

Def $n \geq 1$ とし, $\zeta_n = \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$ とする。

$\Phi_n(x) := \prod_{\substack{0 \leq k < n \\ (n, k) = 1}} (x - \zeta_n^k)$ を n 次 n 分多項式という。

Thm $\Phi_n(x)$ は $\mathbb{Q}[x]$ のモニック $\phi(n)$ 次既約多項式

($\because$) $f(x) = \text{Irr}(\mathbb{Q}; \zeta_n)$ とする。任意の素数 $p \nmid n$ に対し $f(\zeta_n^p) = 0$ を言えばよい。

$$\Delta := \prod_{0 \leq i < j < n} (\zeta_n^i - \zeta_n^j)^2 = \pm n^n \text{ は初等的である}$$

$f(x) \mid x^n - 1$ in $\mathbb{Q}(x)$ より $f(x) \in \mathbb{Z}[x]$ がわかる (ガウス補題, まだやらない)

$f(\zeta_n^p) \neq 0$ とすると, $f(\zeta_n^p) \in \overline{\mathbb{Q}}$ だから $f(x^p) \equiv f(x)^p \pmod{p}$ より $f(\zeta_n^p) \in p\overline{\mathbb{Q}}$

これより $\exists x \in \overline{\mathbb{Q}}$ s.t. $px = n^n$ かつ $x \in \overline{\mathbb{Q}} \cap \mathbb{Q} = \mathbb{Q}$ で矛盾が生じた //

Cor $\forall n \geq 1$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ はガロワ拡大で, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

($\because$) 明らか //

$$\left(\begin{array}{c} \sigma_x: \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n) \\ \zeta_n \mapsto \zeta_n^x \end{array} \right) \leftarrow \psi_x$$

1 の n 乗根の応用

Thm (Wedderburn) 有限斜体 D は可換 (つまり体) である。

($\because$) $Z = \{x \in D \mid \forall a \in D, ax = xa\}$ は D の部分体 かつ $Z = \mathbb{F}_q$ ($q = p^m$, p : 素数)

とする。 $\dim_Z D = n$ とし, $n > 1$ とする。

$a \in D \setminus Z$ に対し $C(a) := \{x \in D \mid xa = ax\}$ ($\subseteq Z$) は D の真の部分斜体

かつ $\dim_Z C(a) =: d_a$ に対し $1 < d_a < n$ 。又, 連鎖律より $d_a \mid n$ 。

D^x の類等式 $g^n - 1 = g - 1 + \sum_a \frac{g^n - 1}{g^{da} - 1}$ から $\Phi_n(g) \mid g - 1$ が導かれるが、これは矛盾、

Def $p \geq 3$: 奇素数, $m \in \mathbb{F}_p^x$ $\left(\frac{m}{p}\right) = \begin{cases} 1 & \exists x \in \mathbb{F}_p^x \text{ s.t. } x^2 = m \text{ in } \mathbb{F}_p^x \\ -1 & \text{o.w.} \end{cases}$ (レジャントレ記号)

Lemma $\left(\frac{m}{p}\right) = m^{\frac{p-1}{2}}$ in $\mathbb{F}_p^x$

① $\mathbb{F}_p^x = \{g^0, g^1, \dots, g^{p-1}\}$ とし, $m = g^k$ とし, $\left(\frac{m}{p}\right) = (-1)^k$ から従う //

Def $p \geq 3$: 奇素数, $W_p := \sum_{x \in \mathbb{F}_p^x} \left(\frac{x}{p}\right) \zeta_p^x \left(\in \mathbb{Z}[\zeta_p]\right)$: Gauss 和

Thm $W_p^2 = (-1)^{\frac{p-1}{2}} \cdot p$

① $W_p^2 = \sum_{x, y \in \mathbb{F}_p^x} \left(\frac{xy}{p}\right) \zeta_p^{x+y} = \sum_{\substack{x, y \neq 0 \\ \text{in } \mathbb{F}_p}} \left(\frac{x^2 y}{p}\right) \zeta_p^{x+xy} = \sum_{x \neq 0} \left(\frac{-1}{p}\right) \zeta_p^0 + \sum_{y \neq 0, -1} \left(\frac{y}{p}\right) \sum_{x \neq 0} \zeta_p^{x(1+y)} = \left(\frac{-1}{p}\right) \cdot p$ //

Cor $p \neq l$: 奇素数, $\left(\frac{l}{p}\right) \left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}} = \left(\frac{-1}{p}\right) \cdot p$

② $\left(\frac{W_p^2}{l}\right) = \left(\frac{-1}{l}\right)^{\frac{p-1}{2}} \left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}} \left(\frac{p}{l}\right)$

mod l として $W_p^l = \sum_{m \neq 0} \left(\frac{m}{p}\right)^l \zeta_p^{lm} = \sum_{m \neq 0} \left(\frac{l^l m}{p}\right) \zeta_p^{lm} = \left(\frac{l}{p}\right) W_p$

よって $\left(\frac{W_p^2}{l}\right) = W_p^{2 \cdot \frac{l-1}{2}} = \left(\frac{l}{p}\right)$ //

③ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

④ $2 = (\zeta_8 + \zeta_8^{-1})^2$ より $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = (\zeta_8 + \zeta_8^{-1})^{p-1} \equiv \frac{\zeta_8^1 + \zeta_8^{-p}}{\zeta_8 + \zeta_8^{-1}} \pmod{p}$

$$\text{Cor } \left(\frac{5}{p}\right) = \begin{cases} 1 & (p \equiv \pm 1 \pmod{5}) \\ -1 & (p \equiv \pm 2 \pmod{5}) \end{cases} \quad \text{for } p \neq 2, 5 : \text{奇素数}$$

$$\text{Cor } p : \text{奇素数} \quad \exists x \exists y \in \mathbb{N} \text{ s.t. } p = x^2 + y^2 \Leftrightarrow p \equiv 1 \pmod{4}$$

① $(\Rightarrow)$ は明らか

$$(\Leftarrow) \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ かつ } \exists z \in \mathbb{F}_p^* \text{ s.t. } z^2 = -1 \text{ in } \mathbb{F}_p$$

$$\text{11.9 乗原理より } -\sqrt{p} < x, y < \sqrt{p} \text{ s.t. } x + yz = 0 \text{ in } \mathbb{F}_p \text{ かつ } \begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\text{よ. } x^2 + y^2 = (x + iy)(x - iy) \in p\mathbb{Z} \text{ かつ } 0 < x^2 + y^2 < 2p //$$

② 今回, $\mathbb{Z}[X]$ の 2 次式 $X^2 + aX + b$ がある $\mathbb{F}_p[X]$ で分解するかどうかを分けたが、これを一般化していくのが例で知られている。

$$\text{Ex. } \exists x \in \mathbb{F}_p^* \text{ s.t. } x^3 = 2 \text{ in } \mathbb{F}_p \Leftrightarrow \exists x \exists y \in \mathbb{N}, p = x^2 + 27y^2 \Leftrightarrow a(p) = 2$$

が知られている (『数論を学ぶ人のための相互法則入門』平松豊一著)

$$\text{ここで } \sum_{n \geq 1} a(n) q^n := q \prod_{n \geq 1} (1 - q^{6n})(1 - q^{18n}) \text{ (形式的なべき級数として)}$$

③ $\exists n \geq 1, \mathbb{Q}(\zeta_n) \supseteq K \supseteq \mathbb{Q}$ となる K を $\mathbb{Q}(\zeta_n)$ 体という。

$K/\mathbb{Q}$ が有限次拡大で $\text{Gal}(K/\mathbb{Q})$ が可換群であることと同値であることを知られている (Kronecker-Weber の定理)

$$\text{Ex } \sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

④ $p : \text{奇素数} \quad \sqrt{p} \in \mathbb{Q}(\zeta_p, \sqrt{-1}) (\subseteq \mathbb{Q}(\zeta_{4p}))$ は $W_p^2 = (-1)^{\frac{p-1}{2}} p$ から従う。

これと $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ より, $d \in \mathbb{Z}$ については確かに $\mathbb{Q}(\sqrt{d})$ は $\mathbb{Q}(\zeta_n)$ 体になっている。

Thm (Kummer #1) $L \subseteq \overline{\mathbb{Q}}$ が Galois #1 s.t. $\text{Gal}(L/K) \cong C_n$
 $\mathbb{Q}(\zeta_n) \subseteq K \Rightarrow \exists a \in L$ s.t. $L = K(a)$ かつ $a^n \in K$

① $\text{Gal}(L/K) = \{\tau^0, \tau^1, \dots, \tau^{n-1}\}$ とする。 $\tau: L \xrightarrow{\sim} L$ を K 線形写像と見たとき τ の固有値の集合を R とする。 $\tau^n = \text{id}_L$ より $\forall r \in R, r^n = 1$ (よって $R \subseteq K$)
 $\text{ord } \tau = n$ より $\exists 0 < k < n, (k, n) = 1, \zeta_n^k \in R$ 。 $R \subseteq K^\times$ (部分群) は
 易しいので $R = \{\zeta_n^k \mid 0 \leq k < n\}$ が成り立つ。

τ の ζ_n 固有ベクトル $a \in L \setminus \{0\}$ が目的のものがあることを示す。

• $b := a^n$ について, $\tau(b) = \tau(a)^n = b$ なるので $b \in L^{\text{Gal}(L/K)} = K$

• $\tau^i(a) = \zeta_n^i a$ なるので $a, \tau(a), \dots, \tau^{n-1}(a)$ は全て異なる

よって $\text{Gal}(L/K(a)) = \{\tau^0\}$ なるので $K(a) = L$ //

応用 (フェルマー素数と作図可能性)

Thm $p \geq 3$: 素数 について, 正 p 角形が作図可能 $\Leftrightarrow \exists k \geq 0$, s.t. $p = 2^{2^k} + 1$

① まず $p = 2^m + 1$ ($m \geq 1$) なる $m = 2^k$ ($k \geq 0$) とならなければならないことを注意する。

又, 正 p 角形が作図可能 $\Leftrightarrow \cos \frac{2\pi}{p} = \frac{1}{2}(\zeta_p + \zeta_p^{-1})$ が作図可能, にも注意する。

$\Rightarrow \mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\cos \frac{2\pi}{p}) \supset \mathbb{Q}$ を考えることにし, $[\mathbb{Q}(\cos \frac{2\pi}{p}) : \mathbb{Q}] = \frac{\phi(p)}{2} = \frac{p-1}{2}$

よって $\frac{p-1}{2} = 2^k$ ($k \geq 0$) とならなければならない。

⊞ $\mathbb{Q}(\zeta_p) \not\subset \mathbb{Q}(\cos \frac{2\pi}{p}) \supseteq \mathbb{Q}$ から $\mathbb{Q}(\cos \frac{2\pi}{p}) \supseteq \mathbb{Q}$ は加群拡大

$\text{Gal}(\mathbb{Q}(\cos \frac{2\pi}{p})/\mathbb{Q}) \simeq C_{2^{k-1}}$ が分かる C_{2^n} には

$$G_0 = C_{2^n} \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\} \quad (\forall i, [G_i : G_{i+1}] = 2)$$

とある正規部分群の列がとれるため, Kummer 拡大をくり返し

各 step で $\sqrt[n]{\text{何らか}}$ を付加する拡大で $\mathbb{Q}$ から $\mathbb{Q}(\cos \frac{2\pi}{p})$ に到達できる //

応用 (3次方程式の解法)

Cor Thm (Kummer 拡大) の設定で: $(\zeta_n, b)^n \in K$ かつ $b = \frac{1}{n} \sum_{k=0}^n (\zeta_n^k, b)$ for all $b \in L$.
 ここで $(\alpha, \theta) := \sum_{k=0}^{n-1} \alpha^k \tau^k(\theta)$ (ラグランジュの解式)

① $\tau(\zeta_n, b) = \zeta_n(\zeta_n, b)$ は易しい。後半は $1 \leq l < n$, $\sum_{k=0}^n \zeta_n^{lk} = 0$ から従う。 //

$X^3 + pX + q = (X - t_1)(X - t_2)(X - t_3)$ かつ "十分一般である" とする

$$\mathbb{Q}(\sqrt{3}, t_1, t_2, t_3)$$

$$\{e\}$$

$$\cup$$

$$\mathbb{Q}(\sqrt{3}, p, q, \Delta)$$

$$\Delta$$

$$A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\cup$$

$$\mathbb{Q}(\sqrt{3}, p, q)$$

$$\Delta$$

$$S_3$$

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_2 - t_3) = \sqrt{D}$$

$$D = (t_1 - t_2)^2(t_1 - t_3)^2(t_2 - t_3)^2 = -(4p^3 + 27q^2)$$

ラグランジュの解式は (ただし, $\langle \tau \rangle = A_3$ とし $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ をとつた)

$$(1, t_1) = t_1 + t_2 + t_3 = 0$$

$$(\zeta_3, t_1) = t_1 + \zeta_3^2 t_2 + \zeta_3 t_3 \quad (*)$$

$$(\zeta_3^2, t_1) = t_1 + \zeta_3 t_2 + \zeta_3^2 t_3$$

これら 3 を乗じて $\mathbb{Q}(\sqrt{3}, \rho, \sqrt{D})$ の元である。計算すると

$$(\zeta_3, t_1)^3 = -\frac{27}{2}\rho - \frac{3\sqrt{3}}{2}\sqrt{D}$$

$$(\zeta_3^2, t_1)^3 = -\frac{27}{2}\rho + \frac{3\sqrt{3}}{2}\sqrt{D}$$

ただし $(\zeta_3, t_1)(\zeta_3^2, t_1) = -3\rho$ である。

(*) を逆に解いて, t_1, t_2, t_3 が求まる, というのが「カルダノ」の公式である。

Ex $x^3 - 15x - 4 = 0$ のとき, $D = 2^2 \cdot 3^3 \cdot 11^2$

よって $t_1 = \sqrt[3]{2+11i} + \sqrt[3]{2-11i}$ ただし $\sqrt[3]{} \cdot \sqrt[3]{} = 5$ ととる。

$(2 \pm i)^3 = 2 \pm 11i$ に気付けばよいが, $(a \pm bi)^3 = 2 \pm 11i$ を解く必要と

$x^3 - 15x - 4 = 0$ に戻してしまう (不還元の場合)

Ex $\cos^3 \alpha - \frac{3}{4} \cos \alpha - \frac{1}{4} \cos 3\alpha = 0$ より

$$\left(\frac{x}{\sqrt{5}}\right)^3 - 3\left(\frac{x}{\sqrt{5}}\right) - \frac{4}{5\sqrt{5}} = 0 \text{ と見比べると } \frac{x}{\sqrt{5}} = 2\cos \alpha \text{ where } \cos 3\alpha = \frac{2}{5\sqrt{5}}$$

7#1 $x = 2\sqrt{5} \cos\left(\frac{1}{3} \arccos \frac{2}{5\sqrt{5}}\right) = 4, \underset{-2-\sqrt{3}}{-3.73\dots}, \underset{-2+\sqrt{3}}{-0.267\dots}$ とも求まる。

注 4次方程式についても, $S_4 \supseteq A_4 \supseteq V_4 \supseteq C_2 \supseteq \{e\}$ に注目すること

解の公式を得ることからできる。ここで $V_4 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right), e\}$
 $C_2 = \left\{\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right), e\right\}$

Thm $K \subseteq \mathbb{R}$: 部分体

$f(x) = x^3 + ax^2 + bx + c \in K[x]$ は既約で 3 実根 t_1, t_2, t_3 を持つとき, 以下を満たす拡大は存在しない:

• $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_S \subseteq \mathbb{R}$ で $t_1 \in K_S$

• $1 \leq i \leq S \exists p_i : \text{素数} \exists u_i \in K_i \setminus K_{i-1} \text{ s.t. } u_i^{p_i} \in K_{i-1}$

(注) この仮定から $x^{p_i} - u_i^{p_i} \in K_{i-1}[x]$ は既約で, $K_i = K_{i-1}(u_i)$ を示す

(1) そのような拡大で $S \geq 1$ が最小の n をとる。当然, $t_2, t_3 \notin K_{S-1}$ としてよい。 $[K_S : K_{S-1}]$ が素数だから $t_1 \notin K_{S-1}$ より $K_S = K_{S-1}(t_1)$

又, $f(x) \in K_{S-1}[x]$ は既約だから $[K_S : K_{S-1}] = 3$

よって $p_S = 3$, $\exists u_S \in K_S \setminus K_{S-1}$ s.t. $u_S^3 \in K_{S-1}$ で $K_S = K_{S-1}(t_1) = K_{S-1}(u_S)$

$M = K_{S-1}(u_S, \zeta_3 u_S, \zeta_3^2 u_S)$ とすると M/K_{S-1} は Galois 拡大だから

$M \supseteq M' := K_{S-1}(t_1, t_2, t_3)$ 。同様に M'/K_{S-1} は Galois 拡大だから $M = M'$

$M' \subseteq \mathbb{R}$ だから $\zeta_3 \in M = M'$ だから矛盾が生じた //

(注) について: $F \subseteq \mathbb{C}$, p : 素数 $x^p - c \in F[x]$: 既約 $\Leftrightarrow \forall f \in F, f^p \neq c$

(1) $\Rightarrow$: 明らか (by 対偶)

$\Leftarrow$: $x^p - c = f(x)g(x)$ $f, g \in F[x]$, $1 \leq \deg f =: n < p$ とする

$f(x) = (x - z_1) \cdots (x - z_n)$ in $\mathbb{C}[x]$ とすると, $z := z_1 z_2 \cdots z_n$ は $z \in F$ で

$z^p = c^n$ 。 $1 = ap + bn$ と $a, b \in \mathbb{Z}$ をとると, $(c^a z^b)^p = c$ になるから //