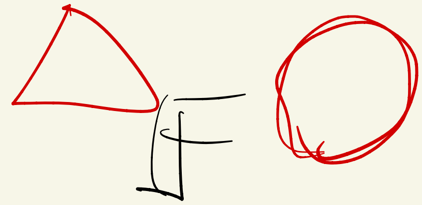
第11回 代数系



ガロアの基本定理

根の置換
対称性

<u>記法</u> $F \subseteq F'$：拡大

$$\mathrm{Gal}(F'/F) := \{\sigma : F' \xrightarrow{\sim} F' \text{ s.t. } \sigma|_F = \mathrm{id}_F\}$$

群

$\cup\!/$ あり意味なし

G

部分体

$$\mathrm{Gal}_F(F')$$

$$G(F'/F)$$

$$(F')^G := \{x \in F' \mid {}^\forall \sigma \in G,\ \sigma(x) = x\}$$

$$\left(\underset{F}{\cup\!|} \ \text{拡大} \right)$$

Rk $F \to F'$：準同型はいつでも単射

前回 $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ はガロア拡大

(Recall $F \subseteq F'$：有限次ガロア拡大

$\Leftrightarrow (F')^{G(F'/F)} = F$)

この講義では 代数体 $\overline{\mathbb{Q}} \supseteq K \supseteq \mathbb{Q}$：部分体

について示す。

・$\overline{\mathbb{Q}}$ を一般に作ることはしない

$F \rightsquigarrow \overline{F}$

・分離拡大に言及しない

(単拡大定理)

準備

Lemma A

$$\begin{tikzcd} \overline{\mathbb{Q}} \arrow[rr, bend left, red, "\exists\,\tau"] & & \\ \forall\, K \arrow[u, phantom, "\cup\!\shortmid" description] \arrow[rr, "\forall\,\psi"] & & \overline{\mathbb{Q}} \\ & \mathbb{Q} \arrow[ul, phantom, "\cup\!\shortmid" description] \arrow[ur, hook] & \end{tikzcd}$$

$$\begin{array}{ccc} & & \overline{\mathbb{Q}} \\ & & \cup\!\shortmid \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sim} & \mathbb{Q}(\sqrt{2}) \\ \sqrt{2} & \mapsto & \sqrt{2} \\ & \mathbb{Q} & \end{array}$$

はある $\tau \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ に拡張される

注 これは普遍性ではない（ただ1つではない）

∵ Zornの補題を用いる

Slogan $\forall$の代数閉体へのうめこみは拡張できる

$$X := \left\{ (L,\theta) \;\middle|\; \begin{tikzcd} \overline{\mathbb{Q}} & & \\ L \arrow[u, phantom, "\cup"] \arrow[drr, "\theta"] & & \\ K \arrow[u, phantom, "\cup"] \arrow[rr, "\psi"] & & \overline{\mathbb{Q}} \\ & \mathbb{Q} \arrow[ul, phantom, "\cup"] \arrow[ur, phantom, "\cup"] & \end{tikzcd} \right\} \neq \emptyset$$

$$X \ni (K,\psi)$$

$$(L,\theta) \leq (L',\theta') \overset{\text{def}}{\iff} \begin{cases} L \subseteq L' \\ \theta'|_L = \theta \end{cases}$$

とすると半順序集合

$\{(L_\lambda,\theta_\lambda)\}_{\lambda\in\Lambda}$ ：全順序部分集合 $\subseteq X$

$\Rightarrow L = \bigcup_{\lambda\in\Lambda} L_\lambda \subseteq \overline{\mathbb{Q}}$ ：体

$I_1 \subseteq I_2 \subseteq \cdots$ ：ideal

$\bigcup I_i$ ：ideal

(例)

$\theta : L \to \overline{\mathbb{Q}}$: well-def

$\alpha \mapsto \theta_\lambda(\alpha)$ if $\alpha \in L_\lambda$

とすると $\forall \lambda \in \Lambda,\ (L_\lambda, \theta_\lambda) \leq (L, \theta)$

よって X は極大元 (M, θ) をもつ

$$
\begin{tikzcd}
\overline{\mathbb{Q}} \supseteq M \arrow[drr, bend left, "\theta"] & & \\
K \arrow[u, phantom, sloped, "\subseteq"] \arrow[rr, "\psi"] & & \overline{\mathbb{Q}}
\end{tikzcd}
$$

$M \subsetneq \overline{\mathbb{Q}}$ とすると, $\alpha \in \overline{\mathbb{Q}} \setminus M$ をとる.

$f(x) = \mathrm{Irr}(M : x) \in M[x]$

$$\begin{tikzcd}
\overline{\mathbb{Q}} & & & \\
M(\alpha) \arrow[u, phantom, "\cup|" description] & & M[x]/(f(x)) \arrow[ll, phantom, "\simeq"] \arrow[d, bend right] & M[x] \arrow[l, two heads] \arrow[dl, "x \mapsto \alpha"] \\
& M \arrow[ul, phantom, "\cup|" description] \arrow[r, "\theta"] & \overline{\mathbb{Q}} &
\end{tikzcd}$$

これは M の極大性に反している。

$\therefore\ M=\overline{\mathbb{Q}}$

$\theta:\overline{\mathbb{Q}}\to\overline{\mathbb{Q}}$ ：単射

（注 $[\overline{\mathbb{Q}}:\mathbb{Q}]=“\infty”$）

$\theta(\overline{\mathbb{Q}})\simeq\overline{\mathbb{Q}}$ 共に代数閉体

$$\begin{array}{c} \overline{\mathbb{Q}} \\ \cup| \\ \theta(\overline{\mathbb{Q}}) \\ \cup| \\ \mathbb{Q} \end{array}$$

代数閉体

$\Rightarrow \theta(\overline{\mathbb{Q}})=\overline{\mathbb{Q}}$ //

Lemma 8

$$\begin{array}{ccc} & & K \subseteq \overline{\mathbb{Q}} \\ & & \cup\!| \\ \mathbb{Q} & \subseteq & k \end{array} \quad \text{有限次} \Rightarrow \exists \gamma \in K \text{ s.t. } K = k(\gamma)$$

(代数拡大)

(i.e. Kはk上単拡大)

Ex

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\ \cup\!| \\ \mathbb{Q}(\sqrt{2}) \end{array}$$

$$\begin{array}{ccc} & & \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \overline{\mathbb{Q}} \\ & & \cup\!| \\ \mathbb{Q} & \subseteq & \mathbb{Q} \end{array}$$

このとき

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}+\sqrt{3}) \\ \| \\ \mathbb{Q}(\sqrt{2},\sqrt{3}) \end{array}$$

$\alpha, \beta \in K$ について $k(\alpha,\beta) = k(\gamma)$
$\exists \gamma \in K$ を言う

$k[x]$
$\rotatebox{90}{$\in$}$

$$f_\alpha(x) = \mathrm{Irr}(k;\underset{\alpha_1}{\underset{\|}{\alpha}}) = (x-\alpha_1)\cdots(x-\alpha_n)$$

in $\overline{\mathbb{Q}}[x]$

$$f_\beta(x) = \mathrm{Irr}(k;\underset{\beta_1}{\underset{\|}{\beta}}) = (x-\beta_1)\cdots(x-\beta_m)$$

$$c \in k \setminus \left\{ \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \;\middle|\; \begin{array}{l} 1 \leq i \leq n \\ 2 \leq j \leq m \end{array} \right\}$$ をとる

(kが∞集合だから可能)

$\gamma = \alpha_1 + c\beta_1$ が求めるもの

($k(\gamma) \subseteq k(\alpha,\beta)$ は明らか)

$$g(X) := f_\alpha(\gamma - cX) \in k(\gamma)[X]$$

claim $g(\beta_1) = 0$

$\forall\, 2 \le j \le m \quad g(\beta_j) \neq 0$

(∵) $g(\beta_1) = f_\alpha(\alpha_1) = 0$

$$g(\beta_j) = f_\alpha(\underline{\alpha_1 + c\beta_1 - c\beta_j}) \neq 0$$

$\neq$

$\alpha_1, \alpha_2, \cdots, \alpha_n$

以上より $\mathrm{GCD}(g(x), f_\beta(x)) = x - \beta_1$

in $\overline{\mathbb{Q}}[x]$

in $k(\gamma)[x]$

(注) $k[x] \subseteq (k(\gamma))[x]$

つまり $\beta_1 = \beta \in k(\gamma)$

$\alpha = \gamma - c\beta \in k(\gamma)$ $\quad \therefore k(\alpha, \beta) \subseteq k(\gamma)$ $\;\;\parallel$

<u>Lemma C</u>

$$\begin{array}{ccc} & K & \subseteq \overline{\mathbb{Q}} \\ & \cup\!\! \mid & \text{有限} \\ \mathbb{Q} \subseteq & k & \end{array}$$

Slogan $G(\overline{\mathbb{Q}}/k)$ は解に推移的に作用する

$$|G(K/k)| \leq [K:k] = [G(\overline{\mathbb{Q}}/k) : G(\overline{\mathbb{Q}}/K)]$$

注 $H \supseteq H'$：部分群 $[H:H'] = |H/H'|$

左剰余類の数

注 $\tau \in G(\overline{\mathbb{Q}}/k)$ $\tau(K)$：k共役

$$\begin{array}{ccc} \overline{\mathbb{Q}} & \xrightarrow{\tau} & \overline{\mathbb{Q}} \\ \cup\!\! \mid & & \cup\!\! \mid \\ \mathbb{Q}(\sqrt[3]{2}) & \simeq & \mathbb{Q}(\sqrt[3]{2}\omega) \\ \cup\!\! \mid & & \\ \mathbb{Q} & & \end{array}$$

$\mathbb{Q}[x]/(x^3-2)$

(ii) $K = k(\alpha)$ とする

$$f(x) = \mathrm{Irr}(k : \alpha) = (x-\alpha_1)\cdots(x-\alpha_n)$$

$f(x) \in k[x]$, $\alpha = \alpha_1$, in $\overline{\Omega}[x]$

$\tau \in G(K/k)$ は $\tau(\alpha)$ で決まる

τ を $G(\overline{\Omega}/k)$ に拡張しておく

一方 $f(\tau(\alpha)) = 0$

$$f(\tau(\alpha)) = \tau(f(\alpha)) = f(\alpha)$$

$$\begin{tikzcd}
\overline{\Omega} \arrow[r, "\tau"] & \overline{\Omega} \\
K \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\tau"] & K \arrow[u, phantom, "\cup" rotate=90] \\
& k \arrow[ul, phantom, "\cup"] \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

よって $|G(K/k)| \leq n = [K : k]$

$R=\{\alpha_1,\cdots,\alpha_n\}$：根の集合

$G(\overline{\mathbb{Q}}/k) \curvearrowright R$

$(\tau,\alpha_i) \mapsto \tau(\alpha_i)$

<u>主張</u> この作用の orbit は 1つ

$\because$

$$\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[rr, "\sim", "\tau"'] & & \overline{\mathbb{Q}} \\
k(\alpha_1) \arrow[u, phantom, "\cup" rotate=90] \arrow[rr, "\sim"] & & k(\alpha_s) = k[x]/(f(x)) \arrow[u, phantom, "\cup" rotate=90] \\
& k \arrow[ul, phantom, "\cup"] \arrow[ur, phantom, "\cup"] &
\end{tikzcd}$$

Lemma A より 拡張できて $\tau(\alpha_1)=\alpha_s$

よって

$$\mathrm{Stab}_{G(\overline{\mathbb{Q}}/k)}(\alpha_1) = G(\overline{\mathbb{Q}}/K)$$

注 $K = k(\alpha_1)$

$$\therefore \left(G(\overline{\mathbb{Q}}/k) : G(\overline{\mathbb{Q}}/K) \right) = |R| = n$$

Lemm C によって 有限群

Lemma D

$$\begin{array}{ccc} & K & \subseteq \overline{\mathbb{Q}} \\ & \cup & \text{有限} \\ \mathbb{Q} \subseteq & k & \end{array}$$

$G \le \mathrm{Gal}(K/k)$ 部分群

について $[K : K^G] = |G|$

$$\begin{tikzcd} \overline{\mathbb{Q}} \arrow[r, "\tau"] & \overline{\mathbb{Q}} \\ \mathbb{Q}(\sqrt{2}) \arrow[u, phantom, "\cup"] \arrow[r] & \mathbb{Q}(\sqrt{2}) \arrow[u, phantom, "\cup"] \\ & \mathbb{Q} \arrow[ul, phantom, "\cup"] \arrow[u, phantom, "\cup"] \end{tikzcd}$$

$\forall \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K^G) \quad \tau(K) = K$

(∵) $K = K^G(\alpha)$ とする

$f(x) = \mathrm{Irr}(K^G ; \underset{\underset{\alpha_1}{\shortparallel}}{\alpha}) = (x-\alpha_1)\cdots(x-\alpha_n)$

$\underset{K^G[x]}{\cap}$ in $\overline{\mathbb{Q}}[x]$

$$g(x) := \prod_{\sigma \in G} (x - \sigma(\alpha)) \in K^G[x]$$

((∵) $\sigma \in G$: fix $\begin{array}{c} G \to G \\ x \mapsto \sigma x \end{array}$ は bij)

$g(\alpha) = 0$ (∵ $G \ni \mathrm{id}$)

f の最小性より $f(x) \mid g(x)$

一方で $\sigma(\alpha)$ は $\alpha_1 \sim \alpha_n$ のどれか

$\sigma \neq \sigma'$ in $G \Rightarrow \sigma(\alpha_1) \neq \sigma'(\alpha_1)$

$(\because\ \sigma(\alpha_1) = \alpha_1 \Rightarrow \sigma = id_K)$

(よって $\deg g(x) = |G|$)

$g(x) \mid f(x)$ in $\overline{\mathbb{Q}}[x]$

$\Downarrow$

in $K^G[x]$

$\therefore f(x) = g(x)$

よって $n = |G|$

$$\begin{array}{ccc}
\overline{\mathbb{Q}} & \xrightarrow{\tau} & \overline{\mathbb{Q}} \\
\cup & & \cup \\
K^G(\alpha_1) = K & \xrightarrow{\tau|_K} & K^G(\alpha_s) \subseteq K \\
\cup & & \cup \\
& K^G &
\end{array}$$

同様に $\tau(\alpha_1) = \cancel{\alpha_1 \sim \alpha_n}\ \alpha_s$

αどれか だだない

$\forall 1 \leq i \leq n\ (\alpha_i \in K)$

Lem A, B, C, D ⇒ 言いかえ

(拡張 代数閉体) 単拡大 固定体について

$G(\overline{\mathbb{Q}}/k)$ が根に推移的に作用する

Prop $K \subseteq \overline{\mathbb{Q}}$
$\quad\;\; \cup\!\mid$ 有限 かつ Galois拡大
$\mathbb{Q} \subseteq k$

$\left(\text{i.e. } K^{G(K/k)} = k \right)$

$\Leftrightarrow \quad G(\overline{\mathbb{Q}}/k) \twoheadrightarrow G(K/k)$ が well-def

$\sigma \longmapsto \sigma|_K$ (注 このときLemAより全射)

$\left(\text{i.e. } \forall \sigma \in G(\overline{\mathbb{Q}}/k),\ \sigma(K) \subseteq K \right)$

"="

注

$$\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[r, "\exists"] & \overline{\mathbb{Q}} \\
K \arrow[u, phantom, sloped, "\subset"] \arrow[r, "\forall"] & K \arrow[u, phantom, sloped, "\subset"] \\
& k \arrow[ul, phantom, sloped, "\subset"] \arrow[u, phantom, sloped, "\subset"]
\end{tikzcd}$$

$\boxed{\Rightarrow}$ Lem D

$\boxed{\Leftarrow}$ $\to$ のKer $= G(\overline{\mathbb{Q}}/K)$

準同型 thm より

$$G(K/k) \simeq G(\overline{\mathbb{Q}}/k) / G(\overline{\mathbb{Q}}/K)$$

個数をとると Lem C より

$$|G(K/k)| = [K : k] \leftarrow 系$$

$K = k(\alpha)$

$$\mathrm{Irr}(k;\alpha) = (x-\alpha_1) \cdots (x-\alpha_n)$$

$\mathrm{Irr}(k;\alpha) = f(x) \in k[x]$, $\alpha = \alpha_1$

~~in $\mathbb{Q}[x]$~~

与の二と利 in $K[x]$

$\forall i$, $\sigma_i \in \mathrm{Gal}(K/k)$ s.t. $\sigma_i(\alpha) = \alpha_i$

与から $K^{G(K/k)} = k$ を示す

$b \in K$ は $b = c_0\alpha^0 + c_1\alpha^1 + \cdots + c_{n-1}\alpha^{n-1}$

(ここで $c_0 \sim c_{n-1} \in k$)

$b \in K^{G(K/k)}$ とする

$$b = \sigma_2(b) = c_0\alpha_2^0 + c_1\alpha_2^1 + \cdots + c_{n-1}\alpha_2^{n-1}$$

$$\vdots$$

$$b = \sigma_n(b) = c_0\alpha_n^0 + c_1\alpha_n^1 + \cdots + c_{n-1}\alpha_n^{n-1}$$

$$\begin{pmatrix} b \\ \vdots \\ b \end{pmatrix} = \underline{\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & & \alpha_n^{n-1} \end{pmatrix}} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

Van der Monde より $\underline{\qquad\qquad}$ は $\det \neq 0$

$$\det = \pm \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

クラメルの公式より

$1 \le i < n \Rightarrow c_i = 0$

e.g.

$$c_1 = \frac{\det_{ui}\begin{pmatrix} 1 & b & \text{残り} \\ \vdots & \vdots & \\ 1 & b & \end{pmatrix}}{\det \underline{\qquad\qquad}} = 0$$

//

系 $\begin{array}{c} K \subseteq \overline{\mathbb{Q}} \\ \cup\!\! \mid \\ \mathbb{Q} \subseteq k \end{array}$ がガロア拡大

$$\Rightarrow |G(K/k)| = [K:k]$$

Thm（ガロア理論の基本定理）

$\begin{array}{c} K \subseteq \overline{\mathbb{Q}} \\ \cup\!\! \mid \\ \mathbb{Q} \subseteq k \end{array}$ がガロア拡大

$$F \longmapsto G(K/F)$$

$$\{F \mid k \subseteq F \subseteq K\} \qquad \{G \mid G \subseteq G(K/k)\}$$

中間体　　　　部分群

$$K^G \longleftarrow\!\!\shortmid\; G$$

は1:1対応を与える。

∵) (P) $K^{G(K/F)} = F$ を言う（$\supseteq$ は明らか）

(Q) $G(K/K^G) = G$ を言う（$\supseteq$ 〃）

<u>claim</u> ${}^{\forall}_{\Bbbk \le} F \subseteq K$, K/F はガロア拡大

（$\Rightarrow$ (P)）

∵) $\sigma \in G(\overline{\mathbb{Q}}/F) \subseteq G(\overline{\mathbb{Q}}/\Bbbk)$

$\sigma(K) = K$ と check より OK //

系より $|G(K/K^G)| = [K : K^G] \underset{\text{Lem D}}{=} |G|$

よって (Q) //

<u>Cor</u> Thmの対応で

F_1, F_2 が k共役

$k \subset F_1, F_2 \subset K$ $\Longleftrightarrow$ $G(K/F_1), G(K/F_2)$ が $G(K/k)$ の共役部分群

$(K \supset)$

<u>Cor</u> F/k が ガロア拡大

$\Longleftrightarrow$ $G(K/F) \triangleleft G(K/k)$

このとき $G(F/k) \simeq G(K/k)/G(K/F)$

∵ $G(K/k) \twoheadrightarrow G(F/k)$ が全射

$$\left(\begin{tikzcd}
\bar{k} \arrow[r] & \bar{k} \\
K \arrow[u, phantom, "\subset" rotate=90] \arrow[r] & K \arrow[u, phantom, "\subset" rotate=90] \\
F \arrow[u, phantom, "\cup" rotate=180] \arrow[r] & F \arrow[u, phantom, "\cup" rotate=180] \\
 & k \arrow[ul, phantom, "\cup"] \arrow[u, phantom, "\subset"]
\end{tikzcd}\right)$$

$F_2 = \sigma F_1$ のとき　　$\sigma \in \cancel{Gal(\overline{\mathbb{Q}}/k)}$

$Gal(K/k)$ としてよい

$$\begin{tikzcd}
\overline{\mathbb{Q}} \arrow[r] & \overline{\mathbb{Q}} \\
K \arrow[u, phantom, "\cup"] \arrow[r] & K \arrow[u, phantom, "\cup"] \\
& k \arrow[ul, phantom, "\cup"] \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

$G(K/F_2) \hookrightarrow G(K/F_1)$ は well-def

$\tau \longmapsto \sigma^{-1}\tau\sigma$

$$\sigma^{-1}\tau\sigma(x) \quad x \in F_1$$
$$\shortparallel$$
$$\sigma^{-1}\sigma(x) = x$$

$\therefore\ \underline{G(K/F_1) = \sigma^{-1}G(K/F_2)\sigma}$

逆に ＿＿＿ なら $F_2 = \sigma F_1$ を示す

$\sigma F_1 \subseteq F_2$ を示す

$\because$ $K^{\mathrm{Gal}(K/F_1)} = F_1$

$$\cup\!\!\!\!\shortmid\quad \{x \in K \mid \underbrace{\sigma^{-1}\tau\sigma(x) = x}_{\Downarrow \atop \tau\sigma(x) = \sigma(x)} \quad \forall \tau \in \mathrm{Gal}(K/F_2)\}$$

よって $\sigma F_1 = F_2$

(あるいは役割を変えて $\sigma^{-1} F_2 \subseteq F_1$
一方で $F_1 \subseteq \sigma^{-1} F_2$ からも出る)

Ex $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \overline{\mathbb{Q}}$

$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) \\ \parallel \\ K \\ \cup \\ \mathbb{Q} \end{array}$$

最小多項式は

$x^4-10x+1$

$= (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x+(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}-\sqrt{3}))$

claim $K/\mathbb{Q}$ はガロア拡大

☺ 解は $\alpha_1 = \sqrt{2}+\sqrt{3} = \alpha$

$\alpha_2 = \sqrt{2}-\sqrt{3} = -1/\alpha$

$\alpha_3 = -\sqrt{2}+\sqrt{3} = 1/\alpha$

$\alpha_4 = -(\sqrt{2}+\sqrt{3}) = -\alpha$

K の $\mathbb{Q}$ 共役体 $K(\alpha_i) = K$

(i.e. $\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ σK aで) //

よって

$$G = \mathrm{Gal}(K/\mathbb{Q})$$

$$= \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

$\sigma_i(\alpha) = \alpha_i$ で決まる

$|G| = 4$ なので $G = C_2 \times C_2$ or C_4

$\parallel$

p^2

$\forall i,\ \sigma_i^2 = \mathrm{id}$ は容易。これから $G \simeq C_2 \times C_2$

F

$$\begin{array}{ccccc} & & \mathbb{Q}(\sqrt{2}+\sqrt{3}) & & \\ & \cup & \cup & \cup & \\ \mathbb{Q}(\sqrt{2}) & & \mathbb{Q}(\sqrt{3}) & & \mathbb{Q}(\sqrt{6}) \\ & \cup & \cup & \cup & \\ & & \mathbb{Q} & & \end{array}
\qquad
\begin{array}{ccccc} & & \{e\} & & \\ & / & | & \backslash & \\ H_2 & & H_3 & & H_4 \\ & \backslash & | & / & \\ & & G \simeq C_2 \times C_2 & & \end{array}$$

例えば

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})^{\sigma_2}$$

$$H_2 = \{\underset{e}{\underset{\shortparallel}{\sigma_1}}, \sigma_2\}$$

$$H_3 = \{\sigma_1, \sigma_3\}$$

$$H_4 = \{\sigma_1, \sigma_4\}$$

たとえば

$$\sigma_2(\sqrt{2}) = \sigma_2\left(\frac{\alpha - \frac{1}{\alpha}}{2}\right)$$

$$= \frac{\alpha_2 - \frac{1}{\alpha_2}}{2} = \frac{-\frac{1}{\alpha} + \alpha}{2} = \sqrt{2}$$

省略

$$\sigma_3(\sqrt{2}) = \frac{\alpha_3 - \frac{1}{\alpha_3}}{2} = \frac{-\alpha + \frac{1}{\alpha}}{2} = -\sqrt{2} = \sigma_4(\sqrt{2})$$

全く同様に

$\sigma_3(\sqrt{3}) = \sqrt{3}$

$\sigma_4(\sqrt{6}) = \sqrt{6}$　も含める。

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$= \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \;\middle|\; \begin{matrix} a,b \\ c,d \in \mathbb{Q} \end{matrix} \right\}$$

<u>Ex</u>　$K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$　$\omega = \dfrac{-1+\sqrt{-3}}{2}$

$$\begin{array}{ccc} & K & \\ / & | & \backslash \\ \mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\sqrt[3]{2}\omega^2) & \mathbb{Q}(\sqrt[3]{2}\omega) \\ \cup\!| & & \\ \mathbb{Q} & & \end{array}$$

全て $\mathbb{Q}[x]/(x^3-2)$ と同型

$$\begin{array}{ccc} \overline{\mathbb{Q}} & \longrightarrow & \overline{\mathbb{Q}} \\ \cup\!| & & \cup\!| \\ \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sim} & \mathbb{Q}(\sqrt[3]{2}\omega) \end{array}$$

$\mathbb{Q}(\sqrt[3]{2})$ はガロア拡大ではない

claim $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}$ は
がロア拡大

㊀ 省略

$G = Gal(K/\mathbb{Q})$ とおくと

$$D_3 \cong \mathfrak{S}_3$$

$|G| = 6$ より $G \simeq C_6$ or $\mathfrak{S}_3$

2p

がロア拡大でない中間体があることより

$G \simeq \mathfrak{S}_3$

$\sigma, \tau \in G(K/\mathbb{Q})$

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ $\quad$ $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$

$\sigma(\sqrt{-3}) = \sqrt{-3}$ $\quad$ $\tau(\sqrt{-3}) = -\sqrt{3}$

となるものがあることがわかる（省略）

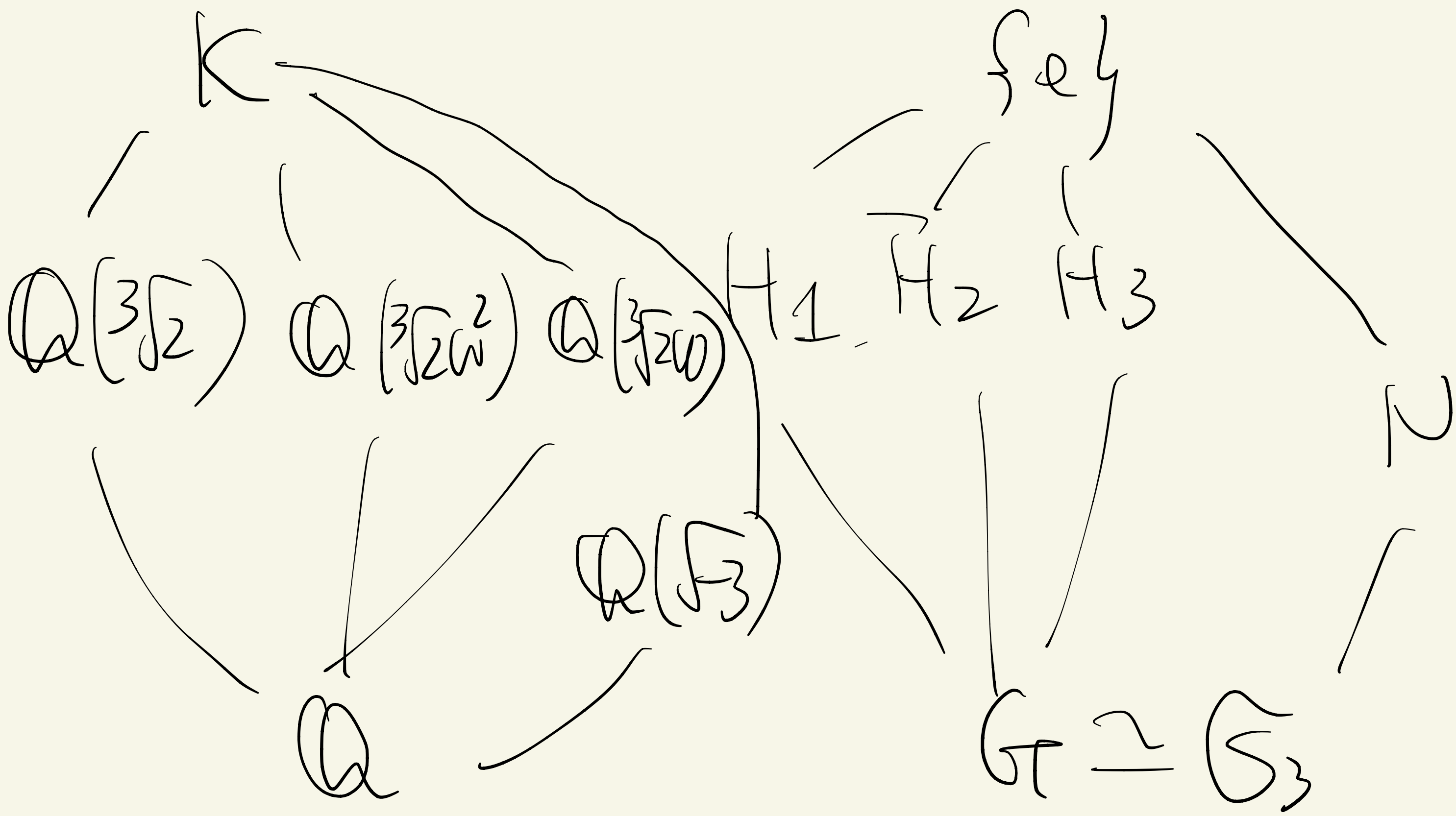
今 $\sigma^3 = 1$

$\tau^2 = 1$

$$G = \left\{ \begin{array}{l} e,\ \sigma,\ \sigma^2 \\ \tau,\ \sigma\tau,\ \sigma^2\tau \end{array} \right\}$$

$$\begin{array}{cc} \| & \| \\ \tau\sigma^2 & \tau\sigma \end{array}$$

$N = \{e, \sigma, \sigma^2\}$



$$\|$$

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

Open Problem ガロアの逆問題

G : 有限群 $\exists K/\mathbb{Q}$: Galois 拡大

s.t. $G(K/\mathbb{Q}) \simeq G$

$\mathbb{Q}(\sqrt[4]{2})$ $x^4 - 2$ $x^3 - 2$

$\cup$

$\mathbb{Q}$