第12 代数系

円分体　前回 有限体

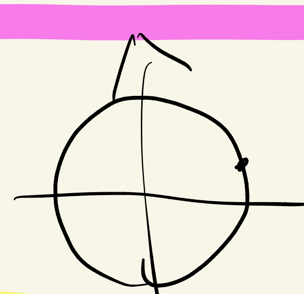
<u>円分多項式</u> 原始n乗根の方程式

$n=2$ $\zeta_2 = -1$ $x+1=0$

$n=3$ $\zeta_3 = \frac{-1\pm\sqrt{-3}}{2}$ $x^2+x+1=0$

$$\boxed{\underline{\text{Def}}\quad \Phi_n(x) := \prod_{\substack{1\leq k<n \\ (k,n)=1}} (x-\zeta_n^k)}$$

$\zeta_n := \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$



Schur

$$\boxed{\underline{\text{Thm}}\quad \Phi_n(x) \in \mathbb{Z}[x] \text{ でモニック 既約 } (\text{次数} = \varphi(n))}$$

Rk $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Cor $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ はガロア拡大

$$G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\sigma_x : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n) \longmapsfrom [x]$$

$$\zeta_n \mapsto \zeta_n^x$$

がロア拡大なこと

$$\mathbb{Q}(\zeta_n^k) = \mathbb{Q}(\zeta_n)$$

$$(k,n)=1 \qquad \exists \exists\ ka+bn=1$$

$$\mathbb{Q}[x]/(\Phi_n(x))$$

応用 1の巾根の応用

Thm (Wedderburn thm)

D：有限斜体 ⇒ 体

証 $Z=\{x\in D \mid \forall a\in D.\ ax=xa\}$

$\subseteq D$：部分体

$Z=\mathbb{F}_q \qquad q=p^m$

$\dim_Z D=n \qquad n>1$ とする.

$a\in D\setminus Z \qquad C(a)=\{x\in D \mid xa=ax\}$

$Z \subsetneq C(a) \subsetneq D$

$C(a)$ は D の部分斜体

$\dim_{Z} C(a) =: d_a$ とすると

連鎖律 $\dim_{Z} C(a) \underline{\dim_{C(a)} D} = n$

左ベクトル空間

$1 < d_a < n \qquad d_a \mid n$

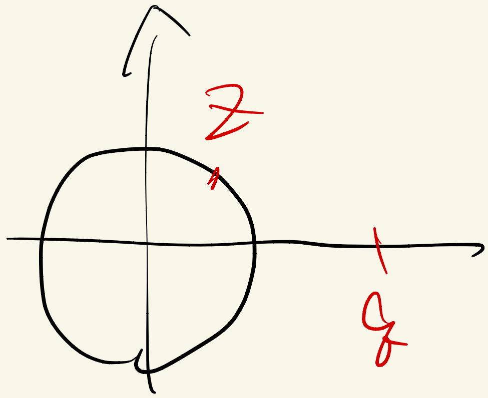
類等式

$$D^\times = Z^\times \bigsqcup_a \frac{D^\times}{C(a)^\times}$$

$$q^n - 1 = q - 1 + \sum_a \frac{q^n - 1}{q^{d_a} - 1}$$

よって $\Phi_n(q) \mid q - 1$ これは矛盾

$\Phi_n(q) = (q - \zeta_n^{0})(q - \zeta_n^{2}) \cdots$



$z \neq 1$, $|z| = 1$ なる

$|q - z| > |q - 1|$ //

平方剰余の相互法則

Def $p \geq 3$ 奇素数

$n \in \mathbb{F}_p^\times$ $\quad \left(\frac{n}{p}\right) = \begin{cases} 1 & \exists x \in \mathbb{F}_p^\times \ x^2 = n \\ -1 & \text{o.w.} \end{cases}$ in $\mathbb{F}_p$

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

∵ $\mathbb{F}_p^\times = \{g^0, g^1, \dots, g^{p-1}\}$ このとき

$$\left(\frac{n}{p}\right) = 1 \iff n = g^{2k} \quad \exists k$$

は同値

$$n = g^{l} \Rightarrow n^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^{l} = (-1)^{l}$$

系 $\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right)$

<u>Def</u> $p \geq 3$: 奇素数

$$W_p := \sum_{x \in \mathbb{F}_p^{\times}} \left(\frac{x}{p}\right) \zeta_p^{x} \in \mathbb{Q}[\zeta_p]$$

: Gauss 和

<u>Thm</u> $W_p^{2} = (-1)^{\frac{p-1}{2}} p$

$$W_p^2 = \sum_{x,y \neq 0} \left(\frac{xy}{p}\right) \zeta_p^{x+y}$$

$y \mapsto xy$

$\mathbb{F}_p^{\times}$

$$= \sum_{x,y \neq 0} \left(\frac{x^2 y}{p}\right) \zeta_p^{x(1+y)}$$

$$= \sum_{x \neq 0} \left(\frac{-1}{p}\right) + \sum_{y \neq 0,-1} \left(\frac{y}{p}\right) \left(\sum_{x \neq 0} \zeta_p^{x(1+y)} \right)$$

$$\sum_{x \neq 0} \zeta_p^{x(1+y)} = 0$$

$$= p \cdot \left(\frac{-1}{p}\right)$$

$$1 + \zeta_p + \dots + \zeta_p^{p-1} = 0$$

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

(:)

$$\left(\frac{w_p^2}{\ell}\right) = \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}}\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right)$$

$w_p^2 = (-1)^{\frac{p-1}{2}}\cdot p$　一方で mod ℓ で

$$\left(\frac{n}{p}\right) \equiv (n)^{\frac{p-1}{2}}$$

$$\left(\frac{\ell}{p}\right)\left(\frac{\ell^{-1}}{p}\right) = 1$$

$$w_p^\ell = \sum_{x\neq 0}\left(\frac{x}{p}\right)^{\cancel{\ell}}\zeta_p^{x\ell} = \sum_{x\neq 0}\left(\frac{\ell^{-1}x}{p}\right)\zeta_p^{x}$$

$$= \left(\frac{\ell}{p}\right) w_p$$

$$\left(\frac{w_p^2}{\ell}\right) = w_p^{2\frac{\ell-1}{2}} = \left(\frac{\ell}{p}\right)$$

$\underline{\text{Cor}}$ $\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 5 \\ -1 & p \equiv \pm 2 \mod 5 \end{cases}$

$p \neq 5$: 奇素数

$\because$ $\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}} = 1$

$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$

$\underline{\text{Cor}}$ p : 奇素数

$\exists x \exists y \in \mathbb{N}$ $p = x^2 + y^2 \Longleftrightarrow p \equiv 1 \pmod 4$

$\underline{\text{Ex}}$ $5 = 1^2 + 2^2$

57

$\Rightarrow$ は明らか

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

$\exists z \in \mathbb{F}_p \quad z^2 = -1$

$0 \leq x, y < \sqrt{p}$ で　$(\sqrt{p}+1)^2 > p$

$x + yz$ in $\mathbb{F}_p$ を考える

ハトの巣原理から

$x + yz = x' + y'z$ in $\mathbb{F}_p$

$(x, y) \neq (x', y')$

となるに

$-\sqrt{p} < x, y < \sqrt{p}$　$x + yz = 0$ in $\mathbb{F}_p$

与 $x^2 + y^2 \underset{\text{mod } p}{\equiv} (x+yz)(x-yz)$

$p\mathbb{Z}$ の

に含まれる $0 < x^2 + y^2 < 2p$ //

$x^2+ax+b \quad a,b\in\mathbb{Q}$ が

どの $\mathbb{F}_p[x]$ で分解するか知りたい。

<u>Ex</u> x^2-5

これの一般化

<u>Ex</u> x^3-2 がどの $\mathbb{F}_p$ で解をもつか

$\Longleftrightarrow a(p)=2$ ($\Leftrightarrow \exists x \exists y,\ p=x^2+27y^2$)

$$\sum_{n\geq 1} a(n)q^n = q \times (1-q^6)(1-q^{12})(1-q^{18})(1-q^{24})\cdots(1-q^{18})(1-q^{36})(1-q^{54})\cdots$$

$$= q - q^7 + \cdots$$

q^{31}

$a(31)=2$

q^{30}

1 1 1 −1

<u>Ex</u> $31 = 2^2+27\cdot 1^2$

Ex

$$(1-q)(1-q^2)(1-q^3)(1-q^4)\cdots$$

$$=\sum_{m\in\mathbb{Z}}(-1)^m q^{\frac{(3m\pm1)m}{2}}$$

すかすか

(Euler 5角数定理)

$3=2^2-1$

$8=3^2-1$

$\mathbb{Q}(\zeta_n) \supseteq K \supseteq \mathbb{Q}$

$\Rightarrow$ $K/\mathbb{Q}$: ガロア拡大

$G(K/\mathbb{Q})$: アーベル

逆も成立

Ex $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$

$\zeta_3 = \dfrac{1+\sqrt{-3}}{2}$

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) & \\ \rotatebox{45}{$\subset$} & & \cup \\ \mathbb{Q}(\sqrt[3]{2}) & & \\ & \rotatebox{-45}{$\cup$} & \\ & & \mathbb{Q} \end{array}$$

非可換

$G(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \simeq \mathfrak{S}_3$

$$W_p^2 = (-1)^{\frac{p-1}{2}} p \in \mathbb{Q}[\zeta_p]$$

$$\sqrt{p} \in \mathbb{Q}(\sqrt{-1}, \zeta_p) \subseteq \mathbb{Q}(\zeta_{2p})$$

これから $\forall d \in \mathbb{Q}$

$\mathbb{Q}(\sqrt{d})$ は円分体

<u>Thm</u>

$$\begin{array}{ccc} & L \subseteq \overline{\mathbb{Q}} & \\ & \cup\!\!\mid & \\ \mathbb{Q}(\zeta_n) \subseteq & K & \end{array}$$

がGal拡大 $G(L/K) \simeq C_n$

$\Rightarrow \exists a \in L$ s.t. $L = K(a)$

$a^n \in K$

∵ $Gal(L/K)=\{\tau^0,\tau^1,\cdots,\tau^{n-1}\}$とする

$\tau: L\to L$: K-linearとみると、

固有値の集合 R

$\tau^n=id$　$\forall r\in R,\ r^n=1$　∴ $R\subseteq K$

$\mathrm{ord}\,\tau=n$ より Rはある原始1のn乗根をふくむ

claim　$R\subseteq K^\times$: 部分群

∵ $\tau(A)=\alpha A$　$\tau(AB)=\alpha\beta AB$ //
$\tau(B)=\beta B$

a：τのζ_n固有ベクトルをとる

$\tau(a) = \zeta_n a$ が 求めるaを示す

$b = a^n \in K$?

$\tau(b) = b$ を check する

$$\begin{array}{l} \tau(b) \\ \parallel \\ \tau(a)^n = (\zeta_n a)^n = a^n \end{array}$$

$K(a) = L$

Galoisの基本定理から $G(L/K(a)) = \{e\}$ をcheckする

$G(L/K)$

$\because$ $\tau^i(a) = \zeta_n^i a$ より //

<u>応用</u> フェルマー素数と作図可能性

<u>Thm</u> $p \geq 3$：素数

正p角形が作図可 $\Longleftrightarrow$ $\exists k \geq 0$ $p = 2^{2^k}+1$

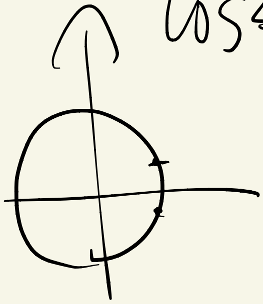
注 $p = 2^n + 1$ が素数 $\Rightarrow$ nは2の巾

(∵ $2^{3n}+1$ は 2^3+1 で割れるから

$x^3+1 = (x+1)(\quad)$)

$\boxed{\Rightarrow}$ $\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}\left(\cos\frac{2\pi}{p}\right) \supseteq \mathbb{Q}$

$\zeta_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, $\quad \cos\frac{2\pi}{p} = \frac{1}{2}\left(\zeta_p + \zeta_p^{-1}\right)$



$\left[\mathbb{Q}\left(\cos\frac{2\pi}{p}\right) : \mathbb{Q}\right] = \frac{\varphi(p)}{2} = \frac{p-1}{2}$ が2の巾

$\boxed{三}$ $\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}(\cos\frac{2\pi}{p}) \supsetneq \mathbb{Q}$

$G = G(\mathbb{Q}(\cos\frac{2\pi}{p})/\mathbb{Q}) \simeq C_{2^{2^k-1}}$

$p-1 = 2^{2^k}$

一般に

$$G = C_{2^n} \supsetneq C_{2^{n-1}} \supsetneq C_{2^{n-2}} \supsetneq \cdots \supsetneq C_2 \supsetneq C_1 = \{e\}$$

比 $= 2$

応用 (3次方程式の解法) お話

Cor Kummer 拡大の設定で

$$\begin{array}{c} L \subseteq \overline{\mathbb{Q}} \\ \cup| \\ \mathbb{Q}(\zeta_n) \subseteq K \end{array}$$

がある s.t. $G(L/K) \cong C_n$

$\Rightarrow L = K(a) \quad \exists a \in L$

$a^n \in K$

$\forall b \in L \quad (\zeta_n, b) := b + \zeta_n^{-1}\tau(b) + \cdots + \zeta_n^{-(n-1)}\tau^{n-1}(b)$

ラグランジュ分解式

は $(\zeta_n, b)^n \in K$

$$b = \frac{1}{n}\sum_{k=0}^{n} (\zeta_n^{k}, b)$$

固有空間への射影

Ex $n=3$

$$(\zeta_3^0, \theta) = \theta + \tau(\theta) + \tau^2(\theta)$$

$A \parallel$

$$(\zeta_3, \theta) = \theta + \zeta_3^{-1}\tau(\theta) + \zeta_3^{-2}\tau^2(\theta)$$

$B \parallel$

$$(\zeta_3^2, \theta) = \theta + \zeta_3^{-2}\tau(\theta) + \zeta_3^{-1}\tau(\theta)$$

$C \parallel$

$$\theta = \frac{A+B+C}{3} \quad \because \ \zeta_3^0 + \zeta_3^1 + \zeta_3^2 = 0$$

$$\zeta_3\theta + \tau(\theta) + \zeta_3^{-1}\tau^2(\theta)$$

$\parallel$

$\tau(B) = \zeta_3 B$ & check

$\parallel$

$$\tau(\theta) + \zeta_3^{-1}\tau^2(\theta) + \zeta_3^{-2}\theta$$

$$x^3+px+q=(x-t_1)(x-t_2)(x-t_3)$$

が十分一般であると仮定

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

$$\Delta=(t_1-t_2)(t_1-t_3)(t_2-t_3)$$

$$\zeta_3=\frac{1\pm\sqrt{-3}}{2}$$

$$\mathbb{Q}(\sqrt{-3},t_1,t_2,t_3)$$
$$\cup\!|$$
$$\mathbb{Q}(\sqrt{-3},p,q,\Delta)$$
$$\cup\!|$$
$$\mathbb{Q}(\sqrt{-3},p,q)$$
$$\|$$
$$\mathbb{Q}(\sqrt{-3},t_1,t_2,t_3)^{\mathfrak{S}_3}$$

$$\{e\}$$
$$\triangle$$
$$A_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$$
$$\triangle$$
$$\mathfrak{S}_3$$

$$t_1+t_2+t_3=0$$
$$p=t_1t_2+t_1t_3+t_2t_3$$
$$q=-t_1t_2t_3$$

Rk. $\overline{\mathbb{Q}}\supseteq L$, $L\cup K$, $K\supseteq\mathbb{Q}$

$$G\subseteq G(L/K)$$

$L\supseteq L^G$ は ガロア拡大

ラグランジュの分解式　$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

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

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

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

これらの3乗は $\mathbb{Q}(\sqrt{-3}, p, q, \sqrt{D})$ の元

$\tau B = \zeta_3 B$

$\tau C = \zeta_3 C$

$\mathfrak{S}_3 \setminus A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

$B \leftrightarrow C$　　$B \mapsto \zeta_3 C$　$B \mapsto \zeta_3^2 C$

$C \mapsto \zeta_3^2 B$　$C \mapsto \zeta_3 B$

よって $B^3 + C^3$, $B^3 C^3$ は $\mathfrak{S}_3$ 不変（つまり p と q で書ける）

Ex　1の3乗根　$\dfrac{-1+\sqrt{-3}}{2}$

$\sqrt[3]{1}$

1の9乗根　$\sqrt[9]{1}$　$\sqrt[3]{\dfrac{-1+\sqrt{-3}}{2}}$

ζ_n　1の7乗根　1の5乗根　$\dfrac{\sqrt{5}-1}{4}$

Ex　$x^3-15x-4=0$　解　4, $-2-\sqrt{3}$, $-2+\sqrt{3}$

$\sqrt[3]{2+11i}+\sqrt[3]{2-11i}$

$(2\pm i)^3=2\pm 11i$

一般に $(a+bi)^3=2+11i$

$a,b\in\mathbb{R}$

3倍角の公式

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

とくらべる

$$x = 2\sqrt{5}\cos\left(\frac{\arccos\frac{2}{5\sqrt{3}}}{3}\right)$$

(注) 4次方程式

$x^3 + px + q = 0$

3次方程式の解

$x = u + v$

0次　1次

$$\begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix} = x^3 + y^3 + z^3 - 3xyz$$

$$= (x+y+z)(x+\zeta_3 y+\zeta_3^2 z)$$

4次方程式の解の公式　$(x+\zeta_3^2 y+\zeta_3 z)$

不還元の場合

3次方程式で実根3つ(係数実)は複素数を1回も使わないようなやコン表示をもたない

ガロア基本定理

・円分体
・有限体

$L \supseteq K$ ガロア拡大のとき

$L^{G(L/K)} = K$

$\{G(L/K)$の部分群$\} \overset{1:1}{\longleftrightarrow} \{M \mid K \subseteq M \subseteq L\}$

$G(L/M) \longleftarrow M$

$G \longmapsto L^{G}$