資料15-1

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

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

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

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

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

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

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

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

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

□

$\boxed{\text{問題14-2}}$ 以下を示せ。

(1) 素数 p と正の整数 e について、$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}})$.

(2) 正の奇数 n について、$\Phi_{2n}(x) = (-1)^{\varphi(n)}\Phi_n(-x)$. $\left(\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|\right)$

(3) $\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$. □

$\zeta_{24} = e^{2\pi i/24}$

$\boxed{\text{解答例}}$

(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

$$\omega^{k+pl} \qquad \Big(k \in \{\underbrace{1, 2, \dots, p-1}_{p-1\text{個}}\},\ l \in \{\underbrace{0, 1, \dots, p^{e-1}-1}_{p^{e-1}\text{個}}\}\Big)$$

と書ける。これの p^{e-1} 乗

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

はちょうど 1の原始 p 乗根全体に一致し、

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

はちょうど1の p^{e-1} 乗根全体に一致するので

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

$x^{p^{e-1}} -$ (1の原始 p 乗根)

$x - \omega^k \times$ (1の p^{e-1} 乗根) ⟵ $\omega^k = (\omega^{p^{e-1}})^k$ の p^{e-1} 乗根

(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：

ω が1の原始 $2n$ 乗根 $\Longleftrightarrow$ $-\omega$ は1の原始 n 乗根

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

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

n は奇数なので $(-\omega)^n = 1$.

$d|n$, $d<n$ のとき、$\omega^{2d} \neq 1$ 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。

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

$2n$ の $2n$ より小さい正の約数は ① d $(d|n)$ または ② $2d$ $(d|n, d<n)$ と書ける。

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

②の場合：上の結果より $\omega^d \neq 1$ となる。ゆえに、$\omega^{2d} = 1$ ならば $\omega^d = -1$ となり、$(-\omega)^d = 1$ 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，

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

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

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

(3) $$\Phi_{24}(x) = \frac{x^{24}-1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4+1)(x^4-x^2+1)} = \frac{x^{24}-1}{(x^{12}-1)(x^4+1)}$$

$$= \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1$$ ← 非常にシンプルな形になった！

$\Phi_{24}(x)=0$ を x^4 について解くと，$x^4 = \dfrac{1\pm\sqrt{-3}}{2} = \dfrac{2\pm2\sqrt{-3}}{4} = \dfrac{(i\pm\sqrt{3})^2}{4}$.

ゆえに，$x^2 = \pm\dfrac{i\pm\sqrt{3}}{2} = \pm\dfrac{2i\pm2\sqrt{3}}{4} = \pm\dfrac{(\sqrt{-i}\pm\sqrt{3i})^2}{4}$

ここで $\sqrt{-i} = \dfrac{1-i}{\sqrt{2}}$，$\sqrt{3i} = \sqrt{3}\,\dfrac{1+i}{\sqrt{2}}$ とおいた．（このとき $\sqrt{-i}\sqrt{3i} = \sqrt{3}$）

ゆえに，$x = \pm\dfrac{\sqrt{-i}\pm\sqrt{3i}}{2}$，$\pm i\,\dfrac{\sqrt{-i}\pm\sqrt{3i}}{2}$． ← 8次方程式 $\Phi_{24}(x)=0$ の8個の解

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

逆に，$\zeta_{24}^6 = (e^{2\pi i/24})^6 = e^{\pi i/2} = i$，

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

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

□

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

$\boxed{\text{解答例}}$ $n \leqq 104$ 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. □

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

WolframAlpha

Cyclotomic[105, x]

Input

$C_{105}(x)$

Result

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

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

$\boxed{\text{解説}}$ $\mathbb{Q}(\zeta_n) = (\Phi_n(x)$ の $\mathbb{Q}$ 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,

$$\{1\text{の原始 } n \text{ 乗根全体}\} = \{\zeta_n^k \mid k \in \mathbb{Z} \text{ かつ } \underset{\substack{\Updownarrow \\ \gcd(n,k)=1}}{\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times}\}.$$

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

ゆえに, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ に対して, $\sigma(\zeta_n) = \zeta_n^k$ という条件で定まる $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ 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.

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

$$(\sigma\tau)(\zeta_n) = \sigma(\zeta_n^l) = \sigma(\zeta_n)^l = (\zeta_n^k)^l = \zeta_n^{kl}.$$

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

これで示すべきことが示された. □