特定の5次方程式のGalois群が交代群 A_5 となることの完全な証明

本稿では、特定の5次多項式が有理数体 $\mathbb{Q}$ 上で交代群 (alternating group) A_5 を Galois群として持つことの完全な証明を与えます。証明の核となる既約性の厳密な確認、完全平方となる判別式の系統的な構成法、S_5 の推移的部分群の分類、および Dedekind の定理を用いた有限体上での具体的な因数分解を詳細に記述します。

対象となる4つの5次多項式

本稿で証明の対象とする、判別式が平方数となる x^5+ax+b 型の多項式は以下の4つです。

- **最初の例：** $f_1(x) = x^5 + 20x + 16$
- **具体例1：** $f_2(x) = x^5 + 20x + 32$
- **具体例2：** $f_3(x) = x^5 + 95x + 76$
- **具体例3：** $f_4(x) = x^5 + 220x + 176$

1. 有理数体上の既約性の完全な証明

これらの方程式の Galois群が5次対称群 S_5 の推移的部分群となるためには、多項式が有理数体 $\mathbb{Q}$ 上で既約であることが必須です。ここでは各多項式の既約性を証明します。

> **具体例2 ($x^5 + 95x + 76$) と 具体例3 ($x^5 + 220x + 176$) の既約性証明 (Eisensteinの判定法)**
>
> 整数係数多項式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ について、ある素数 p が存在して「すべての a_i が p の倍数」「最高次係数は p の倍数でない」「定数項 a_0 は p^2 の倍数でない」を満たすとき、その多項式は $\mathbb{Q}$ 上既約である（アイゼンシュタインの判定法）。
>
> - **具体例2 ($x^5 + 95x + 76$)：**
> $95 = 5 \times 19$、$76 = 4 \times 19$ である。素数 $p = 19$ に注目すると、係数 95 と 76 はともに 19 で割り切れる。また、定数項 76 は $19^2 = 361$ では割り切れない。したがって、Eisensteinの判定法により $\mathbb{Q}$ 上で既約である。
> - **具体例3 ($x^5 + 220x + 176$)：**
> $220 = 20 \times 11$、$176 = 16 \times 11$ である。素数 $p = 11$ に注目すると、係数 220 と 176 はともに 11 で割り切れる。また、定数項 176 は $11^2 = 121$ では割り切れない。したがって、Eisensteinの判定法により $\mathbb{Q}$ 上で既約である。
>
> □

> **最初の例 ($x^5 + 20x + 16$) と 具体例1 ($x^5 + 20x + 32$) の既約性証明 (有限体への還元)**
>
> これらの多項式には直接 Eisensteinの判定法を適用できる素数がないため、素数 $p = 3$ を法とする有限体 $\mathbb{F}_3$ 上での既約性を確認する。
>
> - **最初の例 ($x^5 + 20x + 16$)：**
>   法 3 で還元すると $x^5 + 2x + 1$ となる。
> $x = 0, 1, 2$ を代入すると、それぞれ $1, 4 \equiv 1, 32 + 4 + 1 \equiv 1 \pmod 3$ となり根を持たないため、1次の因数を持たない。

2次の因数を持つか確認するため、$\mathbb{F}_3$ 上のすべての2次既約多項式 $(x^2+1, x^2+x+2, x^2+2x+2)$ で割った余りを計算する。
$(x^5+2x+1) = (x^2+1)(x^3-x) + 1$ (余り 1)
$(x^5+2x+1) = (x^2+x+2)(x^3-x^2+2x) + x + 1$ (余り $x+1 \neq 0$)
$(x^5+2x+1) = (x^2+2x+2)(x^3+x^2+2x) + x + 1$ (余り $x+1 \neq 0$)
いずれも割り切れないため2次因数も持たない。したがって $\mathbb{F}_3$ 上で既約であり、元の多項式も $\mathbb{Q}$ 上既約である。

- **具体例1 ($x^5+20x+32$)：**
  法 3 で還元すると x^5+2x+2 となる。
  $x=0,1,2$ を代入すると、それぞれ $2, 5 \equiv 2, 32+4+2 \equiv 2 \pmod 3$ となり根を持たないため、1次の因数を持たない。
  同様に2次既約多項式で割る。
  $(x^5+2x+2) = (x^2+1)(x^3-x) + 2$ (余り 2)
  $(x^5+2x+2) = (x^2+x+2)(x^3+2x^2+2x) + x + 2$ (余り $x+2 \neq 0$)
  $(x^5+2x+2) = (x^2+2x+2)(x^3+x^2+2x) + x + 2$ (余り $x+2 \neq 0$)
  割り切れないため、これも $\mathbb{F}_3$ 上で既約であり、$\mathbb{Q}$ 上既約である。

□

2. 判別式の確認

多項式 $f(x) = x^5 + ax + b$ の判別式 Δ は、公式 $\Delta = 256a^5 + 3125b^4$ で与えられる。4つの例について判別式を計算し、完全平方であることを確認する。

多項式	a	b	判別式 Δ の素因数分解	完全平方か
$x^5+20x+16$	20	16	$2^{16} \cdot 5^6 = (2^8 \cdot 5^3)^2$	はい
$x^5+20x+32$	20	32	$2^{18} \cdot 5^6 = (2^9 \cdot 5^3)^2$	はい
$x^5+95x+76$	95	76	$2^{10} \cdot 5^6 \cdot 19^4 = (2^5 \cdot 5^3 \cdot 19^2)^2$	はい
$x^5+220x+176$	220	176	$2^{16} \cdot 3^2 \cdot 5^6 \cdot 11^4 = (2^8 \cdot 3 \cdot 5^3 \cdot 11^2)^2$	はい

3. 判別式が平方数となる x^5+ax+b 型多項式の構成法

ここで対象としている多項式群はランダムなものではなく、意図的に判別式が完全平方となるよう構成されています。ここではその生成メカニズムを示します。

> **命題 (平方判別式を持つ係数のパラメータ化)**
> 任意の整数 t に対して、係数 a, b を次のように定める：
>
> $$a = 5(5t^2-1), \quad b = 4(5t^2-1)$$
>
> このとき、多項式 x^5+ax+b の判別式 Δ は常に有理数体上で完全平方となる。

> **構成の導出と証明.**
>
> x^5+ax+b の判別式は $\Delta = 4^4a^5 + 5^5b^4$ である。
> ここで、a と b に共通のパラメータ k を導入し、$a=5k$、$b=4k$ と置く。判別式に代入すると、
>
> $$\Delta = 4^4(5k)^5 + 5^5(4k)^4 = 4^4 \cdot 5^5 \cdot k^5 + 5^5 \cdot 4^4 \cdot k^4$$

> 共通因数 $4^4 \cdot 5^5 \cdot k^4$ でくくり出すと、
>
> $$\Delta = 4^4 \cdot 5^5 \cdot k^4(k+1) = (16 \cdot 25 \cdot k^2)^2 \cdot 5(k+1) = (400k^2)^2 \cdot 5(k+1)$$
>
> 前半の $(400k^2)^2$ は平方数であるため、残りの部分 $5(k+1)$ が平方数になれば全体が完全平方となる。
> ある整数 t を用いて $5(k+1) = 25t^2$ と置くと、
>
> $$k+1 = 5t^2 \implies k = 5t^2 - 1$$
>
> これを元の式に戻せば、目的のパラメータ化 $a = 5(5t^2-1), b = 4(5t^2-1)$ を得る。
>
> □

この構成法に t を代入すると、検証中の具体例が生成されます。

- $t=1$： $k=4 \implies a=20, b=16$ (最初の例 $x^5+20x+16$)
- $t=2$： $k=19 \implies a=95, b=76$ (具体例2 $x^5+95x+76$)
- $t=3$： $k=44 \implies a=220, b=176$ (具体例3 $x^5+220x+176$)

4. S_5 の推移的部分群の分類

既約な5次多項式の Galois群は、根に対して推移的に作用するため、S_5 の推移的部分群となります。共役を除くと以下の5種類しか存在しません。

群の名称	記号	位数	A_5 に含まれるか（偶置換のみか）
巡回群 (Cyclic group)	Z_5	5	**はい**
二面体群 (Dihedral group)	D_5	10	**はい**
フロベニウス群 (Frobenius group)	F_{20}	20	いいえ
交代群 (Alternating group)	A_5	60	**はい**
対称群 (Symmetric group)	S_5	120	いいえ

判別式が完全平方である事実から、Galois群は表のうち Z_5, D_5, A_5 のいずれかに絞り込まれます。

5. Dedekindの定理と $(1,1,3)$ 型の素因数分解の明示

> **命題 (Dedekind の定理)**
> $f(x) \in \mathbb{Z}[x]$ をモニック多項式とする。判別式を割り切らない素数 p を法として $f(x)$ を有限体 $\mathbb{F}_p$ 上で因数分解したとき、その既約因子の次数が $(n_1, n_2, \ldots, n_k)$ であれば、$f(x)$ の Galois群はサイクル型が $(n_1, n_2, \ldots, n_k)$ である置換を含む。

群を A_5 と特定させるためには、長さ3の巡回置換（位数3の元）の存在を示す必要があります。以下の通り、すべての例において、判別式を割り切らない適切な素数 p を選ぶことで $\mathbb{F}_p$ 上で $(1,1,3)$ 型に分解されることを示します。

> **最初の例： $x^5+20x+16$ (素数 $p=7$)**
> $p=7$ は $\Delta = 2^{16} \cdot 5^6$ を割り切らない。

法 7 において $20 \equiv -1, 16 \equiv 2$ より、$x^5 - x + 2 \equiv 0 \pmod 7$。
$x = 4, x = 5$ は根である（$4^5 - 4 + 2 \equiv 0, 5^5 - 5 + 2 \equiv 0 \pmod 7$）。
$(x-4)(x-5) \equiv x^2 - 2x - 1 \pmod 7$ で割ると、

$$x^5 - x + 2 \equiv (x-4)(x-5)(x^3 + 2x^2 + 5x + 5) \pmod 7$$

3次式 $x^3 + 2x^2 + 5x + 5$ は $\mathbb{F}_7$ 上で根を持たないため既約。したがって分解型は $(1, 1, 3)$ である。

具体例1： $x^5 + 20x + 32$ **(素数** $p = 67$**)**
$p = 67$ は $\Delta = 2^{18} \cdot 5^6$ を割り切らない。
$\mathbb{F}_{67}$ において、$x = 3$ および $x = -4$ は根となる（$f_2(3) = 335 = 67 \times 5 \equiv 0$、
$f_2(-4) = -1072 = 67 \times (-16) \equiv 0 \pmod{67}$）。
$(x-3)(x+4) = x^2 + x - 12$ で元の多項式を多項式の除算で割ると、

$$x^5 + 20x + 32 \equiv (x-3)(x+4)(x^3 - x^2 + 13x - 25) \pmod{67}$$

この3次式 $x^3 - x^2 + 13x - 25$ は $\mathbb{F}_{67}$ 上で根を持たず既約である。したがって分解型は $(1, 1, 3)$ である。

具体例2： $x^5 + 95x + 76$ **(素数** $p = 31$**)**
$p = 31$ は $\Delta = 2^{10} \cdot 5^6 \cdot 19^4$ を割り切らない。
法 31 において、$95 \equiv 2$、$76 \equiv 14$ より $x^5 + 2x + 14 \pmod{31}$。
$x = 8$ および $x = -10 \equiv 21$ が根である。
$(x-8)(x+10) = x^2 + 2x - 80 \equiv x^2 + 2x + 13 \pmod{31}$ で割ると、

$$x^5 + 95x + 76 \equiv (x-8)(x+10)(x^3 - 2x^2 - 9x + 13) \pmod{31}$$

3次式 $x^3 - 2x^2 - 9x + 13$ は $\mathbb{F}_{31}$ 上で根を持たないため既約。したがって分解型は $(1, 1, 3)$ である。

具体例3： $x^5 + 220x + 176$ **(素数** $p = 13$**)**
$p = 13$ は $\Delta = 2^{16} \cdot 3^2 \cdot 5^6 \cdot 11^4$ を割り切らない。
法 13 において、$220 \equiv 12$、$176 \equiv 7$ より $x^5 + 12x + 7 \pmod{13}$。
$x = 3$ と $x = 4$ が根となる（$f_4(3) \equiv 243 + 36 + 7 = 286 = 13 \times 22 \equiv 0$ など）。
$(x-3)(x-4) = x^2 - 7x + 12 \equiv x^2 + 6x - 1 \pmod{13}$ で割ると、

$$x^5 + 220x + 176 \equiv (x-3)(x-4)(x^3 + 7x^2 + 11x + 6) \pmod{13}$$

3次式 $x^3 + 7x^2 + 11x + 6$ に $\mathbb{F}_{13}$ の元を代入しても 0 にならないため既約。したがって分解型は $(1, 1, 3)$ である。

6. 結論

以上のすべての数学的検証を統合します。

1. 対象となる4つの5次方程式はすべて有理数体上で既約です。これにより、その Galois群 G は5次対称群 S_5 の推移的部分群となります。
2. すべての判別式が完全平方であるため、G は交代群 A_5 の部分群でなければなりません。候補は A_5, D_5 (位数10), Z_5 (位数5) の3つに限定されます。
3. Dedekind の定理と、各多項式に対して具体的に提示した法 p での $(1, 1, 3)$ 型の因数分解から、G は必ず長さ3の巡回置換（位数3の元）を含みます。D_5 と Z_5 は位数が3の倍数ではないため、位数3の元を含み得ず棄却されます。

ゆえに、提示された4つの例はすべて、その Galois群が交代群 A_5 と同型であることが完全に証明されました。