{ 乗根の個数})$ であることを使った、 \square

$$\begin{aligned}
 (3) \quad \Phi_{24}(x) &= \frac{x^{24}-1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4+1)(x^4-x^2+1)} = \frac{x^{24}-1}{(x^{12}-1)(x^4+1)} \\
 &= \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1
 \end{aligned}$$

$$\Phi_{24}(x)=0 \text{ を } x^4 \text{ について解くと, } x^4 = \frac{1 \pm \sqrt{-3}}{2} = \frac{2 \pm 2\sqrt{-3}}{4} = \frac{(\bar{\omega} \pm \sqrt{3})^2}{4}.$$

$$\text{ゆえに, } x^2 = \pm \frac{\bar{\omega} \pm \sqrt{3}}{2} = \pm \frac{2\bar{\omega} \pm 2\sqrt{3}}{4} = \pm \frac{(\sqrt{-1} \pm \sqrt{3})^2}{4}$$

$$\text{ここで } \sqrt{-1} = \frac{1-\bar{\omega}}{\sqrt{2}}, \quad \sqrt{3}\bar{\omega} = \sqrt{3} \frac{1+\bar{\omega}}{\sqrt{2}} \text{ とおいた. (このとき } \sqrt{-1}\sqrt{3}\bar{\omega} = \sqrt{3})$$

$$\text{ゆえに, } x = \pm \frac{\sqrt{-1} \pm \sqrt{3}\bar{\omega}}{2}, \quad \pm \bar{\omega} \frac{\sqrt{-1} \pm \sqrt{3}\bar{\omega}}{2}, \quad \leftarrow 8 \text{ 次方程式 } \Phi_{24}(x)=0 \text{ の } 8 \text{ 個の解}$$

$$\text{これより, } \mathbb{Q}(\zeta_{24}) = (\Phi_{24}(x) \text{ の } \mathbb{Q} \text{ 上での最小分解体}) \subset \mathbb{Q}(\bar{\omega}, \sqrt{2}, \sqrt{3}).$$

$$\text{さらに, } \zeta_{24}^6 = (e^{2\pi i/24})^6 = e^{\pi i/2} = \bar{\omega},$$

$$\zeta_{24}^3 = e^{\pi i/4} = \frac{1+\bar{\omega}}{\sqrt{2}}, \quad \zeta_{24}^4 = e^{\pi i/3} = \frac{1+\sqrt{3}\bar{\omega}}{2} \text{ より, } \mathbb{Q}(\bar{\omega}, \sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\zeta_{24}).$$

$$\text{これで, } \mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\bar{\omega}, \sqrt{2}, \sqrt{3}) \text{ が示された.}$$

□

問題 14-3 $\Phi_n(x)$ の係数は常に $0, \pm 1$ だけになるか? \square

解答例 $n \leq 104$ のとき, $\Phi_n(x)$ の係数は $0, \pm 1$ だけになる.

しかし, $\Phi_{105}(x)$ の係数には -2 が現れる. \square

<https://www.wolframalpha.com/input/?i=Cyclotomic%5B105%2C+x%5D&lang=ja>



Cyclotomic[105, x]

Input

$C_{105}(x)$

Result

$$x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$$

問題 14-4 $n \in \mathbb{Z}_{>0}$, $\zeta_n = e^{2\pi i/n}$ のとき, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ となることを示せ. \square

解説 $\mathbb{Q}(\zeta_n) = (\Phi_n(x) \text{ の } \mathbb{Q} \text{ 上での最小分解体})$ なので ζ_n の共役元の全体は

1 の原始 n 乗根全体に一致する、そして、

$$\{1 \text{ の原始 } n \text{ 乗根全体}\} = \{\zeta_n^{\bar{k}} \mid \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times\}.$$

さらに, $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ は $\sigma(\zeta_n) = \zeta_n^{\bar{k}} \ (\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times)$ と一対一に対応している,

ゆえに, $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ に対して, $\sigma(\zeta_n) = \zeta_n^{\bar{k}}$ という条件で定まる

$\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ を対応させる写像 ρ が群の準同型であることを示せばよい,

$\sigma, \tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ が $\sigma(\zeta_n) = \zeta_n^{\bar{k}}, \tau(\zeta_n) = \zeta_n^{\bar{l}}$ をみたすとき,

$$(\sigma\tau)(\zeta_n) = \sigma(\zeta_n^{\bar{l}}) = \sigma(\zeta_n)^{\bar{l}} = (\zeta_n^{\bar{k}})^{\bar{l}} = \zeta_n^{\bar{k}\bar{l}},$$

ゆえに, $\rho(\sigma\tau) = \overline{k\bar{l}} = \bar{k}\bar{l} = \rho(\sigma)\rho(\tau)$.

これで示すべきことが示された.

\square