5次多項式 $x^5 - x^4 + 1$ の Galois 群の決定と Dedekind の定理

概要とインフォーマルな解説：

この記事では、有理数体 $\mathbb{Q}$ 上の5次多項式 $f(x) = x^5 - x^4 + 1$ の Galois 群を決定するプロセスを詳細に解説します。有限体上の還元（モジュロ演算）や多項式の判別式といった基本的な計算手法から出発し、最終的に Galois 群が5次対称群 S_5 になることを見事に証明します。

また、その理論的支柱となる「Dedekind の定理」についても、代数的整数論の基礎事項を交えながら自己完結的 (self-contained) な証明を与えています。抽象的な理論が具体的な方程式の解の対称性を見事に暴き出す、Galois 理論の醍醐味をお楽しみください。なお、以下の数学的な定義や証明は、厳密性を保つために「だ・である調」で記述します。

1. 基礎概念の定義と準備

具体的な計算に入る前に、議論の前提となるいくつかの代数学の基本概念を定義しておく。

定義: 既約 (irreducible) と可約 (reducible)

体 K 上の多項式 $f(x)$ が、より次数の低い2つの K 係数多項式の積として $f(x) = g(x)h(x)$ と表せないとき、その多項式は K 上で**既約 (irreducible)** であるという。逆に、そのような積に分解できる場合は**可約 (reducible)** であるという。

定義: 最小分解体 (splitting field) と Galois 群 (Galois group)

多項式 $f(x) \in \mathbb{Q}[x]$ のすべての根 $\alpha_1, \dots, \alpha_n$ を有理数体に添加した体 $L = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ を $f(x)$ の**最小分解体 (splitting field)** と呼ぶ。体拡大 $L/\mathbb{Q}$ の自己同型群を **Galois 群 (Galois group)** と呼び、$\mathrm{Gal}(L/\mathbb{Q})$ で表す。この群の各元は根の置換を引き起こすため、自然に n 次対称群 (symmetric group) S_n の部分群 $\mathrm{Gal}(L/\mathbb{Q}) \subset S_n$ と見なすことができる。

2. $\pmod 3$ における $f(x)$ の既約性

多項式 $f(x) = x^5 - x^4 + 1$ が、要素数 3 の有限体 $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, -1\}$ 上において既約 (irreducible) であることを示す。

$f(x)$ は5次式であるため、もし $\mathbb{F}_3$ 上で可約 (reducible) であると仮定すると、その因数分解には必ず**1次式**または**2次式**が含まれなければならない（因数の次数の和が $5 = 1 + 4 = 2 + 3$ となるため）。したがって、$f(x)$ が1次因数も2次因数も持たないことを示せば、既約性が証明される。

ステップ1：1次因数を持たないことの証明

因数定理より、多項式が1次因数を持つことと、その体に根を持つことは同値である。有限体の要素全体（乗法群 $\mathbb{F}_3^\times = \mathbb{F}_3 \setminus \{0\}$ の元と 0）を $f(x)$ に代入し、$\pmod 3$ で 0 になるか確認する。

- $x = 0$ のとき： $f(0) = 0^5 - 0^4 + 1 = 1 \not\equiv 0 \pmod 3$
- $x = 1$ のとき： $f(1) = 1^5 - 1^4 + 1 = 1 \not\equiv 0 \pmod 3$
- $x = -1$ のとき： $f(-1) = (-1)^5 - (-1)^4 + 1 = -1 - 1 + 1 = -1 \equiv 2 \not\equiv 0 \pmod 3$

いずれの場合も根とならないため、$f(x)$ は1次因数を持たない。

ステップ2：2次因数を持たないことの証明

もし $f(x)$ が2次因数を持つならば、$\mathbb{F}_3$ 上のモニックな既約2次多項式で割り切れるはずである。モニック2次多項式 $x^2 + ax + b$ $(a, b \in \mathbb{F}_3)$ のうち既約なものを探す。定数項 $b = 0$ だと x を因数に持ち可約となるため、$b = 1$ または $b = -1$ である。これらに $x = 0, 1, -1$ を代入し、根を持たないものを抽出すると以下の3つが得られる。

1. $p_1(x) = x^2 + 1$
2. $p_2(x) = x^2 + x - 1$
3. $p_3(x) = x^2 - x - 1$

これらで $f(x)$ を割った余りが 0 にならないことを確認する。割り算の代わりに剰余環 $\mathbb{F}_3[x]/(p_i(x))$ での計算、すなわち $p_i(x) \equiv 0$ として次数を下げる方法を用いる。

- **$p_1(x) = x^2 + 1$ の場合：** $x^2 \equiv -1$ となる。
  $x^4 \equiv 1, x^5 \equiv x$ より、$f(x) \equiv x - 1 + 1 = x \not\equiv 0$。
- **$p_2(x) = x^2 + x - 1$ の場合：** $x^2 \equiv -x + 1$ となる。
  $x^3 \equiv x(-x + 1) = -x^2 + x \equiv -(-x + 1) + x = 2x - 1 \equiv -x - 1$
  $x^4 \equiv x(-x - 1) = -x^2 - x \equiv -(-x + 1) - x = -1$
  $x^5 \equiv -x$

よって、$f(x) \equiv -x - (-1) + 1 = -x + 2 \equiv -x - 1 \not\equiv 0$。

- $p_3(x) = x^2 - x - 1$ **の場合：** $x^2 \equiv x + 1$ となる。
  $x^3 \equiv x(x+1) = x^2 + x \equiv (x+1) + x = 2x + 1 \equiv -x + 1$
  $x^4 \equiv x(-x+1) = -x^2 + x \equiv -(x+1) + x = -1$
  $x^5 \equiv -x$
  よって、$f(x) \equiv -x - (-1) + 1 = -x + 2 \equiv -x - 1 \not\equiv 0$。

すべての既約2次多項式で割り切れないため、$f(x)$ は2次因数を持たない。以上より、$f(x)$ は $\pmod 3$ で既約 (irreducible) である。

3. $\pmod 2$ における $f(x)$ の素因子分解

次に、要素数 2 の有限体 $\mathbb{F}_2 = \{0, 1\}$ 上において $f(x)$ の素因子分解 (prime factorization) を行う。$\mathbb{F}_2$ では $-1 \equiv 1$ であるため、$f(x) \equiv x^5 + x^4 + 1 \pmod 2$ となる。

まず1次因数（根）の有無を確認する。

- $x = 0$ のとき、$f(0) = 1 \not\equiv 0 \pmod 2$
- $x = 1$ のとき、$f(1) = 1 + 1 + 1 = 3 \equiv 1 \not\equiv 0 \pmod 2$

根を持たないため、1次因数は存在しない。したがって、可約であるとすれば「2次式 $\times$ 3次式」の形に分解される。

$\mathbb{F}_2$ 上のモニック既約2次多項式を探す。定数項は 1 でなければならず、$x^2 + 1$ は $(x+1)^2$ と可約であるため、根を持たない唯一の既約2次多項式は $x^2 + x + 1$ のみである。
実際に多項式の割り算（筆算）を実行すると、次のように割り切れる。

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

商として得られた3次多項式 $g(x) = x^3 + x + 1$ の既約性を確認する。3次式が可約であれば必ず1次因数（根）を持つが、$g(0) = 1 \not\equiv 0$、$g(1) = 3 \equiv 1 \not\equiv 0$ より根を持たない。ゆえに $g(x)$ も既約である。
結論として、$\pmod 2$ における素因子分解は以下の通りとなる。

$$f(x) \equiv (x^2 + x + 1)(x^3 + x + 1) \pmod 2$$

4. 多項式の判別式と計算

> **定義: 判別式 (discriminant) と終結式 (resultant)**

> n 次モニック多項式 $f(x)$ の根を $\alpha_1, \ldots, \alpha_n$ とするとき、判別式 $\Delta(f)$ は根の差の積の平方 $\prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$ として定義される。これは導関数 $f'(x)$ との Sylvester 終結式 (resultant) $R(f, f')$ を用いて、$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f')$ と計算できる。終結式は $R(f, g) = \mathrm{lc}(g)^{\deg f} \prod_{g(\beta)=0} f(\beta)$（ただし $\mathrm{lc}(g)$ は g の最高次係数）という性質を持つ。

今回 $n = 5$ より、符号は $(-1)^{10} = 1$ となり $\Delta(f) = R(f, f')$ である。$f(x) = x^5 - x^4 + 1$ の導関数は $f'(x) = 5x^4 - 4x^3 = 5x^3(x - \frac{4}{5})$ である。これより $f'(x)$ の根は $x = 0$ （3重根）と $x = \frac{4}{5}$ である。

終結式の性質を用いて計算すると：

$$R(f, f') = 5^5 \cdot \{f(0)\}^3 \cdot f\left(\frac{4}{5}\right)$$

それぞれの値を計算する。

- $f(0) = 1$
- $f\left(\frac{4}{5}\right) = \left(\frac{4}{5}\right)^5 - \left(\frac{4}{5}\right)^4 + 1 = \frac{1024 - 1280 + 3125}{3125} = \frac{2869}{3125}$

これらを代入すると、$5^5 = 3125$ より分母が相殺され、

$$\Delta(f) = 3125 \cdot 1^3 \cdot \frac{2869}{3125} = 2869$$

となる。続いて素因数分解を行うと、$2869 \div 19 = 151$ を得る。$\sqrt{151} < 13$ であり、11 以下の素数 $\{2, 3, 5, 7, 11\}$ のいずれでも割り切れないため、151 は素数である。よって判別式の素因数分解は

$$\Delta(f) = 19 \times 151$$

となる。

5. Galois 群の決定

これまでの結果を統合し、最小分解体 L の Galois 群 $G = \mathrm{Gal}(L/\mathbb{Q})$ を決定する。ここで、次のセクションで証明する **Dedekind の定理** を用いる。

判別式が $\Delta(f) = 19 \times 151$ であるため、素数 $p = 2, 3$ は判別式を割り切らない。したがって、$\pmod 2$ および $\pmod 3$ での分解情報を Dedekind の定理に安全に適用することができる。

1. **5次巡回置換 (5-cycle) の存在：**
   $\pmod 3$ において $f(x)$ は次数 5 の既約多項式であった。Dedekind の定理より、G は長さ 5 の巡回置換 (cycle) を含む。これより $f(x)$ は $\mathbb{Q}$ 上でも既約であり、G は S_5 の推移的部分群 (transitive subgroup) であることがわかる。

2. **互換 (transposition) の存在：**
   $\pmod{2}$ において $f(x) \equiv (x^2+x+1)(x^3+x+1)$ と分解された。次数が2と3の既約因子の積であるため、Dedekind の定理より、G は巡回置換の型 (cycle type) が $(2,3)$ である元 $\sigma = \tau\rho$ を含む。ここで τ は長さ2の巡回置換（すなわち互換）、ρ は長さ3の巡回置換であり、互いの作用する要素の集合の積集合は空集合 $\varnothing$ である。
   互いに素な置換は可換であるため、σ の3乗を計算すると $\sigma^3 = \tau^3\rho^3$ となる。τ の位数は2、ρ の位数は3であるから、$\tau^3 = \tau$ かつ $\rho^3 = e$（単位元）となる。ゆえに $\sigma^3 = \tau$ となり、G は互換 τ を含むことが示された。

群論の定理として、「素数 q に対し、S_q の推移的部分群が互換を含むならば、その群は S_q 全体に一致する」という事実が知られている。本問では $q=5$ であり、条件をすべて満たすため、

$$\mathrm{Gal}(L/\mathbb{Q}) = S_5$$

であることが証明された。

6. Dedekind の定理の自己完結的 (self-contained) な証明

定理 (Dedekind)

整数係数のモニック多項式 $f(x)$ の判別式を $\Delta(f)$ とする。素数 p が $\Delta(f)$ を割り切らないとき、$f(x) \pmod{p}$ が $\mathbb{F}_p$ 上で次数 $d_1, d_2, \ldots, d_k$ の既約多項式の積に分解されるならば、$f(x)$ の $\mathbb{Q}$ 上の Galois 群 $G \subset S_n$ は、互いに素な巡回置換の積として巡回置換の型 (cycle type) が $(d_1, d_2, \ldots, d_k)$ である元を含む。

証明

多項式 $f(x) \in \mathbb{Z}[x]$ の $\mathbb{Q}$ 上の最小分解体を K とし、Galois 群を $G = \mathrm{Gal}(K/\mathbb{Q})$ とする。K の整数環 (ring of integers) を $\mathcal{O}_K$ とする。$f(x)$ の根 $\alpha_1, \ldots, \alpha_n$ はモニックな整数係数多項式の根であるため、代数的整数であり $\alpha_i \in \mathcal{O}_K$ を満たす。

有理素数 p の生成するイデアル $p\mathcal{O}_K$ の素イデアル分解を考え、その素イデアル (prime ideal) の1つを $\mathfrak{P}$ とする（$\mathfrak{P} \subset \mathcal{O}_K, \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$）。剰余体 (residue field) $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ は、有限体 $\mathbb{F}_p$ の有限次拡大体となる。

Galois 群 G は $\mathcal{O}_K$ の素イデアルに自然に作用する。$\mathfrak{P}$ をそれ自身に写す G の元からなる部分群を**分解群 (decomposition group)** と呼び、$D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ と定義する。$\sigma \in D_{\mathfrak{P}}$ は $k_{\mathfrak{P}}$ 上の自己同型を誘導するため、自然な群準同型 $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ が得られる。

定理の仮定 $p \nmid \Delta(f)$ は、多項式が重根を持たないこと、すなわち拡大 $K/\mathbb{Q}$ において素数 p が**不分岐**

(unramified) であることを意味する。代数的整数論の基本定理により、不分岐であることと ϕ の核である**惰性群 (inertia group)** $I_{\mathfrak{P}}$ が自明（$I_{\mathfrak{P}} = \{\mathrm{id}\}$）であることは同値である。さらに ϕ は全射であるため、同型 $D_{\mathfrak{P}} \cong \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ が成立する。

有限体の Galois 群 $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ は、元を p 乗する **Frobenius 自己同型 (Frobenius automorphism)** $\mathrm{Frob}_p(x) = x^p$ によって生成される巡回群である。この同型対応により、$D_{\mathfrak{P}} \subset G$ の中に Frob_p に対応する唯一の元 $\sigma_{\mathfrak{P}}$ が存在する。これを Frobenius 元と呼び、すべての $x \in \mathcal{O}_K$ に対して $\sigma_{\mathfrak{P}}(x) \equiv x^p \pmod{\mathfrak{P}}$ を満たす。

次に、この $\sigma_{\mathfrak{P}}$ の根 α_i に対する作用を調べる。$\pmod{\mathfrak{P}}$ での還元を $\bar{\alpha}_i = \alpha_i \pmod{\mathfrak{P}}$ と表す。$p \nmid \Delta(f)$ より、還元された多項式 $\bar{f}(x)$ も $\mathbb{F}_p$ 上で重根を持たない。すなわち $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ は $k_{\mathfrak{P}}$ においてすべて相異なる。このため、α_i に対する $\sigma_{\mathfrak{P}}$ の置換作用と、$\bar{\alpha}_i$ に対する Frob_p の置換作用は完全に同型になる：

$$\sigma_{\mathfrak{P}}(\alpha_i) = \alpha_j \iff \mathrm{Frob}_p(\bar{\alpha}_i) = \bar{\alpha}_j$$

有限体 $\mathbb{F}_p$ 上で $\bar{f}(x)$ が既約多項式 $\bar{g}_m(x)$ の積に分解されているとする。$\bar{\alpha}_i$ はいずれかの $\bar{g}_m(x)$ の根である。$\bar{g}_m(x)$ は $\mathbb{F}_p$ 係数なので、$\mathrm{Frob}_p(x) = x^p$ を作用させても $\bar{g}_m(x)$ の根の集合はそれ自身に写される。$\bar{g}_m(x)$ が次数 d_m の既約多項式であることから、その根に Frob_p を繰り返し適用すると d_m 回で元に戻り、その部分集合上で長さ d_m の巡回置換として作用する。

全体として、根の集合 $\{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\}$ は各 $\bar{g}_m(x)$ の根の集合という互いに素な（共通部分が $\varnothing$ である）部分集合に分割され、Frob_p はそれぞれの部分集合上で長さ $d_1, \ldots, d_k$ の巡回置換として作用する。元の Galois 群 G に含まれる $\sigma_{\mathfrak{P}}$ も全く同じ置換構造を持つため、その巡回置換の型は $(d_1, d_2, \ldots, d_k)$ となる。これで定理が証明された。■

参考文献

- Milne, J. S. (2022). *Fields and Galois Theory*. Kea Books. Available at https://www.jmilne.org/math/Books/FT0.pdf (Chapter 4, Theorem 4.34 を参照)