

ガロア理論における多項式のガロア群の決定と有限体への還元

本稿では、有理数体上の多項式のガロア群 (Galois group) を決定する手法について、具体的な結果（命題や定理）とその完全な証明、および理解を助ける自己完結的 (self-contained) な解説と具体例を展開する。特に、多項式の実根の個数からのアプローチや、有限体への還元を用いる強力な手法について詳細に論じる。

1. 基礎概念の準備

本題に入る前に、以降の議論で暗黙のうちに用いられるガロア理論および代数的整数論の基本概念を定義しておく。これにより、証明の論理的な構造を明確にする。

定義 1.1: 最小分解体とガロア群

体 K 上の多項式 $f(X) \in K[X]$ に対し、 $f(X)$ が一次式の積に完全に分解され、かつそのすべての根によって生成される K の拡大体を **最小分解体 (splitting field)** と呼び、 K_f などと表す。 K の標数が 0 であるか、有限体である場合、 K_f/K はガロア拡大となる。この拡大の自己同型群 $\text{Gal}(K_f/K)$ を、 $f(X)$ の K 上の **ガロア群 (Galois group)** と呼ぶ。

定義 1.2: 分離的多項式と判別式

多項式 $f(X)$ が代数閉包において重根をもたないとき、**分離的 (separable)** であるという。モニック多項式 $f(X) = \prod_{i=1}^n (X - \alpha_i)$ の **判別式 (discriminant)** $D(f)$ は次のように定義される。

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

$D(f) \neq 0$ であることと、 $f(X)$ が分離的であることは同値である。判別式は根の対称式であるため、ガロア群の作用で不変であり、基礎体 K に属する（整数係数の場合は $\mathbb{Z}$ に属する）。

定義 1.3: 分解群と惰性群

代数体 L の代数的整数環を O_L とする。 $\mathbb{Z}$ の素イデアル $p\mathbb{Z}$ の O_L における素イデアル分解の 1 つの因子を $\mathfrak{p}$ とおく。ガロア群 $G = \text{Gal}(L/\mathbb{Q})$ の部分群であって、 $\mathfrak{p}$ を不変にするものの全体を **分解群 (decomposition group)** と呼び、 $D_{\mathfrak{p}}$ と表す。

$$D_{\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

さらに、剰余体 $O_L/\mathfrak{p}$ 上の恒等写像を引き起こす $D_{\mathfrak{p}}$ の元の全体を **惰性群 (inertia group)** と呼び、 $I_{\mathfrak{p}}$ と表す。 p が $L/\mathbb{Q}$ で不分岐であるとき、 $I_{\mathfrak{p}}$ は自明群となる。

2. 素数次数の多項式と対称群に関する補題

以下の具体例の計算で共通して利用される、実根の個数に基づく強力な補題を証明する。

補題 2.1

素数 p を次数とする有理数体 $\mathbb{Q}$ 上の既約多項式 $f(X) \in \mathbb{Q}[X]$ が、複素数体 $\mathbb{C}$ においてちょうど $p - 2$ 個の実根と 2 個の虚根をもつならば、 $f(X)$ の $\mathbb{Q}$ 上のガロア群 G は、対称群 S_p と同型である。

補題 2.1 の証明

$f(X)$ の $\mathbb{C}$ における根の集合を $\Omega = \{\alpha_1, \alpha_2, \dots, \alpha_p\}$ とおく。ガロア群 G は根の集合 Ω の置換群として忠実に作用するため、対称群 S_p の部分群 $G \subset S_p$ と見なすことができる。

$f(X)$ は $\mathbb{Q}$ 上既約であるから、ガロア理論の基本定理より G は Ω 上に推移的 (transitive) に作用する。軌道・安定化群の定理より、 G の位数 $|G|$ は根の個数 $|\Omega| = p$ で割り切れる。ここでコーシーの定理 (Cauchy's theorem) を群 G に適用すると、 G は位数 p の元をもつことがわかる。対称群 S_p における位数 p の元は p 次巡回置換のみであるから、 G はある p 次巡回置換を含む。

一方、仮定より $f(X)$ はちょうど 2 個の虚根をもつ。これらを互いに複素共役な α_1, α_2 とし、残りの $p - 2$ 個の実根を $\alpha_3, \dots, \alpha_p$ とする。複素共役をとる自己同型を τ とすると、 τ は $\mathbb{C}$ の自己同型であり、 $f(X)$ の係数が実数 (有理数) であることから、根の集合 Ω を Ω に写す。したがって $\tau \in G$ である。

この τ の Ω 上の作用を考えると、実根 $\alpha_3, \dots, \alpha_p$ をすべて固定し、虚根 α_1 と α_2 のみを入れ替える。すなわち、 τ は Ω 上で互換 $(1\ 2)$ として作用している。

群論の基本的な事実として、対称群 S_p (ただし p は素数) において、 p 次巡回置換と 1 つの互換をともに含む部分群は、 S_p 全体に一致することが知られている。したがって、 $G = S_p$ である。

3. 具体的な多項式のガロア群 (例 2.35 とその拡張)

補題 2.1 を用いて、低次数の具体的な既約多項式のガロア群を決定する。

例 2.35 (I): $X^3 + 3X + 3$ のガロア群

$f(X) = X^3 + 3X + 3$ の $\mathbb{Q}$ 上のガロア群は S_3 である。

証明

アイゼンシュタインの既約性判定法 (Eisenstein's criterion) を素数 $p = 3$ に対して適用する。定数項 3 は 3 で割り切れ $3^2 = 9$ で割り切れない。1 次の係数 3 は 3 で割り切れる。最高次 X^3 の係数 1 は 3 で割り切れない。したがって、 $f(X)$ は $\mathbb{Q}$ 上既約である。

実変数 X の関数として $f(X)$ の増減を調べる。導関数は $f'(X) = 3X^2 + 3$ であり、すべての実数 X に対して $f'(X) > 0$ となる。ゆえに $f(X)$ は単調増加関数である。また、 $\lim_{X \rightarrow -\infty} f(X) = -\infty$ および $\lim_{X \rightarrow \infty} f(X) = \infty$ であるから、中間値の定理より $f(X) = 0$ は実数解をただ 1 つもつ。

$f(X)$ の次数は素数 3 であり、実根をちょうど $3 - 2 = 1$ 個もつため、残りの 2 根は虚根である。補題 2.1 より、 $f(X)$ のガロア群は S_3 に同型である。

■

例 2.35 (2): $X^5 - 16X + 2$ のガロア群

$g(X) = X^5 - 16X + 2$ の $\mathbb{Q}$ 上のガロア群は S_5 である。

証明

アイゼンシュタインの既約性判定法を素数 $p = 2$ に対して適用する。定数項 2 は 2 で割り切れ 4 で割り切れない。1 次の係数 -16 は 2 で割り切れる。 X^2, X^3, X^4 の係数は 0 であり 2 で割り切れる。最高次の係数 1 は 2 で割り切れない。したがって、 $g(X)$ は $\mathbb{Q}$ 上既約である。

導関数は $g'(X) = 5X^4 - 16$ である。 $g'(X) = 0$ を解くと、 $X^4 = 16/5$ より $X = \pm 2/\sqrt[4]{5}$ を得る。 $\alpha = 2/\sqrt[4]{5}$ とおく。ここで、 $1 < 5 < 16$ より $1 < \sqrt[4]{5} < 2$ であるから、 $1 < \alpha < 2$ が成り立つ。

$g(X)$ の極値の符号を評価する。極大値は $g(-\alpha) = -\alpha^5 + 16\alpha + 2$ である。 $\alpha^4 = 16/5$ を用いると、 $g(-\alpha) = -\alpha(16/5) + 16\alpha + 2 = \frac{64}{5}\alpha + 2 > 0$ となる。極小値は $g(\alpha) = \alpha^5 - 16\alpha + 2 = \alpha(16/5) - 16\alpha + 2 = -\frac{64}{5}\alpha + 2$ である。 $\alpha > 1$ であるから、 $-\frac{64}{5}\alpha + 2 < -\frac{64}{5} + 2 = -10.8 < 0$ となる。

$\lim_{X \rightarrow -\infty} g(X) = -\infty$ および $\lim_{X \rightarrow \infty} g(X) = \infty$ であることと、極大値が正、極小値が負であることから、中間値の定理により $g(X)$ は区間 $(-\infty, -\alpha)$ 、 $(-\alpha, \alpha)$ 、 (α, ∞) においてそれぞれ 1 つずつ、合計 3 つの実根をもつ。

$g(X)$ の次数は素数 5 であり、実根をちょうど $5 - 2 = 3$ 個もつため、残りの 2 根は虚根である。補題 2.1 より、 $g(X)$ のガロア群は S_5 に同型である。

■

類似例: $X^5 - 4X + 2$ のガロア群

論法が全く同じになる別の 5 次多項式の例として、 $f(X) = X^5 - 4X + 2$ を挙げる。この多項式の $\mathbb{Q}$ 上のガロア群も対称群 S_5 に同型である。

証明

Eisensteinの既約性判定条件を素数 $p = 2$ に対して適用する。定数項 2 は 2 で割り切れ 4 で割り切れない。1 次の係数 -4 と X^2, X^3, X^4 の係数 0 はすべて 2 で割り切れる。最高次係数 1 は 2 で割り切れない。したがって、 $f(X)$ は $\mathbb{Q}$ 上既約である。

導関数は $f'(X) = 5X^4 - 4$ である。 $f'(X) = 0$ を解くと、 $X = \pm \sqrt[4]{4/5}$ となる。 $\alpha = \sqrt[4]{4/5}$ とおく。 $4/5 < 1$

であるから $0 < \alpha < 1$ である。

極大値は $X = -\alpha$ のときであり、 $f(-\alpha) = -\alpha^5 + 4\alpha + 2 = \alpha(4 - \alpha^4) + 2$ となる。 $\alpha > 0$ かつ $4 - \alpha^4 = 4 - 4/5 = 16/5 > 0$ であるため、極大値 $f(-\alpha) > 0$ である。極小値は $X = \alpha$ のときであり、 $f(\alpha) = \alpha^5 - 4\alpha + 2 = \alpha(4/5 - 4) + 2 = -3.2\alpha + 2$ となる。ここで $\alpha = (0.8)^{0.25} > 0.8$ であるから（厳密には $0.8^4 = 0.4096 < 0.8$ ）、 $f(\alpha) < -3.2(0.8) + 2 = -2.56 + 2 = -0.56 < 0$ である。

極大値が正、極小値が負であるため、同様に $f(X)$ はちょうど 3 つの実根をもつ。次数 5 は素数であり、実根をちょうど $5 - 2 = 3$ 個もつため、補題 2.1 により、そのガロア群は S_5 となる。

■

4. 奇素数次数のパラメータ族（例 2.36）

任意の素数 p に対して、ガロア群が S_p となるような有理数体上の多項式を具体的に構成する。

例 2.36

p を奇素数とすると、多項式 $f(X) = X^3(X-2)(X-4)\cdots(X-2(p-3)) - 2$ は $\mathbb{Q}$ 上既約であり、ちょうど $p-2$ 個の実根をもつ。よってそのガロア群は S_p である。

証明

まず $f(X)$ の次数を確認する。積の部分 $\prod_{k=1}^{p-3}(X-2k)$ には X の 1 次式が $p-3$ 個掛け合わされている。これに X^3 を掛けるため、 $f(X)$ の次数は $3 + (p-3) = p$ である。したがって $f(X)$ は p 次多項式である。

[既約性の証明]

$f(X)$ を展開して $f(X) = X^p + a_{p-1}X^{p-1} + \cdots + a_1X + a_0$ とおく。定数項 a_0 は -2 である。元の形から、 X^3 が全体に掛けられているため、 $a_1 = a_2 = 0$ である。 $k \geq 3$ に対する係数 a_k は、 $X^3 \prod_{k=1}^{p-3}(X-2k)$ を展開した際の X^k の係数である。この積の各因子 $(X-2k)$ の定数項部分はすべて偶数であるため、展開して得られる係数 $a_3, \dots, a_{p-1}$ はすべて 2 の倍数となる。最高次 X^p の係数は 1 である。以上より、 $f(X)$ は定数項が 2 の倍数かつ 4 の倍数ではなく、最高次以外のすべての係数が 2 の倍数である。アイゼンシュタインの既約性判定法により、 $f(X)$ は $\mathbb{Q}$ 上既約である。

[実根の個数の証明]

$g(X) = X^3 \prod_{k=1}^{p-3}(X-2k)$ とおくと、 $f(X) = 0$ は $g(X) = 2$ と同値である。 $g(X)$ の実根は、0（3 重根）および $2, 4, \dots, 2(p-3)$ （すべて単根）である。区間 $(0, 2)$ および $(2k, 2k+2)$ ($k = 1, \dots, p-4$) のそれぞれにおいて、 $g(X)$ は両端点で 0 となる。ロルの定理 (Rolle's theorem) より、各区間の内部に導関数 $g'(X) = 0$ となる点が少なくとも 1 つ存在する。そのような区間は全部で $p-3$ 個あるため、 $g'(X) = 0$ となる相異なる正の実根が少なくとも $p-3$ 個存在する。また、0 は $g(X)$ の 3 重根であるから、0 は $g'(X) = 0$ の 2 重根である。 $g'(X)$ は $p-1$ 次多項式であるから、これらで $g'(X) = 0$ の $(p-3) + 2 = p-1$ 個の根がすべて実数として見つかったことになる。すなわち、極値をとる点はすべて実数である。

極値をとる正の点を小さい順に $y_0, y_1, \dots, y_{p-4}$ とおく。 $y_0 \in (0, 2)$ であり、 $y_k \in (2k, 2k+2)$ である。 $g(X)$ のグラフはこれらの区間で符号を交互に変える。特に、 X 軸の正の部分で極大となるのは、 $g(X)$ が正の値をとる区間 $(2i, 2i+2)$ (i は奇数) においてである。極大値が 2 よりも大きいことを示す。区間 $(2i, 2i+2)$ 内の整数点 $X = 2i+1$ における $g(X)$ の値を評価する。

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

この値は正の整数たちの積であり、特に最初の因子は $(2i+1)^3 \geq 3^3 = 27$ である。他の因子もすべて奇数の整数であるから絶対値は 1 以上である。したがって、 $g(2i+1) \geq 27 > 2$ となる。極大値はこの値以上であるから、すべての正の極大値は 2 よりも大きい。

一方、極小値をとる区間では $g(X) < 0 < 2$ である。したがって、 $g(X) = 2$ は、隣り合う極小値と極大値の間にちょうど 1 つの解をもつ。 $X \leq 0$ においては、項 $X^3 \leq 0$ であり、他の $(X-2k)$ の項はすべて負である。負の因子の数は $p-3$ 個であり、 p が奇素数であることから偶数個である。ゆえに $X < 0$ のとき $\prod (X-2k) > 0$ となり、 $g(X) < 0$ となる。したがって $X \leq 0$ に解はない。

区間 $(0, 2)$ での極小値 $g(y_0)$ は負であり、次の極大値 $g(y_1)$ は 2 より大きい。この間に解が 1 つある。最後の極小値 $g(y_{p-4}) < 0$ の右側では、 $g(X)$ は単調増加して ∞ に向かうため、そこにも解が 1 つある。解が一つずつ存在する区間は、全部で「極値の個数 $p-3$ 」から「両端の状況」を考慮してちょうど $p-2$ 個となる。したがって、 $f(X)$ はちょうど $p-2$ 個の実根をもつ。補題 2.1 によりそのガロア群は S_p となる。

■

理解を助ける例: $p = 5$ の場合の検証

上記の抽象的な構成がいかにうまく機能するかを実感するために、 $p = 5$ の場合を具体的に計算する。公式に $p = 5$ を代入すると、積の部分は $k = 1$ から $5 - 3 = 2$ までとなる。

$$f(X) = X^3(X-2)(X-4) - 2$$

展開すると $f(X) = X^5 - 6X^4 + 8X^3 - 2$ となる。これは Eisenstein の既約性判定条件 ($p = 2$) により $\mathbb{Q}$ 上既約である。

$g(X) = X^3(X-2)(X-4)$ とおく。導関数は $g'(X) = 5X^4 - 24X^3 + 24X^2 = X^2(5X^2 - 24X + 24)$ である。 $g'(X) = 0$ の正の根は $X = (12 \pm \sqrt{24})/5$ である。これらは $\beta_1 \approx 1.42$ および $\beta_2 \approx 3.38$ と近似できる。

β_1 は区間 $(0, 2)$ にあり、極大となる。評価のために $X = 1$ を代入すると、 $g(1) = 1^3(1-2)(1-4) = 3 > 2$ である。したがって極大値は確実に 2 より大きい。 β_2 は区間 $(2, 4)$ にあり、極小となる。評価のために $X = 3$ を代入すると、 $g(3) = 3^3(3-2)(3-4) = -27 < 0$ である。

極大値が 2 より大きく、極小値が 0 より小さいため、 $g(X) = 2$ のグラフは $Y = 2$ とちょうど 3 箇所で交わる。よって実根はちょうど $5 - 2 = 3$ 個となり、証明の挙動が完全に再現されている。

5. 可解な素数次方程式とアフィン変換群 (定理 2.37)

方程式が代数的に可解（根がベキ根で表される）であるという強い条件が、ガロア群の構造をどのように制限するかを示す。

定理 2.37 (Galois の遺稿)

$\text{char} K = 0$ とし、 $f \in K[X]$ を素数 p 次既約多項式とする。 f のすべての根がベキ根による表示をもてば、ガロア群 $\text{Gal}(f)$ は、 $\mathbb{F}_p$ のアフィン変換群

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in H, b \in \mathbb{F}_p \right\}$$

に同型である。ただし、 H は $\mathbb{F}_p^\times$ のある部分群である。

証明

f のガロア群を $G = \text{Gal}(f)$ とおく。 f のすべての根がベキ根による表示をもつという仮定は、方程式 $f(X) = 0$ が代数的に可解であることを意味する。基礎体 K の標数が 0 であるから、可解性の基本定理により、ガロア群 G は可解群 (solvable group) である。また、 f は既約多項式であるから、 G は f の p 個の根からなる集合 Ω の上に推移的に作用する。

G は可解群であるから、自明でないアーベル正規部分群 $N \subset G$ をもつ。 N は Ω 上に作用する。 N は G の正規部分群であり、 G が推移的であることから、 N のすべての軌道は同じ長さをもつ。その長さを d とすると、 d は $|\Omega| = p$ を割り切る。 p は素数であるから、 $d = 1$ または $d = p$ である。もし $d = 1$ ならば、 N は Ω の各点を固定することになり、忠実な作用から N は自明群 $\{\text{id}\}$ となってしまう。これは N が自明でないことに矛盾する。したがって $d = p$ であり、 N 自身が Ω 上に推移的に作用する。

アーベル群が推移的に作用する場合、その作用は正則 (regular) である (すなわち、各点の安定化部分群が自明となる)。これにより、 N の位数は $|\Omega| = p$ に等しい。位数 p の群は巡回群であるから、 $N \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ (加法群) となる。 Ω の要素を $\mathbb{F}_p$ の要素と同一視し、 N の作用を $\mathbb{F}_p$ 上の平行移動 $\tau_b : x \mapsto x + b$ ($b \in \mathbb{F}_p$) と見なすことができる。

任意の $\sigma \in G$ は正規部分群 N を自身に写す。すなわち、任意の平行移動 τ_b に対して、 $\sigma\tau_b\sigma^{-1} \in N$ となる。これは、 $\sigma\tau_b\sigma^{-1} = \tau_c$ となる $c \in \mathbb{F}_p$ が存在することを意味する。この対応 $b \mapsto c$ は $\mathbb{F}_p$ の自己同型であるから、ある $a \in \mathbb{F}_p^\times$ が存在して $c = ab$ と書ける。

したがって、任意の $x \in \mathbb{F}_p$ に対して、

$$\sigma(x + b) = \sigma(\tau_b(x)) = \tau_{ab}(\sigma(x)) = \sigma(x) + ab$$

が成り立つ。ここで $x = 0$ とおき、 $\sigma(0) = d$ とおくと、

$$\sigma(b) = \sigma(0) + ab = ab + d$$

となる。これは、 σ が $\mathbb{F}_p$ 上のアフィン変換 $b \mapsto ab + d$ として作用していることを示している。

よって、 G は $\mathbb{F}_p$ 上のアフィン変換群の部分群に同型である。アフィン変換群は行列を用いて

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

と表される。 G は平行移動全体 N を含むため、 b は $\mathbb{F}_p$ 全体を動く。一方、 a の取り得る値の集合を H とすると、 H は乗法群 $\mathbb{F}_p^\times$ の部分群となる。

■

理解を助ける例: $X^5 - 2$ のガロア群とアフィン変換

定理 2.37 の主張がいかに具体的に実現されるかを見るため、 $f(X) = X^5 - 2$ を考える。これは $\mathbb{Q}$ 上既約である。

$f(X)$ の根は $\sqrt[5]{2}$ と 1 の原始 5 乗根 $\zeta = e^{2\pi i/5}$ を用いて、 $\Omega = \{\sqrt[5]{2}\zeta^k \mid k \in \{0, 1, 2, 3, 4\}\}$ と表される。すべて

の根はベキ根で書けている。最小分解体 $L = \mathbb{Q}(\sqrt[5]{2}, \zeta)$ の $\mathbb{Q}$ 上の拡大次数は 20 であり、ガロア群 G の位数は 20 である。根を $\alpha_k = \sqrt[5]{2}\zeta^k$ と表記し、添字 k を有限体 $\mathbb{F}_5$ の元と見なす。

G は以下の 2 つの自己同型 σ と τ によって生成される。

- $\sigma(\sqrt[5]{2}) = \sqrt[5]{2}\zeta$ および $\sigma(\zeta) = \zeta$
- $\tau(\sqrt[5]{2}) = \sqrt[5]{2}$ および $\tau(\zeta) = \zeta^2$

根 α_k に対する作用を計算すると、

$$\sigma(\alpha_k) = \sigma(\sqrt[5]{2}\zeta^k) = (\sqrt[5]{2}\zeta)\zeta^k = \sqrt[5]{2}\zeta^{k+1} = \alpha_{k+1}$$

$$\tau(\alpha_k) = \tau(\sqrt[5]{2}\zeta^k) = \sqrt[5]{2}(\zeta^2)^k = \sqrt[5]{2}\zeta^{2k} = \alpha_{2k}$$

となる。 σ は添字に対して $k \mapsto k+1$ という「平行移動」、 τ は $k \mapsto 2k$ という「定数倍」を引き起こしている。任意の元は変換 $k \mapsto ak+b$ ($a \in \mathbb{F}_5^\times, b \in \mathbb{F}_5$) となり、 G がアフィン変換群に完全に一致することがわかる。

6. 有限体への還元とガロア群の決定 (命題 2.38)

有理数体上の多項式を有限体上へ還元 (reduction) することで、元のガロア群の情報を抽出する。この命題の完全な証明 (単射性と全射性) を詳細に行う。

命題 2.38

モニックな分離的整係数多項式 $f \in \mathbb{Z}[X]$ に対して、 $\bar{f} \in \mathbb{F}_p[X]$ を係数を素数 p を法として考えたものとする。 $\bar{f}$ も分離的ならば、 $\bar{f}$ の $\mathbb{F}_p$ 上のガロア群 $\text{Gal}((\mathbb{F}_p)_{\bar{f}}/\mathbb{F}_p)$ は、自然に f の $\mathbb{Q}$ 上のガロア群 $\text{Gal}(\mathbb{Q}_f/\mathbb{Q})$ の部分群と見なせる。

証明

$L = \mathbb{Q}_f$ を f の最小分解体とし、 $G = \text{Gal}(L/\mathbb{Q})$ をそのガロア群とする。 O_L を L の代数的整数環とする。 f の根 $\alpha_1, \dots, \alpha_n$ はすべて代数的整数であるから、 O_L に属する。素数 p が生成するイデアル pO_L の素イデアル分解を $pO_L = \mathfrak{P}_1 \dots \mathfrak{P}_g$ とする。一つ素イデアルを固定し、 $\mathfrak{P} = \mathfrak{P}_1$ とおく。

分解群を $D_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ とする。剰余体 $k_{\mathfrak{P}} = O_L/\mathfrak{P}$ を考える。 $\sigma \in D_{\mathfrak{P}}$ は $\mathfrak{P}$ を不変に保つため、任意の $x \in O_L$ について、 $\bar{\sigma}(x) = x \pmod{\mathfrak{P}}$ とするとき、 σ は $k_{\mathfrak{P}}$ 上の自己同型 $\bar{\sigma}$ を $\bar{\sigma}(x) = \overline{\sigma(x)}$ によって well-defined に引き起こす。これにより、自然な群準同型写像 $\phi: D_{\mathfrak{P}} \rightarrow \text{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ が $\phi(\sigma) = \bar{\sigma}$ として定義される。この ϕ が同型写像であることを示す。

(1) ϕ の単射性の証明

$\sigma \in \text{Ker}(\phi)$ を任意にとる。これは $\phi(\sigma)$ が恒等写像であり、任意の $x \in O_L$ に対して $\sigma(x) \equiv x \pmod{\mathfrak{P}}$ が成り立つことを意味する。根 α_i ($1 \leq i \leq n$) に対しても $\sigma(\alpha_i) \equiv \alpha_i \pmod{\mathfrak{P}}$ となる。一方、 σ は根を置換するため、ある j が存在して $\sigma(\alpha_i) = \alpha_j$ となる。すなわち $\alpha_j \equiv \alpha_i \pmod{\mathfrak{P}}$ であり、 $\alpha_j - \alpha_i \in \mathfrak{P}$ となる。

仮に $i \neq j$ と仮定する。 f の判別式 $D(f) = \prod_{k < l} (\alpha_k - \alpha_l)^2$ は、因子として $(\alpha_i - \alpha_j)^2$ を含むため、 O_L において $\alpha_j - \alpha_i$ の倍数である。ゆえに $D(f) \in \mathfrak{P}$ である。 $D(f)$ は $\mathbb{Z}$ の元であるから、 $D(f) \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ となり、 $D(f)$ は p の倍数となる。これは還元された多項式 $\bar{f}$ の判別式 $D(\bar{f})$ が $\mathbb{F}_p$ で 0 になることを意味し、 $\bar{f}$ が重根

をもつことになる。しかし仮定より $\bar{f}$ は分離的であるため矛盾である。したがって $i = j$ であり、すべての i に対して $\sigma(\alpha_i) = \alpha_i$ となる。 L は α_i たちで生成されるため、 $\sigma = \text{id}$ となり、単射性が示された。

(2) ガロア群の推移的な作用 (補題)

全射性を示す準備として、 G が素イデアルの集合 $\{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$ の上に推移的に作用することを確認する。ある $\mathfrak{P}_k$ が軌道に含まれないと仮定する。中国の剰余定理 (Chinese remainder theorem) により、 $x \equiv 0 \pmod{\mathfrak{P}_k}$ かつ任意の $\sigma \in G$ に対して $x \equiv 1 \pmod{\sigma(\mathfrak{P}_1)}$ を満たす $x \in O_L$ が存在する。ノルム $N_{L/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x)$ を考えると、 $x \in \mathfrak{P}_k$ より $N_{L/\mathbb{Q}}(x) \in \mathfrak{P}_k \cap \mathbb{Z} = p\mathbb{Z} \subset \mathfrak{P}_1$ である。 $\mathfrak{P}_1$ は素イデアルであるから、ある $\tau \in G$ について $\tau(x) \in \mathfrak{P}_1$ 、すなわち $x \in \tau^{-1}(\mathfrak{P}_1)$ となる。しかし構成条件より $x \equiv 1 \pmod{\tau^{-1}(\mathfrak{P}_1)}$ であるため矛盾である。よって作用は推移的である。

(3) ϕ の全射性の証明

$k_{\mathfrak{P}}$ は $\mathbb{F}_p$ の有限次分離拡大であるから、原始元定理より $k_{\mathfrak{P}} = \mathbb{F}_p(\bar{\alpha})$ となる原始元 $\bar{\alpha} \neq \bar{0}$ がとれる。中国の剰余定理により、 $\alpha \equiv \bar{\alpha} \pmod{\mathfrak{P}_1}$ かつ $i \geq 2$ に対して $\alpha \equiv 0 \pmod{\mathfrak{P}_i}$ を満たす $\alpha \in O_L$ を選ぶ。

多項式 $h(X) = \prod_{\sigma \in G} (X - \sigma(\alpha))$ を考える。 $h(X) \in \mathbb{Z}[X]$ であり、法 p での還元を $\bar{h}(X) \in \mathbb{F}_p[X]$ とおく。 $\bar{h}(\bar{\alpha}) = 0$ であるから、 $\bar{\alpha}$ の最小多項式 $m(X)$ は $\bar{h}(X)$ を割り切る。

$\text{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ の任意の元 $\bar{\tau}$ をとる。 $\bar{\tau}(\bar{\alpha})$ も $m(X)$ の根であるため、 $\bar{h}(X)$ の根となる。すなわち、ある $\sigma \in G$ が存在して $\overline{\sigma(\alpha)} = \bar{\tau}(\bar{\alpha})$ が成り立つ。

もし $\sigma \notin D_{\mathfrak{P}}$ ならば、 $\sigma^{-1}(\mathfrak{P}_1) = \mathfrak{P}_i$ ($i \geq 2$) となる (推移性より)。 α の構成から $\alpha \in \sigma^{-1}(\mathfrak{P}_1)$ 、すなわち $\sigma(\alpha) \in \mathfrak{P}_1$ となり、 $\overline{\sigma(\alpha)} = \bar{0}$ を得る。しかし $\bar{\tau}$ は同型であり $\bar{\alpha} \neq \bar{0}$ なので $\bar{\tau}(\bar{\alpha}) \neq \bar{0}$ となり矛盾する。よって $\sigma \in D_{\mathfrak{P}}$ である。

$\sigma \in D_{\mathfrak{P}}$ であるため $\phi(\sigma)$ が定義でき、 $\phi(\sigma)(\bar{\alpha}) = \overline{\sigma(\alpha)} = \bar{\tau}(\bar{\alpha})$ となる。生成元の上で一致するため $k_{\mathfrak{P}}$ 全体で $\phi(\sigma) = \bar{\tau}$ となり、全射性が示された。

以上より $D_{\mathfrak{P}} \cong \text{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ である。また O_L が f の根を含むため、 $k_{\mathfrak{P}}$ は $\bar{f}$ の最小分解体と一致し、 $\text{Gal}((\mathbb{F}_p)_{\bar{f}}/\mathbb{F}_p) \cong D_{\mathfrak{P}} \subset G$ と見なせる。

■

7. 還元定理と判別式を用いたガロア群の決定 (具体例)

命題 2.38 は、素数を変えて還元することで、ガロア群の様々な部分群 (あるいは置換の型) を見つけるための非常に強力な実践的道具となる。判別式の情報と組み合わせることで、完全な決定が可能になる。

応用例 1: $X^3 - X - 1$ のガロア群

$f(X) = X^3 - X - 1$ の $\mathbb{Q}$ 上のガロア群 G を決定する。 $G \subset S_3$ である。

法 $p = 2$ での還元 $\bar{f}_2(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$ は、 $\mathbb{F}_2$ の元 $0, 1$ を代入しても根をもたないため既約である。そのガロア群は位数 3 の巡回群であるから、命題 2.38 により G は 3 次巡回置換 (3-サイクル) を含む。

法 $p = 5$ での還元 $\bar{f}_5(X) \in \mathbb{F}_5[X]$ に $X = 2$ を代入すると 0 になる。因数分解すると $\bar{f}_5(X) = (X - 2)(X^2 + 2X + 3)$ となる。2 次因子 $X^2 + 2X + 3$ は $\mathbb{F}_5$ で根をもたず既約である。この還元され

た多項式のガロア群は位数 2 の巡回群であるから、命題 2.38 により G は互換 (2-サイクル) を含む。

$G \subset S_3$ は 3-サイクルと互換の両方を含むため、 $G = S_3$ である。

応用例 2: $X^5 - X^4 + 1$ のガロア群

より高度な例として、 $f(X) = X^5 - X^4 + 1$ の $\mathbb{Q}$ 上のガロア群 G を決定する。 $G \subset S_5$ である。

第1段：判別式の計算

モニック多項式 f の判別式は、導関数 $f'(X)$ との終結式 (resultant) を用いて

$D(f) = (-1)^{5 \cdot 4/2} \text{Res}(f, f') = \text{Res}(f, f')$ となる。 $f'(X) = 5X^4 - 4X^3 = X^3(5X - 4)$ の根は 0 と $4/5$ である。 $f(0) = 1$ 、 $f(4/5) = (4/5)^4(-1/5) + 1 = 2869/3125$ である。

$$D(f) = 5^5 \cdot (f(0))^3 \cdot f(4/5) = 3125 \cdot 1^3 \cdot \frac{2869}{3125} = 2869$$

2869 は有理数の平方数ではない。ガロア群 G が交代群 A_n に含まれるための必要十分条件は判別式が平方元であることなので、 $D(f)$ が平方数でないことから $G \not\subset A_5$ であり、 G は少なくとも1つの奇置換を含む。

第2段：法3での還元

$p = 3$ で還元した $\bar{f}_3(X) = X^5 + 2X^4 + 1 \pmod{3}$ は、 $\mathbb{F}_3$ の元を代入しても根をもたず、また $\mathbb{F}_3$ 上の 2 次既約多項式 ($X^2 + 1$, $X^2 + X + 2$, $X^2 + 2X + 2$) のいずれで割っても余りが出るため、 $\mathbb{F}_3$ 上既約である。命題 2.38 より、 G は長さ 5 の巡回置換 (5-サイクル) をもつ。

第3段：法2での還元

$p = 2$ で還元した $\bar{f}_2(X) = X^5 + X^4 + 1 \pmod{2}$ は、

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

と分解される。両因子は $\mathbb{F}_2$ で根をもたず既約である。命題 2.38 より、 G は長さ 2 の巡回置換と長さ 3 の巡回置換の積である元 τ をもつ。 τ の位数は 6 であり、 τ^3 を考えると、 G は 2-サイクル (互換) を含むことがわかる。

結論

対称群 S_5 の部分群が 5-サイクルと互換の両方を含むならば、 S_5 全体に一致することが群論により知られている。したがって $G = S_5$ である。これは判別式の情報 (奇置換を含む) とともに完全に整合している。

参考文献

堀田良之, 『可換環と体』, 岩波書店 (2006).

<https://www.iwanami.co.jp/book/b265842.html>

Serge Lang, *Algebra*, Revised Third Edition, Springer (2002).

<https://link.springer.com/book/10.1007/978-1-4613-0041-0>

J. S. Milne, *Fields and Galois Theory*, Course Notes (2022).

<https://www.jmilne.org/math/CourseNotes/FT.pdf>