4次方程式と5次以上の方程式の Galois 理論

Galois 生誕 200 年記念 数学科リレー講座 6 日目

担当: 網谷 泰治　2011 年 8 月 27 日 (土)

まわるまわるよ　時代はまわる
別れと出逢いをくり返し
今日は倒れた旅人たちも　生まれ変って歩き出すよ

中島みゆき　『時代』

1　Galois 理論とは？

Galois 理論では, 何が分かるのか。最初に説明します。

以下, 有理数のなす集合を $\mathbb{Q}$ と表します。係数が有理数の n 次方程式 (以下, 代数方程式とよぶ) の根になる数, 言い換えると

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0, \quad a_1, \ldots, a_n : \text{有理数}$$

の根になる数を **代数的数** とよびます。代数的数の全体を $\overline{\mathbb{Q}}$ で表します。有理数 q は方程式 $x - q = 0$ の根ですから, 次の包含関係が成り立ちます。

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \text{ (任意の有理数は, 代数的数)}$$

代数的数といっても, 他にどのようなものがあるのか, 方程式だけを眺めていても分かってきません。いくつか例を挙げてみましょう。

例 1　(代数的数の例)

(a) $\sqrt{2}$, $\sqrt{-1}$ は代数的数となる。

というのは, $\sqrt{2}$ と $\sqrt{-1}$ はそれぞれ方程式

$$x^2 - 2 = 0, \qquad x^2 + 1 = 0$$

の根となるからですね。

(b) $\sqrt{2} + \sqrt{-1}$ も代数的数となる。

各自で理由を考えてみましょう。
(ヒント：$x - \sqrt{2} = \sqrt{-1}$ と変形し, 両辺を平方してみよう。係数を有理数にするため, 同様の操作をさらに繰り返す。)

$\mathbb{Q}$ および $\overline{\mathbb{Q}}$ では, $+, -, \times, \div$ の操作を行っても, また同じ集合の数を定めます。その集合内で四則演算を自由に行える (数学用語では四則演算で「閉じている」といいます), そのような性質をもつ集合を **体**[1] (たい) とよびます。

さて, べき乗根の記号 $\sqrt[m]{\ }$ を何回か有理数と組み合わせて四則演算を行う。そうして得られる数全体を S とおきます。

例えば, S の数 (元) としては,

$$\frac{\sqrt[3]{2}+1}{2}, \quad 3\sqrt{2+\sqrt{2}} - \sqrt{-3}\sqrt[3]{2}$$

などがあります。このような数の集合 S は定義より四則演算で閉じているから, 体となります。すると,

$$\mathbb{Q} \subset S \subset \overline{\mathbb{Q}}$$

[1] $\overline{\mathbb{Q}}$ が体となることは, 自明でなく, それ自体ひとつの定理です。証明を割愛しますが, 知りたい人は [1] pp.21–23 を参照して下さい。

であることが分かりますが, ここで私が皆さんに伝えたいと願う, Galois 理論の帰結となることは次です。

Galois 理論から導かれること

$S \neq \overline{\mathbb{Q}}$, すなわち「有理数とべき乗根では決して表されることのない数を根にもつ代数方程式が存在する！」

実は, このことを最初に証明したのはノルウェーの数学者 Abel (1802–1829) です。方程式の次数が 4 以下の場合は, 任意の根は有理数とべき乗根で表せます。Abel が証明したことは「有理数とべき乗根で表せない数を根にもつ 5 次方程式が存在する」ということでした。このことは, 5 次方程式の根の公式が存在しないことと全く同じことです。しかし, Abel の方法では, どのような方程式の根が, 有理数とべき乗根で表せるかという点がはっきりしないのです。

Galois (1811–1832) の仕事はこの点をクリアにしたといえると私は考えます。それまで知られていた根の置換のアイデアを利用しつつ「正規部分群」という新しい概念を導入して, 方程式の根が有理数とべき乗根で表せるための必要十分条件を発見したのです。

おおまかにいって, 代数方程式がなぜ「解ける」のか, そして原理的にはどのように「解ける」のかということを説明できる理論が「Galois 理論」なのです。

「Galois 理論から導かれること」に, 実感がなかなか湧いてこない人もいるかも知れません。脱線は覚悟のうえで, 別の表現の仕方を試みたく思います。

代数的数を宇宙空間に存在する星と想像してみましょう。また, べき乗根と四則演算を使って代数方程式を解くという操作を, 望遠鏡を使って宇宙空間の星を望むことと喩えてみましょう。Galois 理論の結論として分かることは, どんな望遠鏡を使ったとしても決して見つけることのできない星が存在するということなのです。それは, 望遠鏡をいろいろ変えても期待の星が見つけられなかったからその星は存在しない, ということではありません。数学的な秩序に従って考察すると, 決して見えない星が存在していなくてはならないということが分かる, これが Galois 理論の結論なのです。

見ることのできない星を, 理論を通して認識することができる。Galois 理論の奥深さを感じます。

本講義のねらい

- 代数方程式が「解ける」ということは, どのように定式化されるかを理解しよう
- 「4 次方程式は, なぜ解けるのか」を理解しよう
- 「一般的な 5 次以上の方程式には, 根の公式が なぜ存在しないか」を理解しよう

2　代数方程式の Galois 群

Galois 群を説明するための例として, 3 次方程式

$$X^3 + aX + b = 0, \qquad a, b\text{: 有理数}$$

を取り上げます[2]。その 3 つの根を x_1, x_2, x_3 としましょう。3 つの根の置換 σ を考えます。たとえば, x_1, x_2, x_3 をそれぞれ x_2, x_3, x_1 に対応させる置換 σ は

$$\sigma = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

と表すことにします。真中のように根をいちいち書くのは煩わしいため, 右辺のように添字を移動させると考えます。置換 σ は 1, 2, 3 を下に記した 2, 3, 1 にそれぞれ移す規則を定めています。したがって, 関数のように考えて, 以下のように記します。

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 1$$

2 つの置換 σ, τ に対して, 「積 $\sigma \circ \tau$」を考えることができます。この積を次のように定めます。$1 \leq k \leq 3$ とするとき,

$$\begin{aligned}(\sigma \circ \tau)(k) &= \sigma(\tau(k)) \\ &= (k\,\text{を}\tau\text{で移動した値}\tau(k)\,\text{を, 更に}\sigma\text{で移動した値})\end{aligned}$$

こうして定めた積に関して, 3 次の置換全体は「群」を成します。この群を 3 **次対称群** といい, 記号で S_3 と表します。つまり,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ p & q & r \end{pmatrix} \;\middle|\; p, q, r \text{ は } 1, 2, 3 \text{ の並べ替え} \right\}$$

[2]本稿では, 3 次方程式は X^2 の項のないものと仮定します。実際には, 任意の 3 次方程式は $\mathbb{Q}$ の範囲でこの形に変形できますから, 根の置換を考える場合, 一般性は失われないのです。

さて, 3 次方程式の Galois 群の定義をしよう。

定義 1 (Galois 群)

3 次方程式 $F(X) = 0$ の根を x_1, x_2, x_3 とする。次の条件①と②が同値となるとき, S_3 の部分群 G は 3 次方程式 $F(X) = 0$ の **Galois 群** であるという。

① 分数式 $q(x_1, x_2, x_3)$ の 値 が有理数であること。

② G の任意の置換 σ を施しても 式の値は変化しない こと,
数式で言い換えると, 任意の $\sigma \in G$ に対して

$$q(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = q(x_1, x_2, x_3)$$

であること。

【補足】

- n 次方程式の Galois 群も同様に, 根を x_1, x_2, x_3 から $x_1, \ldots, x_n$ に, S_3 を S_n に取り替えて定められます。
- x, y, z の分数式とは,

$$\frac{(x, y, z \text{ の整式})}{(x, y, z \text{ の整式})}$$

で表される式を指します。整式 $(x + 2y - z$ など) も分数式に含めます。

- $q(x_1, x_2, x_3)$ は式として考えているのではなく, 分数式 $q(x, y, z)$ に $x = x_1,\ y = x_2,\ z = x_3$ を代入して得られる値を表します。

Galois 群の性質

- Galois 群の元 σ は有理数を変化させない。

  つまり, $k \in \mathbb{Q}$ について　$k \overset{\sigma}{\mapsto} k$　となる。

- 根の間には, σ によって入れ替えが生じる。

  つまり, 根 x_i $(1 \leq i \leq 3)$ について　$x_i \overset{\sigma}{\mapsto} x_{\sigma(i)}$　となる。

自己同型群と Galois 群

S_3 の部分群として定義された Galois 群と, 体上の自己同型群で定義された Galois 群 (より正確には, $\mathbb{Q}$ 上における $\mathbb{Q}(x_1, x_2, x_3)$ の自己同型群) は以下の通り同一視できます。

置換 $\sigma \in G$ に $\mathbb{Q}$ 上の自己同型 $f_\sigma \in \mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3)/\mathbb{Q})$ を以下のように対応させます。

$p(x, y, z)$, $q(x, y, z)$ をそれぞれ有理数係数の整式とするとき,

$$f_\sigma\left(\frac{q(x_1, x_2, x_3)}{p(x_1, x_2, x_3)}\right) = \frac{q(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})}{p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})}$$

と定義すると, σ によって自己同型 f_σ が得られます。

逆に, 自己同型 f を与えると x_1, x_2, x_3 の根の置換 (つまり, G の元) が 1 通りに定まります。よって, 群の同型

$$G \cong \mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3)/\mathbb{Q})$$

が得られるため, この意味で両辺の群は同じと考えてよいのです。

例２　(Galois 群の決定)

差積 $\Delta(x_1, x_2, x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$ の２乗を３次方程式の **判別式** (discriminant) といい, D と表します。D の値は３次方程式 $X^3 + aX + b = 0$ の係数を使って計算できます。実際には, 次のように計算されます。(意欲的な人は計算してみよう。解と係数の関係を使います。)

$$D = -4a^3 - 27b^2$$

さて, 分数式 $q(x_1, x_2, x_3)$ として差積をえらぶと考えてみましょう。a, b の値が与えられた具体的な状況で差積の値を計算した結果, もし有理数でなければ, Galois 群の定義から差積の値を変化させる置換が存在するわけですね。この原理を用いて, Galois 群を求めてみよう。

例として $X^3 + 2 = 0$ の Galois 群を求めてみましょう。
係数をみると $a = 0,\ b = 2$ となるから,　$D = -108$　です。
ゆえに,　$\Delta(x_1, x_2, x_3) = \pm 6\sqrt{-3}$　で, 差積の値は有理数ではありません。したがって, Galois 群の定義から, G の置換 σ に対応する $\mathbb{Q}$ 上における $\mathbb{Q}(x_1, x_2, x_3)$ の自己同型写像 f_σ のうち

$$f_\sigma(\Delta(x_1, x_2, x_3)) \neq \Delta(x_1, x_2, x_3)$$

をみたすものが必ず存在します。一方, Δ は差積 (交代式) であり, さらに交代群 A_3 の置換は交代式の値を動かさないから, σ は交代群 A_3 の置換ではありえません。ところが, A_3 は S_3 の部分群で S_3 の次に大きいものであるから, Galois 群 G は S_3 と一致しなくてはなりません。ゆえに　$G = S_3$　となります。

3 次方程式の Galois 群について, 一般に次のことが成立する。

定理 1 (3 次方程式の Galois 群の分類)

$\mathbb{Q}$ の範囲で既約な (つまり, 因数分解できないような) 3 次方程式

$$X^3 + aX + b = 0, \qquad a, b \in \mathbb{Q}$$

の Galois 群 G は, 判別式 $D = -4a^3 - 27b^2$ の値によって,
次のように分類される。

① $\Delta = \pm\sqrt{D}$ が有理数 $\quad\Longrightarrow\quad$ $G = A_3 \cong \mathbb{Z}_3$ (3 次巡回群)

② $\Delta = \pm\sqrt{D}$ が有理数でない $\quad\Longrightarrow\quad$ $G = S_3$

【補足】$a_1, \ldots, a_n$ を 変数 とするとき,

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0$$

を **一般代数方程式** という。この方程式の Galois 群は n 次対称群 S_n と等しいことが知られている。証明については [1] pp.105–106 を参照するとよいと思います。

3　体の拡大と Galois 群の縮小

代数方程式が「解ける」ということを, 数学的にきちんと定めておきたい。そこで, ポイントになるのが, 「係数体の拡大」の考え方なのです。

このことを説明するため, “解けた” 方程式と “解けていない” 方程式の 2 つの例を見てみよう。

$$X(X-1)(X+1)=0 \quad \cdots ①, \qquad X(X^2+1)=0 \quad \cdots ②$$

①では, 根は　$(x_1,x_2,x_3)=(0,-1,1)$　となっていて, “解けた” 状態の方程式です。一方, ②は “解けていない”。もう一歩というところですね。“解けた” 状態にするには, さらに因数分解して

$$X(X-i)(X+i)=0 \quad \cdots ②', \quad i=\sqrt{-1}\text{は虚数単位}$$

としなくてはなりません。すると, 根は　$(x_1,x_2,x_3)=(0,-i,i)$
と問題なく求まります。

①と②′ の方程式で「見かけ」上で異なるところは,

- ①の係数はすべて有理数である
- ②′ の係数には有理数ではない $\sqrt{-1}$ が付け加わっている

この点にありますね。係数の範囲が,

$$\mathbb{Q} \subset (\mathbb{Q}\text{の数に}\sqrt{-1}\text{を数として付け加えた集合})$$

と拡大されていることに注意します。実際には, 右側の集合を四則演算について閉ざして, 体としておきます。

こうして出来上がった体を記号で $\mathbb{Q}(\sqrt{-1})$ と表し, $\sqrt{-1}$ を添加した $\mathbb{Q}$ の **拡大体** とよびます。

例３　(拡大体の例)

(1)　$\mathbb{Q}(\sqrt{a})$,　ただし a は有理数

(i) a が有理数の平方ならば,　$\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$

(ii) a が有理数の平方でないならば,

$$\mathbb{Q}(\sqrt{a}) = \{p + q\sqrt{a} \mid p, q \in \mathbb{Q}\}$$

$$(2)\quad \mathbb{Q}(\sqrt[3]{2}) = \left\{ \frac{d + e\sqrt[3]{2} + f\sqrt[3]{4}}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} \;\middle|\; a, b, c, d, e, f \in \mathbb{Q} \right\}$$

実際に拡大体となることを示す方法について, 例を通して考え方を説明します。(1)(ii) のケースで, $\mathbb{Q}(\sqrt{a})$ が $\mathbb{Q}$ の拡大体となる ことを示すと考えてみよう。まず, $\mathbb{Q}$ を部分集合として含んでいることを確かめます。これは, $p+q\sqrt{a}$ の q に 0 を代入すると値は $p \in \mathbb{Q}$ となるから,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{a})$$

となるわけです。また, 四則演算で閉じていることとは,

(a)　和　$(p + q\sqrt{a}) + (r + s\sqrt{a}) = A + B\sqrt{a}$

(b)　差　$(p + q\sqrt{a}) - (r + s\sqrt{a}) = A + B\sqrt{a}$

(c)　積　$(p + q\sqrt{a})(r + s\sqrt{a}) = A + B\sqrt{a}$

(d)　商　$\dfrac{p + q\sqrt{a}}{r + s\sqrt{a}} = A + B\sqrt{a}$

と有理数 A, B を使って表せること。各 (a)–(d) について A, B を p, q, r, s, a で表し, 実際に p, q, r, s, a の分数式となることを確認するのです。チャレンジしてみましょう。

さて, ①と②の方程式の Galois 群の方を見ていきましょう。
それぞれ方程式は,

① $X(X-1)(X+1)=0,$ ② $X(X^2+1)=0$

でしたね。①の根 $(x_1,x_2,x_3)=(0,-1,1)$ はすべて $\mathbb{Q}$ の元です。一方, 方程式の Galois 群の置換は, 根の移動を起こします。ところが, 置換 σ は $\mathbb{Q}$ の元を動かさないため, ①の根も動かしません。

②の方を考えてみます。②の根は $(x_1,x_2,x_3)=(0,-i,i)$ です。$x_1=0$ は $\mathbb{Q}$ の元ですが, $x_2=-i,\ x_3=i$ は体 $\mathbb{Q}$ の外側にはみ出てしまっているわけです。②の方程式の Galois 群の置換は, 0 を動かさないのですが, $\pm i$ については動かすことができるわけです。$\pm i$ を $\pm i$ に対応させる恒等置換と, $\pm i$ を $\mp i$ に対応させる置換との 2 つの置換があります。以上のことを, 次のような図で説明できます。

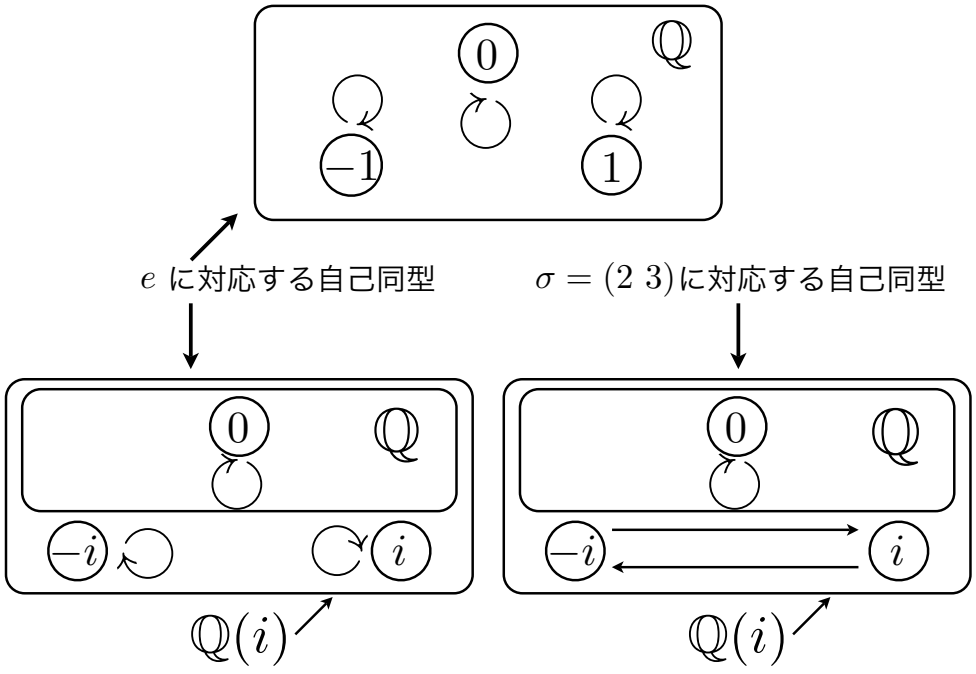

図 1

まとめると,

① $G = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} : S_3\text{の単位元} \right\}$,

② $G = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ (2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

となります。この結果から, “解けた” 方程式の Galois 群は, 恒等置換のみからなる部分群となっていることが分かります。

ここで学んだことを整理しましょう。

$F(X) = 0$ が解けた状態

$\Leftrightarrow$ $\mathbb{Q}$ の範囲で $F(X) = (X - x_1)(X - x_2)(X - x_3)$

$\Leftrightarrow$ $F(X) = 0$ の Galois 群 $G = \{e\}$

実は, このあとの考え方が大事なのです。“解けている” 条件を, 逆に Galois 群の立場から捉え直すという考え方をするのです。
別の言い方をすると,

Galois 群を見ると, その方程式が解けているか, そうでないかが分かる。

このことが単に仮説ではなく, 実際に成り立つように, うまく係数体をコントロールして, Galois 群というものを 定義する のです。標語的な言い方をすると, 方程式の Galois 群は, 解けているかどうかを判定する「リトマス試験紙」のようなものです。

話を具体的にして, 説明します。②を解いたとき, 方程式の形は

$$X(X-i)(X+i)=0$$

となっていますが, これも “解けた状態” として Galois 群の方にその情報を押し込んで考えたい。そこで, $i=\sqrt{-1}$ を $\mathbb{Q}$ に添加した上での Galois 群を新たに定義してやるわけです。

定義 2 (拡大体上の Galois 群)

3 次方程式 $F(X)=0$ の根を x_1, x_2, x_3 とする。次の条件①と②が同値となるとき, S_3 の部分群 G' は 3 次方程式 $F(X)=0$ の $\mathbb{Q}(i)$ **上の Galois 群** であるという。

① $\mathbb{Q}(i)$ の数を係数とする分数式 $q(x_1, x_2, x_3)$ の値は $\mathbb{Q}(i)$ の数であること。

② G' の任意の置換 σ を施しても 式の値は変化しない こと, 数式で言い換えると, 任意の $\sigma \in G$ に対して

$$q(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = q(x_1, x_2, x_3)$$

であること。

従来考えてきた有理数係数の代数方程式の Galois 群を

$\mathbb{Q}$ 上での方程式の Galois 群

とよぶことにし, $\mathbb{Q}(i)$ 上でのそれと区別します。

すると, $\pm i$ を $\mp i$ に対応させる置換は, $\mathbb{Q}$ 上での Galois 群の置換ではありますが, i を固定しないから $\mathbb{Q}(i)$ 上の Galois 群の置換ではなくなります。よって, 次が成り立ちます。

$\textcircled{2}'$の $\mathbb{Q}(i)$ 上の Galois 群は $G' = \{e\}$

大切なことは, 方程式を解く際,

係数の拡大体をとること $\longleftrightarrow$ Galois 群を縮小すること

の両方の操作が対応していることです。

それでは, いよいよ可解性の定義を説明します。方程式を解くことは, 有理数とべき乗根をいくつか組み合わせて, 方程式の根を表すということですね。また, べき乗根で表すということは, べき乗根を「添加する」ということ。方程式を解くということを数学的に定式化すると, 次のようになります。

定義 3 (方程式の可解性)

有理数係数の n 次方程式 $F(X)=0$ の n 個の根を, 重複しているものを含めて, $x_1, x_2, \ldots, x_n \in \mathbb{C}$ とおく。方程式が次の性質 $(*)$ をもつとき, $F(X)=0$ は **開べきで解ける** という。

性質 $(*)$

m を自然数とし, 任意の $1 \leq j \leq m$ について

$$K_j = K_{j-1}(\sqrt[\ell_j]{a_j})$$

をみたすような体の拡大列 (記号 $(\star)$ と表す)

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_{m-1} \subset K_m = \mathbb{Q}(x_1, \ldots, x_n)$$

が少なくとも 1 つ存在する。ここで ℓ_j は自然数で, a_j は K_{j-1} の数のうち, K_{j-1} の数の ℓ_j 乗とはならないものとする。

【解説】　数学では, 定義の意味をはっきりと理解することが欠かせないのです。そこに巧妙なアイデアが隠されていることがあるからです。以下, 3 点に絞って説明します。

- 実際には, $K_0 = \mathbb{Q}$ に　ある数を添加したものを考えます。その添加する数とは, 体の拡大 $K_0 \subset K_m$ の拡大次数を N とするとき, $X^N = 1$ の **原始根** (すなわち, N 乗して初めて 1 となる根)ζ です。

まず, 添加してよい理由は次の通りです。

(a) 「ζ は有理数の開べきを繰り返して表すことができる」, ここで定義した意味で「$F(X) = X^N - 1 = 0$ は開べきで解ける」ことが別口できちんと証明されます。

(b) 中間の拡大に現れる 1 の原始根の「べき数」は N を割り切ることが分かっているため, 最初の時点で ζ を添加しておけば, 中間の拡大に現れる原始根を表すことができます。

「$F(X) = X^N - 1 = 0$ は開べきで解ける」という定理は Gauss によるものです。付録 A を参照のこと。

次に, 原始根 ζ を添加する必要性は何でしょうか。実は, ζ を添加することで,

$$\mathrm{Aut}(K_j/K_{j-1}) \text{ が巡回群}$$

となるのです。後述する Galois の定理の条件で現れますが, 拡大体の列と部分群の列をうまくフィットさせることができるわけです。このために, 原始根を添加する必要があるのです。

- $K_0 = \mathbb{Q}(\zeta)$ とします。a_j を K_{j-1} の数のべき乗では表せないとなぜ仮定するのか, その意味を解説します。これは, つまり「ムダ」を省くことなのです。

  もし $a_j = k^{\ell_j}$ $(k \in K_{j-1})$ と表されるならば, $X^{\ell_j} - a_j = 0$ の根は, $X^{\ell_j} = 1$ の原始根 ζ_j を用いて

$$k,\ k\zeta_j,\ k\zeta_j^2, \ldots,\ k\zeta_j^{\ell_j - 1}$$

と表されます。K_{j-1} には, あらかじめ k, ζ が含まれており, ζ_j は

ζ のべき乗で表せるので

$$K_{j-1}(\sqrt[\ell_j]{a_j}) = K_{j-1}(k, \zeta_j) = K_{j-1}(k, \zeta) = K_{j-1}$$

となってしまい, もとに戻ってしまいます。

ですから, $K_{j-1} \neq K_j$ を導くための仮定が, 「a_j は K_{j-1} のべきでは表せない」ということなのです。

- m と n が等しいことは仮定しません。$m \neq n$ の場合も確かに存在します。付録 A の例題にある方程式がその例になっています。確認してみて下さい。

体の拡大列を Galois 群の部分群の列に置き換えることで, 方程式の可解性を群の言葉で表せるのです。これこそが Galois 理論のエッセンスです！

可解条件 (Galois の定理)

代数方程式 $F(X)=0$ を考える。方程式 $F(X)=0$ が開べきで解けるためには, Galois 群 G の部分群の列

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m \quad \cdots\cdots (\star\star)$$

で, 次の3つの条件をみたすものが存在することが必要十分である:

(1) $G_m = \{e\}$

(2) G_j は G_{j-1} の正規部分群

(3) 商群 G_{j-1}/G_j は巡回群

さらに, 群 G_{j-1} $(1 \leq j \leq m)$ は $F(X)=0$ の K_{j-1} 上の Galois 群である。逆に, K_{j-1} は G_{j-1} の置換で動かないような数の集合 (固定体) と一致する。この意味で, 拡大体の列 $(\star)$ と部分群の列 $(\star\star)$ は1対1に対応する。

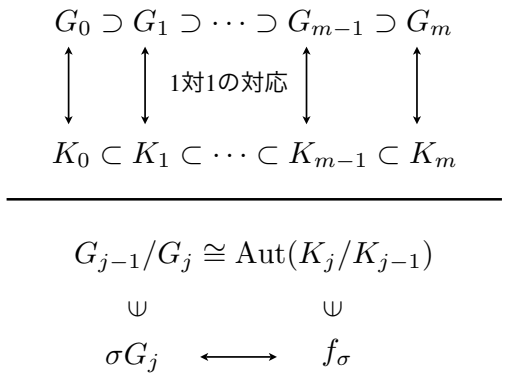

図2

4 節では 4 次方程式の解法を紹介し, この Galois の定理を通して, 一般 4 次方程式はなぜ開べきで解けるのかを解説します。また, 4 次方程式の解法は, S_4 の正規部分群の列および $\mathbb{Q}$ の拡大列を用いて, どのように解釈できるのか, を見ていくことにします。

5 節では 5 次以上の一般代数方程式はなぜ開べきで解けないのか, その理由を Galois の定理に帰着させることにより, 理解してみましょう。仮定する知識は付録 B に載せてありますから, 細かなことはひとまず置いておくことにして, とにかく前進する心意気で臨みましょう。

4　4 次方程式

$a, b, c \in \mathbb{Q}$ とし, 3 次の項のない 4 次方程式を考えます。

$$F(X) = X^4 + aX^2 + bX + c = 0 \quad \cdots\cdots (*)$$

任意の 4 次方程式は, $\mathbb{Q}$ の範囲で X^3 の項のない方程式に変形できます。

実際に　$X^4 + \alpha X^3 + \beta X^2 + \gamma X + \delta = 0 \ \ (\alpha, \beta, \gamma, \delta \in \mathbb{Q})$　が与えられたとき, 変数変換

$$X = Y - \frac{\alpha}{4}$$

を考え, この式を左辺に代入すると, Y の 4 次方程式が得られます。計算すると, Y^3 の項が消えますね。また, 係数は有理数です。

4.1　4 次方程式の解法のスケッチ

方針: 4 次式を 2 次式の積に因数分解できるよう係数を定める。

$$\begin{aligned} X^4 + aX^2 + bX + c &= (X^2 + kX + \ell)(X^2 - kX + m) \\ &= X^4 + (\ell + m - k^2)X^2 + k(m - \ell)X + \ell m \end{aligned}$$

これが X の恒等式であると見なして, k, ℓ, m の値を定めます。
各係数を比較して,

$$a = \ell + m - k^2, \qquad b = k(m - \ell), \qquad c = \ell m$$

初めの 2 つを, m, ℓ について解くと,

$$2m = k^2 + a + \frac{b}{k}, \qquad\qquad 2\ell = k^2 + a - \frac{b}{k}$$

3 つ目の式 $c = \ell m$ に代入して整理すると,

$$k^6 + 2ak^4 + (a^2 - 4c)k^2 - b^2 = 0$$

そこで, $s = k^2$ とおくと, この方程式は s の 3 次方程式となるから, Cardano の公式により s が求まります。ゆえに, k, ℓ, m の値が求まることになります。この値をもとの因数分解の式に代入して, 2 つの 2 次方程式を解けばよいのです。すると, 方程式 $(*)$: $X^4+aX^2+bX+c=0$ の根が求められます。

4.2 Klein の 4 元群

Galois の定理を用いて, 4 次方程式が開べきで解けることを群の立場から眺めてみたい。

そのために準備しておくものは, **Klein の 4 元群** です。これは, 4 次対称群 S_4 の部分群で,

$$V_4 = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

と表されます。ここで, $(1\ 2)(3\ 4)$ は互換の積を表します。具体的に書き表すと,

$$(1\ 2)(3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

実は, 次のことが成り立ちます。

V_4 は 4 次交代群 A_4 の正規部分群

この事実は, 各自で確かめてみてください。正規部分群についてのよい練習問題です。

3 節で紹介した Galois の定理では, S_4 の正規部分群と $\mathbb{Q}$ の拡大体とが 1 対 1 に対応することを紹介したわけですが, Klein の 4 元群 V_4 に対応する $\mathbb{Q}$ の拡大体を求めてみましょう。

そのために, V_4 の置換で動かしても, 不変な数を見つけ出します。というのは, 求める拡大体は V_4 の **固定体**, すなわち

$$\mathbb{Q}(x_1, x_2, x_3, x_4)^{V_4} = \{s \mid f_\sigma(s) = s\} \quad \subset \mathbb{Q}(x_1, x_2, x_3, x_4)$$

であり, 固定体を得るために添加するべき数は V_4 の置換で不変であるからです。ここで, $\mathbb{Q}$ 上既約な 4 次方程式 $F(X) = 0$ の 4 根を, x_1, x_2, x_3, x_4 とおきました。

さて, V_4 の置換のタイプを睨んで,

$q_1 = (x_1+x_2)(x_3+x_4), q_2 = (x_1+x_3)(x_2+x_4), q_3 = (x_1+x_4)(x_2+x_3)$

とおきましょう。特筆すべきは, 次の性質です。

q_1, q_2, q_3 は $G(X) = X^3 - 2aX^2 + (a^2 - 4c)X + b^2 = 0$ の根

この性質は「4 次方程式の根の公式」のところで利用しますが, 「4 次方程式がどのように開べきで解けるか」を説明する上で重要です。性質を認めて, 前に進むことにしましょう。

さて, q_1, q_2, q_3 のすべてを不変にする置換は, S_4 において

(q_1を不変にする置換)$\cap$(q_2を不変にする置換)$\cap$(q_3を不変にする置換)

と表せることに注意します。このことから, 各 q_i $(1 \leq i \leq 3)$ を別々に考えて, 各式の値を不変にする置換を考えればよいことになりますね。

4 次の置換 σ のうち, 値 $q_1 = (x_1 + x_2)(x_3 + x_4)$ を不変にするものは, 次の 5 タイプのいずれかです。

① V_4 の任意の置換, ② $(1\ 2)$, ③ $(3\ 4)$,

④ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, ⑤ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

気になる人は置換を作用させて, 式 q_1 の値が動かないことを確かめてみましょう。また, 簡単に確かめられますが, 置換②–⑤はいずれも奇

置換です。同様に, 置換 σ で q_2 を不変にするもの, q_3 を不変にするものは, それぞれ V_4 の任意の置換と他 4 つの奇置換からなります。そのとき, 奇置換は合計で 12 個出てきますが, それらは相異なることが実際に確かめられます。

よって, $F(X)=0$ の $\mathbb{Q}$ 上の Galois 群が S_4 である事実から,

$$\text{置換}\sigma\text{は}\, q_1, q_2, q_3\text{を不変にする} \quad \Leftrightarrow \quad \sigma \in V_4$$

が分かります。それゆえに q_1, q_2, q_3 を添加した体 $\mathbb{Q}(q_1, q_2, q_3)$ 上では, $F(X)=0$ の Galois 群は V_4 であることがこうして導けたわけです。

4.3 4 次方程式が解ける理由

一般 4 次方程式 $F(X)=0$ の Galois 群は

$$\mathrm{Aut}(\mathbb{Q}(x_1, x_2, x_3, x_4)/\mathbb{Q}) \cong S_4$$

となります。ここで, 各 x_i $(1 \leq i \leq 4)$ を $F(X)=0$ の根とします。S_4 の正規部分群の列

$$S_4 \supset A_4 \supset V_4 \supset U \supset \{e\}$$

をとりましょう。ここで, e は S_4 の単位元を表し, U は V_4 の中の 2 つの置換からなる正規部分群を表します。U の選び方は, 3 通りあります:

$$U_1 = \{e,\ (1\ 2)(3\ 4)\},\ U_2 = \{e,\ (1\ 3)(2\ 4)\},\ U_3 = \{e,\ (1\ 4)(2\ 3)\}$$

以下の事実を, $U = U_1$ として説明します。他の 2 ケースも同様ですから, 興味ある人はフォローしてみましょう。

S_4 の正規部分群の列は, Galois の定理の可解条件 (1)–(3) をすべてみたす。

この事実を全部説明することはしませんが, (3) の成立 (つまり商群が巡回群であること) のみチェックしておきます。問題の商群は,

$$S_4/A_4 = \{eA_4,\ (1\ 2)A_4\},$$

$$A_4/V_4 = \{eV_4,\ (1\ 2)(1\ 3)V_4,\ (1\ 3)(1\ 2)V_4\},$$

$$V_4/U_1 = \{eU_1,\ (1\ 3)(2\ 4)U_1\}$$

ですね。ここでは, A_4/V_4 が巡回的となることだけチェックしよう。

$\sigma = (1\ 2)(1\ 3)V_4$ とします。巡回置換ですが,

$$(a\ b\ c) = \begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix} \quad \longleftarrow \quad 4\text{次の置換に注意}$$

と略記します。

$$\begin{aligned}
\sigma^2 &= (1\ 2)(1\ 3)(1\ 2)(1\ 3)V_4 \\
&= (2\ 1\ 3)(2\ 1\ 3)V_4 \quad \longleftarrow \quad (1\ 2)(1\ 3)\text{ を計算} \\
&= (1\ 2\ 3)V_4 \quad \longleftarrow \quad (2\ 1\ 3)(2\ 1\ 3)\text{ を計算} \\
&= (1\ 3)(1\ 2)V_4
\end{aligned}$$

$$\begin{aligned}
\sigma^3 &= \sigma^2\sigma \\
&= (1\ 3)(1\ 2)(1\ 2)(1\ 3)V_4 \\
&= (1\ 3)(1\ 3)V_4 \\
&= eV_4
\end{aligned}$$

となり, σ 以外の A_4/V_4 の元が現れるため, A_4/V_4 は巡回群となることが分かります。残りの 2 つの群も巡回群となることがチェックできます。(興味ある人はこの確認を各自で行ってください。) したがって, Galois の定理から方程式 $F(X) = 0$ は開べきで解けることが分かるのです。

4.4 添加する数

さて, 正規部分群の列に対応する拡大体の列を考えましょう。

$$\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset \mathbb{Q}(x_1, x_2, x_3, x_4)$$

各体を拡大するとき, 添加する数を一体どのように選べばよいのでしょうか？
少々込み入った話になってきますが, 順に考えていきましょう。

まず, K_1 は $\mathbb{Q}$ に, どの数を添加したものか, を考えます。添加する数は, S_4 の置換では変化するが, A_4 の置換では変化しない数ですね。方程式の差積 $\Delta = \pm\sqrt{D}$ について,

$$\sigma\Delta = \Delta \quad \Longleftrightarrow \quad \sigma \in A_4 \quad \text{(偶置換は差積の値を固定)}$$

が成り立っているから, $K_1 = \mathbb{Q}(\sqrt{D})$ ですね。

第2に, K_2 は K_1 にどのような数を添加して得られるかを考えます。$K_2 = \mathbb{Q}(q_1, q_2, q_3)$ であることを4.2節で説明しました。これを $K_1(\star)$ の形で表してみましょう。そのためには, K_1 上の Galois 群 A_4 の置換では変化するが, V_4 の置換では変化しない数を見つけて, 添加すればよいわけです。実際,

$$A_4\text{の置換 } \sigma \text{ は } q_1\text{を不変にする} \quad \Longleftrightarrow \quad \sigma \in V_4$$

となるから, $K_2 = K_1(q_1)$ が分かります。

第3に, K_3 を $K_2(\star)$ の形で表してみます。U の選び方は3通りありましたから, U の選び方で K_3 が変わります。場合分けして考察しましょう。

$U = U_1$ の場合, 置換 $\sigma = (1\ 2)(3\ 4)$ で不変だが, V_4 のどれかの置換で値が変化するような数を K_2 に添加すると K_3 が得られます。そのような数は, $x_1 + x_2$ であるから, $\quad K_3 = K_2(x_1 + x_2)$ $\quad$ です。

$U = U_2, U_3$ の場合も, 同様に

$$K_3 = K_2(x_1 + x_3), \quad K_3 = K_2(x_1 + x_4)$$

となることが示されるのです。

4.5 4 次方程式の根の公式

4 節で学んだことの集大成として, 4 次方程式

$$F(X) = X^4 + aX^2 + bX + c = 0, \quad a, b, c : \text{有理数}$$

の根の公式を導いてみましょう。

まず, 根を x_1, x_2, x_3, x_4 とすると,

$$\begin{aligned} F(X) &= (X - x_1)(X - x_2)(X - x_3)(X - x_4) \\ &= X^4 - (x_1 + x_2 + x_3 + x_4)X^3 + \cdots + x_1x_2x_3x_4 \end{aligned}$$

と展開されるから, 解と係数の関係から

$$X^3\text{の係数}: (x_1 + x_2) + (x_3 + x_4) = 0$$

となります。一方, q_1 の定義から

$$(x_1 + x_2)(x_3 + x_4) = q_1$$

よって, 添字を適切に取り替えて

$$x_1 + x_2 = \sqrt{-q_1}, \quad x_3 + x_4 = -\sqrt{-q_1}$$

とできる。同様にして,

$$x_1 + x_3 = \sqrt{-q_2}, \quad x_2 + x_4 = -\sqrt{-q_2}$$

$$x_1 + x_4 = \sqrt{-q_3}, \quad x_2 + x_3 = -\sqrt{-q_3}$$

q_1, q_2, q_3 を与えられた定数と考え, $x_1, \ldots, x_4$ についての 1 次方程式とみて, これらを解くと, 4 次方程式の根の公式が導かれます。

$$(*) \begin{cases} x_1 &= (\sqrt{-q_1} + \sqrt{-q_2} + \sqrt{-q_3})/2 \\ x_2 &= (\sqrt{-q_1} - \sqrt{-q_2} - \sqrt{-q_3})/2 \\ x_3 &= (-\sqrt{-q_1} + \sqrt{-q_2} - \sqrt{-q_3})/2 \\ x_4 &= (-\sqrt{-q_1} - \sqrt{-q_2} + \sqrt{-q_3})/2 \end{cases}$$

q_1, q_2, q_3 は, 3 次方程式 $G(X) = 0$ の根ですから, 4 次方程式は平方根と立方根を積み重ねて解けていることが分かります。4.4 節で考察したことを踏まえて, もう少し精密に観察してみよう。

- 拡大 $\mathbb{Q} \subset K_1$ では $\sqrt{D}$ を添加したため, 平方根を 1 回とり,
- 拡大 $K_1 \subset K_2$ では 3 次方程式の根 q_1 を添加したため,
  立方根を 1 回とり,
- 拡大 $K_2 \subset K_3$ では, 平方根を 1 回とっていることが分かります。

解く手順をまとめておきます。

① $G(X) = X^3 - 2aX^2 + (a^2 - 4c)X + b^2 = 0$ を,
Cardano の公式を使って解く。

② ①の根が q_1, q_2, q_3 となる。これらを $(*)$ に代入すると,
4 根 $x_1, \ldots, x_4$ が得られる。

最後にクイズを出して, 4 次方程式の節を終えたく思います。図 3 は S_4 の恒等置換 e に対応した恒等変換を表しています。S_4 の置換の個数は全部で $4! = 24$ あります。それでは, 図 3 を 23 枚分作って, 残りの 23 個の置換に対応する自己同型写像を書き入れてみて下さい。

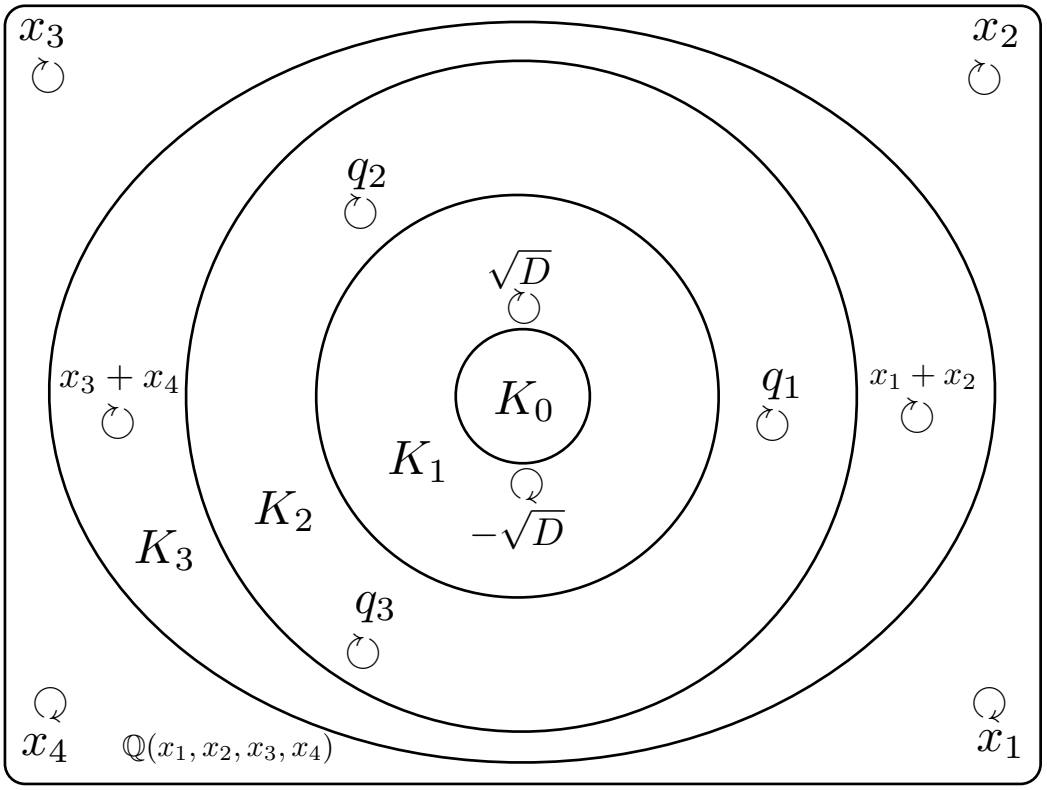

図 3

5　5 次以上の代数方程式

5 次以上の代数方程式の根の公式が存在しないことを, Galois の定理を用いて群論的な視点から示します。

Galois の定理の可解条件 (1)–(3) をみたすような群 G を **可解群** とよぶことにします。次の性質が成り立ちます。

可解群の性質

N を可解群 G の部分群とすると, N も再び可解群となる。

この性質を認めることにして, 次の定理を証明します。まずは分からなくても通読してみましょう。分からないところは, あとでフォローしてみましょう。

Abel–Galois の定理

$n \geq 5$ のとき, 一般 n 次代数方程式は開べきでは解けない。

【証明】　まず, 5 次の場合を考察し, その結果を用いて 5 次以上の場合を証明します。

① $n = 5$ のとき, 背理法で示す。一般 5 次方程式 $F(X) = 0$ が開べきで解けたと仮定する。その方程式の Galois 群は S_5 であるが, Galois の定理から S_5 は可解群でなければならない。よって, 上の性質より部分群 A_5 もまた可解群となる。

一方, 定理 4(付録 B) から A_5 より真に小さい正規部分群は $\{e\}$ のみである。すると, A_5 は可解となるため, 正規部分群の列

$$A_5 \supset \{e\}$$

は可解条件の (3) をみたさなくてはならない。したがって, 商群

$$A_5/\{e\} = A_5$$

が巡回群でなければならない。しかし, これは不合理である。というのは, 仮に A_5 が巡回群であったならば, A_5 の各置換は σ^m の形で表され, それゆえ

$$\sigma^i\sigma^j = \sigma^m = \sigma^j\sigma^i \quad (i+j=m,\ i\geq 0,\ j\geq 0)$$

となるから A_5 の各置換は積の順序を入れ替えても計算の結果として得られる置換自体は変化しないはずである。ところが, 次の A_4 の置換

$$\sigma_1 = (1\ 3)(1\ 2), \quad \sigma_2 = (1\ 5)(1\ 4)$$

をとると,

$$\begin{aligned}
\sigma_1\sigma_2 &= (1\ 3)(1\ 2)(1\ 5)(1\ 4) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \\
\sigma_2\sigma_1 &= (1\ 5)(1\ 4)(1\ 3)(1\ 2) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}
\end{aligned}$$

となって, $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$ となってしまい矛盾を生じてしまう。ゆえに, 可解条件の (3) がみたされないことになり, A_5, したがって S_5 は可解群でない。以上より, 一般 5 次方程式は開べきで解けない。

② $n \geq 6$ とする。一般 n 次方程式 $F(X) = 0$ の Galois 群は S_n である。n 次の置換のうち, $(n-5)$ 文字 $(6, 7, \ldots, n)$ を固定するようなもの全体は S_5 と見なせ, これは S_n の部分群をなす。仮に S_n が可解群であったとすると, 性質から S_5 も可解群。これは, ①で証明した結果に反してしまう。よって, S_n は可解群ではないことが分かったから, 一般 n 次方程式 $F(X) = 0$ は開べきで解けない。

①, ②から定理が証明された。 □

【注意】　間違えやすいのですが,「5 次以上の任意の方程式は, 開べきで解けない」というのは正しくありません。5 次以上の方程式でも, 開べきで解けるものはあります。付録 A を参照のこと。

6　1のべき乗根 (付録 A)

この節では, n 次方程式 $X^n-1=0$ が開べきで解けるという, Gauss による定理を紹介します。計算を通して, 雰囲気を掴んでみましょう。

例題 1

$F(X)=X^4+X^3+X^2+X+1=0$ の $\mathbb{Q}$ 上の Galois 群を求めよ。

【解答】　$F(X)$ は, $\mathbb{Q}$ の範囲では既約 (因数分解できない) であり,

$$F(X)=\frac{X^5-1}{X-1}$$

と変形できるから, $F(X)=0$ の 4 根はいずれも 1 の 5 乗根で 1 とは異なります。その 1 つの根は,

$$x_1=\cos\left(\frac{360^\circ}{5}\right)+i\sin\left(\frac{360^\circ}{5}\right)\neq 1$$

となります。根を表すため, 複素数の de Moivre の公式

$$(\cos\theta+i\sin\theta)^m=\cos(m\theta)+i\sin(m\theta),\quad m:\text{整数}$$

を使います。すると,

$$\begin{aligned}x_1^5&=\left(\cos\left(\frac{360^\circ}{5}\right)+i\sin\left(\frac{360^\circ}{5}\right)\right)^5\\&=\cos\left(\frac{360^\circ}{5}\times 5\right)+i\sin\left(\frac{360^\circ}{5}\times 5\right)\\&=1\end{aligned}$$

となり, 確かに x_1 が 1 の 5 乗根となっていることが分かります。

他の 3 根は, $k=2,3,4$ として,

$$x_k=\cos\left(\frac{360^\circ}{5}\times k\right)+i\sin\left(\frac{360^\circ}{5}\times k\right)$$

と表せます。複素数 $a+bi$ を座標 (a,b) に対応させて, 5 つの複素数 $1, x_1, \ldots, x_1^4$ を平面上で表してみよう。これらの根は, 図 4 では正 5 角形の頂点を表しており, x_1 をかけると根が O(極) のまわりに回転している様子が視覚的に捉えられますね。

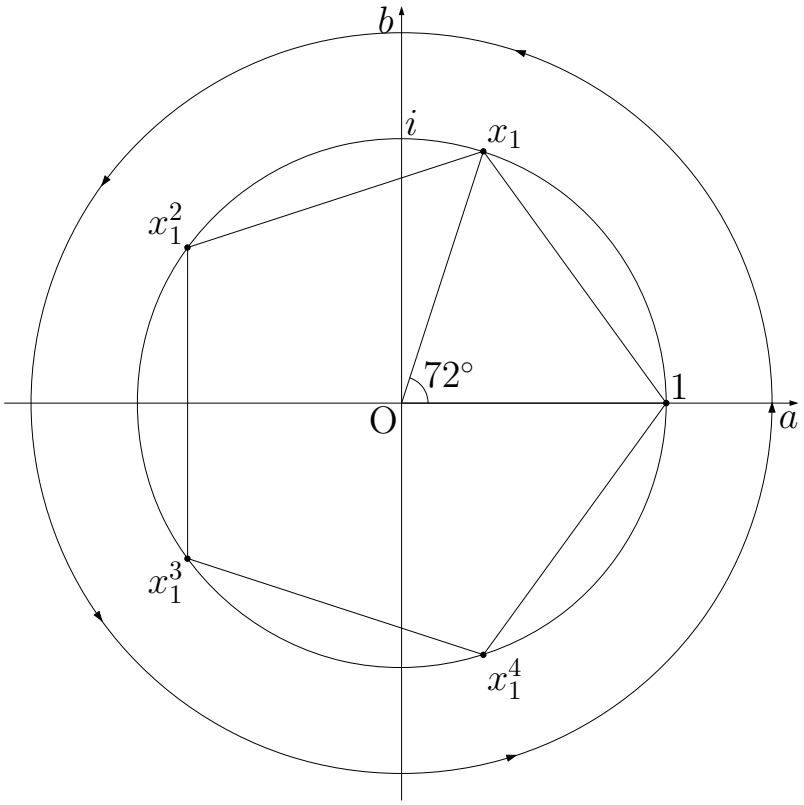

図 4

Galois 群 G を求めよう。4 根の間の関係を見ると,

$$x_2 = x_1^2, \quad x_3 = x_1^3, \quad x_4 = x_1^4 \quad \cdots\cdots (*)$$

となる。4 根の置換を考えたい。a 軸を始線とし極 O となす角を 2 倍する平面変換は, 根の置換を与えます。この置換は

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3)$$

で巡回置換となり, その位数は 4 ですね。

したがって, $\sigma, \sigma^2, \sigma^3, \sigma^4 = e$ は相異なる置換となります。この 4 つの置換は確かに G の置換です。

逆に, G の中の置換のうち, 4 根の間の関係 $(*)$ をみたすものは $e, \sigma, \sigma^2, \sigma^3$ の 4 つに限られます。ゆえに, $G = \{e, \sigma, \sigma^2, \sigma^3\} \cong \mathbb{Z}_4$ $\square$

一般に, 次が成立します。

定理 2

p を素数とする。方程式 $X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 = 0$ の $\mathbb{Q}$ 上の Galois 群を G とすると,

$$G = \{e, \sigma, \sigma^2, \ldots, \sigma^{p-2}\} \cong \mathbb{Z}_{p-1} \quad (p-1) \text{ 次の巡回群}$$

さて, 例題 1 の方程式は「相反方程式」といって, 具体的に根を求める方法を高校数学で学びます。

ここでは, Galois 群を調べることにより, 開べきで解けるプロセスを確認しましょう。例題 1 の Galois 群 G の正規部分群を見てみよう。正規部分群の列は,

$$\{e\} \subset \{e, \sigma^2\} \subset G$$

真中にある位数 2 の部分群を H とする。これが G の正規部分群となることは容易に確かめられます。各自で考えてみてください。

H に対応する拡大体 M は $\mathbb{Q}$ にどんな数を添加したものでしょうか? 体の拡大列は

$$L = \mathbb{Q}(x_1, x_2, x_3, x_4) \supset M \supset \mathbb{Q}$$

ですね。M を作るには, x_1, x_2, x_3, x_4 の分数式となる α のうち, σ^2 で不変な数を添加すればよいのですね。分数式には整式も含まれます。そこで, どのような 1 次式が σ^2 で不変かを調べます。

そのために, a, b, c, d, e を有理数として, 1 次式

$$\alpha = ax_4 + bx_3 + cx_2 + dx_1 + e$$

を考えます。4 根の関係式

$$x_2 = x_1^2, \quad x_3 = x_1^3, \quad x_4 = x_1^4$$

を代入して,

$$\alpha = ax_1^4 + bx_1^3 + cx_1^2 + dx_1 + e$$

を得ます。また,

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3)$$

となるから,

$$\begin{aligned} & f_{\sigma^2}(\alpha) = \alpha \ (\sigma^2 \text{ で } \alpha \text{ は不変}) \\ \Leftrightarrow \quad & ax_1 + bx_1^2 + cx_1^3 + dx_1^4 + e = ax_1^4 + bx_1^3 + cx_1^2 + dx_1 + e \\ \Leftrightarrow \quad & (a-d)x_1^3 + (b-c)x_1^2 + (c-b)x_1 + (d-a) = 0 \end{aligned}$$

方程式 $F(X) = 0$ は $\mathbb{Q}$ 上既約となるため, x_1 は 3 次以下の代数方程式の根となることはない。ゆえに, $a = d,\ b = c$ であり, その結果として

$$\begin{aligned} \alpha &= a(x_1^4 + x_1) + b(x_1^3 + x_1^2) + e \\ &= a\left(\frac{1}{x_1} + x_1\right) + b\left(\frac{1}{x_1^2} + x_1^2\right) + e \end{aligned}$$

が成り立ちます。

さらに, ここで $s = \dfrac{1}{x_1} + x_1$ とおくと,

$$\frac{1}{x_1^2} + x_1^2 = \left(\frac{1}{x_1} + x_1\right)^2 - 2 = s^2 - 2$$

となるから,

$$\alpha = as + b(s^2 - 2) + e$$

をみたすことが分かります。ゆえに, α は s の多項式で表せます。そこで, a, b, e は任意であったから, 特に $a = 1, b = e = 0$ とおいてあげると $\alpha = s$ となります。これが, σ^2 で不変な数となります。

それでは, s の値を具体的に求めよう。方程式 $F(X) = 0$ に $X = x_1$ を代入して, $x_1^2 \neq 0$ で両辺を割ると,

$$x_1^2 + x_1 + 1 + \frac{1}{x_1} + \frac{1}{x_1^2} = 0$$

$$\Leftrightarrow \quad (s^2 - 2) + s + 1 = 0$$

$$\Leftrightarrow \quad s^2 + s - 1 = 0$$

この 2 次方程式を解いて, $s = \dfrac{-1 \pm \sqrt{5}}{2}$ となります。根は明らかに有理数ではありません。ゆえに,

$$M = \mathbb{Q}(s) = \mathbb{Q}(\sqrt{5})$$

また, $\{e\}$ に対応する拡大体が $L = M(\sqrt{-3 - s})$ となることは各自で確かめてみましょう。

以上の計算から, 拡大列は

$$\mathbb{Q} \subset \mathbb{Q}(s) \subset \mathbb{Q}(s, \sqrt{-3 - s})$$

となることが分かります。添加する数を見ると, 4 次方程式

$$F(X) = X^4 + X^3 + X^2 + X + 1 = 0$$

は平方根を 2 回とって解けていることが認められますね。

Gauss (1777–1855) によって, 一般に次が証明されています。

定理 3

n 次方程式 $X^n - 1 = 0$ は, 開べきで解ける。ゆえに, 1 のべき乗根は, 開べきで表せる。

【注意】　Galois 理論は, 5 次以上の方程式が解けないことを示すわけではありません。定理 3 のような特別な形をした方程式は, n の値によらず常に解けることをいっているのです。

7　交代群と正規部分群 (付録 B)

交代群 A_n の性質

(1) A_n は 3 次の巡回置換によって生成される。

(2) S_5 には 20 個の 3 次巡回置換がある。それら 20 個は, すべて A_5 の中にあり共役 (きょうやく) である。

※　共役の定義は【補足】を参照。

【証明】　以下, a, b, c, d は自然数を表す。

(1) 任意の偶置換は偶数個の互換の積で表せる。そこで, 互換 2 個に着目する。2 つの互換に同じ数を含む場合とそうでない場合の 2 タイプがある。それらは,

$$(a\ b)\ (a\ c), \qquad (a\ b)\ (c\ d)$$

であるが両方とも

$$(a\ b)\ (a\ c) = (a\ c\ b),$$

$$(a\ b)\ (c\ d) = (a\ b)\ (b\ c)\ (b\ c)\ (c\ d) = (b\ c\ a)\ (c\ d\ b)$$

となり, 3 次の巡回置換で表せる。ゆえに, A_n は 3 次の巡回置換で生成される。

(2) 異なる 5 つのものから 3 つをとって並べる並べ方は,

${}_5\mathrm{P}_3 = 5 \cdot 4 \cdot 3 = 60$ 通りある。

一方, 1 つの 3 次巡回置換に対しては,

$$(a\ b\ c) = (b\ c\ a) = (c\ a\ b)$$

のように 3 通りの表記がある。ゆえに, S_5 には $60/3 = 20$ 個の 3 次巡回置換がある。

次は共役であることを示そう。そのためには, 任意の 2 つの 3 次巡回置換 σ, τ に対して,

$$\tau = \rho\sigma\rho^{-1}, \quad \text{すなわち} \quad \tau\rho = \rho\sigma \quad \cdots\cdots (*)$$

をみたす置換 ρ がとれることをいえばよい。

$\sigma = (1\ 2\ 3)$, $\tau = (a\ b\ c)$ とおくと,

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

とすればよい。$(*)$ をみたすことは各自で計算して確かめよ。□

【補足】　置換群 G の中の置換 x を固定します。ある置換 $g \in G$ によって,

$$y = gxg^{-1} \quad \cdots\cdots (\star)$$

と表される置換 y を x の **共役** な置換といいます。$(\star)$ の両辺に g を右からかけることで, x と共役な置換とは

$$gx = yg$$

となるような置換yとも言い換えられますね。

なお, 置換群Gの部分群Nが次の性質をみたすとき, このNをGの**正規部分群**であるといいます。

(性質)　任意の$\sigma \in H$および任意の$\tau \in G$に対して　$\tau\sigma\tau^{-1} \in H$

例 4　n次交代群A_nはn次対称群S_nの正規部分群である。

上の性質に基づいて, 各自で証明してみましょう。

定理 4

5次交代群 A_5 の正規部分群は, $\{e\}$ と A_5 のみである。

【証明】　$N \neq \{e\}$ であるような正規部分群を考える。$N = A_5$を示せばよい。Nの中の置換σは5次の偶置換であるから, σを互換で表したとき, その個数を$0, 2, 4$とできる。個数が0の場合は$\sigma = e$となり, 2の場合は適切に数字を取り替えて,

$$\sigma = (1\ 3)(1\ 2), \quad (1\ 2)(3\ 4)$$

としてよい。同様に個数が4の場合,

$$\sigma = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$$

としてよい。証明のアイデアはNの中に3次巡回置換を1つ作ることである。

(a) $\sigma = (1\ 3)(1\ 2)$ のときを考える。$\sigma = (1\ 2\ 3)$であり, この巡回置換と残りのA_5の19個の3次巡回置換はA_5においてすべて共役。したがって, NはA_5の正規部分群ゆえ, すべての3次巡回置換を含む。また, 一方で交代群は3次巡回置換全体で生成されるから, $N = A_5$となる。

(b) $\sigma = (1\ 2)(3\ 4)$ のとき, $\tau = (1\ 2)(3\ 5)$ とすれば, τ は A_5 の中にあるから,

$$\tau\sigma\tau^{-1} = (1\ 2)(4\ 5)$$

は N の中にある。ゆえに,

$$(\tau\sigma\tau^{-1})\sigma = (4\ 5)(3\ 4) = (4\ 3\ 5)$$

となり, 3 次巡回置換は N の中にある。(a) と同じ理由により, すべての 3 次巡回置換は N の中にある。よって, $N = A_5$ となる。

(c) $\sigma = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$ のときは, 同様に $N = A_5$ がいえる。このことは, 各自で確かめてください。

以上, (a)–(c) のいずれのケースにおいても $N = A_5$ となったから, 題意が示された。 □

参考文献

[1] 足立恒雄, 『ガロア理論講義』, 日本評論社, 1996 年.

[2] 倉田令二朗, 『ガロアを読む—第 I 論文研究』, 日本評論社, 1987 年.

[3] 中村亨, 『ガロアの群論』, 講談社, 2010 年.

[4] 藤崎源二郎, 『体とガロア理論』, 岩波書店, 1991 年.

[1] は, 私が大学生の時分に代数学の講義で学んだテキストで, 明快な語り口の著者を彷彿させます。概念の導入の意義をすっきりと解説している好著であると思います。本稿の執筆に際しても導入の部分や定理の証明の部分をベースにしています。

[2] では, 古典的な意味での代数方程式のガロア群が紹介されています。ガロア理論のテキストは数多く出版されていますが, 体上の自己同型群の立場で記述されているものがほとんどです。本書は n 次対称群の部分群として定義してあり, 本稿ではその記述の部分で参考にしました。

[3] は, 近年出版された一般向けの書物です。著者によると朝日カルチャーセンターの講座で内容を紹介したとのこと。そのためか, 必然的に難解な概念は出てきますがレベルを下げることなく分かり易く書かれており, 非常に読みやすい感がありました。説明の方法の部分で参考にした。ガロア理論の内容をもっと知りたいと願う人には薦めたい 1 冊です。

[4] は, ガロア理論を学ぶ人のための本格的な専門書です。大部で, 非常に丁寧に書かれております。また, 豊富に具体例を載せるなど, 理解するための配慮が随所になされております。本稿を執筆する際, 例を含めて細々とした調べものをすることがあり, その点で本書を参考にしました。はっきりしないところなどは, この本で調べると大抵解決すると思います。しかし, 数学独特の公理的な叙述法に慣れること, さらに基本的な代数学の知識を備えておくことができないと, 自分で調べて内容を理解することは難しいかも知れません。