

素数 p に対するある多項式のGalois群の決定

本稿では、素数 p に対する特定の p 次多項式の有理数体 $\mathbb{Q}$ 上での Galois群 (Galois group) が、対称群 S_p になることの完全な証明を与える。議論の飛躍をなくし、自己完結的 (self-contained) な解説となるよう、基礎となる概念の定義や定理の証明、具体例の計算から詳述する。

1. 問題設定

素数 p に対して、以下の $\mathbb{Q}$ 係数多項式 $f(X)$ を考える。

$$f(X) = X^3 \prod_{k=1}^{p-3} (X - 2k) - 2$$

ここで、積の記号 $\prod$ は $p = 3$ のとき空積となるため、1 とみなす。このとき、多項式 $f(X)$ の $\mathbb{Q}$ 上の Galois群が p 次対称群 S_p と同型になることを証明する。

2. 基礎概念と定理の準備

定義 1 (Galois群 / Galois group)

多項式 $f(X) \in \mathbb{Q}[X]$ の分解体を K とするとき、体の拡大 $K/\mathbb{Q}$ の自己同型群 $\text{Gal}(K/\mathbb{Q})$ のことを $f(X)$ の Galois群と呼ぶ。Galois群は、多項式 $f(X)$ の根の置換群として自然に作用する。

定義 2 (推移的 / transitive)

群 G が集合 X に作用しているとする。任意の $x, y \in X$ に対して、ある $g \in G$ が存在して $g \cdot x = y$ となるとき、この作用は推移的 (transitive) であるという。既約多項式の Galois群は、その多項式の根の集合に対して推移的に作用する。

定理 3 (Eisensteinの判定法 / Eisenstein's criterion)

整数係数多項式 $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ について、ある素数 q が存在して以下の3条件を満たすとき、 $f(X)$ は $\mathbb{Q}$ 上既約である。

- $q \nmid a_n$ (最高次の係数は q で割り切れない)
- すべての $0 \leq i \leq n-1$ について $q \mid a_i$ (それ以外のすべての係数は q で割り切れる)
- $q^2 \nmid a_0$ (定数項は q^2 で割り切れない)

定理 4 (Cauchyの定理 / Cauchy's theorem)

有限群 G の位数が素数 p で割り切れるならば、 G は位数 p の要素を持つ。

補題 5 (対称群の生成)

p を素数とする。 p 次対称群 S_p の部分群 G が、推移的 (transitive) に作用し、かつ互換 (transposition) と長さ p の巡回置換 (p -cycle) を含むならば、 $G = S_p$ である。

補題5の証明

G は互換 τ と長さ p の巡回置換 σ を含むとする。要素を適当に並べ替えることで、 $\sigma = (1, 2, \dots, p)$ と仮定してよい。このとき、 $\tau = (a, b)$ ($1 \leq a < b \leq p$) と表せる。

$k = b - a$ とおく。 p は素数であるから、 k は p と互いに素であり、 σ^k もまた長さ p の巡回置換である。要素を再度並べ替え、 σ^k の作用を新たな $(1, 2, \dots, p)$ と見なすことで、 $\tau = (1, 2)$ と仮定して一般性を失わない。

ここで $\sigma\tau\sigma^{-1}$ を計算すると、 $(\sigma(1), \sigma(2)) = (2, 3)$ となる。同様に $\sigma^m\tau\sigma^{-m}$ を順次計算することで、すべての隣接互換 $(1, 2), (2, 3), \dots, (p-1, p)$ が G に含まれることがわかる。

任意の互換は隣接互換の積で表される。例えば $(1, 3) = (2, 3)(1, 2)(2, 3)$ である。対称群 S_p は互換全体によって生成されるため、すべての互換を含む G は S_p 全体に一致する。

■

3. 具体例による観察

一般の証明に入る前に、直観的な理解を深めるため、 $p = 3$ および $p = 5$ の場合を具体的に観察する。

例1: $p = 3$ の場合

積の部分が空積となるため、 $f(X) = X^3 - 2$ である。この方程式の根は実数根 $\sqrt[3]{2}$ が1つと、虚数根 $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (ω は1の原始3乗根) の2つである。

Eisensteinの判定法 (素数 $q = 2$) より $\mathbb{Q}$ 上既約であり、分解体 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の拡大次数は6である。根の集合 $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ に対する複素共役は、虚数根の2つを入れ替え、実数根を固定する。すなわち互換として作用する。群の位数が6であり、推移的かつ互換を含むため、Galois群は S_3 に一致する。

例2: $p = 5$ の場合

$p = 5$ のとき、 $2(p-3) = 4$ であるから、多項式は $f(X) = X^3(X-2)(X-4) - 2$ となる。展開すると $f(X) = X^5 - 6X^4 + 8X^3 - 2$ である。

$g(X) = X^5 - 6X^4 + 8X^3$ とおくと、導関数は $g'(X) = 5X^4 - 24X^3 + 24X^2 = X^2(5X^2 - 24X + 24)$ となる。 $g'(X) = 0$ の根は $X = 0$ (重複度2) と、 $5X^2 - 24X + 24 = 0$ の解である $X = \frac{12 \pm \sqrt{24}}{5} \approx 1.42, 3.38$ である。

各極値における $g(X)$ の値を概算する。極大値をとる $X \approx 1.42$ では、 $g(1.42) \approx 4.2 > 2$ となる。極小値をとる $X \approx 3.38$ では $g(3.38) < 0$ となる。したがって、関数 $y = g(X)$ のグラフは直線 $y = 2$ と区間 $(0, 2)$ で2回、区間 $(4, \infty)$ で1回交わる。これにより $f(X) = 0$ は実数根をちょうど3つ持ち、残りの2つは複素共役な虚数根となる。実数根の個数が $5 - 2 = 3$ 個となることが確認できる。

4. 一般の素数 p に対する証明

与えられた多項式 $f(X) = X^3 \prod_{k=1}^{p-3} (X - 2k) - 2$ について、Galois群が S_p となることを以下の3つのステップで完全に証明する。

ステップ 1: $f(X)$ の $\mathbb{Q}$ 上での既約性

関数 $g(X)$ を $g(X) = f(X) + 2 = X^3 \prod_{k=1}^{p-3} (X - 2k)$ と定義する。 $g(X)$ を展開した式を以下のように表す。

$$g(X) = X^p + c_{p-1}X^{p-1} + \cdots + c_3X^3$$

$g(X)$ の非ゼロの根は $2, 4, \dots, 2(p-3)$ であり、これらはすべて偶数である。根と係数の関係により、係数 c_m ($3 \leq m \leq p-1$) はこれらの偶数の基本対称式を用いて表される。したがって、すべての c_m は 2 の倍数である。

$f(X)$ を係数ごとに書き下すと以下のようになる。

$$f(X) = X^p + c_{p-1}X^{p-1} + \cdots + c_3X^3 + 0 \cdot X^2 + 0 \cdot X - 2$$

素数 $q = 2$ に対して Eisenstein の判定法を適用する。

1. 最高次の係数は 1 であり、2 で割り切れない。
2. それ以外の係数 $c_{p-1}, \dots, c_3$ および 0 はすべて 2 の倍数である。
3. 定数項は -2 であり、2 で割り切れるが、 $2^2 = 4$ では割り切れない。

以上より、定理3 (Eisensteinの判定法) から、 $f(X)$ は $\mathbb{Q}$ 上既約であることが示された。

ステップ 2: 実数根と虚数根の個数の評価

$f(X) = 0$ の根、すなわち $g(X) = 2$ を満たす実数根の個数を調べる。 $p = 3$ の場合は例1で既に実数根が1個、虚数根が2個であることが示されているため、以下では $p \geq 5$ を仮定する。

1. $g'(X)$ の根の分布

$g(X)$ は $X = 0$ を重複度3の根として持ち、さらに $X = 2, 4, \dots, 2(p-3)$ を単純根として持つ。相異なる根は $1 + (p-3) = p-2$ 個存在する。Rolleの定理 (Rolle's theorem) より、各区間 $(0, 2), (2, 4), \dots, (2p-8, 2p-6)$ の内部に、導関数 $g'(X)$ の根が少なくとも1つ存在する。これらの区間は $(p-3)$ 個あるため、ここで $p-3$ 個の実数根が得られる。

また、 $g(X)$ は X^3 を因数に持つため、 $X = 0$ は $g'(X)$ の重複度2の根である。 $g'(X)$ の次数は $p-1$ 次であるから、これまでに見つかった $2 + (p-3) = p-1$ 個の根が $g'(X)$ のすべての根である。したがって、各区間 $(2j, 2j+2)$ において $g'(X)$ の根はちょうど1つであり、 $g(X)$ はその区間でただ1つの極値を持つ。

2. 極値の評価

各区間内での $g(X)$ の極値の符号を調べる。区間 $(2j, 2j+2)$ 内の任意の x について、 $x - 2k$ は $k \leq j$ ならば正、 $k \geq j+1$ ならば負である。負の因数の個数は $(p-3) - j$ 個となる。 p は奇素数であるため $p-3$ は偶数であり、 $g(X)$ の符号は $(-1)^{p-3-j} = (-1)^{-j} = (-1)^j$ と一致する。

すなわち、 j が偶数のとき $g(X) > 0$ となり極大値を持ち、 j が奇数のとき $g(X) < 0$ となり極小値を持つ。

$j \in \{0, 2, \dots, p-5\}$ を満たす偶数 j について、区間 $(2j, 2j+2)$ の中点 $x = 2j+1$ における $|g(x)|$ の値を評価する。

$$|g(2j+1)| = (2j+1)^3 \prod_{k=1}^{p-3} |2j+1-2k|$$

- $j = 0$ のとき: $|g(1)| = 1^3 \cdot \prod_{k=1}^{p-3} |1-2k| = 1 \cdot 3 \cdot 5 \cdots (2p-7) = (2p-7)!!$ である。 $p \geq 5$ より $2p-7 \geq 3$ なので $|g(1)| \geq 3 > 2$ となる。

- $j \geq 2$ のとき: $(2j+1)^3 \geq 5^3 = 125 > 2$ であり、残りの積部分は整数の積であるため1以上である。したがって $|g(2j+1)| > 2$ となる。

以上より、偶数 j に対応する各区間において $g(X)$ の極大値は 2 より厳密に大きい。

3. $g(X) = 2$ の実数根の個数

中間値の定理 (intermediate value theorem) と $g(X)$ の単調性から、 $g(X) = 2$ は各偶数 j の区間 $(2j, 2j+2)$ にちょうど2つの実数根を持つ。該当する偶数 j は $0, 2, \dots, p-5$ の $\frac{p-3}{2}$ 個存在するため、ここから $2 \times \frac{p-3}{2} = p-3$ 個の実数根が得られる。

奇数 j の区間では極小値が負であり、 $g(x) < 0$ を保つため根を持たない。定義域の両端については以下の通りである。

- $x < 0$ では $g'(x) > 0$ かつ $g(0) = 0$ なので $g(x) < 0$ となり、根を持たない。
- $x > 2p-6$ では $g'(x) > 0$ かつ $g(2p-6) = 0$ なので単調増加し、 $g(x) \rightarrow \infty$ となる。したがって $g(X) = 2$ はこの範囲でただ1つの実数根を持つ。

結論として、 $f(X)$ の実数根の総数は $(p-3) + 1 = p-2$ 個となる。代数学の基本定理より $f(X)$ は複素数体 $\mathbb{C}$ 上で p 個の根を持つため、残りの2つの根は互いに複素共役な虚数根である。

ステップ 3: Galois群の決定

$f(X)$ の $\mathbb{Q}$ 上の Galois群を $G = \text{Gal}(K/\mathbb{Q})$ とする（ここで K は $f(X)$ の分解体である）。

ステップ1より $f(X)$ は $\mathbb{Q}$ 上既約であるため、 G は $f(X)$ の p 個の根からなる集合 X に推移的 (transitive) に作用する対称群 S_p の部分群であるとみなせる。

既約多項式の分解体 K は $\mathbb{Q}$ の p 次拡大体を部分体として含むため、拡大次数 $[K:\mathbb{Q}] = |G|$ は p の倍数である。したがって定理4 (Cauchyの定理) より、 G は位数 p の要素を持つ。 S_p における位数 p の要素は、長さ p の巡回置換 (p -cycle) に限られる。

さらにステップ2より、 $f(X)$ の根のうちちょうど2つが虚数根であり、残りの $p-2$ 個は実数根である。複素共役をとる自己同型 $\sigma: \mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$ を分解体 K に制限した写像 $\sigma|_K$ は、 G の要素である。この自己同型は $p-2$ 個の実数根をすべて固定し、2つの虚数根のみを入れ替えるため、根の置換群 S_p の部分群として見たとき、まさに互換 (transposition) として作用する。

以上により、 G は推移的であり、かつ長さ p の巡回置換と互換を含む S_p の部分群であることが示された。補題5より、 $G = S_p$ であることが結論付けられる。

■

5. 引用文献

- [1] Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). John Wiley and Sons. [Publisher's Page](#)
- [2] Serre, J.-P. (1992). *Topics in Galois Theory*. Research Notes in Mathematics. A K Peters/CRC Press. <https://indico.math.cnrs.fr/event/11410/attachments/4760/7351/SerreTopicsGaloisTheory.pdf>