ガロア理論への招待

— なぜ五次方程式は解けないのか —

ほの

2025 年 8 月 6 日

概要

私たちは中学校で、二次方程式を解くための便利な**「解の公式」**を学びます。では、三次、四次、そして五次方程式にも、同じように万能な解の公式は存在するのでしょうか。

この素朴な疑問は、16 世紀に三次・四次方程式の公式が発見されて以来、300 年もの間、多くの数学者たちを悩ませてきた大きな謎でした。この長年の問いに終止符を打ち、現代数学の扉を開いたのが、若き天才**エヴァリスト・ガロア**です。

本書は、ガロアが遺した革命的なアイデアへの招待状です。彼は、方程式の性質を「解の入れ替え」という**対称性**の観点から捉え、それを**「群」**という新しい言葉で記述しました。この美しい理論を通じて、「なぜ五次以上の方程式には解の公式が存在しないのか」という謎が、いかに鮮やかに解き明かされるのかを追体験します。

数学の特別な知識は必要ありません。「なぜだろう？」という好奇心だけを頼りに、一緒にこの美しい数学の物語を旅してみましょう。

目次

はじめに：解の公式をめぐる冒険

皆さんは、中学校の数学で二次方程式 $ax^2 + bx + c = 0$ の解の公式を学んだことを覚えているでしょうか。

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

この公式の素晴らしい点は、どんな係数 a, b, c が与えられても、四則演算（足し算・引き算・掛け算・割り算）と平方根（$\sqrt{}$）という基本的な計算だけで、必ず解を求められる**万能性**にあります。この公式は、古代バビロニアの時代からその原型が知られており、まさに人類の叡智の結晶の一つと言えるでしょう。

さて、方程式の次数を上げて、三次、四次、五次と考えていくと、自然と次のような疑問が湧いてきます。

「三次以上の高次方程式にも、二次方程式のような万能な解の公式は存在するのだろうか？」

この問いは、多くの数学者たちを魅了し、そして苦しめてきた壮大なテーマでした。ルネサンス期の 16 世紀イタリアでは、タルタリア、カルダノ、フェラーリといった数学者たちの熾烈な競争の末、ついに**三次方程式と四次方程式の解の公式が発見**されます。それらは二次方程式の公式よりずっと複雑ではありましたが、確かに係数の四則演算とべき根（平方根や立方根）だけで解を表すものでした。

数学者たちは歓喜し、当然のように次の目標である「五次方程式の解の公式」の発見に乗り出しました。しかし、ここから事態は一変します。誰一人として、五次方程式の解の公式を見つけることができなかったのです。ラグランジュやコーシーといった第一級の数学者たちが挑戦しても、その謎は解けませんでした。300 年もの時間が、ただいたずらに過ぎていきました。

不可能の壁に突き当たった数学者たちは、やがて考え方を変え始めます。「どうやって公式を見つけるか」ではなく、**「そもそも解の公式は存在するのか？」**と。

この数学史上の大きな謎に終止符を打ち、現代数学の扉を開いたのが、わずか 21 歳の若さで決闘に散った天才、**エヴァリスト・ガロア**です。彼は、方程式を正面から解こうとするのではなく、その裏に隠された「構造」と「対称性」に着目しました。そして、「解ける方程式」と「解けない方程式」を分ける絶対的な境界線を発見したのです。

本書は、このガロアが遺した革命的な理論への招待状です。なぜ、あれほど多くの数学者たちが解の公式を見つけられなかったのか。その答えは、「公式が存在しないから」でした。この驚くべき結論に、ガロアがいかにして辿り着いたのか。彼の独創的なアイデアの軌跡を追いながら、一緒にこの美しい数学の物語を旅していきましょう。

1　物語の登場人物たち — 群と体

1.1　体：計算の舞台

ガロア理論の物語は、二つの重要な登場人物、「体（たい）」と「群（ぐん）」によって織りなされます。まずは、計算の「舞台」となる**体**から見ていきましょう。

私たちは普段、有理数、実数、複素数といった数の世界で、足し算や掛け算を自由に行っています。これらの世界に共通するのは、「四則演算（足し算・引き算・掛け算・割り算）がいつでも不自由なくできる」という性質です。数学では、このような便利な計算の舞台を「体」と呼び、次のように定義します。

定義：体 (Field)

集合 K が「体」であるとは、K に「和」と「積」の二種類の演算が定義されていて、以下の性質がすべて成り立つことをいいます。

1. **和について**
   - 自由に足し算・引き算ができる（専門的には「アーベル群をなす」といいます）。
   - 足し算の単位元「0」が存在する。
2. **積について**
   - 0 を除いた集合の元で、自由に掛け算・割り算ができる。
   - 掛け算の単位元「1」が存在する。
3. **分配法則**が成り立つ。つまり、$a(b+c) = ab + ac$ が成り立つ。

この定義は少し抽象的に見えますが、要するに**「いつもの四則演算が矛盾なくできる数の集まり」**のことだと考えてください。

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、いずれも体の代表的な例です。
- **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、つまり割り算が自由にできないからです。例えば、2 は整数ですが、その逆数 $1/2$ は整数ではありません。

さて、ここからがガロア理論にとって重要な考え方です。方程式を解くとき、私たちはしばしば今いる数の世界を「拡大」する必要に迫られます。例えば、方程式 $x^2 - 2 = 0$ を考えましょう。この方程式の解 $\pm\sqrt{2}$ は、有理数体 $\mathbb{Q}$ の中には存在しません。

そこで私たちは、$\mathbb{Q}$ の世界に新しい住人である $\sqrt{2}$ を「添加」し、四則演算ができるように最小限の世界を広げた、新しい体 $\mathbb{Q}(\sqrt{2})$ を作ります。この体は、a, b を有理数として $a + b\sqrt{2}$ という形で書ける数全体からなります。このように、ある体に新しい元を付け加えてより大きな体

を作ることを**体の拡大**と呼びます。

定義：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 の演算が一致するとき、L を K の**拡大体**といい、L/K と書いて**体の拡大**と呼びます。

方程式を解くという行為は、その方程式の係数が含まれる体（例えば $\mathbb{Q}$）から出発し、解がすべて含まれるような拡大体（例えば $\mathbb{Q}(\sqrt{2})$）へと、計算の舞台を広げていく旅路なのだと考えることができます。ガロア理論では、この「体の拡大」の構造を詳しく調べることになります。

1.2 群：対称性の言葉

物語の二人目の登場人物は、「群（ぐん）」です。もし「体」が計算の舞台であるならば、**「群」はその舞台上で演じられる「対称性」を記述するための言葉**です。

「対称性」と聞くと、皆さんは何を思い浮かべるでしょうか。例えば、正三角形を考えてみましょう。この正三角形を回転させたり、ひっくり返したりしても、元の図形とぴったり重なる操作があります。

- 何もしない（恒等操作）
- 120 度回転、240 度回転
- 3 つの頂点を通る軸でひっくり返す操作（3 種類）

これらの「図形を変化させない操作」の集まりは、ある操作の後に続けて別の操作を行っても、結果はまた別の「変化させない操作」になる、という美しい構造を持っています。数学では、このような「操作の集まり」が持つ構造を「群」と呼びます。

定義：群 (Group)

集合 G と、その上の演算「$\cdot$」が「群」であるとは、以下の 3 つの性質がすべて成り立つことをいいます。

1. **結合法則が成り立つ**：どの 3 つの元 a, b, c についても、$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ。
2. **単位元が存在する**：ある特別な元 e が存在し、どの元 a についても、$a \cdot e = e \cdot a = a$ となる。（何もしない操作に相当します。）
3. **逆元が存在する**：どの元 a にも、その「逆の操作」である元 a^{-1} が存在し、$a \cdot a^{-1} = a^{-1} \cdot a = e$ となる。

この「群」という概念は非常に強力で、図形の対称性だけでなく、物理学の法則や音楽の構造など、世の中の様々な「対称性」を記述することができます。

ガロア理論の物語で最も重要な役割を果たすのが、**対称群 (Symmetric Group)** と呼ばれる

群です。これは、いくつかのものを「並べ替える」という操作すべてを集めた群です。

定義：対称群 S_n

n 個のものを並べ替えるすべての操作（置換）の集まりがなす群を、n 次対称群といい、$\boldsymbol{S_n}$ と書く。その要素の総数は $n! = n \times (n-1) \times \cdots \times 1$ 個である。

補足：3 次対称群 S_3

例えば、$\{1, 2, 3\}$ という 3 つの数字を並べ替える操作は、$3! = 6$ 通りあります。これが S_3 の元です。

- e: 何もしない。「(1)(2)(3)」
- (1 2): 1 と 2 を入れ替える。「(1 2)(3)」
- (1 3): 1 と 3 を入れ替える。「(1 3)(2)」
- (2 3): 2 と 3 を入れ替える。「(2 3)(1)」
- (1 2 3): 1 を 2 へ、2 を 3 へ、3 を 1 へ動かす（巡回）。
- (1 3 2): 1 を 3 へ、3 を 2 へ、2 を 1 へ動かす（巡回）。

実は、先ほどの正三角形の 6 つの対称性の集まりは、この S_3 と全く同じ構造を持っています。頂点に 1, 2, 3 と名前をつければ、図形の操作と数字の入れ替えがぴったり対応するのです。

天才ガロアが発見したのは、まさにこのことでした。方程式の解たちが持つ「対称性」もまた、この「対称群」という言葉で記述できるのではないか？ 次の章では、いよいよ物語の核心、「方程式」と「群」を結びつけるガロアの画期的なアイデアを見ていくことにしましょう。

2　方程式に隠された対称性 — ガロア群

前の章で、物語の二人の登場人物「体」と「群」を紹介しました。ここからは、いよいよガロア理論の真髄に迫ります。ガロアの天才的なひらめきは、この二つの概念を「方程式」という舞台の上で結びつけた点にあります。

まずは、最も単純な例から始めましょう。有理数（$\mathbb{Q}$）を係数に持つ、あの方程式です。

$$x^2 - 2 = 0$$

この方程式の解は、ご存知の通り $\alpha_1 = \sqrt{2}$ と $\alpha_2 = -\sqrt{2}$ です。これらの解は有理数ではありませんが、解の間には興味深い「対称性」が隠されています。

ここで、二つの解を入れ替える操作を考えてみましょう。つまり、「$\sqrt{2}$ を見たら $-\sqrt{2}$ に置き換え、$-\sqrt{2}$ を見たら $\sqrt{2}$ に置き換える」という操作です。この操作を σ と名付けます。

この操作 σ を、解たちの関係式に施してみると、何が起こるでしょうか。例えば、解の和と積を計算すると、

- **和:** $\alpha_1 + \alpha_2 = \sqrt{2} + (-\sqrt{2}) = 0$
- **積:** $\alpha_1 \times \alpha_2 = \sqrt{2} \times (-\sqrt{2}) = -2$

となります。結果の 0 と -2 は、どちらも有理数（係数の体 $\mathbb{Q}$ の元）です。では、この和と積の式全体に、先ほどの入れ替え操作 σ を行ってみましょう。

- **和への操作:** $\sigma(\alpha_1 + \alpha_2) = \sigma(\alpha_1) + \sigma(\alpha_2) = (-\sqrt{2}) + \sqrt{2} = 0$
- **積への操作:** $\sigma(\alpha_1 \times \alpha_2) = \sigma(\alpha_1) \times \sigma(\alpha_2) = (-\sqrt{2}) \times \sqrt{2} = -2$

驚くべきことに、**解を入れ替えても、計算結果である有理数 0 と -2 は全く変化しません。**この「入れ替え」は、係数の世界 $\mathbb{Q}$ にとっては「何も起きなかった」のと同じことなのです。このような操作は、方程式の係数体が持つ構造を保つ、**「許された入れ替え」**と考えることができます。

ガロアの基本発想

方程式の係数が含まれる体 K を基準に考えたとき、その方程式の解たちを入れ替える操作のうち、**K の元を不変に保つような「許された入れ替え」**が存在する。
そして、この「許された入れ替え」の操作全体を集めると、それは**群をなす。**

この、方程式一つひとつに固有の群こそが、ガロア理論の主役である**ガロア群**です。方程式が「解ける」か「解けない」かという運命は、すべてこのガロア群の構造に刻み込まれているのです。

次のセクションでは、このガロア群をもう少し正確に定義し、その性質を探っていきましょう。

2.1 ガロア群とは？

前のセクションでは、方程式の解を入れ替えても、係数の体 $\mathbb{Q}$ の元が変わらない「許された入れ替え」が存在することを見ました。この直感的なアイデアを、もう少し数学的に厳密な言葉で定義しましょう。

まず、体の拡大 L/K を考えます。このとき、L から L への写像（関数のようなもの）σ で、以下の二つの条件を満たすものを考えます。

1. σ は体の演算を保つ（つまり、$\sigma(a+b) = \sigma(a) + \sigma(b)$ と $\sigma(ab) = \sigma(a)\sigma(b)$ が成り立つ）。
2. σ は小さい方の体 K の元を動かさない（つまり、すべての $k \in K$ に対して $\sigma(k) = k$ となる）。

このような特別な写像を、L の K **自己同型写像** と呼びます。難しく聞こえるかもしれませんが、これはまさに先ほど見た「係数体を不変に保つ解の入れ替え」を一般化したものです。

そして、この「許された入れ替え」の操作をすべて集めたものが、ガロア群です。

定義：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、L/K の**ガロア群**といい、$\boldsymbol{Gal(L/K)}$ と書く。
特に、K を係数体とする方程式 $f(x) = 0$ のガロア群とは、その方程式のすべての解を含む最小の拡大体（これを**分解体** L といいます）についてのガロア群 $Gal(L/K)$ のことを指す。

この定義により、どんな方程式にも、その「対称性」を表すガロア群という名の群を対応させることができるようになりました。では、我々の最終目標である「一般の」五次方程式のガロア群は、一体どのような群になるのでしょうか。ここに、ガロア理論における一つの重要な事実があります。

定理：一般方程式のガロア群

係数が互いに独立な「一般の」n 次方程式のガロア群は、n 次対称群 $\boldsymbol{S_n}$ となる。
したがって、一般の五次方程式のガロア群は、五次対称群 $\boldsymbol{S_5}$ である。

これは非常に重要な結果です。なぜなら、「一般の」五次方程式が解けるかどうかという問題は、**「対称群 S_5 がどのような性質を持っているか」**という、完全に群論の問題に置き換えられたからです。

補足：低次方程式のガロア群

では、解の公式が存在する二次、三次、四次方程式のガロア群はどうなっているのでしょうか。

- **二次方程式**: ガロア群は S_2（またはその部分群）。S_2 は要素数 2 の非常に単純な群です。
- **三次方程式**: ガロア群は S_3（またはその部分群）。S_3 は要素数 6 の群で、少し複雑ですが、ある意味で「分解可能」な良い性質を持っています。
- **四次方程式**: ガロア群は S_4（またはその部分群）。S_4 は要素数 24 とさらに大きくなりますが、これもまた S_3 と同様に「分解可能」な構造をしています。

どうやら、二次、三次、四次方程式に解の公式が存在することと、それらのガロア群 S_2, S_3, S_4 が持つ「分解可能」という共通の性質には、深い関係がありそうです。

とすれば、我々が次に問うべきは自ずと明らかでしょう。五次対称群 S_5 は、S_2, S_3, S_4 と同じように「良い性質」を持っているのでしょうか？ それとも、何か決定的に異なる構造をしているのでしょうか？ この問いに答えるため、次の章ではガロア理論の心臓部である「ガロアの基本定理」を探検し、体と群の対応関係をさらに詳しく見ていくことにします。

3　ガロア理論の心臓部 — 基本定理

前の章で、私たちは方程式一つひとつに、その対称性を表す「ガロア群」が定まることを見ました。ここからは、ガロア理論で最も美しく、そして最も重要な定理である**「ガロアの基本定理」**を探検します。この定理は、方程式の構造を解き明かすための、完璧な地図の役割を果たします。

まず、その地図が記述する二つの世界、「体の世界」と「群の世界」の構造を詳しく見てみましょう。

3.1　体の塔と群の塔

ガロア理論は、体の拡大 L/K を考えます。これは、小さい体 K（基地）と、それに解などを添加して作られた大きい体 L（目的地）の関係でした。しかし、多くの場合、基地と目的地の「中間」には、様々な中継地点が存在します。

例：体の「中継地点」

例えば、$K = \mathbb{Q}$ に $\sqrt{2}$ と $\sqrt{3}$ を添加した体 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ を考えましょう。このとき、K と L の間には、

- $M_1 = \mathbb{Q}(\sqrt{2})$（$\sqrt{2}$ だけの世界）
- $M_2 = \mathbb{Q}(\sqrt{3})$（$\sqrt{3}$ だけの世界）
- $M_3 = \mathbb{Q}(\sqrt{6})$（$\sqrt{6}$ だけの世界）

といった「中間体」が存在します。このように、体の拡大の内部には、しばしば階層構造が見られます。これを**体の塔**と呼ぶことにしましょう。

一方で、群の世界にも同じような階層構造があります。ガロア群 $G = Gal(L/K)$ の中には、それ自身がまた群となっているような部分集合、すなわち**部分群**が存在します。これもまた、大きい群から小さい群へと続く**群の塔**と見なすことができます。

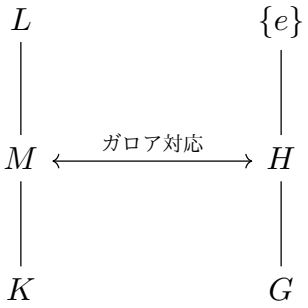
さて、ここからがガロアの天才的な洞察です。彼は、これら二つの塔が、全く無関係に存在しているのではなく、**驚くほど美しい対応関係にある**ことを見抜きました。

ガロアの洞察：体と群の対応

体の拡大 L/K における「中間体の塔」と、そのガロア群 $G = Gal(L/K)$ の「部分群の塔」の間には、**一対一の対応**が存在する。

この対応は、ただの対応ではありません。それは、まるで鏡に映したかのように、**包含関係が逆転する**という不思議な性質を持っています。

体の世界　　群の世界



図のように、

- 最も大きい中間体（L 自身）には、最も小さい部分群（単位元 $\{e\}$ のみからなる群）が対応します。
- 最も小さい中間体（K 自身）には、最も大きい部分群（G 全体）が対応します。

つまり、**体が大きくなればなるほど、対応する群は小さくなる**のです。これは、体が大きいほど、その体を不変に保つような「許された入れ替え」（自己同型写像）の種類が少なくなる、と考えれば直感的に理解できるでしょう。

この驚くべき対応関係こそが、ガロアの基本定理の骨子です。次のセクションで、この定理のより正確な主張を見ていきましょう。

3.2　ガロアの基本定理

前のセクションでは、体の塔と群の塔の間に、鏡写しのような不思議な対応関係があることを見ました。この対応関係を、数学的に厳密かつ明快に記述したものが、ガロア理論の頂点に輝く**「ガロアの基本定理」**です。

この定理は、体の拡大 L/K が「ガロア拡大」と呼ばれる良い性質を持つ場合に成り立ちます。（※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。）この定理は、まさに体の世界と群の世界を繋ぐ完璧な「辞書」や「翻訳機」に例えることができます。

定理：ガロアの基本定理

体のガロア拡大 L/K と、そのガロア群 $G = Gal(L/K)$ を考える。このとき、以下の 3 つの主張が成り立つ。

■1. **ガロア対応 (Galois Correspondence)**　L/K の**中間体** M $(K \subseteq M \subseteq L)$ の集合と、G の**部分群** H $(H \subseteq G)$ の集合の間には、**包含関係を逆転させる 1 対 1 の対応**が存在する。

- 中間体 M には、群 $H = \{\sigma \in G \mid \text{すべての } m \in M \text{ に対し } \sigma(m) = m\}$ が対応する。
- 部分群 H には、体 $M = \{l \in L \mid \text{すべての } \sigma \in H \text{ に対し } \sigma(l) = l\}$ が対応する。

■2. **拡大次数と群の位数**　上記 (1) の対応において、体の拡大の「大きさ」と群の「大きさ」は、次のように完璧に対応している。

$$[L : M] = |H| \quad \text{かつ} \quad [M : K] = [G : H]$$

ここで、$[L : M]$ は体の拡大次数（体の大きさの比のようなもの）、$|H|$ は群の位数（元の個数）、$[G : H]$ は部分群 H の指数（$|G|/|H|$ のこと）を表す。

■3. **正規拡大と正規部分群**　この定理で最も重要な部分が、以下の同値関係である。

中間拡大 M/K が**正規拡大**（※）である　$\Longleftrightarrow$　対応する部分群 H が G の**正規部分群**である

さらに、この条件が成り立つとき、M/K のガロア群は、G を H で割った**商群** G/H と同型になる。

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

(※正規拡大とは、それ自身がガロア拡大となるような「素性の良い」拡大のことです。)

補足：この定理の強力さ

この定理の何がそれほど強力なのでしょうか。それは、**体の世界の複雑な問題を、群の世界の（比較的）簡単な問題に翻訳できる**点にあります。
例えば、「中間体 M をすべて見つけなさい」という問題は、多くの場合非常に困難です。しかし、この定理を使えば、「ガロア群 G の部分群 H をすべて見つけなさい」という代数の問題に置き換えることができます。
とりわけ強力なのが主張 (3) です。体の「良い性質（正規拡大）」と、群の「良い性質（正規部分群）」が完全に対応していることを示しています。これが、次章で登場する「可解群」の概念と結びつき、方程式が解けるかどうかの謎を解く最終的な鍵となるのです。

3.3　最も重要な対応：正規拡大と正規部分群

ガロアの基本定理の中でも、方程式の可解性（解の公式が存在するかどうか）に直結する、最も重要で深遠な部分が、主張 (3) の「正規拡大」と「正規部分群」の対応です。

もう一度、その主張を確認しましょう。

中間拡大 M/K が**正規拡大**である　$\Longleftrightarrow$　対応する部分群 H が G の**正規部分群**である

この対応がなぜそれほどまでに重要なのでしょうか。その理由を理解するために、少しだけ「正規部分群」の性質に踏み込んでみましょう。

定義：正規部分群 (Normal Subgroup)

群 G の部分群 H が「正規部分群」であるとは、大まかに言うと、G **の中で「特別な地位」を与えられた、安定した部分群**のことです。G のどの元で操作しても、H は全体として変化しません。

正規部分群がなぜ特別かというと、それによって親である群 G を「割り算」し、新しい小さな群を作り出すことができるからです。この新しい群を**商群（しょうぐん）**G/H と呼びます。

正規部分群の役割：群の「分解」

正規部分群 H が存在するということは、大きな群 G の構造を、

- 部分群 H の構造
- 商群 G/H の構造

という、**二つのより単純な群の構造に「分解」して調べられる**ことを意味します。これは、複雑なものをより小さな部品に分解して理解する、という科学の基本的なアプローチと同じです。

ガロアの基本定理が告げているのは、この群の世界における「分解」という操作が、体の世界の構造と完璧に連動しているという驚くべき事実です。

つまり、ガロア群 G が正規部分群 H を持ち、G/H という商群に分解できるならば、それに対応する体の拡大 L/K もまた、中間体 M によって、L/M と M/K という二つのより単純な拡大に「分解」できるのです。

この対応関係が、いよいよ方程式の解の公式の存在問題に光を当てます。思い出してください。「解の公式がある（べき根で解ける）」とは、体をべき根で次々と拡大していく「根基拡大の塔」を建設できることでした。

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

実は、この塔の一つひとつのステップ、K_{i+1}/K_i は、とても性質の良い「正規拡大」になっています。

次章への架け橋

体の世界で「べき根による正規拡大の塔」を建設できるということは、ガロアの基本定理によれば、群の世界でガロア群 G を「正規部分群の塔」によって分解できる、ということに他なりません。

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

そして、各ステップの商群 G_i/G_{i+1} は、べき根拡大に対応する単純な群（アーベル群）になります。

このように「分解可能」な群は、特別な名前で呼ばれています。それが次章のテーマである

「可解群」です。方程式が解けるかどうかの問題は、ついに「そのガロア群は、可解群であるか？」という、純粋な群論の問題へとたどり着きました。

4　解の公式と「可解群」

これまでの章で、私たちは方程式の「対称性」を記述するガロア群と、その構造を解き明かす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、これらの道具を使って、物語の最初の問い「解の公式は存在するか？」という問題に決着をつけます。

そのためにはまず、「解の公式がある」とは一体どういうことなのか、その正体を数学の言葉で正確に捉え直す必要があります。

4.1　解の公式の正体

私たちは、二次方程式 $ax^2 + bx + c = 0$ の解の公式を何度も見てきました。

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

この式の構造をじっと眺めてみましょう。この式は、方程式の**係数** a, b, c から出発して、

1. **四則演算**（足す、引く、掛ける、割る）
2. **べき根**（ここでは平方根 $\sqrt{}$）

という二種類の操作を有限回だけ組み合わせて作られています。三次や四次方程式の（非常に複雑な）解の公式も、その構造は同じで、四則演算とべき根（平方根 $\sqrt{}$ と立方根 $\sqrt[3]{}$）だけで構成されています。

この観察を、私たちが学んできた「体の言葉」で表現してみましょう。

1. まず、係数を含む体 K（例えば $K = \mathbb{Q}$）からスタートします。
2. 次に、K の中のある元のべき根 $\sqrt[n_1]{a_1}$ を考え、それを体に添加して新しい体 $K_1 = K(\sqrt[n_1]{a_1})$ を作ります。（体を拡大します。）
3. さらに、今作った体 K_1 の中のある元のべき根 $\sqrt[n_2]{a_2}$ を添加して、$K_2 = K_1(\sqrt[n_2]{a_2})$ を作ります。
4. この操作を有限回繰り返して、体の塔 $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$ を建設します。

このように、べき根の添加を積み重ねて作られる体の拡大を**根基拡大（こんきかくだい）**と呼びます。

この言葉を使えば、「解の公式が存在する」ということを、次のように厳密に定義できます。

定義：べき根で解ける (Solvable by Radicals)

方程式が**「べき根で解ける」**とは、その方程式のすべての解が、係数体 K のある**根基拡大**に含まれていることをいう。

一見すると抽象的ですが、これはまさしく**「解の公式」というものの正体を、体の拡大の言葉で記述した**に過ぎません。

さて、これでパズルのピースが一つはまりました。「解の公式の存在」を「根基拡大の塔が存在する」ことだと捉え直したのです。ガロアの基本定理によれば、この体の塔は、ガロア群における「部分群の塔」に対応しているはずです。

では、この「根基拡大」という特別な体の塔に対応するガロア群は、一体どのような特別な性質を持つのでしょうか？ その答えこそが、次のセクションのテーマである**「可解群」**なのです。

4.2　可解群：分解できる群

前のセクションで、「解の公式がある」という問題は、「根基拡大の塔を建設できるか」という体の問題に言い換えられました。そして、ガロアの基本定理は、この体の塔がガロア群における「部分群の塔」に対応することを教えてくれます。

では、この特別な体の塔に対応するガロア群は、一体どのような性質を持つのでしょうか。その答えが、本章の主役である**「可解群（かけいぐん）」**です。

複雑な機械の仕組みを理解したいとき、私たちはそれを分解して、一つひとつの単純な部品の働きを調べます。群論の世界でも、同じような考え方ができます。複雑な群を、より単純な構成要素に「分解」して理解しよう、というアプローチです。群論における最も単純で扱いやすい部品が、**アーベル群（可換群）**です。これは、演算の順番を交換しても結果が変わらない（$a \cdot b = b \cdot a$）、おとなしい性質の群です。

この「分解」というアイデアを数学的に表現したのが、可解群の定義です。

定義：可解群 (Solvable Group)

群 G が**「可解群」**であるとは、次のような部分群の列（塔）が存在することをいう。

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

この列は、以下の 2 つの条件を満たさなければならない。

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

この定義は、一見すると複雑に見えるかもしれません。しかし、その本質は**「群 G が、アーベル群という単純な部品に、段階的に分解できる」**ということを述べているに過ぎません。正規部分群で次々と割り算していくことで、その構造を完全に解き明かせる群、それが可解群なのです。

補足：「可解」という名前の由来

なぜこのような群が「可解」群と呼ばれるのでしょうか。それは、歴史的に、この群が**「(べき根で）解ける」代数方程式の研究から生まれた**からです。方程式がべき根で解けるという性質が、そのガロア群がこの「分解可能な構造」を持つという性質に、影のように寄り添っている。ガロアは、この驚くべき対応関係を発見し、方程式の可解性 (solvability) にちなんで、この群の性質を「可解 (solvable)」と名付けたのです。

これで、物語のクライマックスに向けた二つの重要な概念が出揃いました。

- **体の世界**：「べき根で解ける」（根基拡大の塔）
- **群の世界**：「可解群」（アーベル群で分解できる群の塔）

この二つの概念は、果たしてどのような関係にあるのでしょうか。次のセクションで、ガロア理論が導き出す、運命の結論を見ていきましょう。

4.3　運命の同値関係

私たちは今、二つの異なる世界で、それぞれ非常によく似た構造を持つ「塔」を見てきました。

- **体の世界**：係数体から出発し、べき根を次々と添加していく「根基拡大の塔」。これは「解の公式が存在する」ことに対応していました。
- **群の世界**：ガロア群から出発し、正規部分群で次々と割り算していく「可解群の塔」。商群はすべて単純なアーベル群になるのでした。

これら二つの塔は、単に似ているだけなのでしょうか。それとも、そこには何か運命的な繋がりが隠されているのでしょうか。

ガロア理論が最終的にたどり着いた結論は、まさに後者でした。この二つの概念は、単に似ているのではなく、**表裏一体の関係にある**のです。これこそが、ガロア理論が方程式論にもたらした最も輝かしい帰結です。

定理：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。

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

この定理は、私たちの旅における「ロゼッタストーン」です。これにより、私たちはついに、方程式という解析的な世界の言葉を、群という純粋に代数的な世界の言葉へと、完全に翻訳できるようになったのです。

この「運命の同値関係」が確立されたことで、300 年来の謎であった「五次方程式の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 $\boldsymbol{S_5}$ であった。
では、この**五次対称群 $\boldsymbol{S_5}$ は、可解群なのだろうか？**

もし、S_5 が可解群であるならば、一般の五次方程式はべき根で解ける、つまり解の公式が存在することになります。もし、S_5 が可解群でないならば、一般の五次方程式はべき根で解けず、解の公式は存在しないことになります。

もはや、複雑な方程式の式変形に頭を悩ませる必要はありません。ただ、群 S_5 の構造を、その「分解可能性」という一点から見つめるだけでよいのです。

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、その驚くべき理由を解き明かしていきます。

5　結論 — アーベル＝ルフィニの定理の証明

私たちはついに、物語の頂上が目前に見える場所までたどり着きました。体、群、ガロア対応、そして可解群。これまでに手に入れてきた強力な道具の数々を今こそ組み合わせ、300 年来の謎であった「五次方程式の解の公式の存否」に、最終的な結論を下す時です。

証明は、**背理法（はいりほう）**という論理展開を用います。つまり、まず「一般の五次方程式に、べき根を用いた解の公式が存在する」と仮定し、そこから論理を慎重に進めていくことで、最終的に「矛盾」を導き出すのです。矛盾が示されれば、最初の仮定が誤っていた、すなわち「解の公式は存在しない」と結論できるわけです。

では、すべてのピースを並べて、論理の最終ステップを確認しましょう。

1. **【仮定】**まず、**「一般の五次方程式に解の公式が存在する」と仮定します。**
2. **【第 4 章より】**この仮定は、第 4 章で学んだ体の言葉によれば、「一般の五次方程式は**べき根で解ける**」ということを意味します。
3. **【運命の同値関係より】**そして、ガロア理論のクライマックスであった「運命の同値関係」（4.3 節）によれば、方程式がべき根で解けるならば、その方程式のガロア群は必ず**可解群**でなければなりません。
4. **【第 2 章より】**一方で、第 2 章で学んだように、一般の五次方程式のガロア群は、五つのものを任意に入れ替える群、すなわち**五次対称群 $\boldsymbol{S_5}$** であることがわかっています。
5. **【論理的な帰結】**以上のステップを繋ぎ合わせると、最初の仮定から、次のような強力な結論が導かれます。

ここまでの結論

もし、一般の五次方程式に解の公式が存在するならば、
そのガロア群である**五次対称群 $\boldsymbol{S_5}$ は、必ず可解群でなければならない。**

すべては、この一点に集約されました。私たちの長い旅は、今や、たった一つの純粋な群論の

問いに姿を変えたのです。

五次対称群 S_5 は、果たして可解群なのでしょうか？

次のセクションでは、この最後の問いに答えるため、対称群 S_n の構造に最後のメスを入れ、なぜ $n = 2, 3, 4$ の世界と $n = 5$ の世界が、天国と地獄ほども違うのかを明らかにします。

5.1 S_5 の構造：分解できない「怪物」

前のセクションで、私たちの壮大な冒険は、たった一つの問いへと集約されました。

「五次対称群 S_5 は、可解群なのか？」

この問いに答えるため、対称群 S_n の構造を詳しく見ていきましょう。

まず、解の公式が存在する低次の方程式に対応するガロア群、S_2, S_3, S_4 がなぜ可解群なのかを思い出してみましょう。

- $\boldsymbol{S_2}$: 元は 2 個しかなく、アーベル群です。したがって、定義から明らかに可解群です。
- $\boldsymbol{S_3}$: $S_3 \triangleright A_3 \triangleright \{e\}$ という正規部分群の列を持ち、商群 S_3/A_3 と $A_3/\{e\} \cong A_3$ は共にアーベル群です。よって、S_3 は可解群です。
- $\boldsymbol{S_4}$: 計算は複雑ですが、S_4 もまた、アーベル群を商群に持つような正規部分群の列に分解することができます。したがって、S_4 も可解群です。

ここまでは、すべて順調です。では、$n = 5$ で一体何が変わるのでしょうか。

S_n の分解を考える上で鍵となるのが、**交代群 (Alternating Group)** $\boldsymbol{A_n}$ と呼ばれる特別な正規部分群です。これは、S_n の要素のうち「偶置換」と呼ばれるものだけを集めた群で、その大きさは S_n のちょうど半分 $(n!/2)$ です。S_5 の場合、その大きさは $5! = 120$ なので、交代群 A_5 の大きさは 60 となります。

S_5 が可解群であるためには、$S_5 \triangleright A_5 \triangleright \cdots \triangleright \{e\}$ というように、分解の連鎖を続ける必要があります。次のステップは、A_5 を分解することです。つまり、A_5 の中に、商群がアーベル群になるような、都合の良い正規部分群を見つけなければなりません。

しかし、ここですべての試みは絶望的な壁に突き当たります。

定理：交代群 A_5 の性質

位数 60 の交代群 $\boldsymbol{A_5}$ は、**単純群 (Simple Group)** である。

「単純群」とは何でしょうか。それは、群論の世界における「原子」のような存在です。

定義：単純群 (Simple Group)

群 G が「単純群」であるとは、その正規部分群が、自分自身 G と、単位元のみからなる自明な群 $\{e\}$ の二つしか存在しないことをいう。

単純群は、それ以上分解することができない、群の究極の構成要素です。そして、交代群 A_5 は、この分解不可能な「原子」だったのです。さらに重要なことに、A_5 はアーベル群ではありません（例えば、A_5 の中で $(1\ 2\ 3)(3\ 4\ 5) \neq (3\ 4\ 5)(1\ 2\ 3)$ となり、演算は非可換です）。

これが致命的でした。A_5 は単純群なので、その正規部分群は A_5 自身か $\{e\}$ しかありません。

- もし $\{e\}$ を正規部分群として選ぶと、商群 $A_5/\{e\} \cong A_5$ はアーベル群ではありません。

したがって、A_5 を分解してアーベル群を得ることは不可能なのです。分解の連鎖は、$S_5 \triangleright A_5$ の時点で完全に断ち切られてしまいます。

結論

交代群 A_5 が非可換な単純群であるため、
五次対称群 S_5 は、可解群ではない。

私たちはついに、最後の問いに対する答えを得ました。S_5 は、それ以下の対称群とは構造的に全く異なる、「分解できない怪物」をその内に秘めていたのです。さあ、この最後の真実を手に、次のセクションで、私たちの旅の最終目的地である定理の証明を完成させましょう。

5.2　証明の完成

長い旅路の果てに、私たちは今、すべてのピースを手にしました。点と点とが繋がり、一本の線となって、ついに壮大な証明がその姿を現します。

私たちの論理の再確認

証明の出発点となった、背理法による論理構成を思い出しましょう。

- **【仮定】**もし、一般の五次方程式に解の公式が存在するならば、
- **【帰結】**そのガロア群である五次対称群 S_5 は、**可解群でなければならない。**

この論理的な繋がりは、ガロア理論によって保証された、揺るぎないものでした。

そして、まさに前のセクションで、私たちはこの物語の核心に触れました。

しかし、五次対称群 S_5 は、**可解群ではなかった。**

その理由は、位数 60 の交代群 A_5 が「非可換な単純群」という、それ以上分解不可能な「群の原子」であったためです。

これで、すべてが出揃いました。私たちの最初の仮定「一般の五次方程式に解の公式が存在する」は、「S_5 は可解群である」という結論を導きます。しかし、数学的な事実として、「S_5 は可解群ではない」のです。

一つの事柄が、真実であり、かつ真実でない、ということはあり得ません。ここに**矛盾**が生じました。

論理学において、矛盾の発生は、議論の出発点となった「仮定」そのものが誤っていたことを意味します。したがって、私たちの最初の仮定は、棄却されなければなりません。

証明の完了

「一般の五次方程式に解の公式が存在する」という仮定は、数学的な矛盾を導く。
ゆえに、この仮定は誤りである。

これにより、300 年以上にわたる数学者たちの探求の歴史に、終止符が打たれました。私たちはついに、アーベルとガロアが到達した、数学史における金字塔の一つを証明したのです。

定理：アーベル＝ルフィニの定理

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。**

この結論が示しているのは、数学者たちの能力や創意工夫が足りなかった、ということではありません。そうではなく、五次方程式の解が持つ「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なのです。解の公式の不存在は、いわば必然的な運命でした。

これで、本書の主題であった謎は、完全に解き明かされました。最後の「おわりに」では、この偉大な理論を遺した天才ガロアの生涯と、彼の発見がその後の数学に与えた広大な影響について、少しだけ触れてみたいと思います。

おわりに：ガロアの遺したもの

二次方程式の解の公式という、馴染み深い一本の式から始まった私たちの旅は、今、終わりを告げようとしています。体を拡大し、群の対称性を追い求め、私たちはついに「五次方程式の解の公式は存在しない」という、数学史に輝く一つの頂へとたどり着きました。ここまで、長い道のりを共に歩んでくださった読者の皆様に、心から感謝申し上げます。

この壮大な理論を私たちに遺してくれた人物、エヴァリスト・ガロアは、そのあまりにも短い生涯でも知られています。19 世紀フランスの激動の時代、彼は共和主義者として政治活動に身を投じながら、画期的な数学の研究に没頭しました。しかし、彼の先進的な論文は、当時の数学界の権威であったコーシーやポアソンといった大学者たちには理解されず、二度にわたって正当な評価を受けることなく失われるという不運に見舞われます。

そして 1832 年 5 月 30 日、恋愛をめぐるいざこざが原因とされる決闘で、彼は命を落とします。わずか 20 歳でした。決闘の前夜、死を覚悟したガロアは、自らの数学的な発見のすべてを友人に宛てた最後の手紙に書き殴りました。その余白には、「僕には時間がない」という悲痛な走り書きが残されていたと伝えられています。

彼の死から 10 年以上が過ぎた後、この手紙に記されたアイデアが数学者ジョゼフ・リウヴィルによって見出され、ようやくその真価が世界に認められることになりました。ガロアが解き明か

したことは、単に五次方程式の問題だけではありませんでした。彼が遺した最大の功績は、**「群」という概念を用いて、対象の「対称性」を調べる**という、全く新しい数学の視点を導入したことです。

この「ガロア理論」の考え方、すなわち、ある数学的な対象を、その構造を不変に保つ変換の群（ガロア群）と関連付けて調べるという方法は、現代数学における最も強力で普遍的なパラダイムの一つとなりました。整数論、代数幾何学、位相幾何学、さらには物理学の素粒子論や、現代の暗号理論に至るまで、ガロアのアイデアは様々な分野に深く浸透し、豊かな実りをもたらし続けています。

一人の若者の頭の中に閃いたアイデアが、時代を超えてこれほど広大な知的世界を築き上げたのです。

本書で体験した物語が、皆様にとって、数学という学問が単なる計算や公式の暗記ではなく、その背後にある美しい構造や概念の繋がりを探求する、創造的で人間的な営みであることを感じる一助となれば、それに勝る喜びはありません。

おまけの章：ガロアのアイデア、その先へ — 現代に生きる対称性の言葉

本書では、代数方程式の解の公式をめぐる謎を、ガロア理論という「対称性の言葉」を用いて解き明かしました。しかし、ガロアが遺した**「ある対象の性質を、その対称性を記述する『群』と対応させて調べる」**という強力なアイデアは、代数方程式の世界を遥かに超えて、現代数学や情報社会の至る所で輝きを放っています。

この章では、その広大な世界を少しだけ覗いてみましょう。ガロアのアイデアが、どのように姿を変え、新たな問題に光を当てているのか、その雰囲気を感じていただければ幸いです。

5.3　微分ガロア理論 —「解けない」微分方程式

皆さんは、高校の積分で e^{-x^2} のような関数に出会ったときに、「この関数の原始関数（積分した結果）は、私たちが知っているような単純な関数（初等関数）では書くことができない」と聞いたことがあるかもしれません。代数方程式に「解の公式が存在しない」ように、微分方程式にも「綺麗な形の解が存在しない」ことがあるのです。

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。

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**

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、例えば $y' - y = 0$ 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**と呼ばれる世界を拡大していきます。

そして、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。

微分ガロア理論の結論

線形微分方程式が、指数・対数・三角関数やその積分といった「初等的な関数」で解けるかどうかは、その微分ガロア群の構造が「可解」であるかどうかによって、完全に決定される。

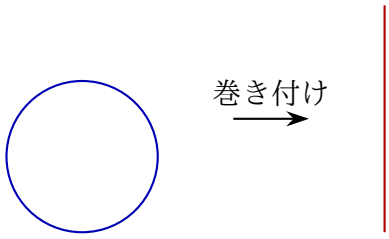
この理論を用いることで、「e^{-x^2} の積分が初等関数で書けないこと」や、「ベッセル関数」や「ガンマ関数」といった特殊な関数がなぜ必要になるのかを、数学的に厳密に証明することができます。

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。

5.4　空間被覆のガロア理論 — 図形の「分解」

ガロアのアイデアが、代数とは一見すると全く異なる分野、図形の性質を研究する**トポロジー（位相幾何学）**の世界でも、そっくりな形で現れることを見てみましょう。

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「布」で覆って調べる、という考え方があります。この「布」を**被覆空間（ひふくくうかん）**と呼びます。例えば、円周（S^1）という図形を考えてみてください。この円周は、無限に長い一本の直線（$\mathbb{R}$）を、ぐるぐると巻き付けることで「覆う」ことができます。このとき、直線が被覆空間となります。



円周 S^1（空間 X）　直線 $\mathbb{R}$（被覆空間 $\tilde{X}$）

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ます。

ガロア理論とのアナロジー

古典ガロア理論		空間被覆理論
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 $\tilde{M}$
ガロア群 $Gal(L/K)$	$\longleftrightarrow$	**基本群 $\boldsymbol{\pi_1(X)}$**

空間の「穴」の情報を表す**基本群 $\boldsymbol{\pi_1(X)}$** 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「被覆空間」の様々な種類と、その空間の基本群 $\boldsymbol{\pi_1(X)}$ の「部分群」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。

この理論のおかげで、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。その裏に全く同じ「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。

5.5　数論との深い関係 — 素数の世界の法則

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。

皆さんは、「$5 = (1+2i)(1-2i)$」のように、普段「素数」だと思っている数が、複素数などを含むより広い数の世界（**代数体**）では、さらに分解できてしまう例を見たことがあるかもしれません。一方で、素数 3 は、この世界でも分解されず素数のままです。

体を拡大したとき、素数がどのように振る舞うのか。その法則は何か？

この、数論における中心的な問いに答えるための最も強力な武器が、ガロア理論なのです。考え方は、これまでと同じです。有理数体 $\mathbb{Q}$ に、例えば $\sqrt{-1}$ を添加した体 $\mathbb{Q}(i)$ のような代数体を考え、そのガロア群 $Gal(\mathbb{Q}(i)/\mathbb{Q})$ を調べます。

ガロア群と素数

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、完全に予言される。

具体的には、各素数 p に対応する**フロベニウス元**と呼ばれるガロア群の特別な元が、その素数

の振る舞いのすべてを支配しています。素数がどのように分解されるかという数論の問題が、ガロア群の元の性質を調べるという代数の問題に、見事に翻訳されるのです。

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「アーベル拡大」のすべてを完璧に記述する、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。そこでは、ガロア群が、数論の世界だけでなく、調和解析や幾何学といった全く異なる分野の対象と、深いレベルで結びついていることが示唆されています。

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。

5.6　情報・符号理論への応用

最後に、ガロアの理論が現代社会で最も身近な形で応用されている例を見てみましょう。皆さんが普段何気なく使っている技術、例えば、

- 傷のついた CD や DVD でも、問題なく音楽や映像が再生できる。
- QR コードの一部が隠れたり汚れたりしていても、スマートフォンで正しく読み取れる。
- 遥か彼方の宇宙探査機から、ノイズの多い電波に乗って正確なデータが地球に届く。

これらのことを可能にしているのは、**「誤り訂正符号（あやまりていせいふごう）」**と呼ばれる技術であり、その心臓部にはガロアの理論から生まれた数学が使われています。

この技術の主役は、**有限体（ゆうげんたい）**または**ガロア体（ガロアたい）**と呼ばれる、元が有限個しかない特殊な体です。これはガロア自身が発見したもので、例えば $\{0, 1, 2, \ldots, p-1\}$（p は素数）の世界で、矛盾なく四則演算を定義したものです。

ガロア体と誤り訂正符号

デジタルデータ（0 と 1 の列）を、このガロア体上の数字の列と見なします。そして、元のデータに「冗長性」を持たせるような数学的な処理を施したものを、実際に送信・記録します。この処理のルールが「符号」です。
もし途中でデータの一部が失われたり、エラーが発生したりしても、ガロア体の持つ美しい代数構造を利用することで、受信側で「本来あるべきだった正しいデータ」を数学的に復元することができるのです。

特に、**リード・ソロモン符号**と呼ばれる強力な誤り訂正符号は、ガロア体の上で定義される多項式の性質を巧みに利用したもので、CD や DVD、QR コード、デジタル放送、データストレージなど、現代のデジタル技術に無くてはならない存在となっています。

19 世紀初頭、一人の若き数学者が純粋な知的好奇心から探求した、方程式の根の対称性という極めて抽象的な理論。それが、150 年以上の時を経て、私たちのデジタル社会の信頼性を根底から

支える技術として花開いたのです。これは、基礎科学の持つ、予測不能で計り知れない価値を物語る、最も美しい実例の一つと言えるでしょう。

これで、ガロアのアイデアを巡る私たちの長い旅は終わりです。一つの素朴な疑問から始まった道が、いかに豊かで広大な世界に繋がっているか、その一端を感じていただけたなら幸いです。