ガロア理論への招待

どうして 5 次方程式は解けないのか？

ほの

2025 年 8 月 8 日

概要

本書は、代数方程式の**べき根による解法**の可能性とその限界を、代数学の観点から解説するものです。そのために、まず**体**とその**拡大**、そして対称性を記述する**群**という基本的な代数構造を定義します。

中心となるのは、体の拡大の構造が、**ガロア群**と呼ばれる群の構造と、**ガロアの基本定理**によって密接に結びつけられることを示すことです。この理論的枠組みを用いて、「方程式がべき根で解ける」という条件を「ガロア群が**可解群**である」という条件に翻訳します。

最終的に、一般五次方程式のガロア群が可解群ではないことを証明し、なぜその**代数的な解の公式が存在しない**のかを論理的に結論付けます。さらに、この理論が持つ普遍的な視点が、現代数学や情報技術の分野でどのように応用されているかについても展望します。

目次

1 代数方程式と体の拡大 3

1.1 代数的解法とは何か 3

1.2 体と係数体 3

1.3 体の拡大 4

2 対称性を記述する言語：群 5

2.1 置換とその集まり 5

2.2 群の定義 6

2.3 対称群と部分群 7

2.4 正規部分群と剰余群 8

第 I 部　ガロア理論の核心 11

3 体の拡大を司る群：ガロア群 11

3.1 体の自己同型写像 11

3.2 ガロア群の定義 12

3.3 例題：ガロア群の計算 13

4 ガロアの基本定理 15
4.1 ガロア対応 15
4.2 定理の含意 16

第 II 部 五次方程式の非可解性の証明 17

5 べき根による可解性と可解群 18
5.1 べき根による拡大の性質 18
5.2 累冪根拡大とガロア群 19
5.3 可解群の定義 20

6 五次方程式のガロア群と非可解性 21
6.1 一般 n 次方程式のガロア群 21
6.2 対称群 S_n $(n \leq 4)$ の構造 22
6.3 交代群 A_n と単純群 24
6.4 S_5 の非可解性 26
6.5 結論：アーベル=ルフィニの定理 27

第 III 部 ガロア理論の展望 27

7 ガロア理論の射程 28
7.1 微分方程式の理論へ 28
7.2 整数論への応用 29
7.3 幾何学との関連 30
7.4 楕円関数を使えば五次方程式は解ける 31

1　代数方程式と体の拡大

1.1　代数的解法とは何か

ある代数方程式の解を、その方程式の**係数**から出発し、**四則演算（和、差、積、商）**と**べき根（平方根、立方根など）**の操作を有限回だけ用いて表現する方法を、その方程式の**代数的解法**と呼びます。また、そのような形で表される解の公式を「代数的な解の公式」と呼びます。

例えば、二次方程式 $ax^2 + bx + c = 0$ $(a \neq 0)$ の解の公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

は、まさしく代数的解法の典型例です。この公式は、係数である a, b, c に対して、四則演算と平方根 $\sqrt{}$ という操作のみで構成されています。

三次、四次方程式においても、解の公式はより複雑な形をしていますが、同様に四則演算とべき根のみで記述されることが 16 世紀に発見されました。ここから、数学者たちの関心は、一般の五次方程式、あるいはそれ以上の次数の代数方程式においても、同様の代数的解法が存在するのか、という問題に向けられました。

この問いに答えるため、ガロア理論ではこの「代数的解法」という概念を、より厳密な数学の言葉で捉え直すことから始めます。それが次節以降で解説する「体」とその「拡大」という概念です。

1.2　体と係数体

前節で述べた「代数的解法」を厳密に議論するためには、計算の「舞台」となる数の集合を明確に定義する必要があります。例えば、有理数、実数、複素数といった数の世界は、いずれもその中で四則演算が自由に行えるという共通の性質を持っています。数学では、このような計算体系を**体（たい）**と呼びます。

定義 1.1：体 (Field)

集合 K が**体**であるとは、K に和「$+$」と積「$\cdot$」の 2 つの演算が定義されており、以下の性質がすべて満たされる代数構造のことをいいます。

1. **和について：** K のどの元 a, b に対しても $a + b$ が定まり、自由に足し算・引き算ができる（専門的には、集合 K は和についてアーベル群をなします）。
2. **積について：** K の 0 でないどの元 a, b に対しても $a \cdot b$ が定まり、自由に掛け算・割り算ができる（専門的には、K から 0 を除いた集合 $K \setminus \{0\}$ は積についてアーベル群をなします）。
3. **分配法則：** K のどの元 a, b, c に対しても、$a \cdot (b + c) = a \cdot b + a \cdot c$ が成り立ちます。

簡単に言えば、「**四則演算が矛盾なく自由に行える数の集合**」が体であると考えて構いま

せん。

補足：体の例と、体でない例

- **体の例:** 有理数全体の集合 $\mathbb{Q}$、実数全体の集合 $\mathbb{R}$、複素数全体の集合 $\mathbb{C}$ は、いずれも体の代表例です。
- **体でない例:** 整数全体の集合 $\mathbb{Z}$ は体ではありません。なぜなら、掛け算の逆演算である割り算が自由にできないためです。例えば、$2 \in \mathbb{Z}$ ですが、その積に関する逆元である $1/2$ は $\mathbb{Z}$ の元ではありません。

代数方程式を考える際、私たちはまず、その方程式の係数がすべて含まれている体を考えます。これを**係数体（けいすうたい）**と呼びます。係数体は、方程式の解を探す旅の「出発点」となる基準の世界です。

例えば、方程式 $x^2 - x - 1 = 0$ の係数は $1, -1$ であり、これらはすべて有理数です。したがって、この方程式を考える上での自然な係数体は、有理数体 $\mathbb{Q}$ となります。方程式の解 $\frac{1 \pm \sqrt{5}}{2}$ は $\mathbb{Q}$ の中には存在しませんが、係数体 $\mathbb{Q}$ は解を探索するための基盤となります。

1.3 体の拡大

多くの場合、ある体に係数を持つ方程式の解は、その体の中には存在しません。例えば、有理数体 $\mathbb{Q}$ を係数体とする二次方程式

$$x^2 - 2 = 0$$

を考えます。この方程式の解は $x = \pm\sqrt{2}$ ですが、これらの解は係数体である $\mathbb{Q}$ の元ではありません。

この解を扱うためには、計算の舞台である $\mathbb{Q}$ を、$\sqrt{2}$ を含むより大きな体に「広げる」必要があります。この新しい体は、$\mathbb{Q}$ のすべての元と $\sqrt{2}$ を含み、かつそれ自身も体、すなわち四則演算について閉じていなければなりません。結果として、この新しい体は

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

という形の数全体の集合となります。このように、ある体により大きな体を構成することを、体の**拡大**と呼びます。

定義 1.2：体の拡大 (Field Extension)

ある体 K が、より大きな体 L の部分集合であり、かつ K と L の演算が（K の元に対しては）一致するとき、K は L の**部分体**（subfield）である、または L は K の**拡大体**（extension field）であるといいます。この関係を、体の**拡大**と呼び、L/K と表記します。

$\mathbb{Q}(\sqrt{2})$ は、体 $\mathbb{Q}$ に元 $\sqrt{2}$ を**添加（てんか）**して得られる最小の拡大体です。同様に、方程式 $x^2 + 1 = 0$ の解 $i = \sqrt{-1}$ は実数体 $\mathbb{R}$ には含まれませんが、$\mathbb{R}$ に i を添加することで、すべての複素数を含む体 $\mathbb{C} = \mathbb{R}(i)$ へと拡大されます。

重要：代数的解法と体の拡大

「方程式をべき根で解く」という操作は、「係数体 K から出発し、べき根を次々と添加して体を拡大していく」という一連のプロセスとして正確に捉え直すことができます。

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

ここで、各ステップ K_{i+1} は、K_i の元にべき根を添加することで作られます。そして、最終的な拡大体 K_m が方程式のすべての解を含むとき、その方程式はべき根で解けたことになります。
したがって、代数的解法の存在問題は、**「このような体の拡大の列を構成できるか」**という、体の構造に関する問題へと置き換えられます。ガロア理論は、この体の拡大の構造を「群」という道具を用いて解析します。

2　対称性を記述する言語：群

2.1　置換とその集まり

体の拡大の構造を調べるための鍵となるのが「群」という代数構造です。群の概念を理解するために、まずはその最も代表的な例である**置換（ちかん）**から始めます。

単純な例として、3 つの数字 $\{1, 2, 3\}$ の並べ替えを考えます。この並べ替え、すなわち「n 個のものを 1 列に並べる順序を入れ替える操作」を**置換**と呼びます。例えば、「1 と 2 を入れ替える」という置換は、写像として

$$\sigma : \{1, 2, 3\} \to \{1, 2, 3\}, \quad \sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$$

と表すことができます。この置換は、元の要素と移動先の要素を上下に並べて

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

と表記したり、あるいはより簡潔に、数の動きを追跡する**巡回置換記法**を用いて $\sigma = (1\ 2)$ と表記します。これは「1 は 2 へ、2 は 1 へ移り、3 は不変である」ことを意味します。

3 つの数字 $\{1, 2, 3\}$ の置換は、全部で $3! = 6$ 通り存在します。これらを巡回置換記法で書き出すと以下のようになります。

- $e = (1)(2)(3)$: 何も動かさない置換（恒等置換）。
- $(1\ 2)$: 1 と 2 を入れ替える置換。
- $(1\ 3)$: 1 と 3 を入れ替える置換。
- $(2\ 3)$: 2 と 3 を入れ替える置換。
- $(1\ 2\ 3)$: 1 を 2 へ、2 を 3 へ、3 を 1 へ動かす置換。
- $(1\ 3\ 2)$: 1 を 3 へ、3 を 2 へ、2 を 1 へ動かす置換。

重要：置換の積

置換の最も重要な性質は、2 つの置換を続けて行う操作（**合成**）を考えられる点です。これを置換の**積**と呼びます。例えば、$\sigma = (1\ 2)$ と $\tau = (1\ 3)$ の積 $\sigma \circ \tau$ を考えてみましょう。（操作は右から左へ順に行います。）

- $1 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 3$
- $3 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2$
- $2 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 1$

結果として、この操作は「1 を 3 へ、3 を 2 へ、2 を 1 へ」と動かす置換となり、これは $(1\ 3\ 2)$ と一致します。つまり、$(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ となります。

この「3 つのものの置換」全体の集まりは、置換の積という演算について、非常に良い性質を持っていることがわかります。

1. **閉じている:** どの 2 つの置換の積も、また別の置換になっています。
2. **単位元の存在:** 何も動かさない置換 e が存在し、どの置換と積をとっても相手を変えません。
3. **逆元の存在:** どの置換に対しても、その操作を元に戻す「逆の置換」が存在します。例えば、$(1\ 2\ 3)$ の逆の操作は $(1\ 3\ 2)$ です。

このように、ある操作の集まりが演算についてなす、閉じた安定的なシステム。これが次節で定義する「群」の基本的なイメージです。

2.2 群の定義

前節で見た置換の集まりが持つ性質は、数学の様々な場面に現れる非常に普遍的な構造です。数学では、このような構造を抽象化し、**群（ぐん）**と呼びます。

定義 2.1：群 (Group)

集合 G と、その上の二項演算 $\circ$ の組 $(G, \circ)$ が**群**であるとは、以下の 3 つの公理を満たすことをいいます。

1. **結合法則 (Associativity):** G の任意の元 a, b, c に対して、次の式が成り立つ。
$$(a \circ b) \circ c = a \circ (b \circ c)$$
2. **単位元の存在 (Identity element):** G のすべての元 a に対して、次の式を満たす特別な元 $e \in G$ が存在する。この e を**単位元**と呼ぶ。
$$e \circ a = a \circ e = a$$
3. **逆元の存在 (Inverse element):** G の各元 a に対して、次の式を満たす元 $a^{-1} \in G$

が必ず存在する。この a^{-1} を a の**逆元**と呼ぶ。

$$a \circ a^{-1} = a^{-1} \circ a = e$$

補足：置換のなす群

前節で考えた n 個のものの置換全体の集合は、演算として置換の合成を考えると、群の公理をすべて満たします。この群を n **次対称群** と呼び、S_n と表記します。S_n の要素の総数（群の**位数**といいます）は $n!$ です。例えば、$\{1, 2, 3\}$ の置換の集まりは、位数 $3! = 6$ の 3 次対称群 S_3 となります。

群の定義では、演算の順序を交換できるか、すなわち $a \circ b = b \circ a$ が成り立つかどうかは問われていません。この交換法則が成り立つ群は、特別な名前で呼ばれます。

定義 2.2：アーベル群 (Abelian Group)

群 $(G, \circ)$ が、その任意の元 a, b について交換法則

$$a \circ b = b \circ a$$

を満たすとき、この群を**アーベル群**（または**可換群**）と呼びます。

整数全体の集合 $\mathbb{Z}$ は、和を演算としてアーベル群をなします。しかし、対称群 S_n は $n \geq 3$ のとき、アーベル群では**ありません**。例えば S_3 において、前節で見たように $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ でしたが、逆の順で計算すると

$$(1\ 3) \circ (1\ 2) = (1\ 2\ 3)$$

となり、結果が一致しません。このような群を**非可換群**と呼びます。この**可換か非可換か**という性質の違いが、ガロア理論において極めて重要な役割を果たします。

2.3 対称群と部分群

ガロア理論において中心的な役割を果たすのが、前節で導入した対称群 S_n です。S_n は n 個の対象の間のすべての置換を元としており、その意味で n 個のものが持ちうる最大限の「対称性」を表現する群と考えることができます。後の章で見るように、一般の n 次代数方程式の「対称性」を表現するのは、まさにこの n 次対称群 S_n なのです。

さて、ある大きな群の構造を詳しく調べるために、その中に含まれる小さな群に着目するという手法が有効です。これを**部分群**の概念として定式化します。

定義 2.3：部分群 (Subgroup)

群 $(G, \circ)$ の空でない部分集合 H が、G と同じ演算 $\circ$ によってそれ自身も群となるとき、H を G の**部分群**であるといいます。

部分群であるためには、部分集合 H が以下の条件を満たす必要があります。

1. **演算について閉じている:** H の任意の元 a, b に対して、$a \circ b$ も H の元でなければなりません。
2. **単位元を含む:** G の単位元 e は、H の元でなければなりません。
3. **逆元について閉じている:** H の任意の元 a に対して、その逆元 a^{-1} も H の元でなければなりません。

例：S_3 の部分群

位数 6 の対称群 $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ を考えます。この S_3 は、自明な部分群（$\{e\}$ と S_3 自身）の他に、以下のような部分群を持ちます。

- $H_1 = \{e, (1\ 2)\}$
- $H_2 = \{e, (1\ 3)\}$
- $H_3 = \{e, (2\ 3)\}$
- $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

例えば、A_3 が部分群であることを確認してみましょう。$(1\,2\,3) \circ (1\,3\,2) = e$、$(1\,2\,3) \circ (1\,2\,3) = (1\ 3\ 2)$ など、どの 2 つの元の積も A_3 の中に収まっており、単位元を含み、各元の逆元も A_3 の中に存在します。この A_3 は **3 次交代群**と呼ばれ、S_3 の中で特に重要な役割を担います。
一方で、例えば $K = \{e, (1\,2), (1\,3)\}$ は S_3 の部分群では**ありません**。なぜなら、$(1\,2) \circ (1\,3) = (1\ 3\ 2)$ となりますが、この元は K に含まれていないため、演算について閉じていないからです。

このように、群の部分群をすべてリストアップすることで、その群がどのような「部品」から構成されているのか、その内部構造を明らかにすることができます。次節では、部分群の中でも特に「良い」性質を持つ**正規部分群**について学びます。これは、群をより単純な要素に「分解」するための鍵となります。

2.4 正規部分群と剰余群

群の構造を解析する上で、部分群の中でも特に重要な役割を担うのが**正規部分群（せいきぶぶんぐん）**です。正規部分群は、群をより単純な構成要素に「分解」することを可能にする、いわば「良い」部分群です。

正規部分群を定義するために、まず**剰余類（じょうよるい）**という概念を導入します。

定義 2.4：剰余類 (Coset)

群 G とその部分群 H が与えられたとき、G の任意の元 g に対して、部分集合

$$gH = \{gh \mid h \in H\}$$

を、g を代表元とする H の**左剰余類**と呼びます。同様に、$Hg = \{hg \mid h \in H\}$ を**右剰余類**と呼びます。

一般に、左剰余類 gH と右剰余類 Hg は一致するとは限りません。例えば、$G = S_3$ とその部分群 $H = \{e, (1\ 2)\}$ を考えます。$g = (1\ 3)$ をとると、

- 左剰余類: $(1\ 3)H = \{(1\ 3)e, (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$
- 右剰余類: $H(1\ 3) = \{e(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}$

となり、$(1\ 3)H \neq H(1\ 3)$ です。しかし、部分群によっては、どの元 g をとっても常に $gH = Hg$ が成り立つ場合があります。このような特別な部分群が正規部分群です。

定義 2.5：正規部分群 (Normal Subgroup)

群 G の部分群 N が、任意の $g \in G$ に対して

$$gN = Ng$$

を満たすとき、N は G の**正規部分群**であるといいます。これは、任意の $g \in G$ と任意の $n \in N$ に対して、gng^{-1} が再び N の元となることと同値です。

例えば、S_3 の部分群 $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ は、S_3 の正規部分群であることが確認できます。

重要：剰余群（商群）

正規部分群が重要なのは、それが「**剰余群（じょうよぐん）**」または「**商群（しょうぐん）**」と呼ばれる新しい群を構成する土台となるからです。
群 G とその正規部分群 N があるとき、その剰余類全体の集合

$$G/N = \{gN \mid g \in G\}$$

には、自然な形で群の構造を入れることができます。演算を

$$(aN) \circ (bN) = (ab)N$$

と定義すると、この演算によって G/N は群となります。この群を G の N による**剰余群**と呼びます。この演算が矛盾なく定義できるのは、N が正規部分群であるとき、またそのときに限られます。

剰余群 G/N を考えることは、群 G の構造を、正規部分群 N の構造と、より位数の小さな剰余群 G/N の構造に「分解」して調べることに対応します。この「**群の分解**」という考え方が、方程式が「解ける」とはどういうことかを、群の言葉で明らかにするための鍵となるのです。

例：S_3 における正規部分群と非正規部分群の比較

対称群 S_3 を用いて、正規部分群であるものとそうでないものの違いを具体的に見てみましょう。

1. **正規部分群の例：$N = A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$**

A_3 が S_3 の正規部分群であることを示すには、任意の $g \in S_3$ と任意の $n \in A_3$ に対して、gng^{-1} が再び A_3 の元となることを確認します。例えば、$g = (1\ 2)$ を選んでみましょう（$g^{-1} = (1\ 2)$ です）。

- $n = e$ のとき: $(1\ 2)e(1\ 2)^{-1} = e \in A_3$
- $n = (1\ 2\ 3)$ のとき: $(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) \in A_3$
- $n = (1\ 3\ 2)$ のとき: $(1\ 2)(1\ 3\ 2)(1\ 2)^{-1} = (1\ 2)(1\ 3\ 2)(1\ 2) = (1\ 2\ 3) \in A_3$

他のどの $g \in S_3$ を選んで計算しても、結果は必ず A_3 の中に収まります。この性質により、S_3 を剰余類 A_3 と $(1\ 2)A_3$ に「分解」し、それらを元とする位数 2 の剰余群 S_3/A_3 を考えることができるのです。

2. **正規部分群ではない例：$H = \{e, (1\ 2)\}$**

次に、部分群 $H = \{e, (1\ 2)\}$ が正規部分群では**ない**ことを見てみましょう。正規部分群ではないことを示すには、gng^{-1} が H の元にならないような例を一つ見つければ十分です。ここでは、$g = (1\ 3)$ を選んでみましょう（$g^{-1} = (1\ 3)$ です）。H の元として $n = (1\ 2)$ をとります。

$$gng^{-1} = (1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3)$$

計算の結果 $(2\ 3)$ は、もとの部分群 $H = \{e, (1\ 2)\}$ の元では**ありません**。したがって、H は S_3 の正規部分群ではないと結論できます。

この場合、左剰余類と右剰余類が一致しないため（例えば $(1\ 3)H \neq H(1\ 3)$）、剰余類の集合 S_3/H の上に矛盾なく演算を定義することができず、剰余群を構成することはできません。

このように、正規部分群は、群を構成要素（自身と剰余群）に分解することを許す、非常に「素性の良い」特別な部分群なのです。

第 I 部

ガロア理論の核心

3　体の拡大を司る群：ガロア群

3.1　体の自己同型写像

これまでの章で、体の拡大と群という 2 つの基本的な代数構造を学びました。いよいよ、この 2 つの構造を結びつけるガロア理論の中心的な概念を導入します。その鍵となるのが、体の「対称性」を捉える**自己同型写像**です。

代数学では、ある数学的構造（この場合は体の構造）を保つような写像（関数）を考えることが非常に重要です。体の構造とは、和と積の演算によって定まっています。

定義 3.1：体の自己同型写像 (Field Automorphism)

体 L からそれ自身への全単射な写像 $\sigma : L \to L$ が、任意の元 $a, b \in L$ に対して、

1. **和を保つ:** $\sigma(a+b) = \sigma(a) + \sigma(b)$
2. **積を保つ:** $\sigma(ab) = \sigma(a)\sigma(b)$

という 2 つの条件を満たすとき、σ を L の**自己同型写像**と呼びます。

自己同型写像とは、体の演算構造を一切壊すことなく、元を入れ替える操作と考えることができます。

例：複素数体の自己同型写像

複素数体 $\mathbb{C}$ を考えます。複素共役をとる写像 $\sigma : \mathbb{C} \to \mathbb{C}$ を

$$\sigma(a+bi) = a - bi \quad (a, b \in \mathbb{R})$$

と定義します。この写像 σ は、和と積の構造を保つため、$\mathbb{C}$ の自己同型写像です。例えば、σ は実数 $a \in \mathbb{R}$ を不変に保ちますが（$\sigma(a) = a$）、虚数 i は $-i$ に移します。

ガロア理論で特に重要となるのは、体の拡大 L/K を考えたときに、L の自己同型写像の中でも、基礎体 K の元を「固定」する、つまり動かさないような写像です。

定義 3.2：K-自己同型写像 (K-automorphism)

体の拡大 L/K が与えられたとき、L の自己同型写像 σ が、基礎体 K のすべての元 k に対して

$$\sigma(k) = k$$

を満たすとき、σ を L の **K-自己同型写像**と呼びます。

K-自己同型写像は、基礎体 K の世界には何の変化も与えず、その拡大体 L の元だけを入れ替える可能性のある「許された操作」と解釈できます。例えば、体の拡大 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ を考えましょう。写像 $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$ は、$\mathbb{Q}(\sqrt{2})$ の自己同型写像です。この写像は、任意の有理数 $q \in \mathbb{Q}$ に対して $\sigma(q) = q$ を満たすため、$\mathbb{Q}$-自己同型写像です。この写像は、$\sqrt{2}$ を $-\sqrt{2}$ へと、つまり方程式 $x^2 - 2 = 0$ の一つの解をもう一つの解へと移しています。

次節では、この K-自己同型写像の全体が集まって「群」をなすことを見ます。それこそが、ガロア理論の主役であるガロア群です。

3.2　ガロア群の定義

前節で定義した K-自己同型写像は、体の拡大 L/K における「対称性」を捉える操作でした。ここでの重要な事実は、ある体の拡大 L/K における K-自己同型写像の**全体**を集めると、写像の合成を演算として、それ自身が**群をなす**ということです。

この集合が群の公理を満たすことを確認してみましょう。L/K の K-自己同型写像の集合を G とします。

1. **演算について閉じている:** $\sigma, \tau \in G$ とすると、その合成 $\sigma \circ \tau$ もまた、L の自己同型写像であり、かつ K の元を不変に保つため、$\sigma \circ \tau \in G$ となります。
2. **結合法則:** 写像の合成は、一般に結合法則 $(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$ を満たします。
3. **単位元の存在:** 恒等写像 $\mathrm{id}(x) = x$ は、明らかに K-自己同型写像であり、単位元として機能します。
4. **逆元の存在:** 各 $\sigma \in G$ は全単射なので逆写像 σ^{-1} が存在します。この σ^{-1} もまた K-自己同型写像となることが示せます。

したがって、K-自己同型写像の集合は、群としての条件をすべて満たします。この群こそがガロア群です。

定義 3.3：ガロア群 (Galois Group)

体の拡大 L/K が与えられたとき、L の K-自己同型写像の全体がなす群を、拡大 L/K の**ガロア群**といい、$Gal(L/K)$ と書く。

この定義を、私たちの本来の目的である代数方程式に適用します。ある体 K に係数を持つ多項式 $f(x)$ を考えます。このとき、$f(x)$ のすべての根を含むような K の最小の拡大体を、$f(x)$ の**分解体（ぶんかいたい）**と呼びます。

定義 3.4：方程式のガロア群

K に係数を持つ方程式 $f(x) = 0$ の**ガロア群**とは、その分解体を L としたときの、ガロア群 $Gal(L/K)$ のことを指す。

ガロア群の基本性質

方程式 $f(x) = 0$ のガロア群の各元 σ は、その方程式の根を、別の根へと移します。つまり、α が $f(x) = 0$ の一つの根であれば、$\sigma(\alpha)$ もまた $f(x) = 0$ の根となるのです。
これは、σ が係数体 K の元を不変にすることから証明できます。ガロア群とは、いわば**「方程式の根の入れ替えで、係数体の構造と両立するようなもの」**全体の集まりなのです。
これにより、方程式の根が持つ対称性は、ガロア群という群の構造として完全に捉えることができます。

3.3 例題：ガロア群の計算

ガロア群の定義をより深く理解するために、いくつかの具体的な体の拡大についてガロア群を計算してみましょう。

例題 1：$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$

体の拡大 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ を考えます。これは、$\mathbb{Q}$ に係数を持つ方程式 $x^2 - 2 = 0$ の分解体です。この拡大のガロア群 $G = Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ を求めます。
G の元である $\mathbb{Q}$-自己同型写像を σ とします。$\mathbb{Q}(\sqrt{2})$ の任意の元は $a + b\sqrt{2}$ $(a, b \in \mathbb{Q})$ と書けます。σ は $\mathbb{Q}$ の元を不変に保つので、$\sigma(a) = a$, $\sigma(b) = b$ です。したがって、

$$\sigma(a + b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a + b\sigma(\sqrt{2})$$

となり、σ の行き先は $\sigma(\sqrt{2})$ の値だけで完全に決まります。
ガロア群の元は方程式の根を根に移すので、$\sigma(\sqrt{2})$ は $x^2 - 2 = 0$ の根、すなわち $\sqrt{2}$ または $-\sqrt{2}$ のどちらかでなければなりません。

1. $\sigma(\sqrt{2}) = \sqrt{2}$ **の場合：** このとき、$\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$ となります。これは恒等写像 id です。
2. $\sigma(\sqrt{2}) = -\sqrt{2}$ **の場合：** このとき、$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ となります。この写像を τ とおきます。

以上より、K-自己同型写像は id と τ の 2 つしか存在しません。よって、ガロア群は $G = \{\mathrm{id}, \tau\}$ となります。この群は位数が 2 であり、演算は $\tau \circ \tau = \mathrm{id}$ となるため、位数 2 の巡回群（C_2 と表記される）と同型です。

例題 2：$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

次に、もう少し複雑な例として、体の拡大 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ を考えます。これは、$\mathbb{Q}$ に係数を持つ方程式 $(x^2 - 2)(x^2 - 3) = 0$ の分解体です。このガロア群 $G = Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ を求めます。

$\mathbb{Q}$-自己同型写像 σ は、$\sigma(\sqrt{2})$ と $\sigma(\sqrt{3})$ の値によって完全に決まります。

- $\sigma(\sqrt{2})$ は $x^2-2=0$ の根なので、$\pm\sqrt{2}$ のどちらかです。
- $\sigma(\sqrt{3})$ は $x^2-3=0$ の根なので、$\pm\sqrt{3}$ のどちらかです。

これらの組み合わせから、以下の 4 つの異なる自己同型写像が得られます。

1. σ_1: $\sigma_1(\sqrt{2})=\sqrt{2}$, $\sigma_1(\sqrt{3})=\sqrt{3}$（恒等写像 id）
2. σ_2: $\sigma_2(\sqrt{2})=-\sqrt{2}$, $\sigma_2(\sqrt{3})=\sqrt{3}$
3. σ_3: $\sigma_3(\sqrt{2})=\sqrt{2}$, $\sigma_3(\sqrt{3})=-\sqrt{3}$
4. σ_4: $\sigma_4(\sqrt{2})=-\sqrt{2}$, $\sigma_4(\sqrt{3})=-\sqrt{3}$

したがって、ガロア群 $G=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ は位数 4 の群となります。この群のすべての元（単位元を除く）は、2 回合成すると単位元に戻る（$\sigma_2^2=\sigma_3^2=\sigma_4^2=\mathrm{id}$）という性質を持っています。これは位数 4 の巡回群 C_4 ではなく、**クラインの四元群** V_4 と呼ばれるアーベル群と同型です。

これらの例から、体の拡大の様子が、ガロア群という有限群の構造に反映されていることが見て取れます。次の章では、この対応関係を一般化するガロアの基本定理を学びます。

補足：ガロア群の本質 ―「区別できない」元の入れ替え

ガロア群がなぜ体の「対称性」を捉えるのか、その本質を直観的に理解するための一つの視点があります。それは、**「係数体の立場からは区別できない元を、入れ替える操作」**としてガロア群を捉える考え方です。

一番わかりやすい例は、実数体 $\mathbb{R}$ を係数体とする方程式 $x^2+1=0$ です。この方程式の解は、ご存知の通り i と $-i$ です。

さて、**実数 $\mathbb{R}$ の世界だけを使って、i と $-i$ を区別することができるでしょうか？** i の定義は「2 乗して-1 になる数」ですが、この性質は $-i$ も同様に満たします。どちらも代数方程式の解を満たすという点で実数係数の多項式ではその違いを認識することができません。実数係数のどんな代数的な関係式（例えば $ax^3+bx+c=0$）でも、z がそれを満たすならば、必ずその共役である $\bar{z}$ もその関係式を満たします。つまり、z と $\bar{z}$ は、係数体 $\mathbb{R}$ の立場からは「代数的に区別がつかない」存在なのです。

この「区別のできなさ」こそが、対称性の源泉です。体の拡大 $\mathbb{C}/\mathbb{R}$ におけるガロア群 $Gal(\mathbb{C}/\mathbb{R})$ の非自明な元は、複素共役をとる写像 $\sigma(a+bi)=a-bi$ でした。この操作は、まさに「区別できない」i と $-i$ を入れ替える操作に他なりません。この入れ替えを行っても、基礎体である $\mathbb{R}$ の世界の法則（＝実数係数の関係式）は一切変わらないため、これは許された「内部対称性」となります。

この視点は、他の体の拡大にも適用できます。例えば、$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ のガロア群を考えます。有理数 $\mathbb{Q}$ の立場からは、$\sqrt{2}$ と $-\sqrt{2}$ はどちらも「2 乗して 2 になる数」であり、代数的に

区別できません。そして、$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ の非自明な元は、まさに $\sqrt{2}$ と $-\sqrt{2}$ を入れ替える操作でした。
このように、ガロア群とは、

係数体の視点からは区別できない解たちを入れ替える、
整合性を保った操作（対称性）の集まり

と見なすことができます。方程式を解く旅の中で生まれる「曖昧さ」そのものが、群という豊かな数学的構造をなしているのです。

4　ガロアの基本定理

前の章では、体の拡大 L/K に対して、ガロア群 $Gal(L/K)$ という群を対応させる方法を学びました。ガロア理論が革命的である理由は、この対応が単なる対応付けに留まらず、2 つの世界の「内部構造」の間に、驚くほど美しく、そして厳密な関係があることを見抜いた点にあります。その関係を完全に記述するのが、ガロア理論の頂点に輝く**ガロアの基本定理**です。

この章では、この定理の主張を一つずつ見ていきます。（※より厳密には、この定理は「有限次ガロア拡大」という良い性質を持つ体の拡大で成り立ちます。本書で扱う方程式の分解体は、すべてこの条件を満たすと考えて構いません。）

4.1　ガロア対応

ガロアの基本定理の核心は、体の拡大の構造とガロア群の構造が、鏡に映したかのように対応していることを主張する点にあります。具体的には、体の拡大 L/K の**中間体**と、ガロア群 $Gal(L/K)$ の**部分群**との間に、完璧な 1 対 1 の対応が存在するのです。

- **体の世界**: 体の拡大 L/K には、$K \subseteq M \subseteq L$ を満たすような「中間体 M」がいくつも存在する可能性があります。
- **群の世界**: ガロア群 $G = Gal(L/K)$ には、様々な「部分群 H」が存在します。

この 2 つの世界の対応関係は、以下のようにして得られます。

1. **中間体から部分群へ:** 中間体 M があるとき、その M の元をすべて不変にするようなガロア群の元を集めると、それは部分群をなします。これは $Gal(L/M)$ に他なりません。
2. **部分群から中間体へ:** 部分群 H があるとき、その H に属するすべての写像で不変に保たれるような L の元を集めると、それは中間体をなします。これを H の**固定体**と呼び、L^H と書きます。

この驚くべき事実は、これら 2 つの操作が互いに逆の関係にあり、中間体と部分群の間に完璧な対応を与えているということです。

ガロアの基本定理（その 1）：ガロア対応

体の拡大 L/K を有限次ガロア拡大とする。このとき、

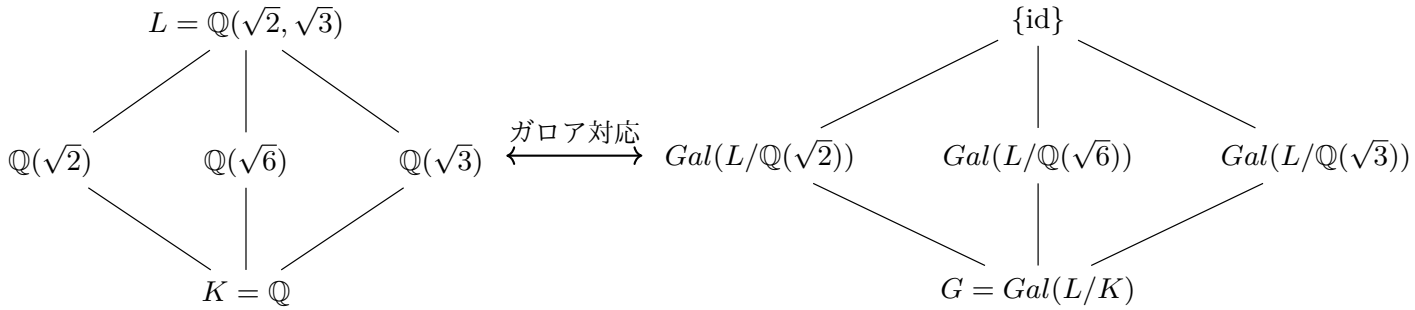
L/K の中間体の集合と、ガロア群 $Gal(L/K)$ の部分群の集合の間には、
上記の対応によって、1 対 1 の対応（全単射）が存在する。

この対応は**包含関係を逆転**させる。すなわち、中間体 M_1, M_2 とそれに対応する部分群 H_1, H_2 について、

$$M_1 \subseteq M_2 \quad \Longleftrightarrow \quad H_1 \supseteq H_2$$

が成り立つ。

この対応関係を**ガロア対応**と呼びます。$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/K = \mathbb{Q}$ の場合、この対応は以下の図のように可視化できます。左の「体の束」では、上へ行くほど体は大きくなります。一方、右の「群の束」では、上へ行くほど群は小さくなり、部分群は上にあります。体の拡大と群の縮小が対応しているのがわかります。



ガロア対応の発見により、中間体を探すという体の問題を、部分群を探すという群論の問題に完全に置き換えることができるようになりました。

4.2　定理の含意

前節で述べたガロア対応は、体の世界の「地図」と群の世界の「地図」が、包含関係を逆転させる形でぴったりと重なることを示しました。ガロアの基本定理は、さらに踏み込んで、この対応が量的にも質的にも完璧であることを明らかにします。

まず、体の拡大の「大きさ」である拡大次数と、群の「大きさ」である位数との間に、正確な関係が存在します。

ガロアの基本定理（その 2）：拡大次数と群の位数

体の拡大 L/K を有限次ガロア拡大とし、$G = Gal(L/K)$ とする。中間体 M と、それに対応する部分群 $H = Gal(L/M)$ について、それぞれの「大きさ」は以下の関係で結ばれる。

- 拡大 L/M の次数は、部分群 H の位数（元の個数）に等しい。

$$[L:M] = |H|$$

- 拡大 M/K の次数は、G における H の指数（$|G|/|H|$）に等しい。

$$[M:K] = [G:H]$$

ここで、体の拡大次数 $[L:M]$ は、体 L を体 M 上のベクトル空間と見なしたときの次元のことで、体の「大きさの比」のようなものです。この定理により、体の拡大の階層構造が、ガロア群の位数の関係に正確に反映されていることがわかります。

さらに、ガロアの基本定理で最も重要かつ深遠な部分が、部分群の中でも特別であった「正規部分群」に関する主張です。

ガロアの基本定理（その 3）：正規拡大と正規部分群

体の拡大 L/K を有限次ガロア拡大とし、$G = Gal(L/K)$ とする。中間体 M と、それに対応する部分群 H について、以下の 2 つの条件は**同値**である。

1. 部分群 H が、G の**正規部分群**である。
2. 中間体の拡大 M/K が、**正規拡大**である。

（※正規拡大とは、簡単に言えば、K に係数を持つ既約多項式が M 内に一つでも根を持つならば、そのすべての根が M 内に存在する、という性質を持つ「自己完結した」拡大のことです。）

さらに、この条件が成り立つとき、拡大 M/K のガロア群は、剰余群 G/H と同型になる。

$$Gal(M/K) \cong G/H$$

この最後の主張こそ、ガロア理論が方程式の可解性の問題を解決する上での核心部分です。体の拡大の「分解」（L/K を L/M と M/K に分ける）が、群の「分解」（G を H と G/H に分ける）と完璧に連動することを示しているからです。

これで、ガロア理論という強力な「辞書」が完成しました。この辞書を用いることで、次章以降、「方程式がべき根で解ける」という体の世界の言葉が、群の世界のどのような言葉に翻訳されるのかを解き明かしていきます。

第 II 部

五次方程式の非可解性の証明

5　べき根による可解性と可解群

これまでに、体の拡大の構造とガロア群の構造を結びつける「ガロアの基本定理」という強力な道具を手に入れました。いよいよこの道具を使い、本書の主題である「代数方程式がべき根で解けるか」という問題を、群の言葉へと翻訳していきます。

5.1　べき根による拡大の性質

まず、「方程式がべき根で解ける」という言葉の意味を、体の拡大の言葉を用いて厳密に定義し直す必要があります。二次方程式の解の公式を思い出すと、その解は係数に四則演算とべき根 ($\sqrt{}$) を施すことで得られました。この操作を体の言葉で表現すると、「係数体から出発し、べき根を次々と添加して体を拡大していく」プロセスに対応します。この「べき根を繰り返し添加する拡大」を**累冪根拡大**と呼ぶことにします。

定義 5.1：べき根による可解性

体 K に係数を持つ方程式 $f(x) = 0$ が**べき根で解ける**（solvable by radicals）とは、$f(x) = 0$ のすべての解を含むような拡大体 L であって、K から L へ至る次のような体の列（**累冪根拡大**）が存在することをいいます。

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L$$

この体の列は、すべての $i = 0, \ldots, m-1$ について、

$$K_{i+1} = K_i(\alpha_i) \quad \text{ただし} \quad \alpha_i^{n_i} \in K_i \text{となる整数 } n_i > 0 \text{ が存在する}$$

という条件を満たします。各ステップは、前の体にその体の元のべき根を一つ添加する**冪根拡大**となっています。

この定義によって、解の公式の存在問題は、「係数体から出発して、その方程式の分解体を覆うような累冪根拡大を構成できるか」という、体の拡大に関する問題へと完全に言い換えられました。

では、この累冪根拡大の各ステップ、すなわち「冪根拡大」は、ガロア群の観点から見てどのような性質を持つのでしょうか。

冪根拡大とガロア群

体の拡大 L/K が、$L = K(\alpha)$ かつ $\alpha^n \in K$ と書ける単純な**冪根拡大**だとします。このような拡大のガロア群 $Gal(L/K)$ は、非常に「良い」性質を持ちます。

簡単のため、係数体 K が「1 の n 乗根」をすべて含んでいると仮定します。このとき、拡大 L/K のガロア群 $Gal(L/K)$ は、**アーベル群**（しかも巡回群）になることが証明されています。

この事実は極めて重要です。**「べき根で解ける」という条件を構成する基本的な部品（冪根拡大）が、ガロア群の世界では「アーベル群」という基本的な部品に対応していることを示唆している**からです。

このことから、次のような推論が成り立ちます。**もし方程式がべき根で解ける（＝累冪根拡大が存在する）ならば、ガロアの基本定理を通じて、その方程式のガロア群もまた、アーベル群を部品とするような、ある種の「分解可能」な構造を持っているはず**である、と。この「分解可能な群」こそが、次々節のテーマである**可解群**です。

5.2　累冪根拡大とガロア群

前節では、「方程式がべき根で解ける」ことを、体の「累冪根拡大」の存在として定義し直しました。では、この累冪根拡大の存在は、その方程式のガロア群の構造にどのような制約を課すのでしょうか。ここに、ガロアの基本定理が決定的な役割を果たします。

ガロアの基本定理によれば、体の拡大の列（塔）は、ガロア群の部分群の列（塔）に鏡写しのように対応します。累冪根拡大

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m$$

に対して、その分解体を覆う十分大きな拡大体のガロア群 $G = Gal(L/K)$ を考えると、対応する部分群の列が存在します。

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{\mathrm{id}\}$$

ここで、$H_i = Gal(L/K_i)$ であり、包含関係が逆転しています。

この群の列の性質を詳しく見てみましょう。累冪根拡大の各ステップ K_{i+1}/K_i は、ある元のべき根を添加する冪根拡大でした。このような拡大のガロア群 $Gal(K_{i+1}/K_i)$ は、（1 のべき根が十分に含まれているという条件下で）アーベル群になることを見ました。一方で、ガロアの基本定理（その 3）によれば、この拡大に対応する部分群の間の関係は、

$$Gal(K_{i+1}/K_i) \cong H_i/H_{i+1}$$

と表せます（※）。ただし、これは H_{i+1} が H_i の正規部分群である、という重要な条件の下で成り立ちます。累冪根拡大の各ステップが良い性質を持つことから、この正規性の条件も満たされるように拡大の塔を調整できることがわかります。

累冪根拡大とガロア群の分解可能性

以上の考察をまとめると、以下の極めて重要な関係が導かれます。
方程式がべき根で解ける（＝累冪根拡大が存在する）

$$\Updownarrow$$

その方程式のガロア群 G が、次のような部分群の列を持つ。

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{e\}$$

この列は、

1. 各 G_{i+1} は、G_i の**正規部分群**である（記号 $\rhd$ はこの意味を表す）。
2. 各剰余群 G_i/G_{i+1} は、すべて**アーベル群**である。

つまり、「べき根で解ける」という体の性質は、そのガロア群が「アーベル群を部品として、段階的に分解できる」という構造的な性質に、完全に翻訳されるのです。この特別な性質を持つ群こそが、次節で定義する**可解群**に他なりません。

（※厳密には、$Gal(K_{i+1}/K_i)$ は $Gal(L/K_i)/Gal(L/K_{i+1})$ すなわち H_i/H_{i+1} と同型になります。）

5.3　可解群の定義

前節の議論から、方程式がべき根で解けるという条件は、そのガロア群が「アーベル群を商群とする正規部分群の列に分解できる」という純粋に群論的な性質に置き換えられることがわかりました。この極めて重要な性質を持つ群は、その発見の経緯にちなんで、特別な名前で呼ばれています。

定義 5.2：可解群 (Solvable Group)

群 G が**可解群**であるとは、次の条件を満たす部分群の有限列（**可解列**）が存在することをいいます。

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{e\}$$

この列は、以下の 2 つの条件を満たさなければなりません。

1. 各 G_{i+1} は、G_i の**正規部分群**である（記号 $\rhd$ はこの意味を表します）。
2. 各剰余群 G_i/G_{i+1} は、すべて**アーベル群**である。

補足：「可解」という名前の由来

この群が「可解」群と呼ばれるのは、まさにこれが、代数方程式が「（べき根で）解ける」ための条件に由来するからです。方程式の可解性（solvability）が、そのガロア群のこの構造

的な性質（solvable-ness）と直結していることを、ガロアは突き止めました。

これまでの議論をすべて統合することで、私たちはついに、方程式論の問題を群論の問題へと完全に翻訳する、ガロア理論の金字塔と言うべき定理にたどり着きます。

定理 5.1：べき根による可解性のためのガロアの規準

ある代数方程式が**べき根で解ける**ための必要十分条件は、その方程式のガロア群が**可解群であること**である。

$$\text{方程式がべき根で解ける} \quad \Leftrightarrow \quad \text{そのガロア群が可解群である}$$

この定理は、私たちの長い旅における「ロゼッタストーン」です。これにより、何世紀にもわたる数学者たちの探求の末、解の公式の存在問題は、次のたった一つの問いに集約されることになりました。

最終的な問い

一般の五次方程式のガロア群は、五次対称群 S_5 であることが知られている。したがって、一般五次方程式に代数的な解の公式が存在するかどうかという問題は、

「五次対称群 S_5 は、可解群であるか？」

という、純粋な群論の問題と完全に同値になる。

もし S_5 が可解群ならば、解の公式は存在します。もしそうでなければ、存在しません。物語は、いよいよ最終章へ。次章では、この最後の問いに答えるべく、対称群 S_n の構造を調べ、なぜ $n = 5$ で状況が劇的に変化するのかを解き明かしていきます。

6　五次方程式のガロア群と非可解性

前章までの議論により、方程式の可解性は、そのガロア群が可解群であるか否か、という群論の問題に完全に帰着されました。本章では、この規準を用いて、五次方程式の非可解性を証明します。その第一歩として、まず「一般の」方程式のガロア群がどのような群になるのかを確定させる必要があります。

6.1　一般 n 次方程式のガロア群

これまで、$x^2 - 2 = 0$ のような、係数が具体的な数である方程式を考えてきました。しかし、私たちが問題にしている「解の公式」とは、どんな係数が与えられても適用できる万能な公式のことです。これを数学的に扱うためには、係数を具体的な数ではなく、互いに独立な変数（文字）とみなした**一般 n 次方程式**を考える必要があります。

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

このとき、係数体は $a_1, \ldots, a_n$ を変数として含む有理関数の体 $K = \mathbb{Q}(a_1, \ldots, a_n)$ となります。

では、この一般 n 次方程式のガロア群はどのような群になるのでしょうか。結論は、次の非常に重要な定理によって与えられます。

定理 6.1：一般 n 次方程式のガロア群

一般の n 次代数方程式のガロア群は、**n 次対称群** S_n と同型である。

この定理が成り立つ理由は、直観的には次のように理解できます。ガロア群の元は、方程式の n 個の根 $\alpha_1, \ldots, \alpha_n$ の置換（入れ替え）でした。もし方程式の係数が具体的な数であれば、根の間に何らかの特別な代数的関係式が成立している可能性があり、許される置換が制限されることがあります。例えば、$x^4 - 1 = 0$ の根 $\{1, -1, i, -i\}$ の間には $1 + (-1) = 0$ といった関係があるため、どんな置換でも許されるわけではなく、ガロア群は S_4 より小さな部分群となります。

しかし、**一般**方程式では、係数は互いに何の関係もない独立な変数です。そのため、その根の間にも、あらかじめ定められた特別な代数的関係は一切存在しません。根たちは、いわば「最も自由な」状態にあります。したがって、根たちの間のいかなる置換も、係数体の構造とは矛盾せず、すべてが許された対称性となります。その結果、ガロア群はすべての置換を含む群、すなわち対称群 S_n 全体となるのです。

結論

この定理により、私たちが解明すべき各次数の一般方程式のガロア群が確定します。

- 一般二次方程式のガロア群は S_2
- 一般三次方程式のガロア群は S_3
- 一般四次方程式のガロア群は S_4
- **一般五次方程式のガロア群は** S_5

これで、前章の「最終的な問い」の前提が完全に正当化されました。一般五次方程式がべき根で解けるかどうかは、まさしく「対称群 S_5 が可解群であるか」という問いに懸かっているのです。

6.2　対称群 S_n $(n \leq 4)$ の構造

前節で、一般の n 次方程式のガロア群が n 次対称群 S_n であることを見ました。そして、方程式がべき根で解けるための条件は、そのガロア群が「可解群」であることでした。二次、三次、四次方程式には解の公式が存在することがわかっているので、そのガロア群である S_2, S_3, S_4 は、すべて可解群でなければなりません。本節では、それが実際に正しいことを、可解群の定義に沿って確認してみましょう。

S_2 の可解性

$S_2 = \{e, (1\ 2)\}$ は位数が 2 の群です。この群は、元の演算が可換（$e \circ (1\ 2) = (1\ 2) \circ e$）であるため、アーベル群です。したがって、可解列として

$$S_2 \rhd \{e\}$$

を考えれば、剰余群 $S_2/\{e\} \cong S_2$ はアーベル群なので、定義より S_2 **は可解群**です。

S_3 の可解性

S_3 は位数 6 の非可換群ですが、その中には正規部分群が存在しました。特に重要なのが、位数 3 の**交代群** A_3 です。

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

A_3 は S_3 の正規部分群であり（部分群の指数が 2 なので正規部分群）、これを用いて次の可解列を構成できます。

$$S_3 \rhd A_3 \rhd \{e\}$$

この列が可解列の条件を満たすか確認します。

1. S_3/A_3: この剰余群の位数は $|S_3|/|A_3| = 6/3 = 2$ です。位数が 2 の群は必ずアーベル群です。
2. $A_3/\{e\}$: この剰余群は A_3 そのものです。A_3 は位数 3 の巡回群であり、アーベル群です。

すべての剰余群がアーベル群なので、S_3 **は可解群**です。

S_4 の可解性

S_4 は位数 24 の、さらに複雑な非可換群です。しかし、これもまた可解群であることが示せます。S_4 は、位数 12 の交代群 A_4 を正規部分群として持ちます。さらに、A_4 は、位数 4 の**クラインの四元群** V_4 と呼ばれる正規部分群を持ちます。

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

V_4 自身はアーベル群であり、さらに位数 2 の正規部分群（例えば $H = \{e, (1\ 2)(3\ 4)\}$）を持ちます。これにより、次のような正規部分群の列（可解列）を構成できます。

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

この列の各剰余群の位数を計算すると、$|S_4/A_4| = 2$, $|A_4/V_4| = 3$, $|V_4/H| = 2$, $|H/\{e\}| = 2$ となり、これらはすべて素数位数なので、各剰余群は巡回群、すなわちアーベル群です。したがって、S_4 **も可解群**であることが結論付けられます。

ここまでの結論

二次、三次、四次の一般方程式に解の公式が存在するという事実は、それらのガロア群である S_2, S_3, S_4 がすべて可解群であるという群論的な事実と、完璧に対応しています。
残る問題はただ一つ。この構造は、$n = 5$ の場合にも続くのでしょうか？ 対称群 S_5 の構造は、果たして S_4 までと同じように「分解可能」なのでしょうか。

6.3 交代群 A_n と単純群

前節では、S_2, S_3, S_4 がすべて可解群であることを確認しました。その証明の鍵となったのは、いずれの場合も対称群 S_n が、その正規部分群である**交代群** A_n を持っていたことです。（※交代群 A_n は、偶数回の互換で書ける置換のみを集めたもので、位数 $n!/2$ の S_n の正規部分群です。）

可解性の議論は、まず $S_n \triangleright A_n$ という分解から始まります。剰余群 S_n/A_n の位数は常に 2 なので、この部分は必ずアーベル群になります。したがって、S_n が可解群であるかどうかは、次のステップ、すなわち**「交代群 A_n 自身が可解群であるか」**という問題に完全に依存します。

$n = 3, 4$ の場合、A_3, A_4 は可解群でした。では、$n = 5$ の場合はどうでしょうか。A_5 の構造を調べると、私たちは驚くべき壁に突き当たります。その壁を理解するために、群論における「原子」の概念を導入します。

定義 6.1：単純群 (Simple Group)

群 G が、自明な部分群（$\{e\}$ と G 自身）以外に**正規部分群を一切持たない**とき、その群を**単純群**と呼びます。

単純群は、剰余群によってそれ以上分解することができない、群の世界の基本的な構成要素です。可解群が「分解できる群」であるならば、単純群はまさしくその対極にある「**分解不可能な群**」なのです。

そして、ここですべての状況を一変させる、群論における非常に深く、重要な定理が登場します。

定理 6.2：交代群の単純性

交代群 A_n は、$n = 5$ 以上のとき、**単純群**である。

この定理が、五次方程式が解けないことの数学的な核心です。$n = 5$ の場合、A_5（位数は $5!/2 = 60$）は単純群となります。これが A_5 の可解性に与える影響を見てみましょう。

A_5 が可解群であるためには、$A_5 \triangleright G_1 \triangleright \dots$ という可解列が存在しなければなりません。しかし、A_5 は単純群なので、その正規部分群 G_1 として考えられるのは $\{e\}$ のみです。すると、可解列の最初のステップは $A_5 \triangleright \{e\}$ となります。この剰余群は $A_5/\{e\} \cong A_5$ です。したがって、A_5 が可解であるためには、この剰余群 A_5 自身がアーベル群でなければなりません。

しかし、A_5 はアーベル群では**ありません**。例えば、(1 2 3) と (3 4 5) はどちらも A_5 の元で

すが、

$$(1\ 2\ 3) \circ (3\ 4\ 5) \neq (3\ 4\ 5) \circ (1\ 2\ 3)$$

となり、積は非可換です。

結論

1. A_5 は単純群であるため、その正規部分群は $\{e\}$ と A_5 しか存在しない。
2. 可解性の条件から剰余群 $A_5/\{e\} \cong A_5$ を考える必要があるが、これはアーベル群ではない。

したがって、**交代群 A_5 は可解群ではない**と結論付けられます。

$n = 4$ までは続いていた「分解可能」な構造は、$n = 5$ で現れるこの「分解不可能な非可換単純群」A_5 によって、完全に断ち切られてしまうのです。

補足：なぜ A_5 は分解できないのか？ ―単純群の本質

「A_n は $n \geq 5$ で単純群である」という定理は、なぜ五次方程式が解けないのか、その理由の核心です。ここでは、なぜ A_4 は分解できて、A_5 は分解できないのか、その構造的な違いを直観的に見てみましょう。

群の分解を阻む「共役」という操作

ある部分群 N が「正規部分群」であるための条件は、N の任意の元 n と、G の任意の元 g に対して、

$$gng^{-1}$$

という元（n の g による**共役**といいます）が、**再び N の中に戻ってくる**ことでした。正規部分群とは、いわば「G のどんな元でかき混ぜても、中身が外に漏れ出さない、安定した部分群」のことです。単純群であるとは、このような安定した部分群が $\{e\}$ と全体以外に存在しないことを意味します。

A_4 が分解できる理由：V_4 という「安定な避難所」

A_4（位数 12）は可解群でした。なぜなら、$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ という位数 4 の正規部分群を持っていたからです。なぜ V_4 は正規部分群なのでしょうか。V_4 の元（e 以外）は、「2 つのペアを入れ替える」という共通の形をしています。例えば、A_4 の元 $g = (123)$ で、V_4 の元 $n = (13)(24)$ を共役で「かき混ぜて」みましょう。共役の計算は、元の数字を g で変換することで簡単に行えます。

$$gng^{-1} = (123)(13)(24)(123)^{-1} = (g(1)g(3))(g(2)g(4)) = (21)(34) = (12)(34)$$

計算すると、元の $n = (13)(24)$ は、同じく V_4 の仲間である $(12)(34)$ に変換されました。他のどの元で計算しても、V_4 **の元は V_4 の元に移るだけで、外に漏れ出すことはありませ**

ん。V_4 は共役操作に対して「閉じている」安定な避難所なのです。このため、A_4 は V_4 によって分解可能でした。

A_5 が分解できない理由：「避難所」の不在

A_5（位数 60）の構造が根本的に異なるのは、この V_4 のような「安定な避難所」となる非自明な正規部分群が存在しない点です。A_5 の元は、3-サイクル（例：(123)）、5-サイクル（例：(12345)）、そして 2 つのペアの入れ替え（例：$(12)(34)$）などから構成されます。

A_5 の単純性の証明の概略は、次のような論理に基づいています。

1. もし A_5 に $\{e\}$ 以外の正規部分群 N が存在すると仮定します。
2. N から何か一つ元 n を取り出します。n がどんな形の元であれ（5-サイクルなど）、うまく A_5 の元 g を選んで共役 gng^{-1} を計算すると、必ず **3-サイクル**（例えば (123) など）を N の中に作り出せてしまうことが示せます。
3. 一旦、正規部分群 N の中に一つでも 3-サイクル（例えば (123)）が存在すると、共役操作によって、$(124), (125), (234), \ldots$ といった**すべての 3-サイクル**を次々と N の中に生成できてしまいます。
4. そして、3-サイクル全体は、A_5 という群全体を生成してしまうことが知られています。
5. したがって、N は $\{e\}$ 以外の元を一つでも含むと、自動的に A_5 全体と一致せざるを得ません。

つまり、A_5 の内部では、どんな小さな火種（$\{e\}$ 以外の元）も、共役操作によって次々と燃え広がり、群全体を飲み込んでしまうのです。そこには V_4 のような、延焼を食い止める「防火壁」＝正規部分群が存在しません。この「内部的に固く、分解を許さない」構造こそが、A_5 が単純群であることの本質なのです。

6.4 S_5 の非可解性

これまでの長い議論の末、私たちはついに最後の問いに答える準備が整いました。一般五次方程式のガロア群である対称群 S_5 は、果たして可解群なのでしょうか。

証明は、背理法を用います。まず、「S_5 は可解群である」と仮定し、そこから論理的な矛盾を導きます。

証明 S_5 が可解群であると仮定します。この仮定は、S_5 には次のような可解列が存在することを意味します。

$$S_5 = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{e\}$$

この列の最初のステップ $S_5 \rhd G_1$ に着目します。G_1 は S_5 の正規部分群でなければなりません。群論の事実として、S_5 の非自明な正規部分群は、交代群 A_5 のみであることが知られています。

したがって、この可解列の最初の有効なステップは、必ず $G_1 = A_5$ でなければなりません。

$$S_5 \rhd A_5 \rhd G_2 \rhd \cdots \rhd G_m = \{e\}$$

このことは、部分群の列 $A_5 \rhd G_2 \rhd \cdots \rhd \{e\}$ が、A_5 の可解列をなしていることを意味します。つまり、「S_5 **が可解群である」と仮定すると、その部分群である「A_5 もまた可解群でなければならない**」という結論が導かれます。

しかし、これは前節で示した結論と矛盾します。私たちは、前節で「A_5 は非可換な単純群であるため、可解群では**ない**」ことを証明しました。

ここに、論理的な矛盾が生じました。したがって、最初の仮定「S_5 は可解群である」が誤っていたと結論付けられます。

■

結論

対称群 S_5 は、可解群ではない。

6.5　結論：アーベル=ルフィニの定理

すべてのピースが、今一つにつながります。

1. **ガロアの規準（定理 5.1）：** 一般五次方程式がべき根で解けるための必要十分条件は、そのガロア群 S_5 が可解群であること。
2. **本章の結論:** S_5 は可解群ではない。

この二つの事実から、数学の歴史における最も重要な定理の一つが、揺るぎない結論として導かれます。

定理 6.3：アーベル

五次以上の一般の代数方程式には、その係数の四則演算とべき根の有限回の操作によって解を表すような、**代数的な解の公式は存在しない。**

これは、数学者たちの能力が足りなかったから解の公式を見つけられなかった、ということではありません。そうではなく、五次方程式の根が持つ「対称性」の構造（ガロア群 S_5 の構造）が、べき根という操作で表現できるような単純な「分解可能」な構造をしていなかった、という数学的な事実がその根底にあったのです。解の公式の不存在は、いわば必然的な運命でした。

第 III 部

ガロア理論の展望

7　ガロア理論の射程

本書では、代数方程式の可解性という問題を軸に、ガロア理論を解説してきました。しかし、ガロアが遺した思想、すなわち「**ある数学的対象を、その構造を不変に保つ変換の群（対称性の群）と関連付けて理解する**」というパラダイムは、代数方程式論を遥かに超えて、現代数学の様々な分野で力強く生き続けています。この最終章では、その広大な世界の一部を垣間見ることにしましょう。

7.1　微分方程式の理論へ

高校の積分で、e^{-x^2} のような関数の原始関数（積分した結果）は、私たちがよく知るような単純な関数（初等関数）では書けない、と学んだことがあるかもしれません。代数方程式に「べき根による解の公式」が存在しないように、微分方程式にも「初等関数による解の公式」が存在しない場合があるのです。なぜ、そのようなことが断言できるのでしょうか。その問いに、古典的なガロア理論と驚くほどよく似た考え方で答えるのが、**微分ガロア理論**です。

微分ガロア理論は、次のアナロジー（類推）に基づいています。

アナロジー：古典ガロア理論と微分ガロア理論

古典ガロア理論		**微分ガロア理論**
代数方程式	$\longleftrightarrow$	線形微分方程式
べき根で解けるか？	$\longleftrightarrow$	初等関数で解けるか？
体の拡大	$\longleftrightarrow$	微分体の拡大
ガロア群	$\longleftrightarrow$	微分ガロア群
可解群であるか？	$\longleftrightarrow$	可解性に関連する性質を持つか？

古典理論が「べき根」を添加して体を拡大したように、微分ガロア理論では、微分演算 d/dx を構造として持つ**微分体**という世界を考えます。そして、$y' = y$ の解である e^x や、$y' = 1/x$ の解である $\log x$ といった、微分方程式の解を添加して微分体を拡大していきます。

その拡大の「対称性」を記述するのが**微分ガロア群**です。これは、体の四則演算だけでなく、微分という操作まで含めて不変に保つような「許された入れ替え」の集まりです。そして、古典理論における可解群に対応する概念が、微分ガロア群（これは線形代数群になります）に対しても定義されます。

微分ガロア理論の主結果

線形微分方程式が、指数・対数・代数関数などの**初等的な関数**を用いて（専門的にはリウヴィル拡大を用いて）解けるための必要十分条件は、その微分ガロア群が**可解性に関連する性質を持つ**ことである。

この理論を用いることで、「e^{-x^2} の積分が初等関数で書けないこと」や、「ベッセル関数」や「ガンマ関数」といった特殊な関数がなぜ必要になるのかを、数学的に厳密に証明することができます。ここでもまた、ガロアの「対称性を群で記述する」というアイデアが、一見すると全く異なる分野の問題を解決するための、強力な光となっているのです。

7.2　整数論への応用

ガロア理論が最も深遠な形で応用されている分野の一つが、数の世界の究極の謎、すなわち素数の性質を探る**整数論**です。

私たちは普段、整数環 $\mathbb{Z}$ の中で素因数分解を考えます。しかし、数の世界を有理数体 $\mathbb{Q}$ から、代数的な数を添加した**代数体**（例えば $\mathbb{Q}(i)$ や $\mathbb{Q}(\sqrt{2})$）へと拡大すると、素数たちの振る舞いは劇的に変化します。

中心的な問いは、「**有理数体 $\mathbb{Q}$ の素数は、体を拡大した先でどのように振る舞うのか？**」というものです。例えば、ガウス整数環 $\mathbb{Z}[i]$（$\mathbb{Q}(i)$ の整数）の世界を考えてみましょう。

- 素数 5 は、$5 = (1+2i)(1-2i)$ となり、もはや素数ではなく、2 つの数に**分解**します。
- 素数 3 は、この新しい世界でもこれ以上分解できず、素数のままです（**惰性**するといいます）。
- 素数 2 は、$2 = (1+i)(1-i) = -i(1+i)^2$ となり、実質的に数の 2 乗に分解されます（**分岐**するといいます）。

なぜ素数によって、このような異なる運命が待ち受けているのでしょうか。この法則を完全に予言するのが、ガロア理論です。

ガロア群と素数の分解法則

ある素数 p が、代数体 K の中でどのように分解されるか（素数のままか、2 つに分かれるか、など）という運命は、その体のガロア群 $Gal(K/\mathbb{Q})$ の構造によって、完全に決定される。

具体的には、各素数 p に対して、**フロベニウス元**と呼ばれるガロア群の特別な元が対応します。そして、このフロベニウス元が群の中でどのような振る舞いをするか（例えば、その元の位数など）が、素数 p の分解の仕方を正確に反映しているのです。素数がどのように分解されるかという整数論の問題が、ガロア群の元の性質を調べるという代数の問題に、見事に翻訳されます。

この考え方は、20 世紀の整数論における金字塔である**類体論（るいたいろん）**へと発展しました。類体論は、ガロア群がアーベル群になるような体の拡大（アーベル拡大）のすべてを、係数体

の言葉だけで完璧に記述する、非常に美しい理論です。さらに、ガロア群がアーベル群でない、より複雑な非アーベル拡大を理解しようとする試みは、現代数学における最も壮大な研究プログラムの一つである**ラングランズ・プログラム**へと繋がっています。

ガロア理論は、単に方程式を解くための道具ではありません。それは、素数という数の世界の根源的な法則を解き明かすための、現代整数論に不可欠な基本言語となっているのです。

7.3　幾何学との関連

ガロア理論が示す「拡大」と「対称性の群」の対応という構造は、代数学の世界にとどまらず、図形の性質を研究する**位相幾何学（トポロジー）**の世界にも、驚くほどよく似た形で現れます。

トポロジーでは、複雑な図形（空間）を理解するために、その図形をより単純な図形で「覆う」という手法を取ることがあります。この覆いかぶさる空間を**被覆空間（ひふくくうかん）**と呼びます。最も基本的な例は、円周 S^1 と直線 $\mathbb{R}$ の関係です。無限に長い直線 $\mathbb{R}$ を、ぐるぐると円周 S^1 に巻きつけることで、円周を完全に「覆う」ことができます。

驚くべきことに、この「空間を被覆する」という関係の全体像は、ガロアの基本定理と瓜二つの構造で記述することができるのです。

アナロジー：ガロア理論と被覆空間論

古典ガロア理論		**被覆空間論**
体の拡大 L/K	$\longleftrightarrow$	空間の被覆 $\tilde{X} \to X$
中間体 M	$\longleftrightarrow$	中間被覆空間 M
ガロア群 $Gal(L/K)$	$\longleftrightarrow$	基本群 $\pi_1(X)$ の部分群

このアナロジーでは、空間の「穴」の情報を表す**基本群** $\pi_1(X)$ という群が、ガロア群の役割を果たします。そして、ガロアの基本定理とそっくりな、次の定理が成り立ちます。

被覆空間の分類定理

ある（性質の良い）空間 X の「連結な被覆空間」の種類と、その空間の基本群 $\pi_1(X)$ の「部分群」の種類の間には、1 対 1 の対応が存在する。

ここでもまた、体の拡大が中間体を持つように、被覆空間にも「中間被覆」があり、それらが基本群の部分群と見事に対応しているのです。この定理のおかげで、ある空間を「覆う」方法が何通りあるか、という幾何学的な問題を、その空間の基本群の構造を調べるという、純粋に代数的な問題に翻訳して解くことができます。

体の拡大の階層構造と、図形の被覆の階層構造。その背後に全く同じ「ガロア対応」の構造が隠れているという事実は、ガロアのアイデアが持つ、分野を超えた普遍性と美しさを物語っています。

7.4　楕円関数を使えば五次方程式は解ける

本書の結論は、「一般五次方程式に代数的な解の公式は存在しない」というものでした。しかし、ここで注意すべきは、この主張が「**べき根に限った**代数的な解の公式は存在しない」という意味である、という点です。もし、べき根よりもさらに強力な「道具」を使うことを許すならば、五次方程式の解を係数から導くことは不可能ではありません。

19 世紀、数学者たちはこの問題意識のもと、三角関数を一般化した**楕円関数（だえんかんすう）**という強力な新しい道具を研究していました。そして 1858 年、フランスの数学者シャルル・エルミートは、この楕円関数（正確には、関連する楕円モジュラー関数）を用いて、一般五次方程式の解を具体的に書き下すことに成功したのです。

なぜ、べき根では解けなかったのに、楕円関数を使えば解けるのでしょうか。その答えは、またしてもガロア群の構造に隠されています。

A_5 と正二十面体

五次方程式がべき根で解けない根源的な理由は、そのガロア群の「心臓部」である交代群 A_5 が、可解群ではない「非可換な単純群」であることでした。しかし、この A_5 という群は、全く別の世界に驚くべき姿で現れます。実は、A_5 は、プラトン立体の一つである**正二十面体（せいにじゅうめんたい）**の回転対称性の群と、群として完全に同型なのです。

$$A_5 \cong （正二十面体の回転群）$$

この事実は、五次方程式という純粋な代数学の問題と、正二十面体という幾何学の問題が、対称性という観点から見て本質的に同じ構造を持っていることを示唆しています。そして、この正二十面体の対称性は、複素平面上では楕円モジュラー関数というもので見事に記述することができます。

つまり、次のような美しい対応関係が成り立っているのです。

- **べき根**という道具の対称性は、**可解群**の構造に対応する。
- **楕円関数**という道具の対称性は、A_5 **のような群**の構造に対応する。

五次方程式のガロア群 S_5（および A_5）が持つ対称性の構造は、べき根という道具で分解するには複雑すぎました。しかし、正二十面体の対称性という、より高度で豊かな構造を持つ楕円関数にとっては、まさしく格好の相手だったのです。

ガロア理論は、単に「五次方程式は解けない」という不可能性を証明しただけではありません。ガロア群の構造を明らかにすることで、なぜ解けないのかという理由を解明し、さらには「どのような新しい道具（数学）を用いれば解けるのか」ということへの道筋までをも、示してくれたのです。不可能の壁の先には、代数学、幾何学、解析学が融合する、さらに広大で美しい数学の世界が広がっていました。

補足：正二十面体と楕円モジュラー関数

正二十面体の対称性（回転群）が A_5 と同型であるという事実は、五次方程式を幾何学的に捉え直す道を開きました。その繋がりを理解する鍵は、「**立体射影**」と「**不変式**」という概念です。

ステップ 1：対称性を複素平面へ写す

まず、正二十面体を球に内接させ、その球の中心を原点に置きます。次に、球の北極から光を当てて、球の表面上の点を南極が接する複素平面上に投影します。これを**立体射影**といいます。この操作によって、正二十面体の各頂点や面は、複素平面上の点に対応します。そして、正二十面体を回転させるという 3 次元的な操作は、複素平面上の**メビウス変換**（$z \mapsto \frac{az+b}{cz+d}$ という形の変換）へと翻訳されます。こうして、A_5 と同型な正二十面体の回転群は、複素平面上で作用する 60 個のメビウス変換の群として表現できます。

ステップ 2：対称性を特徴づける「不変式」

ある変換の集まり（群）に対して、その変換を施しても値が変わらない関数を**不変式**と呼びます。例えば、$f(x) = x^2$ は、$x \mapsto -x$ という変換に対して不変です。同様に、正二十面体の対称性に対応する 60 個のメビウス変換のすべてに対して不変な、特殊な多項式（または有理関数）を構築することができます。この「**正二十面体不変式**」は、いわば正二十面体の対称性そのものを凝縮したような数式です。クラインは、任意の五次方程式を、この不変式を用いた特定の形の方程式（**正二十面体方程式**）に変換できることを示しました。

ステップ 3：楕円モジュラー関数による「逆引き」

ここで、全く別の分野の主役、**楕円モジュラー関数**（特に **j-不変量**）が登場します。j-不変量は、非常に高度な対称性（モジュラー群 $SL(2,\mathbb{Z})$ に対する不変性）を持つ関数です。この関数は、複素数の上半平面から複素数全体への対応をつけ、いわば複素平面の「究極の地図」のような役割を果たします。

クラインの発見の核心は、この j-不変量の持つ豊かな対称性を利用すると、正二十面体方程式を解くことができる、ということでした。非常に粗いアナロジーですが、これは次のような操作に似ています。

- $y = x^5$ という関係があるとき、y の値から x の値を求めるには、$x = \sqrt[5]{y}$ という「逆関数」を使います。
- 五次方程式は、係数から作られるある値 Y が、根から作られる「正二十面体不変式」の値 X と結びついている、という関係式と見なせます。
- この Y から X を求めるという「逆関数」の役割を、楕円モジュラー関数（j-不変量）が果たしてくれるのです。

つまり、楕円モジュラー関数は、べき根よりも遥かに強力な「超越的な”ものさし”」とし

て機能し、べき根では分解できなかった A_5 の対称性を「ほどく」力を持っているのです。結論として、正二十面体と楕円モジュラー関数は**複素平面**という舞台の上で、**対称性**という共通言語を通じて結びつきます。ガロア群 A_5 を幾何学的に実現したものが正二十面体であり、その対称性を解析的に克服する道具が楕円モジュラー関数だったのです。