

A rectangular area with a blue background showing a sky with light clouds over a calm ocean surface.

Calculating Galois Group with *Magma*

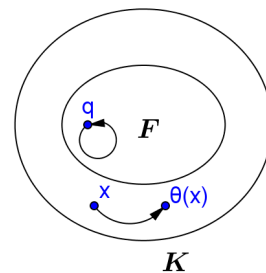
2017年7月2日
Cabri 研究会
生越 茂樹

§ 1. Galois群 の定義

体 K が、体 F 上の(= F 係数の)ある既約多項式の最小分解体となる時、 K を F の Galois拡大(正規拡大)という。この時、 K の F 上の自己同型群(= F の要素を固定する K の自己同型群)全ての集合を「 K の F 上のGalois群」といい $\text{Gal}(K/F)$ と表す。即ち、 $\text{Gal}(K/F)$ の要素を θ とすると、

$\forall x, y \in K, \forall q \in F$ に対し

$$\begin{cases} \theta(x+y) = \theta(x) + \theta(y) \\ \theta(xy) = \theta(x)\theta(y) \\ \theta(q) = q \end{cases}$$



$f(x)$ が F 上の多項式で $f(x)=0$ のとき、 $\theta(f(x))=f(\theta(x))=0$ が成り立つので $\theta(x)$ も $f(x)=0$ の解である。即ち、 θ は $f(x)=0$ の解の置換となる。

§ 2. Galois群 の例

[大原則] F 上の既約方程式 $f(x)=0$ の解は, 全て同等である (代数的に区別できない).
即ち 任意の 2 解を α, β とすると $F(\alpha) \cong F(\beta)$

例: $\mathbb{Q}$ 上の方程式 $f(x)=0$ が $\sqrt{2}$ を解に持てば $(-\sqrt{2})$ も解にもつ. そして $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$
 $1+\sqrt[3]{5}$ を解にもつと, $1+\sqrt[3]{5}\omega$, $1+\sqrt[3]{5}\omega^2$ も解にもつ. また $\mathbb{Q}(1+\sqrt[3]{5}) = \mathbb{Q}(1+\sqrt[3]{5}\omega) = \mathbb{Q}(1+\sqrt[3]{5}\omega^2)$

【例 1】 $f(x)=x^2-3$ の Galois 群

$f(x)=0$ の解は $\alpha=\sqrt{3}$, $\beta=-\sqrt{3}$

$K=\mathbb{Q}(\alpha, \beta)$ とすると $K=\mathbb{Q}(\alpha)$

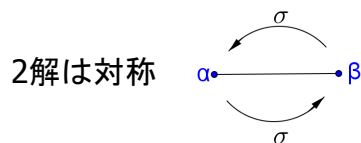
また

$\begin{cases} e(\alpha)=\alpha \text{ とすると, } e(\beta)=e(-\alpha)=-e(\alpha)=-\alpha=\beta, \\ \sigma(\alpha)=\beta \text{ とすると, } \sigma(\beta)=\sigma(-\alpha)=-\sigma(\alpha)=-\beta=\alpha \end{cases}$

「 α の像は α または β 」だから, $\leftarrow$
 $G(K/\mathbb{Q}) = \{e, \sigma\}$ (位数 2 の巡回群 C_2)

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2}) = \{a+b\sqrt{2} \mid a \in \mathbb{Q}, b \in \mathbb{Q}\}$
 $\mathbb{Q}(\sqrt[3]{5}) = \{a+b\sqrt[3]{5}+c(\sqrt[3]{5})^2 \mid a \in \mathbb{Q}, b \in \mathbb{Q}, c \in \mathbb{Q}\}$
 $\mathbb{Q}(\sqrt[3]{5}\omega) = \{a+b\sqrt[3]{5}\omega+c(\sqrt[3]{5}\omega)^2 \mid a \in \mathbb{Q}, b \in \mathbb{Q}, c \in \mathbb{Q}\}$
この場合も $\mathbb{Q}(\sqrt[3]{5}) \cong \mathbb{Q}(\sqrt[3]{5}\omega)$

$\theta \in G(K/F)$ とすると
「 $\theta(\alpha^2-3)=\theta(0)=0$ 」だから
 $\theta(\alpha^2-3)=\theta(\alpha)^2-\theta(3)=\theta(\alpha)^2-3=0$
 $\therefore \theta(\alpha)$ は $f(x)=0$ の解の一つ



既約3次方程式の3解は対称なので Galois群は S_3 (3次対称群)となることが多い.
 しかし, 特別な関係 ($\sqrt{D}$ が有理数, D は判別式)があると巡回群になる.

【例2】 $f(x) = x^3 - 3x + 1$ の Galois 群

$f(x) = 0$ の解を α, β, γ , 判別式を D とすると,

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha = -3 \quad \dots \textcircled{1} \\ \alpha\beta\gamma = -1 \end{cases}$$

$$D = -4(-3)^3 - 27 \cdot 1^2 = 81 = 9^2 \quad \dots \textcircled{2}$$

$$\therefore (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = \pm 9 \in \mathbb{Q}$$

「 $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = -9$ 」 とすると, ①及び「 $\alpha^3 = 3\alpha - 1$ 」より

$$\beta - \gamma = \frac{1}{(\alpha - \beta)(\alpha - \gamma)} = \frac{1}{\alpha^2 - (\beta + \gamma)\alpha + \beta\gamma} = \frac{1}{\alpha^2 - (-\alpha)\alpha - \frac{1}{\alpha}} = \frac{9\alpha}{2\alpha^3 - 1} = \frac{3\alpha}{2\alpha - 1}$$

$$\text{「}\beta + \gamma = -\alpha\text{」と連立して} \quad \beta = \frac{-\alpha^2 + 2\alpha}{2\alpha - 1}, \quad \gamma = \frac{-\alpha^2 - \alpha}{2\alpha - 1} \quad \dots \textcircled{3}$$

よって $K = \mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha)$ となり, 同型写像は α の像で決まる. $\dots \textcircled{4}$

$\therefore e(\alpha) = \alpha$ とすると, $e(\beta) = \beta, e(\gamma) = \gamma$ (e は恒等写像)

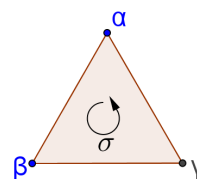
次に $\sigma(\alpha) = \beta$ とする. この時 $\sigma(\beta) = \alpha$ とすると $\sigma(\gamma) = \gamma$. しかし対称性より α, β も γ の式で表されるので $\sigma(\gamma) = \gamma$ のとき, $\sigma(\alpha) = \alpha$ となり矛盾. よって $\sigma(\beta) = \gamma$. 同様にして $\sigma(\gamma) = \alpha$. すなわち

$$\sigma(\alpha) = \beta, \sigma(\beta) = \gamma, \sigma(\gamma) = \alpha$$

④より, $\#G(K/\mathbb{Q}) = 3$ ($\#G$ は Galois群の位数) だから $G(K/\mathbb{Q}) = \{e, \sigma, \sigma^2\}$ (位数3の巡回群 C_3)

$$\leftarrow \begin{array}{l} x^3 + px + q = 0 \text{ の判別式;} \\ D \equiv (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = -4p^3 - 27q^2 \end{array}$$

$$G(K/\mathbb{Q}) = \{e, \sigma, \sigma^2\}$$



$\sqrt{D}$ が有理数でない既約3次方程式の3解は完全に対称で, 全ての解の置換が可能.
すなわち Galois群は S_3 (3次対称群)となる. [$\because$ 例2と同様にして $Q(\alpha, \beta, \gamma) = Q(\sqrt{D}, \alpha)$]

【例3】 $f(x) = x^3 + px + q = 0$ の解

一般に $x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x^2 + y^2 + z^2 - xy - yz - zx) = (x+y+z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z)$

$x^3 + px + q$ と比べて, $p = -3yz, q = y^3 + z^3$ (ここで $y = -u, z = -v$ とおく)

$$\text{よって } \begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \end{cases} \text{ をみたす } u, v \text{ を見つけると, } f(x) = 0 \text{ の解は } \begin{cases} \alpha = u + v \\ \beta = \omega u + \omega^2 v \\ \gamma = \omega^2 u + \omega v \end{cases}$$

$$u^3, v^3 \text{ は } t^2 + qt - \frac{p^3}{27} = 0 \text{ の2解となる. } t = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = \frac{-q \pm \sqrt{-(27q^2 + 4p^3)/(-27)}}{2} = -\frac{q}{2} \pm \frac{\sqrt{-D/27}}{2} \text{ だから,}$$

(D は $f(x) = 0$ の判別式) 解は次の様になる.

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \sqrt[3]{-\frac{q}{2} - \sqrt{R}}, \quad \beta = \omega \sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \omega^2 \sqrt[3]{-\frac{q}{2} - \sqrt{R}}, \quad \gamma = \omega^2 \sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \omega \sqrt[3]{-\frac{q}{2} - \sqrt{R}} \quad \left(R = -\frac{D}{108} \right)$$

同型写像として

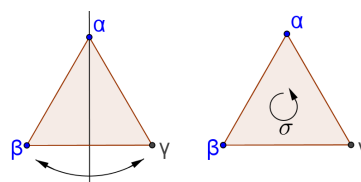
$$\tau: \sqrt{R} \rightarrow -\sqrt{R} \text{ (} x^2 = R \text{ の別の解を取る), } \sigma: \sqrt[3]{-\frac{q}{2} + \sqrt{R}} \rightarrow \omega \sqrt[3]{-\frac{q}{2} + \sqrt{R}} \text{ (} x^3 = -\frac{q}{2} + \sqrt{R} \text{ の別の解を取る)}$$

とすると「 $uv = -p/3 \in Q$ 」より u が決まると v も決まるので,

$$\begin{cases} \tau(\alpha) = \alpha, \tau(\beta) = \gamma, \tau(\gamma) = \beta \\ \sigma(\alpha) = \beta, \sigma(\beta) = \gamma, \sigma(\gamma) = \alpha \end{cases}$$

ゆえに α, β, γ の間に特別な関係のない ($\sqrt{D}$ が有理数でない) 時は

$$G(K/Q) \cong D_3 (\text{正3角形の2面体群}) \cong S_3 \text{ (3次対称群)}$$



例4. $f(x) = x^3 - 6x - 6$

$D = -108$ なので $\sqrt{D}$ は有理数でない.

解の公式より, $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$, $\beta = \sqrt[3]{2} \omega + \sqrt[3]{4} \omega^2$, $\gamma = \sqrt[3]{2} \omega^2 + \sqrt[3]{4} \omega$.

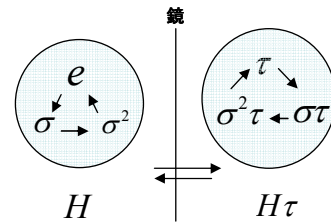
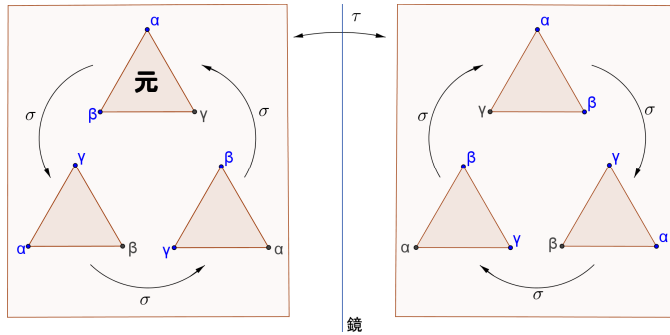
この時 τ : 「3乗根内の数字(2と4)の入替」, σ : 「 $x^3 = 2$ の解の入替 $\sqrt[3]{2} \rightarrow \sqrt[3]{2}\omega$ 」となり,

$$\begin{cases} \tau(\alpha) = \alpha, \tau(\beta) = \gamma, \tau(\gamma) = \beta \\ \sigma(\alpha) = \beta, \sigma(\beta) = \gamma, \sigma(\gamma) = \alpha \end{cases} \quad G \equiv G(K/Q) = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

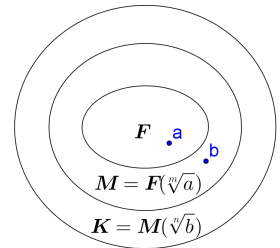
$H = \{e, \sigma, \sigma^2\}$ とすると $G = \{H, H\tau\}$. さらに $G \triangleright H \triangleright \{e\}$ (正規列)で

$$G/H \cong \{e, \tau\}, \quad H/\{e\} \cong H = \{e, \sigma, \sigma^2\}$$

$G \triangleright H$ は
 H が G の正規部分群
 である事を表す記号



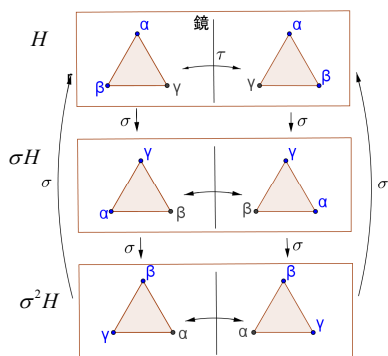
一般に, 体 F が必要な累乗根を含んでいる時, $G \triangleright H \triangleright \{e\}$ かつ $\#(G/H) = m$,
 $\#(H/\{e\}) = n$ (m, n 素数) とすると, $f(x) = 0$ の解は $\sqrt[m]{\dots \sqrt[n]{a} \dots}$ の結合で表される.
 (逆も成り立つ. また正規列の長さが伸びても同様.)



例5. $\mathbb{Q}$ 上の3次方程式 $f(x)=0$ が $\sqrt{1+\sqrt[3]{2}}$ を解に持つことはあるか？

[説明 A] ない. 対称性より $\pm\sqrt{1+\sqrt[3]{2}}, \pm\sqrt{1+\sqrt[3]{2}\omega}, \pm\sqrt{1+\sqrt[3]{2}\omega^2}$ も解に持つはずなので $f(x)$ は 6次以上.

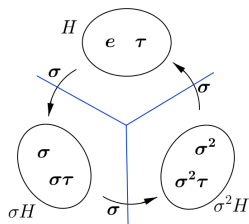
[説明 B] ない. $\sqrt{1+\sqrt[3]{2}}$ を解に持てば「 $G \triangleright H \triangleright \{e\}$ かつ $\#(G/H)=3, \#(H)=2$ 」となるはず. 例えば $H = \{e, \tau\}$ とすると, $G = H + \sigma H + \sigma^2 H$. しかし H は $G (\cong S_3)$ の正規部分群ではないので 不適.



$$\begin{cases} \tau = (\beta, \gamma) \text{ とすると } \tau H = H, & \tau(\sigma H) = \sigma^2 H, & \tau(\sigma^2 H) = \sigma H \\ g_1 = (\alpha, \beta) \text{ とすると } g_1 H = \sigma^2 H, & g_1(\sigma H) = \sigma H, & g_1(\sigma^2 H) = H \\ g_2 = (\gamma, \alpha) \text{ とすると } g_2 H = \sigma H, & g_2(\sigma H) = H, & g_2(\sigma^2 H) = \sigma^2 H \end{cases}$$

例えば (β, γ) は H を H に移すが, (β, α) は H を $\sigma^2 H$ に移す.
 (β, γ) と (β, α) は α, β, γ の対称性から同じ働きを持つはずなので
 矛盾する. このように $g \in H$ なら, g に共役な $a^{-1}ga (\forall a \in G)$ も
 H に入らないといけない.

故に H は共役類の和集合 = 正規部分群となる.



$$G \triangleright H \iff \forall a \in G \text{ に対し } a^{-1}Ha = H \iff H \text{ は 共役類の和}$$

既約4次方程式の4解は対称なので Galois群は S_4 (4次対称群)となることが多い. しかし, 特別な関係があると A_4 (4次交代群), V_4 (Kleinの4元群), D_4 (正方形の2面体群), C_4 (4次巡回群)のいずれかになる.

例6. (円分多項式) $f(x) = x^4 + x^3 + x^2 + x + 1$

$\zeta = \cos \frac{\pi}{5} + i \sin \frac{\pi}{5}$, $x_k = \zeta^k$ ($k=1,2,3,4$) とすると

$f(x)=0$ の解は x_1, x_2, x_3, x_4 . ここで $\sigma(\zeta) = \zeta^2$ と

定めると, σ は $K = Q(\zeta)$ の同型写像で, σ は次の様に x_k を移す.

$\zeta \rightarrow \zeta^2 \rightarrow \zeta^4 \rightarrow \zeta^3 (\rightarrow \zeta)$

よって $\sigma^4(\zeta) = \zeta$ となるので

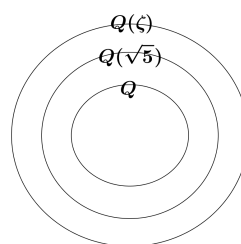
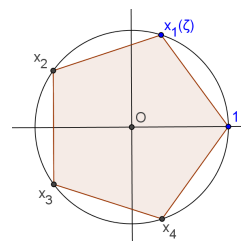
$G \equiv G(K/Q) = \{e, \sigma, \sigma^2, \sigma^3\} = C_4$ (4次の巡回群)

ここで $H = \{e, \sigma^2\}$ とすると, $G \supset H \supset \{e\}$. $\#(G/H) = \#(H) = 2$

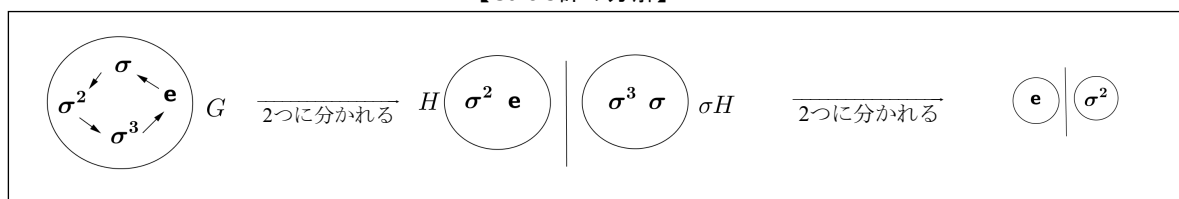
よって $f(x)=0$ は平方根を2回取ることによって解ける.

$$\left(\zeta = \cos \frac{\pi}{5} + i \sin \frac{\pi}{5} = \frac{-1 + \sqrt{5} + \sqrt{10 - 2\sqrt{5}} i}{4} \right)$$

【Galois群の分解】



[$x^2 = 5$ と $x^2 = 2\sqrt{5} - 10$ による拡大]



既約4次方程式(複2次式)のGalois群は, 特別な関係がないときは D_4 (正方形の2面体群) となる.

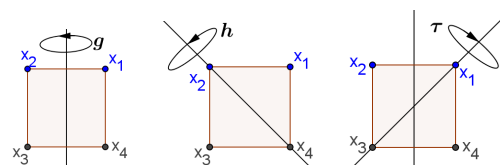
例7. (複2次式) $f(x) = x^4 - 6x^2 + 3$ の Galois群

$t^2 - 6t + 3 = 0$ の 2 解は $3 + \sqrt{6}$, $3 - \sqrt{6}$.

よって $f(x) = 0$ の解は

$$x_1 = \sqrt{3 + \sqrt{6}}, x_3 = -\sqrt{3 + \sqrt{6}}, x_2 = \sqrt{3 - \sqrt{6}}, x_4 = -\sqrt{3 - \sqrt{6}}$$

同型写像の生成元は



g :「 $x^2 = 6$ の 2 解の取替え」, h :「 $x^2 = 3 + \sqrt{6}$ の 2 解の取替え」, τ :「 $x^2 = 3 - \sqrt{6}$ の 2 解の取替え」
の 3 種類ある. これを正方形 $x_1 x_2 x_3 x_4$ に関する置換で表すと

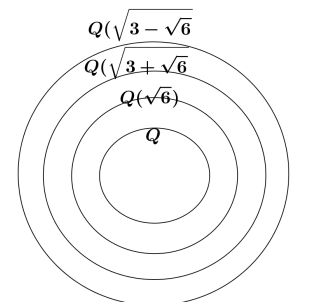
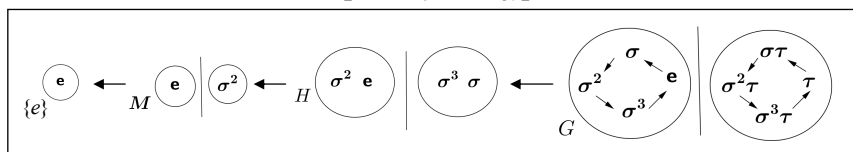
g :「中線に関する折り返し」, h :「対角線 $x_2 x_4$ に関する折り返し」, τ :「対角線 $x_1 x_3$ に関する折り返し」
となる. そして $h \circ g = \sigma$ とおくと「なす角が 45° の 2 直線に関する折り返しの合成は 90° の回転」
だから, σ は 90° の回転を表す. 故に K を $f(x)$ の分解体とすると,

$$G(K/Q) = \langle g, h, \tau \rangle = \langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_4 \text{ (正方形の2面体群)}$$

ここで $H = \{e, \sigma, \sigma^2, \sigma^3\}$, $M = \{e, \sigma^2\}$ とおくと, $G \triangleright H \triangleright M \triangleright \{e\}$

$\#(G/H) = \#(H/M) = \#(M) = 2$ なので, Galois群の位数 $\#(G) = 2^3 = 8$

【Galois群の分解】



[$x^2 = 6$ と $x^2 = 3 \pm \sqrt{6}$ による拡大]

解の間に特別な関係のあるときは, 既約複2次式のGalois群は C_4 や V_4 になる.

例8. (複2次式: $\sqrt{\text{定数項}}$ が有理数のとき) $f(x) = x^4 - 10x^2 + 1$ の Galois 群

$t^2 - 10t + 1 = 0$ の 2 解は $u = 5 + 2\sqrt{6} = (\sqrt{3} + \sqrt{2})^2$, $v = 5 - 2\sqrt{6} = (\sqrt{3} - \sqrt{2})^2$.

故に $f(x) = 0$ の解は $x_1 = \sqrt{3} + \sqrt{2}$, $x_3 = -(\sqrt{3} + \sqrt{2})$, $x_2 = \sqrt{3} - \sqrt{2}$, $x_4 = -(\sqrt{3} - \sqrt{2})$

ところが $x_1 x_2 = 1 \in Q$ だから, 同型写像の(独立な)生成元は

τ :「 $x^2 = 6$ の 2 解の取替え」, σ :「 $x^2 = 5 + 2\sqrt{6}$ の 2 解の取替え($x_1 \leftrightarrow x_3$)」
の 2 種類に減る. ところが $x_2 = 1/x_1$ だから, σ は x_2 と x_4 も入れ替える.

よって, 正方形 $x_1 x_2 x_3 x_4$ に関する置換で表すと,

τ :「中線 l に関する折り返し」, σ :「中心に関する対称移動 (π の回転)」

となる. そして $\tau\sigma(=\sigma\tau)$ は「中線 m に関する折り返し」となるので

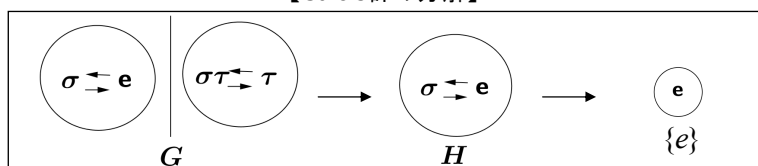
$\sigma^2 = \tau^2 = (\sigma\tau)^2 = (\tau\sigma)^2 = e$ が成り立つ. ゆえに ガロア 群は,

$$G(K/Q) = \langle \sigma, \tau, \sigma\tau \rangle = \{e, \sigma, \tau, \sigma\tau\} \cong V_4 (\text{クラインの4元群}) \cong C_2 \times C_2$$

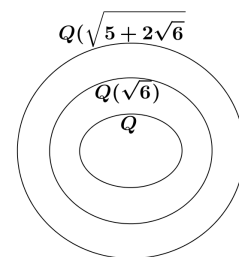
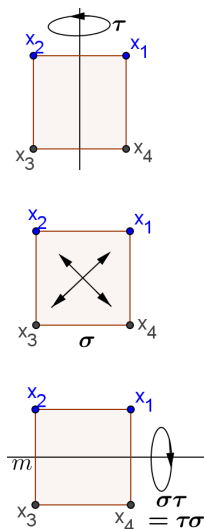
ここで $H = \{e, \sigma\}$ とおくと $G = H + \tau H$, $G \supset H \supset \{e\}$, $\#(G/H) = \#(H) = 2$

であるから, 解は $\sqrt{\dots\sqrt{\dots}}$ の形になる. ($f(x)$ の $\sqrt{\text{定数項}}$ が有理数なら同様.)

【Galois 群の分解】



(他の例; $f_1: x^4 - 4x^2 + 2 = 0$, $f_2: x^4 + 8x + 12 = 0$ とすると $G(f_1) \cong C_4$, $G(f_2) \cong A_4$)



[$x^2 = 6$ と $x^2 = 5 + 2\sqrt{6}$ による拡大]

1796年3月30日の朝 目覚めた時、19歳のGauss は 正17角形の作図が可能な事を発見した。

例9 (円分多項式) $f(x) = x^{16} + x^{15} + x^{14} + \cdots + x^3 + x^2 + x + 1$

$\zeta = \cos(\pi/17) + i \sin(\pi/17)$, $x_k = \zeta^k$ ($k=1,2,\dots,16$) とすると

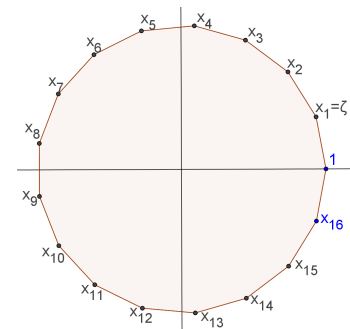
$f(x)=0$ の解は $x_1, x_2, \dots, x_{16}$. ここで $\sigma(\zeta) = \zeta^3$ と定めると,

σ は $K=Q(\zeta)$ の同型写像で, σ は次の様に x_k を移す.

$$\zeta \rightarrow \zeta^3 \rightarrow \zeta^9 \rightarrow \zeta^{10} \rightarrow \zeta^{13} \rightarrow \zeta^5 \rightarrow \zeta^{15} \rightarrow \zeta^{11} \rightarrow$$

$$\zeta^{16} \rightarrow \zeta^{14} \rightarrow \zeta^8 \rightarrow \zeta^7 \rightarrow \zeta^4 \rightarrow \zeta^{12} \rightarrow \zeta^2 \rightarrow \zeta^6 \rightarrow \zeta \quad (\rightarrow \zeta)$$

$\sigma^{16} = e$ だから $G \equiv G(K/Q) = \{e, \sigma, \sigma^2, \sigma^3, \dots, \sigma^{16}\} = C_{16}$ (16次の巡回群)



ここで $H = \{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}, \sigma^{12}, \sigma^{14}\}$, $M = \{e, \sigma^4, \sigma^8, \sigma^{12}\}$, $N = \{e, \sigma^8\}$ とすると,

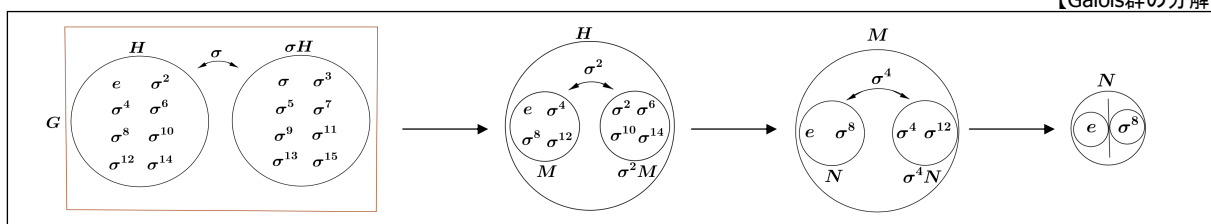
$G \triangleright H \triangleright M \triangleright N \triangleright \{e\}$. $\#(G/H) = \#(H/M) = \#(M/N) = \#(N) = 2$

よって $f(x)=0$ は平方根を 4 回取ることによって解ける. 故に 正17角形は作図できる.

$$\left(\cos \frac{2\pi}{17} = 116 \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{\sqrt{68 + 12\sqrt{17}} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}} \right) \right)$$

$$\cos \frac{\pi}{17} = \sqrt{\left(1 + \cos \frac{2\pi}{17} \right) / 2} \quad \text{だから, 上の式のさらに平方根をとった式になる.}$$

【Galois群の分解】



§ 3. Magma (<http://magma.maths.usyd.edu.au/>)

【参考文献】

1. [初心者のためのMagma](#), 2. [An introduction to algebraic algebra](#), 3. homepage>documentations, 4. Google

【コマンドの例(ごくごく一部)】

- | | |
|--|--|
| 1. Galois群の計算
例: <code>P<x>:=PolynomialAlgebra(Rationals());</code>
<code>//PolynomialRing も大丈夫</code>
<code>f:=x^3-3*x+1;</code>
<code>G:=GaloisGroup(f); G;</code> | 11. 分解体 <code>SplittingField(f)</code> |
| 2. 組成列 (分解できる組成列が正規列)
<code>CompositionSeries(G)</code> | 12. 円分体 <code>CyclotomicPolynomial(n)</code> , <code>CyclotomicField(n)</code> |
| 3. 可解群か? <code>IsSoluble(G)</code> | 13. 解を求める <code>Roots(f)</code> , <code>Roots(f,F)</code> (Fは体) |
| 4. 剰余群 <code>CosetAction(G,H)</code> | 14. 因数分解 <code>Factorization(f)</code> |
| 5. 対称群, 交代群 <code>Sym(n)</code> , <code>Alt(n)</code>
二面体群 <code>DihedralGroup(n)</code>
巡回群 <code>CyclicGroup(n)</code>
置換群 (例: Klein4元群. 自分で定義するしかない?)
<code>PermutationGroup<4 (1,2)(3,4),(1,3)(2,4)></code> | 15. 既約か? <code>IsIrreducible(f)</code> //trueなら同型写像も |
| 6. 部分群, 正規部分群
例: <code>sub<G (1, 4, 2, 5, 3), (2, 5)(3, 4)></code>
<code>//Gの部分群. 右側は生成元(Generators)</code>
<code>IsSubfield(G,H);</code> または <code>H in G;</code>
<code>NormalSubgroups(G); IsNormal(G,H);</code> | 16. 環 <code>Rationals()</code> , <code>IntegerRing()</code> , <code>PolynomialRing()</code> , |
| 7. 直積 <code>DirectProduct(X,Y)</code> | 17. 体 <code>RationalField()</code> , <code>RealField()</code> , <code>ComplexField()</code> ,
<code>NumberField()</code> , <code>FiniteField()</code> |
| 8. 商群(G/N) <code>quo<G N></code> | 18. $\mathbb{Z}_n$ <code>Integers(n)</code> |
| 9. イデアル 例: <code>ideal<P x^2+1>;</code> | 19. 部分体 <code>Subfields(G)</code> |
| 10. Galois閉包(normal closure)
<code>ncl<G H></code> , H^G , H^u (uに共役なHの要素の集合) | 20. 体の拡大
例: $x^2+x+1=0$ の解によるQの拡大
<code>[a] E<x>:=ext<RationalField() t^2+t+1>;</code>
<code>K<y>:=PolynomialAlgebra(E)</code>
<code>[b] P<x>:=PolynomialAlgebra(Rationals());</code>
<code>F<t>:=NumberField(x^2+x+1)</code> |
| | 21. 固定体 <code>FixedField(G,H)</code> |
| | 22. 固定群 <code>FixedGroup(G,F)</code> |
| | 23. 型変換(coercion) <code>A!x</code> (xをタイプAに変換)
例 「 <code>Integers(12) ! 57</code> 」は 9 |
| | 24. $A=B?$, $A \neq B?$ <code>A eq B</code> , <code>A neq B</code> ($A=B$ は使えない) |
| | 25. $A < B$, $A > B$, $A \leq B$, $A \geq B?$ <code>A lt B</code> , <code>A gt</code> , <code>A le B</code> , <code>A ge B</code> |
| | 25. Range, Set <code>[1..n]</code> , <code>{1,2,3}</code> |
| | 26. 関数定義 例: <code>f:=func<x,y x^2+y^2>;</code> |
| | 27. for文 例: list 表示 <code>for g in G; do g (body); end for;</code> |
| | 28. If文 例: <code>if a gt b then a^2; end if;</code> (else も使える) |

「ガロア理論」の参考文献

- 伴 克馬「ガロア理論の世界観」(「現代思想」2008年11月号)
- 小林 吹代「ガロア理論'超'入門」(技術評論社)
- 小島 寛之「天才ガロアの発想力」(技術評論社)
- 草場 公邦「ガロワと方程式」(朝倉書店)
- 石井俊全「ガロア理論の頂を踏む」(ベレ出版)
- 高木貞治「代数学講義」(共立出版)
- 彌永 昌吉「ガロアの時代 ガロアの数学〈第2部〉」(シュプリンガー)

【注】Magmaに関しては、日本語の本はまだ出ていない。

Pdf では小冊子「[初心者のためのMagma](#)」(13p) がある。

英語の本は amazon では1冊ある。

英語のPdf は、Magmaの「homepage>Documentations」と辿ると、

HandBook(膨大, 辞書), First steps in Magma (短い, 12p)

Solving problems with Magma(中級者向け) の3つがある。

他には「[An introduction to algebraic algebra with magma](#)」

(初級者向け) があり、この第4章と第19章を主に参考にした。