数学の魅力をイメージする

方程式のガロア群

（その具体的な計算法）

松田 修

2023 年 10 月 5 日

はじめに

本書は，ガロア理論のストーリー（１９世紀のフランスの少年が作った理論）の続本である．したがって，前本に扱われた群や体に関するある程度の知識は仮定している．

さて，今や高校数学においては，微分積分の基礎的なことは当たり前のように扱われ，多くの高校生たちは，微分積分に関するさまざまな計算ができる．

しかし，たとえば，微分の逆操作が定積分に関係するという微分積分学の基本定理や，三角関数の正確な定義を理解しようとすると，$\varepsilon - \delta$ 論法といったものなどが必要になり，それらを理解することはそれほど簡単なことではない．

それでも，微分積分の内容を直感的にある程度認めていけば，微分積分の基本的な計算や応用問題に取り組むことができる．

本書は，ガロア理論の知識を直感的にある程度認め，与えられた方程式のガロア群が判定できるようになることを目的とする．ガロア群が判定できるようになると，少しガロア理論がわかったような気になり，うれしいと感じるからである．

最後に，津山高専の学生の白神百花さんと加藤夏帆さんは，本書を丁寧に読んでくださり，いくつかの誤植を指摘してくださいました．また，第 10 章では，稲垣佑都さんの卒業研究から得られた研究結果を紹介させていただきました．みなさまに，心から感謝いたします．

目次

第 1 章

方程式の最小分解体の拡大次数

$\mathbb{Q}$ 係数の n 次方程式

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_{n-1} x + a_n = 0$$

を考える．このとき，解 $x_1,\ x_2, \cdots, x_n$ を含んだ $\mathbb{Q}$ の拡大体の中で，拡大次数が最小であるものを n 次式方程式の**最小分解体**という．

この章では，方程式が与えられたとき，その最小分解体の拡大次数をどのように求めればよいかについて説明する．

$\mathbb{Q}$ 係数の 3 次方程式

$$x^3 - 2x^2 - 3x + 6 = 0 \tag{1.1}$$

を考える．そして，この方程式の最小分解体 M の $\mathbb{Q}$ 上の拡大次数を求めよう．

まず，この方程式の左辺は，$\mathbb{Q}$ 上で

$$x^3 - 2x^2 - 3x + 6 = (x-2)(x^2-3)$$

と因数分解できる．したがって，$x_1 = 2$ は (1.1) の解である．明らかに x_1 の最小多項式は $x - 2$ であり，x_1 は $\mathbb{Q}$ の元であるため，$\mathbb{Q}$ に x_1 を添加した体 $\mathbb{Q}(x_1)$ は $\mathbb{Q}$ で

ある．すなわち，

$$\mathbb{Q}(x_1) = \mathbb{Q}(2) = \mathbb{Q}$$

である．

次に，2 次式 $x^2 - 3$ を考える．この 2 つの解を x_2 と x_3 とする．このとき，$x_2 = \sqrt{3},\ x_3 = -\sqrt{3}$ であることは明らかであるが，今後のことを考えて，このことは知らないものとしておこう．

$\mathbb{Q}$ に x_2 を添加した体 $\mathbb{Q}(x_2)$ を考え，$\mathbb{Q}(x_2)$ 上で 2 次式 $x^2 - 3$ を $x - x_2$ で割ると，商が $x + x_2$，余りが $x_2^2 - 3 = 0$ となり，したがって $x^2 - 3$ は

$$x^2 - 3 = (x - x_2)(x + x_2)$$

と因数分解される．これより，

$$x_3 = -x_2$$

であり，x_3 は $\mathbb{Q}(x_2)$ の元であることがわかる．

以上のことから，$\mathbb{Q}(x_2)$ は (1.1) の最小分解体 M であり，$\mathbb{Q}(x_2)$ の最小多項式は 2 次式であるため，M の $\mathbb{Q}$ 上の拡大次数 $[M : \mathbb{Q}]$ は

$$[M : \mathbb{Q}] = [\mathbb{Q}(x_2) : \mathbb{Q}] = 2$$

となる．

K 上共役の定義

K を体，x と y を K 上代数的な元，すなわち，どちらもある K 係数の代数方程式の解であるとする．さらに，x と y の最小多項式が一致しているとき，すなわち，x も y も K の元でなく $K(x) = K(y)$ であるとき，x と y は K 上**共役**であるという．

上の議論において，x_2 と x_3 の $\mathbb{Q}$ 上の最小多項式は一致していた．したがって，x_2 と x_3 は $\mathbb{Q}$ 上**共役**である．

一般に，K 係数の 2 次方程式の 2 つの解は，K 上共役である．

今度は，$\mathbb{Q}$ 係数の 4 次方程式

$$x^4 + 2 = 0 \tag{1.2}$$

を考える．そして，この方程式の最小分解体 M の $\mathbb{Q}$ 上の拡大次数を求めよう．

この方程式 (1.2) の 4 つの解は全て $\mathbb{Q}$ の元ではない．そこで，x_1 を (1.2) のある解とする．そして $\mathbb{Q}$ に x_1 を添加した体 $\mathbb{Q}(x_1)$ を考え，$\mathbb{Q}(x_1)$ 上で 4 次式 $x^4 + 2$ を因数分解すると，

$$x^4 + 2 = (x - x_1)(x^3 + x_1x^2 + x_1^2x + x_1^3) = (x - x_1)(x + x_1)(x^2 + x_1^2)$$

となる．x_1 の最小多項式は 4 次式であるので，

$$[\mathbb{Q}(x_1) : \mathbb{Q}] = [\mathbb{Q}(x_2) : \mathbb{Q}] = 4$$

となる．このとき，(1.2) の解 $x_2 = -x_1$ は $\mathbb{Q}(x_1)$ であるので，x_1 と x_2 は $\mathbb{Q}$ 上共役である．

続いて，$K = \mathbb{Q}(x_1)$ 係数の 2 次方程式

$$x^2 + x_1^2 = 0 \tag{1.3}$$

の解を x_3，x_4 とする．x_3 と x_4 は K 上共役であるので，$K(x_3) = K(x_4)$ であり，

$$[K(x_3) : K] = [K(x_4) : K] = 2$$

である．

$\mathbb{Q}$ から最小分解体 M までの拡大次数を求めるために，以下の公式が証明されている．

定理（拡大次数の公式）　M を $\mathbb{Q}$ 係数の最小分解体，K を $\mathbb{Q} \subset K \subset M$ なる体（**中間体**という）とする．このとき，

$$[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}]$$

が成り立つ．

定理（拡大次数の公式）から，方程式 (1.2) の最小分解体を M とすると，$M = K(x_3)$ であり

$$[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}] = 2 \times 4 = 8$$

となる．

Memorize：方程式の最小分解体の拡大次数

$\mathbb{Q}$ 係数の 4 次方程式 $x^4 + 2 = 0$ のある解を x_1 とすると，$\mathbb{Q}$ 上 x_1 と共役な解 x_2 が存在し，$K = \mathbb{Q}(x_1)$ と置くと $[K : \mathbb{Q}] = 4$ となる．さらに，解 x_3 と x_4 に対して $K(x_3) = K(x_4)$，そして $[K(x_3) : K] = 2$ である．したがって，$x^4 + 2 = 0$ の最小分解体 M について $[M : \mathbb{Q}] = [K(x_3) : K][k : \mathbb{Q}] = 8$ となる．

問題 1. $\mathbb{Q}$ 係数の方程式 $x^4+x+1=0$ を考える．以下の問いに答えよ．

(1) $x^4+x+1=0$ の 1 つの解を x_1 とする．このとき，$K=\mathbb{Q}(x_1)$ 上で方程式の左辺は

$$x^4+x+1=(x-x_1)(x^3+x_1x^2+x_1^2x+x_1^3+1)$$

と因数分解されることを示せ．

(2) $x^4+x+1=0$ の x_1 とは異なる解を x_2 する．このとき，$K(x_2)$ 上で

$$x^3+x_1x^2+x_1^2x+x_1^3x+1=(x-x_2)\{x^2+(x_1+x_2)x+x_1^2+x_1x_2+x_2^2\}$$

と因数分解されることを示せ．

(3) $x^4+x+1=0$ の最小分解体を M とするとき，$[M:\mathbb{Q}]$ を求めよ．

問題 2. 以下の $\mathbb{Q}$ 係数の方程式の最小分解体を M とするとき，$[M:\mathbb{Q}]$ を，それぞれ求めよ．

(1) $x^4+9=0$

(2) $x^5-2x^3+3x^2-6=0$

(3) $x^6+x^4+3x^3+2x+2=0$

第 2 章

方程式のガロア群の位数

$\mathbb{Q}$ 係数の n 次方程式

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_{n-1} x + a_n = 0$$

は，$\mathbb{Q}$ 上に解を持つとき $\mathbb{Q}$ 上**可約**であるといい，そうでないとき $\mathbb{Q}$ 上**既約**であるという．そして，既約である n 次方程式の最小分解体を M とする．このとき，M の $\mathbb{Q}$ 自己同型写像全体に対応する n 次対称群 S_n の部分群 G のことを，n **次方程式のガロア群**，または単に**方程式の群**という．

この章では，可能性のある方程式のガロア群の位数を説明する．

群の定義を復習する．

群の定義　演算が定義された集合 G は，任意の $x, y, z \in G$ について以下の条件をみたすとき**群**と呼ばれる．

（条件 1）結合法則 $(xy)z = x(yz)$ が成り立つ．

（条件 2）$xe = ex = x$ となる単位元 e が存在する．

（条件 3）$xx^{-1} = x^{-1}x = e$ となる逆元 x^{-1} が存在する．

そして，H が G の部分集合であり，H 自体も群であり，かつ H の単位元は G の単位元でもあるとき，H は G の**部分群**であるといった．方程式のガロア理論で扱うガロア群は有限群である．そして $\sharp G$ で群 G の**位数**（G の元の個数）を表す．次の有用な定理を挙げておく．

定理（ラグランジュの定理）　G を群，H を G の部分群とすると，$\sharp H$ は $\sharp G$ の約数である．

$\mathbb{Q}$ に α を添加した体 $\mathbb{Q}(\alpha)$ について，$\mathbb{Q}(\alpha)$ から自分自身への写像を φ する．$\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 自己同型写像の定義を復習する．

$\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 自己同型写像の定義

α は有理数ではない数とする．φ が $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ **自己同型写像**とは，変換する前の $\mathbb{Q}(\alpha)$ の数と変換した後の $\mathbb{Q}(\alpha)$ の数が 1 対 1 に対応付けるものであって，さらに以下の 2 つの条件を満たすものである．

（条件 1）$\mathbb{Q}(\alpha)$ のどんな数 x, y に対しても

$$(1)\ \ \varphi(x+y)=\varphi(x)+\varphi(y) \qquad (2)\ \ \varphi(xy)=\varphi(x)\varphi(y)$$

（条件 2）$\mathbb{Q}$ の数 u に対しては

$$(3)\ \ \varphi(u)=u$$

“$\mathbb{Q}$ 自己同型写像”をどのように作ればよいのか？ これに対応する回答として，ガロア理論では，以下の重要な定理が証明されている．そしてこの定理は，同時に $\mathbb{Q}$ 係数の n 次方程式のガロア群が定理で示された n 次対称群 S_n の部分群であることを主張している．

定理（$\mathbb{Q}$ 自己同型写像と置換の関係） $\mathbb{Q}$ 係数の n 次方程式の最小分解体を M とする．このとき，M の $\mathbb{Q}$ 自己同型写像について，以下が成り立つ．

(1) M の $\mathbb{Q}$ 自己同型写像の個数は，$[M:\mathbb{Q}]$ に一致する．

(2) M の $\mathbb{Q}$ 同型写像は，n 次方程式の n 個の解の内，$\mathbb{Q}$ の解以外の解同士を変換するものとして定義できる．

(3) M の $\mathbb{Q}$ 自己同型写像は，n 次方程式の解に作用する n 次対称群 S_n のある置換に対応し，それらの置換全体は S_n の部分群である．

ガロア理論の核となる定理を紹介する．その準備として，ガロア群の部分群と最小分解体に含まれる $\mathbb{Q}$ の拡大体に関するいくつかの概念を整理する．

$\mathbb{Q}$ 係数の n 次方程式の最小分解体を M，G をこの方程式のガロア群とする．そして，G の部分群 H に対して，$\mathcal{F}(H)$ を H の全ての元に関して不変な M の元全体とする．このとき，$\mathcal{F}(H)$ は $\mathbb{Q}$ と M の間の中間体となる．また，K を $\mathbb{Q}$ と M の中間体とし，$\mathcal{G}(K)$ を K の全ての元に関して不変な G の元全体とする．このとき，$\mathcal{G}(K)$ は G の部分群となる．そしてガロア群 G の部分群 H と，$\mathbb{Q}$ と M の中間体 $\mathcal{F}(H)$ は，1 対 1 に対応する．逆に，$\mathbb{Q}$ と M の中間体 K とガロア群 G の部分群 $G(K)$ も，1 対 1 に対応する．それが以下の定理である．

定理（ガロア群の部分群と中間体の１対１対応）

$H_1 \subset H_2$ ならば $\mathcal{F}(H_1) \supset \mathcal{F}(H_2)$ であり，$K_1 \subset K_2$ ならば $\mathcal{G}(K_1) \supset \mathcal{G}(K_2)$ が成り立ち，さらに，

$$\mathcal{G}(\mathcal{F}(H)) = H, \quad \mathcal{F}(\mathcal{G}(K)) = K$$

が成り立つ．

以上の準備のもとで，既約な n 次方程式がどのような群となる可能性があるのかを考えていく．

まず，既約な $\mathbb{Q}$ 係数の 3 次方程式

$$x^3 + ax^2 + bx + c = 0 \tag{2.1}$$

のガロア群はどのようなものになるのかを考えよう．

方程式の解を $x_1,\ x_2,\ x_3$ とし，

$$K_1 = \mathbb{Q}(x_1),\quad K_2 = K_1(x_2),\quad M = K_2(x_3)$$

と置く．ここで，M は 3 次方程式の最小分解体で，K_1 と K_2 は $\mathbb{Q}$ と M の間の中間体である．

(I) 一般的場合，体の拡大の拡大次数は，

$$[K_1 : \mathbb{Q}] = 3,\quad [K_2 : K_1] = 2,\quad [M : K_2] = 1$$

である．特に，$M = K_2$ である．したがって，

$$[M : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : K_1] = 6$$

となる．一般的な 3 次方程式のガロア群は S_3 であり，$\sharp S_3 = 3! = 6$ でなので，この場合のガロア群は S_3 といえる．

(II) $L = K_1 = K_2$ となる場合が考えられる．このとき，

$$[L : \mathbb{Q}] = 3$$

であり，体 L において 3 次方程式は

$$(x - x_1)(x - x_2)(x - x_3)$$

と因数分解される．したがって，$M = L$ であり，この場合のガロア群 G の位数は $\sharp G = 3$ となる．

以上のことから，既約な $\mathbb{Q}$ 係数の 3 次方程式のガロア群は S_3 以外には，可能性として $\sharp G = 3$ となるものがあることがわかった．

次に，既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{2.2}$$

のガロア群はどのようなものになるのかを考えよう．

方程式の解を $x_1,\ x_2,\ x_3,\ x_4$ とし，

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

と置く．ここで，M は 4 次方程式の最小分解体である．

(I) 一般的な 4 次方程式のガロア群は S_4 であり，$\sharp S_4 = 4! = 24$ である．

(II) $L = K_2 = K_3,\ L \neq K_1$ となる場合が考えられる．このとき，

$$[K_1 : \mathbb{Q}] = 4$$

であり，体 K_1 において 4 次方程式は

$$(x - x_1)(\,3\text{次式})$$

と因数分解される．そして，

$$[L : K_1] = 3$$

であり，体 L において 4 次方程式は

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)$$

と因数分解される．したがって，$L = M$ である．よって，この場合のガロア群 G の位数は $\sharp G = 4 \times 3 = 12$ となる．

(III) $L = K_1 = K_2,\ L \neq K_3$ となる場合が考えられる．このとき，

$$[L : \mathbb{Q}] = 4$$

であり，体 L において 4 次方程式は

$$(x - x_1)(x - x_2)(\,2\text{次式})$$

と因数分解される．したがって，$K_3 = M$ であり

$$[M : L] = 2$$

となる．よって，この場合のガロア群 G の位数は $\sharp G = 4 \times 2 = 8$ となる．

(IV) $L = K_1 = K_2 = K_3$ となる場合が考えられる．このとき，

$$[L : \mathbb{Q}] = 4$$

であり，体 L において 4 次方程式は

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)$$

と因数分解される．したがって，$L = M$ でありこの場合のガロア群 G の位数は $\sharp G = 4$ となる．

以上のことから，既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群は S_4 以外には，可能性として $\sharp G = 12, 8, 4$ となるものがあることがわかった．

Memorize：4 次方程式のガロア群の位数

既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

のガロア群 G は，方程式の解を $x_1,\ x_2,\ x_3,\ x_4$ とし，

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

を考えると，（1）一般的な場合，（2）$L = K_2 = K_3,\ L \neq K_1$ である場合，（3）$L = K_1 = K_2, L \neq K_3$ である場合，（4）$L = K_1 = K_2 = K_3$ である場合を考えることで，可能性として $\sharp G = 24, 12, 8, 4$ が得られる．

問題 3. 既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5 + ax^4 + bx^3 + cx^2 + dx + f = 0$$

のガロア群 G の可能性のある位数を求めよ.

問題 4. 既約な $\mathbb{Q}$ 係数の 6 次方程式

$$x^6 + ax^5 + bx^4 + cx^3 + dx^2 + fx + g = 0$$

のガロア群 G の可能性のある位数を求めよ.

第 3 章

対称群の基礎知識

対称群 S_n とは，$1, 2, \cdots, n$ である n 個の数字の置換全体の集合であり，その位数は $\sharp S_n = n!$ である．したがって，G が S_n の部分群であれば，G の位数は $n!$ の約数である．

この章では，S_n の部分群に関する基礎知識を説明する．

$\mathbb{Q}$ 係数の n 次方程式のガロア群 G は n 次対称群 S_n の部分群である．そして，前章で述べた定理（$\mathbb{Q}$ 同型写像と置換の関係）の (2) から G は n 次方程式の n 個の解を変換するものである．

一方，G が

$$\begin{gathered}『i \neq j \in \{1, 2, \cdots, n\} \text{ である任意の } i, j \text{ に対して} \\ \sigma(i) = j \text{ となる } \sigma \in G \text{ が存在する}』\end{gathered}$$

という性質をもつとき，G は**推移的**であるという．以下の定理が証明されている．

定理（ガロア群の推移性） 既約な $\mathbb{Q}$ 係数の n 次方程式のガロア群 G は推移的であり，逆に方程式のガロア群 G が推移的ならば，その方程式は既約である．

以下，S_n とその部分群について詳細に説明していく．

$n \geq 2$ の場合 $\sharp S_n$ は偶数なので，S_n の部分群 G で $\sharp G = n!/2$ であるものが存在する可能性がある．

そこで，S_5 の元である置換 $(1\ 4\ 2\ 5)$ を考えると，これは

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

と互換 $(a\ b)$ の積で分解することができる．一般に，S_n の元である置換 $(i_1\ i_2\ \cdots\ i_r)$ は，

$$(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{r-1}\ i_r)$$

というように，互換の積で分解できる．特に，恒等置換 e は $e = (1\ 2)(1\ 2)$ と分解できる．さらに，$(i_1\ i_2\ i_3)$ というタイプの置換は

$$(i_1\ i_2\ i_3) = (i_1\ i_2)(i_2\ i_3)$$

と分解される．

しかし，置換を互換の積で分解する方法は上の方法だけではない．それでも分解の個数は同じであることが証明されている．

定理（S_n の生成元）　$n \geq 2$ のとき n 次対称群 S_n は $(1\ 2),\ (1\ 3),\ \cdots,\ (1\ n)$ という n 個の互換から生成される．すなわち，

$$S_n = \langle (1\ 2),\ (1\ 3),\ \cdots,\ (1\ n) \rangle$$

である．特に S_2 は巡回群である．

置換 σ が偶数個の互換の積で分解されるとき σ を**偶置換**と呼ぶ．特に e は偶置換である．さらに，$(i_1\ i_2\ i_3)$ というタイプの置換も偶置換である．

一方，置換 σ が奇数個の互換の積で分解されるとき σ を**奇置換**と呼ぶ．

S_n の元である置換のうち，偶置換全体は S_n の部分群であることは明らかで，これを n **次交代群**と呼び A_n で表す．$\sharp A_n = n!/2$ である．

定理（A_n の生成元） $n \geq 3$ のとき n 次交代群 A_n は $(1\,2\,3),\ (1\,2\,4),\ \cdots,\ (1\,2\,n)$ という n 個の互換から生成される．すなわち，

$$A_n = \langle (1\ 2\ 3),\ (1\ 2\ 4),\ \cdots,\ (1\ 2\ n) \rangle$$

である．特に A_3 は巡回群である．

S_2 や A_3 は巡回群であったが，一般に巡回群に関する以下の 2 つの定理が証明されている．

定理（位数 p の群） p を素数，G を群，$\sharp G = p$ とする．このとき G は巡回群である．

定理（位数 pq の群） p, q を $p > q$ で $p \not\equiv 1 \pmod{q}$ をみたす素数，G を群，$\sharp G = pq$ とする．このとき G は巡回群である．

さて，3 次対称群 S_3 は，

$$S_3 = \{e,\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

であり，正三角形に作用する群である．ここで，置換 $(1\ 2\ 3)$ と $(1\ 3\ 2)$ は正三角形に回転という作用を与えるもので，置換 $(1\ 2)$ と $(1\ 3)$ と $(2\ 3)$ は鏡映という作用を与えるものである．そして，

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

であることから，$\sigma = (1\ 2\ 3),\ \tau = (1\ 2)$ と置くと

$$S_3 = \langle \sigma,\ \tau \rangle,\quad \sigma^3 = \tau^2 = e,\ \tau\sigma\tau = \sigma^{-1}$$

であることがわかる．

一般に

$$G = \langle \sigma,\ \tau \rangle,\quad \sigma^n = \tau^2 = e,\quad \tau\sigma\tau = \sigma^{-1}$$

を満たす G は，n 次**二面体群**といい，

$$D_n$$

で表す．ただし $n \geq 3$ であり，そして $\sharp D_n = 2n$ である．

したがって，S_3 は 3 次二面体群 D_3 である．さらに，S_3 において

$$N = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle$$

を考えると，N は S_3 の正規部分群である．そして

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

であることから，$H = \langle (1\ 2) \rangle$ と置くと，

$$S_3 = NH,\quad N \cap H = \{e\}$$

であることが分かる．

一般に，以下の定理が証明されている．

定理（二面体群 D_n の構造）　n 次二面体群 $D_n = \langle \sigma,\ \tau \rangle$ を考える．ただし $\sigma^n = \tau^2 = e,\ \tau\sigma\tau = \sigma^{-1}$ とする．このとき，$N = \langle \sigma \rangle$ は D_n の正規部分群であり，さらに $H = \langle \tau \rangle$ とすると，$N \cap H = \{e\}$ であり，$D_n = NH$ が成り立つ．

さて，一般に 2 つの群 G_1 と G_2 に対して，

$$G_1 \times G_2 = \{(x, y) \mid x \in G_1,\ y \in G_2\}$$

を，G_1 と G_2 の**直積**という．このとき，$G_1 \times G_2$ の任意の元 (x_1, y_1), (x_2, y_2) について

$$(x_1, y_1)(x_2, y_2) = (x_1x_2,\ y_1y_2)$$

と定めることで，直積 $G_1 \times G_2$ は群となる．特に単位元は (e_1, e_2) である．明らかに，

$$\sharp(G_1 \times G_2) \leq (\sharp G_1)(\sharp G_2)$$

である．

S_4 の置換 $\sigma = (1\ 2)(3\ 4)$ と $\tau = (1\ 3)(2\ 4)$ に対して，2 つの巡回群

$$H_1 = \langle\sigma\rangle,\quad H_2 = \langle\tau\rangle$$

の直積 $H_1 \times H_2$ を考えよう．

$$\sigma^2 = e,\quad \tau^2 = e$$

であることから，定義に従えば，

$$H_1 \times H_2 = \{(e, e),\ (\sigma, e),\ (e, \tau),\ (\sigma, \tau)\}$$

である．このことから，$\sharp(H_1 \times H_2) = 4$ となる．

一方，S_4 の位数 4 の部分群

$$V_4 = H_1H_2 = \{e,\ \sigma,\ \tau,\ \sigma\tau\}$$

を考える．これは**クラインの四元群**と呼ばれる．明らかに $V_4 \subset A_4$ である．さらに，H_1 と H_2 はどちらも V_4 の正規部分群であること，$H_1 \cap H_2 = \{e\}$ であることも簡単にわかる．そして，V_4 の元とは $H_1 \times H_2$ の元は 1 対 1 に対応しているようにみえる．

定義（同型）　2 つの群 G と G' について, G と G' 間に 1 対 1 の写像 f が存在して，f が以下の条件を満たすとき，G と G' は**同型**であるといい，$G \cong G'$ で表す.

〈条件〉 $\sigma, \tau \in G$ に対して $f(\sigma\tau) = f(\sigma)f(\tau)$

上の条件を満たす写像 f は**準同型写像**と呼ばれている．この写像 f は，G の演算を G' の演算に替える役割をもっている．そして，G と G' が同型とは，G と G' の群としての構造が同じであるということを意味している.

直積に関する群の同型について，以下の定理が証明されている.

定理（２つの正規部分群と直積の関係）　H_1, H_2 を群 G の正規部分群で,

$$G = H_1H_2, \quad H_1 \cap H_2 = \{e\}$$

を満たすものとする．このとき，$G \cong H_1 \times H_2$ が成り立つ.

以上のことを元に，以下では既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{3.1}$$

のガロア群 G について，再考しよう.

改めて，方程式 (3.1) の解を $x_1,\ x_2,\ x_3, x_4$ とし,

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

を考えると,（1）一般的な場合,（2）$L = K_2 = K_3$, $L \neq K_1$ である場合,（3）

$L = K_1 = K_2, L \neq K_3$ である場合，（4）$L = K_1 = K_2 = K_3$ である場合を考えることで，可能性として $\sharp G = 24, 12, 8, 4$ が得られた．

明らかに $\sharp G = 24$ のとき $G = S_4$ であり，$\sharp G = 12$ のとき $G = A_4$ である．

$\sharp G = 8$ のとき，最小分解体 M までの拡大体の様子は，（3）の場合であり，$[L : \mathbb{Q}] = 4$ で $[M : L] = 2$ であった．そして，以下の 3 つのケースを考えることで，G は 4 次二面体群 D_4 であることがわかる．

（ケース 1）$[L : \mathbb{Q}] = 4$ に対応する群が，巡回群 $N = \langle \sigma \rangle$, $\sigma^4 = e$ のとき，$[M : L] = 2$ に対応する群として $H = \langle \tau \rangle$, $\tau^2 = e$ であるため，ガロア群 G は 4 次二面体群 D_4 となる．たとえば，$\sigma = (1\ 2\ 3\ 4)$, $\tau = (1\ 3)$, $D_4 = \langle (1\ 2\ 3\ 4), (1\ 3) \rangle$ がある．

（ケース 2）$[L : \mathbb{Q}] = 4$ に対応する群として，$H_1 = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ であるタイプが考えられる．H_2 を位数 2 の巡回群で，$H_1 \cap H_2 = \{e\}$ を満たすものとして作った直積 $H_1 \times H_2$ は位数 8 である．しかし，

$$H_2 = \langle (1\ 3) \rangle, \langle (1\ 4) \rangle, \langle (2\ 3) \rangle, \langle (2\ 4) \rangle$$

が考えられるが，どの H_2 で $G = H_1 H_2$ を作っても $\sharp G > 8$ となる．

（ケース 3）$[L : \mathbb{Q}] = 4$ に対応する群として，クラインの四元群

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

が考えられる．H を位数 2 の巡回群で，$V_4 \cap H = \{e\}$ を満たすものとして作った直積 $V_4 \times H$ は位数 8 である．しかし，ケース 2 と同じ理由から $\sharp V_4 > 8$ となる．

Memorize：4 次方程式のガロア群のタイプ

既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群 G は，S_4, A_4, D_4, C_4, V_4 のいずれかである．

問題 5. G を既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群で，$\sharp G = 4$ とする．このとき，G は 4 次巡回群 C_4 かクラインの四元群 V_4 であることを証明せよ．

問題 6. 既約な $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + ax^3 + bx^2 + cx + d = 0$ の方程式の解を $x_1,\ x_2,\ x_3,\ x_4$ とし，

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

とする．このとき，次を満たすガロア群は S_4, A_4, D_4, C_4, V_4 のどれか判定せよ．

(1)　$K_1 = K_2,\ K_2 \neq K_3$ である場合

(2)　$K_1 \neq K_2,\ K_2 = K_3$ である場合

第 4 章

判別式 D と交代群 A_n

既約な $\mathbb{Q}$ 係数の n 次方程式のガロア群 G は n 次対称群 S_n の部分群である．この章では，G の種類をどのように見分けることができるかについて説明していく．

$\mathbb{Q}$ 係数の 2 次方程式

$$x^2 + bx + c = 0$$

を考える．この解を x_1, x_2 とすると

$$x_1 + x_2 = -b, \quad x_1 x_2 = c$$

である．一方,

$$x_1 = \frac{-b + \sqrt{b^2 - 4c}}{2}, \quad x_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}$$

なので，$x_1 - x_2 = \sqrt{b^2 - 4c}$ である．したがって,

$$(x_1 - x_2)^2 = b^2 - 4c$$

を得る．$D = b^2 - 4c$ を 2 次方程式の**判別式**という．

定義（判別式 D）　$\mathbb{Q}$ 係数の n 次方程式の解を $x_1,\ x_2,\ \cdots,\ x_n$,

$$\Delta = \prod_{i<j}(x_i - x_j) = (x_1 - x_2)(x_1 - x_3)\cdots(x_{n-1} - x_n)$$

とし，さらに，$D = \Delta^2$ とする．Δ を n 次方程式の解の**差積**，D を n 次方程式の**判別式**という．

3 次方程式

$$x^3 + ax^2 + bx + c = 0 \tag{4.1}$$

の解を $x_1,\ x_2,\ x_3$ とする．

このとき，

$$x_1 + x_2 + x_3 = -a,\quad x_1x_2 + x_2x_3 + x_3x_1 = b,\quad x_1x_2x_3 = -c$$

である．

一方，差積 Δ は

$$\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

である．そして判別式 D を計算すると，以下のようになる．

$$\begin{aligned} D &= (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 \\ &= -4x_1x_2x_3(x_1 + x_2 + x_3)^3 + (x_1 + x_2 + x_3)^2(x_1x_2 + x_2x_3 + x_3x_1)^2 \\ &\quad +18x_1x_2x_3(x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_3x_1) \\ &\quad -4(x_1x_2 + x_2x_3 + x_3x_1) - 27x_1^2x_2^2x_3^2 \end{aligned}$$

したがって，

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \tag{4.2}$$

を得る．

さて，既約な $\mathbb{Q}$ 係数の 3 次方程式のガロア群 G の置換 σ を Δ に作用させることを，

$$\sigma(\Delta)$$

と書くことにする．

たとえば，$\sigma = (1\ 2)$ を Δ に作用させると，x_1 と x_2 が入れ替わり

$$\begin{aligned}\sigma(\Delta) &= (x_2 - x_1)(x_2 - x_3)(x_3 - x_1) = -(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \\ &= -\Delta\end{aligned}$$

となる．

たとえば，$\sigma = (1\ 2)(2\ 3)$ を Δ に作用させると，x_1 は x_2 に，x_2 は x_3 に，x_3 は x_1 と入れ替わるので，

$$\begin{aligned}\sigma(\Delta) &= (x_2 - x_1)(x_3 - x_2)(x_3 - x_1) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \\ &= \Delta\end{aligned}$$

となる．

つまり，$\sigma \in A_3$ なら σ は偶置換なので $\sigma(\Delta) = \Delta$ であり，$\sigma \notin A_3$ なら σ は奇置換なので $\sigma(\Delta) = -\Delta$ である．

したがって，$G = S_3$ のとき，σ はガロア群の元，つまり最小分解体の $\mathbb{Q}$ 自己同型写像の元であることと，$\sigma(\Delta) = \pm\Delta$ であることから $D \in \mathbb{Q}$ であることが分かる．特に，

$$『G = A_3 \text{ ならば } D \in \mathbb{Q}^2』$$

ことがいえる．ここで，$D \in \mathbb{Q}^2$ とは，ある $\eta \in \mathbb{Q}$ によって $D = \eta^2$ と書けることを意味する．以下の定理が証明されている．

定理（判別式 D と交代群 A_n）　G を $\mathbb{Q}$ 係数の n 次方程式のガロア群，D を判別式とする．このとき，$G \subset A_n$ であることの必要十分条件は $D \in \mathbb{Q}^2$ である．

$\mathbb{Q}$ 係数の 3 次方程式

$$x^3 - 3x + 1$$

のガロア群 G を求めてみよう．(4.2) と $a = 0,\ b = -3,\ c = 1$ より

$$D = -4b^3 - 27c^2 = 9^2$$

である．したがって，$G = A_3$ である．

Memorize：3 次方程式の判別式 D

$$D = \Delta^2, \quad \Delta = \prod_{i<j}(x_i - x_j)$$

3 次方程式 $x^3 + ax^2 + bx + c = 0$ の判別式は

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

$D \in \mathbb{Q}^2$ なら 3 次方程式のガロア群は A_3 ある．

問題 7. 以下の $\mathbb{Q}$ 係数の 3 次方程式のガロア群を求めよ．

(1) $x^3 - 6x^2 + 6$　　(2) $x^3 - 6x^2 + 8$

問題 8. 既約な $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + ax^3 + bx^2 + cx + d = 0$ のガロア群 G がクラインの四元群 V_4 であるとき，$D \in \mathbb{Q}^2$ であることを証明せよ．

問題 9. 既約な $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + ax^3 + bx^2 + cx + d = 0$ のガロア群 G が 4 次巡回群 C_4 であるとき，$D \notin \mathbb{Q}^2$ であることを証明せよ．

第 5 章

商群と可解群

方程式のガロア群が可解群であるとき，その方程式はべき根で解ける．これがガロア理論の主張である．可解群は群の割り算から得られる商群を使って定義される．

N を群 G の正規部分群とする．すなわち，任意の $x \in G$ に対して

$$xN = Nx$$

が成り立っているとする．

そこで，$x, y \in G$ について

$$x \sim y \quad \Leftrightarrow \quad xN = yN$$

と定義すると，$\sim$ は同値関係となる．

さらに，$C(x) = xN$ を，x を代表とする**同値類**といい，同値類全体を

$$G/N = \{C(x) \mid x \in G\}$$

と表す．G/N の演算は，

$$C(x)C(y) = C(xy)$$

と定義される．勿論これは $C(x)$ の代表元 x の取り方によらず定義できる（well-difined）．そして，G/N は群となる．特に，単位元は $C(e)$ であり，$C(x)$ の逆元は $C(x^{-1})$ である．

定義（商群）　N を群 G の正規部分群とする．このとき，

$$G/N = \{C(x) \mid x \in G\}$$

を，N による G の**商群**または**剰余群**という．

たとえば，n 次交代群 A_n は n 次対称群 S_n の正規部分群であることは明らかである．したがって，$\sigma \in S_n,\ \sigma \notin A_n$ である σ を用いて，商群

$$S_n/A_n = \{A_n,\ \sigma A_n\}$$

をつくることができる．明らかに $S_n/A_n = \langle \sigma A_n \rangle$ なので，商群 S_n/A_n は 2 次の巡回群である．

一般的な既約な $\mathbb{Q}$ 係数の 3 次方程式のガロア群は S_3 であるが，S_3 の正規部分群は巡回群 $A_3 = \langle (1\ 2\ 3) \rangle$ で，A_3 の正規部分群は $\{e\}$ のみであり，このことから，S_3 の正規部分群

$$S_3 \supset A_3 \supset \{e\}$$

に対して，商群 S_3/A_3 と $A_3/\{e\} = A_3$ が作れて，これらはどちらも巡回群である．既約な $\mathbb{Q}$ 係数の 3 次方程式のガロア群 S_3 は，このような構造をもっているのである．

さて，S_4 の置換 $\sigma = (1\ 2)(3\ 4)$ と $\tau = (1\ 3)(2\ 4)$ に対して，クラインの四元群

$$V_4 = \{e,\ \sigma,\ \tau,\ \sigma\tau\}$$

を考える．ここで，$\sigma\tau = (1\ 4)(2\ 3)$ である．

$\eta \in S_4$ に対して $\eta(i)$ で η による番号 i の置換の番号を表す．たとえば，$\eta = (2\ 4\ 3)$ のとき，

$$\eta(1) = 1,\ \ \eta(2) = 4,\ \ \eta(3) = 2,\ \ \eta(4) = 3$$

である．そして，$\eta^{-1} = (2\ 3\ 4)$ であり

$$\eta\sigma\eta^{-1} = (2\ 4\ 3)(1\ 2)(3\ 4)(2\ 3\ 4) = (1\ 4)(2\ 3) = (\eta(1)\ \eta(2))(\eta(3)\ \eta(4))$$
$$\eta\tau\eta^{-1} = (2\ 4\ 3)(1\ 3)(2\ 4)(2\ 3\ 4) = (1\ 2)(3\ 4) = (\eta(1)\ \eta(3))(\eta(2)\ \eta(4))$$
$$\eta(\sigma\tau)\eta^{-1} = (2\ 4\ 3)(1\ 4)(2\ 3)(2\ 3\ 4) = (1\ 3)(2\ 4) = (\eta(1)\ \eta(4))(\eta(2)\ \eta(3))$$

となる．実は，一般の $\eta \in S_4$ に対して

$$\eta(i\ j)(k\ l) = \eta^{-1} = (\eta(i)\ \eta(j))(\eta(k)\ \eta(l))$$

が成り立つ．したがって，V_4 は S_4 の正規部分群であり，さらに，V_4 は A_4 の正規部分群でもある．この場合，商群 A_4/V_4 の位数は 3 であるため巡回群である．また，$H = \langle(1\ 2)(3\ 4)\rangle$ とすると．これは V_4 の正規部分群であることも簡単にわかる．

したがって，一般的な既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群は S_4 であるわけであるが，S_4 の正規部分群の列として

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

を考えることができ，これらから得られる商群は，それぞれ位数 2 の巡回群 S_4/A_4，位数 3 の巡回群 S_4/V_4，位数 2 の巡回群 V_4/H，位数 2 の巡回群 $H/\{e\}$ である．既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群 S_4 は，このような構造をもっているのである．

定義（可解群）　群 G のある正規列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$

に対して，商群 G_0/G_1，G_1/G_2，$\cdots$，G_{r-1/G_r} はすべてアーベル群であるとする．このとき，G を**可解群**と呼ぶ．

（注意）上の定義においてアーベル群 G とは $x, y \in G$ に対して $xy = yx$ を満たすものである．特に，巡回群はアーベル群である．

Memorize：S_4 の可解性

一般的な既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群 S_4 は，その正規部分群の列として

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

をもち，S_4/A_4 は位数 2 の巡回群，S_4/V_4 は位数 3 の巡回群，V_4/H は位数 2 の巡回群，$H/\{e\}$ は位数 2 の巡回群となる．したがって，S_4 は可解群である．

問題 10. $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + x^3 + x^2 + x + 1 = 0$ のガロア群 G は，可解群であることを証明せよ．

問題 11. n 次二面体群 D_n は可解群であることを証明せよ．

第 6 章

ガロアの定理

$\mathbb{Q}$ 係数の n 次方程式のガロア群が可解群であることと，$\mathbb{Q}$ 係数の n 次方程式がべき根を用いて解けることの関係について説明する．

たとえば，

$$x = \sqrt[3]{4} - \sqrt[3]{2}$$

を考よう．このとき，

$$x^3 = -6\sqrt[3]{4} + 6\sqrt[3]{2} + 2$$

である．よって $\mathbb{Q}$ 係数の 3 次方程式

$$x^3 + 6x - 2 = 0 \tag{6.1}$$

を得る．このことは，$x_1 = \sqrt[3]{4} - \sqrt[3]{2}$ が方程式 (6.1) の解であることを示している．そして，x_1 は体 $\mathbb{Q}$ の 3 次拡大体

$$K = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

の数である．したがって，方程式 (6.1) の右辺は体 K で因数分解されて

$$(x - x_1)(x^2 + x_1 x + x_1^2 + 6) = 0 \tag{6.2}$$

となる．さらに，

$$x^2 + x_1 x + x_1^2 + 6 = 0 \tag{6.3}$$

を，2 次方程式の解の公式で解くことができて，残りの 2 つの解

$$x_2 = \frac{-x_1 + \sqrt{-3x_1^2 - 24}}{2}, \quad x_3 = \frac{-x_1 - \sqrt{-3x_1^2 - 24}}{2}$$

が得られる．$x_1,\ x_2$ は K の 2 次拡大体体 $M = K(\sqrt{-3x_1^2 - 24})$ の数であり，M は方程式 (6.1) の最小分解体となる．さらに，方程式 (6.1) の解はすべて，最小分解体 M の中でべき根で解けることがいえる．

さて，$K_0 = \mathbb{Q},\ K_1 = K,\ K_2 = M$ と置いて．上で述べてきた方程式 (6.1) の最小分解体 M の拡大列

$$K_0 \subset K_1 \subset K_2$$

のそれぞれの最小多項式をみてみよう．

まず，K_0 上 3 次拡大である体 $K_1 = \mathbb{Q}(\sqrt[3]{2})$ の生成元 $\alpha_1 = \sqrt[3]{2}$ の最小多項式は

$$x^3 - 2, \quad 2 \in K_0$$

である．そして，K_1 上 2 次拡大である体 $M = K_2 = K_1(\sqrt{-3x_1^2 - 24})$ の生成元 $\alpha_2 = \sqrt{-3x_1^2 - 24}$ の最小多項式は

$$x^2 - (-3x_1^2 - 24), \quad -3x_1^2 - 24 \in K_1$$

である．

このように，拡大体 $K_j = K_{j-1}(\alpha_j)$ の最小多項式はすべて

$$x^{t_j} - u_j, \quad u_j \in K_{j-1}$$

という形になっていることがわかる．以下のことが定義される．

定義（べき根を用いて解ける方程式）　$\mathbb{Q}$ 係数の n 次方程式 $f(x)=0$ の最小分解体 M に対して，$M \subset L$ となる体 L が以下の条件を満たすように作れるとき，n 次方程式 $f(x)=0$ は**べき根によって解ける**という．

(1)　$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$

(2)　$K_j = K_{j-1}(\alpha_j)$（ただし $1 \leq j \leq r$）で，α_j の K_{j-1} 上の最小多項式は $x^{t_j} - u_j$，$u_j \in K_{j-1}$ である．

拡大体 $K_j \supset K_{j-1}$ が (2) を満たすとき，K_j は K_{j-1} の**べき根拡大**であるという．

さて，$\mathbb{Q}$ から M の拡大次数 $[M:\mathbb{Q}]$ を求めると

$$[M:\mathbb{Q}] = [M:K][K:\mathbb{Q}] = 2 \times 3 = 6$$

である．したがって，方程式 (6.1) のガロア群は 3 次対称群 S_3 である（判別式 $D=-198$ であることからもわかる）．そして S_3 は

$$S_3 \supset A_3 \supset \{e\}$$

で，商群 S_3/A_3 は位数 2 の巡回群，商群 $A_3/\{e\}$ も位数 2 の巡回群であることから，可解群である．以下の定理が証明されている．

ガロアの定理　$\mathbb{Q}$ 係数の n 次方程式 $f(x)=0$ がべき根によって解けるための必要十分条件は，方程式のガロア群 G が可解群であることである．

$n=2,3,4$ のとき対称群 S_n は可解群であるので，上のガロアの定理から，この場合における一般的な $\mathbb{Q}$ 係数の n 次方程式は，べき根によって解けることがいえる．

Memorize：べき根拡大とガロアの定理

$\mathbb{Q}$ 係数の n 次方程式の最小分解体 M を含むある体 L で，L までの拡大の列が順次，べき根拡大となっているとき，n 次方程式はべき根で解けるという．

ガロアの定理は，n 次方程式はべき根で解けるための必要十分条件が方程式のガロア群が可解群であるというものである．

ガロアの定理より，$n = 2, 3, 4$ のとき対称群 S_n は可解群であるので，この n に関して一般的な $\mathbb{Q}$ 係数の n 次方程式はべき根によって解ける．

問題 12. $\mathbb{Q}$ 係数の 3 次方程式 $x^3 - 3x + 1 = 0$ がべき根によって解けることを，ガロアの定理を用いて証明せよ．

問題 13. $\mathbb{Q}$ 係数の 4 次方程式 $x^4 + 2x^2 - 4 = 0$ がべき根によって解けることを，ガロアの定理を用いて証明せよ．

第 7 章

４次方程式のガロア群の決定

既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群のガロア群は,

$$S_4,\quad A_4,\quad D_4,\quad V_4,\quad C_4$$

の５つのタイプしかない．問題は，4 次方程式が与えられたとき，そのガロア群をどのようにして決定できるかである．

既約な $\mathbb{Q}$ 係数の4 次方程式

$$x^4 + bx^3 + cx^2 + dx + e = 0 \tag{7.1}$$

が与えられたとき, 判別式 D が $D \in \mathbb{Q}^2$ であるとき, 方程式のガロア群 G は $G \subset A_4$ なので，$G = A_4,\ V_4$ に絞られる．

A_4 か V_4 を判別する新たな方法が必要である．

そこで,

$$x^4 + bx^3 + cx^2 + dx + e = 0 \tag{7.2}$$

の解を $x_1,\ x_2,\ x_3,\ x_4$ とする．そして，

$$\begin{aligned} t_1 &= x_1x_2 + x_3x_4, \\ t_2 &= x_1x_3 + x_2x_4, \\ t_3 &= x_1x_4 + x_2x_3 \end{aligned}$$

と置く．さらに，

$$R_4(x) = (x - t_1)(x - t_2)(x - t_3)$$

と置く．このとき，4 次方程式 (7.2) の解と係数の関係から，$\mathbb{Q}$ 係数の 3 次方程式

$$R_4(x) = x^3 - cx^2 + (bd - 4e)x + 4ce - b^2e - d^2$$

が得られる．

定義（4 次方程式のリゾルベント）　$\mathbb{Q}$ 係数の 3 次方程式

$$R_4(x) = x^3 - cx^2 + (bd - 4e)x + 4ce - b^2e - d^2$$

を 4 次方程式 $x^4 + bx^3 + cx^2 + dx + e = 0$ の**リゾルベント**と呼ぶ．

4 次方程式のリゾルベント $R_4(x)$ の重要性も，$R_4(x) = 0$ の最小分解体 M_r にある．つまり，$R_4(x) = 0$ は 3 次方程式なので，M_r の $\mathbb{Q}$ 上の拡大次数は，

$$[M_r : \mathbb{Q}] = 6,\ 3,\ 2,\ 1$$

のいずれかとなる．以下の重要な定理が証明されている．

定理（4 次方程式の分類）　M を既約な $\mathbb{Q}$ 係数の 4 次方程式 $f(x)=0$ の最小分解体，M_r を $R_4(x)=0$ の最小分解体，$m=[M_r:\mathbb{Q}]$ と置く．このとき方程式のガロア群 G に関して以下のことが成り立つ．

(1) $G=S_4 \iff m=6$
(2) $G=A_4 \iff m=3$
(3) $G=C_4,\ D_4 \iff m=2$
(4) $G=V_4 \iff m=1$

[注意]　定理（4 次方程式の分類）において，もし $m=3,6$ ならば $R_4(x)$ は $\mathbb{Q}$ 上既約であり，$m=2,1$ ならば $R_4(x)$ は $\mathbb{Q}$ 上既約でないことを意味する．

既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4+8x+12=0 \tag{7.3}$$

のガロア群 G を決定しよう．

リゾルベント $R_4(x)$ を求めると，$b=c=0,\ d=8,\ e=12$ より

$$\begin{aligned} R_4(x) &= x^3-cx^2+(bd-4e)x+4ce-b^2e-d^2 \\ &= x^3-48x-64 \end{aligned}$$

である．もし $R_4(x)$ の 1 つの解 x_1 が $x_1\in\mathbb{Q}$ ならば，それは x_1 は 64 の約数でなければならないが，簡単な計算からそれはないことがわかる．したがって，$R_4(x)$ は $\mathbb{Q}$ 上既約である．よって，G は S_4 か A_4 である．そこで，3 次方程式の判別式をみる．$a=0,\ b=-48,\ c=-64$ より

$$D=-4a^3c+a^2b^2+18abc-4b^3-27c^2=576^2$$

である．よって，$R_4(X)=0$ のガロア群は A_3 であるので，$m=3$ である．したがって，$G=A_4$ である．

残された問題は，4 次方程式のガロア群が D_4 または C_4 であった場合，これをどのようにして区別するかである．

既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4 + 5x^2 + 5 = 0 \tag{7.4}$$

を考える．このとき，

$$x^2 = \frac{-5 \pm \sqrt{5}}{2}$$

より，

$$x = \pm\sqrt{\frac{-5 \pm \sqrt{5}}{2}}$$

であるので，$[M : \mathbb{Q}] = 4$ より $M = C_4$ であることがわかる．

一方，このリゾルベント $R_4(x)$ を求めると，$b = 0,\ c = 5,\ d = 0,\ e = 5$ より

$$\begin{aligned} R_4(x) &= x^3 - cx^2 + (bd - 4e)x + 4ce - b^2e - d^2 \\ &= x^3 - 5x^2 - 20x + 100 \\ &= (x - 5)(x^2 - 10x - 10) \end{aligned}$$

である．そして，2 次方程式 $x^2 - 10x - 10 = 0$ より

$$x = \pm 2\sqrt{5}$$

が得られる．つまり $R_4(x) = 0$ の最小分解体は $M_r = \mathbb{Q}(\sqrt{5})$ である．そしてこれは，方程式 (7.4) が M_r 上可約であることを意味する．

次に，既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4 - 3 = 0 \tag{7.5}$$

を考える．明らかに，この解は，

$$x = \pm\sqrt[4]{3},\ \ \pm\sqrt{-1}\sqrt[4]{3}$$

であるので，$[M:\mathbb{Q}]=8$ より $M=D_4$ であることがわかる．

一方，このリゾルベント $R_4(x)$ を求めると，$b=c=d=0,\ e=-3$ より

$$\begin{aligned} R_4(x) &= x^3-cx^2+(bd-4e)x+4ce-b^2e-d^2 \\ &= x^3-+12x \\ &= x(x^2+12) \end{aligned}$$

である．そして，2 次方程式 $x^2-+12=0$ より

$$x=\pm 2\sqrt{-3}$$

が得られる．つまり $R_4(x)=0$ の最小分解体は $M_r=\mathbb{Q}(\sqrt{-3})$ である．そしてこれは，方程式 (7.4) が M_r 上既約であることを意味する．以下の定理が証明されている．

定理（C_4 と D_4 の判別）　$m=[M_r:\mathbb{Q}]=2$ とする．このとき，4 次方程 $f(x)=0$ のガロア群 G に関して以下のことが成り立つ．

(1)　$G=C_4 \iff f(x)=0$ は M_r 上可約である．

(2)　$G=D_4 \iff f(x)=0$ は M_r 上既約である．

既約な $\mathbb{Q}$ 係数の 4 次方程式

$$x^4+x^3+x^2+x+1=0 \tag{7.6}$$

のガロア群 G を決定しよう．

リゾルベント $R_4(x)$ を求めると，$b=c=d=e=1$ より

$$\begin{aligned} R_4(x) &= x^3-cx^2+(bd-4e)x+4ce-b^2e-d^2 \\ &= x^3-x^2-3x-2 \\ &= (x-2)(x^2+x-1) \end{aligned}$$

である．したがって，$R_4(x)=0$ の最小分解体は $M_r=\mathbb{Q}(\sqrt{5})$ である．よって

$m = 2$ であるので $G = C_4,\ D_4$ である．さらに，方程式 (7.6) は，

$$\left\{x^2 + \left(\frac{1+\sqrt{5}}{2}\right)x + 1\right\}\left\{x^2 + \left(\frac{1-\sqrt{5}}{2}\right)x + 1\right\} = 0$$

となるので，方程式 (7.6) は M_r 上可約である．したがって，$G = C_4$ である．

Memorize：4 次方程式の判別

$m = [M_r : \mathbb{Q}]$ と置く．

(1) $G = S_4 \iff m = 6$

(2) $G = A_4 \iff m = 3$

(3) $G = C_4 \iff m = 2$ で $f(x) = 0$ は M_r 上可約

　　$G = D_4 \iff m = 2$ で $f(x) = 0$ は M_r 上既約

(4) $G = V_4 \iff m = 1$

問題 14. 次の既約な $\mathbb{Q}$ 係数の 4 次方程式のガロア群は S_4, A_4, D_4, C_4, V_4 のどれか判定せよ．

(1) $x^4 + 3x + 3 = 0$　　(2) $x^4 + 5x + 5 = 0$

(3) $x^4 + 7x + 7 = 0$　　(4) $x^4 - 8x + 12 = 0$

(5) $x^4 + 1 = 0$

第 8 章

5 次方程式のガロア群の種類

既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ のガロア群 G は，$\sharp G = 120,\ 60,\ 20,\ 10,\ 5$ であることを説明する．これに対応するガロア群は 5 次対称群 S_5，5 次交代群 A_5，位数 20 のフロベニウス群 F_{20}，10 次二面体群 D_5，5 次巡回群 C_5 である．

既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5 + ax^4 + bx^3 + cx^2 + dx + f = 0 \tag{8.1}$$

のガロア群 G は，5 次対称群 S_5 の部分群である．そして G の可能性として，

$$\sharp G = 120,\ 60,\ 40,\ 30,\ 20,\ 15,\ 10,\ 5$$

となるものが考えられる．結論からいえば，S_5 を除くと G の次数は，

$$\sharp G = 60,\ 20,\ 10,\ 5$$

である．そしてこれらに対応する群は，それぞれ，5 次交代群 A_5，位数 20 のフロベニウス群 $F_{20} = C_5C_4$ (ただし $C_5 \cap C_4 = \{e\}$，C_5 は F_{20} の正規部分群)，10 次二面体群 D_5，5 次巡回群 C_5 である．

定理（S_5 と A_5 の非可解性）　既約な $\mathbb{Q}$ 係数の 5 次方程式のガロア群 G について以下が成り立つ.

(1)　$G = S_5,\ A_5$ は可解群でない.

(2)　$G = F_{20}, D_5, Z_5$ は可解群である.

定理（S_5 と A_5 の非可解性）の (2) が成り立つことは明らかである（興味ある読者は各自証明してみよう）ので，(1) について説明する.

A_5 が可解群でないことは，背理法で証明される．すなわち，A_5 が可解群であれば，A_5 の正規部分群 N が存在して A_5/N がアーベル群となることを仮定して矛盾を導くのである．まず

$$A_5 = \langle (1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 2\ 5) \rangle$$

であった．そこで，$i,\ j,\ k \in \{3,4,5\}$ で $i \neq k,\ j \neq k$ として，

$$\sigma = (1\ i\ k) = (1\ i)(i\ k), \quad \tau = (k\ 2\ j) = (k\ 2)(2\ j)$$

と置くと，$\sigma,\ \tau \in A_5$ である．A_5/N はアーベル群であることを仮定しているので，$\sigma,\ \tau \in A_5$ に対して，

$$(\sigma N)(\tau N) = (\tau N)(\sigma N)$$

である．したがって，

$$(\sigma\tau\sigma^{-1}\tau^{-1})N = (\sigma N)(\tau N)(\sigma N)^{-1}(\tau N)^{-1} = N$$

である．一方，

$$\sigma\tau\sigma^{-1}\tau^{-1} = (1\ i\ k)(k\ 2\ j)(j\ 2\ k) = (1\ 2\ k) \in A_5$$

である．よって $(1\ 2\ k) \in A_5$ である．これは $N = A_5$ を意味する．しかし，A_5 はアーベル群でないので仮定は正しくないという結論が得られ，A_5 は可解群でないことが示されるのである.

S_5 が可解群でないことは，部分群である A_5 が可解群でないことからわかる．なぜならば，一般に，

『可解群 G の部分群 N は可解群である』

という命題が成り立つ（興味ある読者は各自証明してみよう）ので，その待遇からいえるからである．

それでは，$\sharp G = 15$ となるものは存在しないことを説明しよう．

方程式の解を $x_1,\ x_2,\ x_3,\ x_4,\ x_5$ とし，

$$K_1 = \mathbb{Q}(x_1),\quad K_2 = K_1(x_2),\quad K_3 = K_2(x_3),\quad K_4 = K_2(x_4),\quad M = K_4(x_5)$$

と置く．ここで，M は 5 次方程式の最小分解体である．$\sharp G = 15$ となるためには，$L = K_1 = K_2$ でなければならない．なぜならば，この場合 L において

$$(x - x_1)(x - x_2)(\,3\text{次式})$$

と因数分解されるからである．したがって，この群 G は 2 つの元で生成される．ところが，定理（位数 pq の群）より，位数 15 の群は巡回群である．したがって，$\sharp G = 15$ となるものは存在しないのである．

$\sharp G = 30, 40$ であるガロア群 G が存在しないことを説明したい．しかしそのためには，いくつかの準備が必要である．

f を G から G' への準同型写像とする．このとき，

$$Ker(f) = \{\sigma \in G \mid f(\sigma) = e'\ \}$$

を f の**核**または**カーネル** f という．$Ker(f)$ が G の部分群であることは明らかである．さらに次の重要な定理が証明されている．

定理（核の正規性）　f を G から G' への準同型写像とする．このとき $Ker(f)$ は G の正規部分群である．

H を群 G の部分群とすると，G の中に H に関係する正規部分群が存在することが証明されている．以下がその定理である．

定理（正規部分群の存在）　H を群 G の部分群とし，$n = \sharp G/\sharp H$ とする．このとき，G から S_n への準同型写像 $f : G \to S_n$ で，$Ker(f) \subset H$ となるものが存在する．

5 次交代群 A_5 は可解群ではなかった．実はそれだけでなく，A_5 の正規部分群は A_n と $\{e\}$ のみであることが証明されている．つまり，$n \geq 5$ のときの A_5 は**単純群**なのである．そして，このことから次のことが証明される．

定理（S_5 の正規部分群）　S_5 の正規部分群は，S_5 と A_5 と $\{e\}$ のみである．

以上の準備から，既約な $\mathbb{Q}$ 係数の 5 次方程式のガロア群 $G \subset S_5$ に $\sharp G = 30, 40$ であるものが存在しないことが示すことができる．

例えば，$\sharp G = 30$ としよう．そうすると，$n = \sharp(S_5)/\sharp(G) = 4$ である．したがって，定理（正規部分群の存在）から準同型写像 $f : S_5 \to S_4$ で $Ker(f) \subset G$ となるものが存在する．$Ker(f)$ は S_5 の正規部分群である．S_5 の正規部分群 N は S_5 と A_5 と $\{e\}$ のみである．したがって，$Ker(f) = \{e\}$ となる．もし $f(\sigma) = f(\tau)$ なら f は準同型写像なので，$f(\sigma^{-1}\tau) = f(\sigma)f(\tau)^{-1} = e'$ であり，$Ker(f) = \{e\}$ より $\sigma^{-1}\tau = e$ となり $\sigma = \tau$ がいえる．しかし $\sharp S_5 > \sharp S_4$ より，これは矛盾である．した

がって，$\sharp G = 30$ であるものが存在しないのである．$\sharp G = 40$ であるものが存在しないことも同様に示される（各自で証明してみよう）．

Memorize：5 次方程式のガロア群 G

(1) 可解群でないもの
　5 次対称群 S_5，　5 次交代群 A_5
(2) 可解群であるもの
　位数 20 のフロベニウス群 F_{20}，　10 次二面体群 D_5，　5 次巡回群 C_5

問題 15. 既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ の方程式の解を $x_1,\ x_2,\ x_3,\ x_4,\ x_5$ とし，

$$K_1 = \mathbb{Q}(x_1),\quad K_2 = K_1(x_2),\quad K_3 = K_2(x_3),\quad K_4 = K_3(x_4),\quad M = K_4(x_5)$$

とする．このとき，次を満たす方程式はべき根で解けるかどうかどれか判定せよ．

(1)　$x_2 \notin K_1,\ x_3 \notin K_2,\ x_4 \in K_3$ である場合
(2)　$x_2, x_3 \in K_1$ である場合

問題 16.（**チャレンジ問題**）可解群 G の部分群 N は可解群であることを証明せよ．

問題 17.（**チャレンジ問題**）5 次方程式のガロア群 G に $\sharp G = 40$ であるものは存在しないことを証明せよ．

第 9 章

5 次方程式 $x^5 + ax + b = 0$ のガロア群の決定

既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ は，$x = y - a/5$ と置くと，

$$y^5 + py^3 + qy^2 + ry + s = 0 \tag{9.1}$$

と変換される（**チルンハウス変換**という）．さらに，(9.1) は，

$$x^5 + ax + b = 0 \tag{9.2}$$

と単純化できることが知られている．(9.2) を**ブリング-ジェラード標準形**と呼ぶ．

この章では，既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5 + ax + b = 0$ について，このタイプの方程式のガロア群を，どのようにして決定するのかについて説明する．そのために重要な道具は，判別式 D とリゾルベント $R_5(x)$ である．

5 次方程式のガロア群の決定においても，判別式 D は重要である．以下の定理は与えられた方程式のガロア群の決定に重要である．

定理（判別式 D）　既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax+b=0$ のガロア群 G について以下が成り立つ.

(1) $D=256a^5+3125b^4$

(2) $G=A_5, D_5, C_5 \quad \Longleftrightarrow \quad D\in\mathbb{Q}^2$

(3) G が可解群 $\quad\Longrightarrow\quad D>0$

例えば，既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5-3x+1=0$$

の判別式 D を計算すると，$a=-3,\ b=1$ より

$$D=256a^5+3125b^4=-59083$$

したがって，定理（判別式）より $G=S_5$ である.

例えば，既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5+2=0$$

の判別式 D を計算すると，$a=0,\ b=2$ より

$$D=256a^5+3125b^4=50000=2^4\times 5^5$$

したがって，定理（判別式）より $G=S_5$ または $G=F_{20}$ であることまではいえる.

次に，5 次方程式のリゾルベント $R_5(x)$ について説明していく.

これから定義する 5 次方程式のリゾルベント $R_5(x)$ は F_{20} で不変な式である．そのため，既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax^x+b=0$ の解を x_1,x_2,x_3,x_4,x_5 とし，さらに

$$F_{20}=\langle(1\ 2\ 3\ 4\ 5),\ (2\ 3\ 5\ 4)\rangle$$

とする．そして，

$$\begin{aligned}\theta_1 &= x_1^2x_2x_5+x_1^2x_3x_4+x_2^2x_1x_3+x_2^2x_4x_5+x_3^2x_1x_5+x_3^2x_2x_4\\ &\quad +x_4^2x_1x_2+x_4^2x_3x_5+x_5^2x_1x_4+x_5^2x_2x_3\end{aligned}$$

と置く．このとき θ_1 に置換 $(1\ 2\ 3\ 4\ 5)$ を作用させたもの $(1\ 2\ 3\ 4\ 5)\theta_1$ は

$$\begin{aligned}(1\ 2\ 3\ 4\ 5)\theta_1 &= x_2^2x_3x_1+x_2^2x_4x_5+x_3^2x_2x_4+x_3^2x_5x_1+x_4^2x_2x_1+x_4^2x_3x_5\\ &\quad +x_5^2x_2x_3+x_5^2x_4x_1+x_1^2x_2x_5+x_1^2x_3x_4\\ &= \theta_1\end{aligned}$$

であり，θ_1 に置換 $(2\ 3\ 5\ 4)$ を作用させたもの $(2\ 3\ 5\ 4)\theta_1$ も

$$\begin{aligned}(2\ 3\ 5\ 4)\theta_1 &= x_1^2x_3x_4+x_1^2x_5x_2+x_3^2x_1x_5+x_3^2x_2x_4+x_5^2x_1x_4+x_5^2x_3x_2\\ &\quad +x_2^2x_1x_3+x_2^2x_5x_4+x_4^2x_1x_2+x_4^2x_3x_5\\ &= \theta_1\end{aligned}$$

である．これは θ_1 が F_{20} の作用で不変であることを意味する．次に，

$$\begin{aligned}\theta_2 &= (1\ 2\ 3)\theta_1\\ &= x_1^2x_2x_5+x_1^2x_3x_4+x_2^2x_1x_4+x_2^2x_3x_5+x_3^2x_1x_2+x_3^2x_4x_5\\ &\quad +x_4^2x_1x_5+x_4^2x_2x_3+x_5^2x_1x_3+x_5^2x_2x_4\end{aligned}$$

$$\begin{aligned}\theta_3 &= (1\ 3\ 2)\theta_1\\ &= x_1^2x_2x_3+x_1^2x_4x_5+x_2^2x_1x_4+x_2^2x_3x_5+x_3^2x_1x_5+x_3^2x_2x_4\\ &\quad +x_4^2x_1x_3+x_4^2x_2x_5+x_5^2x_1x_2+x_5^2x_3x_4\end{aligned}$$

$$\begin{aligned}\theta_4 &= (1\ 2)\theta_1\\ &= x_1^2x_2x_3+x_1^2x_4x_5+x_2^2x_1x_5+x_2^2x_3x_4+x_3^2x_1x_4+x_3^2x_2x_5\\ &\quad +x_4^2x_1x_2+x_4^2x_3x_5+x_5^2x_1x_3+x_5^2x_2x_4\end{aligned}$$

$$\begin{aligned}\theta_5 &= (2\ 3)\theta_1\\ &= x_1^2x_2x_4+x_1^2x_3x_5+x_2^2x_1x_5+x_2^2x_3x_4+x_3^2x_1x_2+x_3^2x_4x_5\\ &\quad +x_4^2x_1x_3+x_4^2x_2x_5+x_5^2x_1x_4+x_5^2x_2x_3\end{aligned}$$

$$\begin{aligned}\theta_6 &= (1\ 3)\theta_1 \\ &= x_1^2x_2x_4 + x_1^2x_3x_5 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_4 + x_3^2x_2x_5 \\ &\quad + x_4^2x_1x_5 + x_4^2x_2x_3 + x_5^2x_1x_2 + x_5^2x_3x_4\end{aligned}$$

をそれぞれ定義する．これらはすべて F_{20} の作用で不変であることがわかる（各自で確かめてみよう）．そして，5 次方程式の**リゾルベント** $R_5(x)$ を

$$R_5(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)(x-\theta_4)(x-\theta_5)(x-\theta_6) \tag{9.3}$$

と定義する．

既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax+b=0$ について，$R_5(x)$ を解と係数の関係式から計算すると

$$\begin{aligned}R_5(x) = x^6 &+ 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 \\ &+ (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4)\end{aligned} \tag{9.4}$$

となる．

定理（リゾルベント $R_5(x)$ による判定） 既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax+b=0$ のガロア群 G が可解群，すなわち $G = F_{20}, D_5, C_5$ であることの必要十分条件は，$R_5(x)=0$ のある解 x_1 が $x_1 \in \mathbb{Q}$ となることである．

改めて，既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5 + 2 = 0$$

を考える．これは $D = 2^4 \times 5^5$ であることから $G = S_5$ または $G = F_{20}$ であった．そこで，リゾルベント $R_5(x)$ を計算すると，

$$R_5(x) = x^6 - 50000x$$

である．明らかに $x_1 = 0 \in \mathbb{Q}$ は解であるので，定理（リゾルベント $R_5(x)$ による判定）より，$G = F_{20}$ が得られる．

既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5 + 20x + 16 = 0$$

を考える．判別式 D を計算すると，$a = 20,\ b = 16$ より

$$D = 256a^5 + 3125b^4 = 2^{16} \times 5^6$$

したがって，定理（判別式）より $G = A_5, D_5, C_5$ である．リゾルベント $R_5(x)$ を計算すると，

$$R_5(x) = x^6 + 160x^5 + 16000x^4 + 1280000x^3 + 64000000x^2 + 1433600000x + 4096000000$$

であり，$R_5(x) = 0$ は $\mathbb{Q}$ に解を持たない．したがって，定理（リゾルベント $R_5(x)$ による判定）より，$G = A_5$ が得られる．

既約な $\mathbb{Q}$ 係数の 5 次方程式

$$x^5 - 5x - 12 = 0$$

を考える．判別式 D を計算すると，$a = -5,\ b = -12$ より

$$D = 256a^5 + 3125b^4 = 2^{12} \times 5^6$$

したがって，定理（判別式）より $G = A_5, D_5, C_5$ である．リゾルベント $R_5(x)$ を計算すると，

$$R_5(x) = x^6 - 40x^5 + 1000x^4 - 20000x^3 + 250000x^2 - 66400000x + 976000000$$

であり，$R_5(x) = 0$ は $x_1 = 40 \in \mathbb{Q}$ という解をもつ．したがって，定理（リゾルベント $R_5(x)$ による判定）より，$G = D_5,\ C_5$ である．

一方，$y = x^5 - 5x - 12$ と置いて，これを x で微分すると

$$y' = 5x^4 - 5 = 5(x - 1)(x + 1)(x^2 + 1)$$

となる．したがって，$y=x^5-5x-12$ のグラフは，$x=1,-1$ で極値をとり，

$$y(1)=-16,\quad y(-1)=-8$$

であるので，$y=x^5-5x-12$ の実数解は唯一つである．よって，$x^5-5x-12=0$ の実数解を x_1，$K=\mathbb{Q}(x_1)$ とし，最小分解体を L とすると，

$$[L:\mathbb{Q}]=[L:K][K:\mathbb{Q}]=2\times 5=10$$

となる．したがって $G=D_5$ である．

Memorize：5 次方程式 $x^5+ax+b=0$ の判別

(1) $D=256a^5+3125b^4$

(2) $G=A_5,D_5,C_5 \iff D\in\mathbb{Q}^2$

(3) G が可解群 $\implies D>0$

(4) $R_5(x)=x^6+8ax^5+40a^2x^4+160a^3x^3+400a^4x^2$
$+(512a^5-3125b^4)x+(256a^6-9375ab^4)$

(5) $G=F_5,D_5,C_5 \iff R_5(x)=0$ のある解 x_1 が $x_1\in\mathbb{Q}$

問題 18. 次の既約な $\mathbb{Q}$ 係数の 5 次方程式のガロア群は S_5,A_5,F_{20},D_5,C_5 のどれか判定せよ．

(1) $x^5-55x+88=0$　　(2) $x^5-5x+12=0$

(3) $x^5+15x+12=0$　　(4) $x^5+5x+1=0$

(5) $x^5+11x+44=0$　　(6) $x^5+15x+44=0$

問題 19.（**チャレンジ問題**）既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax+b=0$ のガロア群には C_5 が存在しないことを証明せよ．

第 10 章

（付録）ガロア群が A_5 である 5 次方程式

当然のことであるが，既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5+ax^4+bx^3+cx^2+dx+e=0$ のガロア群 G は，a,b,c,d,e の範囲を限定すると，いたるところ $G=S_5$ であることがわかる．したがって，その他のガロア群をもつ 5 次方程式の係数 a,b,c,d,e は，どういったものだろうかというテーマが立つ．

この章では，特にガロア群が A_5 である 5 次方程式について，著者らが行った研究を紹介する．

ガロア群が A_5 である 5 次方程式について，2019 年に稲垣佑都（津山工業高等専門学校 4 年）が行った．稲垣は SageMath という数学フリーソフトを用いた研究からガロア群が A_5 である 5 次方程式は，リュカ数やフィボナッチ数に関係していることを発見した．

n 番目のリュカ数 L_n とは，$L_0=2,\ L_1=1$ で $n\geq 2$ のとき

$$L_n=L_{n-1}+L_{n-2}$$

を満たすものである．

また，n 番目のフィボナッチ数 F_n とは，$F_0 = 0$, $F_1 = 1$ で $n \geq 2$ のとき

$$F_n = F_{n-1} + F_{n-2}$$

を満たすものである．

L_n と F_n については，双曲線 $5x^2 - y^2 = \pm 4$ と関係があることは古くから知られている．例えば，$x = F_1 = 1, y = L_1 = 1$ のとき $5x^2 - y^2 = 4$，$x = F_2 = 1, y = L_2 = 3$ のとき $5x^2 - y^2 = -4$，$x = F_3 = 2, y = L_3 = 4$ のとき $5x^2 - y^2 = 4$，$x = F_4 = 3, y = L_4 = 7$ のとき $5x^2 - y^2 = -4$ となる．

定理（双曲線とリュカ数とフィボナッチ数の関係）　自然数の組 (x, y) が $5x^2 - y^2 = \pm 4$ を満たすことの必要十分条件は $x = F_n$, $y = L_n$ である．ただし，$n \geq 1$ とする．

以下，稲垣の研究結果を紹介する．以下，n は自然数とする．

定理（A_5 をもつ $x^5 + ax + b = 0$）[稲垣，松田]　$u_n = L_{2n+1}L_{2n+3}$ とする．このとき 5 次方程式 $x^5 + 5u_n x \pm 4u_n = 0$ のガロア群は A_5 である．

定理（A_5 をもつ $x^5 + ax + b = 0$）の証明は，$n \geq 4$ のとき $u_n + 1 = 5F_{2n+2}^2$ であること，$u_n \not\equiv 0 \bmod 3$ であること，$D^2 \in \mathbb{Q}^2$ であること，そして，$R_5(x) = 0$ が整数解をもたないことから証明される．

証明はまだ終わっていないが，稲垣が発見した以下の 7 つの予想を紹介する．

予想 1．　$n = 1, n \geq 3$ とし，$s_n = \pm 10L_{2n-1}$, $t_n = \pm 24L_{2n-1}$（復号同順）とする．このとき 5 次方程式 $x^5 + s_n x^2 + t_n = 0$ のガロア群は A_5 である．

予想 2．　$s_n = L_{2n+1}$, $t_n = L_{2n}$ とする．このとき 5 次方程式 $x^5 + 15x^3 \pm 81s_n = 0$ と $x^5 - 15x^3 \pm 81t_n = 0$ のガロア群は A_5 である．

予想 3．　$n \neq 3$ とし，$s_n = L_{2n-}^2$, $t_n = L_{2n}^2 - 4$ とする．このとき 5 次方程式 $x^5 + 5x^4 + 64s_n = 0$, $x^5 - 5x^4 - 64s_n = 0$, $x^5 + 5x^4 - 64t_n = 0$, $x^5 - 5x^4 + 64t_n = 0$ のガロア群は A_5 である．

予想 4．　$n \neq 3$ のとき,5 次方程式 $x^5 + 5x^4 - 20x^2 - 8(L_{2n} - 2) = 0$ のガロア群は A_5 である．

予想 5．　5 次方程式 $x^5 + 10x^3 + 25x \pm 8L_{n+1} = 0$ のガロア群は A_5 である．

予想 6．　5 次方程式 $x^5 + nx^4 + 25x + 9n = 0$ のガロア群は A_5 である．

予想 7．　5 次方程式 $x^5 + 5x^4 + 15x + (125F_{2n+1} - 53) = 0$ のガロア群は A_5 である．

5 次方程式のガロア群の研究テーマはまだまだありそうである．そして，研究にはリゾルベント $R_5(x)$ は必要不可欠である．

最後に，既約な $\mathbb{Q}$ 係数の 5 次方程式 $x^5 + px^3 + qx^2 + rx + s = 0$ に関して D.S.DUMMIT の研究から得られた $R_5(x)$ を紹介する．

$$R_5(x) = x^6 + 8rx^5 + Sx^4 + Tx^3 + Ux^2 + Vx + W$$

ここで,

$$
\begin{aligned}
S &= 2pq^2 - 6p^2r + 40r^2 - 50qs \\
T &= -2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 15p^2qs - 400qrs + 125ps^2 \\
U &= p^2q^4 - 6p^3q^2r - 8q^4r + 9p^4r^2 + 76pq^2r^2 - 136p^2r^3 + 400r^4 \\
&\quad -50pq^3s + 90p^2qrs - 1400qr^2s + 625q^2s^2 + 500prs \\
V &= -2pq^6 + 19p^2q^4r - 51p^3q^2r^2 + 3q^4r^2 + 32p^4r^3 + 76pq^2r^3 \\
&\quad -256p^2r^4 + 512r^5 - 31p^3q^3s - 58q^5s + 117p^4qrs + 105pq^3rs \\
&\quad +260p^2qr^2s - 2400qr^3s - 108p^5s^2 - 325p^2q^2s^2 + 525p^3rs^2 \\
&\quad +2750q^2rs^2 - 500pr^2s^2 + 625pqs^3 - 3125s^4 \\
W &= q^8 - 13pq^6r + p^5q^2r^2 + 65p^2q^4r^2 - 4p^6r^3 - 128p^3q^2r^3 + 17q^4r^3 \\
&\quad +48p^4r^4 - 16pq^2r^4 - 192p^2r^5 + 256r^6 - 4p^5q^3s - 12p^2q^5s \\
&\quad +18p^6qrs + 12p^3q^3rs - 124q^5rs + 196p^4qr^2s + 590pq^3r^2s \\
&\quad -160p^2qr^3s - 1600qr^4s - 27p^7s^2 - 150p^4q^2s^2 - 125pq^4s^2 \\
&\quad -99p^5rs^2 - 725p^2q^2rs^2 + 1200p^3r^2s^2 + 3250q^2r^2s^2 \\
&\quad -2000pr^3s^2 - 1250pqrs^3 + 3125p^2s^4 - 9375rs^4
\end{aligned}
$$

である.

参考文献

本書を制作するにあたり，以下の論文や書籍を参考にした.

[1] D. S. Dummit, Solving solvable quintics, Mathematics of computation volume 57, number 195, pp.387-195 (1991).

[2] Blair K. Spearman and Kenneth S. Williams, ON SOLVABLE QUINTICS $x^5 + ax + b$ AND $x^5 + ax^2 + b$, ROCKY MOUNTAIN JOURNAL OF MATHEMATICS Vol.28, No.2 (1998).

[3] 大迎規宏，可解な５次方程式について，平成 15 年度学位論文，兵庫教育大学大学院，学校教育研究科，教科・領域教育選考，自然系コース，

[4] Patrick Morandi, Field and Galois Theory, Graduate Texts in Mathematics 167, Springer, 1996.

[5] 彌永昌吉，有馬哲，浅枝陽, 代数入門, 東京図書 (1990).

[6] 中村滋, フィボナッチ数の小宇宙, 日本評論社 (2002).

問題の解答

問題 1. (1) 略　(2) 略　(3) 24

問題 2. (1) 4　(2) 12　(3) 36

問題 3. 120, 60, 40, 30, 20, 15, 10, 5

問題 4. 720, 360, 240, 180, 144, 90, 72, 60, 48, 36, 30, 24, 18, 12, 6

問題 5. 略

問題 6. (1) D_4 (2) A_4

問題 7. (1) S_3 (2) A_3

問題 8. $V_4 \subset A_4$ だから

問題 9. $C_4 \not\subset A_4$ だから

問題 10. $G = C_4$ で $C_4 \subset \{e\}$ だから

問題 11. $D_n = \langle \sigma, \tau \rangle$ で $\sigma^n = \tau^2 = e,\ \tau\sigma\tau = \sigma^{-1}$ で，$N = \langle \sigma \rangle$ とすると，N は D_n の正規部分群である．よって正規部分列 $D_n \supset N \supset \{e\}$ を考えると，D_n/N は位数 2 の巡回群，$N/\{e\}$ も巡回群なので，D_n は可解群.

問題 12. $G = S_3$ で S_3 は可解群であるので，べき根で解ける.

問題 13. $G = D_4$ で D_4 は可解群であるので，べき根で解ける.

問題 14. (1) D_4　(2) C_4　(3) S_4　(4) A_4　(5) V_4

問題 15. (1) べき根で解けない.　(2) べき根で解ける.

問題 16. 略

問題 17. 略

問題 18. (1) A_5　(2) D_5　(3) F_{20}　(4) S_5　(5) D_5　(6) F_{20}

問題 19. 略